ASTES

Advances in Science, Technology & Engineering Systems Journal

Special Issue

Innovation in Computing, Engineering Science & Technology

2024-25

www.astesj.com
ISSN: 2415-6698

EDITORIAL BOARD
(Special Issue)

Editor-in-Chief

Guest Editors

Editorial

The Special Issue on *Innovation in Computing, Engineering Science & Technology 2024–25* in the *Advances in Science, Technology and Engineering Systems Journal (ASTES Journal)* arrives at a pivotal moment when interdisciplinary integration and rapid technological evolution are reshaping both research and practice. Across computing, engineering science, and applied technologies, innovation is no longer confined to isolated domains; rather, it is driven by the convergence of intelligent systems, sustainable engineering, and data-centric methodologies. This issue reflects that transformation by bringing together contributions that explore emerging paradigms such as artificial intelligence–driven optimization, smart infrastructure, advanced materials, digital transformation, and next-generation communication systems. Collectively, these works underscore a shared objective: to translate theoretical advances into scalable, real-world solutions that address complex global challenges.

A defining feature of the contributions in this issue is their emphasis on applicability and societal relevance. Authors have demonstrated how innovative computational techniques ranging from machine learning models to distributed computing architectures are being integrated into engineering workflows to enhance efficiency, reliability, and adaptability. At the same time, engineering innovations presented here move beyond traditional boundaries, incorporating sustainability principles, energy efficiency considerations, and human-centered design. Whether in the development of smart cities, intelligent healthcare systems, or resilient industrial processes, the research highlights a shift toward solutions that are not only technically robust but also environmentally and socially responsible.

Equally noteworthy is the strong interdisciplinary character that permeates this collection. The challenges of the modern era climate change, urbanization, resource scarcity, and digital security cannot be addressed within siloed disciplines. The articles in this issue exemplify how collaborative approaches, combining expertise from computing, engineering, and applied sciences, can yield more holistic and impactful outcomes. This interdisciplinary synergy is particularly evident in areas such as cyber-physical systems, Internet of Things (IoT) applications, and data-driven engineering, where innovation emerges from the seamless integration of hardware, software, and analytical frameworks.

The Special Issue also reflects the growing importance of emerging technologies in shaping the future of research and industry. Advances in artificial intelligence, edge computing, blockchain technologies, and advanced manufacturing techniques are redefining how systems are designed, implemented, and maintained. The contributions herein not only explore these technologies but also critically examine their limitations, scalability, and ethical implications. Such balanced perspectives are essential to ensure that innovation proceeds responsibly and inclusively, with due consideration of security, privacy, and long-term societal impact.

From an editorial perspective, this issue represents a concerted effort to provide a platform for high-quality, forward-looking research that bridges theory and practice. The diversity of topics and methodologies reflects the journal's commitment to fostering a comprehensive understanding of innovation in science and engineering systems. It is our hope that the insights presented will inspire further research, encourage cross-disciplinary collaboration, and support the development of technologies that contribute meaningfully to global progress.

This Special Issue ultimately highlights that innovation is not a singular achievement but an ongoing process one that requires continuous exploration, critical evaluation, and collaborative engagement. By showcasing cutting-edge research and practical advancements, it contributes to the evolving dialogue on how computing, engineering science, and technology can collectively shape a more sustainable, efficient, and intelligent future.

Guest Editor

Prof. Nicolae Tudoroiu

ADVANCES IN SCIENCE, TECHNOLOGY AND ENGINEERING SYSTEMS JOURNAL

Special Issue **August 2024**

CONTENTS

Lightning Detection System for Wind Turbines Using a Large-Diameter Rogowski Coil
by Sarawuth Pramualsingha, Kazuo Yamamoto and RikutoTanaka

Utilizing 3D models for the Prediction of Work Man-Hour in Complex Industrial Products using Machine Learning
by Ahmet Emin Ünal, Halit Boyar, Burcu Kuleli Pak and Vehbi Çağrı Güngör

Advanced Fall Analysis for Elderly Monitoring Using Feature Fusion and CNN-LSTM: A Multi-Camera Approach
by Win Pa Pa San and Myo Khaing

Development and Application of Value Karuta to Understand Value in Lean Management: Initial Small-group Trial in Japan and the UK
by Tamao Kobayashi and Koichi Murata

Evaluation of a Classroom Support System for Programming Education Using Tangible Materials
by Koji Oda, Toshiyasu Kato and Yasushi Kambayashi

On Adversarial Robustness of Quantized Neural Networks Against Direct Attacks
by Abhishek Shrestha and Jürgen Großmann

True Random Number Generator Implemented in ReRAM Crossbar Based on Static Stochasticity of ReRAMs
by Tanay Patni and Abhijit Pethe

Hardware and Secure Implementation of Enhanced ZUC Steam Cipher Based on Chaotic Dynamic S-Box
by Mahdi Madani, El-Bay Bourennane and Safwan El Assad

A Study of the Digital Health Management Needs of the Elderly
by Ya Gao, Fatma Layas, Xiangyu Dong, Yijing Li and Jiayi Li

Energy Management Policy and Strategies in ASEAN
by Wai Yie Leong, Yuan Zhi Leong and Wai San Leong

Assistive System for Collaborative Assembly Task using Augmented Reality
by Woratida Sawangnamwong and Siam Charoenseang

ASTES

Advances in Science, Technology and Engineering Systems Journal
Vol. 9, No. 6, 01-11 (2024)
www.astesj.com
Special Issue on Innovation in Computing, Engineering Science & Technology

ASTES Journal
ISSN: 2415-6698

Utilizing 3D models for the Prediction of Work Man-Hour in Complex Industrial Products using Machine Learning

Ahmet Emin Ünal[*,1,2], Halit Boyar[1], Burcu Kuleli Pak[1], Vehbi Çağrı Güngör[3]

[1]*R&D Department, Adesso Turkey, Istanbul, 34398, Turkey*

[2]*Dept. of Comp. Engineering, Istanbul Technical University, Istanbul, 34485, Turkiye*

[3]*Dept. of Comp. Engineering, Abdullah Gül University, Kayseri, 38080, Turkiye*

ARTICLE INFO

Article history:
Received: 20 September, 2024
Accepted: 04 November, 2024
Revised: 05 November 2024
Online: 18 November, 2024

Keywords:
Complex Industrial Products
Metal Sheet Stamping
Work Man-hour Prediction
Machine Learning
Gradient Boosting

ABSTRACT

The integration of machine learning techniques in industrial production has the potential to revolutionize traditional manufacturing processes. In this study, we examine the efficacy of gradient-boosting machine learning models, specifically focusing on feature engineering techniques, applied to a novel dataset with 3D product models pertaining to work man-hours in metal sheet stamping projects, framed as a regression task. The results indicate that LightGBM and XGBoost surpass other models, and their effectiveness is further enhanced by employing feature selection and synthetic data generation methods. The optimized LightGBM model exhibited superior performance, achieving a MAPE score of 10.78%*, which highlights the effectiveness of gradient boosting mechanisms in handling heterogeneous data sets typical in custom manufacturing. Additionally, we introduce a methodology that enables domain experts to observe and critique the results through explainable AI visualizations.*

1. Introduction

This manuscript serves as an extension of a previous study on predicting work man-hours of complex industrial products, originally presented in 2023 4th International Informatics and Software Engineering Conference (IISEC) [1].

This study aims to contribute to the application of machine learning in industrial production by focusing on enhancing efficiency, productivity, and decision-making, specifically targeting work man-hour prediction in metal sheet stamping. By addressing this challenge, our research provides insights that fit within the broader scope of machine learning advancements in manufacturing. The integration of machine learning techniques in industrial production has the potential to revolutionize traditional manufacturing processes. Predictive systems for forecasting production and operational costs are crucial in shaping the future of machine learning applications in industrial production, and this study directly contributes to this important research area by focusing on work man-hour prediction.

In the field of complex industrial product management, where a custom configuration is needed for every product, accurately predicting the work man-hour for a product is essential for ensuring successful project completion. Rapid and precise responses to customer inquiries are crucial to maintaining competitiveness in the industry. However, given the complex and configurable nature of products, traditional methods of cost estimation may not provide the needed speed and accuracy. In the conventional approach, according to the domain knowledge of experts who shared the required dataset, they estimate the man-hour using customer requirements, 3D models, past similar projects, and a comprehensive analysis of the product. Traditional cost estimation methods have struggled to keep pace with the increased complexity and competitive environment of the industry, highlighting the need for more advanced approaches.

Recently, machine learning techniques have shown promising empirical results in improving the accuracy of various cost prediction models across many industrial sectors. This study builds upon these advancements by applying machine learning specifically to work man-hour prediction in the metal sheet stamping industry, addressing unique challenges in custom, short-run production. Recent studies have explored the application of machine learning in enhancing cost estimation in manufacturing processes. In [2], the authors applied back-propagation neural networks (BPN) and least squares support vector machines (LS-SVM) to address product life cycle cost estimation challenges, demonstrating the potential of ma-

[*]Corresponding Author: Ahmet Emin Ünal, Fax: +90 212 346 20 03, Phone: +90 212 346 20 02 & ahmet.unal@adesso.com.tr

chine learning in this area. Similarly, in [3], authors emphasized the importance of selecting a standard set of attributes for developing machine learning models for building project cost estimation, showcasing the advancements that machine learning offers in accurate cost estimation within the construction sector.

Research in [4] focused on explainable artificial intelligence for manufacturing cost estimation and machining feature visualization, indicating a growing interest in deep learning approaches for estimating manufacturing costs. In [5], authors proposed the use of two-dimensional (2D) and three-dimensional (3D) convolutional neural networks (CNN) for manufacturing cost estimation, highlighting the potential of deep learning methods in this context. In [6], authors explored early cost estimation in customized furniture manufacturing using machine learning, showcasing the application of machine learning for estimating costs in specific manufacturing niches. Furthermore, [7] discussed how intelligent job shop scheduling (JSS) systems, powered by machine learning and artificial intelligence solutions, aim to reduce costs based on specific cost functions, such as making span or economic cost. Additionally, [8] conducted an empirical study in the automotive industry, where they proposed machine learning as an advanced cost estimation method.

The use of neural networks in machining operations has been highlighted as advantageous in reducing uncertainties within the cost estimation process. In [9], authors emphasized the capacity of neural networks to enhance cost estimation accuracy in machining operations, showcasing the potential of machine learning in refining cost estimation models. In [10], authors compared various machine learning methods for estimating the manufacturing cost of jet engine components, displaying the effectiveness of different machine learning approaches in cost estimation for the aerospace industry. Moreover, in [11], authors developed methods for direct cost estimation in manufacturing parts, with recent studies leveraging deep learning techniques to predict manufacturing costs based on 3D CAD models. Additionally, [12] highlighted how machine learning improves prediction performance in surface generation and roughness in ultraprecision machining, emphasizing the role of machine learning in advancing automation and digitization in manufacturing processes.

Forecasting the work man-hour for producing complex industrial products poses distinct challenges. In contrast to conventional manufacturing methods that entail bulk production of identical units, often running into thousands or millions, metal sheet stamping operations are frequently tailored with short-run, tailored orders. This variability in design, materials, and processes complicates work man-hour estimations. Furthermore, the time-sensitive nature of such projects, combined with intense industry competition, demands swift and accurate cost estimates. The automotive sector serves as an example, predominantly employing manufacturing through sheet metal stamping projects [13].

The reliance on custom orders in the metal sheet stamping industry results in significant variability between projects, often leading to discrepancies in cost estimations. This variability complicates accurate cost prediction and underscores the importance of developing advanced estimation methods to mitigate financial and operational risks. An inaccurate prediction not only affects the financial bottom line but can also disrupt the broader supply chain, delay projects, and damage client relationships. In the worst cases, it may cause the rejection of profitable projects due to overestimated costs or the acceptance of unprofitable ones due to underestimations.

In the context of sheet metal stamping, where high production rates and cost-effectiveness are crucial factors, inaccurate cost predictions can result in suboptimal decision-making regarding material selection, tooling design, and process optimization [14]. This can lead to increased scrap rates, rework, and overall inefficiencies in the production line. Moreover, inaccurate cost predictions may also affect the competitiveness of manufacturers in the market, as cost overruns can erode profit margins and hinder the ability to offer competitive pricing [15]. Furthermore, inaccurate cost predictions in metal sheet stamping can impact the overall sustainability of manufacturing operations. For instance, if the estimated costs do not align with the actual expenses incurred during the stamping process, it can lead to increased waste generation, energy consumption, and environmental impacts [16]. This can undermine efforts to improve the environmental performance of manufacturing processes and reduce the overall carbon footprint of sheet metal stamping operations. Moreover, inaccurate cost predictions can also affect the quality and reliability of stamped metal parts. Suboptimal cost estimations may result in compromises in material selection, tooling quality, or process parameters, leading to variations in part dimensions, surface finish, or mechanical properties [17]. This can ultimately impact the functionality and performance of the stamped components, leading to potential quality issues and customer dissatisfaction.

Accurate cost predictions are essential for ensuring the economic viability, operational efficiency, and sustainability of metal sheet stamping processes. Inaccuracies in cost estimations can lead to significant issues, such as poor cost control, reduced competitiveness, increased environmental impact, and compromised product quality. Accurate predictions are crucial to prevent these issues, ensuring manufacturers can make informed decisions, maintain market competitiveness, and promote sustainable practices. This study aims to address these challenges by leveraging advanced machine learning techniques to enhance cost estimation accuracy in the metal sheet stamping process. Therefore, leveraging advanced cost estimation methods, such as machine learning algorithms or finite element modeling, can help mitigate the risks associated with inaccurate cost predictions and optimize the overall performance of sheet metal stamping processes.

The integration of machine learning in cost estimation processes within the manufacturing sector has shown significant promise in enhancing accuracy, efficiency, and decision-making. From product life cycle cost estimation to customized furniture manufacturing and jet engine component cost estimation, machine learning methods have demonstrated their versatility and effectiveness in optimizing cost estimation models. As manufacturing industries continue to deploy advanced technologies, the role of machine learning in cost estimation will become even more pivotal in driving operational excellence and cost-effectiveness.

In this study, we examine the efficacy of gradient-boosting machine learning models, specifically focusing on feature engineering techniques. We apply these methods to a novel dataset related to work man-hours in metal sheet stamping projects, framing the problem as a regression task. The results indicate that LightGBM and XGBoost surpass other models, and their effectiveness is further improved by employing feature selection and synthetic data generation

techniques.

Our study utilizes gradient boosting machine learning models, known for their efficacy with tabular data, and uniquely incorporates domain-specific knowledge tailored to the metal sheet stamping industry. This integration of expert insights and historical data aims to capture the unique challenges of custom, short-run production, setting our approach apart from general-purpose cost estimation models. This approach aims to enhance the predictive accuracy by integrating insights from historical data and expert analysis, tailored specifically to the nuances of metal sheet stamping.

A significant advancement in gradient boosting is the development of the XGBoost algorithm, known for its scalability and efficiency in building tree boosting models [18]. XGBoost, an integrated learning technique utilizing the gradient boosting algorithm, has been successfully applied in diverse industrial domains. For example, it has been used in predicting power demand for industrial customers [19] and transforming the used car market by accurately predicting prices [20]. The robustness and performance of XGBoost have been demonstrated in various applications, underscoring its effectiveness in industrial cost prediction tasks. Furthermore, the application of gradient boosting in industrial contexts extends to addressing specific challenges in cost prediction and optimization. NGBoost, a gradient boosting approach utilizing Natural Gradient, has been developed to tackle technical challenges in probabilistic prediction, thereby enhancing the accuracy and reliability of predictive models [21]. Additionally, diversified gradient boosting ensembles have been employed for predicting the cost of forwarding contracts, showcasing the versatility of gradient boosting methods in effectively handling regression and classification problems [22].

In the realm of energy consumption modeling, gradient boosting machines have been utilized to model the energy consumption of commercial buildings, demonstrating improved prediction accuracy compared to traditional regression models and random forest algorithms [23]. Similarly, in the context of cargo insurance frequency prediction, XGBoost has shown superior accuracy compared to other machine learning models, highlighting the efficacy of gradient boosting in diverse industrial prediction tasks [24].

The utilization of gradient boosting algorithms, such as XGBoost and LightGBM, has significantly impacted industrial cost prediction by enhancing prediction accuracy, scalability, and robustness in diverse industrial settings. From energy consumption modeling to customer attrition prediction, gradient boosting has emerged as a powerful tool for optimizing predictive models and improving decision-making processes in industrial cost estimation and optimization tasks. This study examines the effectiveness of gradient boosting machine learning models as well as feature engineering strategies on a new dataset concerning work man-hours in a metal sheet stamping project, framed as a regression task. The results indicate that LightGBM and XGBoost yield better performance compared to other models, and that feature selection along with synthetic data generation enhance the outcomes. The main aims of this research are as follows:

1. Compare the performance of different machine learning models and feature engineering techniques for work man-hour prediction in metal sheet stamping projects.
2. Identify key variables and features that contribute to the accuracy of work man-hour predictions.
3. Assess the integration of industry-specific knowledge into machine learning models, evaluating its impact on predictive accuracy.

The structure of this paper is outlined as follows: Section II reviews the existing research on various methodologies for forecasting work man-hours in industrial projects; Section III provides an explanation of the utilized dataset; Section IV provides a detailed account of the model experiments conducted during the study; Section V presents a discussion of the experimental findings; and Section VI offers concluding remarks.

2. Related Works

Various studies across industrial fields such as automotive, construction, and furniture manufacturing have explored the prediction of production costs, labor costs, and material costs using diverse machine learning methods. The application of these techniques varies significantly based on the industry's specifics and the nature of the available data, highlighting the need for industry-specific adaptations of general methodologies.

In [25], authors employed several machine learning models on wheel cost data of 1340 automobiles. After implementing feature selection techniques, their findings revealed that Support Vector Regression (SVR) achieved the highest R^2 value in the cross-validation set. Interestingly, Linear Regression (LR) scored better in the test set, which may suggest that simpler models can sometimes outperform more complex ones in less volatile environments. This finding is relevant to our research as it underscores the importance of evaluating model complexity in the context of specific data characteristics, which is crucial for optimizing cost prediction accuracy in our own study.

Voxelization is a fundamental process in feature extraction for cost prediction tasks, especially in industrial production settings. It involves converting 3D CAD models or point cloud data into a structured voxel grid, which is particularly important for enabling deep learning models like Convolutional Neural Networks (CNNs) to effectively process and analyze complex geometries. This process is crucial in our research as it allows us to capture detailed geometric features that directly impact cost prediction accuracy, especially in scenarios involving intricate part designs. By using voxelization, we can ensure that our models effectively learn from the geometric complexity of the industrial components, leading to more precise predictions. Various studies in computer science and point cloud processing emphasize the importance of voxelization in processing point cloud data for tasks like object detection and feature extraction [26, 27]. In the field of mechanical parts manufacturing, authors of [28] innovatively applied Convolutional Neural Networks (CNN) to predict manufacturing costs. By utilizing voxelization to transform 3D models into a trainable format, they achieved a mean absolute percentage error ($MAPE$) of 6.34%. This approach underscores the potential of advanced image processing techniques in enhancing feature extraction for cost prediction models. Voxel-based methods have shown particular success in the aerospace industry as well, where converting complex 3D geometries of jet engine components into voxel grids allows for more accurate cost estimation and defect

detection. Techniques like Fully Convolutional Networks (FCN) and autoencoders, as discussed in [29] and [30], further enhance voxel-based feature extraction for tasks such as object detection and image processing.

The furniture manufacturing industry also demonstrates the importance of early cost estimation due to its highly customizable nature. In [31], authors compared various algorithms, such as Extra Trees Regressors (ETR), Gradient Boosting Regressors (GBR), and Random Forest (RF) on data from 1026 products of a Lithuanian furniture manufacturer. The RF algorithm exhibited superior performance, achieving an R^2 score of 0.84, which highlights the effectiveness of ensemble methods in handling heterogeneous data sets typical in custom manufacturing.

Random Forest, as a versatile machine learning algorithm, excels at handling high-dimensional data and capturing complex relationships, making it ideal for cost prediction and optimization in industrial production. Its robust performance in classification and regression tasks supports accurate component classification and production cost prediction, essential in custom manufacturing [32]. Additionally, Random Forest has been instrumental in developing efficient predictive maintenance systems, enabling organizations to anticipate equipment failures, optimize maintenance schedules, and improve production performance [33]. Its interpretability is particularly beneficial in environments where stakeholders must understand the factors influencing costs or production outcomes, aiding decision-making processes [34]. Furthermore, Random Forest's capability to manage complex interactions and highly correlated variables makes it well-suited for settings with intricate production processes and variable interdependencies [35]. Given its flexibility and strong adaptability in real-world applications, Random Forest is a reliable choice to improve production efficiency and optimize cost prediction in the landscape of custom manufacturing [36]. These studies supports our methodology by demonstrating the value of using ensemble methods like Random Forest to effectively manage variability and complexity, similar to the challenges faced in our study of cost prediction for metal sheet stamping.

Parallel to our focus, in [37], authors developed an early cost estimation model specifically for stamping dies, employing Artificial Neural Networks (ANN), which demonstrated a deviation of 8.28% on test data. This study exemplifies the applicability of ANN in industries where data can be nonlinear and complex. ANNs excel in nonlinear cost estimation for custom manufacturing due to their ability to capture complex nonlinear relationships between variables and costs which is vital to model intricate scenarios [38, 39]. They surpass traditional methods in prediction accuracy, thus optimizing schedules and enhancing decision-making processes [39, 40]. Furthermore, ANNs adapt flexibly to changing data patterns, effectively managing the intricacies of custom manufacturing cost data [41, 42]. They are adept at extracting relevant features from complex datasets and recognizing hidden patterns, which is crucial for optimizing cost estimation models [43, 44]. Despite their complexity, efforts to enhance the interpretability of ANNs help provide transparency in the decision-making process [45, 44]. Ensemble methods involving ANN improve prediction accuracy and reduce errors, thus bolstering the robustness and reliability of models [46]. Furthermore, ANNs demonstrate excellent generalization to unseen data and maintain robust performance in diverse scenarios [47], significantly enhancing cost estimation processes, optimizing resource allocation, and supporting decision making in custom manufacturing environments. The capabilities of ANNs justify their use as a benchmark in managing the complex interactions and nonlinear relationships inherent in cost data for metal sheet stamping. By evaluating ANNs, we tried to find the best approach for achieving high prediction accuracy and reliability, thereby enhancing the efficiency of our cost estimation model.

Additional research efforts in man-hour prediction across various industries further enrich our understanding. For instance, In [48], authors targeted the power transformers manufacturing sector, comparing Support Vector Machines (SVM), Gaussian Process Regression (GPR), and Adaptive Neural Fuzzy Inference System (ANFIS) models. GPR was found to outperform the others in their dataset, potentially due to its effectiveness in managing noise and uncertainty in production data.

In [49], authors focused on the shipbuilding industry, implementing Multiple Linear Regression (MLR) and Classification and Regression Tree (CART) to predict man-hours in sub-processes. CART outperformed MLR, likely due to its superior handling of categorical and nonlinear data, which are common in such fragmented production processes.

In the construction sector, authors of [50] combined Random Forest (RF) and Linear Regression (LR) to predict Building Information Modeling (BIM) labor costs, finding that the hybrid approach outperformed individual methods. This suggests the potential benefits of methodological hybridization in enhancing prediction accuracy.

These studies collectively highlight the diverse applications and potential of machine learning in cost prediction across industries, informing our approach and methodology in the metal sheet stamping industry, where the challenges of custom, short-run production dominate.

Table 1: Comparison of Existing Studies for Man-hour Prediction of Industrial Products.

Dataset and Paper	SS	# of Features*	Best Model	Year
[37]	150	8	ANN	2014
[49]	300k	11	CART	2015
[51]	99	11	LS-SVM (PSO)	2015
[28]	400k	3D Voxels	CNN	2020
[50]	19	9	RF + LR	2020
[31]	1026	18	RF	2021
[25]	1340	>13	LR	2021
[48]	1249	9	GPR	2022
[52]	>8	4	LS-SVM (PSO)	2023
[53]	1605	10	LR	2023
[1]	4000	47	LightGBM (Optuna)	2023
Our	4890	47 + 3D	LightGBM (Optuna)	2024

SS: Sample Size, **Feature count prior to preprocessing operations*

3. Data

In this research, we utilized two distinct datasets pertaining to the output of sheet metal stamping parts to forecast the operational costs involved in the manufacturing process. These datasets encompass details on the product features as well as the die characteristics necessary for each operation. The primary variable of interest is the work man-hour for each operation, referred to as 'OperationCost.' These datasets were supplied by a sheet metal stamping company.

The supplied product information data set encompasses details regarding each individual product (or part). The data set comprises information on 875 products. It includes the following features:

- **InquiryID**: Distinct identifier assigned to each individual part inquiry.
- **SheetThickness**: Thickness of the metal sheet required for manufacturing the part, represented as a floating-point number.
- **NetX and NetY**: Dimensions of the sheet metal, specified as length and width, respectively.
- **ContourSize**: Size of the contour of the final manufactured part.
- **SurfaceArea**: Total surface area of the completed part.
- **SheetTsMax**: Measure of the tensile strength of the sheet material.
- **SheetElongation**: Attribute describing the elongation capacity of the metal sheet.
- **MetalHardness**: Categorical attribute denoting the hardness of the sheet metal, classified as Soft, Medium, or Hard.
- **Year**: The calendar year in which the inquiry quotation request was received.
- **YearDay**: The specific day of the year, ranging from 0 to 365, on which the inquiry was recorded.

The data set for operations encompasses details related to the attributes of the die and the operations required for the production of each product. The dataset comprises a total of 4000 operations, wherein each product is subjected to between 2 to 8 sequential operations, with certain operations potentially being carried out concurrently. The sub-operations are expressed as natural language strings, which had to be parsed with regex. The dataset features the following attributes:

- **OperationID**: A unique identifier assigned to each row within the operations dataset.
- **InquiryID**: An identifier corresponding to the specific part for which the operation is conducted.
- **OperationOrder**: An indicator of the arrangement of the operation within the manufacturing process.
- **PressTonnage**: The tonnage required in the press during the stamping process.
- **DieX, DieY, DieZ**: The dimensions (length, width, height) of the die.
- **DieWeight**: The weight of the die measured in kilograms.
- **DieFilling**: The percentage of the die's internal space that is filled.
- **Sub-operation features**: Boolean and integer features denoting the presence or frequency of various sub-operations (such as metal sheet blanking, shearing, bending, etc.) and other configurations relevant to the die. The string comprises a series of sub-operation types accompanied by the respective frequency of their execution, with each sub-operation type separated by a comma. Through the use of regular expressions to parse this string, we obtained a frequency list of the sub-operations, which was subsequently integrated into the dataset as die directions T, R, L (booleans indicating the die direction top, right, and left respectively); and sub-operation type execution counts. The sub-operations can be descripbed as:
  - **BLANK**: Cuts out a flat metal piece (blank) from a larger sheet, typically in the shape needed for further forming.
  - **SHEAR**: Cuts or trims metal along a straight or curved line to achieve specific dimensions or separate parts.
  - **BEND**: Deforms the sheet along a straight axis to create angles, folds, or flanges, turning flat sheets into 3D shapes.
  - **DRAW**: Pulls metal into a die cavity to form deep, hollow shapes, commonly used for creating cups or cylindrical parts.
  - **GAUGE**: Measures and controls the thickness of the sheet or part to ensure uniformity and adherence to specifications.
  - **WELD**: Joins two or more metal parts together, typically by applying heat or pressure, to create a single assembly.
  - **PROG (Progressive Stamping)**: Uses multiple stations in a single die to perform a sequence of operations (like blanking, bending, and drawing) on a single part as it moves through the press.
  - **OTHER**: Other infrequent sub-operation types within the dataset, such as coining, ironing, flanging, hemming, embossing, etc., are collected under this type.
- **work man-hour**: The man-hour of operation, serving as the target variable, which we seek to forecast.

For each set of operational data, the corresponding product information from the product dataset is appended. Consequently, this merging of datasets enables machine learning models to predict the work man-hours for each operation. Subsequently, professionals can integrate these costs to establish the target cost for the operations of a given product. There are numerous suboperations, characterized by interconnections among them. Following consultations

with domain experts, suboperations were categorized into primary groups.

Despite the comprehensive nature of the datasets, several data quality issues were identified that could potentially impact model performance. The distribution of the 'OperationCost' variable, our primary target, exhibited notable skewness, predominantly featuring lower values and discrete increments, often in multiples of 50. This pattern suggests possible label noise due to rounding or estimation practices in recording work man-hours. Additionally, the inclusion of operations with costs below 250 and above 3000 introduced potential sampling bias, as these extremes may represent atypical production scenarios or the involvement of subcontractors utilizing different procedures and equipment. Inconsistencies in the numerical representation of sub-operation counts and missing values in certain features necessitated careful data preprocessing and imputation strategies. These biases and noise within the dataset could lead to challenges such as model overfitting or underfitting, adversely affecting the generalization performance of the predictive models. Nonetheless, in this study, these anomalies were retained following preliminary data cleaning, as they are essential for the model to accommodate these atypical samples to ensure robust learning outcomes.

In the previous study [1], the number of samples was lower, which increased after newly processed and provided data samples from the data source. A better way to represent 3D products and the sequential nature of operations can be suggested to increase the performance of the models. Thus, in this study, we added features to represent 3D attributes of the parts. We were able to acquire some features after processing the STL files of each part. These features are volume of the part that is calculated after voxelization of the part, surface area of the part that is calculated directly from the mesh, and number of triangles in the part file (which was correlated with the complexity of the part).

For each sub-operation within the operations, there were inconsistent numerical representations of the step count. This value is incorporated as a new numeric feature when it is available and assigned a value of 0 in its absence. Additionally, the operation dataset is adjusted to include the aggregate count of subsequent and preceding suboperations to provide temporal context to the model. Furthermore, we enhance the whole feature set through the process of feature crossing, which involves the application of multiplicative combinations of pairs of features, as well as the inclusion of squared terms of individual features. Although this method results in an exponential increase in the total number of features, subsequent feature selection is used to mitigate the overall expansion. Specifically, we retain only the features whose importance exceeds the expected importance of the original features.

Given the characteristics of the manufacturing processes, data on certain sub-operation types exhibited imbalances and sparsity in the dataset. This hindered machine learning models from effectively generalizing these operations. To address this issue, we applied the Synthetic Minority Over-sampling Technique (SMOTE) [54] to create synthetic data for these underrepresented sub-operation types. By thoroughly analyzing the dataset's intrinsic patterns and relationships, such as interactions between product dimensions, material properties, and operational parameters, we ensured that the synthetic samples accurately reflected the complexities of real-world metal sheet stamping operations. Subsequently, we employed the Tomek-link method [55] to prune the synthetic data, thereby reducing noise and preventing potential overfitting. This approach not only augmented the dataset's diversity and volume but also led to a significant reduction in the mean absolute error (MAE) for the rare sub-process types, while the other sub-processes exhibited minimal changes. Consequently, the machine learning models were able to learn more generalized and nuanced patterns, improving their predictive performance on unseen data and enhancing their applicability in practical settings.

4. Methods

The data's label values are adjusted by a constant factor to enhance stability during training. Both categorical and numerical features have been reviewed with domain experts and tailored to suit the requirements of each algorithm. Following feature processing, new features are generated based on the data's sequential nature. These novel features encompass information on past and future operations for a single operational step. In the quotation process, experts determine sequential procedures, and similar operations may incur varying costs depending on their position within the sequence.

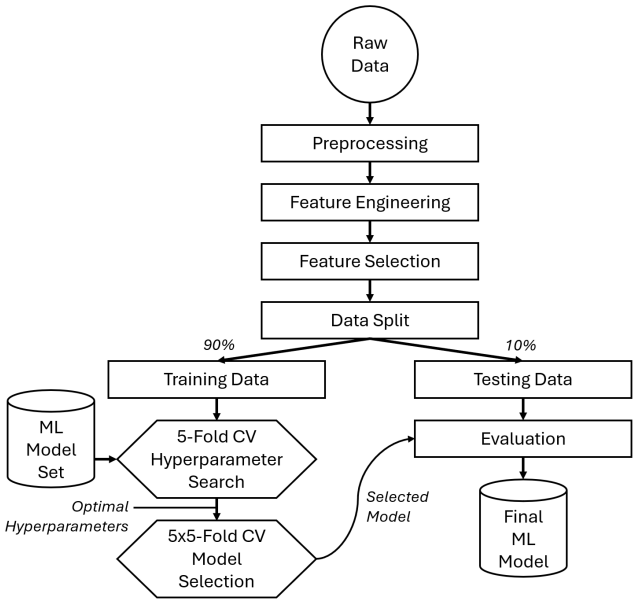


Figure 1: The flow diagram of the process.

Once pre-processing and feature engineering are completed, forward feature selection is employed to reduce the number of features for more stable training. This greedy algorithm in machine learning aims to determine the most relevant features for model prediction. It starts with an empty set and incrementally adds features that most improve model performance until no further significant enhancement is observed or all features are included. Although this method seeks to minimize redundancy and maximize relevance, it can be computationally intensive with high-dimensional datasets and may not always find the optimal subset due to possible local optima.

The data is subsequently divided, with 90% allocated to the training set and 10% to the test set. This test set is used to observe

the capability of the model in unseen data. Each machine learning model undergoes 5-fold cross-validation on the training set to identify the best hyper-parameters. The Optuna library [56] is utilized for hyper-parameter optimization.

To assess the performance of each experimented machine learning model, we conducted 5x5 cross-validation on the training set using the optimal hyper-parameters identified during the hyper-parameter tuning phase. *MAE* and *MAPE* were employed as metrics to compare the various models. Figure 1 provides a flow diagram of the architecture, illustrating how the models are trained and compared.

We conducted trials with a variety of machine learning models. Given their proven effectiveness on tabular datasets, our primary investigation centered on LightGBM [57] as we acquired best results with this method in our previous study [1], while still comparing the method with XGBoost [58]. Additionally, to establish benchmarks, we explored Random Forest, Support Vector Regression, and Multilayer Perceptron techniques. For the models' assessment, we utilized mean absolute error (MAE) and mean absolute percentage error (*MAPE*). MAE quantifies the average absolute deviation between the forecasted and observed values, whereas *MAPE* calculates the average percentage deviation between the predicted and true values.

To operationalize the predictive models developed in this study, we implemented a 3D shape-based pricing service designed to integrate seamlessly with the company's existing quotation system. This service provides a machine learning-based tool for predicting industrial product prices, specifically focusing on work-hour estimation for labor costs. It accepts inputs such as 3D models in STL format and various numerical and categorical parameters; including material thickness, type, surface area, hardness, and operation-specific details like mold dimensions and press types, all of which are elaborated in the data section.

Users interact with the service via application programming interface (API) which may be augmented into a dedicated user interface, permitting manual data input or the selection of pre-existing components from the system. The API also allows users to enable or disable the inclusion of 3D data in the predictions. Upon receiving input, the system extracts key features from the 3D model, such as triangle count, total surface area, and volume. These features, along with additional parameters, are fed into the selected machine learning model.

The predicted work hours are converted into a labor cost using a configurable multiplier, allowing the cost to be adjusted based on departmental rates or project-specific requirements. The system also calculates department-specific costs proportionally to the work hours, providing a detailed cost breakdown for activities such as CAD, CAM, 2D cutting, drilling & machining, assembly, measurement, and various CNC processes. This flexible approach enables users to make informed pricing decisions quickly, streamlining the cost estimation process.

For deployment and integration, the service is containerized using Docker and designed to run on-premises to ensure data confidentiality. It exposes a set of API endpoints for various functionalities, including data operations, model training, and prediction. These APIs allow for uploading 3D models and tabular data, configuring cost ratios, training new models, and making predictions. The service supports both single models trained on the entire dataset and ensemble models trained using 5-fold cross-validation, providing options for balancing performance and computational efficiency. This modular and secure design facilitates easy integration with other applications and supports the scalability of the solution within the company's infrastructure.

5. Results and Discussion

In this section, we present a comprehensive analysis of our findings. We begin with an overview of the experimental setup used for hyperparameter tuning, followed by a detailed examination of model experimentation results. Subsequently, we delve into model interpretability through the utilization of SHAP values. Finally, we examine the results of software testing, with particular emphasis on usability and performance metrics.

5.1. Experimental Setup

In our experiments with machine learning models, we meticulously optimized the hyperparameters to enhance the models' performance in predicting work man-hours for metal sheet stamping projects. The hyperparameter tuning was conducted using the Tree-structured Parzen Estimator available in the Optuna library [56], which efficiently explores the hyperparameter space to identify optimal settings.

An investigation of the final acquiredhyperparemeters of a model, LightGBM, can provide a more profound comprehension of the obtained results. The final model employed the 'dart' boosting type, which integrates dropout techniques into the boosting process to prevent overfitting by randomly dropping trees during training. We selected a learning rate of 0.33 to accelerate convergence, allowing the model to learn efficiently from the data without excessively prolonging the training time. A maximum depth of 30 and a high number of leaves (208) were set to enable the model to capture complex nonlinear relationships inherent in the manufacturing data, accommodating the intricate interactions among numerous features.

Minimal regularization was applied, with λ_{l1}, λ_{l2} set to near-zero values (1.06×10^{-8} and 2.97×10^{-4}, respectively), indicating that strong regularization was unnecessary due to effective overfitting control by other parameters like feature and bagging fractions. To introduce randomness and promote generalization, we utilized a feature fraction of 0.5675 and a bagging fraction of 0.84 with a bagging frequency of 2. This ensured that each iteration trained on a random subset of features and data samples, reducing the risk of the model becoming too tailored to specific patterns in the training set.

We set the minimum data in a leaf to 1, allowing the model to capture rare patterns and exceptions in the data, which is crucial for accurately predicting work man hour costs associated with infrequent sub-operation types. The maximum bin was configured to 212, permitting finer discretization of continuous features and enabling the model to capture subtle variations in feature values that significantly impact the target variable. By leveraging the Optuna library's Tree-structured Parzen Estimator for hyperparameter optimization, we were able to systematically explore the hyperparameter space and identify the optimal settings that maximized the model's

predictive performance. This careful tuning was essential for developing a robust model capable of achieving high predictive accuracy and meeting our target error rate, thereby effectively supporting decision-making processes in the manufacturing workflow.

5.2. Model Experimentation Results

We utilized the test set and implemented 5x5 cross-validation on the training set to evaluate various models. For the assessment, Mean Absolute Error (*MAE*) and Mean Absolute Percentage Error (*MAPE*) metrics were chosen due to their interpretability and wide acceptance within the domain. The outcomes of these evaluations are presented in Table 2. As expected, LightGBM and XGBoost exhibited superior performance compared to other models, with LightGBM achieving the lowest *MAE* and *MAPE* values during cross-validation (CV). The results on the test data from the top-performing model (LightGBM) are depicted in Figure 2. Based on consultations with industry experts, a model must exhibit a maximum *MAPE* of 10% to be deemed valuable, which constitutes the target Key Performance Indicator (KPI) for this study. The findings suggest that the majority of samples fall within this acceptable range. Furthermode, the models were compared using a variety of KPI metrics. Figure 3 depicts the proportion of samples accurately predicted according to these selected KPI metrics across all experiments. The selected 10% error threshold KPI target is also indicated in the Figure 3 as a red dashed line. For the top-selected model, it is apparent that 75% of the samples are within this acceptable range. Therefore, given the complexity of the task, we conclude that it is feasible to develop and deploy models for predicting work man hour costs in the sheet metal stamping industry.

Table 2: Comparison table of the cross validation results

Models	Results	
	5x5 CV MAPE	***5x5 CV MAE***
LightGBM*	10.89%	71.49
LightGBM	**10.78%**	**70.37**
XgBoost*	11.30%	73.72
XgBoost	11.23%	72.25
KNN Regressor	20.55%	122.01
MLP	16.61%	105.25
Linear Regression	26.35%	136.99

Models that end with "*" indicates that the model is trained without the additional 3D data features.

We further assessed how feature engineering techniques affect model performance. Our findings revealed that performance notably improves for both LightGBM and XgBoost after applying feature selection and generating synthetic data for chosen features. It is important to highlight that cost prediction in any field may be constrained by data representation limitations. The features depicting the product and operations might be overly generic, lacking detailed representation for each training example. Additionally, given the typical scarcity of industrial data in cost estimation tasks, additional efforts could focus on data augmentation. This could unlock the potential of more sophisticated machine learning models, such as Transformers and DNNs.

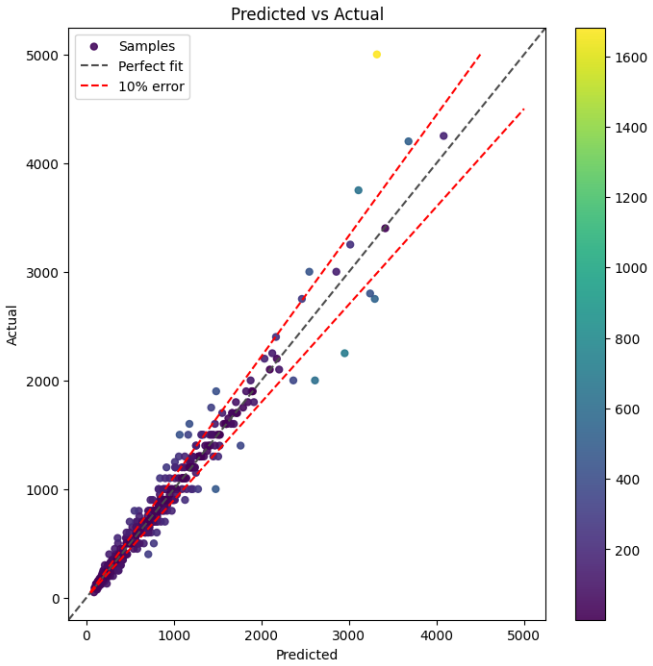


Figure 2: Evaluation of the best model on the test set.

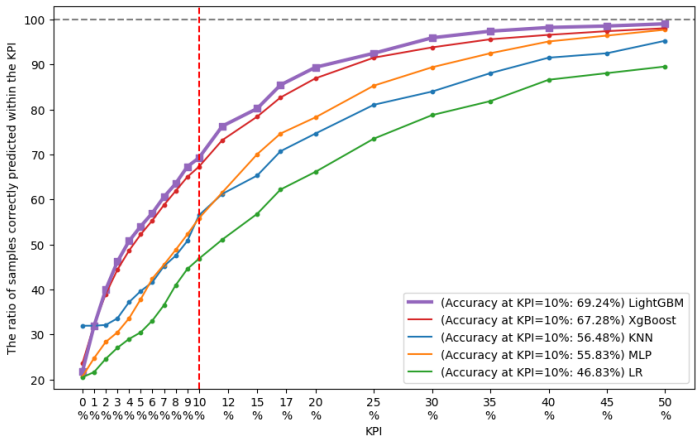


Figure 3: Change of the ratio of samples correctly predicted within different KPI metrics.

5.3. Model Interpretability

In addition, to gain deeper insights into the model's decision-making process, we employ SHAP (SHapley Additive exPlanations) values [59] to interpret the contribution of each feature to the predictions. SHAP is a model-agnostic interpretability method based on cooperative game theory, which assigns each feature an importance value by calculating its average marginal contribution across all possible feature combinations. By analyzing the SHAP values for our model, we found that press tonnage, the presence of a progressive operation, and die dimensions (DieX, DieY, DieZ) significantly influence the work man-hour estimation, as depicted in Figure 4. These features

have the highest SHAP values, indicating they contribute most to the predicted costs.

Specifically, higher press tonnage is associated with increased work man-hours, aligning with domain knowledge that higher tonnage presses require more setup time and operational complexity. The presence of a progressive operation also contributes to higher predicted man-hours due to the additional tooling and coordination required for such operations. Larger die dimensions (length, width, height) impact the prediction by indicating more substantial or complex dies, which typically necessitate more labor for handling and setup. We also observed that the high triangle count of the part 3D model, which correlates with the high part complexity, increases the work man-hours in general.

Other features, such as material properties and other sub-operation counts, have a comparatively moderate effect on the prediction. The SHAP analysis enhances the interpretability of our model by illustrating how each feature influences the output, ensuring that the model's behavior aligns with expert understanding. This transparency in the decision-making process not only validates the model's reliability but also builds trust with stakeholders by demonstrating that the predictions are based on logical and explainable factors relevant to the manufacturing context.

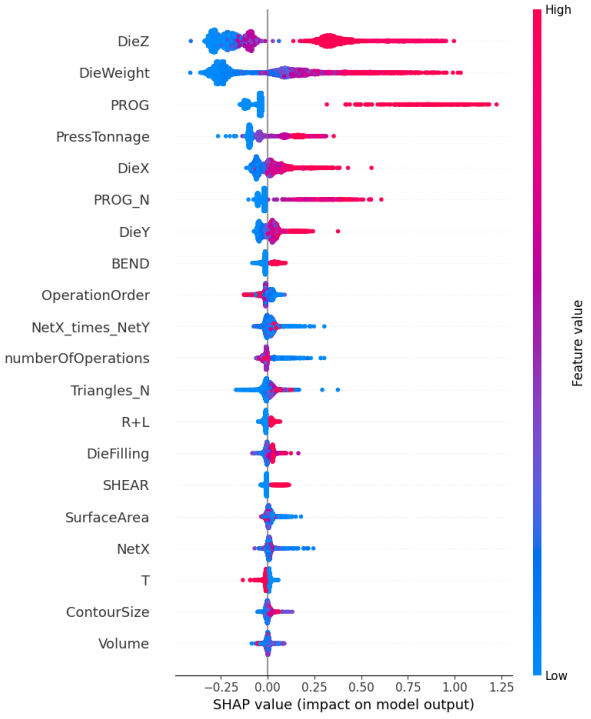


Figure 4: The SHAPley summarization of the features.

5.4. Software Test Results

In our implementation of the pricing service, LightGBM was selected due to its superior performance in predicting work hours, achieving a target error rate of less than or equal to 10%. The adoption of this machine learning model has significantly reduced the time required to generate quotations. On average, the inference time of the model is less than 15 seconds. While the analysis of the 3D part can add some time, especially if the data is not already stored in the database, resulting in a total average inference time of approximately 2 minutes ± 15 seconds, the overall process still represents a substantial improvement. Considering the reported time from the manufacturer, this approach reduces the time taken to respond to customer inquiries by 90%, which is crucial in industries where speed is a competitive advantage. This significant reduction in response time not only enhances operational efficiency but also provides a competitive edge in the fast-paced metal sheet stamping industry.

6. Conclusions

In this study, we extended our previous study on work-man hour forecasting in metal sheet stamping processes by conducting a comparative assessment of the efficiency of diverse machine learning algorithms. Additionally, the research investigates the influence of different feature engineering strategies on the results. This problem is formulated and analyzed within the framework of a regression model. We identified the most influential variables and features affecting work man-hours within the field. Additionally, we examined the performance of the models and outlined current limitations that require further investigation. The findings indicated that LightGBM and XGBoost achieved the highest accuracy (lowest *MAPE* error of 10.78%) compared to other experimented models. exhibiting commendable performance. While the initial study improved the predictive performance of the models through feature selection and synthetic data generation techniques, the present study focused on augmenting the dataset with additional real-world data and incorporating advanced feature engineering methods. With the additional improvements, most influential variables contributing to the work man-hour was similar to the previous study, as the the die dimensions, the amount of press tonnage, and the presence of progressive operations, with the exception of die weight. Collaboration with domain experts proved instrumental in understanding the utilization of certain features and the overall constraints of the project. Overall, our research underscores the potential of machine learning models in the context of work man-hours for metal sheet stamping projects and emphasizes the importance of feature engineering and the incorporation of domain-specific knowledge in enhancing model performance. The main limitation of this research is the insufficient availability of real-world data, which obstructs the application of deep learning techniques that could more effectively utilize the 3D models. Future research could focus on improved data representation methods using the 3D part data, such as image renders of the 3D part. Additionally, further research may explore the deployment of deep learning methods, that are adept at leveraging voxel-based 3D data.

Conflict of Interest The authors declare that they have no conflict of interest.

Acknowledgment This work was supported by the TÜBTAK TEYDEB Program with Project no: 9210055. The dataset and the use case problem were provided by ERMETAL A.Ş. The authors thank Cem Yıldız and Ali Erman Erten for sharing their expertise with us.

References

[1] A. E. Ünal, H. Boyar, B. Kuleli Pak, C. Yıldız, A. E. Erten, V. C. Güngör, "Man-hour Prediction for Complex Industrial Products," 4th International Informatics and Software Engineering Conference, 2023.

[2] T. Yeh, S. Deng, "Application of machine learning methods to cost estimation of product life cycle," International Journal of Computer Integrated Manufacturing, **25**(4-5), 340–352, 2012, doi:10.1080/0951192x.2011.645381.

[3] H. Salleh, "Selecting a standard set of attributes for the development of machine learning models of building project cost estimation," Planning Malaysia, **21**, 2023, doi:10.21837/pm.v21i29.1359.

[4] S. Yoo, N. Kang, "Explainable artificial intelligence for manufacturing cost estimation and machining feature visualization," Expert Systems With Applications, **183**, 115430, 2021, doi:10.1016/j.eswa.2021.115430.

[5] F. Ning, Y. Shi, M. Cai, W. Xu, X. Zhang, "Manufacturing cost estimation based on a deep-learning method," Journal of Manufacturing Systems, **54**, 186–195, 2020, doi:10.1016/j.jmsy.2019.12.005.

[6] O. Kurasova, V. Marcinkevičius, V. Medvedev, B. Mikulskienė, "Early cost estimation in customized furniture manufacturing using machine learning," International Journal of Machine Learning and Computing, **11**(1), 28–33, 2021, doi:10.18178/ijmlc.2021.11.1.1010.

[7] L. Yang, J. Li, F. Chao, P. Hackney, M. Flanagan, "Job shop planning and scheduling for manufacturers with manual operations," Expert Systems, **38**(7), 2018, doi:10.1111/exsy.12315.

[8] F. Bodendorf, J. Franke, "Application of the technology acceptance model to an intelligent cost estimation system: an empirical study in the automotive industry," 2022, doi:10.24251/hicss.2022.144.

[9] M. Atia, J. Khalil, M. Mokhtar, "A cost estimation model for machining operations; an ann parametric approach," Journal of Al-Azhar University Engineering Sector, **12**(44), 878–885, 2017, doi:10.21608/auej.2017.19195.

[10] J. Loyer, E. Henriques, M. Fontul, S. Wiseall, "Comparison of machine learning methods applied to the estimation of manufacturing cost of jet engine components," International Journal of Production Economics, **178**, 109–119, 2016, doi:10.1016/j.ijpe.2016.05.006.

[11] F. Silva, V. Sousa, A. Pinto, L. Ferreira, M. Pereira, "Build-up an economical tool for machining operations cost estimation," Metals, **12**(7), 1205, 2022, doi:10.3390/met12071205.

[12] K. Manjunath, S. Tewary, N. Khatri, K. Cheng, "Monitoring and predicting the surface generation and surface roughness in ultraprecision machining: a critical review," Machines, **9**(12), 369, 2021, doi:10.3390/machines9120369.

[13] H. Y. Gong, J. Y. Wang, Z. H. Zhao, "Study on the springback characteristics of cr340la steel during the typical auto part stamping process," Advanced Materials Research, **322**, 98–101, 2011, doi:10.4028/www.scientific.net/amr.322.98.

[14] R. Zeng, L. Huang, J. Li, "Fracture prediction in sheet metal stamping based on a modified ductile fracture criterion," Key Engineering Materials, **639**, 543–550, 2015, doi:10.4028/www.scientific.net/kem.639.543.

[15] S. Zvonov, Y. Klochkov, "Computer-aided modelling of a latch die cutting in deform - 2d software system," Key Engineering Materials, **685**, 811–815, 2016, doi:10.4028/www.scientific.net/kem.685.811.

[16] S. Kokare, "Toward cleaner space explorations: a comparative life cycle assessment of spacecraft propeller tank manufacturing technologies," The International Journal of Advanced Manufacturing Technology, **133**(1-2), 369–389, 2024, doi:10.1007/s00170-024-13745-y.

[17] M. Moghadam, C. Nielsen, N. Bay, "Analysis of the risk of galling in sheet metal stamping dies with drawbeads," Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture, **234**(9), 1207–1214, 2020, doi:10.1177/0954405420911307.

[18] T. Chen, "Xgboost: a scalable tree boosting system," 2016, doi:10.48550/arxiv.1603.02754.

[19] F. Wang, "Extended-window algorithms for model prediction applied to hybrid power systems," Technologies, **12**(1), 6, 2024, doi:10.3390/technologies12010006.

[20] S. Guo, "Revolutionizing the used car market: predicting prices with xgboost," Applied and Computational Engineering, **48**(1), 173–180, 2024, doi:10.54254/2755-2721/48/20241349.

[21] T. Duan, A. Avati, D. Ding, K. Thai, S. Basu, A. Ng, et al., "Ngboost: natural gradient boosting for probabilistic prediction," 2019, doi:10.48550/arxiv.1910.03225.

[22] D. Ruta, M. Liu, L. Cen, Q. Vu, "Diversified gradient boosting ensembles for prediction of the cost of forwarding contracts," 2022, doi:10.15439/2022f291.

[23] S. Touzani, J. Granderson, S. Fernandes, "Gradient boosting machine for modeling the energy consumption of commercial buildings," Energy and Buildings, **158**, 1533–1543, 2018, doi:10.1016/j.enbuild.2017.11.039.

[24] P. Panjee, "A generalized linear model and machine learning approach for predicting the frequency and severity of cargo insurance in Thailand's border trade context," Risks, **12**(2), 25, 2024, doi:10.3390/risks12020025.

[25] F. Bodendorf, J. Franke, "A machine learning approach to estimate product costs in the early product design phase: a use case from the automotive industry," Procedia CIRP, **100**, 643–648, 2021.

[26] L. Liu, E. Chen, Y. Ding, "Tr-net: a transformer-based neural network for point cloud processing," Machines, **10**(7), 517, 2022, doi:10.3390/machines10070517.

[27] Z. Yang, Y. Sun, S. Liu, X. Shen, J. Jia, "Std: sparse-to-dense 3d object detector for point cloud," in Proceedings of the IEEE International Conference on Computer Vision, 204, 2019, doi:10.1109/iccv.2019.00204.

[28] F. Ning, Y. Shi, M. Cai, W. Xu, X. Zhang, "Manufacturing cost estimation based on a deep-learning method," Journal of Manufacturing Systems, **54**, 186–195, 2020.

[29] X. Zhang, "Multiattention mechanism 3d object detection algorithm based on rgb and lidar fusion for intelligent driving," Sensors, **23**(21), 8732, 2023, doi:10.3390/s23218732.

[30] B. Huang, Y. Feng, T. Liang, "A voxel generator based on autoencoder," Applied Sciences, **12**(21), 10757, 2022, doi:10.3390/app122110757.

[31] O. Kurasova, V. Marcinkevičius, V. Medvedev, B. Mikulskienė, "Early cost estimation in customized furniture manufacturing using machine learning," International journal of machine learning and computing, **11**(1), 28–33, 2021.

[32] V. Svetnik, A. Liaw, C. Tong, J. Culberson, R. Sheridan, B. Feuston, "Random forest: a classification and regression tool for compound classification and qsar modeling," Journal of Chemical Information and Computer Sciences, **43**(6), 1947–1958, 2003, doi:10.1021/ci034160g.

[33] H. Zermane, A. Drardja, "Development of an efficient cement production monitoring system based on the improved random forest algorithm," The International Journal of Advanced Manufacturing Technology, **120**(3-4), 1853–1866, 2022, doi:10.1007/s00170-022-08884-z.

[34] G. Pan, "Xgboost and random forest algorithm for supply fraud forecasting," 2022, doi:10.1117/12.2641948.

[35] C. Strobl, A. Boulesteix, T. Kneib, T. Augustin, A. Zeileis, "Conditional variable importance for random forests," BMC Bioinformatics, **9**(1), 2008, doi:10.1186/1471-2105-9-307.

[36] A. Ziegler, I. König, "Mining data with random forests: current options for real-world applications," Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, **4**(1), 55–63, 2013, doi:10.1002/widm.1114.

[37] B. Özcan, A. Fığlalı, "Artificial neural networks for the cost estimation of stamping dies," Neural computing and applications, **25**, 717–726, 2014.

[38] Z. Leszczyński, T. Jasiński, "An artificial neural networks approach to product cost estimation: the case study for electric motor," Informatyka Ekonomiczna, **1**(47), 72–84, 2018, doi:10.15611/ie.2018.1.06.

[39] B. Waziri, K. Bala, S. Bustani, "Artificial neural networks in construction engineering and management," International Journal of Architecture Engineering and Construction, **6**(1), 2017, doi:10.7492/ijaec.2017.006.

[40] M. Meharie, W. Mengesha, Z. Gariy, R. Mutuku, "Application of stacking ensemble machine learning algorithm in predicting the cost of highway construction projects," Engineering Construction & Architectural Management, **29**(7), 2836–2853, 2021, doi:10.1108/ecam-02-2020-0128.

[41] I. Peško, V. Mučenski, M. Šešlija, N. Radović, A. Vujkov, D. Bibić, et al., "Estimation of costs and durations of construction of urban roads using ann and svm," Complexity, 1–13, 2017, doi:10.1155/2017/2450370.

[42] S. Magdum, A. Adamuthe, "Construction cost prediction using neural networks," Ictact Journal on Soft Computing, **8**(1), 1549–1556, 2017, doi:10.21917/ijsc.2017.0216.

[43] O. Durán, N. Rodríguez, L. Consalter, "Neural networks for cost estimation of shell and tube heat exchangers," Expert Systems With Applications, **36**(4), 7435–7440, 2009, doi:10.1016/j.eswa.2008.09.014.

[44] M. Bouabaz, M. Hamami, "A cost estimation model for repair bridges based on artificial neural network," American Journal of Applied Sciences, **5**(4), 334–339, 2008, doi:10.3844/ajassp.2008.334.339.

[45] K. Kim, I. Han, "Application of a hybrid genetic algorithm and neural network approach in activity-based costing," Expert Systems With Applications, **24**(1), 73–77, 2003, doi:10.1016/s0957-4174(02)00084-2.

[46] M. Juszczyk, "Early fast cost estimates of sewerage projects construction costs based on ensembles of neural networks," Applied Sciences, **13**(23), 12744, 2023, doi:10.3390/app132312744.

[47] A. Zouidi, F. Fnaiech, K. Al-Haddad, "A multi-layer neural network and an adaptive linear combiner for on-line harmonic tracking," 2007, doi:10.1109/wisp.2007.4447612.

[48] K. Işık, S. E. Alptekin, "A benchmark comparison of Gaussian process regression, support vector machines, and ANFIS for man-hour prediction in power transformers manufacturing," Procedia Computer Science, **207**, 2567–2577, 2022.

[49] M. Hur, S. K. Lee, B. Kim, S. Cho, D. Lee, D. Lee, "A study on the man-hour prediction system for shipbuilding," Journal of Intelligent Manufacturing, **26**, 1267–1279, 2015.

[50] C. H. Huang, S. H. Hsieh, "Predicting BIM labor cost with random forest and simple linear regression," Automation in Construction, **118**, 103280, 2020.

[51] T. Yu, H. Cai, "The prediction of the man-hour in aircraft assembly based on support vector machine particle swarm optimization," Journal of Aerospace Technology and Management, **7**, 19–30, 2015.

[52] S. Guo, T. Jiang, "Cost prediction of equipment system using LS-SVM with PSO," in 2007 International Conference on Wireless Communications, Networking and Mobile Computing, 5285–5288, IEEE, 2007.

[53] X. Hu, M. Lu, S. AbouRizk, "BIM-based data mining approach to estimating job man-hour requirements in structural steel fabrication," in Proceedings of the Winter Simulation Conference 2014, 3399–3410, IEEE, 2014.

[54] N. V. Chawla, K. W. Bowyer, L. O. Hall, W. P. Kegelmeyer, "SMOTE: synthetic minority over-sampling technique," Journal of artificial intelligence research, **16**, 321–357, 2002.

[55] R. M. Pereira, Y. M. Costa, C. N. Silla Jr., "MLTL: A multi-label approach for the Tomek Link undersampling algorithm," Neurocomputing, **383**, 95–105, 2020, doi:https://doi.org/10.1016/j.neucom.2019.11.076.

[56] T. Akiba, S. Sano, T. Yanase, T. Ohta, M. Koyama, "Optuna: A next-generation hyperparameter optimization framework," in Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining, 2623–2631, 2019.

[57] G. Ke, Q. Meng, T. Finley, T. Wang, W. Chen, W. Ma, et al., "Lightgbm: A highly efficient gradient boosting decision tree," Advances in neural information processing systems, **30**, 2017.

[58] T. Chen, C. Guestrin, "Xgboost: A scalable tree boosting system," in Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining, 785–794, 2016.

[59] S. M. Lundberg, S. I. Lee, "A unified approach to interpreting model predictions," Advances in neural information processing systems, **30**, 2017.

Advances in Science, Technology and Engineering Systems Journal Vol. 9, No. 6, 12-20 (2024)

www.astesj.com

Special Issue on Innovation In Computing, Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

Advanced Fall Analysis for Elderly Monitoring Using Feature Fusion and CNN-LSTM: A Multi-Camera Approach

Win Pa Pa San[1], Myo Khaing[2]

[1]*Image and Signal Processing Lab, University of Computer Studies, Mandalay, Mandalay, 05071, Myanmar*

[2]*Faculty of Computer Science, University of Computer Studies, Mandalay, Mandalay, 05071, Myanmar*

ARTICLE INFO

Article history:
Received: 15th September, 2024
Revised: 30th September, 2024
Accepted: 15th October, 2024
Online: 30th November, 2024

Keywords:
Feature Fusion
Human Silhouette Image (HSI)
Silhouette History Images (SHI)
Dense Optical Flow (DOF)
Convolutional Neural Network (CNN)
Long Short-Term Memory (LSTM)

ABSTRACT

As society ages, the imbalance between family caregivers and elderly individuals increases, leading to inadequate support for seniors in many regions. This situation has ignited interest in automatic health monitoring systems, particularly in fall detection, due to the significant health risks that falls pose to older adults. This research presents a vision-based fall detection system that employs computer vision and deep learning to improve elderly care. Traditional systems often struggle to accurately detect falls from various camera angles, as they typically rely on static assessments of body posture. To tackle this challenge, we implement a feature fusion strategy within a deep learning framework to enhance detection accuracy across diverse perspectives. The process begins by generating a Human Silhouette Image (HSI) through background subtraction. By combining silhouette images from two consecutive frames, we create a Silhouette History Image (SHI), which captures the shape features of the individual. Simultaneously, Dense Optical Flow (DOF) extracts motion features from the same frames, allowing us to merge these with the SHI for a comprehensive input image. This fused representation is then processed using a pre-trained Convolutional Neural Network (CNN) to extract deep features. A Long Short-Term Memory (LSTM) Recurrent Neural Network (RNN) is subsequently trained on these features to recognize patterns indicative of fall events. Our approach's effectiveness is validated through experiments on the UP-fall detection dataset, which includes 1,122 action videos and achieves an impressive 99% accuracy in fall detection.

1. Introduction

The aging population is rapidly growing worldwide, leading to a significant increase in the number of elderly individuals who require constant care and monitoring. As a result, the ratio of family caregivers to elderly individuals is becoming increasingly unbalanced, especially in countries with higher life expectancies. This imbalance has created a pressing need for automatic health monitoring systems that can provide timely and efficient care for the elderly. One of the most critical aspects of such health monitoring systems is the detection of falls, a leading cause of injury and hospitalization among older adults.

Falls among the elderly can occur for various reasons, including heart attacks, high blood pressure, and other home accidents. The consequences of falls can be severe, often leading to a decline in physical and mental health, reduced mobility, and increased dependence on caregivers. Therefore, accurately detecting falls in real-time is essential for preventing further injuries and ensuring prompt medical attention. Despite the importance of fall detection, traditional vision-based systems face significant challenges in achieving reliable performance across different environments and camera viewpoints.

In recent years, computer vision and machine learning have paved the way for more sophisticated fall detection systems. Convolutional Neural Networks (CNNs) have shown remarkable success in various image processing and object recognition tasks, making them suitable candidates for analyzing video data in fall detection applications. However, static image-based approaches often struggle to capture the temporal dynamics of fall events, which are crucial for accurate detection. This limitation can be addressed by integrating Recurrent Neural Networks (RNNs), particularly Long Short-Term Memory (LSTM) networks, which excel at learning temporal dependencies in sequential data.

* Win Pa Pa San, University of Computer Studies, Mandalay, Mandalay, 05071, Myanmar, +959262988945, winpapasan@ucsm.edu.mm

The proposed fall detection system leverages the strengths of both CNNs and LSTMs, combined with a feature fusion approach to enhance the accuracy and robustness of fall detection. The system utilizes multiple cameras to capture different viewpoints of the monitoring area, providing a comprehensive view of the scene. Human silhouette images are extracted from two consecutive video frames and fused into a Silhouette History Image (SHI), which serves as a shape feature representing the subject's posture over time. Additionally, Dense Optical Flow (DOF) is computed to capture motion features between frames, offering valuable information about the subject's movements.

By fusing SHI and DOF features, the system creates a rich representation of both spatial and temporal aspects of the scene. These fused features are then fed into a pre-trained CNN to extract deep features, which are subsequently processed by an LSTM network to recognize fall events. The use of multiple cameras ensures that the system can detect falls from various angles, overcoming the limitations of single-camera setups. Furthermore, the feature fusion approach enables the system to capture subtle changes in posture and movement, improving the overall detection accuracy.

To evaluate the effectiveness of the proposed system, experiments were conducted using the publicly available UP-Fall detection dataset. The results demonstrate that the proposed method outperforms traditional vision-based fall detection systems, achieving superior performance in terms of accuracy and robustness. This research highlights the potential of combining feature fusion with CNN-LSTM architectures for developing advanced fall detection systems that can significantly enhance the safety and well-being of elderly individuals.

The primary aim of this research is to develop an advanced fall detection system that accurately identifies fall events in real-time, leveraging feature fusion and CNN-LSTM architectures within a multi-camera setup. The specific objectives are:

To design a robust fall detection framework that integrates shape and motion features using Silhouette History Images (SHI) and Dense Optical Flow (DOF).

- To employ a pre-trained CNN for deep feature extraction and an LSTM network for temporal sequence analysis to improve fall detection accuracy.
- To validate the effectiveness of the proposed system through extensive experiments using a publicly available dataset, ensuring its practical applicability in various indoor environments.

The motivation for this research stems from the growing need for reliable and efficient fall detection systems in elderly care. With the increasing elderly population, there is a heightened demand for solutions that can monitor and ensure the safety of older adults, particularly those living alone or in assisted living facilities. Existing fall detection systems often struggle with accuracy due to limitations in capturing dynamic movements and variations in camera viewpoints. By addressing these challenges through the integration of advanced machine learning techniques and a multi-camera approach, this research aims to provide a more dependable solution that enhances the quality of life for the elderly.

Traditional vision-based fall detection systems face several challenges, including:

- Inability to capture temporal dynamics of fall events, leading to missed detections or false alarms.
- Limited performance due to reliance on single-camera setups, which cannot cover all angles and may result in occlusions.
- Difficulty in accurately distinguishing between falls and other similar activities, such as sitting down abruptly.

The proposed system combines CNN and LSTM networks to leverage their strengths in spatial and temporal feature extraction. The use of multiple cameras ensures comprehensive coverage of the monitored area, reducing the likelihood of occlusions and improving detection reliability. Feature fusion of SHI and DOF provides a rich representation of both posture and movement, enabling the system to differentiate between falls and non-fall activities more accurately.

This research makes several key contributions to the field of fall detection:

- Introduction of a novel feature fusion approach that combines SHI and DOF to capture both shape and motion characteristics of potential fall events.
- Development of a hybrid CNN-LSTM architecture that effectively integrates spatial and temporal features for enhanced fall detection performance.
- Implementation of a multi-camera system that overcomes the limitations of single-camera setups, providing a more robust and reliable solution for real-world applications.
- Extensive experimental validation using the UP-Fall detection dataset, demonstrating the superior accuracy and robustness of the proposed method compared to traditional systems.

By addressing the limitations of existing fall detection approaches and introducing innovative solutions, this research contributes to the advancement of health monitoring technologies, ultimately improving the safety and well-being of elderly individuals. Moreover, the proposed system can be applied to a smart home system to assist and provide telehealth services for the elderly.

This paper is organized as follows. Section I describes the objectives, motivations, system problem with solution, and contribution of this study. The literature survey about various fall detections is analyzed in Section II. The system overview and the detailed explanation of this study are presented and the experimental results and comparison with the results of the other existing methods are presented in Section III. Some discussion about the pros and cons of the proposed system are discussed in Section IV. Finally, the conclusion and future work are drawn in Section V.

2. Related Work

The advancement of sophisticated sensors and devices has captured the interest of many researchers focused on artificial intelligence systems. This is particularly true for applications such

as smart home systems, patient monitoring, surveillance, and elderly monitoring, where various sensor-based and camera-based approaches have been proposed. Fall detection systems, in particular, can be classified into two categories based on the sensors used: sensor-based and camera (vision)-based.

2.1. Sensor-based Fall detection

Fall detection sensors typically incorporate accelerometers and gyroscopes to monitor the acceleration and orientation of elderly individuals. When attached to various body parts, accelerometers collect acceleration data during falls. One proposed system [1] employs accelerometers and gyroscopes mounted on the gait to assess balance, detect falls, and evaluate fall risk. In a different approach, Lindeman et al. integrated accelerometer sensors into a hearing aid positioned behind the ear [2]. Another fall detection system [3] identifies falls and locates the fallen individual. This system utilizes a sensor attached to the waist to detect backward and sideways falls based on the wearer's final orientation.

Additionally, the authors in [4] developed a machine learning-based fall detection system that utilizes temporal and magnitude features extracted from acceleration signals. These features were used to train a Support Vector Machine classifier for fall identification. Bianchi et al. implemented a fall detection system using barometric pressure sensors, evaluating its performance against accelerometer-based systems; this system classifies falls based on postural orientation and altitude changes [5]. In [6], another system was proposed that not only detects falls but also assesses injury severity, employing multiple accelerometers attached to joints to analyze three-axis acceleration data. Furthermore, in [7], the authors introduced a fall detection system that combines accelerometer sensors with the Discrete Wavelet Transform (DWT) and Support Vector Machine (SVM) algorithm.

2.2. Vision-based Fall detection

Numerous fall detection systems have been developed in recent years, each utilizing different techniques to enhance accuracy and reliability. A notable approach employs key points of the human skeleton detected via OpenPose, as demonstrated in [8]. This system identifies falls based on the speed of descent of the hip joint, the centerline angle, and the body's width-to-height ratio. While it achieves 98.3% sensitivity, 95% specificity, and 97% accuracy on a dataset of 60 falling and 40 non-falling actions, the system encounters challenges with partial occlusion and recognizing falls from multiple directions.

Another vision-based approach for fall detection, utilizing multiple cameras and convolutional neural networks (CNNs), was proposed in [9]. This system leverages optical flow to capture relative motion between consecutive images and trains three CNN models to process visual features from different camera angles. The results on the UP-Fall detection dataset demonstrated 95.64% accuracy, 97.95% sensitivity, and 83.08% specificity. However, the system's performance is impacted by environmental changes and occlusions. In [10], the authors developed a fall detection system that employs features extracted by Inception v3 and a MobileNet model for human detection. By applying transfer learning, they achieved 98.5% accuracy, 97.2% specificity, and 93.47% sensitivity on the FDD dataset, and 91.5% accuracy, 94% specificity, and 100% sensitivity on the URFD dataset. Nonetheless, managing occlusions continues to pose a significant challenge.

Similarly, in [11], the authors proposed a vision-based fall detection method using CNNs, which involved a three-step training process: initial training with ImageNet, motion modeling with UCF101, and fine-tuning specifically for fall detection. Testing on the URFD, Multicam, and FDD datasets resulted in accuracy rates of 95%, 96%, and 97%, respectively. While the results are promising, the system requires improvements in avoiding image preprocessing issues and managing occlusions and multi-person detection. In [12], the authors combined histograms of oriented gradients (HOG), local binary patterns (LBP), and Caffe features for fall detection. Their system utilized VIBE+ for human detection and extraction, along with SVM for classification, achieving sensitivities of 95%, 93.3%, and 92.9%, and specificities of 97.5%, 92.2%, and 86.4% on the Multicam, Chua's dataset, and their dataset, respectively. However, handling occlusions remains a challenge.

Furthermore, in [13], the authors focused on detecting fallen individuals using assistive robots. Their system utilized features such as the aspect ratio of the bounding box, normalized bounding box width, and bottom coordinate, employing an SVM-based classifier. Testing on the FPDS dataset yielded 100% precision and 99.74% recall. However, the system requires enhancements in occlusion detection and minimizing image preprocessing issues.

These studies underscore several common challenges fall detection systems face, including occlusion handling, adaptability to diverse environmental conditions, effective feature extraction and fusion, thorough testing across varied datasets, and detecting falls in multi-person environments. The proposed advanced fall detection system aims to tackle these issues by integrating shape and motion features, utilizing a hybrid CNN-LSTM architecture, and employing a multi-camera setup. This approach promises to enhance the accuracy and reliability of fall detection, making significant progress toward robust and practical real-world applications.

3. Material and Methods

The purpose system flow of the block diagram illustrating the system flow is shown in Figure. 1 of the Advanced Fall Detection System Using Feature Fusion and CNN-LSTM. They are:

- Video Input: Multiple camera feeds provide input data capturing the indoor environment from different viewpoints.
- Data Preprocessing: Initial processing steps such as frame rate adjustment and background subtraction are performed to prepare the input data for feature extraction.
- Feature Extraction: Shape and motion features are extracted from the preprocessed video frames, capturing relevant information about human postures and movements.
- Feature Fusion: The extracted shape features (SHI) and motion features (DOF) are fused into a unified feature representation, combining both the spatial and temporal information.
- CNN-LSTM: The fused features are input to a hybrid CNN-LSTM architecture, where CNN layers extract spatial features, and LSTM layers model temporal dependencies across frames.

- Fall Detection: The learned features are used for fall event detection, where thresholding and event recognition techniques are applied to identify fall events within the video sequences.
- Classification Output: The system outputs the results of fall event detection, indicating the presence or absence of fall events in the monitored environment.

In this system, the sequential flow of data and processing steps in the fall detection system: In the first step, the fall detection system utilizes multiple camera feeds to capture the indoor environment from diverse viewpoints. These camera feeds serve as the primary input data for the system, providing comprehensive coverage of the monitored area. Before further processing, initial preprocessing steps are conducted to ensure the input data is suitable for feature extraction. This includes adjustments to the frame rate of the video streams to optimize computational efficiency and standard background subtraction techniques to segment foreground objects from the static background.

In the second step the following preprocessing, the system extracts shape and motion features from the preprocessed video frames. Shape features are derived from human silhouette images obtained through background subtraction, while motion features are computed using dense optical flow techniques applied to consecutive frames. These features capture essential information regarding human postures and movements within the monitored environment, serving as discriminative cues for fall event detection.

In the third step, the extracted shape and motion features are fused into a unified feature representation using a feature fusion approach. This fusion process combines spatial and temporal information, leveraging the complementary nature of shape and motion cues to enhance the discriminative power of the feature representation. The fused features, called Silhouette History Image (SHI) and Dense Optical Flow (DOF) Image, respectively, from the input data for subsequent processing stages.

In the fourth step, the fused features are input to a hybrid CNN-LSTM architecture, designed to capture spatial and temporal dependencies within the input data effectively. The CNN component of the architecture extracts spatial features from the fused representations, leveraging convolutional layers to learn hierarchical representations of the input features. These spatial features are then fed into LSTM layers, which model temporal dynamics across consecutive frames, allowing the system to capture the sequential nature of human actions and movements.

In the fifth step, the learned features from the CNN-LSTM architecture are utilized for fall event detection within the video sequences. This involves applying thresholding and event recognition techniques to the learned representations, enabling the system to identify instances of fall events based on predefined criteria. The combination of spatial and temporal features, along with the robust architecture of the CNN-LSTM model, facilitates accurate and reliable fall detection performance.

Finally, the system outputs the results of fall event detection, indicating the presence or absence of fall events in the monitored environment. These results provide valuable insights into the safety and well-being of individuals within the indoor space, enabling timely intervention and assistance in the event of a fall.

Background subtraction is a critical preprocessing step in the fall detection system, aimed at isolating human subjects from the static background in the video feeds. This process involves several stages to accurately detect and segment the moving foreground objects, which is essential for subsequent feature extraction and analysis.

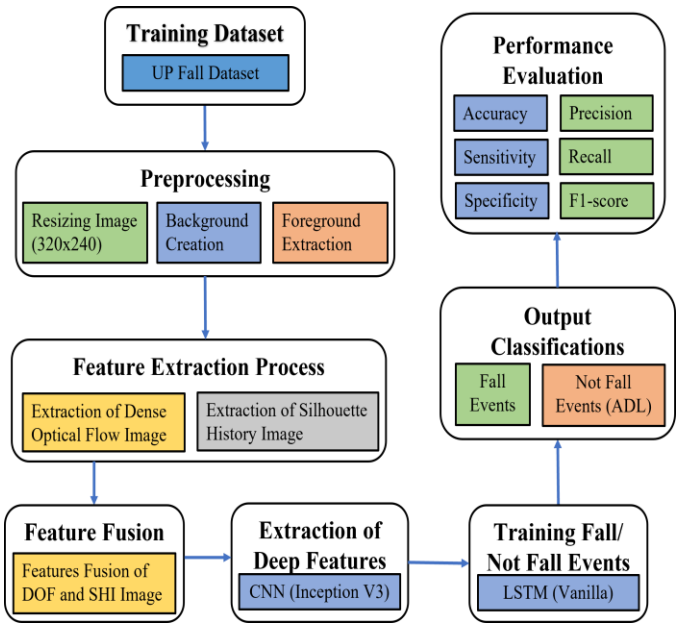


Figure 1: System flow of the advanced fall detection system using feature fusion and CNN-LSTM

3.1. Preprocessing

A) Background Creation

The first step in background subtraction is to create a background frame that represents the static elements in the scene. This is particularly challenging in fall detection scenarios where the human subject is often present throughout the video. Traditional methods like Gaussian Mixture Models (GMM) are inadequate in such cases due to their inability to handle the continuous presence of the subject. Instead, we employ a method based on frame differencing and foreground replacement:

(1) Common Background Frame (CBF) Selection: Identify a frame from the video sequence that does not contain any moving objects or humans. This frame is used as the CBF.
(2) Foreground Replacing: For videos without a clear background frame, the following steps are performed:

- Human Segmentation Mask (M): Utilize Mask-RCNN to generate a segmentation mask for the human subject.
- Pixel Replacement: Replace the pixels in the mask (M) with the corresponding pixels from the CBF using the equation:

$$BF(x,y) = \begin{cases} CBF(x,y) & if\ M(x,y) = 0 \\ F(x,y) & if\ M(x,y) = 1 \end{cases} \quad (1)$$

- Background Frame (BF) Storage: Save the resulting frame as the background frame for the video sequence.

B) Foreground Extraction

Once the background frame (BF) is established, the next step is to extract the foreground objects. This involves comparing each frame (F) of the video to the background frame to identify moving objects:

$$FG(x,y) = \begin{cases} 1 & if\ \ BF(x,y) - F(x,y) \geq TH \\ 0 & otherwise \end{cases} \quad (2)$$

The threshold (*TH*) is the pixel value that can differentiate the moving foreground and background objects. The illustration of the process of foreground extraction results is shown in Figure. 2.

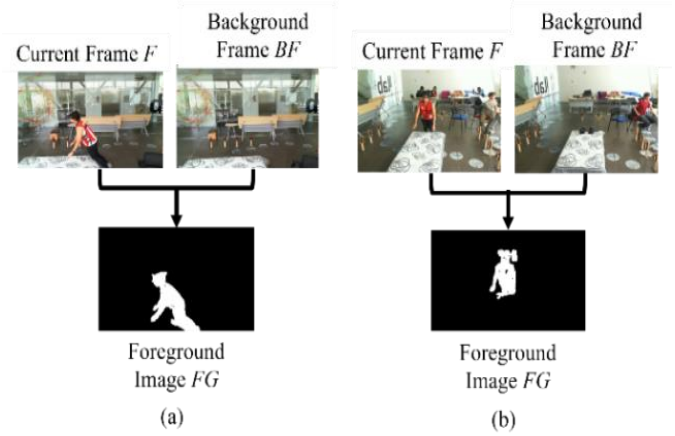


Figure 2: Illustration of foreground extraction results from (a) camera1 and (b) camera2

C) *Noise Removing*

After extracting the foreground, it is essential to filter out noise and ensure only the relevant human subjects are retained:

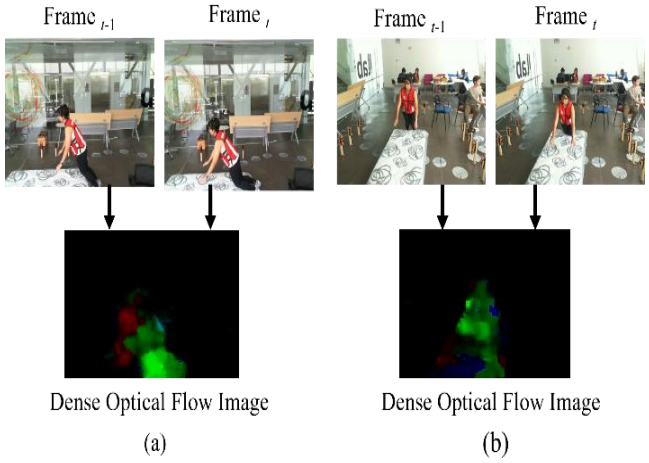


Figure 3: Background subtraction results (1st row: input frames, 2nd row: foreground

(1) Object Classification: Analyze the foreground mask to identify the human subject acting. Non-human objects are considered noise.

(2) Noise Filtering: Apply size-based filtering and morphological operations to remove small, irrelevant objects from the foreground mask. This step ensures that only the significant moving objects (humans) are retained for further processing. Some more sample images of background subtraction results are shown in Figure. 3.

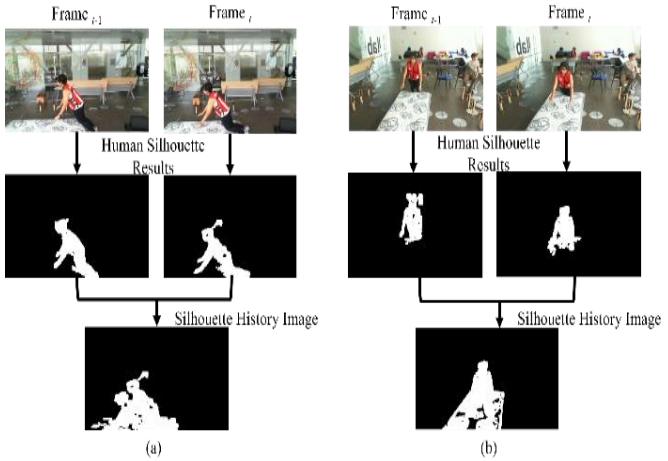


Figure 4: Creation of silhouette history image (SHI) (a) camera1 (b) camera2

3.2. *Feature Extraction*

A) *Extraction of Shape Feature*

To extract the shape feature, the edge smoothing process is performed over the noise-removed human silhouette image (foreground results). Then the resulting human silhouette images of two consecutive frames are combined to create the Silhouette History Image (SHI) results, which are used as the shape features, as shown in Figure. 4.

B) *Extraction of Motion Feature*

Dense optical flow calculation [14] is used for motion feature extraction. Dense optical flow features are extracted from every two consecutive frames. Colors are then assigned to the dense optical flow results using the HSV color space. The orientation value calculated from the dense optical flow is assigned as the Hue value, the Saturation is set to the maximum of 255, and the magnitude value of the dense optical flow is assigned as the Value in the HSV color space. The results of motion feature extraction from Camera1 and Camera2 are shown in Figure. 5 (a) and (b).

3.3. *Feature Fusion*

In this part, SHI and DOF are fused into a single input data for the training model. SHI and DOF have the same image size, and feature fusion (*FF*) is performed using the following equation. The fused feature dimensions will be the same as those of the original input images with 320×240 image size, and the result of feature fusion is shown in Figure. 6.

$$FF(x,y) = \begin{cases} SHI(x,y) & if\ SHI(x,y) = 1\ , DOF(x,y) = 0 \\ DOF(x,y) & otherwise \end{cases} \quad (3)$$

3.4. *Train CNN-LSTM for Fall Detection*

A) *Extraction of Deep Features using Convolutional Neural Network (CNN)*

A convolutional neural network (CNN) is an artificial neural

network designed to process image data and learn to classify and segment various objects within images and videos. The Inception V3 model, known for its effectiveness in image analysis and object detection, is utilized in the system to extract deep features from the input image fusion data. Inception V3, a third edition of Google's Inception CNN, consists of 42 layers. The output from the average pooling layer, a 2048-dimensional feature vector, is used as the deep features for fall detection.

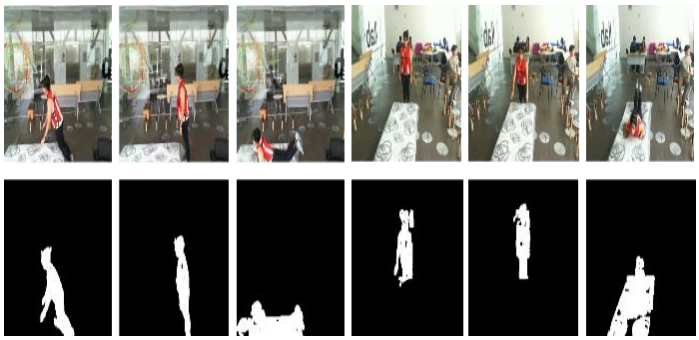


Figure 5: Motion feature extraction results (a) camera1 (b) camera2

B) Training Fall Event Detection Model using Recurrent Neural Network (RNN)

A Recurrent Neural Network (RNN) is designed for learning from sequential or time-series data, where the output depends on prior elements in the sequence. In this system, Long Short-Term Memory (LSTM), which consists of a cell, an input gate, an output gate, and a forget gate, is used for detecting fall events.

As shown in Figure. 7, the fused feature outputs from two cameras are fed into the Inception V3 model, pre-trained on the large ImageNet dataset. The "avg-pool" layer of Inception V3 produces a deep feature vector of length 2048. Deep features from both cameras are combined to create a feature vector of length 4096. This feature vector sequence, comprising 18 frames (spanning 3 seconds), is then fed into an LSTM for training to detect whether the input sequences contain a fall event. The LSTM used for fall detection consists of 2 stacked layers with 512 hidden units, as shown in Figure. 8. We used the ReLU activation function in two hidden layers and in the final output layer, softmax is applied for classifying the fall and not-fall events.

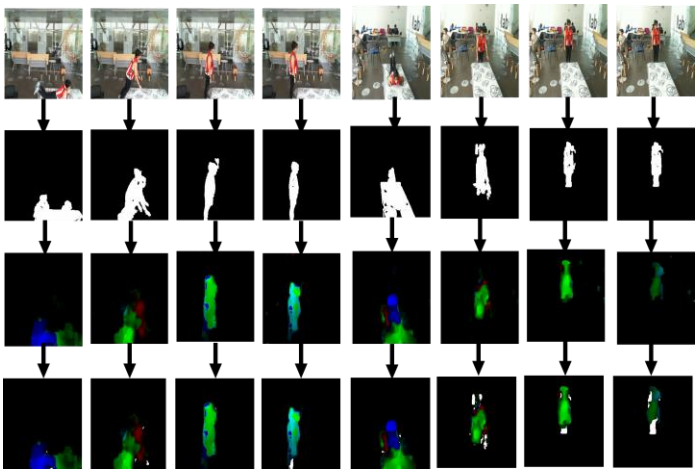


Figure 6: Sample results of feature fusion (1st row: input images, 2nd row: shape feature results, 3rd row: motion feature results, 4th row: feature fusion results)

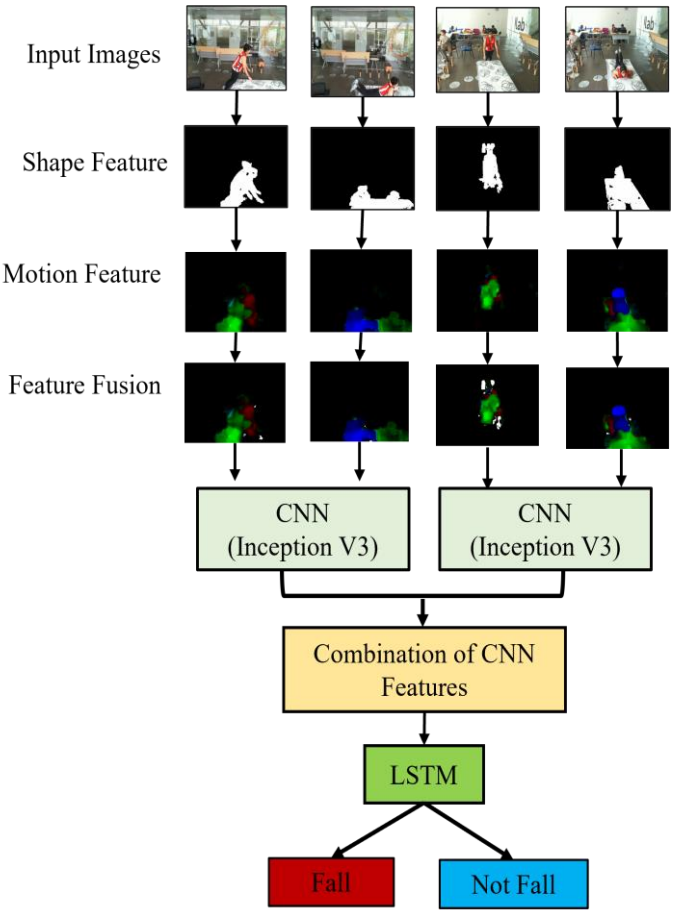


Figure 7: Flow chart of fall detection using CNN-LSTM

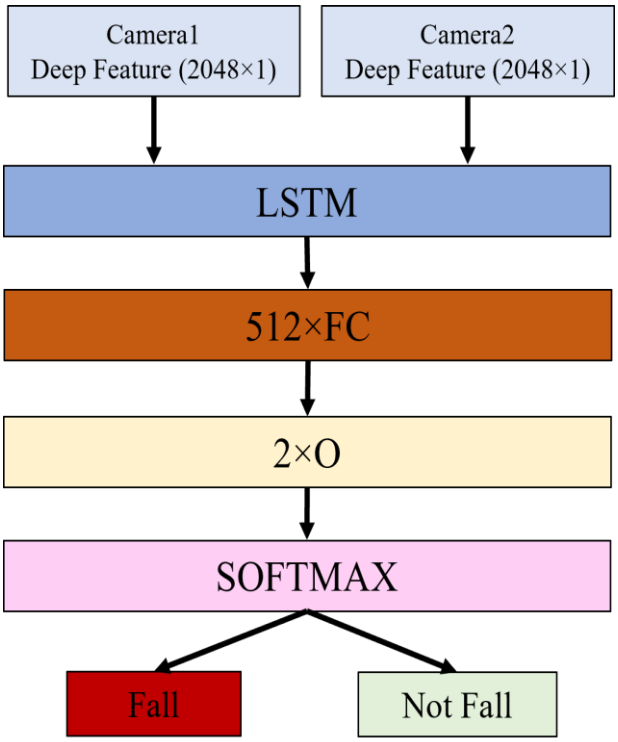


Figure 8: Architecture of fall detection model using CNN-LSTM

4. Experimental Results

4.1. Dataset

The UP-Fall Detection dataset [15], provided by Universidad Panamericana, Mexico in April 2019, includes data from 6 infrared sensors, 6 accelerometers, 3 Raspberry Pi devices, 2 cameras, and 1 brain sensor to create a multimodal dataset for fall detection. This research uses only data from the 2 cameras to implement vision-based fall detection. The dataset contains 1122 videos, each ranging from 10 to 60 seconds in length. These videos comprise 11 activities performed by 17 subjects, each repeated 3 times. Activities 1 to 5 are falls, while the remaining activities are daily living, as detailed in Table I.

The UP-Fall detection dataset provides the action videos with a frame rate of 18 fps. We use the frame rate of 6fps because most fall events take around 2 or 3 secs and according to experiments, 6fps is enough to perform the fall detection. We convert the frame rate of 18 fps into 6 fps by taking every 3rd frame from the image sequence. Then, foreground extraction is applied to 2 cameras, 3 trials, and activity 1 to 11 of all 17 subjects. The resolution of the RGB image is 320×240 and the following are some results of foreground extraction. The experiments are performed on a 2.2GHz Intel Core i7 CPU machine. The features extraction time of SHI and DOF are 0.011 s and 0.031 s respectively. The features fusion and fall detection time (3s video frames) are 0.016 s and 1.5 s respectively using Python. Some test images of the results of falls and others are shown in Figure 9.

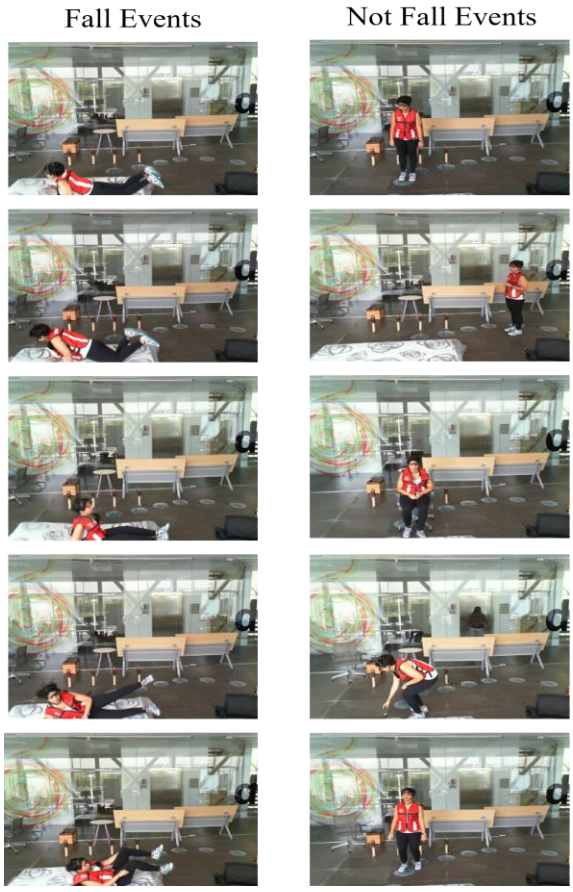


Figure 9: Some test image results of the UP-Fall detection dataset

Table 1: Activities and Their Duration

No.	Activity	Duration (sec)
1	Falling forward using hands	10
2	Falling forward using knees	10
3	Falling backward	10
4	Falling sideward	10
5	Falling while attempting to sit in an empty chair	10
6	Walking	60
7	Standing	60
8	Sitting	60
9	Picking up an object	10
10	Jumping	30
11	Laying	60

4.2. Participants

In the implementation of the advanced fall detection system, we utilized the UP-Fall Detection Dataset [16], which includes 11 activities and three trials per activity. Data were collected from over 17 participants, who were called subjects. Participants performed six simple human daily activities as well as five different types of human falls. During data collection, 17 subjects (9 male and 8 female) ranging from 18–24 years old, mean height of 1.66 m and a mean weight of 66.8 kg, were invited to perform 11 different activities for creating a comprehensive dataset for training and testing the fall detection system. Each participant's data was recorded using multiple modalities, but for this study, we focused solely on the video data captured by two cameras.

- Number of Participants: 17
- Activities: 11 distinct activities (5 fall and 6 daily activities)
- Trials: Each participant performed each activity three times, resulting in multiple video sequences for each activity.

In this research, we train 3 classification models. The first model (CNN-LSTM-2-classes) can classify only two classes such as fall and not-fall events. The second model (CNN-LSTM-7-classes) trained to classify 7 classes: fall events and other activities such as walking, standing, sitting, picking up an object, jumping, and laying. The third model (CNN-LSTM-11-classes) can classify all 11 activities as described in Table. 1.

4.3. Performance Evaluation

For fall detection performance evaluation, we trained and tested the data from the UP-Fall dataset using the same criteria as described in [9]. Data from trials 1 and 2 for 17 subjects were used as the training data, while data from trial 3 were used as the test data. To evaluate the performance of this work, the system uses the following six metrics: Accuracy, Sensitivity, Specificity, Precision, Recall, and F1-score, as given by (4)-(9),[17]. The performance evaluation of the three classification models is described in Table 2.

Moreover, we compare the performance of the proposed system with other approaches as shown in Table 3. We obtained the results of the method in [9] from their paper and used the same evaluation method to compare the results. In Table 3, we can see

that our proposed method produces higher accuracy than the method described in [9].

$$Accuracy = \frac{Number\ of\ Correct\ Predictions}{Total\ Numbers\ of\ Predictions} \quad (4)$$

$$Sensitivity = \frac{True\ Positive}{True\ Positive + False\ Negative} \quad (5)$$

$$Specificity = \frac{True\ Negative}{True\ Negative + False\ Positive} \quad (6)$$

$$Precision = \frac{True\ Positive}{True\ Positive + False\ Positive} \quad (7)$$

$$Recall = \frac{True\ Positive}{True\ Positive + False\ Negative} \quad (8)$$

$$F1Score = 2 \times \frac{Precision.Sensitivity}{Precision + Sensitivity} \quad (9)$$

5. Discussion and Limitations

The proposed system has some limitations in the computational complexity of training the CNN-LSTM model. It needs to extract deep features using CNN and perform sequence classification using LSTM. But that limitation can be overcome by applying high-performance computing devices such as GPU-machines. Another limitation is the occlusion problem. This applied two cameras for detecting fall events. But sometimes falls can occur in an area which only two cameras cannot cover. Therefore, in the future, we plan to extend this research by applying more cameras and configuring the camera set to cover all areas of the home environment of living alone elderly.

Table 2: Performance Evaluation of Three CNN-LSTM Models (Cam1 &Cam2) on UP-Fall Detection Dataset

Models	CNN-LSTM-2 Classes	CNN-LSTM-7 Classes	CNN-LSTM-11 Classes
Accuracy (%)	99	96	93
Sensitivity (%)	98	94	79
Specificity (%)	98	99	99
Precision (%)	99	94	81
Recall (%)	98	94	79
F1-Score (%)	98	94	80

Table 3: Comparison of Fall Detection Model (CNN-LSTM-2 Classes) performance evaluation on UP-Fall Detection Dataset

Method	Espinosa R, et al [9] (Cam1 &Cam2)	Proposed (Cam1 &Cam2)	Proposed (Cam1)	Proposed (Cam2)
Accuracy (%)	95.64	99	99	99
Sensitivity (%)	97.95	98	96	98
Specificity (%)	83.08	98	96	98
Precision (%)	96.91	99	99	97
Recall (%)	-	98	96	98
F1-Score (%)	97.43	98	97	97

6. Conclusion and Future Works

In this research, a vision-based fall detection system using multiple cameras applying CNN-LSTM has been proposed. The main contribution will be taken on the "features extraction and features fusion from multiple cameras", and the architecture of CNN-LSTM for improving fall detection rate. Based on the experimental results performed on the public dataset of the UP-Fall detection dataset, the proposed system got superior performance over the state-of-the-art methods. This fact points out that the feature fusion approach for CNN-LSTM is very effective and promising for the accurate fall detection system. Limitations such as the computation complexity for training CNN-LSTM can be overcome by using high-performance computing devices. Moreover, the multi-camera approach is more cost-effective than the other multi-sensor approaches, and this research will come as applied science research which can give a lot of benefits to human society. In this research, the experiments are only performed on the UP-Fall detection, a large dataset containing 1122 action videos performed by 17 persons. Then, the proposed method got good performance results on that dataset. In the future, to confirm the effectiveness of this proposed method, we will perform more experiments on other datasets of fall detection.

Conflict of Interest

The authors declare no conflict of interest.

Author Contribution

The major portion of the work presented in this paper was carried out by the first author, Win Pa Pa San, under the supervision of the second author, Myo Khaing. Win Pa Pa San also performed the data analysis, implementation, validation, and preparation of the manuscript.

Acknowledgment

I want to extend special thanks to Dr. Myo Khaing, Professor of the Faculty of Computer Science at the University of Computer Studies, Mandalay (UCSM), and Dr. Sai Maung Maung Zaw, Professor and head of the Faculty of Computer Systems and Technologies at the University of Computer Studies, Mandalay (UCSM), for their continuous guidance, support, and suggestions.

References

[1] Q. Li, J.A. Stankovic, M.A. Hanson, A.T. Barth, J. Lach, G. Zhou, 'Accurate, fast fall detection using gyroscopes and accelerometer-derived posture information', Proceedings - 2009 6th International Workshop on Wearable and Implantable Body Sensor Networks, BSN 2009, (June), 138–143, 2009, doi:10.1109/BSN.2009.46.

[2] Y. Li, K.C. Ho, M. Popescu, 'A microphone array system for automatic fall detection', IEEE Transactions on Biomedical Engineering, **59**(5), 1291–1301, 2012, doi:10.1109/TBME.2012.2186449.

[3] Y. Li, Z. Zeng, M. Popescu, K.C. Ho, 'Acoustic fall detection using a circular microphone array', 2010 Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBC'10, 2242–2245,

2010, doi:10.1109/IEMBS.2010.5627368.

[4] H. Wang, D. Zhang, Y. Wang, J. Ma, Y. Wang, S. Li, 'RT-Fall: A Real-Time and Contactless Fall Detection System with Commodity WiFi Devices', IEEE Transactions on Mobile Computing, **16**(2), 511–526, 2017, doi:10.1109/TMC.2016.2557795.

[5] F. Bianchi, S.J. Redmond, M.R. Narayanan, S. Cerutti, N.H. Lovell, 'Barometric pressure and triaxial accelerometry-based falls event detection', IEEE Transactions on Neural Systems and Rehabilitation Engineering, **18**(6), 619–627, 2010, doi:10.1109/TNSRE.2010.2070807.

[6] R.K. Shen, C.Y. Yang, V.R.L. Shen, W.C. Chen, 'A Novel Fall Prediction System on Smartphones', IEEE Sensors Journal, **17**(6), 1865–1871, 2017, doi:10.1109/JSEN.2016.2598524.

[7] B. Wójtowicz, A. Dobrowolski, K. Tomczykiewicz, 'Fall detector using discrete wavelet decomposition and SVM classifier', Metrology and Measurement Systems, **22**(2), 303–314, 2015, doi:10.1515/mms-2015-0026.

[8] H.U. Openpose, 'Fall Detection Based on Key Points of', Symmetry, 2020.

[9] R. Espinosa, H. Ponce, S. Gutiérrez, L. Martínez-Villaseñor, J. Brieva, E. Moya-Albor, 'A vision-based approach for fall detection using multiple cameras and convolutional neural networks: A case study using the UP-Fall detection dataset', Computers in Biology and Medicine, **115**, 2019, doi:10.1016/j.compbiomed.2019.103520.

[10] S. Sherin, P.M.T. Student, A.J. Assistant, 'Human Fall Detection using Convolutional Neural Network', International Journal of Engineering Research & Technology, **8**(6), 1368–1372, 2019.

[11] A. Núñez-Marcos, G. Azkune, I. Arganda-Carreras, 'Vision-based fall detection with convolutional neural networks', Wireless Communications and Mobile Computing, **2017**, 2017, doi:10.1155/2017/9474806.

[12] K. Wang, G. Cao, D. Meng, W. Chen, W. Cao, 'Automatic fall detection of human in video using combination of features', Proceedings - 2016 IEEE International Conference on Bioinformatics and Biomedicine, BIBM 2016, 1228–1233, 2017, doi:10.1109/BIBM.2016.7822694.

[13] S. Maldonado-Bascón, C. Iglesias-Iglesias, P. Martín-Martín, S. Lafuente-Arroyo, 'Fallen people detection capabilities using assistive robot', Electronics (Switzerland), **8**(9), 2019, doi:10.3390/electronics8090915.

[14] T. Hassner, C. Liu, 'Dense image correspondences for computer vision', Dense Image Correspondences for Computer Vision, 1–295, 2015, doi:10.1007/978-3-319-23048-1.

[15] L. Martínez-Villaseñor, H. Ponce, J. Brieva, E. Moya-Albor, J. Núñez-Martínez, C. Peñafort-Asturiano, 'Up-fall detection dataset: A multimodal approach', Sensors (Switzerland), **19**(9), 2019, doi:10.3390/s19091988.

[16] L. Martinez-Villasenor, H. Ponce, K. Perez-Daniel, 'Deep learning for multimodal fall detection', Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics, **2019-Octob**, 3422–3429, 2019, doi:10.1109/SMC.2019.8914429.

[17] M. Sokolova, G. Lapalme, 'A systematic analysis of performance measures for classification tasks', Information Processing and Management, **45**(4), 427–437, 2009, doi:10.1016/j.ipm.2009.03.002.

Advances in Science, Technology and Engineering Systems Journal Vol. 9, No. 6, 21-29 (2024)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

Development and Application of Value *Karuta* to Understand Value in Lean Management: Initial Small-group Trial in Japan and the UK

Tamao Kobayashi, Koichi Murata*

Department of Industrial Engineering and Management, Graduate School of Industrial Technology, Nihon University, Izumi 1-2-1, Narashino City, Chiba, 2758575, Japan

ARTICLE INFO

Article history:
Received: 07 October, 2024
Revised: 05 December, 2024
Accepted: 06 Deember, 2024
Online: 12 December, 2024

Keywords:
Lean management
Value
Card Game
International Comparison
Japan

ABSTRACT

This study proposes the Value Karuta (VK), an application of the traditional Japanese card game karuta. Its goal is to contribute to the understanding of value, which is the first principle of lean management. After stating the problems of lean management and the specifications of VK, this paper confirms the validity of the proposal by discussing two surveys. The first survey explored the utility factors of the cards themselves; it was conducted with a group of students and businesspeople in Japan. The second survey observed the actual situation in the game and was conducted in a group of academics at two UK universities. Both surveys used qualitative methods, such as observation and discussion, and quantitative questionnaires. The results confirm the role of VK as a fundamental tool addressing the need to understand customer value in lean management.

1. Introduction

First, this paper is an extension of work [1] originally presented at the 2023 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM) and contains two surveys. The original work focused on the first survey. This paper also considers the second survey for a comprehensive discussion of the proposal of Value *Karuta* (VK). This necessitated extensive revisions to the Introduction and Literature Review sections of the original work. First, we review the main text.

The difference between the Toyota Production System (TPS) and lean management is that value is added explicitly. This is the first of the five principles of lean management; the other four principles—value stream, flow, pull, and perfection—are included in the TPS. Additionally, across its legacy, there have been many cases in which the methodology has been applied to realize the four principles.

Value can only be defined by the ultimate customer [2], although its identification is difficult. This is because value designers are not customers themselves, and customers are someone else; thus, understanding the value of a customer that one has never met is difficult.

*Corresponding Author Koichi Murata, murata.kouichi30@nihon-u.ac.jp

The second principle is that of the value stream. Although its name includes the word "value," the principle focuses on waste in the value stream. In other words, value is not a direct concern. Value-stream mapping (VSM) is used as a methodology for this principle. It visualizes the overall waste in a value stream. The third to fifth principles include ideas for drastic changes to the value stream and its continuous activities. In other words, the four principles are consistent with the TPS philosophy, namely the absolute elimination of waste [3]. Most studies on lean management have focused on these four principles. The first principle has been addressed in several previous studies. However, if the customer's true value is not understood, the effects of the other principles will not be realized.

This study contributes to understanding customer value, providing an approach that helps people understand many different types of value around the world. Knowing the breadth of the value world suggests the need to understand customer value. To realize this approach, we developed VK by adapting the traditional Japanese card game *karuta*. This paper reports a survey of the initial applications of the game. Two surveys were conducted: the first was conducted in Japan with two groups of university students and businesspeople, and the second was conducted with academics at two UK universities. The first survey focused on the evaluation of the cards, which were game materials. Multiple cards were

https://dx.doi.org/10.25046/aj090603

developed, each containing an academic definition or an example of one value. The survey explored the factors that made these cards effective. The methods used included observing the actual game experience and distributing a questionnaire to the participants. The second survey confirmed whether values were truly being learned from VK, building on the perspectives of the first survey. It also evaluated whether this Japanese card game can be used internationally. These methods are the same as those used in the first survey.

The paper is organized as follows. The next section describes a way of thinking about value in lean management, conventional tools for understanding value, and the relationship between conventional and developed tools. Section 3 describes the research procedure based on two surveys in Japan and the UK in which the game was implemented and evaluated using a questionnaire. Section 4 presents and discusses the research results. Finally, section 5 presents the conclusions of the study.

2. Conventional and Developed Tools

2.1. Value

While searching the literature on values, we discovered that many types of value have been studied. This section reviews 24 types of values by 15 authors of works spanning approximately 150 years, from Marx's time to recent years. These types of value are used in the VK and can be classified into the following four academic fields:

Economics literature illustrates seven types of value: use, exchange, perceived, acquisition, transaction, firm, and intangible value [4-7]. The first four value types were studied relatively early in this review. The fifth and sixth value types were considered in recent years. In seventh value type, intangible resources are becoming what gives firms competitive power.

Psychology literature illustrates two types of value: terminal and instrumental [8]. These two value types comprise the Rokeach Value Survey. Each value has 18 subcategories that organize the essential attributes of human beings. This system continues to be used in numerous investigations.

Sociology literature illustrates three types of value, linking value, cultural value, and dominant social value [9]-[11]. Value in this field expresses social phenomena in the relationships between people. For example, the dominant social value states that the K-pop boom in Korea is a contemporary social phenomenon [11].

Marketing literature illustrates 12 types of value: experience, basis, convenience, sensory, idea, customer, context, consumption, semantic, sticking, self-expression, and environmental value [12]-]19]. Marketing includes the most value types of the four academic fields reviewed in this study. It flourished around the year 2000 and interpreted how people attached meaning to products. Multiple value types are a characteristic of works authored in this field. For example, Wada [14] and Nobeoka [18] propose four and three values, respectively.

This review shows that value has been studied in many fields, especially marketing, which is closely related to the customer. However, no such research has been conducted in the field of lean management.

2.2. Value in Lean Management

How, then, is value handled in lean management? Value is the first of the five principles of lean management [3]. When one reads into the related literature, one learns that if value is not accurately defined, it will be skewed by value chain functions such as strategy, engineering, supplier, and sales. The skew of value (SoV) within each function is as follows [3]:

SoV 1: Preexisting organization-oriented

"Business school-trained senior executives of American firms tell us about their short-term competitive problems and the consequent cost-cutting initiatives."

SoV 2: Technology-oriented

"Designs with more complexity produced with ever more complex machinery were asserted to be just what the customer wanted and just what the production needed."

SoV 3: Supplier relationship-oriented

"The immediate needs of employees and suppliers were prioritized over the needs of the customer, which must sustain any firm in the long term."

SoV 4: Preexisting service-oriented

"Many producers want to make what they are already making. And then, many customers only know how to ask for some variant of what they are already getting."

Lean management has proposed dialogue to overcome SoV. Many value chain players only imagine customer value. If value is something they have never seen before, they will never be able to reach it even if they have a dialogue with the customer.

2.3. Tools to Understand Value in Lean Management and Others

Tools to understand value have been developed outside lean management. The following reviews value proposition (VP) and value engineering (VE) in addition to VSM in lean management.

VSM is a well-known method for identifying waste and improving performance proposed in the lean-manufacturing approach [20], [21]. This tool has been used for process improvement [22] and has been illustrated graphically [23]. Its primary goals are process modeling, investigating process waste, estimating the lead time associated with a certain product flow throughout a system, and estimating process efficiency [24].

The VP is a multifaceted bundle of products, services, prices, communication, and interactions that customers experience in their relationship with the supplier [25]. This conceptualization of the VP as a multifaceted bundle enables a better understanding of the complexity that emerges when integrating sustainability into the value propositions of business models [26].

VE refers to processes designed to reduce costs while maintaining standards [27]. VE complements the target cost and increases the chances of simultaneously reaching cost targets and guaranteeing quality [28].

Although these tools contain the word 'value' within their names, they only consider factors other than value.

2.4. Proposed Value Tool

VK is a valuable tool developed with the concept of "learning value in a fun and easy-to-understand manner" in mind. We have developed VK to be enjoyed as a game. Japan has several indoor games, and *karuta* is a traditional Japanese playing card game [29], [30]. VK was created with reference to the layout and rules of *karuta* [31].

Karuta contributes many functions to Japanese culture, such as community creation and spiritual fulfillment in daily life. It is played in classrooms and family gatherings in Japan, whereas European card games often feature in gambling [32]. *Karuta* also maintains a religious record and features as decoration of Buddhist shrines [33]. Today, competitive *karuta* is a popular sport. Players analyze how to improve their skills using the latest motion capture technology [34]. In an era of low birth rates and an aging society, *karuta* contributes to intergenerational social interactions between older people and children in Japan [35]. Furthermore, it has spread to other Asian countries. For example, an elementary school in Indonesia tried to use *karuta* as a tool for language education [36]. This highlights how *karuta* can have a knowledge acquisition function.

Value *karuta* is designed to understand the 24 types of values described in Section 2.1.

Two cards are used for each value. One was *torifuda* and the other was *yomifuda*. The *torifuda* consists of a front side with the name of the value and an illustration of the corresponding value, and a back side with the name, concept, and outline of the value. The *yomifuda* has three features: the name of the value, an overview, and an easy-to-understand explanation. In the game, one person reads the *yomifuda* (reader) and multiple people read the *torifuda* (takers). The rules are as follows: (1) all cards in *torifuda* are arranged in front of the takers; (2) the reader then reads one *yomifuda*; (3) the takers compete to pick up the *torifuda* with the name of the value read by the reader; and (4) steps (2) and (3) are repeated until no cards remain. Victory or defeat in the game is determined by the number of *karuta* cards taken. Both readers and takers can learn about value through the game. Figures 1 and 2 show examples of *karuta* cards. The advantage of this value tool is that it can be played like a game, and the value can be understood from multiple sources of information. Players receive the visual information of the characters and illustrations written on the *karuta*, and they receive auditory information read during the *karuta* game. Additionally, because *karuta* is a traditional Japanese game, the tool is easily accepted by the Japanese people. A disadvantage of the tool is the need to explain the game to people unfamiliar with *karuta*, including foreigners. Another disadvantage is the fact that the game can only be played with multiple people and not as a single-player game.

3. Research Method

This study consisted of two surveys, as shown in Figure 3. The first survey aimed to evaluate VK materials. The materials refer to the cards that play a central role in the game. The game's success or failure depends on the quality of the materials, and this motivated the first survey. The second survey evaluated the game experience. It aimed to clarify the players' feelings toward the game their impressions of it, and what they learned from the game.

Figure 1: Value Karuta (Japanese version) (From left to right, torifuda, torifuda back, yomifuda)

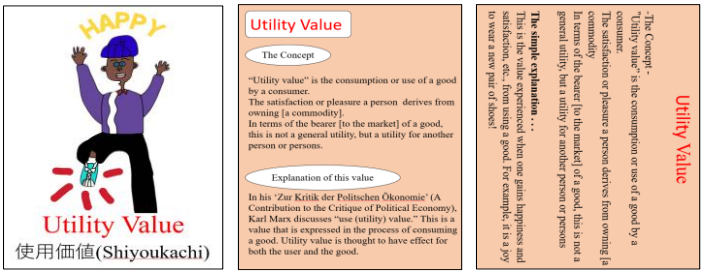


Figure 2: Value Karuta (English version) (From left to right, torifuda, torifuda back, yomifuda)

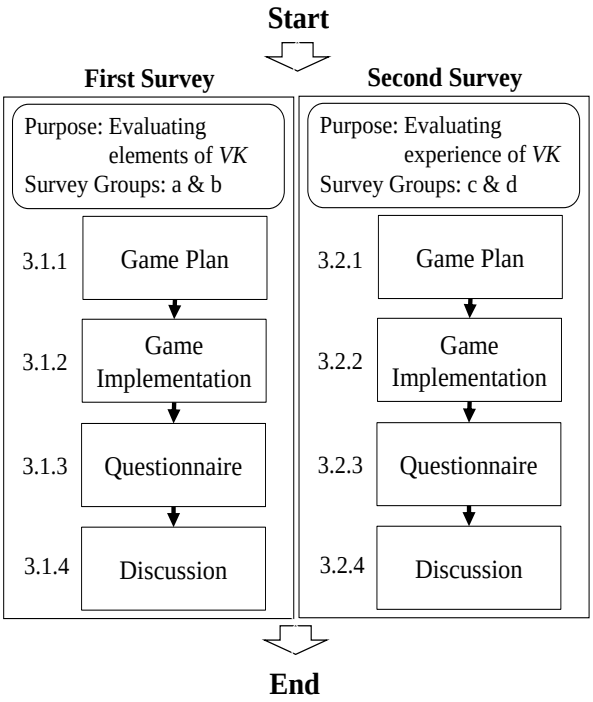


Figure 3: Survey Procedure

Both surveys followed the same four steps: game plan, game implementation, questionnaire, and discussion. Details of the procedure for each survey are provided below.

3.1. First Survey

3.1.1 Game Plan

The survey involved two groups, Group a and Group b. Group a consisted of 13 college students in their twenties, six men and seven women. Two male students were foreigners (Chinese and Turkish), whereas the other students were Japanese.

Group b consisted of seven practitioners of different ages: one in their twenties, two in their thirties, two in their forties, and two in their fifties. There were four males and three females. All were Japanese. Their industries included manufacturing, retail, tax accounting, and real estate.

3.1.2 Game Implementation

Each group played the game twice. When conducting the experiment, we prepared an environment in which the cards were spread out, and the participants could sit around them.

The game for Group a was held at a university seminar camp. In the gymnasium, cards were laid out on the floor, and the game was played while players sat on the floor. The game for Group b was held as an icebreaker for a seminar on lean management. The cards were arranged on a table in the seminar venue, and the participants sat on chairs to play the games.

3.1.3 Questionnaire

After the game ended, we distributed a questionnaire consisting of Questions A–G. Question A was, "Were you satisfied?" This was the players' overall rating of the game. The respondents were asked to respond on a three-point scale (satisfied, neutral, and dissatisfied) and state the reasons for their responses. Question B was, "How was the visibility of the characters on the table of the *torifuda*?" Question C was, "How was the visibility of the characters on the back of the *torifuda*?" Question E was, "How was the visibility of the picture?" These four questions were used to evaluate *karuta*. There were three levels: bad, normal, and good. Question D was, "How much did you enjoy the game?" The aim was for players to have fun. The respondents answered on a six-level scale: 100%, 80%, 60%, 40%, 20%, and 0%. Question F was, "Please write down your favorite value." This item investigated which value players tend to recall and therefore which value tends to leave an impression. Last, Question G was, "Please write down any good points or concerns you have about this game in free description."

3.1.4 Discussion

We analyzed whether the game was effective in promoting the understanding of value. From the results of the questionnaire, we extracted the internal and external factors that promoted the understanding of value. Issues raised by these results were examined further in the second survey.

3.2. Second Survey

3.2.1 Game Plan

The survey had two groups, Group c and Group d. Group c consisted of 15 academics from different UK universities: three in their twenties, seven in their thirties, one in their forties, one in their fifties, and three of unknown ages. There were eight males, four females, and three of unknown gender. Nationality was mixed.

Group d consisted of six academics from a UK university not included in Group c. Three were in their thirties, one in their forties, one in their fifties, and one of unknown age. Nationality was mixed.

3.2.2 Game Implementation

In the first survey, the game was played as part of an event. Before the game, the participants received an explanation of the game rules. In the second survey, the game was played after receiving a detailed explanation of its background and purpose.

Both groups' games were held at UK universities. Another purpose of this second survey was to understand whether *karuta*, a card game that is culturally Japanese, would be accepted in an international environment. For this purpose, we also created and used *karuta* translated from Japanese into English. The cards were made of Washi paper, which is a traditional Japanese paper.

Both groups played the game twice. They arranged cards on a table in the meeting room and sat in chairs to play the game.

3.2.3 Questionnaire

The questionnaire for the second survey consisted of Questions A2–G2. Question A2 was, "Which types of value left an impression on you?" The participants were asked to write an answer regarding the type of value that made an impression on them while playing the game. Question B2 was "How well do you understand value?" Using a five-point scale (5 = understand well, 1 = do not understand), we evaluated whether participants were able to understand value by playing the game. Question C2 was, "Please tell us why you chose the number in Question B2." This item was used to determine the points at which the participants understood the value during the game. Question D2 was, "Please tell us about the difficulty level of VK." Using a five-point scale (5 = easy, 1 = difficult), participants were asked to rate how easy it was to play the game. Question E2 was, "Please tell us your impression of the appearance of VK." It asked the participants how they felt about the game's appearance. The evaluation was performed by selecting one or more of the following seven items: pretty, pleasant, bright, cool, sober, quiet, and other. Question F2 was, "Please tell us about a scene in the game that left an impression on you." This aimed to determine when players concentrate while playing the game. The participants were asked to select one or more of the following four items: "When taking a card," "When looking for a card," "When deciding the winner," and "Other." Question G2 was, "If you have any other comments or opinions, please let us know." These questions sought opinions on aspects of the game other than those addressed in the previous six questions.

3.2.4 Discussion

This step demonstrates the possibility of promoting an understanding of value through VK. The first survey confirmed the effectiveness of the game's materials, specifically the cards themselves. Additionally, the second survey confirmed whether VK would be enjoyable for players who were unfamiliar with the game and whether these players had time to think about value.

4. Research Results

4.1. First Survey Results

Table 1 shows the questionnaire answers by Group a. Twelve people answered "Satisfied," and one person answered "Neither" to Question A. Men who answered "Satisfied" were satisfied with the overall design of the game and *karuta*. The women were satisfied with the cuteness of the illustrations and the rules of the game. Men who answered "Neither" were dissatisfied with the

game's outcome. For Question B, 12 people answered "Good," and one person answered "Bad." For Question C, 12 people answered "Good," and one person answered "Normal." For Question D, 12 out of 13 people answered "100%," and one answered "80%." For Question E, 11 out of 13 people answered "Good," and two answered "Bad." For Question F, two people listed the link and commitment values (respectively), and the other eight values were each listed by one person. These are the value types whose meanings can be inferred from their names. Question G was answered by 8 out of 13 people, five of whom were anonymous. Men's impressions considered how to play *karuta* and the environment. Women's impressions considered the cuteness and fun of *karuta*.

Table 1: Questionnaire Results for Group a

Question	Evaluation	Number of people	Gender		Comment
			Men	Women	
A	Satisfied	12	5	7	*1
	Neither	1	1	0	*2
	Dissatisfied	0	0	0	−
B	Bad	1	1	0	
	Normal	0	0	0	
	Good	12	5	7	
C	Bad	0	0	0	
	Normal	1	1	0	
	Good	12	5	7	
D	100%	12	5	7	
	80%	1	1	0	
	60, 40, 20, 0%	0	0	0	
E	Bad	2	1	1	
	Normal	0	0	0	
	Good	11	5	6	
F	Link Value	2	1	1	
	Sticking Value	2	2	1	
	Intellectual Value	1	1	0	
	Semantic Value	1	1	0	
	Convenience Value	1	1	0	
	Corporate Value	1	0	1	
	Environmental Value	1	0	1	
	Exchange Value	1	0	1	
	Social Value	1	0	1	
	Transaction Value	1	0	1	
G	With Comments	8	3	5	*3
	No Comments	5	3	2	

<Comments on Question A>

*1: That was very fun. / The text and images were easy to understand. The fact that an English notation was included was good. / It was good to know various types of value. / I learned a lot of different values. / I learned a lot of new values. The pictures were cute and fun. / I was able to know the value that I do not usually use. / Good to know the value. /Aiming to be number one, we were able to do it while cooperating. / It was fun. The difference in game activity was easy to understand. / It was fun.

*2: The number is slightly less.

<Comments on Question G>

*3: It is hard to judge by looking at a picture. / Good to learn about value. / Perfect with cushions. / The letters were easy to read, and the pictures were cute. / The pictures were so cute and funny. / I was able to study in an easy-to-understand manner and enjoyed it. / It was nice to have cute pictures on all the karuta cards. I had fun. Thank you. / Good to learn about value. / The writing on the back of the card was a little hard to read. However, I thought it would be easy to understand and global owing to the word notation.

Regarding Group b (Table 2), five people answered "Satisfied," and two answered "Neither" to Question A. Men who answered "Satisfied" commented on the rules of *karuta* and their impressions of *karuta* itself, as well as their nostalgia for playing *karuta*. One commented on the women he enjoyed playing with and how nice the illustrations were. Those who answered "Neither" offered advice on how to improve the rules to achieve the game's goals. All respondents answered "Good" to Questions B and C. Question D was 100% for four people and 80% for three people. All the respondents answered "Good" to Question E. Question F assessed the ability, semantics, and instrumental values. All the respondents answered Question G. Participants primarily raised suggestions for improving the *karuta* rules.

Table 2: Questionnaire Results for Group b

Question	Evaluation	Number of people	Gender		Comment
			Men	Women	
A	Satisfied	5	4	1	*1
	Neither	2	1	1	*2
	Dissatisfied	0	0	0	−
B	Bad	1	1	0	
	Normal	0	0	0	
	Good	7	4	3	
C	Bad	0	0	0	
	Normal	1	1	0	
	Good	7	4	3	
D	100%	4	2	2	
	80%	3	2	1	
	60, 40, 20, 0%	0	0	0	
E	Bad	0	0	0	
	Normal	0	0	0	
	Good	7	4	3	
F	Ability Value	1	1	0	
	Semantic Value	1	0	1	
	Instrumental Value	1	0	1	
	Perceived Value	1	1	0	
	Intangible Value	1	0	1	
	Link Value	1	1	0	
	Unanswered	1	1	0	
G	With Comments	7	5	3	*3
	No Comments	0	0	0	

<Comments on Question A>

*1: It was fun. I think I noticed a lot. However, I think it would be more interesting if the rules were stricter than the karuta itself. / I played karuta for the first time in a while. / I really liked the illustrations. I had a lot of fun learning about values. I had no idea it was worth so much. Please keep doing a good job. / I was able to learn about value while having fun. I learned a lot. / The illustrations were very nice.

*2: It was fun but difficult. / The content was very interesting and a new experience, but I still do not fully understand it.

<Comments on Question G>

*3: It was hard to tell the difference between the values. / The value and its explanation just could not connect, but it was fun. / It is the perfect icebreaker because moving your body creates conversation and stimulates your intellectual curiosity. Awareness of "heh" is a strong motivation to read the text. / It was great to get to know each other as an icebreaker, and it was a great opportunity to learn about values. But the best part was being able to talk to all the students. It was great because I do not usually talk with students. / The pictures were so unique and cute! I think I would have been more absorbed in playing *karuta* if I had had more time to deepen my understanding. It has been a long time since I have played karuta in this form, and it was a lot of fun! / I was able to learn the value through the game (*karuta*) using pictures and easy-to-understand words, so I thought it would be a good idea to get it into my head more smoothly. I would like to hear a more detailed explanation of each value. / I think you can enjoy learning about value through *karuta*. I think it was good that I chose *karuta* as a tool. How about

creating a *karuta* role with rules that are conscious of the understanding and connection of the game and value of *karuta*? Five points if you have XX value, XX value, and XX value, which are connected to XX.

The results of the questionnaire survey confirmed three factors that make the VK effective: (1) nostalgia and design, (2) Japanese naming and type, and (3) the implementation environment. Each of these factors is discussed below.

Regarding nostalgia and design, two observations can be drawn from the questionnaire results. First, *karuta* is a game played by Japanese people when they are young. This is evident from the comment by the businesspeople group: "I played *karuta* for the first time in a long time." Second, the college students expressed many opinions about the illustrations, such as "The pictures were very cute and interesting" and "I'm glad that all the *karuta* cards have cute pictures on them." The illustrations on the *karuta* cards create familiarity.

For naming and Japanese type, college students and businesspeople listed two value types in Question F: linked value and semantic value. Among the 34 values, the linked value was the only one in Japanese *katakana* notation. From the college students' answers, multiple people listed the sticking value. Among the 34 types, the commitment value was the only one in *hiragana* notation. Because the other 32 symbols were written in Chinese characters, it can be assumed that they left an impression. Additionally, it is easy to imagine the meaning of the word "stickiness," and the word "link" has an image that makes one wonder and want to investigate. Both are attractive words that modify value, suggesting that the naming and notation of types of value influence their understanding.

Third, the implementation environments differed between the two groups. The college student group held an event during a seminar camp, whereas the businesspeople held an educational seminar. Comparing the comments on Question G, the college student group had monotonous impressions of the game, such as "It was fun" and "It was interesting." The businesspeople group said, "I want to hear more detailed explanations about each value." This answer makes one aware of technical aspects, such as the rules of VK and the motivation for value learning.

4.2. Second Survey Results

Regarding Group c (Table 3), responses were received from 15 people: eight were men, four were women, and three did not answer. Their ages ranged from their twenties to their fifties, with an average of 30 years. For Question A1, three people answered "Link Value," and two answered "Cultural Value" and "Dominant Value," respectively. For Question B2, the average level of understanding of value was 3.6, and for Question D2, the average level of difficulty was 3.4. From Question E2, 20% of participants answered "pretty" and "bright" regarding the cards' appearance. From Question F2, 53% of participants answered "when looking for a card" regarding the most memorable moment. Nine participants provided a free-form descriptions in Question G2.

Six people answered in Group d (Table 4). Four patients were men and two were women. Their ages ranged from their twenties to their fifties, with an average of 30 years. For Question A2, six respondents provided different answers regarding memorable values. For Question B2, the average understanding of the value types was 3.8, and the average difficulty of Question D2 was 3.5. From Question E2, 67% answered "Pretty" regarding the appearance of the card. From Question F2, 67% answered "when looking for a card" regarding memorable moments. Everyone provided free-form descriptions for Question G2.

Table 3: Questionnaire Results for Group c

Question	Evaluation	Number of people	Gender			Comment
			Men	Women	No Response	
A2	Link Value	3	3	0	0	
	Dominant Value	2	2	0	0	
	Cultural Value	2	2	0	0	
	Environmental Value	1	1	0	0	
	Social Value	1	1	0	0	
	Transaction Value	1	0	0	0	
	Social Value	1	0	0	0	
	Firm Value	1	0	0	0	
	Terminal Value	1	0	0	0	
	Convenience Value	1	0	0	0	
	Intangible Value	1	0	0	0	
	Context Value	1	0	0	0	
	Perceived Value	1	0	0	0	
	Self-Expression Value	1	0	0	0	
	Idea Value	1	0	0	0	
B2	1 (Not Understood)	0	0	0	0	–
	2	3	1	2	0	*1
	3	3	1	2	0	*2
	4	6	4	0	0	*3
	5 (Well Understood)	3	2	0	0	*4
D2	1 (Difficult)	0	0	0	0	
	2	2	1	0	1	
	3	6	3	2	1	
	4	3	2	1	0	
	5 (Easy)	2	1	0	1	
E2	Pretty	7	6	0	1	
	Pleasant	5	3	1	1	
	Bright	7	4	2	1	
	Cool	6	3	1	2	
	Sober	2	2	0	0	
	Quiet	1	0	1	0	
	Other	2	1	0	1	*5
F2	When Taking a Card	4	1	0	3	
	When Looking for a Card	9	4	4	1	
	When Deciding the Winner	2	1	0	1	
	Other	1	1	0	0	*6
G2	With Comments	9	5	1	3	*7
	No Comments	6	3	3	0	

<Answers to Question C2>

*1: The value is a bit hard to understand. / Some values are hard to understand. / Because my English is not good. So interesting is better.

*2: New value for me. / I could not hear the reader clearly. / I am not familiar with each value.

*3: New topic to me - Enjoyed learning while playing Karuta. / I can understand more types of value. / Visual link between theory and images is practical. / It affects us. / I do not have knowledge on this topic, but the game helps.

*4: It was easy with the image and hints in the description. / I can understand most meanings with the cards.

<Other comments of Question E2>

*5: Lose! / Fun / Entertainment

<Other comment of Question F2>

*6: Listening intently.

<Comments on Question G2>

*7: I think it would be better to first let the player familiarize themselves with the intention of the concept before they play. / This is a good game. / Sometimes, it is not clear what the reader read. -> It's a fun game. / Thank you. It was a good idea to use this game. / Thank you.

Table 4: Questionnaire Results for Group d

Question	Evaluation	Number of people	Gender		Comment
			Man	Women	
A2	Customer Value	1	1	0	
	Cultural Value	1	0	1	
	Perceived Value	1	0	1	
	Consumption Value	1	1	0	
	Other	2	2	0	*1
B2	1 (Not Understood)	0	0	0	–
	2	0	0	0	
	3	2	1	1	*2
	4	3	2	1	*3
	5 (Well Understood)	1	1	0	*4
D2	1 (Difficult)	0	0	0	
	2	0	0	0	
	3	2	0	2	
	4	2	2	0	
	5 (Easy)	1	1	0	
E2	Pretty	7	1	2	
	Pleasant	5	4	1	
	Bright	1	1	0	
	Cool	3	3	0	
	Sober	0	0	0	
	Quiet	0	0	0	
	Other	1	1	0	*5
F2	When Taking a Card	2	1	1	
	When Looking for a Card	3	2	1	
	When Deciding the Winner	1	1	0	
	Other	0	0	0	
G2	With Comments	6	4	2	*6
	No Comments	0	0	0	

<Answer to Question A2>

*1: Friendship / Selecting the correct answer was not easy.

<Comments on Question C2>

*2: Previous experience with research. / Value is sub stateless.

*3: Value is a spoof topic and needs further discovery. / This game made me understand different types of value. / Because of my past research on value.

*4: Experience

<Comment on Question E2>

*5: Paper^^

<Comments on Question G2>

*6: Great Game! I had a lot of fun! Thanks! / Thank you, was cursed. / Thank you! / Very pleasant way to learn about value. / Great game to engage with. Fun game, great way to teach and clarify different concepts. Great! / It is a very nice game.

The questionnaire results showed that the game has mostly been well received in the international environment. To be clear, some comments could be interpreted as lip service.

For Question E2 on the appearance of the card itself, "Pretty" was the most common impression for both groups. This demonstrates a similar tendency to what was observed in the first survey. Players, therefore, have positive experiences of the game, regardless of nationality.

Questions D2, F2, and some comments suggested that the game was not difficult or incomprehensible, and the participants were able to concentrate on it. In particular, many participants selected "When looking for a card" in Question F2.

Descriptions of everyday life written on *torifuda* cards are easy for Japanese people to understand and are important hints for finding cards. However, some players commented that the game was too Japanese and difficult for them to understand without cultural context. It is therefore debatable whether the purpose of the game is to understand Japanese culture or types of value.

In both groups, participants found conversations about types of value worthwhile. Even if they chose the wrong card, their mistakes increased their fun as players of the game. This was rarely seen when the game was played in Japan. This difference may provide cross-cultural insights.

From the results of Question A2, as in Japan, there was little overlap in the types of value that made an impression on participants. This result shows that, even if people live in the same environment, they resonate with different value types. In other words, it demonstrates the need to sincerely perceive values other than one's own. This finding implies that the first principle of lean management is important.

4.3. Discussion of Both Surveys' Results

Lean management requires dialogue to understand customer value. Customers are entirely unknown to value chain functions. It is even difficult to understand one's own family and friends. However, value chain functions must understand their customers' needs. Moreover, this understanding includes economic considerations that skew the true value. To address this challenge, this study proposed a new card game. Two surveys were conducted to confirm that the card game is useful for generating dialogue on value. The corresponding results are summarized as follows:

First, the proposed card game utilizes the fun characteristics of card games. In addition, the card game players accepted pictures of each value drawn on each card. Furthermore, the card game is enjoyable for both Japanese people and foreigners. Japanese people can enjoy the card game as a nostalgic experience echoing childhood memories, and non-Japanese people can gain a good experience of Japanese culture. The material and cultural aspects of the card game create a shared platform for producing dialogue between card game players.

Second, each card has one meaning. However, each player has a slightly different interpretation of each card and its meaning. This situation promotes dialogue while playing games. In the original *karuta*, players compete on the number of cards they take, so taking the wrong card leads to a loss. However, in the proposed

karuta, they may experience more enjoyment sharing their understanding of a value when taking the wrong card.

5. Concluding Remarks

In this study, new tools were developed for learning about and applying value. Its utility mainly lies in the ingenuity of providing knowledge about value types using *karuta* with a game-like nature.

In general, acquiring academic knowledge is difficult. *Karuta* was used to ease this difficulty, and simple sentences and pop pictures were found to be effective. This multiplayer game generated substantial conversations among groups in the UK. This phenomenon promoted an understanding of value.

This new tool for directly thinking about value brings benefits to both industry and academia. For industry, by combining a game-like experience with indirect analysis tools such as VSM, VP, and VE, their functions are expanded. This leads to a richer analytical perspective with clearer recognition of the original purpose of VSM, VP, and VE, which is to improve value. For academia, the proposed tool combines a conceptual approach with a practical methodology for value studies. In doing so, it will contribute to promoting the application of understandings of value throughout society.

There are two possible future studies on this topic. The first aims to improve the game to further promote the understanding of value, and the second adjusts the design of this game to help businesspeople. The first strengthens the motivation to understand value. Card games, including *karuta*, have a completion principle: they promote motivation to win. The rules of the game can be improved using this principle. The second study addresses how to utilize the learnings from the game. This relates to the first principle of lean management and supports the understanding that various values exist. Customers of this tool will be predominantly businesspeople. They strive to reduce waste and increase profits. To contribute to their goals, this study must specifically define the role of the game in their activities.

A limitation of this study is that it was based on a simple questionnaire, and because the survey samples were small, the sample size should be increased for statistical analysis in future studies. A more elaborate experimental design will aim to verify earlier results. It is also hoped that more people will experience and understand VK and that the system will be developed to enrich their daily lives. This ought to contribute to the acquisition of new words and awareness of concepts that can be freely expressed in the real world. VK also focuses on understanding the types of value. Therefore, one limitation is how these values can be applied to actual problems. In future, the development of a methodology to address this challenge of application should be considered.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] T. Kobayashi, Y. Ishizaki, H. Tukamoto, M. Sugi, M. Nakane, K. Murata, "A Study on Utility Factors of Value Karuta-Application to College Student and Business Person Groups," in 2023 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), 0865-0869, 2023, doi: 10.1109/IEEM58616.2023.10406441.

[2] J. P. Womack, D. T. Jones, Lean thinking: Banish waste and create wealth in your corporation, Revised and updated, Free Press, 2003.

[3] T. Ōno, Toyota production system: Beyond large-scale production, Productivity Press, 2019.

[4] K. Marx, trans. B. Fowkes, Capital vol. 1: A critique of political economy, Penguin Classics, 1992.

[5] K.B. Monroe, Pricing: Making profitable decisions, McGraw-Hill, 1990.

[6] P.G. Berger, E. Ofekb, "Diversification's effect on firm value," Journal of Financial Economics, **37**(1), 39-65, 1995, doi.org/10.1016/0304-405X(94)00798-6.

[7] L.A. Eisfeldt, E. Kim, D. Papanikolaou, "Intangible value," **28056**, National Bureau of Economic Research, 2020, doi:10.3386/w28056.

[8] M. Rokeach, The nature of human values, Free Press, 1973.

[9] B. Cova, "Community and consumption: Towards a definition of the "linking value" of product or services," European Journal of Marketing, **31**(3/4), 297-316, 1997, doi.org/10.1108/03090569710162380.

[10] C. Marzilli, "Concept analysis of value," International Journal of Recent Advances in Multidisciplinary Research, **3**(11), 1919-1921, 2016, hdl.handle.net/10950/1197.

[11] E. Nesmeyanov, Y. Petrova, R. Bachieva, O. Vasichkina, "The concept of value in modern youth subcultures of K-pop and brony in the period of globalization," SHS Web of Conferences, **72**, 1-6, 2019, doi.org/10.1051/shsconf/20197203025.

[12] B.H. Schmitt, Experiential marketing: How to get customers to sense, feel, think, act, relate, Free Press, 1999.

[13] B.H. Schmitt, A. Simonson, Marketing aesthetics, Prentice Hall, 1997.

[14] M. Wada, Brand Planning and Brand building (Burando kachi kyouso) (in Japanese), Dobunkan Publisher, 2002.

[15] B. Dodds, Managing customer value: Essentials of product quality, customer service, and price decisions, University Press of America, 2003.

[16] J.E. Finch, "The impact of personal consumption values and beliefs on organic food purchase behavior," Journal of Food Products Marketing, **11**(4), 63-76, 2006, doi.org/10.1300/J038v11n04_05.

[17] L.S. Vargo, R. F. Lush, "Evolving to a new dominant logic for marketing," Journal of Marketing, **68**(1), 1-17, 2004, doi.org/10.1509/jmkg.68.1.1.24036.

[18] K. Nobeoka, "Creation of premium value in new product development to avoid commoditization," Journal of Economics and Business Administration, **194**(6), 1-14, 2006, doi: 10.24546/00056119 (in Japanese).

[19] E. Fraj, E. Martinez, "Environmental values and lifestyles as determining factors of ecological consumer behavior: An empirical analysis," Journal of Consumer Marketing, **23**(3), 133-144, 2006, doi.org/10.1108/07363760610663295.

[20] S. Ghosh, K. Lever, "A lean proposal: development of value stream mapping for L'Oreal's artwork process," Business Process Management Journal, **26**(7), 1925-1947, 2020, doi.org/10.1108/BPMJ-02-2020-0075.

[21] B. Singh, S.K. Garg, S.K. Sharma, "Value stream mapping: Literature review and implications for Indian industry," Advanced Manufacturing Technology, **53**(5-8), 799–809, 2011, doi: 10.1007/s00170-010-2860-7.

[22] A. Dadashneiad, C. Valmohammadi, "Investigating the effect of value stream mapping on operational losses: A case study," Journal of Engineering, Design and Technology, **16**(3), 478-500, 2018, doi.org/10.1108/JEDT-11-2017-0123.

[23] F. Jacobs, R.B. Chase, Operations and supply chain management, McGraw-Hill Education, 2017.

[24] I. Alsyouf, R. Al-Aomar, H. Al-Hamed, X. Qiu, "A framework for assessing the cost effectiveness of lean tools," European Journal of Industrial Engineering, **5**(2), 170-197, 2011, doi.org/10.1504/EJIE.2011.039871.

[25] E.D. Ouden, Innovation design: Creating value for people, organizations, and society, Springer, 2012.

[26] H. S. Kristensen, A. Remmen, "A framework for sustainable value propositions in product-service systems," Journal of Cleaner Production, **223**,

25-35, 2019, doi.org/10.1016/j.jclepro.2019.03.074.

[27] P.G. Patterson, R.A. Spreng, "Modelling the relationship between perceived value, satisfaction and repurchase intentions in a business-to-business, services context: An empirical examination," Service Industry Management, **8**(5), 414-434, 1997, doi.org/10.1108/09564239710189835.

[28] C. Homburg, A. Hoppe, R. Schick, "Accounting for preference dependency in target costing - a note," Quantitative Finance and Accounting, **57**, 845-858, 2021, doi.org/10.1007/s11156-021-00962-9.

[29] H. Miyakawa, N. Kuratomo, H. E. B. Salih, K. Zempo, "Auditory Uta-KARUTA: Sonificated card game towards inclusive design," in The 32nd Annual ACM Symposium on User Interface Software and Technology, 90-92, 2019, doi.org/10.1145/3332167.3357125.

[30] S. Yanagihara, H. Koga, "Differences in human and AI memory for memorization, recall, and selective forgetting," Societal Challenges in the Smart Society, 371-384, 2020.

[31] T. Saito, A four-letter idiom karuta that can be learned aloud by Takashi Saito (Saito Takashi no koe ni dashite oboeru yozizyukugo karuta) (in Japanese), Gentosha, 2021.

[32] L.M. Jiang, "A short visual history of abstraction in early modern Japanese Karuta: simplification, reinterpretation, and localization," Journal of Asian Humanities at Kyushu University, **7**, 61-83, 2022, doi.org/10.5109/4843130.

[33] L.M. Jiang, "Sacralizing the playful secular: The deity of Karuta-gambling at the Nose Kannon Hall in Sannohe, Aomori," Arts, **13**(27), 1-16, 2024, doi.org/10.3390/arts13010027.

[34] R. Kitagawa, T. Itoh, "Visualization of swiping motion of competitive Karuta using 3D bone display," in 27th International Conference Information Visualization (IV), 346-351, IEEE, 2023, doi: 10.1109/IV60283.2023.00065.

[35] T. Kamei, W. Itoi, F. Kajii, C. Kawakami, M. Hasegawa, T. Sugimoto, "Six month outcomes of an innovative weekly intergenerational day program with older adults and school‐Aged children in a Japanese urban community," Japanese Journal of Nursing Science, **8**(1), 95-107, 2011, doi.org/10.1111/j.1742-7924.2010.00164.

[36] H. Azimah, "Effect of using Karuta cards on students' ability to comprehend vocabulary (Experimental research for the seventh grade at Sabilul Mukminin Boarding School Binjai)," Jurnal Pendidikan Indonesia, **5**(5), 177-184, 2024, doi.org/10.59141/japendi.v5i5.2772.

Advances in Science, Technology and Engineering Systems Journal Vol. 9, No. 5, 21-29 (2024)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

Evaluation of a Classroom Support System for Programming Education Using Tangible Materials

Koji Oda* [1], Toshiyasu Kato [2], Yasushi Kambayashi [3]

[1]*Department of Information and Telecommunication, Saitama Prefectural Kawaguchi Technical High School, Kawaguchi, 333-0846, Japan*

[2]*Department of Information and Media Engineering, Nippon Institute of Technology, Minamisaitama, 345-0826, Japan*

[3]*Department of Informatics and Data Science, Sanyo-Onoda City University, Sanyo-Onoda, 756-0884, Japan*

ARTICLE INFO

Article history:
Received: 14 September, 2024
Revised: 08 October, 2024
Accepted:09 October, 2024
Online: 18 October, 2024

Keywords:
Tangible materials
Programming education
Classroom support systems
Face-to-face instruction

ABSTRACT

In recent years, the utilization of tangible educational materials has attracted attention on educational settings. They provide hands-on learning experiences for beginners. This trend is especially notable in the field of programming education. Such educational materials are employed in many institutions worldwide. They liberate learners of programming from programming languages that are confined in a small computer screen. On the other hand, in the school setting, classroom time is limited. When instructing more than thirty students, it is hard for instructors to provide adequate guidance for everyone. To address this problem, we have developed a classroom support system for programming education that complements the use of tangible educational materials. With this system, instructors can monitor the real-time progress of each student during the class and analyze which parts of the program many students find challenging. Based on these analytical results, instructors can provide appropriate instructions for individual students and effectively conduct the class. This system is suitable for programming education in high schools. It quantifies each student's ability of programming and track the progress of each student. We administered a questionnaire to both the students and the instructor. The results of the questionnaire show our system is well received by both students and the instructor. Even though our system demonstrates some usefulness for programming beginners, we are aware that our system has some serious limitations such as our rigid model answers.

1. Introduction

This paper is an extension of work originally presented in *2024 Twelfth International Conference on Information and Education Technology* (ICIET 2024) [1]. The work presented the basic idea of system and the results of the preliminary experiments that indicated its usefulness. In this paper, we have extended the paper to explain our system in details and to demonstrate its effectiveness through showing results of larger scale experiments. For programming beginners, numerous GUI programming systems have been proposed. However, the computer screen and the display resolution restrict the students' recognizability of program elements. This problem makes the programming activities difficult especially with lower resolution displays. To address this issue, we developed tangible educational materials named "Jigsaw Coder" for programming education [2]. In the following, we will refer to this as JC. JC consists of multiple cards. Each card has QR code printed on it, and students can construct programs by rearranging them. This enables programming on a desk or even on the floor, which provides much larger space. The user can take a photo to read the complete program by their smartphones and also execute the program on their smartphone. However, such tangible educational materials were designed for self-taught of individual learners. It is challenging for class room use; it is hard for instructors to grasp the progresses of all students when used in a class of more than a few, e.g. thirty, students. The objective of this study is to design and to implement a system that provides instructors information of real-time progresses of the students so

*Corresponding Author: Koji Oda, Saitama Prefectural Kawaguchi Technical High School. mooda194lun@yahoo.co.jp

that he or she can analyses information of students' programming in classes using JC. The system helps instructors to practice much effective use of instruction time.

The authors conducted a preliminary evaluation of JC as prior research [1]. As a result of performing a functional check assuming an actual class, there were no issues with the system's operation with around ten users, and it was possible to conduct a trial evaluation simulating an actual class. This paper demonstrates the effectiveness of JC through an evaluation experiment conducted in actual high school classes.

2. Research Methodology

We have developed a tangible programming system that utilizes JC and Micro:bit for educational purpose. This system allows students to engage in tangible programming, while instructor can monitor their progresses in real-time and perform analysis over their achievements. Subsequently, we conducted classes as part of the evaluation experiments and administrated questionnaires for both instructor and students to assess the effectiveness of the system. In the previous papers, we reported our development and evaluation of the tangible educational materials [3, 4]. The materials involve rearranging multiple cards to program. Then the user makes the system read the QR codes printed on them using a smartphone to execute the program. We call this card-type tangible educational system as JC. Figure 1 shows the flow of the programming process. In the original JC, we used a smartphone; in this study, we decided to utilize Chromebooks, because they are easy to use and widely adopted in many Japanese schools.

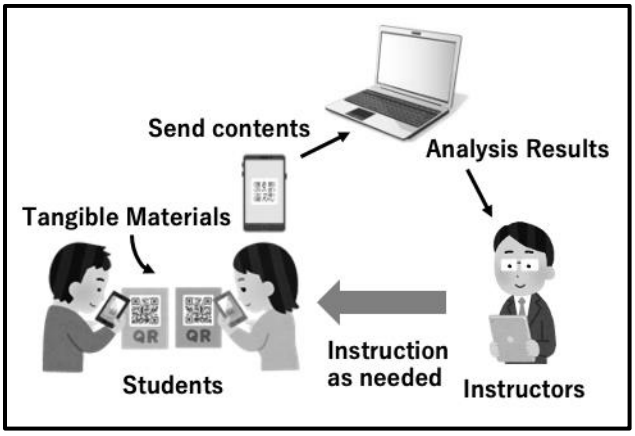


Figure 1: Instruction utilizing tangible education materials

2.1. JC

A client PC (Chromebook) creates a program from QR cards and writes it to the Micro:bit. Simultaneously, the program code is transferred to the server. The server then analyzes the received program code. The analysis flow is as follows.

The server saves the program code as a file and compares it with the corresponding model answer. In the comparison process, it calculates the matching rate with the model answer and identifies the positions of incorrect sections. The answer data for each student--such as student name, first answer time, most recent answer time, final answer time, number of responses, matching rate with the model answer, line numbers and positions of mistakes, and program level--is stored in the database. Subsequently, a web page reads the database and displays the answer information for each student. At this point, based on the answer information, students are classified into three categories: Unanswered, Progress, and Completed. This allows the instructor to easily track each students' progress at a glance. Additionally, a page is generated that allows the instructor to review each students' answer. On this page, it is easy to identify missing, extra, or incorrect parts of the answer. Based on this information, the instructor can provide specific feedback to the students.

2.2. Micro:bit

Micro:bit is a microcontroller designed by the British Broadcasting Corporation (BBC) for programming education. It can display characters and shapes on LEDs and produce sound through a speaker. It also features sensors such as an accelerometer, magnetometer, microphone, temperature sensor, and light sensor, which allow it to recognize vibrations and changes in its environment. Additionally, Micro:bit includes wireless communication capabilities, enabling it to communicate with other Micro:bit. Programming can be done via a browser or app, and programs can be transferred to the Micro:bit for execution. Figure 2 shows a Micro:bit.

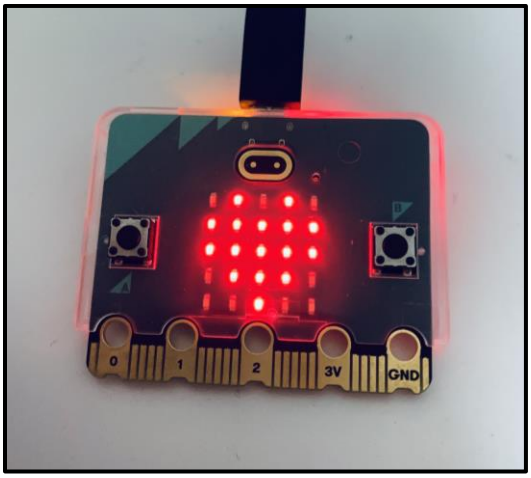


Figure 2: Micro:bit

3. Design And Implementation

We developed our system using Python. The reason for choosing Python is its high readability due to a vast array of libraries. This fact let us build shorter programs. In addition, Python is an interpreted language, enabling immediate execution without compilation, making it suitable for creating prototypes. To run the proposed system, some preparations are needed. The preparation before the class includes:

1) Creating tasks for students (assigning unique task numbers).
2) Creating and placing example answer programs and level configuration files.
3) Inputting students' information.

Carrying out a programming class includes:

1) Starting the server and server program.

2) Connecting Micro:bit to student's Chromebook.

3) Starting the client program.

3.1. Improvement of Jigsaw Coder

In this project, we added three more elements to enable more intuitive rearrangements. The first element is emphasizing the task number. To distinguish which task the student is working on, he or she initially needs to make the system read the QR code for the task number card in JC. Then, the background color of the task number card was changed, and highlighted the numbers by surrounding them with star symbols. The second element is the use of symbols "⊳" and "⊲". These symbols represent the role of "{" and "}" in the conventional programming languages such as C and Java. They are used to denote looping constructs like "Repeat ⊳" and "⊲ End here," aiding in the intuitive understanding of grouping. The third element is "→" and "←", representing arranging cards side by side. These symbols are utilized when specifying conditional statements, such as "If Condition →" and "← Press A Button ⊳". These symbols help learners intuitively grasp the utilization and representation of conditions. Figure 3 shows the cards used by the students.

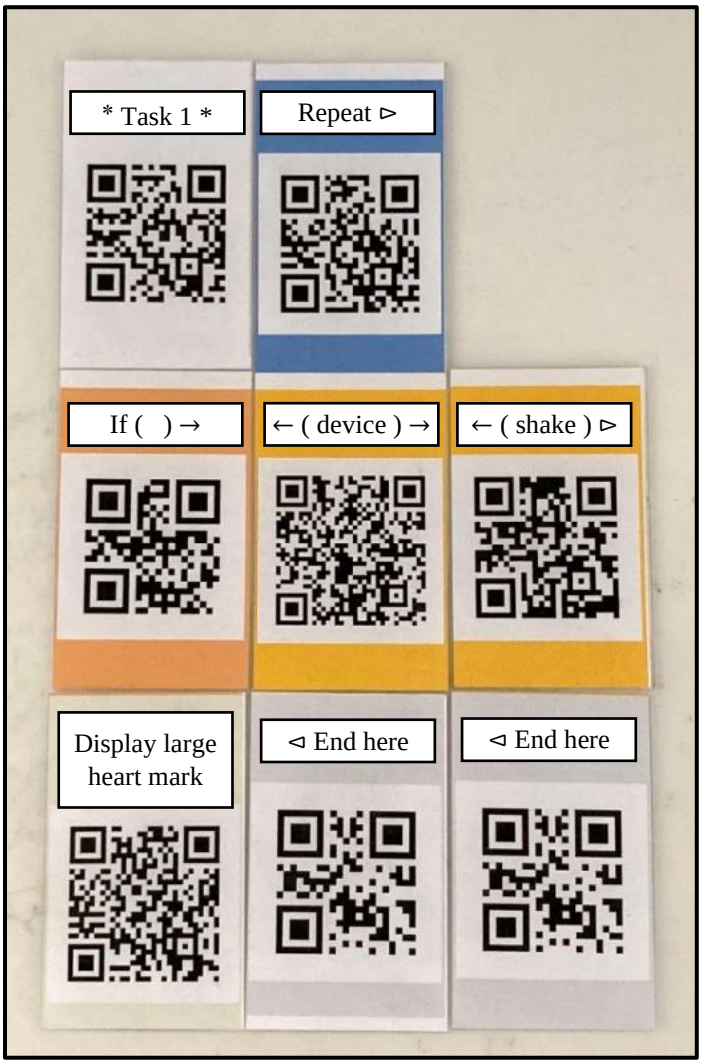


Figure 3: QR cards used in JC

3.2. Operation of the Students' Side (Client Program)

Figure 4 shows the flow of operations for the client program.

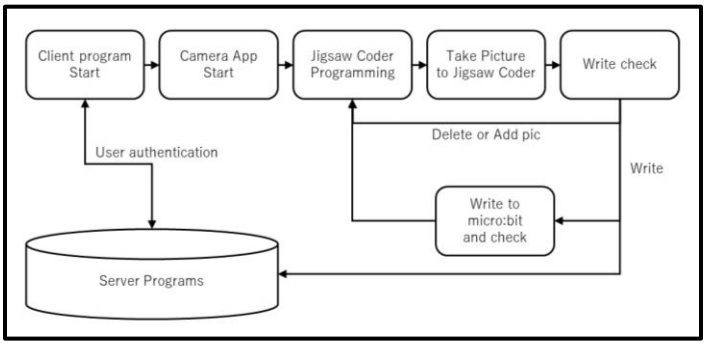


Figure 4: Flow of client program

Upon starting the client program, student authentication is initiated. The system prompts the student to input the grade, class, and the student number. Upon pressing the confirm button, the connection with the server program is established, and the students' name is displayed. Figure 5 shows the user authentication window.

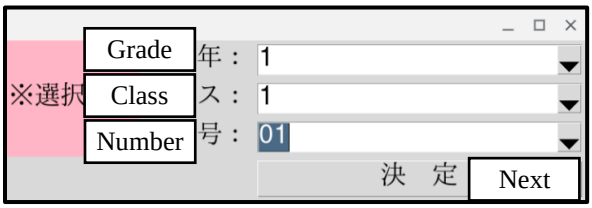


Figure 5: User authentication window

After completing student authentication, students begin programming. Once the students complete their arrangements of the cards, they photograph the cards using the camera application. The client program reads the captured photo, analyzes the QR codes in order, and generates the corresponding program. The captured photos are deleted to save memory space as they are no longer needed. Students can review the generated program in a window and then write it to the Micro:bit after confirmation. Figure 6 shows the confirmation window.

Figure 6: Writing confirmation window

If "Read additional" is selected, the read program is temporarily saved, and the student can capture another photo as the continuation of the program using the camera application. If "No (initialize content)" is selected, the read program is deleted, and the students can take a new photo again from the beginning. If "Yes" is selected, the system initiates the writing process to the

Micro:bit connected to the Chromebook. At this point, the student sends the program they wrote to the server program. The student checks their Micro:bit to ensure that the program is running correctly. If errors are found, the student rearranges the cards and takes another photo again. Figure 7 displays a photo of the system used by students.

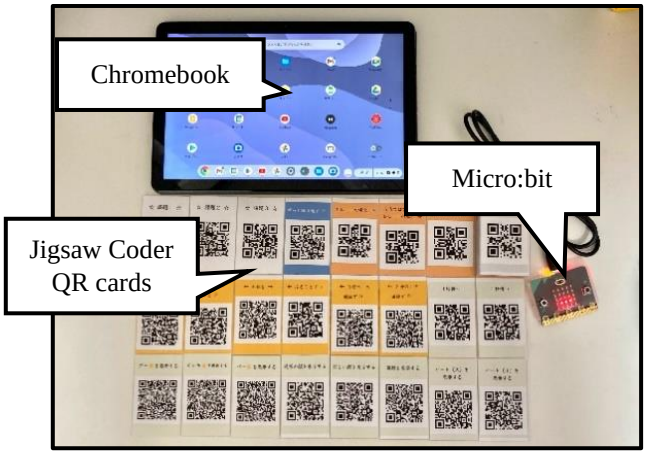


Figure 7: Overview of the student side system of JC

3.3. Operation of the Instructor's Side (Server Program)

Within the server, a database is set to manage a list of students and multiple tasks for them. The database contains a table for the student list, where their information is pre-stored for student authentication purposes. On the other hand, the task table maintains student progress, including the date and time the student first answered, date and time of subsequent attempts, date and time of correct answers, number of attempts, position of incorrect parts of their programs compared to the example answer program and level configuration file, match rate, and the program level calculated from the level configuration file.

3.4. The Web Page for Analysis

The instructor reviews the information in the database on a web page using a browser. This web page accesses the database using PHP and presents the information in an easy-to-review format for the instructor. Figure 8 shows the top page, where the number of programs in progress and completed answer programs for each task are summarized in a table. From the student list page, the instructor can edit or delete student information. It is also possible to import student data from an Excel file.

Each task page consists of two segments. Figures 9 and Figure 10 show the pages for a task. At first, using the first segment, instructor analyzes the parts of the program where students frequently make mistakes. The segment displays an example answer program, highlighting the background color of the areas where many students make mistakes. The background color changes from blue to yellow to red as the number of students who make mistakes increases in that particular section. The second segment is the table summarizing the progress of each student. It is divided into three tables for not answered, in progress, and completed of the programs, compiling details such as date and time of answer, number of attempts, and positions of errors. Using this table, the instructor can grasp the progress of the entire class. Additionally, by selecting a students' ID in this table, the instructor can see a page that compares the students' program and the example answer program for that specific student. Figure 11 shows the comparison page.

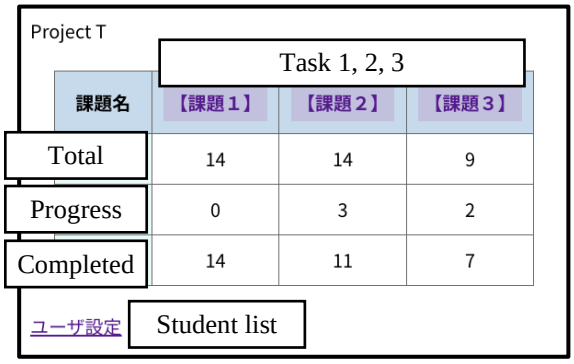


Figure 8: Analysis table on the homepage

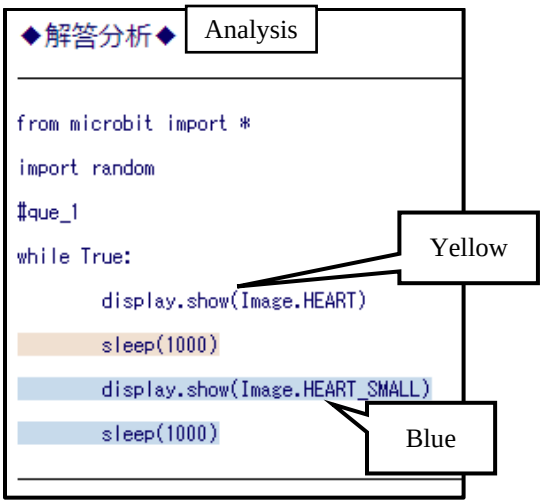


Figure 9: Segment for analyzing answer

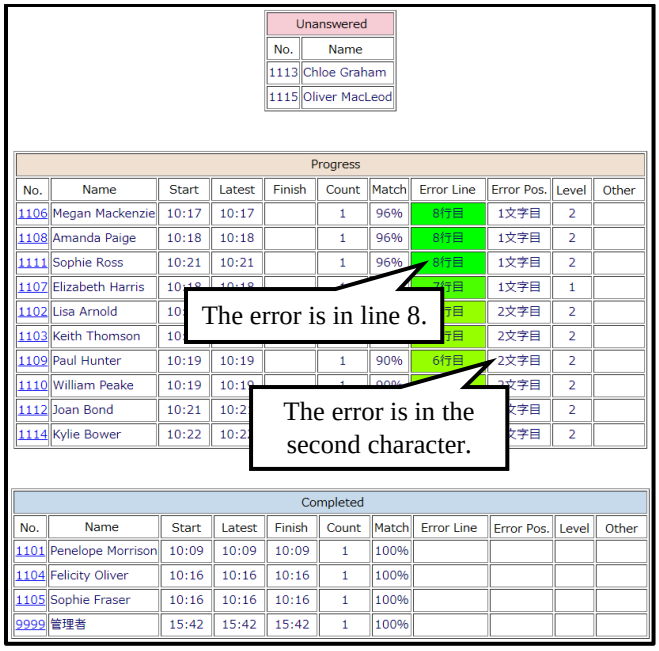


Figure 10: Segment for display answers list

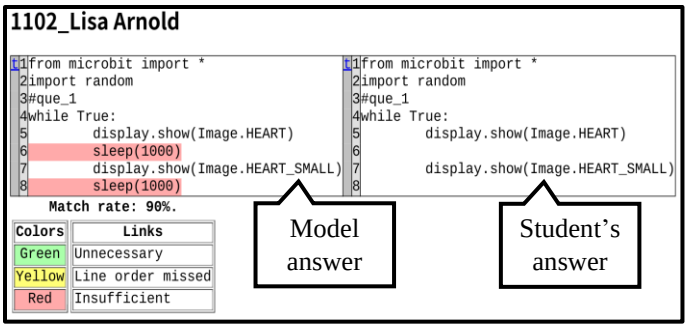


Figure 11: Page for comparing model answer with students' answer

4. Evaluation Experiment

In order to demonstrate the effectiveness of our system, we conducted evaluation experiments on the system. The objectives of the experiments are as follows.

- To determine whether the system can function properly for a large number of students during actual class time.
- If any delays occur, to measure the duration of these delays.
- From the students' perspective, we evaluated "Overall system feedback," "Feedback on sequential processing, repetition, and branching in programming," and asked "Whether programming beginners can develop an interest in programming."
- From the instructor's perspective, we evaluated "Overall system feedback," "Convenience of monitoring student progress," and asked "Areas of potential improvement in the system."

To confirm the above objectives, we let a high school instructor conduct an actual programming class. Afterwards, we administered questionnaires to both the students and the instructor. The students are nineteen first-year students from Gunma Prefectural Annaka General Academic High School. The students had no prior programming experience. The tasks prepared for this evaluation experiment were as follows:

1) Display a large heart mark and a small heart alternately for 1 second each.
2) Pressing the "A" button when the device displays a smiling face, pressing the "B" button when it displays a sad face, and not pressing any button when it displays a neutral face.
3) Shaking the device displays either rock, paper, or scissors for a rock-paper-scissors game.

The objective of task 1 is to facilitate learning of sequential processing and repetition. Task 2 aims to utilize button inputs and learn about branching. Task 3 is an optional task. The goal of this task is to utilize shaking the device as an input and understand the multi-level branching in the context of learning. All tasks involve elements of repetition.

4.1. Experimental Results

We found the system is stable. The instructor felt no perceivable delays. However, on the client side, there were instances where the program stops due to students' input errors.

4.2. Results of the Student Survey

The followings are the questions for the student survey:

1) Did using this material help you grasp the basic structure of a program?
2) Did experiencing this material increase your interest in programming?
3) Please indicate your perceived level of understanding of sequential processing.
4) Please indicate your perceived level of understanding of iterative (repetitive) processing.
5) Please indicate your perceived level of understanding of conditional processing.
6) Please write what you felt on the materials and lessons used in this session.

The questions and answers from the student survey correspond to Figures 12 through 16.

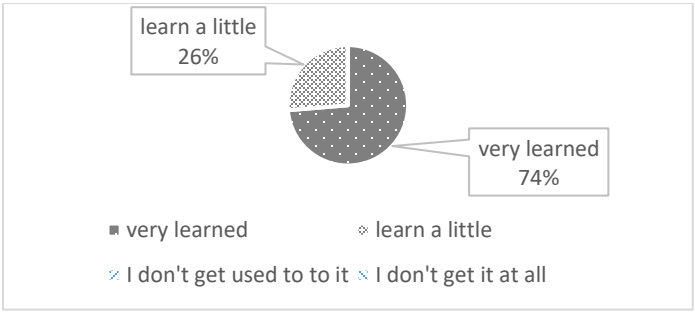


Figure 12: Did using this material help you grasp the basic structure of programming?

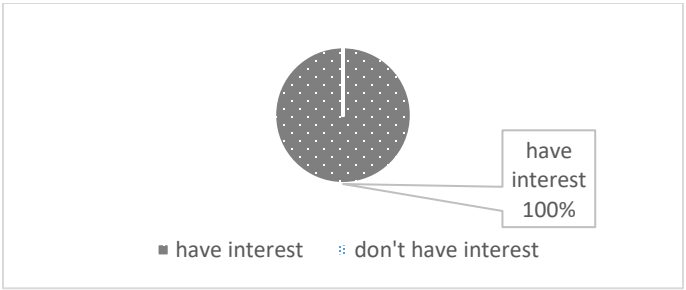


Figure 13: Did experiencing this material increase your interest in programming?

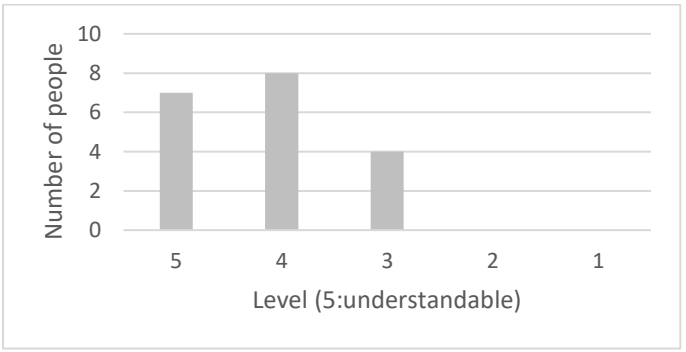


Figure 14: Please indicate your perceived level of understanding of sequential processing.

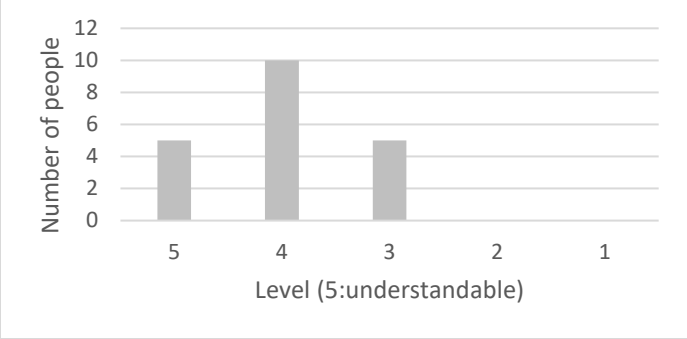


Figure 15: Please indicate your perceived level of understanding of iterative (repetitive) processing.

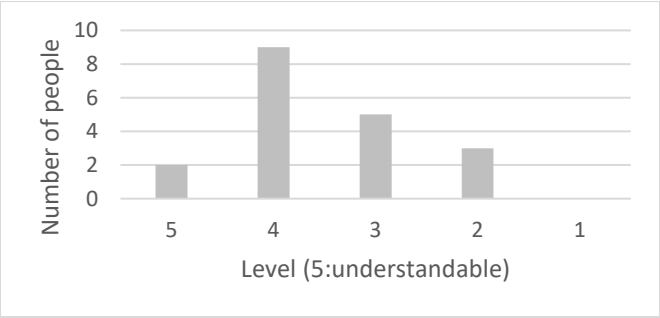


Figure 16: Please indicate your perceived level of understanding of conditional processing.

As an answer to question 6 (Please write what you felt on the materials used in this class.), the following feedbacks were provided:

- The steps were easy to remember.
- The cards were heavy.
- Having the materials allowed for better communication between students and instructors.
- I was able to think and work on my own.
- I couldn't solve the conditional processing problems.

4.3. Results of the Instructor Survey

After class, we conducted a survey for the instructor. The questions and answers are as follows. Questions A through C use a 4-point scale, where 1 indicates the lowest rating and 4 indicates the highest rating, respectively. Table 1 shows the results.

A) Did you comprehend the overall class situations based on the presented analysis results?

B) Did you discover specific problems based on the presented analysis results?

C) Did the classification based on learning levels from the presented analysis results assist for the instruction?

Table 1: Results of the survey for instructor

Question	Answer
A	2
B	3
C	1

D) Please tell us what you like about this system.

- The tangible materials, involving the combination of physical cards, are promising as an introductory tool for those new to programming.
- Taking photos of the program cards is easy and accurate enough.
- We can monitor students' progresses without moving around the classroom.
- We can focus on the students with many errors.
- The three tasks within a two-hour class is appropriate.
- Instead of using the system for real-time monitoring during class, it might be beneficial as a self-learning tool. Results, including errors, could inform instruction for future classes.

E) Please tell us any dissatisfactions or points for improvement of this system.

- It is difficult to take pictures because of the wired Micro:bit connection.
- There were many connection errors with the Micro:bit. I It needs to be improved. It was hard to tell whether it is a connection error or a programming error. It would be good to have an indication lamp or beep sound for that.
- I is unable to identify which part of the program students are struggling.
- When instructors inspect students' programs, they see the corresponding Python code instead of JC cards. It is stressful for instructors without sufficient programming skills.

5. Discussion

This section analyzes and discusses the results of the evaluation experiments.

5.1. Discussion Based on the Student Survey

Survey results indicate positive feedback on the materials. Question 2 reveals that our system successfully developed intellectual inquisitiveness for programming in all the students. Since all the students were beginners, the system effectively achieved its goal of generating motivation for programming. For question 3 on sequential processing, there were many positive responses. Students understood the order of operations by rearranging the cards. This suggests that the card arrangement helped clarify sequential processing. Question 4 on iterative processing also received positive feedbacks. In contrast, question 5 on conditional processing had a lower average rating of 3.53. This lower rating may be due to the task's difficulty. Task 3, designed to teach conditional processing, required two conditionals, which might be challenging. Starting with simpler tasks could improve understanding of conditional processing. Additionally, students might have struggled with the visual and intuitive differences between "if" and "else if," as well as between "→" and "⊳." We need to reconsider the design of JC to make these concepts more intuitive and easier to grasp. We plan to have different notations in the next version.

5.2. Discussion Based on the Instructor Survey

We can obtain several insights from the instructor survey. Questions A and C received negative responses. They indicate problems with the current system. Although instructors could track students' progress without moving around the classroom, they struggled to identify overall student difficulties. Positive responses to question B show the system is effective in identifying issues of individual students. However, question E responses indicate that how the instructor feel the system depends on their background knowledge of Python. The system requires instructors to read Python code on their screens, which may be problematic if their programming skills are insufficient. We may need to reconsider our assumption that the instructor should have sufficient programming skill in Python, and how to show students' progresses to the instructors. We plan to forge a novel means to display students' progresses so that it enhances the system's accessibility and effectiveness for users with varying levels of programming expertise.

5.3. Discussion of the Overall System

The system has not faced performance issues like delays so far. However, future experiments with over thirty students may present challenges. Unforeseen issues such as delays could arise depending on the server's capacity. Currently, a LAMP environment on a Chromebook is used for testing, but a dedicated server may be needed for practical use. Processing programs also needs adjustment to accommodate more number of users. Ensuring the system remains functional even when users cause serious run-time errors is crucial. For instance, adding confirmation dialogs to prevent accidental stops of the client program could reduce such opportunities. The card recognition issues, such as when only nine out of ten cards are recognized due to environmental factors, suggest the need for improving such as providing a new confirmation window.

We are implementing such a confirmation window. Figure 17 shows the new confirmation window that replaces the one shown in Figure 6. Since the message displayed in this window is written in Japanese, we show the corresponding English translation in Figure 18. Displaying the text on the cards before transferring to the Micro:bit could ensure correct card recognition. This approach helps students review their work and strengthen their understanding of both tangible and text-based programming.

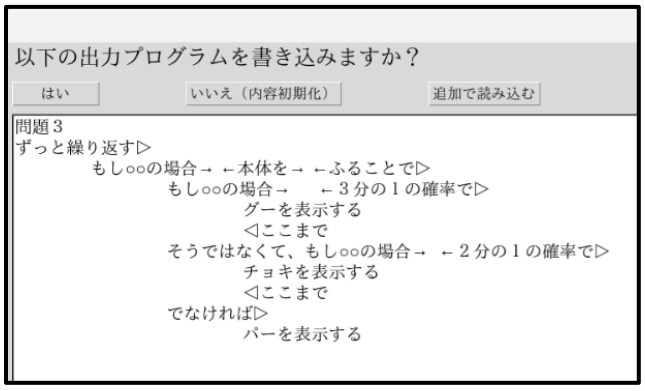


Figure 17: Writing confirmation window in Japanese

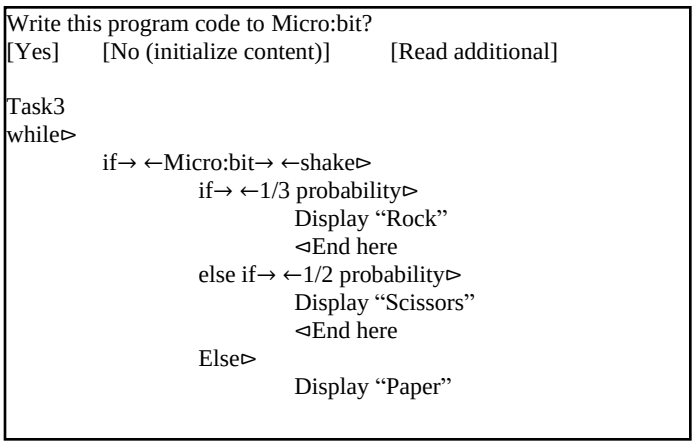


Figure 18: Writing confirmation window in English

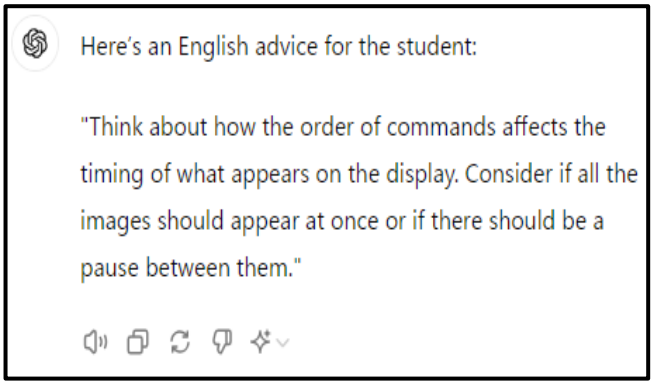


Figure 19: An example of advice generation using ChatGPT

The current limitation of this system is that only one model answer can be set for each task. Since current problem set includes only simple problems, one model answer for each problem is sufficient. We plan to incorporate a parser in our system, and to utilize AI to interpret responses more flexibly. This could identify not only syntax errors, but also semantic errors and runtime errors and provide tailored feedback for each program. Figure 19 shows an example of generated advice. While this example uses a GUI-based ChatGPT, we plan to incorporate the Python API for faster processing.

We are planning to create an individual page for each student. These pages would show the students' progress and provide AI-generated advice on each program so that each students can access to the information tailored for each of them and learn at any time. Students' feedback on the JC materials reveals that the cards are heavy. Currently, acrylic boards are used, which are durable for younger students. We need to explore alternative materials for the cards. Additionally, we are also considering modify the shapes of the cards related to "if," "else if," "else," and "while." This change aims to make the concepts of branching and iteration more intuitive.

6. Related Works

We referred to the literature on the development of tangible educational materials, literature on group learning analysis, and literature on education using Micro:bit, as listed below. Many related studies aim at the development of programming

Table 2: Comparison with other tangible educational materials

Name	Tangible	Analysis Multi-Student	Guidance for Struggling Students	Analysis on Class	Analysis after Class	Generating Individual Feedback
Jigsaw Coder	+	+	+	+	+	-
T-Maze [5]	+	-	-	-	-	-
Plugramming [6]	+	-	-	-	-	-
Strawbies [7]	+	-	-	-	-	-
PaPL [8]	+	+	-	-	+	-
Kamichi's System [9]	-	+	-	+	+	+
Kato's System [10]	-	+	+	+	+	-

educational materials. Wang et al. developed and evaluated a programming-based maze escape game called "T-Maze" [5]. However, environments with multiple students like those in a school classroom setting were not taken into consideration. Tomohito Yashiro et al. developed a tool called "Plugramming" and conducted the construction and evaluation of a collaborative programming system using Scratch [6]. However, it fails to address situations where multiple students stumble at similar parts and encounter similar errors. Felix Hu et al. developed a tangible programming game called "Strawbies" for children aged 5 to 10 [7]. Programming is done using wooden tiles. Since the tiles are not square but have distinctive shapes, the users cannot make incorrect connections. Although the programming flexibility is reduced, it has the advantage of intuitively understandable whether a connection is possible or not. Aditya Mehrotra et al. proposed multiple approaches for programming education conducted in a classroom setting [8]. They utilized program blocks for robot programming and evaluated several methods. However, the evaluation was aimed at assessing the methods, and the system does not provide real-time instructions based on students' progresses. It does not promote knowledge retention either.

In many studies related to programming instruction, the main objective is to support programming. Koichi Kamichi designed a system for programming education without teaching assistants [9]. The system mirror leaners answer to the server, providing automated suggestions of input errors for students and allowing monitoring of the progresses of the students. However, the automatic suggestions for input errors primarily aims to detect syntax errors, not considering programming novices who lack knowledge about logical thinking, which are prerequisites. Furthermore, the system only provides the instructor the number of errors that the student made, and does not provide more detailed analyses. Kato et al. developed a system in which they collected and analyzed the progress of students' programming in classes with teaching assistants and utilized this information effectively for teaching assistants so that they can guide students efficiently [10]. They conducted evaluation experiments demonstrating the system's effectiveness in instructional support. However, this analysis focuses on traditional programming languages and cannot be applied to tangible teaching materials.

Michail et al. systematically reviewed and summarized how the Micro: bit is used in primary education [11]. They reported that many students enjoy to use Micro:bit and found it easy to use. They evaluated it as beneficial for improving programming skills. In the survey, they demonstrated that Micro:bit is a promising tool for approaching STEM education. Dylan et al. conducted a two-week Micro:bit programming education program with 41 high school students[12]. After experiencing basic Micro:bit programming, the students became to be able to program autonomous cars equipped with Micro:bit and ultrasound distance sensors. Pre- and post-tests were conducted, and the results showed that the students' understanding of information processing and algorithms had deepened.

7. Conclusion

In this study, we reported our experiences of development of a classroom support system. This system assists students in programming and instructors who teach them. We conducted evaluation experiments to demonstrate the effectiveness of our system. We show a comparison of Jigsaw Coder (JC) with other related systems in Table 2. In general, it is difficult to monitor each student's progress in programming classes, and JC solves this issue. JC collects and analyzes each student's answer, and provides the instructor information for effective instruction. JC points out program areas where many students are making mistakes in the class. This function helps the instructor to grasp the overall status of the class without inspecting students one by one. Furthermore, JC is a tangible learning system, and it allows students to learn programming through physical interaction. As long as a school can provides Micro:bits, paper QR cards, client PCs, a server PC, and a network, JC can be used in all economic regions around the world. Especially it is beneficial for students in developing countries. We conducted evaluation experiments of JC for high school students. They are new to programming. The students' responses were generally positive. The instructor's responses were also positive that JC could serve as an entry-level tool for programming. It allows the instructor to monitor the students' progress without moving around the classroom to check students one by one. Based on these results, we believe that JC is effective for programming education at a beginners level. On the other hand, authors are aware that the system has a serious limitation. We plan

to revise the system with a parser and an analyzer to assist students building programming skills as well as logical thinking abilities. We reconsider the QR card design and try to make it simple too.

Acknowledgment

This work was partially supported by JSPS KAKENHI Grant Number JP21K02805.

References

[1] K. Oda, T. Kato, Y. Kambayashi, "Development and Evaluation Experiment of a Classroom Support System for Programming Education Using Tangibles Educational Materials," Proceedings of the 12th International Conference on Information and Education Technology (ICIET), 67-71, 2024, DOI: 10.1109/ICIET60671.2024.10542715

[2] T. Kato, K. Oda, Y. Kambayashi, "A Proposal of Educational Programming Environment Using Tangible Materials," Human Systems Engineering and Design (IHSED2023), 1-8, 2023.

[3] Y. Kambayashi, K. Furukawa, M. Takimoto, "Design of Tangible Programming Environment for Smartphones," HCI 2017: HCI International 2017, 448-453, 2017, DOI: 10.1007/978-3-319-58753-0_64

[4] Y. Kambayashi, K. Tsukada, M. Takimoto, "Providing Recursive Functions to the Tangible Programming Environment for Smartphones," HCII 2019, 255-260, 2019, DOI: 10.1007/978-3-030-23525-3_33

[5] D. Wang, C. Zhang, H. Wang, "T-Maze: A Tangible Programming Tool for Children," IDC '11: Proceedings of the 10th International Conference on Interaction Design and Children: 127-135, 2011, DOI: 10.1145/1999030.1999045

[6] T. Yashiro, K. Mukaiyama, Y. Harada, "Programming Tool and Activities for Experiencing Collaborative Design," Information Processing Society of Japan, **59(3)**: 822-833, 2018.

[7] F. Hu, A. Zekelman, M. Horn, F. Judd, "Strawbies: Explorations in Tangible Programming," IDC '15: Proceedings of the 14th International Conference on Interaction Design and Children: 410-413, 2015, DOI: 10.1145/2771839.2771866

[8] A. Mehrotra, C. Giang, N. Duruz, J. Dedelley, A. Mussati, M. Skweres, F. Mondada, "Introducing a Paper-Based Programming Language for Computing Education in Classrooms," ITiCSE '20: Proceedings of the 2020 ACM Conference on Innovation and Technology in Computer Science Education: 180-186, 2020, DOI: 10.1145/3341525.3387402

[9] K. Kamichi, "Designing a Programming Education Support System for Lessons without Practical Assistants," Journal of Sociology Research Institute, **1**: 73-78, 2020.

[10] T. Kato, Y. Kambayashi, Y. Kodama, "Data Mining of Students' Behaviors in Programming Exercises," Smart Education and e-Learning, **59**: 121-133, 2016.

[11] M. Kalogiannakis, E. Tzagaraki, S. Papadakis, "A Systematic Review of the Use of BBC Micro in Primary School," 10th International Conference New Perspectives in Science Education, STEM5036, 2021.

[12] D. G. Kelly, P. Seeling, "Introducing Underrepresented High School Students to Software Engineering: Using the Micro Microcontroller to Program Connected Autonomous Cars," Computer Applications in Engineering Education, **28(3)**: 737-747, 2020, DOI: 10.1002/cae.22244

ASTES

Advances in Science, Technology and Engineering Systems Journal
Vol. 9, No. 6, 30-46 (2024)
www.astesj.com
Special Issue on Innovation in Computing, Engineering Science & Technology

ASTES Journal
ISSN: 2415-6698

On Adversarial Robustness of Quantized Neural Networks Against Direct Attacks

Abhishek Shrestha*, Jürgen Großmann

Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS, System Quality Center (SQC), Critical Systems Engineering, Berlin, 10589, Germany

ARTICLE INFO

Article history:
Received: 14 October, 2024
Revised: 10 December, 2024
Accepted: 11 December, 2024
Online: 23 December, 2024

Keywords:
Deep neural networks
Quantization
Adversarial attacks

ABSTRACT

Deep Neural Networks (DNNs) prove to be susceptible to synthetically generated samples, so-called adversarial examples. Such adversarial examples aim at generating misclassifications by specifically optimizing input data for a matching perturbation. With the increasing use of deep learning on embedded devices and the resulting use of quantization techniques to compress deep neural networks, it is critical to investigate the adversarial vulnerability of quantized neural networks.
In this paper, we perform an in-depth study of the adversarial robustness of quantized networks against direct attacks, where adversarial examples are both generated and applied on the same network. Our experiments show that quantization makes models resilient to the generation of adversarial examples, even for attacks that demonstrate a high success rate, indicating that it offers some degree of robustness against these attacks. Additionally, we open-source Adversarial Neural Network Toolkit (ANNT) to support the replication of our results.

1. Introduction

This paper builds upon our recent work, presented at the 5th ACM/IEEE International Conference On Automation of Software Test [1], which involved a comprehensive study on transferability of adversarial examples among quantized networks under various conditions. In this study, we advance the analysis by examining the efficiency of adversarial attacks on quantized networks when attacks are created and applied on the same network (direct attacks). Together, our previous and current work provide a more complete understanding of how quantization affects network vulnerability by addressing both transfer-based and direct attack scenarios.

Adversarial examples are images with deliberately added perturbations which can cause a network to misclassify the image at a high rate [2]. These perturbation vectors are computed using specific algorithms and often distort an image in such a way that it looks benign or clean to human observers but are enough to cause a network to misclassify the image [3, 4].

As the use of DNNs proliferates over various safety-critical domains like medical diagnosis [5], railway [6], and aviation [7], the possibilities of adversarial examples coercing a network into making adversary-controlled decisions become a severe threat. One of the domains where deep learning is rapidly gaining popularity is the embedded systems. For instance, autonomous systems use AI for decision-making by processing sensory information [8], mobile devices use them for image processing [9], and surveillance systems use them for biometric analysis [10]. However, the implementation of deep learning on edge devices is challenging. While the embedded devices are inherently constrained in terms of memory and power resources [11, 12], the state-of-the-art capabilities of DNNs come at a price of tremendous computational power required for running them. A pre-trained neural network comes with a large number of parameters: AlexNet [13] has 60 million parameters; VGG16 [14], an improvement over AlexNet, has 138 million parameters; similarly, ResNet50 [15], another popular DNN, has 26 million parameters. The presence of these large number of parameters mean that the computational demand at run-time is very high and requires the systems implementing these models to have considerable computing capabilities for a smooth operation.

One of the solutions to the limited resource problem is using a high-performance server that handles the deep learning tasks, with the devices just having to communicate with the server. Another solution, which is more widely adopted, is to deploy optimized versions of a base model on the device itself. On-device deployments has several benefits [16]:

- No need to communicate with the server frequently which saves energy.

*Corresponding Author: Abhishek Shrestha, Fraunhofer FOKUS, Kaiserin-Augusta-Allee 31, 10589 Berlin, Germany, abhishek.shrestha@fokus.fraunhofer.de

- Privacy is maintained as the user data does not leave the device.
- Performance is improved as round-trips to the server is avoided.

Various methods have been developed to optimize models for on-device deep learning [17, 18, 19]. One such effective approach is model compression through quantization [20], which reduces both the computational complexity and memory footprint of a network by lowering the precision of its values from the default 32-bit floating point (float32) to smaller bitwidths.

However, recent studies have shown that quantized networks remain vulnerable to adversarial examples [21, 22]. The adversarial vulnerability is especially concerning in compressed networks because of the wide-spread use and accessibility of embedded devices as compared to the full-scale networks running on high-end servers. Moreover, adversarial examples are found to be transferable [4, 23, 24, 25]. Samples created in one network (source) are found to be effective when applied on another network (target) trained to perform similar tasks. Our prior work [1] investigated this transferability property. Interestingly, we observed that iterative attacks like the Boundary Attack [26] and Carlini-Wagner (CW) attack [27] showed high efficiency in direct attack settings (where the source and target network are same), even when the networks were quantized. In this paper, we present an in-depth analysis of this behaviour, offering further insights into attack effectiveness on quantized networks.

Our contributions with this work are as follows:

- We consider diverse adversarial attack algorithms to assess the adversarial vulnerability of quantized networks against direct attacks. Our analysis shows that even though some attacks succeed with high rate, quantized networks, in general, offer some resistance against both gradient-based and gradient-free attacks as they require higher distortion to become effective, making samples easier to detect.
- We introduce the Adversarial Neural Network Toolkit (ANNT), a holistic application that streamlines the entire process—from training full-precision and quantized models to generating adversarial examples and evaluating robustness—within a single tool. ANNT, together with the trained models and adversarial images provided with this paper, enables the replication of our results—both from this study and our previous work [1]. Furthermore, ANNT can serve as a valuable resource for the research community, simplifying experimentation by allowing users to train quantized models and immediately test their robustness using various adversarial attacks without switching between tools.

2. Scope of the Study

Only untargeted misclassifications are considered. This means, for an attack algorithm, classification to any class other than the true class is considered as a successful attack. Targetted misclassifications that require attack algorithms to cause misclassifications to a specific target class selected by an adversary are not considered.

When quantizing a network, both activation and weight values are quantized to the same bitwidth. Quantization of activation and weights individually to different bitwidths is possible and could be a subject of further work. Moreover, gradients and bias values are not quantized.

Further, the study is limited to only image classifiers. Datasets, attack algorithms, and DNNs are selected accordingly.

3. Background

3.1. Deep Neural Network (DNN)

A DNN can be defined as a function that maps a high-dimensional input to a vector[1] output. More specifically, a DNN is a classification function that can be expressed as:

$$f(\mathbf{x}, \theta) = \mathbf{y} \tag{1}$$

Here, $\mathbf{x} \in \mathbb{R}^m$ is an input of m dimensions, θ represents parameters (weights and biases) learned during training, and $\mathbf{y} \in \mathbb{R}^n$ is a vector representing probability distribution over n classes, meaning that $y_1 + y_2 + y_3 + \ldots + y_n = 1$ and $0 \leq (y_i)_{i=1}^n \leq 1$. Each y_i in $\mathbf{y}$ represents the probability that the input $\mathbf{x}$ is assigned to class i.

Thus, the class assigned to the input $\mathbf{x}$ is determined by the index of the maximum value in the output vector $\mathbf{y}$. Hence, $y_i = f_i(\mathbf{x})$ being i^{th} output of the network, the output label y is given by:

$$\underset{i}{\operatorname{argmax}}\, f_i(\mathbf{x}) = y \tag{2}$$

The network learns by iteratively adjusting θ based on an optimization algorithm that guides the adjustments by moving in the direction opposite to the loss gradient $\nabla_\theta J(\mathbf{x}, y, \theta)$, where $J(\mathbf{x}, y, \theta)$ represents loss function used to train the network. The gradient $\nabla_\theta()$ is computed with respect to the current network parameters θ. In our work, since we use trained networks, θ is constant (therefore ignored in Equation 2).

3.2. Distance Metrics

Various distance metrics can be used to measure the similarity (or dissimilarity) between the benign and adversarial samples. L_p-norm distances are widely used as one of the performance metrics when generating adversarial examples [26, 27, 28].

Let, $\mathbf{x}^{adv} \in \mathbb{R}^m$ be the corresponding adversarial example of a benign sample $\mathbf{x}$, L_p distance between $\mathbf{x}$ and $\mathbf{x}^{adv}$ for $p \in [0, \infty)$ is given by:

$$|\mathbf{x} - \mathbf{x}^{adv}|_p = \left(\sum_{i=1}^m |\mathbf{x}_i - \mathbf{x}_i^{adv}|^p\right)^{\frac{1}{p}} \tag{3}$$

The L_p-norm distances include:

- L_0 distance (Hamming distance): L_0 counts the number of non-zero elements in $|\mathbf{x} - \mathbf{x}^{adv}|_0$, that is, $|\{\mathbf{x}_i - \mathbf{x}_i^{adv} \neq 0\}|$.

[1] The bold letterings indicate that the corresponding values are vector quantities.

When considering image classifiers, each element of the input vector $\mathbf{x}$ is a pixel value, and thus, L_0 basically counts the number of pixels that have altered between $\mathbf{x}$ and $\mathbf{x}^{adv}$ [27, 28].

- L_1 distance (Manhattan distance): From Equation 3, L_1 distance can be expressed as:

$$|\mathbf{x}-\mathbf{x}^{adv}|_1 = \sum_{i=1}^{m} |\mathbf{x}_i - \mathbf{x}_i^{adv}| \tag{4}$$

- L_2 distance (Euclidean distance): As per Equation 3, the Euclidean distance between $\mathbf{x}$ and $\mathbf{x}^{adv}$ is given by:

$$|\mathbf{x}-\mathbf{x}^{adv}|_2 = \sqrt{\sum_{i=1}^{m} (\mathbf{x}_i - \mathbf{x}_i^{adv})^2} \tag{5}$$

L_2 can remain small even where there are minute changes in many pixels [27].

- L_∞ distance (Chebyshev distance): This is given by:

$$|\mathbf{x}-\mathbf{x}^{adv}|_\infty = max(|\mathbf{x}_i - \mathbf{x}_i^{adv}|_{\{i=1,\ldots,m\}}) \tag{6}$$

Thus, L_∞ measures the largest change in pixel values. This can be used to set a maximum limit up to which a pixel value is allowed to change. While any number of pixels can be modified, each pixel can only be modified to this limit.

3.3. Adversarial Examples

Adversarial examples are generated by adding computed perturbations to a clean image, resulting in distorted samples that look almost identical to the original image to human observers, but cause significant changes in the output class probabilities of a classifier, leading to a misclassification in majority of cases [2, 4, 25, 28]. Adversarial samples are crafted at test time and do not require an adversary to have any kind of influence on the training process [29, 30].

If y^{true} be the true label corresponding to a clean image $\mathbf{x}$, then from Equation 2 we have: $\text{argmax}_i f_i(\mathbf{x}) = y^{true}$. If a perturbation vector $\eta \in \mathbb{R}^m$ is added to input $\mathbf{x}$, resulting in a perturbed example $\mathbf{x}^{adv}$ causing successful misclassification, then:

$$\underset{i}{\text{argmax}}\, f_i(\mathbf{x}^{adv}) \neq y^{true} \tag{7}$$

It is also worth noting that not all adversarial examples cause misclassification. These samples have high probability of causing misclassification but do not guarantee misclassification [25]. In this view, all samples created from an adversarial examples generation algorithm are adversarial examples but it is possible that not all of them are successful in fooling a network.

A DNN learns by iteratively reducing loss by utilizing optimization algorithms like the gradient descent. In other words, a network is made to converge to a point where the parameters are such that the resulting class probabilities yield low loss. With this in mind, the basic concept behind generating adversarial samples is to increase the loss such that the class probabilities are manipulated in a way desired by the adversary. Since it is not possible to modify the network parameters θ at test time, the input itself is varied till the goal of misclassification is met. Thus, for generating adversarial examples, the optimization problem becomes:

$$\begin{aligned} \max_{\mathbf{x}^{adv}} \quad & J(\mathbf{x}^{adv}, y, \theta) \\ \text{s.t.} \quad & |\mathbf{x}-\mathbf{x}^{adv}|_p \leq \varepsilon \end{aligned} \tag{8}$$

Where, $\mathbf{x}^{adv} = \mathbf{x} + \eta$ and ε is the maximum allowed perturbation measured in terms of $|\cdot|_p$ utilized by the algorithm to generate the sample.

3.4. Crafting Algorithms

Inducing misclassification through random perturbations is notably more challenging [23] and therefore definite algorithms are required to compute perturbation vectors of specific magnitude and direction. Usually, these algorithms aim to solve the optimization problem in Equation 8. In our original work [1], we considered five conceptually different algorithms to create such attacks. In this work, we use the same algorithms as we want to study the attack efficiency of these attacks on the source network.

Fast Gradient Sign Method (FGSM) [4]: The attack is based on the reasoning that all non-linear models are trained to behave rather linearly to make the training process easier. For instance, commonly used activation functions like ReLU are piecewise linear and even sigmoid functions are tuned to work within the linear part of the curve. As a consequence, adding linear perturbations to the input can break the models.

If perturbation vector η be the distortion introduced to input vector $\mathbf{x}$ such that $\mathbf{x}^{adv} = \mathbf{x} + \eta$. For $|\eta|_\infty < \varepsilon$, where ε is less than the precision of the model, the model should not respond to this distortion. However, for a linear model with weight vector $\mathbf{w}$, this distortion grows by $\mathbf{w} \cdot \eta$ as shown by the relation in Equation 9.

$$\begin{aligned} \mathbf{w} \cdot \mathbf{x}^{adv} &= \mathbf{w} \cdot \mathbf{x} + \mathbf{w} \cdot \eta \\ \mathbf{w}^T \mathbf{x}^{adv} &= \mathbf{w}^T \mathbf{x} + \mathbf{w}^T \eta \end{aligned} \tag{9}$$

To maximize the effect of this distortion, direction of max-norm constrained perturbation η can be aligned with weight vector. Then, m being the average weight of each element of $\mathbf{w}$ and n be the dimension of $\mathbf{w}$, the activation change can be represented as in Equation 10

$$\mathbf{w}^T \eta = \varepsilon mn \tag{10}$$

The consequences of Equation 10 are: (a) Keeping the average weight same, change in activation due to η grows linearly with n. Thus, a small change at input can aggregate to create large change in output at high dimensions. (b) Since all models behave linearly, the concept of this linear perturbation can also be applied to DNNs to cause misclassifications.

Authors then use these ideas to propose FGSM which adds linear distortion to the input in a single step to create adversarial samples. The perturbation vector η is constructed as:

$$\eta = \varepsilon sign(\nabla_{\mathbf{x}} J(\mathbf{x}, y, \theta)) \tag{11}$$

Thus, the adversarially perturbed sample is given by:

$$\mathbf{x}^{adv} = \mathbf{x} + \varepsilon sign(\nabla_{\mathbf{x}} J(\mathbf{x}, y, \theta)) \tag{12}$$

As can be seen, the perturbation is added in the direction of the loss gradient computed with respect to input $\mathbf{x}$. This makes sense because loss gradient gives the direction of the largest increase in loss. Thus, perturbation aligned with this direction is optimal for increasing loss. ε is the L_∞ norm of the perturbation which also gives the distance between $\mathbf{x}$ and $\mathbf{x}^{adv}$.

Jacobian Saliency Map based Attack (JSMA) [29]: The attack generates adversarial examples by establishing a direct relationship between input variations and output changes, allowing it to identify the features most effective in altering the classifier's decision.

The basic idea behind the algorithm can be summed up in three steps:

1. Compute forward derivative of the function learned by the network to create a mapping between rate of change in output with respect to change in input.
2. Create a saliency map based on the computed forward derivative to search for the most sensitive features that produce change towards the adversarial class.
3. Add defined perturbation to the selected features. Keep adding changes iteratively with each iteration computing the forward derivative and the saliency map until the misclassification is achieved.

The forward derivative of a network computes how much the output $\mathbf{y}$ changes due to the change in $\mathbf{x}$. Since a network learns a vector valued function, the forward derivative has to compute change in each element of $\mathbf{y}$ due to change in each element in $\mathbf{x}$. This is basically the Jacobian of the vector valued function learned by the network.

Thus, the forward derivative is given by:

$$\nabla f(\mathbf{x}) = \frac{\partial f(\mathbf{x})}{\partial \mathbf{x}} = \left[\frac{\partial f_j(\mathbf{x})}{\partial x_i}\right]_{i\in 1,\ldots,m, j\in 1,\ldots,n} \tag{13}$$

For more clarity, when assuming a 2-dimensional input $\mathbf{x}$ and output $\mathbf{y}$, the forward derivative is computed as:

$$\nabla f(\mathbf{x}) = \begin{bmatrix} \frac{\partial f_1(\mathbf{x})}{\partial x_1} & \frac{\partial f_1(\mathbf{x})}{\partial x_2} \\ \frac{\partial f_2(\mathbf{x})}{\partial x_1} & \frac{\partial f_2(\mathbf{x})}{\partial x_2} \end{bmatrix} \tag{14}$$

In the Jacobian matrix, a positive rate of change of an output class means that the change in the corresponding input feature will increase its current prediction probability, while a decrease means that it will decrease its prediction probability. Based on this, a saliency map can be constructed which filters the features that are most important based on the given criteria. Equation 15 provides a very basic filter criteria as defined in [29].

$$S(\nabla f(\mathbf{x}),t)[i] = \begin{cases} 0 \text{ if } \frac{\partial f_t(\mathbf{x})}{\partial x_i} < 0 \text{ or } \sum_{j\neq t} \frac{\partial f_j(\mathbf{x})}{\partial x_i} > 0 \\ \left(\frac{\partial f_t(\mathbf{x})}{\partial x_i}\right)\left|\sum_{j\neq t} \frac{\partial f_j(\mathbf{x})}{\partial x_i}\right| \text{ otherwise} \end{cases} \tag{15}$$

Here, t is the target class to which the input is to be misclassified, that is, $t \neq y^{true}$. $S(\nabla f(\mathbf{x}),t)[i]$ is the saliency map computed for i^{th} feature.

Thus, as per Equation 15, from the Jacobian matrix, features that increase the target class probability and at the same time decrease the probabilities of all other classes are weighed. The feature with the highest value is then selected. In each iteration, selected feature is perturbed by a defined amount. This is continued till misclassification is achieved, that is, $\text{argmax}_i f_i(\mathbf{x}) = t$.

In practice, saliency map criteria as defined in Equation 15 is too restricting; thus, an optimized version which selects a pair of features in one iteration is often used [29]. The policy for generating maps may need to be optimized as per requirement. For instance, pairwise selection is usable for CIFAR10 [31] and MNIST [32] datasets but was found to not work for datasets that contain high-resolution images like the ImageNet [27].

Universal Adversarial Perturbation (UAP) [3]: UAP is different from other attacks discussed in this section as it generates image-agnostic perturbations. Instead of computing adversarial images for each image in a dataset, the algorithm aims to find a single perturbation vector from a given subset of data which can then be applied to the entire data distribution to create adversarial samples. These types of perturbations are called Universal Adversarial Perturbations (UAP). The prefix *universal* is used because they are generalizable across new data points that were not used when creating the perturbation.

If $X = \{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n\}$ be a dataset sampled from a data distribution μ, then the goal is to compute a universal perturbation $\boldsymbol{v} \in \mathbb{R}^m$ using X, such that for most $\mathbf{x} \in \mathbb{R}^m$ in μ, Equation 16 is fulfilled.

$$f(\mathbf{x}_k + \boldsymbol{v}) \neq y^{true} \tag{16}$$

The algorithm iterates though each image in X and computes a perturbation vector $\Delta\boldsymbol{v}_k$ that sends the current data point $\mathbf{x}_k + \boldsymbol{v}$ across the decision boundary. Perturbation $\boldsymbol{v}$ is then updated as $(\boldsymbol{v} + \Delta\boldsymbol{v}_k)$.

The perturbation vector $\boldsymbol{v}$ is such that $|\boldsymbol{v}|_p < \xi$, where $|\cdot|_p$ is the desired L_p-norm. To make sure that the magnitude of perturbation $\boldsymbol{v}$ is within ξ, updated $\boldsymbol{v}$ is again projected onto a L_p ball of radius ξ centered at 0. The algorithm stops when a pre-defined fooling rate is obtained on X. If δ be the desired accuracy on X then the required fooling rate is denoted by $(1-\delta)$.

At the end of each iteration, the computed perturbation $\boldsymbol{v}$ is added to all data points in X to create a set of perturbed data points $X_v = \{\mathbf{x}_1 + \boldsymbol{v}, \mathbf{x}_2 + \boldsymbol{v}, \ldots, \mathbf{x}_n + \boldsymbol{v}\}$. The current fooling rate is then given by Equation 17. The algorithm stops when $Err(\mathbf{x}_v) \geq (1-\delta)$.

$$Err(\mathbf{x}_v) = \frac{1}{n}\sum_{k=1}^{n} 1_{[f(\mathbf{x}_k+\boldsymbol{v})\neq f(x_k)]} \tag{17}$$

The individual image perturbation $\Delta\boldsymbol{v}_k$ can be computed using any algorithm. For instance, authors in [3] use DeepFool [33], while [34] uses Projected Gradient Descent (PGD) [35]. In our case, we use FGSM to compute this vector and measure ξ in L_∞.

The Carlini-Wagner (CW) Attack [27]: Carlini and Wagner introduce three variants of one of the most powerful gradient-based adversarial attacks against neural networks. The attacks not only cause misclassification with high success rate but they do so while introducing comparatively low distortion than other attacks like FGSM and JSMA. The three variations of the attacks are based on the L_2, L_0, and L_∞ distance metrics. However, as in our previous

work [1], we only focus on the L_2 version as it is considered to be the strongest [27].

The effectiveness of the attack can be attributed to the optimization problem (Equation 18) that balances two objectives: (1) Minimize distance between adversarial and the original image. (2) Misclassify the image into any class other than the original. This results in adversarial samples that are minimally perturbed while ensuring misclassification.

$$\begin{aligned} &\text{minimize } \|\mathbf{x}^{adv} - \mathbf{x}\|_2^2 + c \cdot l(\mathbf{x}^{adv}); \text{ where,} \\ l(\mathbf{x}^{adv}) &= \max\left(Z_i(\mathbf{x}^{adv}) - \max\left(Z_t(\mathbf{x}^{adv}) : t \neq i\right) + \kappa, 0\right) \end{aligned} \tag{18}$$

In equation 18, $Z_i(\mathbf{x}^{adv})$ is the logit corresponding to the true label and $Z_t(\mathbf{x}^{adv})$ corresponds to any other label $t \neq i$. The equation considers L_2 norm. The amount of distortion or the misclassification confidence can be controlled by varying κ. Larger κ means samples are more stronger (high confidence misclassification) at the cost of higher distortions. On the other hand, c is a positive constant that mediates the trade-off between minimizing perturbation and achieving misclassification. It is determined via binary search during the attack.

Further, the attack considers logits rather than activation values from the softmax layer, this enables the attack to still be effective on networks that apply gradient-masking techniques like the defensive distillation [36]. Moreover, the original paper designs the attack for targeted misclassifications, adapting the objective function accordingly. In this work, we focus on untargeted misclassification and therefore utilize the objective function presented in Equation 18.

The Boundary Attack (BA) [26]: The Attack uses model's decisions on the input points to craft adversarial examples and therefore, unlike other attacks discussed in this section, it does not require access to model parameters or architecture to create adversarial samples.

For each clean image, the algorithm initializes a random adversarial image and iteratively applies perturbations that reduce the L_2 distance between the adversarial and the corresponding clean image. After each iteration, the algorithm checks that the perturbed image remains outside the decision boundary of the original image by querying the model. This process continues until the minimum distance between the clean and adversarial image is achieved.

The algorithm internally uses two parameters, δ and ε to control the perturbations that guide the initialized image towards the clean image. δ controls the magnitude of the perturbations and ε controls the step size towards the clean image. The generation process begins by sampling feature values from a uniform distribution $\mathscr{U}(0,1)$ to create a random image that is adversarial to the clean image. Multiple perturbations are sampled randomly from an iid Gaussian distribution $\mathscr{N}(0,1)$ and are rescaled based on the current value of δ. These perturbations are then projected on a sphere around the clean image and are then added to the random image. From the resulting perturbed images, only those that are still adversarial are selected for further processing. If less than 20% of the perturbed images are adversarial, then this means that the image is already close to the decision boundary, and thus the value of δ is decreased. However, if more than 50% are adversarial, then δ is increased. Finally, to make a movement towards the decision boundary, the perturbations are again scaled by ε and added to the perturbed images. Again, out of the resulting perturbed images, only those that remain adversarial are selected. Value of ε is adjusted by considering similar thresholds as in the case of δ. From the successful adversarial images, the adversarial image that is closest to the initial image in terms of L_2 distance is selected for the next iteration. The loop continues with the updated values of δ and ε until an adversarial image with minimum possible L_2 is obtained. Thus, with each iteration, the adversarial image comes closer to the decision boundary and starts to look like the original image, yet remaining adversarial.

Both δ and ε are adjusted automatically during generation. The number of iterations, however, is provided as input to the algorithm. Fewer iterations result in higher distortion, while more iterations result in less distortion, as the algorithm has more opportunities to bring the initial image closer to the original image.

Moreover, BA is a gradient-free attack as it does not use any type of gradient-information to craft adversarial samples.

3.5. Quantization as a Model Optimization Technique

Quantization reduces the computational complexity during training and inference by reducing the bitwidth of activations, gradients, and weights [18] to lower bitwidth numbers. This allows floating-point multiplications during convolution operations to be replaced with faster bitwise operations. For instance, by binarizing weights and input activations of convolution layers, the dot products during forward pass can be computed with the formula as in Equation 19 [37].

$$\mathbf{x} \cdot \mathbf{y} = \text{bitcount}(\text{AND}(\mathbf{x}, \mathbf{y})), x_i, y_i \in \{0,1\} \forall i \tag{19}$$

Here, $\mathbf{x}$ and $\mathbf{y}$ are two bit vectors and the *bitcount* operation counts the number of 1s in the resulting vector. Equation 19 can be further extended to be valid for any fixed-point integer values. If $\mathbf{x}$ be a sequence of M-bit integers and $\mathbf{y}$ be a sequence of K-bit integers then:

$$\mathbf{x} = \sum_{m=0}^{M-1} c_m(\mathbf{x}) 2^m \tag{20}$$

$$\mathbf{y} = \sum_{k=0}^{K-1} c_k(\mathbf{y}) 2^k \tag{21}$$

where, $(c_m(\mathbf{x}))_{m=0}^{M-1}$ and $(c_k(\mathbf{y}))_{k=0}^{K-1}$ are bit vectors. Then the dot product of $\mathbf{x}$ and $\mathbf{y}$ is given by Equation 22 [37].

$$\mathbf{x} \cdot \mathbf{y} = \sum_{m=0}^{M-1} \sum_{k=0}^{K-1} 2^{k+m} \text{ bitcount}[\text{AND}(c_m(\mathbf{x}), c_k(\mathbf{y}))] \tag{22}$$

Thus, by representing activation, weights, and gradients by integer values, convolution operations between them can be greatly optimized.

There are two types of quantization [20, 22]: *post-training quantization* and *quantization aware training*. In post-training quantization, weights and activation values are quantized after a model is fully trained. Quantization aware training quantizes weights, activations, or gradients during training.

DoReFa-Net [37]: The quantization method quantizes weights, activations, and gradients to lower bitwidths during training. Activation and weight values are quantized during forward pass, while the gradients are quantized during backward pass. Although DoReFa-Net is able to perform low bitwidth quantization of gradients, we do not consider gradient quantization in this work. Thus, the convolution operation between weights and activations during forward pass takes place in low bitwidths, while backward pass still requires convolution between quantized and unquantized values.

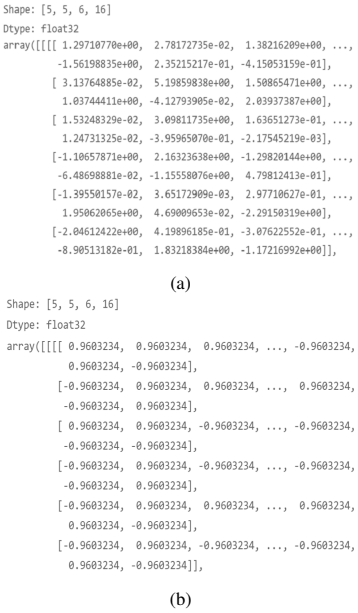


Figure 1: 1-bit quantization of weights using DoReFa-Net: (a) Weight values from a part of a full-precision float32 convolution layer. (b) The same values after 1-bit quantization using DoReFa-Net (without conversion to integers).

If q is a quantized value of p and c is the cost function, then during backward pass, computation as in Equation 23 requires $\frac{\partial q}{\partial p}$ which is not well defined. This creates a problem during back-propagation.

$$\frac{\partial c}{\partial p} = \frac{\partial c}{\partial q} \cdot \frac{\partial q}{\partial p} \tag{23}$$

One of the solution to this problem is to estimate the value of $\frac{\partial q}{\partial p}$, given that $\frac{\partial c}{\partial q}$ is properly defined. These estimators that allow defining custom $\frac{\partial q}{\partial p}$ are called Straight Through Estimators or STEs [38]. DoReFa-Net uses $\mathbf{quantize}_n$ STE [37], which is defined as in Equation 24.

$$\begin{aligned} \textbf{Forward: } & r_o = \frac{1}{2^n - 1}\text{round}((2^n - 1)\ \ r_i) \\ \textbf{Backward: } & \frac{\partial c}{\partial r_i} = \frac{\partial c}{\partial r_o} \end{aligned} \tag{24}$$

Equation 24 uses $\frac{\partial c}{\partial r_o}$ as an approximate of $\frac{\partial c}{\partial r_i}$. In the equation, $r_i \in [0,1]$ is a float32 real number and $r_o \in [0,1]$ is the quantized output value representable by an n-bit number. Since there is always an affine mapping between fixed-point integers and n-bit numbers, the bit-convolutions as specified in Equation 22 can take place between quantized weights and activations during forward pass. This significantly speeds-up the training and inference process.

Figure 1 compares weight values of a convolution layer before and after 1-bit quantization using DoReFa-Net. As illustrated in the figure, the weight values are 1-bit quantized (2 possible values) but the data type remains float32. We maintain the n-bit numbers as float32 and do not convert them to integers. This approach preserves the levelling effect caused due to quantization, but without the speed optimizations that integer representations could provide. However, improving computational speed is not a priority, as the primary goal is to analyze the network's behaviour.

Quantization of weights: DoReFa-Net treats 1-bit quantization of weights differently than n-bit quantization where $n > 1$. For 1-bit quantization, a method similar to [39] is used. The STE is as shown in Equation 25.

$$\begin{aligned} \textbf{Forward: } & r_o = sign(r_i) \times \mathbf{E}(|r_i|) \\ \textbf{Backward: } & \frac{\partial c}{\partial r_i} = \frac{\partial c}{\partial r_o} \end{aligned} \tag{25}$$

Here, $sign(r_i) = 2\mathbb{I}_{r_i>0} - 1$ has two possible values: -1 and 1. $\mathbf{E}(|r_i|)$ is the average of absolute values of all weights in the layer. For n-bit quantization, forward operation as in Equation 26 is used.

$$\textbf{Forward: } r_o = f_w^n(r_i) = 2\text{quantize}_n\left(\frac{\tanh(r_i)}{2\max\left(|\tanh(r_i)|\right)} + \frac{1}{2}\right) - 1 \tag{26}$$

Here, *tanh* bounds the value of r_i within [-1,1]. The expression $\left(\frac{\tanh(r_i)}{2\max\left(|\tanh(r_i)|\right)} + \frac{1}{2}\right)$ results in a value between [0,1], maximum here is taken over all weights in that layer. f_w^n thus quantizes weights to n-bit numbers within [-1,1].

Quantization of activations: The input to each weight layer is quantized with forward operation as defined in Equation 27.

$$\textbf{Forward: } r_o = f_a^n(r_i) = \text{quantize}_n(r_i) \tag{27}$$

Here, r_i is passed through an activation function that limits it within [0,1] before being used as input to f_a^n.

4. Related Work

In our previous work [1], we performed a comprehensive analysis of transferability among quantized and full-precision networks trained on the MNIST and CIFAR-10 datasets. The analysis involved various attack algorithms, as well as variations in model-related properties like architecture and capacity. The findings show that although transferability, in general, remains poor, it may be possible to improve the attack transfer rate using UAP. Further, it was observed that the attacks like BA and CW had high efficiency when applied on the source network even in the case of low-bitwidth networks. Additionally, it was observed that an attacker might be able to predict the success rate of an attack on a target network with different bitwidths, capacities, and architectures based on the performance of the attack when transferred among different bitwidth versions of the source model.

There has been substantial research related to network quantization, adversarial examples, and the impact of adversarial attacks on both full-precision and quantized models, providing significant insights into the vulnerability and robustness of quantized networks.

4.1. Quantization

A survey on various works on quantization of DNNs is presented in [20]. The paper provides an overview of different types and techniques of quantization along with the references to different networks that implement those methods. The case studies presented in the paper involving XNOR-Net [39] and Binaryconnect [40] provide a good starting point for understanding binarized networks.

The paper also provides an introduction to the DoReFa-Net method [37] which is used in this work for quantization. Further, it also compares DoReFa-Net with other quantization methods in terms of accuracy of the resulting quantized networks. The comparisons in this paper helped to confirm that DoReFa-Net had no known issues and that the performance was comparable, if not better, than other similar quantization techniques. This strong performance was a key factor in our decision to select DoReFa-Net for quantization.

Authors in [18] provide details on how TensorFlow Lite [41] can be used for quantization. Although the strategies and the quantization process itself are only focused on TensorFlow Lite's implementation, the findings are significant and can be generalized for other quantization tools as well. The key takeaway is that fine-tuning an already trained network leads to better accuracy models after quantization than training from scratch and that the models with large number of parameters are more resistive to accuracy loss due to quantization. This observation is in agreement with the conclusion drawn from the model configuration experiment in [37].

In [42], authors present an open-source model optimization framework called Mayo which supports multiple compression techniques like the Low-rank Approximation (LRA) [43], quantization and pruning [17]. These compression techniques are implemented through objects called *overriders* which can be applied to any network component like weights, biases, activations or gradients to customize their value. Further, Mayo also allows chaining of multiple overriders meaning that multiple compression techniques can be applied in a sequence. This unique ability enables Mayo to achieve higher compression ratio than any other compression APIs.

However, there are several drawbacks with Mayo; for instance, it uses multiple YAML files for configuration, which makes it customizable but also makes the control flow complex and hard to comprehend for custom implementations. Moreover, there is no clear explanation on how quantization is performed. Authors mention that the quantization is fixed point [42] but do not go into details on how this is done.

The Model Optimization Toolkit[2] from TensorFlow provides multiple methodologies for network quantization. However, the post-training quantization does not support quantization other than 16-bit float and 8-bit integer. The quantization aware training allows to define specific bitwidths for each layer during training, but quantization parameter configuration (like custom bitwidths) are not supported for deployment, meaning that although network layers can be trained at lower bitwidths, model execution takes place at 8 bits. Therefore, lower bitwidth quantization is not possible.

4.2. Adversarial Examples

In [4], authors argue that adversarial examples exist not due to extreme non-linearity or over-fitting of a model, but rather because of its linear behaviour in high dimensions. Authors use this hypothesis to introduce the Fast Gradient Sign Method (FGSM) for creating adversarial examples. FGSM being able to produce successful adversarial examples provides validity to the claim that these examples exploit the model's inherent linearity. The paper also makes an important observation that the adversarial examples exist in broad contiguous regions in input space rather than in fine pockets. For multiple models, these adversarial subspaces are shared. Perturbations leading to the shared subspaces lead to adversarial transfers. Thus, direction of perturbation is important for transferability rather than magnitude.

Authors further explore the concept of adversarial subspaces in [23] where they estimate the dimensionality of this subspace. They find that compared to the input dimension, the dimension of the adversarial subspace is relatively small. The perturbation directions leading to the adversarial subspace are referred to as *adversarial directions*. These orthogonal adversarial directions are shared across multiple models, forming a common subspace. As a result, all adversarial points within this shared subspace are transferable, meaning they can fool any model that share it. Further, authors show that the minimum distance required to cross the decision boundary for any data point is least in the adversarial direction while it is higher in random directions. This means that adding small perturbations is enough to make the data point cross the decision boundary if the perturbation is in the adversarial direction, while larger perturbations are necessary if the perturbation directions are random.

A comprehensive study on how model-specific properties like model accuracy, capacity, and architecture affect transferability is presented in [24]. Here, the authors use Iterative Fast Gradient Sign Method (IFGSM) [25] and FGSM to generate adversarial attacks; hence, the findings are valid only for attacks that leverage loss gradients to create adversarial samples. Authors show that the attacks crafted on low-accuracy networks have very poor transferability regardless of model's capacity and that same architecture transfers are better than different architecture transfers. Further, authors argue that the iterative attacks transfer better than single-step attacks; however, direct attack effectiveness is not considered.

In [30], authors use a custom attack based on Projected Gradient Descent (PGD) algorithm [35] to study both transferability and direct attack effectiveness on various types of networks. Different types of classifiers including Support Vector Machines (SVMs), logistic regression, and neural networks are considered. Authors find that high-complexity networks require less distortion to produce successful adversarial examples because sudden changes in the loss function mean local optima are easier to find. This also meant that highly regularized models were hard to create successful adversarial samples against. Moreover, authors also find that both transferability and attack performance on the source network increases when the hyperparameter value associated with the attack is increased. However, since the attack is gradient-based, the observations, like

[2]https://www.tensorflow.org/model_optimization

[24], are limited for gradient-based attacks.

The study in [44] offers a unique perspective on adversarial examples, arguing that all datasets contain non-robust features which are imperceptible to humans but are highly predictive. Models become sensitive to these features as they learn to rely on them during training. These features are brittle and therefore samples with slight change in them can cause misclassification. Additionally, these features being non-perceptible also means that changes are not visible. The presence of these non-robust features also leads to adversarial examples being transferable because all datasets contain these features and thus models trained on similar datasets are likely to learn similar non-robust features.

In [45], authors present a study on transferability among multiple networks. The paper considers various models including ResNet50, ResNet101, ResNet152, VGG16, and GoogleNet [46]. FGSM, FGM (Fast Gradient Method), and a custom optimization based attack[3] are used to generate adversarial examples. Both FGM and optimization based attack were found to have similar transferability. Interestingly, the transferability between networks with similar architectures was not found to be consistently better than between networks with different architectures, a result that contrasts with [24] but aligns with our findings in [1]. Moreover, the authors observed that the optimization based attack performed better than the other two attacks when applied on the source network, possibly because FGSM and FGM create adversarial samples in a single step and thus sacrifice efficiency for speed.

Authors in [47] use a tool called Deep Learning Verifier (DLV) [48] to generate adversarial examples. DLV performs an exhaustive search within a defined radius around an image and returns all possible adversarial examples (if any) and thus provides a guarantee that apart from the ones that are discovered, the image is robust against all other perturbations within the defined region. In their experiments, authors find that some classes in MNIST dataset had smaller number of effective adversarial samples than others. This indicates that not all classes in a dataset are equally robust and some might be more vulnerable than others.

Regarding adversarial attack generation, there are several popular tools that can be used to implement multiple attack algorithms. For instance, [26] uses FoolBox [49] to implement FGSM and DeepFool [33] attacks; [27] and [23] uses CleverHans library [50] to implement JSMA and FGM, respectively. Moreover, several works like UAP provide open source access to their work[4] so that the community can build on them. In [1] and in this work, we use Adversarial Robustness Toolbox (ART) [51] to create adversarial examples. The library supports comparatively large number of attack algorithms and provides comprehensive documentation for each attack implementation, along with an actively maintained codebase[5].

4.3. Vulnerability of Quantized Networks to Adversarial Examples

In [22], authors use multiple attack algorithms to evaluate the robustness of quantized networks against adversarial attacks. The paper uses DoReFa-Net for network quantization. However, Binary Neural Network (BNN) [52] is used for 1-bit quantization while DoReFa-Net is used only for 2-bit, 3-bit, and 4-bit quantization. The robustness of quantized networks against attacks created on the same network as well as against transfer-based attacks is examined for five attack types: FGSM, Basic Iterative Method (BIM) [25], Simultaneous Perturbation Stochastic Approximation (SPSA) [53], CW attack, and Zeroth Order Optimization (ZOO) [54]. Authors observe that gradient masking caused by activation quantization may increase the robustness of a quantized network against gradient-estimation algorithms like ZOO and gradient-based attacks like FGSM and BIM, but some gradient-estimation algorithms, like SPSA and CW, that are specialized to handle noise function were found to be still effective. These observations are similar to ours as we discuss in Section 7.2. However, we analyse this phenomena further with additional attacks. Furthermore, authors show that weight-only quantization does not affect attack performance at source as the attacks can still produce similar variance in logit values in quantized networks as in full-precision networks.

The work in [21] investigates the transferability of adversarial attacks among compressed networks. The study considers pruning and quantization as compression techniques and uses Mayo [42] for compression. BIM, IFGM, and DeepFool are used to craft adversarial examples. Authors show that the density of a network can be reduced to as low as 15% for both CIFAR10 and MNIST networks without any reduction in the test accuracy. This is interesting because it shows that majority of parameters in a network are not significant and supports the claim in [20] that low-bitwidth quantization works because most parameters in a network are not useful.

Authors in [34] present a transferability study that implements various compression techniques including quantization to analyse the transferability of the UAP attack across compressed networks. A method called Additive Powers-of-two (APoT) [55] is used for quantization. PGD is used to create UAPs. The difference between the UAP crafted using PGD and FGSM (as used in this work) is that the PGD updates the overall noise vector $\boldsymbol{v}$ in mini-batches, while FGSM updates it per image. An important observation is that SVHN dataset [56] was found to be more robust against attacks created and applied on the same network as compared to CIFAR10 even when both CIFAR10 and SVHN were trained on the same network and images in both datasets had the same resolution. This indicates that some datasets are more robust to adversarial attacks due to the nature of data. Further, similar to [22], authors argue that quantization can cause gradient-based attacks to perform poorly on the source network due to gradient masking. Experiments in the paper also show that transferability is poor when source and target networks differ in bitwidths, as well as when they differ in the type of compression algorithm used.

5. Adversarial Neural Network Toolbox (ANNT)

We introduce Adversarial Neural Network Toolbox (ANNT) [57], an open-source tool that provides a unified interface for handling

[3] Optimization based attack implemented by the authors iteratively adds perturbation to a clean sample until the loss is large enough to cause misclassification.
[4] https://github.com/LTS4/universal
[5] https://github.com/Trusted-AI/adversarial-robustness-toolbox

the complete workflow of quantized model training, adversarial image creation, and model robustness evaluation. Figure 2 shows the usability of the tool in terms a basic workflow.

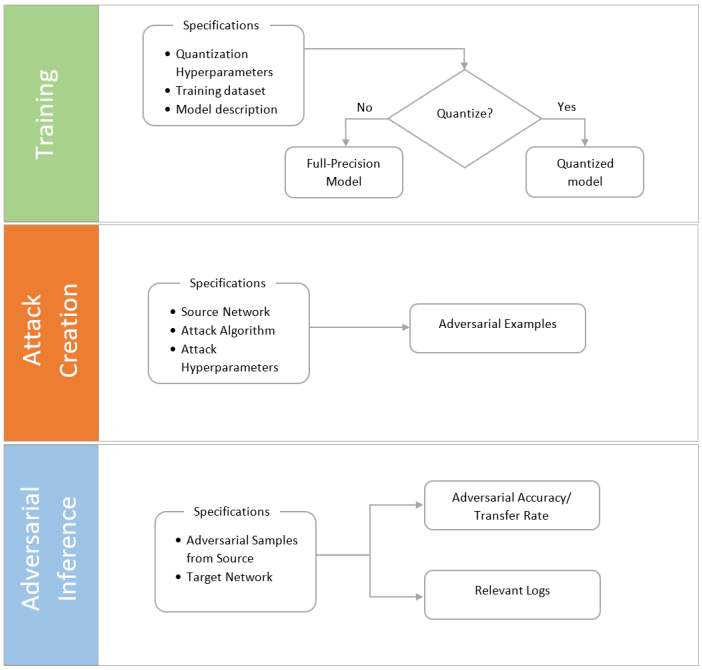


Figure 2: The custom API can be used to train models, create adversarial examples and transfer created adversarial examples.

To train full-precision models, users can provide the model description (architecture), input dataset, and training hyperparameters. Additionally, quantization hyperparameters such as the weight, activation, and gradient bitwidths can be provided to train quantized versions of a network.

The tool provides a unique functionality of generating adversarial examples on a network of specified bitwidth. Users can provide a trained model, quantization bitwidth, adversarial attack algorithm, and attack hyperparameters to create specified number of adversarial samples.

Further, the tool can also be used to perform adversarial inferences on any given target network. The process computes the accuracy of the target network against the input adversarial samples. It also generates other relevant information like the correctly and incorrectly classified samples and average L_∞ and L_2 distance between the successful adversarial and clean samples. Thus, the cumulative information generated is enough to perform a comprehensive analysis of both direct and transfer-based attacks.

The tool can be used as a standalone Python application or as a library. When used as an application, configurations like current task (training/ inference/ attack creation), bitwidths, adversarial attack algorithm (for attack creation), training hyperparameters, and dataset can be provided through a YAML file. The tool then executes the specified task and provides detailed logs of the entire process. When used as a Python library, users can simply import ANNT as a module and utilize the provided interfaces for each task. Additionally, an interface to load the generated samples for visualization is also included. The repository provides a detailed wiki as well as sample notebooks to help users get started with the tool.

In addition to MNIST trained LeNet-5 [32] and CIFAR10 trained Resnets [15] of different capacities including Resnet20, Resnet32, and Resnet44, several custom Convolutional Neural Networks (CNNs) trained on MNIST and CIFAR10 are supported out-of-the-box. Further, five different attack types—FGSM, CW attack, Boundary Attack, JSMA, and UAP—are supported.

The tool is based on TensorFlow 1.13 [58] and uses Tensorpack 0.11 [59] for model training and inference. Further, DoReFa-Net [37] is used for quantization while Adversarial Robustness Toolbox (ART) [51] is used to create adversarial samples.

6. Experimental Setup

6.1. Datasets and Models

The details regarding the datasets and full-precision (32-bit) models used in the experiments are shown in Tables 1 and 2, respectively.

Table 1: MNIST and CIFAR10 datasets.

Dataset	Remarks
MNIST	• 60,000 images in training set, • 10,000 images in test set, • 28x28 grayscale images, • 10 distinct labels
CIFAR10	• 50,000 images in training set, • 10,000 images in test set, • 32x32 colour images, • 10 distinct labels

Table 2: Full-precision (FP) MNIST and CIFAR10 models used in the experiments.

Dataset	Model ID	Test Set Accuracy	Parameters
MNIST	Mnist A	0.991	414K
CIFAR10	Resnet20	0.892	269K

All models were trained from scratch. The MNIST model (named as Mnist A) is a custom CNN while Resnet20 is a ResNet [15] trained on CIFAR10. The model architecture for Mnist A[6] and Resnet20[7] are based on the examples defined in the Tensorpack repository [59].

6.2. Quantization

1-bit, 2-bit, 4-bit, 8-bit, 12-bit, and 16-bit quantized versions of the models in Table 2 were trained. As recommended in [37], the first and last layers were not quantized in favour of better accuracy.

[6]https://github.com/tensorpack/tensorpack/blob/master/examples/basics/mnist-convnet.py
[7]https://github.com/tensorpack/tensorpack/blob/master/examples/ResNet/cifar10-resnet.py

Quantization here refers to weight and activation quantization. Thus, an 8-bit network means both weights and activations are quantized to 8 bits.

Table 3 shows the accuracy of the quantized versions of the Mnist A and Resnet20 models. Like the FP versions, all quantized models were trained from scratch. As can be seen, quantization did not result in noticeable drop in accuracy for models trained on MNIST, while CIFAR10 models show a non-negligible decrease in accuracy. This was expected because DoReFa-Net is known to result in accuracy drops for more natural datasets [37].

Table 3: Test set accuracy of the quantized versions of the Mnist A and Resnet20.

Quantization Bitwidth	Test Set Accuracy *Mnist A*	*Resnet20*
1	0.991	0.834
2	0.991	0.865
4	0.992	0.847
8	0.992	0.829
12	0.991	0.843
16	0.990	0.842

6.3. Attacks and Metrics

Attacks: Table 4 summarizes the attack algorithms used along with other relevant information.

Table 4: Adversarial attack algorithms used and their key characteristics.

Algorithm	Gradient-Based/ Gradient-Free	Iterative/ Single-Step	Distance Metric
FGSM	Gradient-based	Single-step	L_∞
JSMA	Gradient-based	Iterative	L_0
UAP	Gradient-based	Iterative	L_∞
CW	Gradient-based	Iterative	L_2
BA	Gradient-free	Iterative	L_2

Attack hyperparameters: Table 5 shows the selected hyperparameter values for each attack type for both Mnist A and Resnet20 models.

In the case of FGSM, ε controls the magnitude of perturbation introduced to the images. In JSMA, θ is the amount of distortion added per feature in each iteration and γ is the percentage of features allowed to be distorted for an image. For UAP, ε is the perturbation magnitude for FGSM which is used to generate adversarial examples within the UAP (Section 3.4), ξ is the maximum allowed magnitude of perturbation of the UAP noise vector. As recommended in [34], we measure ξ in L_∞. For the Boundary Attack, i is the maximum number of iterations[8]. Finally, for CW attack, $\kappa \geq 0$ controls attack confidence, i is the number of iteration the algorithm runs per image (gradient descent steps), $c > 0$ is a balancing constant used in the optimization problem (Equation 18), b_s is the number of binary search steps to determine c, and c_i is the initial value of c. The values of c_i and b_s were selected based on the original paper [27], while κ was varied to control distortion. The values of hyperparameters in Table 5 were selected such that the images were distorted but yet remained recognizable to human observers.

Table 5: Attack hyperparameter values for the full-precision (FP) and quantized versions of the MNIST and CIFAR10 models.

ModelID	Attack	Hyperparameter	Value
Mnist A	FGSM	ε	0.25
	JSMA	θ	1
		γ (%)	10
	UAP	ε	0.1
		ξ	0.6
	BA	i	15
	CW	κ	5
		i	25
		b_s	20
		c_i	0.01
Resnet20	FGSM	ε	0.05
	JSMA	θ	0.3
		γ (%)	5
	UAP	ε	0.01
		ξ	0.1
	BA	i	12
	CW	κ	5
		i	25
		b_s	20
		c_i	0.01

Attack metrics: Based on the metrics used by the current state of the art, there are two possibilities for representing the effectiveness of an adversarial attack on a network: adversarial accuracy and evasion rate.

Adversarial Accuracy is the accuracy of a network against adversarial examples. It is expressed as the ratio of the number of adversarial examples that are classified correctly by the network to the total number of samples used to attack the network.

For a set of pairs of clean sample and its adversarial counterpart,

$$N = \{(\boldsymbol{x}_1, \boldsymbol{x}_1^{adv}), (\boldsymbol{x}_2, \boldsymbol{x}_2^{adv}), \ldots, (\boldsymbol{x}_n, \boldsymbol{x}_n^{adv})\}$$

the adversarial accuracy is computed as below:

$$\textit{Adv. accuracy} = \frac{\left|\{x^{\text{adv}} \in N : \arg\max_i f_i(x^{\text{adv}}) = y^{\text{true}}\}\right|}{|N|} \quad (28)$$

Here, f is the classifier in which the attack is applied.

Similarly, *evasion rate* gives the success rate of the adversarial attack on a network. It is defined by the ratio of the number of adversarial examples that are classified incorrectly by the network to the total number of samples used to attack the network. This is computed as:

[8]The values of δ and ε, as mentioned in Section 3.4 are adjusted automatically. ART initializes both of them as 0.01, altering this initial value did not create any noticeable change in final quality of samples, and thus were left at their default values for the experiments.

$$\textit{Evasion rate} = \frac{\left|\{x^{\text{adv}} \in N : \arg\max_i f_i(x^{\text{adv}}) \neq y^{\text{true}}\}\right|}{|N|} \quad (29)$$

A network having higher adversarial accuracy means the model is more robust against the attack, while an attack having higher evasion rate means the network is less robust.

Any one of these metrics can be used to represent adversarial robustness. [21, 22, 45] use Equation 28, whereas [23, 24, 30, 34] use Equation 29.

In this paper, we use adversarial accuracy, as we have selected the same metric in [1]. This is simply a preference, using evasion rate would not affect the observations or the results.

Training of all models, adversarial examples creation, and computation of adversarial accuracy on target network were done using ANNT.

7. Experiments, Observations, and Analysis

7.1. Experiments

A random sample of 1,000 clean images was selected from the MNIST dataset (Table 1). Taking FP Mnist A (Table 2), and its quantized counterparts (Table 3) as source networks, adversarial examples were created using all attack types described in Table 4 with attack hyperparameter values as described in Table 5. When creating adversarial examples, inherent inefficiencies of the models were avoided by selecting only those clean samples that were correctly classified by the source network. The samples were then applied on the same source network. The resulting adversarial accuracy of the network, along with the average L_2 and L_∞ distances (as a measure of distortion) between the successful adversarial and clean samples were recorded. The samples were taken again, and the process was repeated for 3 independent runs.

The same procedure was performed for FP Resnet20 (Table 2) and its quantized versions (Table 3). Table 6 shows averaged adversarial accuracies and the L_p distances from the 3 runs for each MNIST and CIFAR10 model.

7.2. Observations and Evaluation

Based on the results in Table 6, the following observations can be made:

Observation 1: The Boundary Attack has high effectiveness. For both CIFAR10 and MNIST models, the Boundary Attack shows very high effectiveness while requiring very less number of iterations to look like the original image. From Figure 3, it can be seen that it just takes about 15 iterations for MNIST and 12 for CIFAR10 for the adversarial images to look like the original image. This also goes along with the observation made in [26] where it takes very less number of iterations to make the initial random image look like the original image with more visible distortions at lower iterations.

The attack's high effectiveness across all models, including the quantized ones, makes sense because it keeps the initialized image adversarial for any number of iterations in all cases.

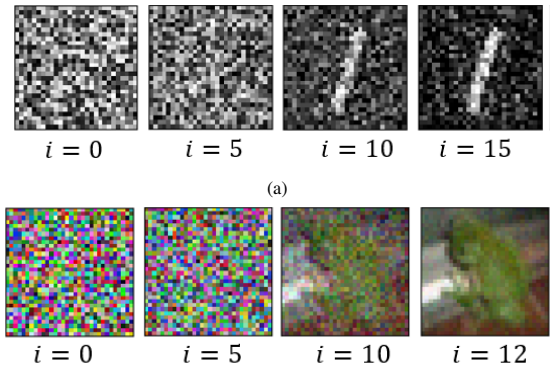


Figure 3: The adversarial image generation progression using the Boundary Attack depicted over multiple iterations on: (a) Mnist A FP model. (b) Resnet20 FP model.

Observation 1.1: Adversarial images generated by the Boundary Attack are more distorted in case of quantized networks. Ideally, when given enough iterations, the Boundary Attack should generate adversarial image which looks exactly like the original image with no visible distortions. However, compared to the FP models, majority of the adversarial images produced with quantized models especially at lower bitwidths were more distorted. This can also be observed in terms of L_2 distances in Table 6 where L_2 distances in case of 1-bit quantized network is higher when compared to the corresponding FP network.

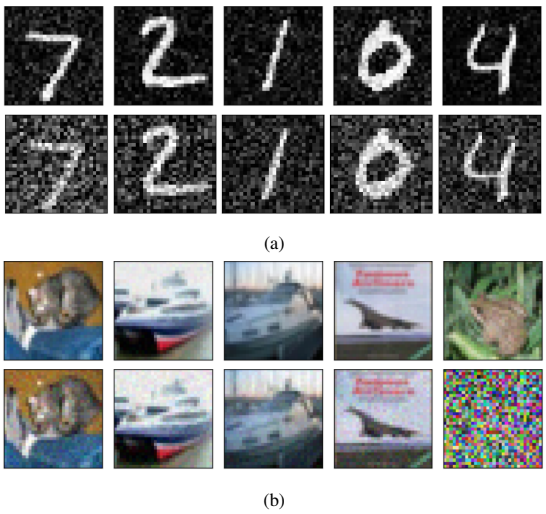


Figure 4: Adversarial examples generated by the Boundary Attack on: (a) Mnist A FP model (top row of 5 images) and 1-bit quantized Mnist A (bottom row of 5 images) for 100 iterations. (b) Resnet20 FP model (top row of 5 images) and 1-bit quantized Resnet20 (bottom-row of 5 images) for 50 iterations. For easier comparison, all image sets are first 5 images from the corresponding datasets.

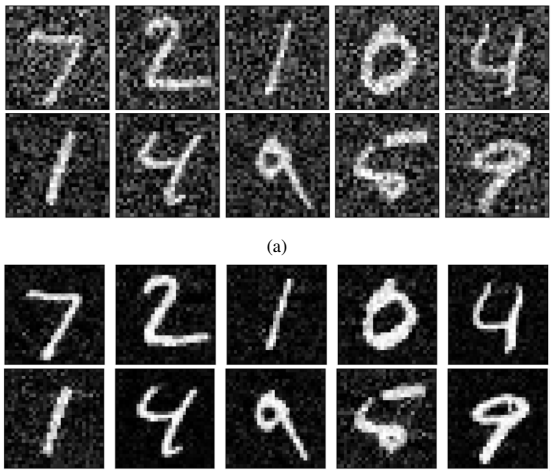
Figure 4 shows a comparison between adversarial images generated from the FP and 1-bit quantized models. As can be seen, the adversarial images for 1-bit models are more distorted with one of the images in the quantized version of Resnet20 being non-recognizable (elaboration in observation 1.2). It can be hypothesized that this is because quantized networks are more resistive to noises in the input data than their FP counterparts. The activation quantization causes activation values to be clipped [21] because of which it

Table 6: The adversarial accuracy of FP and quantized versions of Mnist A and Resnet20 against the five attacks. Attacks were created and applied on the same network. The average L_2 and L_∞ distances between the successful adversarial example and the corresponding clean sample is shown as well.

		Mnist A				ResNet20			
Bitwidth	**Attacks**	**Hyperparameter Values**	**Adversarial Accuracy**	L_2	L_∞	**Hyperparameter Values**	**Adversarial Accuracy**	L_2	L_∞
FP			0.337	5.219	0.25		0.119	2.740	0.05
1			0.845	5.134	0.25		0.137	2.737	0.05
2			0.750	5.116	0.25		0.206	2.742	0.05
4	FGSM	$\varepsilon = 0.25$	0.715	5.128	0.25	$\varepsilon = 0.05$	0.292	2.742	0.05
8			0.678	5.132	0.25		0.299	2.736	0.05
12			0.493	5.120	0.25		0.308	2.736	0.05
16			0.480	5.129	0.25		0.367	2.737	0.05
FP			0.116	5.436	1		0.074	2.425	0.436
1			0.339	7.801	1		0.142	2.504	0.513
2			0.375	6.707	1		0.247	2.581	0.395
4	JSMA	$\theta = 1$, $\gamma = 10\%$	0.140	6.814	1	$\theta = 0.3$, $\gamma = 5\%$	0.419	2.804	0.484
8			0.064	5.739	1		0.351	2.680	0.505
12			0.066	6.370	1		0.469	2.720	0.502
16			0.148	6.981	1		0.430	2.808	0.515
FP			0.114	9.352	0.6		0.176	3.362	0.1
1			0.683	9.073	0.6		0.110	3.430	0.1
2			0.555	8.585	0.6		0.154	3.275	0.1
4	UAP	$\varepsilon = 0.1$, $\xi = 0.6$	0.438	8.685	0.6	$\varepsilon = 0.01$, $\xi = 0.1$	0.169	3.414	0.1
8			0.378	8.648	0.6		0.192	3.308	0.1
12			0.174	8.618	0.6		0.297	3.390	0.1
16			0.162	8.159	0.6		0.175	3.275	0.1
FP			0.037	3.655	0.888		0.000	0.111	0.014
1			0.526	5.220	0.944		0.000	0.822	0.104
2		$\kappa = 5$,	0.558	5.047	0.928	$\kappa = 5$,	0.000	0.360	0.049
4	CW	$i = 25$, $b_s = 20$,	0.148	3.182	0.803	$i = 25$, $b_s = 20$,	0.000	0.249	0.041
8		$c_i = 0.01$	0.190	3.833	0.897	$c_i = 0.01$	0.001	0.155	0.020
12			0.163	3.650	0.874		0.000	0.102	0.013
16			0.106	3.066	0.780		0.000	0.112	0.013
FP			0.000	5.507	0.629		0.000	2.387	0.155
1			0.000	6.259	0.634		0.012	2.816	0.184
2			0.000	4.649	0.507		0.066	2.603	0.170
4	BA	$i = 15$	0.000	4.338	0.488	$i = 12$	0.045	2.859	0.186
8			0.000	4.267	0.493		0.080	2.904	0.189
12			0.001	3.664	0.432		0.002	3.128	0.203
16			0.000	3.235	0.387		0.080	2.803	0.184

becomes hard to produce differential activations from small changes at the input[9], and thus, even when the input has slight perturbations, quantized networks can correctly classify the image. This is also evident from the data from other attack types where for the same value of attack hyperparameters, FGSM, JSMA and UAP perform comparatively bad when the network is quantized. In the case of the Boundary Attack, this could mean that the algorithm cannot further reduce the distortions in an image because then the quantized network will classify the adversarial example correctly.

This hypothesis was put to test by increasing the number of iterations in the Boundary Attack to 1,000 for the 1-bit quantized Mnist A model. As can be seen in Figure 5a, the adversarial images are still equally distorted for 1-bit quantized version; whereas, the distortions are significantly less even for less number of iterations for the FP models, as seen in Figure 5b. Therefore, it would not matter if the iterations are increased any further because the algorithm will not be able to reduce the distortions due to the network being insensitive to small noises at input.



(a)

(b)

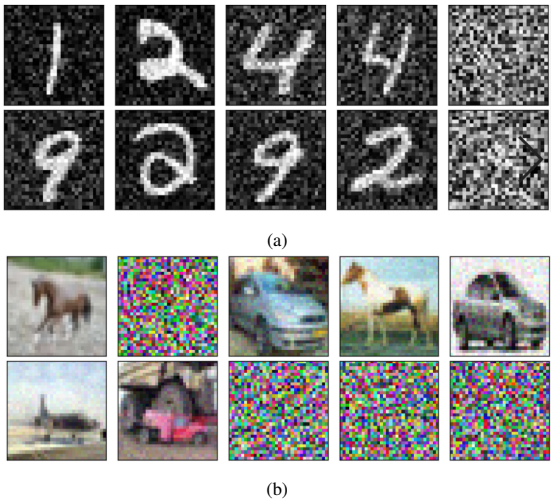
Figure 5: Adversarial examples generated by the Boundary Attack on: (a) 1-bit quantized Mnist A at 1,000 iterations. (b) Mnist A FP model at 200 iterations. Both images are first 10 images from the MNIST dataset.

Quantized networks being more resistive to input noises is also observed in [47] and [34] where the authors find that the perturbations that worked in FP stopped working in quantized networks. Quantization thus acting as a filter for adversarial noise.

Observation 1.2: Imperceptible adversarial images resulting from the Boundary Attack on quantized networks. Apart from the images that are distorted but recognizable to human oracles, the Boundary Attack also resulted in adversarial images that were completely distorted and unrecognizable but only in case of quantized networks. Figure 6 shows adversarial images generated by the Boundary Attack on 1-bit quantized versions of Mnist A and Resnet20 models. As can be seen, multiple images in both figures are unrecognizable.

This could again be due to the algorithm not being able to reduce the distortion any further because of the model being robust against input noises. To verify this, an experiment was performed in which adversarial examples were generated from 3,000 randomly sampled clean images from MNIST and CIFAR10 datasets using the 1-bit quantized versions of Mnist A and Resnet20 as source. The images that seemed to be composed of random pixels were then isolated and inferences were ran on them. It was found that for all of these images, the true class was within top-2 predicted classes. This indicates that the Boundary Attack could not reduce the L_2 distance between the original and the adversarial image any further because any further reduction would cause the image to go inside the decision boundary of the original image making the image no longer adversarial.

Imperceptible images having true labels within top-2 predicted classes also means that although the features in the images in Figure 6 are not recognizable to human observers, the network identifies these features and tries to classify them to the correct class. These features that are non-recognizable to humans but tend to be meaningful and predictive for networks are studied in [44].



(a)

(b)

Figure 6: Adversarial examples generated by the Boundary Attack on: (a) 1-bit quantized Mnist A model at 100 iterations. (b) 1-bit quantized Resnet20 at 50 iterations. The adversarial images were generated from 10 randomly selected clean images from the corresponding datasets.

One of the important qualities of adversarial examples is that they should be classified correctly by human oracles, and since these images are completely distorted, they cannot be considered as adversarial images. Thus, these examples were removed when computing source network performance in Table 6.

It is also worth noting that these imperceptible images are rare. In a set of 3,000 random images, on 3 separate runs, for 1-bit quantized Resnet20 at 12 iterations, only about 280 images on average were imperceptible. Similarly, for 1-bit quantized Mnist A at 15 iterations, on average only about 180 such images were found. Thus, these images formed very small portion of the total adversarial examples generated and only occurred for quantized networks.

The presence of these images when creating adversarial images from the Boundary Attack also suggests that although networks show near-zero resistance against the attack, quantized networks do offer certain form of resilience because valid adversarial images that have less distortion or are at least recognizable to humans become

[9]Weight quantization, on the other hand, does not contribute in poor performance of the attacks when the attacks are crafted in the same network; empirical evidence is presented in [22].

hard to create when networks are quantized.

Observation 2: CIFAR10 models require less distortion than MNIST models to produce misclassification. As can be seen from Table 6, for CIFAR10 models lower distortions are enough for the attacks to perform well, while the MNIST models require comparatively higher value of the attack hyperparameters.

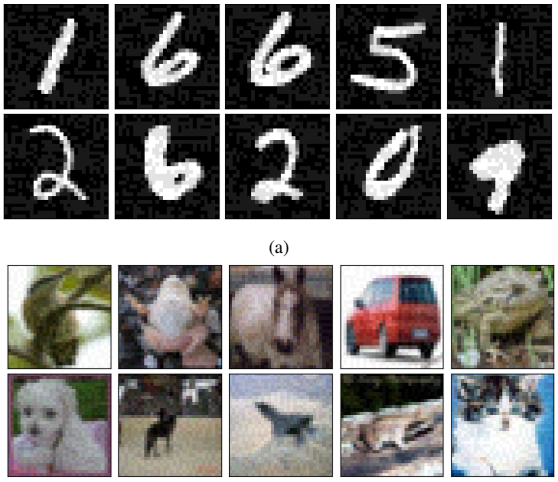


Figure 7: Adversarial examples generated using FGSM on: (a) the FP Mnist A model when $\varepsilon = 0.1$. (b) the FP Resnet20 model when $\varepsilon = 0.025$. The adversarial images were generated from 10 randomly selected clean images from the corresponding datasets.

There are two reasons for this. The first reason is that the MNIST dataset has less intra-class differences [26] which makes the classification problem easier to solve, and thus the network is less sensitive to small changes or perturbations [34]. However, in case of CIFAR10, a single class can have a large variety of objects of different shapes, sizes, and color, and thus a small change in any of the input features is enough to produce misclassification [34]. For instance, considering FGSM with $\varepsilon = 0.1$ in case of FP Mnist A model, the average adversarial accuracy from 3 separate runs on 1,000 samples was found to be 0.831. In contrast, for FP Resnet20 model, for the same attack with $\varepsilon = 0.025$, the average adversarial accuracy was found to be 0.127. Thus, comparatively, CIFAR10 trained network was more vulnerable to the resulting adversarial samples even in relatively low distortion. In both cases, the value of hyperparameter ε is selected such that the distortions were barely visible, as seen in Figure 7. Similar behaviour is reported in [34] with SVHN, an MNIST-like dataset, where SVHN models are more robust to UAP based attacks as compared to CIFAR10 models.

Another reason why CIFAR10 models show more vulnerability is the high-dimensionality of the CIFAR10 dataset as compared to MNIST. For Attacks like FGSM and UAP, which add a constant perturbation to the input in a specific direction, the same value of the constant introduces larger change at the output in higher dimension. This is also evident from Equation 10. Keeping ε constant and increasing n would cause larger change in the activations.

For CW attack as well, we can see that the same value of hyperparameters are more effective in CIFAR10 models as compared to MNIST models.

Observation 3: Quantized models are more robust to loss gradient-based attacks. Quantized models have better adversarial accuracy than their FP counterparts against loss gradient based attacks like FGSM and UAP. Similar behaviour is observed in [21, 22, 34]. The increased robustness can be attributed to the gradient masking caused due to activation quantization. Gradient masking makes the loss surface of the network hard to optimize over[10] [21, 22]. The resulting gradients no longer point to the adversarial examples [22] which makes it harder for these attacks to find useful gradients that can cause misclassification.

In the case of CW attack, high effectiveness can be observed in CIFAR10 models even when the networks are quantized. This is due to the optimization problem (Equation 18) solved by the attack, which, given enough iterations and binary search steps, will lead to misclassification. However, during attack creation, it was harder to craft adversarial samples, especially for lower bitwidths, as the resulting samples were more distorted and took more time to converge. The attack tries to introduce minimal distortion while trying to achieve misclassification (Equation 18), but due to activation quantization, it becomes difficult to achieve this as the network becomes insensitive to small perturbations, especially at lower bitwidths. Hence, even when using logits, where gradients are comparatively more expressive, the attack finds difficulty in converging. This is also evident by the significantly higher L_2 distance in the case of lower bitwidth networks (Table 6) as the attack requires higher values of c and more binary search steps to create samples. Moreover, the table shows that Mnist A has increased L_2 and robustness when quantized, further indicating increased robustness of quantized networks against such attacks.

Observation 4: JSMA performs poorly in quantized networks. The poor performance of JSMA can be explained by how JSMA creates adversarial examples. In each iteration, the JSMA algorithm seeks to find the input features that cause positive change towards the target adversarial class (Equation 15) and at the same time reduce the overall class probabilities of all other classes. When it finds these features, it adds defined amount of distortion to those features (for instance, $\theta = 1$ and $\theta = 0.3$ in Table 6) while also restraining total distortion to a limit ($\gamma = 10\%$ and $\gamma = 5\%$, respectively). When networks are quantized, activation quantization makes the network insensitive to small changes in input as the small noises fail to produce any change in activations. Thus, JSMA struggles to find features that, when distorted by the defined amount, can cause misclassification.

This hypothesis was tested by randomly sampling 2,000 clean samples from MNIST and CIFAR10 datasets and creating adversarial examples using JSMA on Mnist A, Resnet20, and all their quantized versions. Average L_0 distance between the adversarial samples and their corresponding benign counterparts were recorded. Three individual runs were carried out and the average L_0 distance from those runs for each model are as shown in Table 7. As can be seen, on average, quantized networks required more features to be distorted than the corresponding FP model. This indicates that JSMA was struggling to find features to build adversarial examples.

Thus, although not using loss-gradients, the activation quantization causes JSMA to be less effective on quantized networks.

[10]Clipping of activations causes activations to remain in the same bucket causing no change or to switch to another bucket causing large change.

Table 7: Average L_0 distances between the clean and adversarial samples produced using JSMA on the FP and quantized versions of Mnist A and Restnet20 models.

	L_0 **Distance**	
Quantization Level	*Mnist A* ($\theta = 1, \gamma = 10\%$)	*Resnet20* ($\theta = 0.3, \gamma = 5\%$)
FP	50.007	82.592
1	69.047	85.256
2	67.219	102.211
4	55.285	120.840
8	43.437	113.121
12	48.293	121.370
16	53.745	119.264

7.3. Summary

Based on the observations, the following statements can be made:

1. *MNIST models are more robust to adversarial attacks than the CIFAR10 models for some attack types.* FGSM, UAP, CW attack and JSMA were found to be more effective on CIFAR10 models. This can be attributed to the characteristics of the data. MNIST has less variations in a single class, while CIFAR10 has larger variation of objects; thus the classification problem is simpler in case of MNIST as compared to CIFAR10. This is also reflected by the MNIST models being able to achieve very high test accuracies while the test accuracies of the CIFAR10 models are comparatively low (Tables 2 and 3). Further, high dimensionality of CIFAR10 also causes it to have less adversarial robustness.
2. *Quantized networks show resistance against both gradient-based and gradient-free attacks.* Activation clipping causes quantized networks to filter small noises at the input which makes the network more resilient to attacks. This was already known for attacks like FGSM and UAP from the findings in [22] and [34], respectively. This study further demonstrates that this also applies for attacks like JSMA that do not use loss gradients, for search-based attacks like the Boundary Attack, and also for the CW attack that uses logits and a more powerful objective function. Although the Boundary Attack and CW attack depicted very high effectiveness, even on quantized networks, the adversarial samples were found to be more distorted, with the Boundary Attack sometimes producing non-recognizable samples. This can be considered as a form of resilience against the attacks as the samples become more detectable and harder to create. Thus, although limited, quantization seems to provide some resistance against direct adversarial attacks.

8. Discussion

- Attacks like FGSM and UAP, which rely on loss gradients at the output layer to generate adversarial examples, tend to be less effective against quantized networks due to gradient masking [22, 34]. Interestingly, as noted in [22], CW attack demonstrated higher effectiveness in quantized networks, particularly with natural datasets. However, our analysis indicates that quantized networks offer resistance during attack creation. This resistance was also observed with attacks like JSMA and the Boundary Attack, where activation quantization can make networks more robust against direct attacks to some extent.

  Furthermore, the effectiveness of some attack algorithms also depends on the characteristics of the data itself. Models trained on natural datasets like CIFAR10 seem to be more vulnerable to some attacks than those trained on datasets like MNIST. Similar observation was made in [34] for UAP attacks on SVHN and CIFAR10 datasets.

  We consider five different attack algorithms. FGSM is a single-step attack that uses loss gradients to create adversarial examples, whereas JSMA iteratively distorts selected pixels without relying on loss gradient information. UAP, on the other hand, focuses on finding a universal perturbation that can generalize across multiple images, rather than crafting unique adversarial samples for each one. CW attack, in contrast, performs gradient descent towards misclassification. The Boundary Attack is a gradient-free method that generates adversarial samples without requiring access to the model's parameters or training data. Thus, the algorithms are conceptually diverse, allowing the analysis to incorporate a broader range of attack strategies and provide a more comprehensive view on adversarial robustness.

- Reproducibility is a significant challenge in ML. Use of a single tool with well-documented functionality makes it easier for other researchers to reproduce and validate experiments. To facilitate this, we open-source our experimentation tool, ANNT. The consistent interface provided by ANNT for various tasks means that it is easier to standardize experiments and switch between different configurations. Researchers can easily share logs and configurations to replicate experiments.

  The resources used in the experiments in this paper, including trained models, adversarial images, and the experiment results in the form of logfiles (including those from [1]) are available at https://mega.nz/fm/public-links/ql8CwJxb. Thus, the data, along with ANNT is sufficient to replicate the experimental results.

9. Conclusion

In this work, we analyze the adversarial robustness of DNNs under direct attacks. Within this premise, we evaluate multiple attack methods on models trained on CIFAR10 and MNIST datasets and quantized to different bitwidths. Our findings, along with those from [1] indicate that quantization provides some protection against both direct and transfer-based attacks.

We also present ANNT, a tool designed to facilitate the validation of our results and support further research in this area.

References

[1] A. Shrestha, J. Großmann, "Properties that allow or prohibit transferability of adversarial attacks among quantized networks," in Proceedings of the 5th

ACM/IEEE International Conference on Automation of Software Test (AST 2024), AST '24, 99–109, Association for Computing Machinery, New York, NY, USA, 2024, doi:10.1145/3644032.3644453.

[2] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, R. Fergus, "Intriguing properties of neural networks," CoRR, **abs/1312.6199**, 2014, doi:10.48550/arXiv.1312.6199.

[3] S.-M. Moosavi-Dezfooli, A. Fawzi, O. Fawzi, P. Frossard, "Universal adversarial perturbations," in Proceedings of the IEEE conference on computer vision and pattern recognition, 1765–1773, 2017, doi:10.48550/arXiv.1610.08401.

[4] I. J. Goodfellow, J. Shlens, C. Szegedy, "Explaining and Harnessing Adversarial Examples," arXiv preprint arXiv:1412.6572, 2015, doi:10.48550/arXiv.1412.6572.

[5] M. Yasmin, M. Sharif, S. Mohsin, "Neural Networks in Medical Imaging Applications: A Survey," World Applied Sciences Journal, **22**, 12, 2013.

[6] J. Grossmann, N. Grube, S. Kharma, D. Knoblauch, R. Krajewski, M. Kucheiko, H.-W. Wiesbrock, "Test and Training Data Generation for Object Recognition in the Railway Domain," in P. Masci, C. Bernardeschi, P. Graziani, M. Koddenbrock, M. Palmieri, editors, Software Engineering and Formal Methods. SEFM 2022 Collocated Workshops, 5–16, Springer International Publishing, Cham, 2023, doi:10.1007/978-3-031-26236-4_1.

[7] E. C. Pinto Neto, D. M. Baum, J. R. d. Almeida, J. B. Camargo, P. S. Cugnasca, "Deep Learning in Air Traffic Management (ATM): A Survey on Applications, Opportunities, and Open Challenges," Aerospace, **10**(4), 2023, doi:10.3390/aerospace10040358.

[8] J. C.-W. Lin, G. Srivastava, Y.-D. Zhang, "Special Issue Editorial: Advances in Computational Intelligence for Perception and Decision-Making for Autonomous Systems," ISA Transactions, **132**, 1–4, 2023, doi:10.1016/j.isatra.2023.01.031.

[9] Y. Ijiri, M. Sakuragi, Shihong Lao, "Security Management for Mobile Devices by Face Recognition," in 7th International Conference on Mobile Data Management (MDM'06), 49–49, IEEE, 2006, doi:10.1109/MDM.2006.138.

[10] A. I. Awad, A. Babu, E. Barka, K. Shuaib, "AI-powered biometrics for Internet of Things security: A review and future vision," Journal of Information Security and Applications, **82**, 103748, 2024, doi:https://doi.org/10.1016/j.jisa.2024.103748.

[11] H. Cui, Z. Chen, Y. Xi, H. Chen, J. Hao, "IoT Data Management and Lineage Traceability: A Blockchain-based Solution," in 2019 IEEE/CIC International Conference on Communications Workshops in China (ICCC Workshops), 239–244, IEEE, 2019, doi:10.1109/ICCChinaW.2019.8849969.

[12] N. M. Gonzalez, W. A. Goya, R. de Fatima Pereira, K. Langona, E. A. Silva, T. C. Melo de Brito Carvalho, C. C. Miers, J.-E. Mangs, A. Sefidcon, "Fog computing: Data analytics and cloud distributed processing on the network edges," in 2016 35th International Conference of the Chilean Computer Science Society (SCCC), 1–9, IEEE, 2016, doi:10.1109/SCCC.2016.7836028.

[13] A. Krizhevsky, I. Sutskever, G. E. Hinton, "ImageNet Classification with deep convolutional neural networks," Communications of the ACM, **60**(6), 84–90, 2017, doi:10.1145/3065386.

[14] K. Simonyan, A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition," CoRR, **abs/1409.1556**, 2014, doi:10.48550/arXiv.1409.1556.

[15] K. He, X. Zhang, S. Ren, J. Sun, "Deep Residual Learning for Image Recognition," in 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 770–778, IEEE, 2016, doi:10.1109/CVPR.2016.90.

[16] Y. Huang, H. Hu, C. Chen, "Robustness of on-Device Models: Adversarial Attack to Deep Learning Models on Android Apps," in 2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP), 101–110, IEEE, 2021, doi:10.1109/ICSE-SEIP52600.2021.00019.

[17] S. Han, J. Pool, J. Tran, W. J. Dally, "Learning both Weights and Connections for Efficient Neural Networks," Advances in neural information processing systems, **28**, 2015, doi:10.48550/arXiv.1506.02626.

[18] R. Krishnamoorthi, "Quantizing deep convolutional networks for efficient inference: A whitepaper," CoRR, **abs/1806.08342**, 2018, doi:10.48550/arXiv.1806.08342.

[19] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, H. Adam, "MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications," CoRR, **abs/1704.04861**, 2017, doi:10.48550/arXiv.1704.04861.

[20] Y. Guo, "A Survey on Methods and Theories of Quantized Neural Networks," CoRR, **abs/1808.04752**, 2018, doi:10.48550/arXiv.1808.04752.

[21] Y. Zhao, I. Shumailov, R. Mullins, R. Anderson, "To compress or not to compress: Understanding the Interactions between Adversarial Attacks and Neural Network Compression," Proceedings of Machine Learning and Systems, **1**, 230–240, 2020, doi:10.48550/arXiv.1810.00208.

[22] R. Bernhard, P.-A. Moellic, J.-M. Dutertre, "Impact of Low-Bitwidth Quantization on the Adversarial Robustness for Embedded Neural Networks," in 2019 International Conference on Cyberworlds (CW), 308–315, IEEE, 2019, doi:10.1109/CW.2019.00057.

[23] F. Tramèr, N. Papernot, I. Goodfellow, D. Boneh, P. McDaniel, "The Space of Transferable Adversarial Examples," arXiv preprint arXiv:1704.03453, 2017, doi:10.48550/arXiv.1704.03453.

[24] L. Wu, Z. Zhu, C. Tai, W. E, "Understanding and Enhancing the Transferability of Adversarial Examples," arXiv preprint arXiv:1802.09707, 2018, doi:10.48550/arXiv.1802.09707.

[25] A. Kurakin, I. Goodfellow, S. Bengio, "Adversarial examples in the physical world," CoRR, **abs/1607.02533**, 2017, doi:10.48550/arXiv.1607.02533.

[26] W. Brendel, J. Rauber, M. Bethge, "Decision-Based Adversarial Attacks: Reliable Attacks Against Black-Box Machine Learning Models," arXiv preprint arXiv:1712.04248, 2018, doi:10.48550/arXiv.1712.04248.

[27] N. Carlini, D. Wagner, "Towards Evaluating the Robustness of Neural Networks," in 2017 IEEE Symposium on Security and Privacy (SP), 39–57, IEEE, 2017, doi:10.1109/SP.2017.49.

[28] X. Huang, D. Kroening, W. Ruan, J. Sharp, Y. Sun, E. Thamo, M. Wu, X. Yi, "A Survey of Safety and Trustworthiness of Deep Neural Networks: Verification, Testing, Adversarial Attack and Defence, and Interpretability," Computer Science Review, **37**, 100270, 2020, doi:10.48550/arXiv.1812.08342.

[29] N. Papernot, P. McDaniel, S. Jha, M. Fredrikson, Z. B. Celik, A. Swami, "The Limitations of Deep Learning in Adversarial Settings," CoRR, **abs/1511.07528**, 2015, doi:10.48550/arXiv.1511.07528.

[30] A. Demontis, M. Melis, M. Pintor, M. Jagielski, B. Biggio, A. Oprea, C. Nita-Rotaru, F. Roli, "Why Do Adversarial Attacks Transfer? Explaining Transferability of Evasion and Poisoning Attacks," in 28th USENIX security symposium (USENIX security 19), 19, 2019, doi:10.48550/arXiv.1809.02861.

[31] A. Krizhevsky, "Learning Multiple Layers of Features from Tiny Images," 60, 2009.

[32] Y. Lecun, L. Bottou, Y. Bengio, P. Haffner, "Gradient-based learning applied to document recognition," Proceedings of the IEEE, **86**(11), 2278–2324, 1998, doi:10.1109/5.726791, conference Name: Proceedings of the IEEE.

[33] S.-M. Moosavi-Dezfooli, A. Fawzi, P. Frossard, "DeepFool: a simple and accurate method to fool deep neural networks," in Proceedings of the IEEE conference on computer vision and pattern recognition, 2574–2582, 2016, doi:10.48550/arXiv.1511.04599.

[34] A. G. Matachana, K. T. Co, L. Muñoz-González, D. Martinez, E. C. Lupu, "Robustness and Transferability of Universal Attacks on Compressed Models," CoRR, **abs/2012.06024**, 2020, doi:10.48550/arXiv.2012.06024.

[35] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, A. Vladu, "Towards Deep Learning Models Resistant to Adversarial Attacks," arXiv preprint arXiv:1706.06083, 2019, doi:10.48550/arXiv.1706.06083.

[36] N. Papernot, P. McDaniel, X. Wu, S. Jha, A. Swami, "Distillation as a Defense to Adversarial Perturbations against Deep Neural Networks," in 2016 IEEE symposium on security and privacy (SP), 582–597, IEEE, 2016, doi:10.48550/arXiv.1511.04508.

[37] S. Zhou, Y. Wu, Z. Ni, X. Zhou, H. Wen, Y. Zou, "DoReFa-Net: Training Low Bitwidth Convolutional Neural Networks with Low Bitwidth Gradients," CoRR, **abs/1606.06160**, 2018, doi:10.48550/arXiv.1606.06160.

[38] Y. Bengio, N. Léonard, A. Courville, "Estimating or Propagating Gradients Through Stochastic Neurons for Conditional Computation," CoRR, **abs/1308.3432**, 2013, doi:10.48550/arXiv.1308.3432.

[39] M. Rastegari, V. Ordonez, J. Redmon, A. Farhadi, "XNOR-Net: ImageNet Classification Using Binary Convolutional Neural Networks," **9908**, 525–542, 2016, doi:10.1007/978-3-319-46493-0_32, series Title: Lecture Notes in Computer Science.

[40] M. Courbariaux, Y. Bengio, J.-P. David, "BinaryConnect: Training Deep Neural Networks with binary weights during propagations," Advances in neural information processing systems, **28**, 9, 2015, doi:10.48550/arXiv.1511.00363.

[41] TensorFlow Lite, "TensorFlow Lite | ML for Mobile and Edge Devices," 2021.

[42] Y. Zhao, X. Gao, R. Mullins, C. Xu, "Mayo: A Framework for Auto-generating Hardware Friendly Deep Neural Networks," in Proceedings of the 2nd International Workshop on Embedded and Mobile Deep Learning, 25–30, ACM, 2018, doi:10.1145/3212725.3212726.

[43] M. Jaderberg, A. Vedaldi, A. Zisserman, "Speeding up Convolutional Neural Networks with Low Rank Expansions," CoRR, **abs/1405.3866**, 2014, doi:10.48550/arXiv.1405.3866.

[44] A. Ilyas, S. Santurkar, D. Tsipras, L. Engstrom, B. Tran, A. Madry, "Adversarial Examples Are Not Bugs, They Are Features," Advances in neural information processing systems, **32**, 2019, doi:10.48550/arXiv.1905.02175.

[45] Y. Liu, X. Chen, C. Liu, D. Song, "Delving into Transferable Adversarial Examples and Black-box Attacks," CoRR, **abs/1611.02770**, 2017, doi:10.48550/arXiv.1611.02770.

[46] C. Szegedy, Wei Liu, Yangqing Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, A. Rabinovich, "Going deeper with convolutions," in 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 1–9, IEEE, 2015, doi:10.1109/CVPR.2015.7298594.

[47] K. Duncan, E. Komendantskaya, R. Stewart, M. Lones, "Relative Robustness of Quantized Neural Networks Against Adversarial Attacks," in 2020 International Joint Conference on Neural Networks (IJCNN), 1–8, IEEE, 2020, doi:10.1109/IJCNN48605.2020.9207596.

[48] X. Huang, M. Kwiatkowska, S. Wang, M. Wu, "Safety Verification of Deep Neural Networks," **10426**, 3–29, 2017, doi:10.1007/978-3-319-63387-9_1, series Title: Lecture Notes in Computer Science.

[49] J. Rauber, W. Brendel, M. Bethge, "Foolbox: A Python toolbox to benchmark the robustness of machine learning models," CoRR, **abs/1707.04131**, 2018, doi:10.48550/arXiv.1707.04131.

[50] N. Papernot, F. Faghri, N. Carlini, I. Goodfellow, R. Feinman, A. Kurakin, C. Xie, Y. Sharma, T. Brown, A. Roy, A. Matyasko, V. Behzadan, K. Hambardzumyan, Z. Zhang, Y.-L. Juang, Z. Li, R. Sheatsley, A. Garg, J. Uesato, W. Gierke, Y. Dong, D. Berthelot, P. Hendricks, J. Rauber, R. Long, P. McDaniel, "Technical Report on the CleverHans v2.1.0 Adversarial Examples Library," CoRR, **abs/1610.00768**, 2018, doi:10.48550/arXiv.1610.00768.

[51] M.-I. Nicolae, M. Sinn, M. N. Tran, B. Buesser, A. Rawat, M. Wistuba, V. Zantedeschi, N. Baracaldo, B. Chen, H. Ludwig, I. M. Molloy, B. Edwards, "Adversarial Robustness Toolbox v1.0.0," CoRR, **abs/1707.04131**, 2019, doi:10.48550/arXiv.1807.01069.

[52] M. Courbariaux, I. Hubara, D. Soudry, R. El-Yaniv, Y. Bengio, "Binarized Neural Networks: Training Deep Neural Networks with Weights and Activations Constrained to +1 or -1," CoRR, **abs/1602.02830**, 2016, doi:10.48550/arXiv.1602.02830.

[53] J. Uesato, B. O'Donoghue, A. v. d. Oord, P. Kohli, "Adversarial Risk and the Dangers of Evaluating Against Weak Attacks," in International conference on machine learning, 5025–5034, PMLR, 2018, doi:10.48550/arXiv.1802.05666.

[54] P.-Y. Chen, H. Zhang, Y. Sharma, J. Yi, C.-J. Hsieh, "ZOO: Zeroth Order Optimization based Black-box Attacks to Deep Neural Networks without Training Substitute Models," 15–26, 2017, doi:10.1145/3128572.3140448.

[55] Y. Li, X. Dong, W. Wang, "Additive Powers-of-Two Quantization: An Efficient Non-uniform Discretization for Neural Networks," CoRR, **abs/1909.13144**, 2020, doi:10.48550/arXiv.1909.13144.

[56] Y. Netzer, T. Wang, A. Coates, A. Bissacco, B. Wu, A. Y. Ng, "Reading Digits in Natural Images with Unsupervised Feature Learning," in NIPS Workshop on Deep Learning and Unsupervised Feature Learning 2011, 9, 2011.

[57] A. Shrestha, J. Großmann, "Adversarial Neural Network Toolkit," https://github.com/Abhishek2271/AdversarialNeuralNetworkToolkit, 2024.

[58] M. Abadi, P. Barham, J. Chen, Z. Chen, A. Davis, J. Dean, M. Devin, S. Ghemawat, G. Irving, M. Isard, M. Kudlur, J. Levenberg, R. Monga, S. Moore, D. G. Murray, B. Steiner, P. Tucker, V. Vasudevan, P. Warden, M. Wicke, Y. Yu, X. Zheng, "TensorFlow: A system for large-scale machine learning," OSDI'16, 21, USENIX Association, 2016, doi:10.48550/arXiv.1605.08695.

[59] Y. Wu, et al., "Tensorpack," https://github.com/tensorpack/, 2016.

ASTES

Advances in Science, Technology and Engineering Systems Journal
Vol. 9, No. 5, 30-36 (2024)
www.astesj.com
Special Issue on Innovation in Computing, Engineering Science & Technology

ASTES Journal
ISSN: 2415-6698

True Random Number Generator Implemented in ReRAM Crossbar Based on Static Stochasticity of ReRAMs

Tanay Patni*, Abhijit Pethe

Department of Electrical and Electronics Engineering,BITS Pilani K.K. Birla Goa Campus, Goa, India, 403726, India

ARTICLE INFO

Article history:
Received: 31 July, 2024
Revised: 05 October, 2024
Accepted: 06 October, 2024
Online: 30 November, 2024

Keywords:
TRNG
Memristors
ReRAM Crossbar
Static stochasticity

ABSTRACT

True Random Number Generators (TRNG) find applications in various fields, especially hardware security. We suggest a TRNG that exploits the intrinsic static stochasticity of Resistive Switching Random Access Memories (ReRAMs) to generate random bits. Other suggested designs use stochasticity in the switching mechanism, which requires high precision over input voltage and time. In the proposed design, the random bits are produced by comparing the resistance of two ReRAMs in their high resistance states. ReRAM crossbar architectures are being highly researched, and our design is completely compatible with a ReRAM crossbar. The design was verified by simulations and testing the output stream using the NIST randomness test suite. The effect of device-to-device variability was tested on the randomness of the generated output bit stream.

1. Introduction

This paper is an extension of work originally presented in The IEEE Asia Pacific Conference On Circuits And Systems (APCCAS 2023) [1]. Random Numbers find a lot of applications in various fields, including scientific simulations and modeling, games, machine learning, and, most importantly, generating cryptographic keys [2, 3, 4]. Random numbers are generated using specialized hardware called Random Number Generators (RNGs). There are two types of RNGs, Pseudo Random Number Generators (PRNGs) and True Random Number Generators (TRNGs), differentiated based on the principle of number generation. PRNGs generate random numbers using algorithms based on mathematical formulae. While PRNGs are suitable for other applications, they cannot be used for security applications as they are vulnerable to attacks [5, 6], compromising security. TRNGs exploit the stochasticity of physical processes, e.g., Thermal Noise in electrical circuits [7], to generate random numbers. Since the source of randomness in TRNGs is inherently stochastic, they, in principle, can guarantee absolute information security.

Recently, there has been an increase in IoT devices in the market, which are small and have a small power budget. Since they continuously transmit confidential and private information, there is a need for a robust security system within the devices, necessitating a suitable TRNG to generate random numbers for encryption [8, 9]. Current TRNG circuits are made of transistors and are based on thermal noise, jitter in oscillators, random telegraph noise, or chaotic systems [10, 11, 12]. These circuits are bulky, complicated, and consume a lot of power, making them unsuitable for IoT devices.

ReRAM devices can be used as an alternative to design TRNGs. ReRAMs are emerging non-volatile memory devices extensively researched for crossbar architecture. This crossbar architecture finds applications in non-volatile logic, neuromorphic computing, security, in-memory computing, etc. [13, 14]. They consume low power, are small, are compatible with the CMOS fabrication process, and have fast switching speeds. They are also inherently stochastic, making them a good alternative for TRNG circuit design. ReRAMs exhibit stochasticity in two ways – during switching and the resistance values of the stable states. Many ReRAM-based TRNG designs have been suggested in the literature before, mainly focusing on switching stochasticity [15, 16, 17]. These designs require very precise control over voltages and timing, making the circuits complicated to implement. The variability in the resistance value can also be exploited to design TRNG circuits. Since they do not require precise control of input signals, they are easier to implement. One such design compares the resistance value of two devices to extract the output bit [18].

We propose a TRNG circuit based on the above principle, implementable in a ReRAM crossbar. This enables in-situ random number generation for crossbar applications and eliminates the need for a specialized TRNG circuit. The proposed circuit is simulated in Cadence Virtuoso™, and the randomness of the output is verified using the NIST SP 800-22 test suite [19]. We further analyzed the effect of variation in the statistical properties of ReRAM stochas-

*Corresponding Author: Tanay Patni, f20201745@goa.bits-pilani.ac.in

ticity on the randomness of the output. This paper is organized as follows. The theory of ReRAM and its stochasticity is explained in section 2. The simulation setup is described in section 3. The design and results are discussed in section 4. Analysis of variation in device properties on output is done in section 5. Conclusion from this work are presented in section 6.

2. Theory

2.1. Resistive Switching Random Access Memory (ReRAM)

ReRAM is a two-terminal, non-volatile emerging memory device belonging to the family of memristive devices [20, 21]. A memristor, derived from "Memory" and "Resistor," is a two-terminal device whose resistance equals the total amount of charge flown through it. Consequently, the resistance of a ReRAM can be controlled by applying a voltage across the electrodes, and the device can retain its state until an appropriate voltage is applied to change the state. ReRAM consists of a Metal-Insulator-Metal (MIM) stack where the insulator is generally metal oxide. The device works on the principle of ion migration, where ions migrate through the insulator from one terminal to the other, forming a conductive filament when voltage is applied. ReRAM has two states – Low Resistance State (LRS) and High Resistance State (HRS). The conductive filament, formed by the migration of ions, provides a path for current to flow between the filaments, setting the device in the LRS. Switching from HRS to LRS is known as setting the device, and the voltage at which it occurs is known as set voltage. The device is reset when it switches from LRS to HRS; the applied voltage is known as reset voltage. When the magnitude of the applied voltage is greater than the magnitude of the reset voltage, the conductive filament is ruptured. When the magnitude of the applied voltage is less than the set or reset voltage, the device retains its state. The I-V graph of a typical ReRAM device is shown in Figure 1. The state of the device can be sensed by applying a read voltage less than the set/reset voltage and measuring the current.

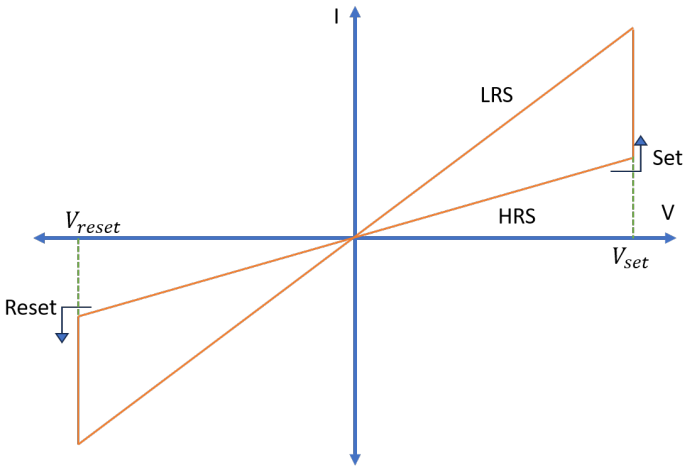


Figure 1: I-V Graph of a typical ReRAM

2.2. Stochasticity in ReRAM

ReRAMs suffer broadly from two types of stochasticity – Dynamic and Static. Dynamic stochasticity is observed during the switching of the states, and variability can be observed in switching voltages and the time required for the device to switch from one state to another [22]. The probability of switching is also random and follows a lognormal distribution [23]. The switching probability increases with an increase in programming amplitude and time for which the voltage pulse is applied. Static stochasticity is the variability in the final resistance value of the device in LRS and HRS. This variability closely follows a lognormal probability density function [24, 25, 26] and hence is modeled as such. The cycle-to-cycle variation in resistance values and switching probabilities is because the filament formation and rupture cannot be precisely controlled in every cycle. The filament's width and length vary from one cycle to another. This is more significant in HRS as the filament length, after breaking, can take up any value as long as it is disconnected from the terminal. This is observed in the device's resistance values, as the resistance variation is much more significant in HRS than in LRS [18]. The inherent dynamic and static stochasticity can be exploited to extract random numbers. The time or voltage required to switch is used in many proposed circuits, but as mentioned earlier, precise control of applied voltage and pulse timing is required, which makes the design complicated. Extracting random bits using static stochasticity is easier because the device is in a stable state, and as long as these states are reached, there is no need for precise control of the input signals. We exploit the significant variance in HRS resistance stochasticity in our proposed design.

3. Simulation

The working of the proposed design was verified by simulation, and further analysis of the variation of device parameters on the randomness of the output was also done. To simulate the ReRAM device, we used the Stanford-PKU RRAM Model [27]. The device is written in Verilog-A and modeled using an internal variable that corresponds to the length of the conductive filament in a device. While a device may have multiple filaments between the two terminals, the model uses a single filament, which acts as a cumulation of all the filaments. The increase in the internal variable corresponds to the growth of filament, and the decrease corresponds to decay. The change in the variable is dependent on the voltage across the terminal. To ensure that the device switches states, the set and reset voltages are set to 2 and -2 volts, respectively, greater than the set and reset voltage of the device, and the read voltage is set to 0.5 volts. The switching behavior of the model is shown in Figure 2.

The resistance of the device is dependent on the gap (g) between the end of the conductive filament and the terminal opposite to the temperature and is given by (1).

$$g = L - l \tag{1}$$

L is the device length, and l, the internal variable, is the length of the filament. If the read voltage is kept constant for the model, the device's resistance is exponentially proportional to g. In other words, the device's resistance in HRS increases exponentially with an increase in g, as shown in Figure 3. A random value of g is

picked from a normal distribution given by (2) to simulate the cycle-to-cycle variation in the device's resistance.

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\frac{x-\mu}{\sigma}^2} \tag{2}$$

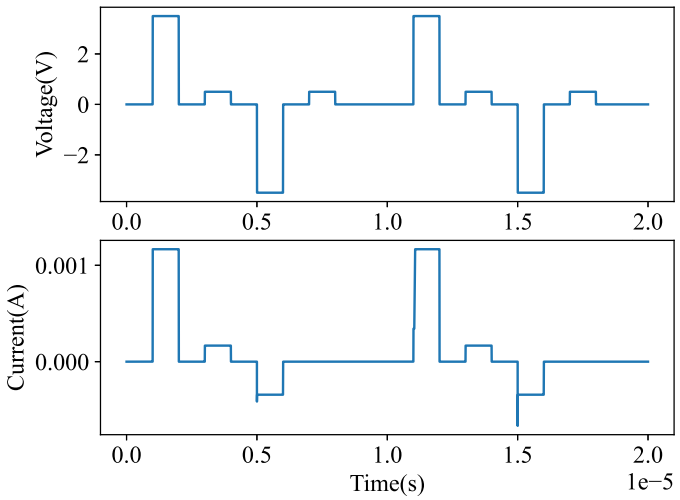


Figure 2: Switching of the states in Stanford-PKU RRAM Model.

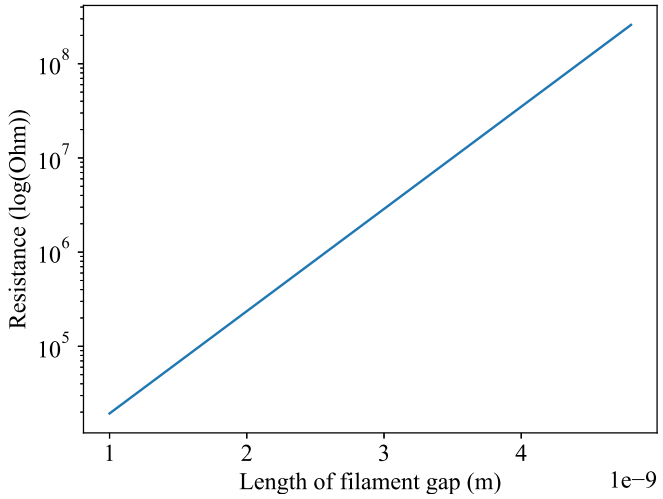


Figure 3: Relation between HRS resistance and g

μ is the mean of the distribution, and σ is the standard deviation. The variation of the random values can be changed by tweaking the values of μ and σ. For the initial simulations, μ was set to 3 nm, and σ was set to 0.1 nm. Since the device's resistance is exponentially related to g, it follows a log-normal distribution when g follows a normal distribution. The cycle-to-cycle variation of HRS for 10000 cycles is shown in Figure 4 and matches the trend followed by the device in [18]. To verify the proposed design, we have picked the same μ and σ for all the devices. The effect of different μ and σ on the output is studied in section 5.

The design requires other circuit components like switches, diodes, and a current direction sensor. We wrote Verilog-A codes for the ideal behavior of these circuits for simulation. The ideal components help us verify the working of our proposed design without affecting the working principle. The switches were modeled after transmission gates controlled by an external voltage source. The diodes have a forward bias voltage drop of 0.7 V. The current direction sensor is programmed to output 1 when the current is positive and 0 when the current is positive.

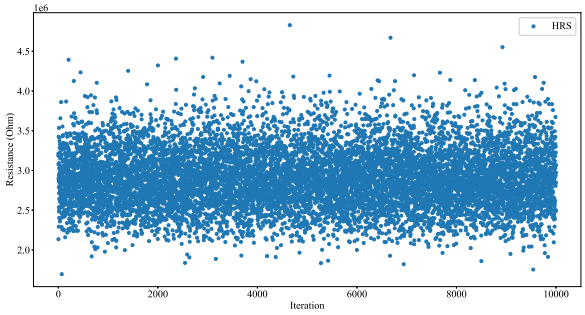


Figure 4: Distribution of HRS and LRS resistance for 10000 set-reset cycles

4. Design and Results

4.1. Working Principle

The working principle for the proposed design is based on the proposed circuit in [18]. In every cycle, two devices are set and then reset to HRS. The devices independently acquire a random resistance value from a log-normal distribution. The resistance values of these two devices are then compared, and the output bit is decided depending on which of the devices has greater resistance. The resistance value in HRS is used because the resistance variation is more significant than LRS.

4.2. Single Bit Design

Our primary aim was to propose a design compatible with a ReRAM crossbar. The proposed design, shown in Figure 5, utilizes a single column of the crossbar and generates one bit per cycle. The design uses two ReRAMs (M1, M2) as the source of randomness and one ReRAM (M3) for bit extraction (explained later). The design uses transmission gates (T1-T5), controlled by voltage sources (C1-C5), as switches. The transmission gates connect the devices to different voltage sources and ground. The design also uses current sensors that sense the current flow direction. The TRNG operation consists of the following steps:

1. One terminal of all three ReRAMs, M1, M2, and M3, is connected to the ground, and the devices are set into LRS by applying a set voltage of 2 V to the other terminal of the devices.

2. All three devices are disconnected from the ground. One of the terminals of M1 and M2 is connected to one of the terminals of M3. The other terminals of M1 and M2 are connected

to their respective voltage sources, and the other terminal of M3 is connected to the current sensor.

3. Read voltage of magnitude 500 mV, and opposite amplitude is applied to M1 and M2 through the voltage sources.

4. The voltage at the common terminal of M1 and M2 is given by the (3), where R1 and R2 is the resistance of M1 and M2 respectively.

$$V = V_{read}\frac{R_2 - R_1}{R_2 + R_1} \tag{3}$$

The voltage is positive and negative depending on the resistance values of M1 and M2, and so is the current direction through the current sensor, given by (4), where R3 is the resistance of M3.

$$I = \frac{1}{R_3}V_{read}\frac{R_2 - R_1}{R_2 + R_1} \tag{4}$$

The current is positive (negative) if the resistance of M1 is smaller (greater) than the resistance of M2.

5. The output bit is decided by the direction of the current sensed by the current sensor. The output bit is 1 if the current is positive and 0 if it is negative.

6. All the ReRAMs are again set to LRS for the next cycle.

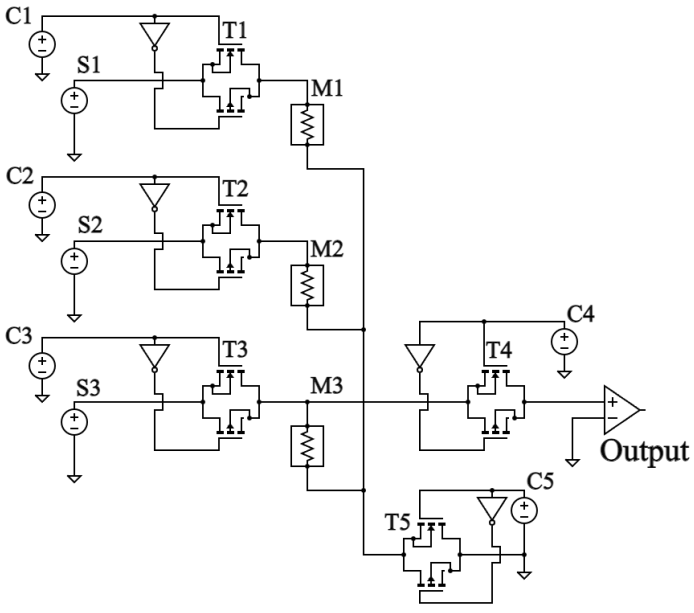


Figure 5: Proposed single-bit design which uses one column of a ReRAM crossbar

The working of the circuit can be seen in Figure 6. The gap, g, and hence the resistance of M1, is lower in cycle one and greater in cycle two than M2. The current through the current sensor is positive and negative in cycles 1 and 2, respectively, as predicted.

4.3. Multi-bit Design

The same principle can be extended to multiple columns in parallel to extract multiple bits in the same cycle. The bits can be read primarily in two ways. Read voltage can be applied multiple times while reading from different columns each time. Or, the bits can be read simultaneously. The second option will consume less time but require more hardware for parallel operation. For verification purposes, we read the output from each column one after the other by applying multiple read signals. The multi-bit design is implemented using a 2x3 ReRAM crossbar and one row of read ReRAMs, considered part of the peripheral circuit, as shown in Figure 7. The design produces three bits per cycle.

The main challenge with using multiple columns is the sneak path current from one column to another, affecting the output bits. We added diodes in the read row to prevent the sneak path current. The diodes prevent the flow in the reverse direction because it is in reverse bias, and since the forward bias voltage is less than the threshold voltage of the diode, no current flows in the forward direction as well. The set voltage applied to the read row is increased to ensure that all ReRAMS are set. The number of bits generated per cycle can be easily increased by increasing the number of columns. However, the number of columns will be limited by the maximum voltage that can be applied as the set voltage for the read row. Also, multiple applications of read voltages in a single cycle may affect the result of the later columns as the devices in these columns may change their state.

4.4. Results and Discussion

Determining the randomness of a sequence of numbers is a challenging task. Generally, a sequence must pass a set of statistical tests to be considered random. We use the NIST SP 800-22 [19] suite of statistical tests to test the sequence generated during the single-bit and multi-bit design simulations. The suite consists of various tests, and a p-value is calculated for each test. If the p-value exceeds 0.01, the sequence passes that particular test. 10,000 bits were generated; their test results are shown in table 1 for single-bit and multi-bit. The generated bit stream passed all the major tests.

The results show that our design can produce a sequence of random numbers. One point to note is the use of ideal switches, diodes, and current sensors for the simulation. We assume that replacing the ideal devices with practical ones will not affect the function of the circuit as long as we ensure that the ReRAMs switch their states, as the design only concerns the final state of the device. The practical devices will mainly affect the set and reset voltages to be applied. This also makes the design immune to variability in threshold voltage and switching time. This flexibility allows the circuit to work with any device as long as the device shows variation in one of the stable states.

The major benefit of the design is that it eliminates the need for additional circuitry to generate random bits. Whenever random bits are required, they can be generated in situ by dedicating some columns of a crossbar for generation. While designing a multi-bit circuit, the designer has the freedom to choose between the number of bits generated per cycle and time per cycle, depending on the constraints.

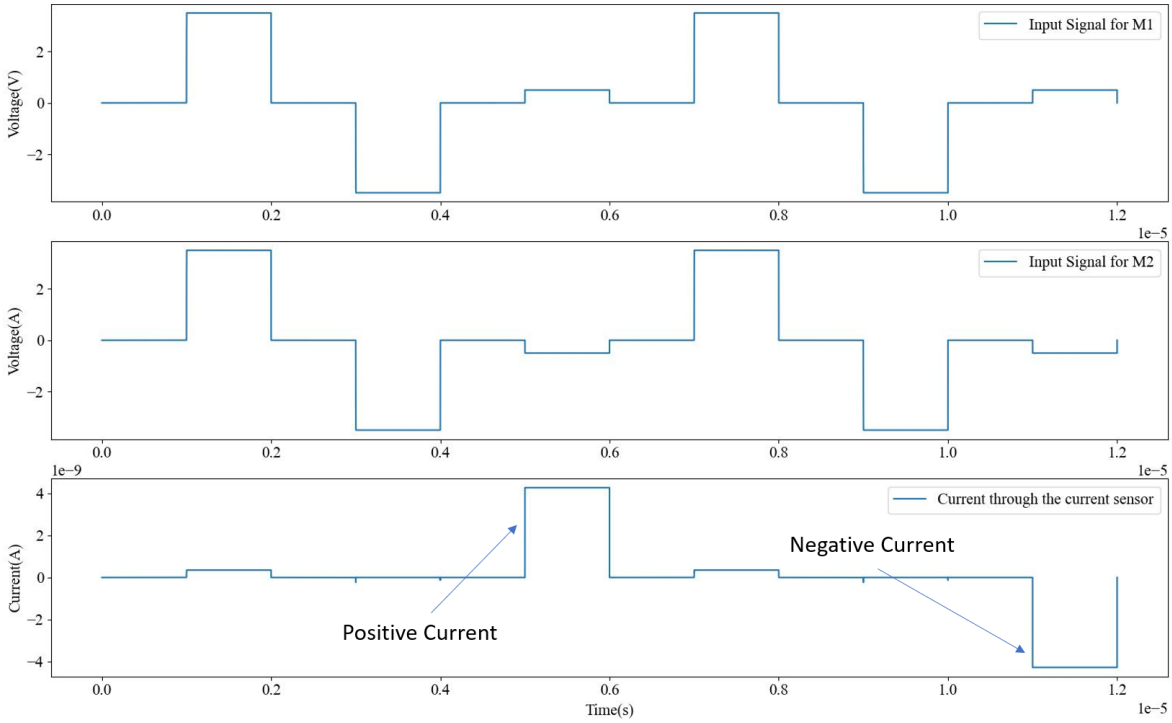


Figure 6: Working of the circuit.

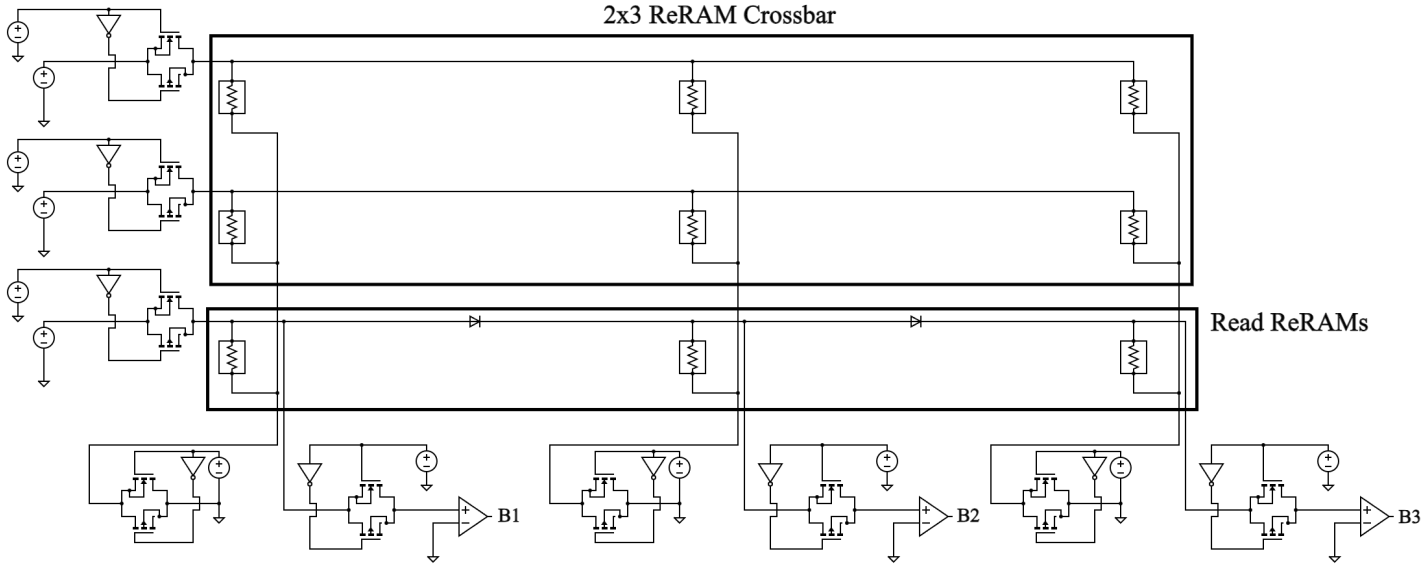


Figure 7: Proposed multi-bit design which uses a 2x3 ReRAM crossbar and a row of read ReRAMs.

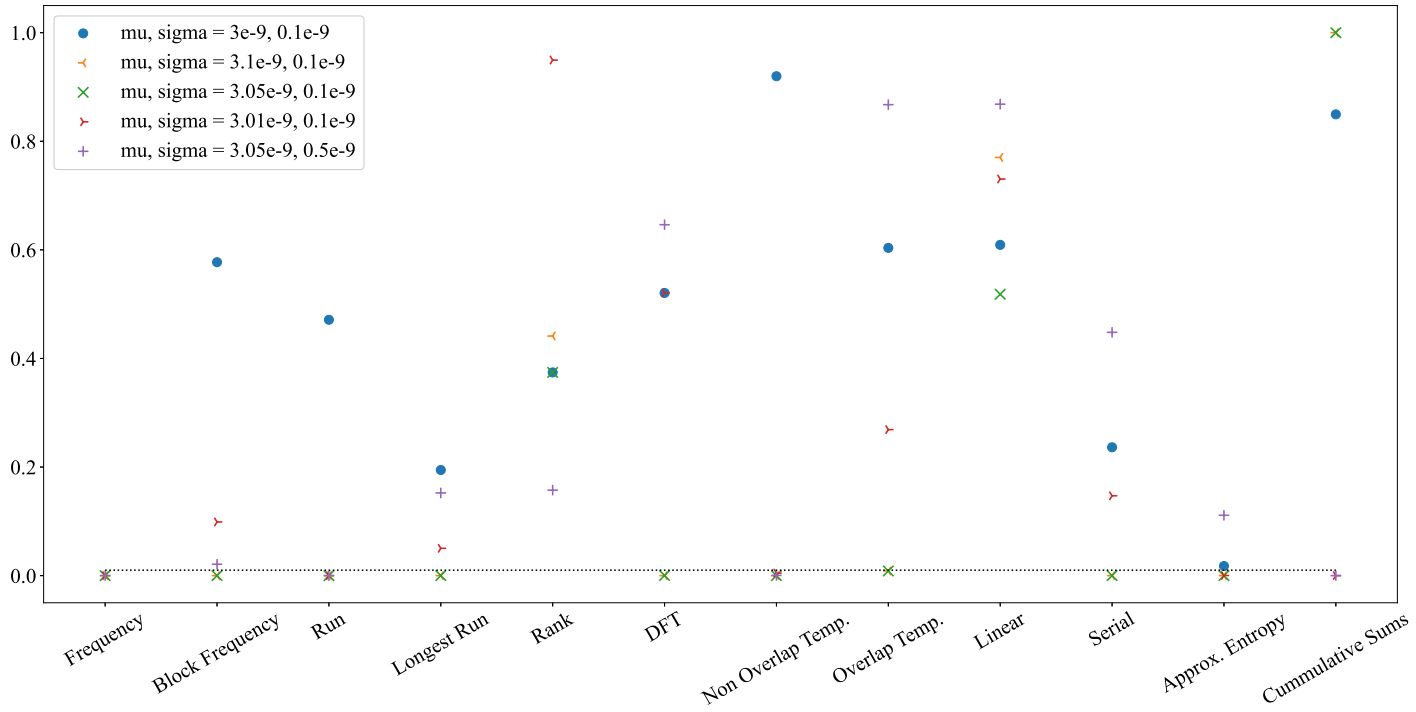


Figure 8: NIST Test Results for different values of μ and σ.

Table 1: NIST Test Result for Single and Multi Bit Circuit

Test	Single Bit		Multi Bit	
	p-value	***Result***	***p-value***	***Result***
Frequency	0.825	Random	0.355	Random
Block Freq.	0.577	Random	0.356	Random
Run	0.471	Random	0.591	Random
Long Run	0.194	Random	0.932	Random
Rank	0.374	Random	0.368	Random
DFT	0.520	Random	0.710	Random
Non-Overlap Temp.	0.919	Random	0.221	Random
Overlap Temp.	0.603	Random	0.932	Random
Linear	0.609	Random	0.147	Random
Serial	0.236	Random	0.368	Random
Approx. Entropy	0.0177	Random	0.586	Random
Cumm. Sum	0.849	Random	0.651	Random

5. Analysis of Statistical Variation

The output's randomness depends on the device properties' stochastic variation. The proposed design involves two devices simultaneously to extract the random bit. The statistical parameters for the random distribution, μ and sigma, were matched for the two devices to verify the working of the circuit. It is also essential to see the effect on the output's randomness if these values are mismatched for the two devices. This analysis is critical to understanding the limitations of the circuit design because of device-to-device variation during fabrication. Bits were extracted by changing the μ and σ of one of the devices, and the randomness of the bit stream was tested using the NIST test suit. The results of different tests are shown in Figure 8.

First, the effect of different mean distances (g) for the two devices was checked by increasing the μ for one device by 3.33%. As seen from the graph, the extracted bits fail to pass most of the tests. Even after decreasing the increase in μ to 1.67%, the bit stream does not pass most tests. Finally, when μ is increased by just 0.33%, the device's output passes most of the test. It can be concluded that the output is very sensitive to device mismatches. The circuit can only tolerate a very low difference in the mean of the gap before it starts generating a non-random output. Thus, very close attention must be paid to device mismatch while fabricating the circuit. An interesting observation is made when the σ of the distribution is also changed when changing μ. Increasing the σ by 400% when the μ of one of the devices is increased by 1.67%, results in the output passing more tests. Hence, a more significant cycle-to-cycle variation can tackle a greater device-to-device variation. While a greater variation is detrimental to most circuits, it benefits the proposed circuit.

6. Conclusion

The proposed TRNG uses inherent randomness in the resistance value of HRS to generate random bits. The design is entirely implementable in ReRAM crossbars. The resistance value of two ReRAMs in HRS in a crossbar is compared, and the output bit depends on their relative values. Circuits for generating both one and multi-bit per cycle are suggested. The circuits were simulated, and the generated bit stream passed almost all NIST randomness test suite tests. The design allows for choosing operating parameters without changing the hardware and will be compatible with various types of ReRAM. Significant device-to-device variability results in

the output bit stream being not random. The effect can be negated by a more significant cycle-to-cycle variation, which is unsuitable for other applications but positively impacts the random number generation application.

Future work will focus on implementing the design on actual hardware and validating the functioning of the design. It will be crucial to study whether the output is affected when the ideal devices are replaced with actual devices and, if so, how. The effect of adjacent columns on the output is also a potential scope of study.

References

[1] T. Patni, A. Pethe, "True Random Number Generator Implemented in ReRAM Crossbar Based on Static Stochasticity of ReRAMs," *2023 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, **7**:55–59, 2023, DOI: 10.1109/APCCAS60141.2023.00024

[2] P. L'Ecuyer, "Random numbers for simulation," *Commun. ACM*, **33**, 10:85–97, 1990, DOI: 10.1145/84537.84555

[3] A. J. Menezes, S. A. Vanstone, P. C. Van Oorschot, *Handbook of Applied Cryptography (1st. ed.)*, CRC Press, Inc., USA, 1996

[4] D. Eastlake, J. Schiller, S. Crocker, "RFC4086: Randomness Requirements for Security," *RFC*, 2005, https://tools.ietf.org/html/rfc4086

[5] Z. Gutterman, B. Pinkas, T. Reinman, "Open to Attack: Vulnerabilities of the Linux Random Number Generator," *Black Hat*, 2006, https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Gutterman.pdf

[6] J. Kelsey, B. Schneier, D. Wagner, C. Hall, "Cryptanalytic Attacks on Pseudorandom Number Generators," *Fast Software Encryption*, *FSE 1998*, *Lecture Notes in Computer Science*, **1372**:12, Springer, Berlin, Heidelberg, 1998, DOI: 10.1007/3-540-69710-1_12

[7] L. Gong, J. Zhang, H. Liu, L. Sang, Y. Wang, "True Random Number Generators Using Electrical Noise," *IEEE Access*, **7**:125796–125805, 2019, DOI: 10.1109/ACCESS.2019.2939027

[8] A. Vassilev, T. Hall, "The Importance of Entropy to Information Security" *Computer*, **47**, 02:78–81, 2014, DOI: 10.1109/MC.2014.47

[9] Z. Liu, D. Peng, "True random number generator in RFID systems against traceability," *CCNC 2006. 2006 3rd IEEE Consumer Communications and Networking Conference*, 620–624, 2006, DOI: 10.1109/CCNC.2006.1593098

[10] F. Pareschi, G. Setti, R. Rovatti, "Implementation and Testing of High-Speed CMOS True Random Number Generators Based on Chaotic Systems," *IEEE Transactions on Circuits and Systems I: Regular Papers*, **57**, 12:3124–3137, 2010, DOI: 10.1109/TCSI.2010.2052515

[11] M. Park, J. C. Rodgers, D. P. Lathrop, "True random number generation using CMOS Boolean chaotic oscillator," *Microelectronics Journal*, **46**, 12, Part A:1364–1370, 2015, DOI: 10.1016/j.mejo.2015.09.015

[12] N. Nguyen, G. Kaddoum, F. Pareschi, R. Rovatti, G. Setti, "A fully CMOS true random number generator based on hidden attractor hyperchaotic system," *Nonlinear Dyn*, **102**:2887–2904, 2020, DOI: 10.1007/s11071-020-06017-3

[13] F. Zahoor, T. Z. Azni Zulkifli, F. A. Khanday, "Resistive Random Access Memory (RRAM): an Overview of Materials, Switching Mechanism, Performance, Multilevel Cell (mlc) Storage, Modeling, and Applications," *Nanoscale Res Lett*, **15**:90, 2020, DOI: 10.1186/s11671-020-03299-9

[14] F. Zahoor, F. A. Hussin, U. B. Isyaku, S. Gupta, F. A. Khanday, A. Chattopadhyay, H. Abbas, "Resistive random access memory: introduction to device mechanism, materials and application to neuromorphic computing," *Discover Nano*, **18**:36, 2023, DOI: 10.1186/s11671-023-03775-y

[15] H. Jiang, D. Belkin, S. E. Savel'ev, S. Lin, Z. Wang, Y. Li, S. Joshi, R. Midya, C. Li, M. Rao, M. Barnell, Q. Wu, J. J. Yang, Q. Xia, "A novel true random number generator based on a stochastic diffusive memristor," *Nat Commun*, **8**:882, 2017, DOI: 10.1038/s41467-017-00869-x

[16] B. Yang, D. Arumí, S. Manich, Á. Gómez-Pau, R. Rodríguez-Montañés, M. B. González, F. Campabadal, L. Fang, "RRAM Random Number Generator Based on Train of Pulses," *Electronics*, **10**:1831, 2021, DOI: 10.3390/electronics10151831

[17] J. Postel-Pellerin, H. Bazzi, H. Aziza, P. Canet, M. Moreau, V. D. Marca, A. Harb, "True random number generation exploiting SET voltage variability in resistive RAM memory arrays," *2019 19th Non-Volatile Memory Technology Symposium (NVMTS)*, 1-5, 2019, doi: 10.1109/NVMTS47818.2019.9043369

[18] T. Zhang, M. Yin, C. Xu, X. Lu, X. Sun, Y. Yang, R. Huang, "High-speed true random number generation based on paired memristors for security electronics," *Nanotechnology*, **28**:455202, 2017, doi: 10.1088/1361-6528/aa8b3a

[19] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, S. Vo, "SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," *Technical Report*, National Institute of Standards & Technology, Gaithersburg, MD, USA, 2010

[20] L. O. Chua, S. M. Kang, "Memristive devices and systems," *Proceedings of the IEEE*, **64**, 2:209-223, 1976, doi: 10.1109/PROC.1976.10092

[21] T. Prodromakis, C. Toumazou, "A review on memristive devices and applications," *2010 17th IEEE International Conference on Electronics, Circuits and Systems*, 934-937, 2010, doi: 10.1109/ICECS.2010.5724666 10.1109/ICECS.2010.5724666

[22] R. Degraeve, A. Fantini, N. Raghavan, L. Goux, S. Clima, B. Govoreanu, A. Belmonte, D. Linten, M. Jurczak, "Causes and consequences of the stochastic aspect of filamentary RRAM," *Microelectronic Engineering*, **147**:171-175, 2015, 10.1016/j.mee.2015.04.025

[23] G. Medeiros-Ribeiro, F. Perner, R. Carter, H. Abdalla, M. D. Pickett, R. S. Williams, "Lognormal switching times for titanium dioxide bipolar memristors: origin and resolution," *Nanotechnology*, **22**, 9:095702, 2011, 10.1088/0957-4484/22/9/095702

[24] Y. Wang, W. Wen, H. Li, M. Hu, "A Novel True Random Number Generator Design Leveraging Emerging Memristor Technology," *Proceedings of the 25th edition on Great Lakes Symposium on VLSI (GLSVLSI '15)*, 271-276, 2015, 10.1145/2742060.2742088

[25] M. Hu, Y. Wang, Q. Qiu, Y. Chen, H. Li, "The stochastic modeling of TiO2 memristor and its usage in neuromorphic system design," *2014 19th Asia and South Pacific Design Automation Conference (ASP-DAC)*, 831-836, 2014, 10.1109/ASPDAC.2014.6742993

[26] S. Yu, B. Gao, Z. Fang, H. Yu, J. Kang, H. S. P. Wong, "Stochastic learning in oxide binary synaptic device for neuromorphic computing," *Frontiers in Neuroscience*, **7**, 2013, 10.3389/fnins.2013.00186

[27] H. Li, Z. Jiang, P. Huang, Y. Wu, H.-Y. Chen, B. Gao, X. Y. Liu, J. F. Kang, H.-S. P. Wong, "Variation-aware, reliability-emphasized design and optimization of RRAM using SPICE model," *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 1425-1430, 2015, 10.7873/DATE.2015.0362

ASTES

Advances in Science, Technology and Engineering Systems Journal
Vol. 10, No. 1, 37-47 (2025)
www.astesj.com
Special Issue on Innovation in Computing, Engineering Science & Technology

ASTES Journal
ISSN: 2415-6698

Hardware and Secure Implementation of Enhanced ZUC Steam Cipher Based on Chaotic Dynamic S-Box

Mahdi Madani*[,1], El-Bay Bourennane[1], Safwan El Assad[2]

[1]*Laboratoire ImViA (EA 7535) , Université Bourgogne Europe, 21000 Dijon, France*

[2]*IETR , University of Nantes/Polytech Nantes, France*

ARTICLE INFO

Article history:
Received: 14 October, 2024
Revised: 05 January, 2025
Accepted: 06 January, 2025
Online: 04 February, 2025

Keywords:
Dynamic S-box
FPGA design
Hardware metrics
ZUC stream cipher
Mobile security
Cryptography
Cryptanalysis

ABSTRACT

Despite the development of the Internet and wired networks such as fiber optics, mobile networks remain the most used thanks to the mobility they offer to the user. However, data protection in these networks is more complex because of the radio channels they use for transmission. Hence, there is a need to find more sophisticated data protection means to face any attack. But, this is not an easy task, especially with the emergence of AI-based attacks. In this context, we proposed in this work a solution that can significantly improve data protection in a new-generation mobile network. Therefore, the main objective of this study is to improve and implement an enhanced version of the standard ZUC algorithm designed by the Data Assurance and Communication Security Research Center of the Chinese Academy of Sciences and standardized by the 3GPP (3rd Generation Partnership Project) organization to ensure the LTE (Long Term Evolution of radio networks) security. The proposed design is principally based on replacing the static S-boxes of the original algorithm (S_0 and S_1) with a chaos-based dynamic S-boxes thus allowing to generate a different key-stream for any change on the secret key and with the best randomness and robustness properties. The two new dynamic S-boxes are initialized with 256 initialization values each (x"00"), then filled in parallel using two chaotic maps that use the ZUC algorithm registers, the CK (Cipher Key), and the IV (Initial Vector) to form two different initial values for each chaotic map. To reach the hardware performance, we implemented the system on a Xilinx XC7Z020 PYNQ-Z2 FPGA platform. The designed architecture occupies low logic resources (1135 Slice LUTs, 762 Slice Registers, and 8 DSP48E1) on the used FPGA device and can reach a throughput of 2515.84 Mbps with a running frequency of 78.62 Mhz by consuming only 0.188 W. To evaluate the resistance of the proposed cryptosystem, we used many security tests (keystream distribution, keystream randomness, key sensitivity, plaintext sensitivity, keyspace, and NIST statistical tests). The experimental results and comparison with other S-boxes based algorithms prove on one hand that using the dynamic S-box technique has enforced considerable data protection against cryptanalysis attacks, and on another that the hardware metrics (used logic resources, achieved throughput, and efficiency) are suitable for real-time applications such as mobile security transmission.

1. Introduction

Despite the development of high throughput Internet based fiber optics, mobile and connected objects networks remain the most used thanks to the mobility and ease they offer to the user. The main component they use is the smartphone which facilitates access to most of our daily services such as video calls, social network messaging, e-payment, smart-home, smart-city, etc.

However, data protection in these networks is more complex due to the physically unprotected radio channels they use for communications.

Hence, it is necessary to find more sophisticated means of data protection to deal with any attacker trying to illegally access data by going directly to the storage location (mainly servers or cloud) or by capturing encrypted data and trying to decrypt it by cracking the encryption algorithm used or looking for the secret key.

Therefore, protecting personal and sensitive information (naturally circulates on the physically unprotected radio transmission

*Corresponding Author: Mahdi Madani, Laboratoire ImViA, Université Bourgogne Europe, 21000 Dijon, France & Mahdi.Madani@u-bourgogne.fr

channel) is not an easy task, especially with the emergence of AI-based (Artificial Intelligence) attacks. This is why a cryptographic algorithm with the best robustness and resistance against computer attacks is needed to success this task. Since many decades, different cryptosystems have been designed as: block ciphers: DES (Data Encryption Standard), AES (Advanced Encryption Standard), KASUMI; stream ciphers: RC4 (Rivest Cipher 4), SNOW-3G, ZUC; hashing functions: DSA (Digital Signature Algorithm), Secure Hash Algorithms SHA-0, SHA-1, SHA-2, SHA-3; chaotic systems: Lorenz, Chen, logistic map, skew tent map, and other methods.

In this study, we evaluate the security performance of the ZUC stream cipher which is designed by the Data Assurance and Communication Security Research Center of the Chinese Academy of Sciences and standardized by the 3GPP (3rd Generation Partnership Project) organization to ensure the LTE (Long Term Evolution of radio networks) security. ZUC algorithm forms also the kernel of the confidentiality (128-EEA3) and integrity (128-EIA3) functions used in the LTE networks security [1, 2]. In addition, we propose an enhanced version that can significantly improve data protection in a new-generation of mobile network.

We started by analyzing the internal architecture of the original ZUC algorithm is based on three main layers, LFSR (Linear Feedback Shift Register), the BR (Bit Reorganization), and the NLF (Non Linear Function) [3]. The state of the art has proven that the ZUC architecture has certain weaknesses that require immediate improvements [4, 5, 6, 7, 8].

To remedy the identified problems, we improved the non linearity part of the standard algorithm by replacing its two static S-boxes (S_0 and S_1) with a chaos-based dynamic S-boxes [9, 10, 11, 12]. The new version allows the generation of different key-streams for any change on the secret key with the best randomness and robustness properties that increase the complexity of cryptanalysis attacks.

This paper is principally based on extending our work initially presented at the ICEET23 conference and improving the performance of the implemented architecture. Therefore, we can summarize the two main contributions of this extended version on: Firstly, we used a chaotic map to generate dynamically the internal two S-boxes (S_0 and S_1) of the ZUC algorithm. The experimental analysis show the respect of the generated S-boxes to the non-linearity recommendations. Secondly, we designed an optimized FPGA implementation with the best hardware metrics. A comparative study with the literature is given to confirm our results on the two listed steps. The proposed architecture consists of using two parallel chaotic maps to generate two dynamic S-boxes SD_0 and SD_1. They are dynamic because the chaotic maps are initialized using control parameters derived from the combination of the CK, the IV, and the internal registers (S_{15}, S_{14}, S_5, and S_7) of the LFSR layer. This technique ensures that any change (one bit is enough) in these three parameters will result in a different S-boxes. Many examples of generated S-boxes are examined using known theoretical tests for similar analysis, and the results are conclusive, unlike the original work which failed some tests.

To reach the hardware implementation, the proposed architecture is coded using a VHSIC Hardware Description Language (VHDL) and implemented on Field-Programmable Gate Array (FPGA) technology [13, 14] to explore its offered parallel calculations capabilities and the low power consumption.

The implementation on a Xilinx XC7Z020 PYNQ-Z2 FPGA hardware platform achieves a throughput of 767.52Mbps at an operating frequency of 94.34 Mhz. The robustness of the proposed architecture is evaluated using the keystream performance: analyzing the uniformity (histogram, chi square), randomness, key sensitivity, plaintext sensitivity, examining the key space complexity, and investigating the NIST (National Institute of Standards and Technology) statistical tests [15].

The experimental results prove on one hand that using the dynamic S-boxes technique has enforced considerable data protection against cryptanalysis attacks, and on another that the hardware metrics (used logic resources, achieved throughput, and efficiency) are suitable for real-time applications such as mobile security transmission.

The reminder of this paper is organized as follows. Section 2 summarize the internal architecture and the processing steps of the regular ZUC stream cipher in its two operating modes. Section 3 describes the proposed architecture including the chaos-based dynamic S-boxes designed to enhance the security and enforce the resistance of the standard algorithm face to attacks. Section 4 presents the FPGA implementation results in terms of the occupied hardware metrics (logic resources, FFs, BRAMs) and the achieved timing metrics (throughput, frequency, efficiency). It also shows the behavioral simulation results under Vivado tools to prove the best functionality of our design. Section 5 investigates cryptanalytic analysis and stream cipher performance allowing to prove the robustness of the proposed scheme. Finally, section 6 summarizes the whole article and gives directions for our perspectives in the future.

2. Original ZUC stream cipher overview

As we already discussed, ZUC algorithm is a word-oriented stream cipher designed by the Data Assurance and Communication Security Research Center of the Chinese Academy of Sciences and standardized by the 3GPP organization to ensure the LTE and 5G (the fifth generation of cellular network technology) security. In this section, we present briefly its internal architecture, its processing steps in the two operating modes, and some attacks from the literature that subjected the standardized version.

ZUC is a word-oriented algorithm that generates a 32-bits word key-stream under the control of a 128-bits CK and 128-bits IV [3, 16, 17]. Its internal architecture is formed by three main interacting layers corresponding to the LFSR, the BR, and the NLF layers, respectively. The LFSR layer is formed by 16 stages of 31-bits registers ($S_0, S_1, \ldots, S_{15}$). The BR layer is composed of 4 stages of 32-bits registers (X_0, X_1, X_2, X_3) filled from the LFSR layer ($S_{15}, S_{14}, S_{11}, S_9, S_7, S_5, S_2, S_0$). The NLF layer is made up of 2 S-boxes (S_O, S_1) and 2 intermediate 32-bits registers (R_1, R_2) sequentially updated based on the output of the BR layer.

The ZUC stream cipher runs in two operating modes to generate a valid output, initialization and key-stream, as described below.

- Initialization mode: consist of loading the control parameters (CK and IV) to initiate the internal states of the LFSR registers according to the following Formula.

$$\begin{cases} S_0 = CK(127:120)||1000100110101111||IV(127:120) \\ S_1 = CK(119:112)||0100110101111100||IV(119:112) \\ S_2 = CK(111:104)||1100010011010111||IV(111:104) \\ S_3 = CK(103:96)||0010011010111110||IV(103:96) \\ S_4 = CK(95:88)||1010111100010011||IV(95:88) \\ S_5 = CK(87:80)||0110101111000101||IV(87:80) \\ S_6 = CK(79:72)||1110001001101011||IV(79:72) \\ S_7 = CK(71:64)||0001001101011111||IV(71:64) \\ S_8 = CK(63:56)||1001101011110000||IV(63:56) \\ S_9 = CK(55:48)||0101111000100111||IV(55:48) \\ S_{10} = CK(47:40)||1101011110001001||IV(47:40) \\ S_{11} = CK(39:32)||0011010111100011||IV(39:32) \\ S_{12} = CK(31:24)||1011110001001101||IV(31:24) \\ S_{13} = CK(23:16)||0111100010011011||IV(23:16) \\ S_{14} = CK(15:8)||1111000100110101||IV(15:8) \\ S_{15} = CK(7:0)||1000111101011001||IV(7:0) \end{cases}$$

Then, combining the output of the NLF layer (W), a primitive polynomial over the Galois Gield $GF(2^{31}-1)$, and a modulo operations [3] to updates the register S_{15} according to Equation 1.

$$\begin{cases} u = W >> 1 \\ v = 2^{15}S_{15} + 2^{17}S_{13} + 2^{21}S_{10} + 2^{20}S_4 \\ \quad +(1+2^8)S_0 \ \ mod\ (2^{31}-1) \\ Fb = (v+u) \ \ mod\ (2^{31}-1) \end{cases} \quad (1)$$

In addition, the remainder registers are right shifted to update the LFSR layer, as follows.

$$\begin{cases} S_{15} = Fb \\ S_{14} = S_{15} \\ S_{13} = S_{14} \\ \cdots \\ S_0 = S_1 \end{cases}$$

This mode is executed for 32 clock cycles without generating output sequence Z, as illustrated in Figure 1.

- Key-stream mode: consist of using the outputs of the NLF (W) and the BR (X_3) layers to generate a 32-bits output key-stream word (Z) at each clock cycle according to Equation 2.

$$Z = W \oplus X_3 \quad (2)$$

The processing of this operating mode is illustrated in Figure 2.

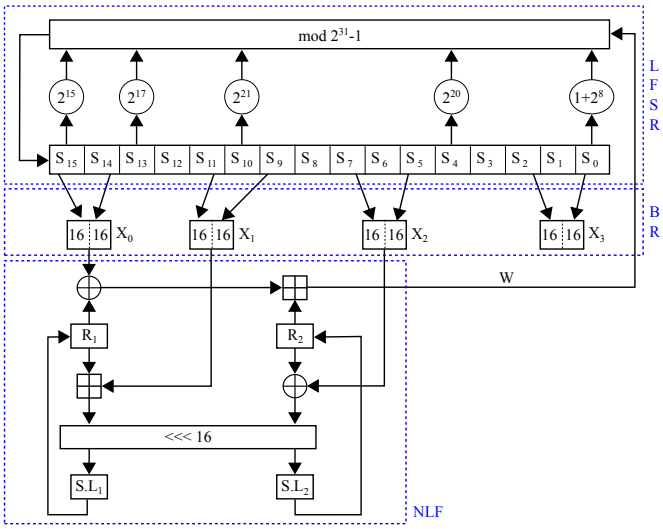


Figure 1: ZUC stream cipher initialization mode.

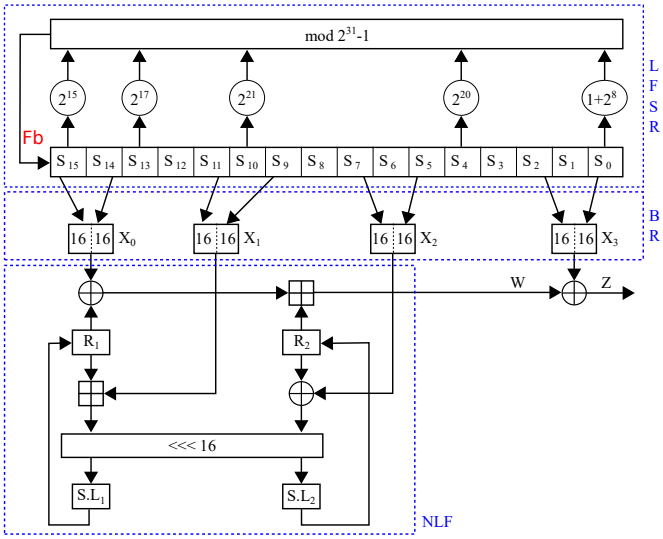


Figure 2: ZUC stream cipher key-stream mode.

Since its inception, the robustness of the ZUC stream cipher has been analyzed and the algorithm has suffered numerous attacks. In the literature several works have identified some drawbacks. Among them, we cite the alternative algebraic analysis [4], differential attacks[5], satisfiability solvers based analysis [6], and NIST statistical analysis [8, 7, 18, 19].

To overcome these weaknesses, we proposed a solution in this work based on enhancing the nonlinear part of the algorithm to resist cryptanalysis attacks. In the following sections, we will detail the technique used and give the results proving the improvement.

3. Proposed chaos-based architecture

In this section, we present the proposed architecture focused on improving security resistance against cryptographic attacks. The

adopted technique is based on the use of a chaos-based dynamic S-boxes by the NLF layer, unlike the original one using two static S-boxes S_0 and S_1.

3.1. Chaotic dynamic S-box implementation

S-boxes known as lookup tables are a non linear functions widely used by cryptographic algorithms. They are defined to ensure no repetition and to generate a non-linear output value [9, 10, 11]. However, if the CK used is cracked, the entire security of the algorithm will be compromised and the encrypted data will be exposed. To overcome this issue, we designed a dynamic chaotic S-box that ensures that even if the internal architecture of the algorithm and the CK are compromised, only modifying the CK will provide good data protection in the future. This will be guaranteed by the chaos map control parameters which change with every small modification in the CK and IV mobile client parameters ensuring a good confusion properties of the NLF layer and generating a random output key-stream.

Basically, ZUC stream cipher runs on two operating modes (initialization and key-stream modes) using two static S-boxes S_0 and S_1. However, the proposed design uses two chaos-based dynamic S-box.

We began initializing the internal LFSR, BR, and NLF layers, like the standard algorithm. The only difference is the replacement of the standard S-boxes (S_0 and S_1) by two new dynamic S-boxes (SD_0 and SD_1) of the same length (16×16) but with internal values initialized to zero at this step. In parallel, we set two logistic chaotic maps using different initial conditions extracted from the BR layer (driven from the control parameters CK and IV) according the Formulas 3 and 4.

$$DK_1 = X0(31\ downto\ 16) \parallel X2(15\ downto\ 0) \tag{3}$$

$$DK_2 = X0(15\ downto\ 0) \parallel X2(31\ downto\ 16) \tag{4}$$

Note that DK_0 and DK_1 form the dynamic keys of the chaotic system, $X0$ and $X2$ are registers from the BR layer, and $\parallel$ is the concatenation operator.

After initializing the chaotic system based on two Logistic maps (non-linear chaotic discrete function), it produces two 32-bits random sequences. The first sequence will be used to complete the dynamic S-box SD_0 and the second sequence to complete the S-box SD_1. The mathematical model of the discrete logistic map is defined by Equation 5.

$$X_{n+1} = \begin{cases} \dfrac{X_n \times (2^N - X_n)}{2^{N-2}} & if\ X_n \neq [3 \times 2^{N-2}, 2^N] \\ 2^N - 1 & if\ X_n = [3 \times 2^{N-2}, 2^N] \end{cases} \tag{5}$$

Where X_{n+1} is the new value calculated from the previous one X_n, N is the output size of the discrete logistic map (N=32-bit).

To fill one S-box, we run the chaotic system that generates 32-bit key-stream words at each clock cycle. We take 8-bits to fill one of the 256 available cells. To avoid repetition, we used a control vector of the same size ($16 \times 16 = 256$) based on a repetition flag set to zero. The principle consists of saving the value (x) on the S-box (at position [i, j], i, j = 0 to 15) and setting the corresponding flag to one (flag [x] = 1). This ensures that If the value is generated again during the filling process, it will be ignored. The block diagram of the algorithm is shown in Figure 3.

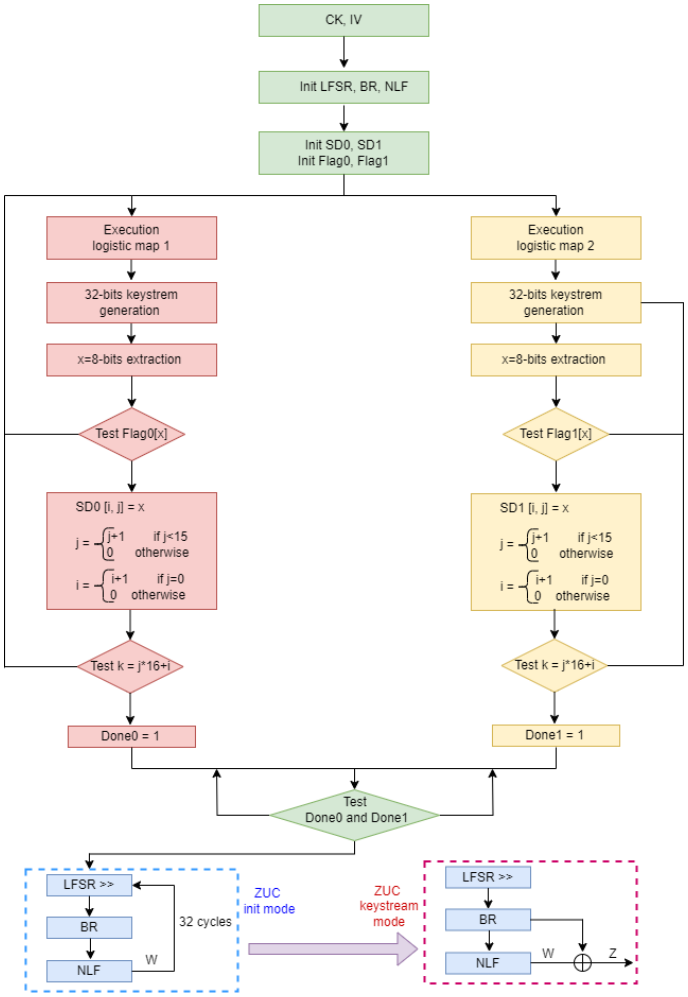


Figure 3: S-boxes generation procedure.

To complete the second S-box in parallel, we used the same principle. Initializing the chaotic maps with different keys ($DK_1 \neq DK_2$) guarantees the generation of two distinct S-boxes. This technique allows the completion of the two dynamic S-boxes without repetition by respecting the principle of creating lookup tables.

After completing both the S-boxes, the proposed ZUC stream cipher will be executed similarly to the original one, with 32 cycles running the initialization mode and then the key-stream mode for the remainder but using the proposed dynamic S-boxes, as explained above. For more clarity, we illustrate the architecture of the proposed design in Figure 4.

3.2. S-box analysis

The security of algorithms using on S-box is principally based on this non-linear component. Therefore, any weakness or problem in its construction will significantly affect the whole security of the algorithm and weaken its resistance to attacks such as linear and

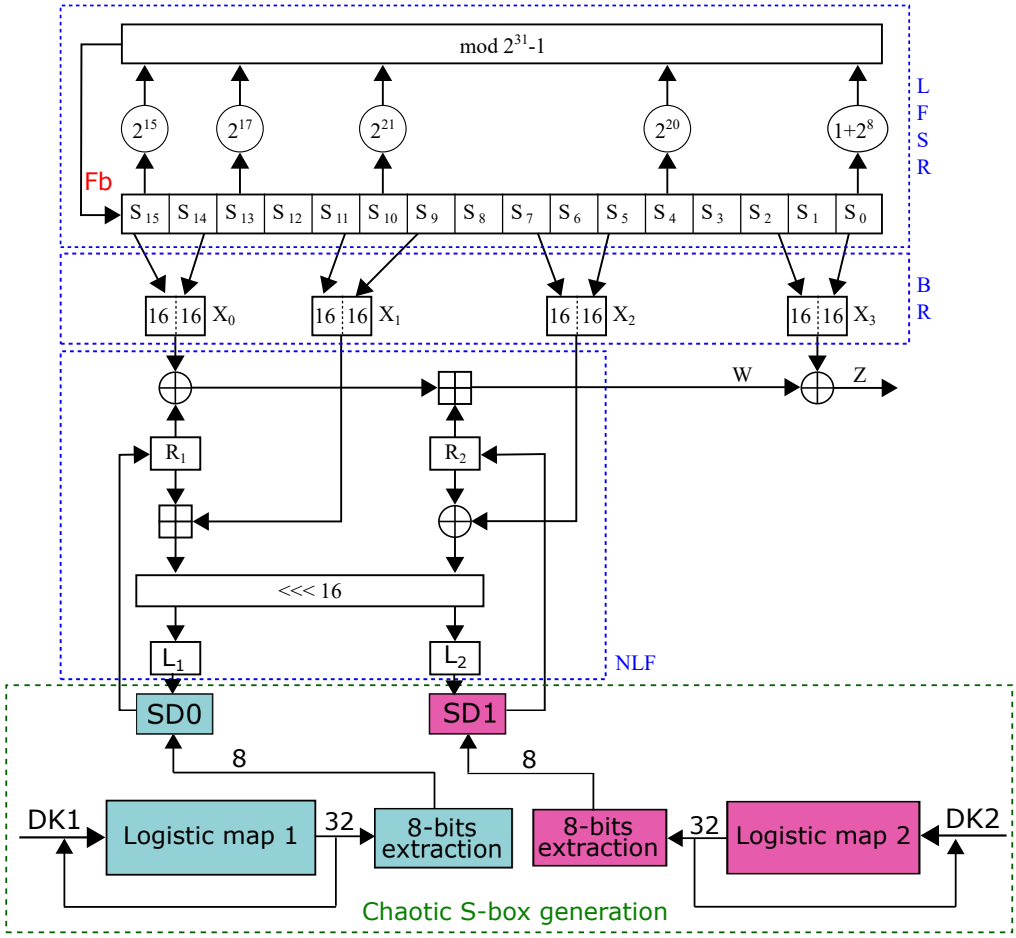


Figure 4: Proposed ZUC with dynamic S-boxes architecture.

differential cryptanalysis. For this, we evaluate the main performances of the proposed dynamic S-box to avoid any unpleasant surprises. To prove the expected high level S-box, we analyzed its satisfactory to the following criteria: bijection, strict avalanche criterion (SAC), non-linearity, output bits independence criterion (BIC), equiprobable input/output XOR distribution, differential approximation probability (DP), and maximum expected linear probability (LP).

To facilitate understanding the analysis, we present in Table 1 a example of a generated S-box using the proposed technique. So, the analysis study in this section will be based on this sample. In Table 2 we give a comparative study with the literature works based on the mentioned criteria.

3.2.1. Bijectivity and non-linearity

The bijective property of an $N \times N$ constructed S-box is respected if there is no repetition of its values in the interval $[0, 2^N - 1]$. Therefore, as we can see from Table 1, our S-box satisfy this criteria because all its values $[0, 255]$ are different.

According to the S-box non-linearity definition given by [23, 34], our S-box highly non-linear because the minimum non-linearity indicator of 100 when $n = 8$. It is better than all the results presented in Table 2.

3.2.2. SAC criterion

As defined by [35], the SAC criteria is satisfied if changing a single input bit will conduct to change a half of the output bits. To evaluate this parameter in our S-box we used the dependence matrix (see [23]). As we can see from Table 2, the mean (0.4976), value is closed to the optimal value (0.5) and the offset value (0.0156) is closed to zero confirming the satisfaction of the SAC criteria.

3.2.3. Output bits independence criterion

Similarly to SAC, the authors in [35] defined BIC indicating the pair-wise independent for a given vector and its corresponding avalanche (complementing 1 bit). Applying this test to our S-box, we obtained a minimum value of BIC non-linearity (100) and a maximum value of DP (7) ([23, 32]) indicating the satisfaction of the BIC criteria.

3.2.4. Equiprobable input/output XOR distribution

For the analyzed S-box, the high value from the maximum expected differential probability matrix is 12 indicating a few imbalance between the input and output XOR distribution on the S-box.

Table 1: A generated S-box using the proposed technique.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	57	97	54	116	40	213	98	165	231	50	7	73	37	47	46	216
1	19	136	238	83	71	207	84	95	48	86	100	225	151	162	255	240
2	112	24	27	128	67	227	94	169	13	79	138	203	201	233	214	142
3	150	107	117	120	102	194	206	32	145	247	215	5	224	96	23	141
4	51	16	146	186	241	236	1	110	68	44	121	108	133	235	55	64
5	184	223	125	183	26	153	137	56	171	119	135	88	167	33	242	17
6	70	82	15	191	62	244	45	114	105	25	91	219	161	217	18	3
7	188	124	232	66	199	87	36	198	239	34	185	52	60	9	182	22
8	89	139	21	11	101	77	190	63	179	200	144	29	75	58	10	69
9	28	38	156	178	148	158	218	130	211	209	74	14	123	115	189	80
A	249	93	140	61	35	134	131	4	49	174	76	143	250	42	204	92
B	85	163	221	254	234	196	175	237	129	181	164	39	173	222	170	251
C	65	157	126	245	106	78	210	172	147	31	6	127	230	160	180	30
D	220	195	109	2	253	176	104	53	226	205	192	111	248	118	193	8
E	243	177	20	229	122	90	41	168	99	149	81	59	113	154	228	208
F	252	197	212	152	159	0	155	43	187	12	246	72	202	103	166	132

Table 2: S-box evaluation results and comparison.

S-Box	Min. non-linearity	Mean SAC	SAC offset	BIC-SAC	Min. BIC non-linearity	Max. XOR	LP
Proposed SD	100	0.4976	0.0156	0.4997	100	12	0.0549
AES	112	0.5048	0.02637	0.5046	112	4	0.015625
Madani et al. [20]	-	0.4625	-	0.4969	51.1	-	-
Dridi et al. [21]	102	0.4948	-	0.4991	103.42	10	0.1094
Cavuşoğlu et al [22]	104	0.5039	0.03809	0.5058	98	10	0.0791
Dragan Lambić [23]	106	0.5034	0.02441	0.5014	100	10	0.070557
Alhadawi et al. [24]	106	0.4943	-	0.4982	104.35	10	0.1250
Lai et al. [25]	104	0.5014	-	0.5028	102.75	10	0.1250
Al Solami [26]	106	0.5017	-	0.5026	104	10	0.1094
Xuanping et al. [27]	-	0.4965	-	0.4965	109.36	-	-
Dragan Lambić [28]	108	-	0.02954	-	104	8	0.035156
Liu et al. [29]	104	-	0.03027	-	98	10	0.0625
Guesmi et al. [30]	104	-	0.0293	-	96	10	0.0625
Fatih et al. [31]	100	-	0.03125	-	100	10	0.070557
Guo Chen [32]	102	-	0.03174	-	100	10	0.088135
Lambić et al. [33]	106	-	0.03	-	100	10	0.079

3.2.5. LP property

The LP criteria, as defined in [23, 36, 37] detect any imbalance between the selected input and output bits using two masks a and b. The obtained result after analyzing our S-box is equal to 0.0549 satisfying the requirement ($LP < 0.079$) given in [33].

3.2.6. Discussion

As it is discussed in the previous paragraphs, and presented in Table 2, we can conclude that the proposed technique is suitable for the construction of strong random S-boxes while it satisfies the requirements and offers best results compared the literature similar works.

4. Hardware requirements of proposed architecture

To explore the material performance of the proposed architecture, we used the structural description on VHDL language for low level implementation. The Register-Transfer-Level (RTL) description has been realized on the Xilinx PYNQ-Z2 FPGA prototyping board after synthesis, place and route steps on the the Xilinx Vivado design suite tools (V.2022.1) [13]. To ensure the best functionality of our design, we performed simulation tests at the different levels of design flow, behavioral, post-synthesis functional, post-synthesis timing, post-implementation functional, and post-implementation timing. After the success of these simulations we generated the bit-file and we programmed the FPGA chip.

4.1. Utilization, timing, and power reports analysis

The main information given on the report-utilization generated by the Xilinx Synthesis Technology (XST) after place and route, the timing metrics, and power requirements are presented in Table 3. As we can see, the designed architecture occupies low logic resources on the used Xilinx PYNQ-Z2 xc7z020clg400-1 FPGA device. More precisely, it requires only 1135 (2.13%) Slice LUTs (743 LUT as Logic and 392 LUT as Distributed RAM), 762 (0.72 %) Slice Registers (Register as Flip Flop), and 8 (3.64 %) DSP48E1. The mean of these tree main parameters (2.16 %) show that the available resources are used efficiently. In terms of timing metrics, the design can reach running frequency of 78.62 Mhz according to Equation 6. Where T = 13 ns and WNS = 0.28 ns (Worst Negative Slack, defined in Vivado implementation report. It gives the worst slack of all the timing paths. It is negative if a timing violation is detected in any path and positive, like our study, if all the paths satisfies the timing requirement). Therefore, the 32-bits stream-cipher generation can reach a throughput of 2515.84 Mbps according to Equation 7. If we consider that the architecture will be executed uniformly on the used logic Slices, we define the efficiency parameter according to Equation 8.

$$Max\_Freq = \frac{1}{T - WNS}\ [MHz] \tag{6}$$

$$Throughput = N \times Max\_Freq\ [Mbps] \tag{7}$$

$$Efficiency = \frac{Throughput}{Slices}\ [Mbps/Slices] \tag{8}$$

The power report indicates a total On-Chip consumption of 0.188 W (43 % dynamic and 57 % static). Therefore, in addition to hardware and timing metrics, this low energy requirement of the architecture favorite its utilization on embedded electronic and real-time data protection applications, like smartphone and IoT (Internet of Think) objects or devices.

5. Security evaluation and discussion

To evaluate the security performance of the proposed dynamic S-box-based ZUC stream cipher, we investigated its resilience against cryptanalysis attacks using the most useful tests known for their effectiveness in validating cryptosystems such as NIST statistical tests, keystream uniformity, keystream randomness, entropy, confusion, and diffusion properties, key sensitivity, and key space.

All the simulations have been implemented in Python 3.7 on a standard computer Intel(R) Core(TM) i7-10710U CPU 1.10 GHz operating under Microsoft Windows 10, 64-bit, 16 GB RAM, and 1.6 GHz cpu-speed.

5.1. Uniformity and key-stream distribution analysis

To evaluate the uniformity of a key-stream generated by the proposed algorithm, we encrypted different images (Figures 5(a), 5(b), 5(c), 5(d), 5(e)) of size 512 × 512 pixels using 2097152 generated bits. Then, we expected the histogram distribution of both the plain and encrypted images in each case. As we can notice in Figure 6 (row 2), the encrypted images are uniformly distributed and spatially spread. Unlike plain images following a distribution concentrated on a defined area of pixels, but not on others (see Figure 5, row 2). Therefore, we conclude that the proposed dynamic S-boxes improves the randomness of the generated output key-stream and ciphered data.

5.2. Uniformity and Chi-Square analysis

To confirm statistically the uniformity accurately of the generated key-stream and cipher-text, we explored the Chi-Square value [38] using Equation 9.

$$\chi_{exp}{}^2 = \sum_{i=1}^{N_c-1} \frac{(O_i - E_i)^2}{E_i} \tag{9}$$

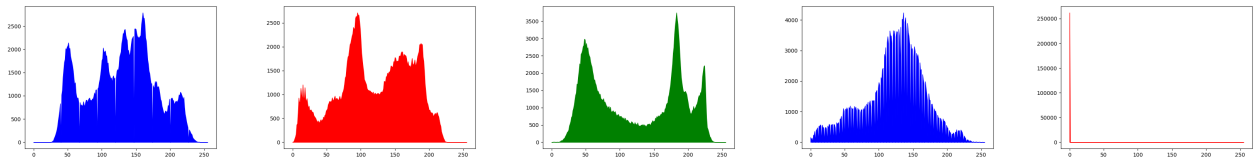
Where $N_c = 2^8 = 256$ is the number of levels, O_i is the calculated occurrence frequency of each gray level, $i \in [0, 255]$ in the histogram of the ciphered image, and E_i is the expected occurrence frequency of the uniform distribution, calculated by $E_i = nb/N_c$. The theoretical value for $\alpha = 0.05$ and $N_c = 256$ is $\chi^2_{th}(255, 0.05) = 293.24$.

The mean value of the experimental Chi-square χ^2_{exp} over 20 cipher images is equal to $\chi^2_{exp} = 263.73$. The obtained value is consistent with the expectations of the definition for this test which considers a uniform cipher-text if the experimental value of its Chi-square is less than the theoretical value, as our case ($\chi^2_{exp} = 263.73 < \chi^2_{th} = 293.24$). According to this analysis, we conclude that the uniformity is confirmed by both the histogram distribution and Chi-square value.

Table 3: FPGA implementation results of the proposed dynamic-Sboxes-based ZUC stream cipher.

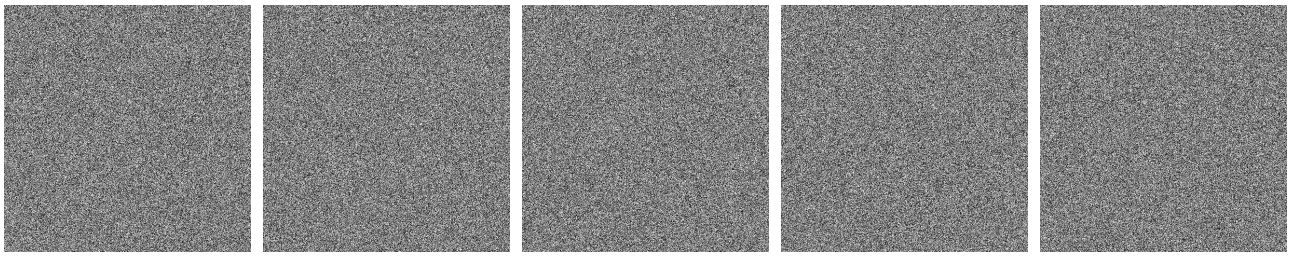
	Parameters	Area Utilization	Area Utilization in %
Board	Family Device	Zynq-7000 7z020-clg400	
Hardware resources	Slice LUTs FFs DSP	374 1135 762 8	(2.81 %) (2.13 %) (0.72 %) (3.64 %)
Time metrics	WNS (ns) Maximum Frequency (MHz) Throughput (Mbps)	0.29 78.68 2515.84	
Efficiency	Efficiency (Mbps/Slices)	6.73	
Consumption	Power (Watts)	0.188	

(a) Lena. (b) Peppers. (c) Lake. (d) Couple. (e) Black.

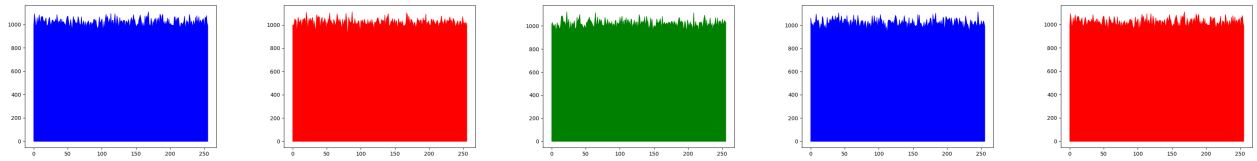


(f) Lena ditribution. (g) Peppers ditribution. (h) Lake ditribution. (i) Couple ditribution. (j) Black ditribution.

Figure 5: Plain images and their distributions.



(a) Lena encrypted. (b) Peppers encrypted. (c) Lake encrypted. (d) Couple encrypted. (e) Black encrypted.



(f) Lena encrypted ditribution. (g) Peppers encrypted ditribution. (h) Lake encrypted ditribution. (i) Couple encrypted ditribution. (j) Black encrypted ditribution.

Figure 6: Encrypted images and their distributions.

5.3. Hamming distance and plain-text sensitivity analysis

To test, the sensitivity to any change on the plain-text, we calculate the average Hamming Distance (HD) between the plain-image (P) and the corresponding cipher-image (C), as given by Equation 10 over 20 different plain images.

$$HD(P,C) = \frac{1}{|N|}\sum_{k=1}^{N}(P[k] \oplus C[k]) \times 100\% \quad (10)$$

Where N is the size in bit of the plain and cipher images.

The obtained results presented in Figure 7 are very close to the optimal value 50%, as defined by the avalanche effect [39] indicating that the probability of bit changes between each ciphered-text and its corresponding plain-text is 50%.

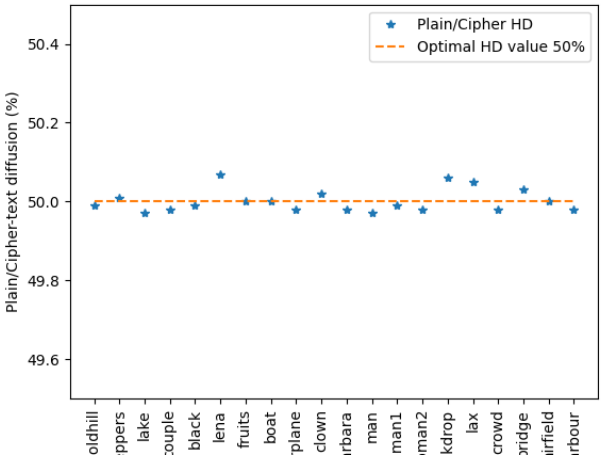


Figure 7: The plain-text sensitivity HD results.

5.4. Hamming distance and secret key sensitivity analysis

Similarly to the previous test, we evaluated the sensitivity to few change on the secret key. The test was performed by ciphering the same plain-image twice using two keys with only one bit of difference to obtain two ciphered-images C_1 and C_2. Then we calculate the HD between C_1 and C_2 using Equation 11 over 100 different secret keys.

$$HD(C_1,C_2) = \frac{1}{|N|}\sum_{k=1}^{N}(C_1[k] \oplus C_2[k]) \times 100\% \quad (11)$$

The obtained results presented in Figure 8 are also very close to the optimal value 50% indicating that a change of only one bit in the secret key leads to a thoroughly different key-stream. This proves the high sensitivity of the proposed ZUC stream to the secret key as defined by the avalanche effect [40] with respect to the confusion property given by Shannon's theory [41, 42]. This means that the complex statistical relationship between the secret key, the plain image, and the encrypted image makes it difficult to recover the secret key even with knowledge of multiple plain-encrypted image pairs.

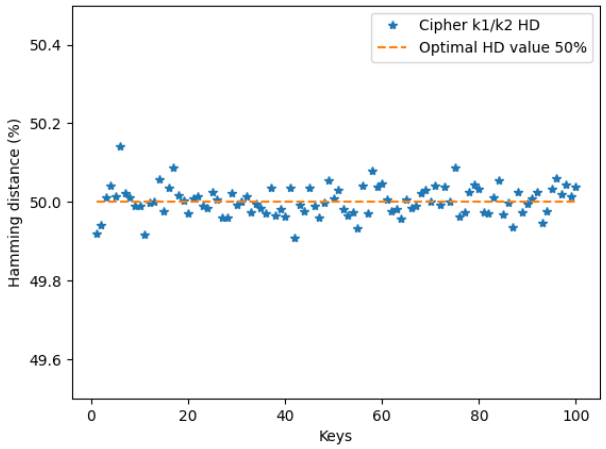


Figure 8: The key sensitivity HD results.

5.5. Key space analysis

The key space of the enhanced ZUC design is improved from 2^{128} to 2^{256} thanks to the use of two dynamic keys to run the chaotic maps and generate the new S-boxes (SD_0 and SD_1). The principle was the combination use of both 128-bits CK and IV to generate the keys KD_1 and KD_2. Therefore, any change in the value of CK or IV leads to the generation of a new S-boxes and a new key-stream, which makes brute-force attacks infeasible.

5.6. NIST statistical tests analysis

For a thorough analysis of the properties of the generated keystream, we used the NIST battery of statistical tests [8, 7, 15, 18, 19]. To explore the fifteenth test, we analyzed a set of 100 generated sequences given by the proposed algorithm. In all the experiments, we set the significance level to 0.01. From the obtained results shown in Table 4, we remark that the proposed ZUC design passes in success all the NIST tests, which prove the high robustness and the best statistical properties of our architecture allowing us to ensure a high-level protection of digital data (text, image, etc.).

5.7. Discussion

As we presented in the above subsections, all the applied experimental results prove the best performance and the enhancement of the generated key-stream. Starting by the uniformity proved by the histogram distribution and the Chi-square value. Then, the sensitivity to any changes in both the plain-text and the secret key proved with respect to the avalanche effect [40] and Shannon's theory [41]. After that, the randomness and the statistical properties proved by the NIST tests. And finally, the complexity of secret key cracking has been doubled by improving the key space from 2^{128} to 2^{256}. Additionally, the high level of the proposed dynamic S-box

Table 4: NIST test results.

Number of test	Type of test	P-Value	Result
1	Frequency (mono-bit) Test	0.437749	success
2	Frequency Test within a Block	0.407566	success
3	Runs Test	0.942123	success
4	Tests for the longest-Run-of-ones in a Block	0.349813	success
5	Binary Matrix Rank Test	0.730751	success
6	Discrete Fourier Transform (Spectral) Test	0.076546	success
7	Non-overlapping Template Matching Test	0.574824	success
8	Overlapping Template Matching Test	0.884123	success
9	Maurer's "Universal Statistical" Test	0.238481	success
10	Linear Complexity Test	0.523428	success
11	Serial Test	0.945384	success
12	Approximate Entropy Test	0.583708	success
13	Cumulative sums Test	0.811180	success
14	Random excursion Test	0.711607	success
15	Random excursion variant Test	0.551820	success

as proved by the main useful criteria (bijection, SAC, non-linearity, BIC, equiprobable input/output XOR distribution, differential approximation probability, maximum expected linear probability) and by the comparison with the literature similar works enforce the whole security of the cryptosystem based on this strong S-box. This means that we have strengthened the resistance of the ZUC stream cipher against cryptanalysis attacks such as brute force attacks, statistical attacks, linear attacks, and differential attacks.

Consequently, we conclude that the combination of the ZUC stream cipher with the proposed dynamic chaotic S-boxes layer increases the data protection for LTE and the new generation of mobile networks.

6. Conclusion

In this article, we have improved the internal architecture of the standardized ZUC stream cipher by combining the original design with a chaos-based generator responsible for generating two dynamic S-boxes (SD_0 and SD_1) in place of the basic static S-boxes (S_0 and S_1). Then, we performed its FPGA-based (Xilinx XC7Z020 ZYNQ platform) implementation using a VHDL description structural language to reach the high performance metrics in terms of material logic resources (Slice LUT, Slice FF, and DSP), and timing requirements (Maximum frequency, WNS, and Throughput). We have also presented the security robustness of the enhanced algorithm as any new proposed cryptosystem.

By analyzing the results obtained, we conclude that the proposed design is adapted to real-time data transmission while achieving a high throughput. In addition, it is suitable for embedded applications while occupying a low area and consuming low energy. Finally, it can ensure a secured transmission of digital data in mobile and IoT networks (it guarantees confidentiality and integrity protections) while resisting brute force, statistical, and differential attacks without modification to the standardized requirements.

In our future work, we will explore how to lighten the computations of the NLF layer while keeping the same level of security. We will also aim to improve the temporal performance to achieve an encryption throughput as close as possible to the order of Gbps.

Conflict of Interest The authors declare no conflict of interest.

Acknowledgment This work was supported by the Bourgogne Franche-Comte region as part of the ANER number 2024PRE00022 project entitled CIAPD.

References

[1] "Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications," Technical specification (TS) TS 35.221 V12.0.0, 3GPP, 2014-09.

[2] "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security Architecture," Technical Specification (TS) ETSI TS 133 401 V11.5.0, 3GPP, 2012-10.

[3] "Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 2: ZUC specification," Technical specification (TS) TS 35.222 V12.0.0, 3GPP, 2014-09.

[4] M. J. AlMashrafi, "A different algebraic analysis of the ZUC stream cipher," in Proceedings of the 4th international conference on Security of Information and Networks (SIN), 139–153, ACM New York, NY, USA ©2011, Sydney, Australia, 2011, doi:10.1145/2070425.2070455.

[5] W. Hongjun, H. Tao, H. Phuong, W. Huaxiong, L. San, "Differential Attacks against Stream Cipher ZUC," in International Conference on the Theory and Application of Cryptology and Information Security, 262–277, ASIACRYPT 2012: Advances in Cryptology, 2012, doi:10.1007/978-3-642-34961-4 17.

[6] F. Lafitte, O. Markowitch, D. Van Heule, "SAT based analysis of LTE stream cipher ZUC," Journal of Information Security and Applications, **22**, 54–65, 2013, doi:10.1016/j.jisa.2014.09.004.

[7] M. Madani, I. Benkhaddra, C. Tanougast, S. Chitroub, L. Sieler, "Enhanced ZUC Stream Cipher Based on a Hyperchaotic Controller System," in The Euromicro Conference on Digital System Design DSD 2017, Work In Progress Session, Vienna, Austria, 30 August-1 September 2017.

[8] M. Madani, C. Tanougast, "Combined and Robust SNOW-ZUC Algorithm Based on Chaotic System," in The International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2018), 1168–1173, IEEE, Glasgow, Scotland, UK, 2018.

[9] F. Özkaynak, "Construction of robust substitution boxes based on chaotic systems," Neural Computing and Applications, **31**, 3317–3326, 2019, doi:10.1007/s00521-017-3287-y.

[10] F. Artuğer, F. Özkaynak, "A method for generation of substitution box based on random selection," Egyptian Informatics Journal, **23**(1), 127–135, 2022, doi:10.1016/j.eij.2021.08.002.

[11] K. Mohamed, M. N. Mohammed Pauzi, F. H. Hj Mohd Ali, S. Ariffin, N. H. Nik Zulkipli, "Study of S-box properties in block cipher," in 2014 International Conference on Computer, Communications, and Control Technology (I4CT), 362–366, 2014, doi:10.1109/I4CT.2014.6914206.

[12] A. Msolli, I. Hagui, A. Helali, "Dynamic S-boxes generation for IoT security enhancement: A genetic algorithm approach," Ain Shams Engineering Journal, **15**(11), 103049, 2024, doi:10.1016/j.asej.2024.103049.

[13] "Zynq-7000 SoC Technical Reference Manual," Ug585 (v1.13), Xilinx, 2021.

[14] "PYNQ Z2 Reference Manual," v1. 1, PYNQ™, 2019.

[15] A. Rukhin, et al, "A Statistical Test Suite for the Random and Pseudorandom Number Generators for Cryptographic Applications," NIST Special Publication 800-22, 2001, Revised: April 2010, doi:http://csrc.nist.gov/rng/SP800-22b.pdf.

[16] "Cid C, Murphy S, Pipir F, Dodd M, ZUC algorithm evaluation repport," Technical report, 2010.

[17] "Knudson LR, Preneel B, Rijman V, Evaluation of ZUC," Technical report, 2010.

[18] M. Madani, I. Benkhaddra, C. Tanougast, S. Chitroub, L. Sieler, "FPGA Implementation of an enhanced SNOW-3G Stream Cipher based on a Hyper-chaotic System," in The 4th international conference on Control, Decision and Information Technologies (CoDIT'17), 1168–1173, IEEE, Barcelona, Spain, 2017.

[19] M. Madani, I. Benkhaddra, C. Tanougast, S. Chitroub, L. Sieler, "Digital Implementation of an Improved LTE Stream Cipher SNOW-3G based on Hyperchaotic PRNG," Security and Communication Networks, Hindawi with John Wiley & Sons, **2017**, 15 pages, 2017, doi:10.1155/2017/5746976.

[20] M. Madani, S. El Assad, C. Tanougast, M. J. Vella, E.-B. Bourennane, O. Deforges, "FPGA-Based Implementation of Enhanced ZUC Stream Cipher Based on Dynamic S-Box," in 2023 International Conference on Engineering and Emerging Technologies (ICEET), 1–6, 2023, doi:10.1109/ICEET60227.2023.10526075.

[21] F. Dridi, S. El Assad, W. El Hadj Youssef, M. Machhout, R. Lozi, "Design, Implementation, and Analysis of a Block Cipher Based on a Secure Chaotic Generator," Applied Sciences, **12**(19), 2022, doi:10.3390/app12199952.

[22] Ü. Cavusoğlu, A. Zengin, I. Pehlivan, S. Kacar, "A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system," Nonlinear Dynamics, **87**(2), 1081–1094, 2017, doi:10.1007/s11071-016-3099-0.

[23] D. Lambić, "A novel method of S-box design based on discrete chaotic map," Nonlinear Dynamics, **87**, 2017, doi:10.1007/s11071-016-3199-x.

[24] H. Alhadawi, M. Zolkipli, M. Ahmad, "A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map," Neural Computing and Applications, **31**, 2019, doi:10.1007/s00521-018-3557-3.

[25] Q. Lai, A. Akgul, C. Li, G. Xu, Ü. Çavusoğlu, "A New Chaotic System with Multiple Attractors: Dynamic Analysis, Circuit Realization and S-Box Design," Entropy, **20**(1), 2018, doi:10.3390/e20010012.

[26] E. Al Solami, M. Ahmad, C. Volos, M. N. Doja, M. M. S. Beg, "A New Hyperchaotic System-Based Design for Efficient Bijective Substitution-Boxes," Entropy, **20**(7), 2018, doi:10.3390/e20070525.

[27] Z. Xuanping, Z. Zhongmeng, W. Jiayin, "Chaotic image encryption based on circular substitution box and key stream buffer," Signal Processing: Image Communication, **29**(8), 902–913, 2014, doi:10.1016/j.image.2014.06.012.

[28] L. Dragan, "A novel method of S-box design based on chaotic map and composition method," Chaos, Solitons & Fractals, **58**, 16–21, 2014, doi:10.1016/j.chaos.2013.11.001.

[29] G. Liu, W. Yang, W. Liu, Y. Dai, "Designing S-boxes based on 3-D four-wing autonomous chaotic system," Nonlinear Dynamics, **82**, 2015, doi:10.1007/s11071-015-2283-y.

[30] R. Guesmi, M. A. Ben Farah, A. Kachouri, M. Samet, "A novel design of Chaos based S-Boxes using genetic algorithm techniques," in 2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA), 678–684, 2014, doi:10.1109/AICCSA.2014.7073265.

[31] F. Özkaynak, A. B. Özer, "A method for designing strong S-Boxes based on chaotic Lorenz system," Physics Letters A, **374**(36), 3733–3738, 2010, doi:10.1016/j.physleta.2010.07.019.

[32] G. Chen, "A novel heuristic method for obtaining S-boxes," Chaos, Solitons & Fractals, **36**(4), 1028–1036, 2008, doi:10.1016/j.chaos.2006.08.003.

[33] M. Š. Dragan Lambić, Publications de l'Institut Mathématique, (113), 109–115.

[34] T. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications: Second edition, 2017.

[35] A. F. Webster, S. E. Tavares, "On the Design of S-Boxes," in H. C. Williams, editor, Advances in Cryptology — CRYPTO '85 Proceedings, 523–534, Springer Berlin Heidelberg, Berlin, Heidelberg, 1986.

[36] L. Keliher, H. Meijer, "A New Substitution-Permutation Network Cipher Using Key-Dependent S-Boxes," in H. C. Williams, editor, SAC 97, 13–26, 1997.

[37] L. Keliher, "Refined Analysis of Bounds Related to Linear and Differential Cryptanalysis for the AES," volume 3373, 42–57, 2004, doi:10.1007/11506447_5.

[38] S. G. Meintains, Z. HLÁÁVKA, "Goodness-of-Fit Tests for Bivariate and Multivariate Skew-Normal Distribution," Scandinavian Journal of Statistics, **37**(4), 701–714, 2010, http://www.jstor.org/stable/41000416.

[39] D. Han, L. Min, G. Chen, "A Stream Encryption Scheme with Both Key and Plaintext Avalanche Effects for Designing Chaos-Based Pseudorandom Number Generator with Application to Image Encryption," International Journal of Bifurcation and Chaos, **26**(5).

[40] D. Han, L. Min, G. Chen, "A Stream Encryption Scheme with Both Key and Plaintext Avalanche Effects for Designing Chaos-Based Pseudorandom Number Generator with Application to Image Encryption," International Journal of Bifurcation and Chaos, **26**(5), 2016, doi:10.1142/S0218127416500917.

[41] C. Shannon, "Communication Theory of Secrecy Systems," Bell Systems Technical Journal, **28**, 656–715, 1949.

[42] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. Noonan, P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," Inf. Sci, **222**, 323–342, 2013.

Advances in Science, Technology and Engineering Systems Journal Vol. 10, No. 2, 42-48 (2025)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology 2024-25

ASTESJ

ISSN: 2415-6698

A Study of the Digital Health Management Needs of the Elderly

Ya Gao[1*], Fatma Layas[2], Xiangyu Dong[1], Yijing Li[1], Jiayi Li[3]

[1] *University of Wales Trinity Saint David, Wales Institute of Science of Art, Swansea, SA18PH, United Kingdom*

[2] *University of Wales Trinity Saint David, Assistive Technologies Innovation Centre, Wales Institute of Science of Art Swansea, SA18PH, United Kingdom*

[5] *Yanching Institute of Technology, Art Institute, Langfang, 065201, China*

ARTICLE INFO

Article history:
Received: 25 October, 2024
Revised: 15 January, 2025
Accepted: 23 January, 2025
Online: 25 April, 2025

Keywords:
Digital health
Health Management
Smart Health Technology
Technology impact
Needs of older people

ABSTRACT

The purpose of this paper is to explore the feasibility and development trend of utilizing smart medical technology for chronic disease health management in older people in the context of ageing at home. As the ageing society intensifies, the elderly population faces multiple health challenges, especially the management of chronic diseases. This paper analyzes the potential of smart medical technologies, such as remote monitoring, artificial intelligence, and the Internet of Things (IoT), to improve the efficiency and quality of health management for older people. By leveraging Maslow's Hierarchy of Needs Theory and Fogg's Behavioral Model, the article explores how to design smart health management products that meet the different health needs of older adults. In addition, the article discusses the barriers that the elderly population may encounter in accepting and using technology, such as the digital divide and technology adaptation issues, and proposes relevant coping strategies. Ultimately, the article concludes that with the continuous development of technology, smart healthcare technology will play an increasingly important role in geriatric health management, helping to improve the health status of older people, enhance their quality of life, and promote the innovation and development of social health management. The research in this paper provides new ideas for designing health management products for older people and supports the design and optimization of intelligent health management services.

1. Introduction

China's ageing level is at the upper-middle level in the world, showing the characteristics of large population size and rapid ageing [1]. Subsequently, the contradiction between the explosive growth in demand for health services for the elderly and the continuous weakening of family care capacity has become increasingly prominent, and the development of digital health management is expected to be an effective way to solve this problem [2].

In the context of the global economic crisis in 2008, IBM proposed the concept of a “Smart Earth” for the first time, arguing that the Internet of Things, the Internet, and intelligence together constitute the “Smart Earth” three elements[3].

In the same year, IBM released its "Smart Healthcare" solution in China, and since then ", Smart Healthcare" has been initially developed in China. With the rapid development of information technology, China's "smart healthcare" practice continues to deepen the development of digital health management, which is an important direction of the broader "smart healthcare" [4]. Intelligent health management uses a new generation of information, communication, artificial intelligence, bioinformatics, and other technological means to sense, analyze, and integrate the information from the three key links of health detection, health assessment, and health intervention so as to respond intelligently to the health needs of an individual or a group [5]. Although digital

*Corresponding Author: Ya Gao, University of Wales Trinity Saint David. 2105341@student.uwtsd.ac.uk

https://dx.doi.org/10.25046/aj100205

health management offers solutions for older adults to cope with physical functioning, chronic diseases, and reduced socialization, older adults' difficulties in using digital health technology cannot be ignored. Personal, social, and technological factors impact the acceptance of digital health management among older adults. Therefore, it is of great significance to study the digital health management model for older people, which adapts to the trend of population ageing and meets the needs of older people. Combined with the concepts related to digital health management, and given the physiological and psychological characteristics of older people, the digital health management model for older adults can be briefly summarized as follows: under the premise of digital health technology adapted to ageing, health monitoring, assessment, and health interventions for older people can be implemented to efficiently, conveniently, and accurately satisfy the health needs of older people at all levels of older people's physiological, psychological, and social needs, and to improve older people's health level. For example, in the future, digital technologies such as artificial intelligence will be deeply integrated with the geriatric health service system, and older people will be able to obtain relevant health management services, such as health monitoring and assessment or guidance on medical treatment, by conversing with the system. The digital health management model will help older people integrate into digital city life and prompt them to improve their health. Digital health management technology also makes it possible for older people to stop being bothered by complex operating systems and to obtain personalized quality health services conveniently.

2. Technologies and Applications Related to Digital Health Management for Older People

Current digital health management technologies for older people include remote monitoring, mobile health, the Internet of Things, smart homes, and artificial intelligence.

Telemonitoring systems help patients collect health data online at home and transmit it to health centers. The telemedicine model provides critical monitoring support for chronic diseases and older people. Wang et al. developed a community-based health monitoring system for older people. The study first used relevant equipment to obtain and record relevant health information such as daily activities, continuous vital signs, and gait of older people, after which the decision support system utilized advanced data mining techniques to count the significant changes in the data and accordingly sent alerts to older people and their families and their The decision support system utilizes advanced data mining techniques to count significant changes and accordingly alerts older people and their families and caregivers to take appropriate interventions to prevent deterioration of health conditions[6]. Remote monitoring technology provides significant support for healthy, safe, and independent living, especially for older adults with chronic conditions such as cardiopulmonary disease, asthma, and heart failure, and has great promise for the future.

The World Health Organization defines "mobile health "as a service delivery method that uses cell phones, tablets, and wearable devices to provide medical support. Through the mHealth platform, health information can be continuously delivered from the patient's end to the doctor, and the doctor's solutions can be delivered to the patient so that problems arising in the patient's body can be judged and solved in advance [7]. Mobile health apps play a significant role in the physical assessment of older people. Silva et al. have developed an app called "Geriatric Assistant" as a practical guide for healthcare professionals to assess older people's health and access up-to-date information comprehensively [8]. Wearable devices have also developed rapidly in recent years. Yu et al. developed a deep-learning model based on wearable device data to monitor falls among older people [9]. Zhong et al. investigated gait assessment applications for older adults to provide favorable support for analyzing regularity, symmetry, and variability of gait length in older adults [10].

The Internet of Things (IoT) connects things to things and things to people through various devices [11]. With the continuous reform and innovation of device functions, IoT technology is deeply developed in the health field to assist in meeting the health management needs of older people. Liu et al. designed a health promotion system for older people using IoT technology, which can organize the long-term dietary and exercise records of older people and assist older people in completing their personal nutritional assessments and health management. IoT is widely used in smart cities, public services, smart homes, life health, and personal care[12]. In addition, the development of IoT technologies such as blockchain technology, tactile internet, and nano-internet is anticipated.

Smart home technology provides a degree of digital linkage or living experience, creating a unique home for the user with sensors and actuators configured together. With the continuous development of smart home technology, smart home products in health and ageing are also emerging. However, while increasing the experience, there is no compelling evidence that smart homes significantly affect the treatment of diseases and the prevention of incapacitation [13].

Artificial intelligence, as a technology, is mainly applied to medical robots to make intelligent machines react similarly to humans through the logical judgment of autonomous intelligence. Current intelligent machines include features such as face recognition, intelligent speech, and deep learning. In addition, artificial intelligence plays a vital role in serving older people. Artificial intelligence software helps older persons sift through exercise, diet, and other health information. To a certain extent, robotic pets can reduce the sense of loneliness among older persons, and chatbots can communicate with older persons and remind them of the time to take medication and have regular medical check-ups [14]. In the future, AI will play a more prominent role in senior living needs. With the continuous progress of science and technology, artificial intelligence technology is gradually reaching its potential great value in the medical field, artificial intelligence technology is gradually realizing its potential great value in the medical field. Artificial intelligence is an important driving force for the new round of technological revolution and industrial change. It is an important driving force for the new round of scientific and technological revolution and industrial change. It is a new technical science that researches and develops theories, methods, technologies and application systems for simulating, extending and expanding human intelligence. It is a new technological science that researches and develops theories, methods, technologies and application systems for simulating, extending and expanding human intelligence. Compared with

traditional management strategies, the technical support provided by AI technology offers a more efficient and convenient way to monitor and treat chronic diseases. The characteristics of AI algorithms enable them to process massive amounts of data to more accurately detect hidden patterns or trends, which is an extremely critical feature for predicting disease progression or evaluating the effectiveness of treatment [15]. Compared to manual labour that requires rest, AI systems can operate 24/7 without interruption, continuously providing real-time feedback and advice to doctors and patients, further improving the efficiency of management. AI-based prediction models also help doctors develop more personalized treatment plans to better meet the individual needs of patients.

3. Impact of Digital Health Technologies on Older Adults

The design has been transformed into a technological design when design activities based on computer network technology and virtual reality technology enter people's lives. Technology has been controversial since the beginning of the industrial age. Optimists believe that technology is the greatest invention of the age, creating things that did not exist in the world and greatly enriching people's lives. On the contrary, pessimistic people believe that technology goes against ethics and morality and even leads to the decline of culture. Of course, in today's age of information technology, people's perception of technology is not simply black and white, especially when it comes to intelligent medicine.

Positive Impacts: Due to the deep plumbing of information technology, we cannot ignore its many positive impacts. On the one hand, IT provides strong technical support for safe and healthy healthcare. On the other hand, it also provides more diverse disease prevention and treatment services for older people.

It is an inevitable trend for digital health technology to provide intelligent services for older people, and it is also a positive role of technology in healthcare services. Telemedicine services enable older people to communicate with their doctors online, reducing to a certain extent the cases in which older people cannot seek medical treatment even for various reasons. This is not only helpful to older persons living in remote areas but also provides vital support to those in poor health and unable to seek medical care in a timely manner.

There is evidence that telemedicine positively impacts the health management of homebound older adults with diabetes, including some reduction in cognitive decline, mortality, hospitalization, and healthcare costs, and may increase disease-related knowledge, adherence, and self-efficacy. On the other hand, healthcare professionals conduct two-way video disease monitoring and health management guidance with home-bound elderly patients through the Internet platform. They can also carry out popularization education, dietary monitoring, rehabilitation guidance, and health risk and medication adherence assessment[16]. Most elderly home-based caregivers must assist older people in their daily lives, monitor their signs, or address emergencies. However, most caregivers do not receive formal training in caregiving. As a result, home-based caregivers need more medical information training and support tools to facilitate stress management and improve their coping skills. Mercy is the world's first virtual medical center, which uses advanced technology to provide telemedicine services, including remote round-the-clock health consultations, emergency care, and home monitoring. Healthcare professionals can collect detailed data from seniors through video monitors to capture some of their sudden symptoms so that treatment can be taken [17]. Telemedicine solves, to some extent, the geographical problem for both healthcare providers and home-based caregivers, as healthcare providers can not only provide psychosocial interventions, training and support to older caregivers (including family members and other informal caregivers) through telemedicine platforms but also offer comprehensive geriatric care programs to caregivers [18].

Negative impact: The use of technology has not been smooth sailing for older people. The conflicts and contradictions that have erupted among older people in the Internet era have forced society to ponder whether the times are moving so fast that we are ignoring a part of the population that technology has forgotten. Does the rapid update of technology have no negative impact? The answer is no.

The dilemma older people face in the Internet era is the “digital divide” phenomenon in the academic world. Scholars generally believe that the fundamental dilemma that prevents older people from using intelligent technologies in a learning-oriented manner is not their lack of interest in or rejection of new technologies but rather their state of existence, conditions, and environment, which leads to their objective “vulnerability” in the face of the promotion and use of intelligent technologies[19]-[20].

The first is vulnerability at the physiological level. This condition is an objective problem for older people when exposed to innovative technologies. With the continuous development of medical technology, there is no doubt that human life expectancy has gradually increased. However, as older people age, the decline in cognitive functions such as vision, hearing, and touch, as well as in cognitive and thinking skills such as attention and memory, remains irreversible. Moreover, these problems become more pronounced with age. This is even though relevant research suggests that most older people are, to some extent, internally or externally motivated to learn intelligent technologies [21]. Differences in educational backgrounds and work experiences make older people, to a certain extent, reflect specific differences. However, the primary trend is similar, i.e., "slow walkers" in the "fast" era of intelligence. Media theory suggests that digital and intelligent technologies are essentially seen as extensions of people's perceptions and have a symbiotic relationship with human beings, being "part of humanity [22]". However, the increasing age of older people and the constant iteration of technology have made the predatory disadvantage of older people even more exceptionally pronounced.

The second is vulnerability at the cultural level. The experience and exposure that older people have accumulated over the long years is a priceless asset, yet it is undeniably a form of entrenchment and constraint for them. This leads them to favor traditional and familiar technologies. They feel a vague sense of alienation in the fast-developing smart era, which leads to a sense of “fear” or “rejection” when facing intelligent technologies. This situation may lead to a lack of interest in and exposure to innovative technologies [23]. Therefore, compared with young people, it is difficult for older people to develop intelligent

technology information literacy and overall cultural atmosphere [24].

In addition, vulnerability has a social dimension. Social support from family members plays a crucial role in helping older people cross the digital divide [25]. However, the role of family support in the intelligent technology enhancement of older people has not been fully utilized; on the one hand, due to the scarcity of time for children and other family members, when older people have digital needs and ask for help from family members, the family members may not have enough patience to teach older people in-depth. Older people have not grasped the essentials of learning digital technology, which, to a certain extent, may deepen their rejection of digital products. On the other hand, it is due to the "generation gap" that limits the willingness and initiative of older people to seek help [26]. The gradual withdrawal of older people from various social relationships has led to a gradual scarcity of their social roles, such as peer and social relationships, and a weakening of their social status, making the conditions for older people to take the initiative in obtaining help weaker and weaker, which will make older people not have enough ability to obtain information related to digital technology, and the tendency to "weaken themselves" is constantly emerging in the use of intelligent technology [27]-[29].

The topic worth exploring is how digital technology can be adapted to an ageing society and practically help make life more convenient for older people. Therefore, while bridging the digital divide, we should accept that ageing is an objective reality of social development. It is undeniable that the development of technology has provided diverse services for older people. However, at the same time, technological development cannot relentlessly leave older people behind. Therefore, we need to start from the perspective of the needs of older people, really see their expectations, and appropriately meet their needs so that intelligent technology can serve the lives of older people more reasonably.

4. Needs analysis of older people

4.1. Hierarchy of needs of older people

Given the diverse and complex needs of elderly patients with chronic diseases, Maslow's needs theory will provide us with directions. Abraham Maslow, an American psychologist, proposed Maslow's theory of needs in 1943, dividing human needs into five levels from low to high: physiological needs, safety needs, social needs, respect needs and self-actualization needs (as shown in the figure below). Everyone has needs, and when low-level needs are satisfied, people pursue higher-level needs. When multiple needs are unsatisfied, people will first pursue the most urgent needs [30].

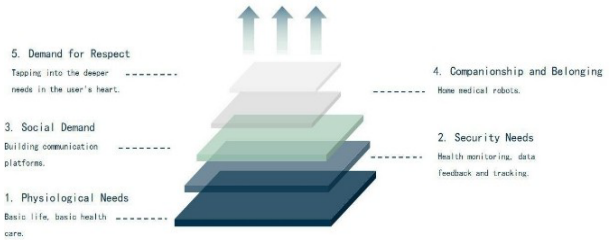


Figure 1: Maslow Hierarchy of Needs

Physiological needs are the most basic necessary for survival. If physiological needs are not met, the lives of older persons are threatened. Therefore, technology supports the basic life and basic medical care of the elderly. Digital health technology uses products or services to solve the fundamental problems of life and medical care for the elderly.

Security needs include personal safety, health protection, moral security, family security and property ownership. Among them, health protection is the foundation of other security needs of older people. In other words, only with a healthy body can older people start other activities. Older adults need health monitoring due to their declining physical functions. Therefore, physiological signs such as heart rate, blood glucose, blood pressure, sleep, etc., can be monitored with data feedback and tracking by using sensing technology to report the physical condition through several critical indicators so that timely treatment and resuscitation can be carried out in dangerous moments to improve the efficiency of medical treatment.

Social needs are higher-level needs, including love, friendship and affection. Compared with physical needs, emotional needs are more detailed. Everyone is in a specific social environment and wants to be cared for. Specific social needs are unavoidable in order to avoid self-enclosure. However, their social needs differ from those of young people; they mostly socialize by organizing activities online and gathering offline, and their channels to broaden their social circle are concentrated offline, and network socialization is just a tool for contacting their feelings. Therefore, the role of community peers in the self-health management of older people is self-evident. Innovative healthcare platforms can connect patients with groups with similar health conditions, promote mutual support and group communication, and increase the social participation of older people. Nowadays, many products have APP services, in which a communication platform can be built for older people, bringing together older people with the same disease who can discuss their daily lives and provide each other with experiences and emotional exchanges.

Respect the need for self-expression of older people. Everyone is unique and has the right to express themselves; of course, older people are no exception. Digitalization has given rise to the development of short videos, and the cost of self-expression has been dramatically reduced, empowering the general public, including older people, with more voice. Used for self-expression is an affirmation of oneself. Digital platforms have brought about a noticeable shift in the daily lives of older adults, providing a platform for those brave enough to express themselves.

Older people build confidence in self-health management, which is conducive to leading a decent life. Therefore, we can make full use of artificial intelligence and sensing technology to enhance the "proactivity" of products, meet the functional needs of users, and even internalize them as part of the bodily functions of the elderly, forming a natural and hidden interaction. In this way, the psychological needs of older people who do not want their physical ageing and defects to show, do not want to be looked at differently by others, and desire to live a decent life like ordinary people can be satisfied.

4.2. Linking Smart Technology to the Needs of Older Adults

In addition to meeting the needs of older people, it is also essential to strengthen the relationship between older people and technology, which helps to enhance their willingness to use innovative products. Therefore, behavioral design is also needed. Through behavioral design, we can stimulate the interest of older people in using innovative products and guide older people who are already using intelligent products to use them more intensively.

In 1930, Harvard psychologist B.F. Skinner created a Skinner box experiment to study how rats respond to rewards. In a box with a control lever, the rats were given food to drop whenever they pushed the lever, a reward that led to the rats quickly learning the skill of pushing the lever. Skinner speculated that if the rewards were designed well, human behavior could be guided by what is now known as Behavioral Design. Professor B.J. Fogg of Stanford University applied behavioral design with computer software and the Internet to provide theoretical support for studying user behavior [31]. Fogg believed that behavior is influenced by motivation, capability cost, and triggers, i.e., the Fogg Behavioral Model (shown below) was produced. The Fogg Behavioral Model shows that the occurrence of behavior needs to satisfy the three critical points of motivation, capacity cost, and triggers, which are favorable conditions for the occurrence of a behavior.

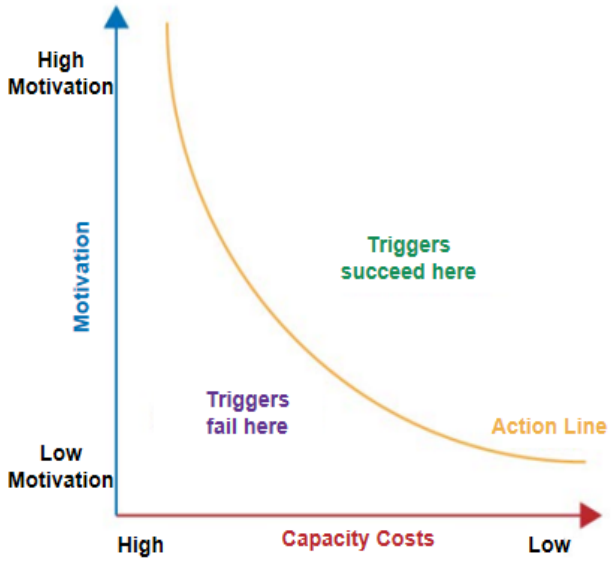


Figure 2: Fogg Behavior Model

① Increase the motivation to use the product: Motivation can be divided into direct and indirect. The user's willingness to use this product is low. Suppose we want to fully integrate ageing and digitalization and make digitalization fully integrated into the lives of older people. In that case, we need to start with the people or environment around older people and indirectly influence the willingness of the elderly group to use intelligent products. Recommendations from friends and relatives are an excellent way to gain motivation. Due to the obvious social needs of older people, getting likes and comments from their friends and relatives on technology products will increase their willingness to use them and achieve the purpose of communication and socialization. In addition, the "family" function also makes online socializing more cohesive. Among them, the "regional family" has very regional attributes and can be accurate to the provinces, cities and streets where the elderly users can not only expand offline social networking but also increase the sense of belonging of older people in use.

② Reduce the cost of using digital products: Motivation to meet the factors and the ability to cost are also indispensable.

a. Reduce the user's time cost, i.e., improve the product's responsiveness and give positive feedback during the waiting process to increase the product's fault tolerance. Otherwise, older people may perceive that they have made a mistake and thus be demotivated to use the product.

b. Reduce learning costs. Intelligent products with clear functional logic and simple interaction may attract many users. For example, in Dou Yin, videos can load automatically, and users can see updated videos by simply sliding up or down. Older people can access their favorite content by simply moving their fingers, and the learning cost is meagre, attracting many elderly users.

③ Increase the triggers to use the product: although the user has generated the motivation to use the product, the capacity cost is not high, but if they need a specific behavior to occur smoothly, the catalyst between the elderly user and the product is also significant, that is the triggers (as shown in the figure below).

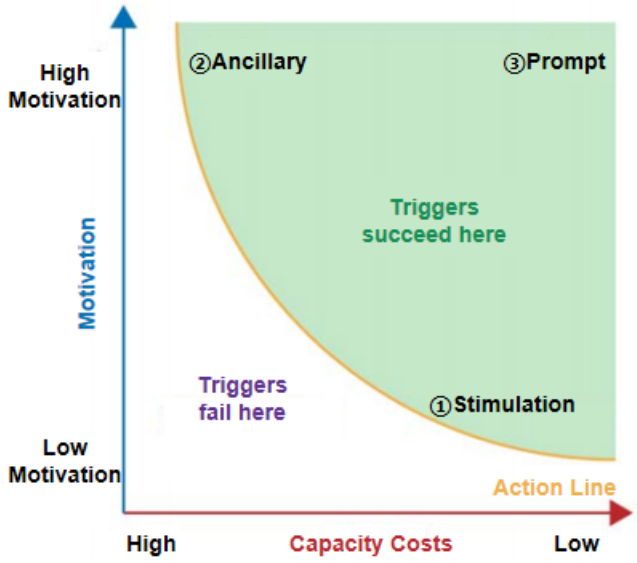


Figure 3: Triggering Factor

a. Reward stimulus is the most common trigger. In the case of a product with low-capacity cost but weak user motivation to use it, reward stimulation affects the user's usage behavior. Getting unexpected rewards when the user uses the product can increase the user's sense of surprise about the product and improve the stickiness of using the product. For example, in the case of Pinduoduo, the help of friends can enable users to obtain a sum of money. Users can get rewards through meagre capacity costs, so users who are not too willing to use the product also develop the behavior of using the product.

b. Assistance and product fault tolerance. When older users are motivated to use the product, but the ability cost is high, appropriate instructions and guidance can reduce the learning cost to a certain extent. "Kaixin Xiaoxiao Le is one of the few popular games among the elderly. In addition to the friendly image design, more importantly, every new element or character in the game will guide the user on how to play, and when a new activity appears, it will also guide the user on how to get the prize. The prompt signals in the product can also communicate with the user to avoid the situation where the user suddenly encounters a problem that leads to an inability to operate.

5. Conclusion

To focus on technology is to focus on the future. Under the premise of comprehensively judging the situation of population ageing and chronic diseases, an in-depth analysis of the positive and negative impacts of intelligent medical technologies will lay the foundation for finding solutions to innovative medical technologies to better meet the needs of older adults in the future. Elderly health management services and products relying on remote monitoring, artificial intelligence and other information technologies mean there are new ways and contents for elderly health management services. In the self-health management of older adults, we need to pay attention to the different levels of health needs and support them.

Guided by the goal of comprehensively improving the health of the elderly population, Maslow's hierarchy of needs theory provides theoretical support for the study of self-health management of older adults. Fogg's behavioral model provides a reference for the design of intelligent health products. This study uniquely combines Maslow's and Fogg's theoretical frameworks to explore and address the particular challenges faced by older adults in chronic disease management. By combining insights from behavioral psychology with cutting-edge technology applications, this study provides innovative perspectives for designing inclusive, personalized health management solutions. It is believed that with the continuous acceleration of the process of scientific and technological innovation, the application of science and technology in the field of digital health will become more and more extensive and will continue to meet the multi-level and diversified needs of the elderly chronic disease group, thus improving the efficiency of health management and quality of life of older people [32].

References

[1] Z.P. Ren, "China ageing report," Development Research, 40(2), 22–30, 2023.

[2] E. Vidal, "Digital literacy program: Reducing the digital gap of the elderly: Experiences and lessons learned," in 2019 International Conference on Inclusive Technologies and Education, IEEE, San Jose del Cabo, Mexico: 117–1173, 2019, doi:10.1109/CONTIE49246.2019.00030.

[3] IBM, Smarter planet, 2008.

[4] M. Chen, "New progress and prospect of smart healthcare in China in 2021," China Medical News, 36, 6–7, 2021.

[5] Q. Zeng, X.Y. Gao, S.Z. Bai, "Theory and practice of smart health management," Chinese Journal of Health Management, 16, 3–6, 2022.[6] H. Wang, Y. Zhao, L. Yu, et al., "A personalized health monitoring system for community-dwelling elderly people in Hong Kong: design, implementation, and evaluation study," *J. Med. Internet Res.,* vol. 22, p. e19223, 2020.

[6] H. Wang, Y. Zhao, L. Yu, J. Liu, I.M. Zwetsloot, J. Cabrera, K. L. Tsui, "A personalized health monitoring system for community-dwelling elderly people in Hong Kong: Design, implementation, and evaluation study," Journal of Medical Internet Research, 22(9), e19223, 2020, doi:10.2196/19223.

[7] R.P. Searcy, J. Summapund, D. Estrin, J.P. Pollak, A. Schoenthaler, A.B. Troxel, J.A. Dodson, "Mobile health technologies for older adults with cardiovascular disease: Current evidence and future directions," Current Geriatrics Reports, 8(1), 31–42, 2019, doi:10.1007/s13670-019-0270-8.

[8] S. Silva, R. Felgueiras, I.C. Oliveira, "Geriatric helper: An mHealth application to support comprehensive geriatric assessment," Sensors, 18(4), 1285, 2018, doi:10.3390/s18041285.

[9] S. Yu, Y. Chai, H. Chen, R.A. Brown, S.J. Sherman, J.F. Nunamaker, "Fall detection with wearable sensors: A hierarchical attention-based convolutional neural network approach," Journal of Management Information Systems, 38(4), 1095–1121, 2021, doi:10.1080/07421222.2021.1990617.

[10] R. Zhong, P. L.P. Rau, "A mobile phone–based gait assessment app for the elderly: Development and evaluation," JMIR mHealth and uHealth, 8(5), e14453, 2020, doi:10.2196/14453.

[11] A. Panarello, N. Tapas, G. Merlino, F. Longo, A. Puliafito, "Blockchain and IoT integration: A systematic survey," Sensors, 18(8), 2575, 2018, doi:10.3390/s18082575.

[12] M. Shakeri, A. Sadeghi-Niaraki, S. M. Choi, S.M.R. Islam, "Performance analysis of IoT-based health and environment WSN deployment," Sensors, 20(20), 5923, 2020, doi:10.3390/s20205923.

[13] L. Liu, E. Stroulia, I. Nikolaidis, A. Miguel-Cruz, A. Rios Rincon, "Smart homes and home health monitoring technologies for older adults: A systematic review," International Journal of Medical Informatics, 91, 44–59, 2016, doi:10.1016/j.ijmedinf.2016.04.007.

[14] J. Rong, X. Ji, X. Fang, M. H. Jee, "Research on material design of medical products for elderly families based on artificial intelligence," Applied Bionics and Biomechanics, 2022, 1–6, 2022, doi:10.1155/2022/7058477.

[15] A.M. Fischer, A. Varga-Szemes, M. Van Assen, L.P. Griffith, P. Sahbaee, J.I. Sperl, J.W. Nance, U.J. Schoepf, "Comparison of artificial intelligence–based fully automatic chest CT emphysema quantification to pulmonary function testing," American Journal of Roentgenology, 214(5), 1065–1071, 2020, doi:10.2214/AJR.19.21572.

[16] C.L. Walker, M. Kopp, R.M. Binford, C.J. Bowers, "Home telehealth interventions for older adults with diabetes," Home Healthcare Now, 35(4), 202–210, 2017, doi:10.1097/NHH.0000000000000522.

[17] L. Klingensmith, L. Knodel, "Mercy virtual nursing: An innovative care delivery model," Nurse Leader, 14(4), 275–279, 2016, doi:10.1016/j.mnl.2016.05.011.

[18] N. C. Chi, G. Demiris, "The roles of telehealth tools in supporting family caregivers: Current evidence, opportunities, and limitations," Journal of Gerontological Nursing, 43(2), 3–5, 2017, doi:10.3928/00989134-20170111-04.

[19] J. Wu, "Study on the current situation and influencing factors of China's elderly people's internet use: Analysis based on CGSS 2017 data," Scientific Research on Aging, 9(9), 43–58, 2021.

[20] S.J. Song, Research on digital divide problems and countermeasures for the elderly in Dalian city, Liaoning Normal University, 2021, doi:10.27212/d.cnki.glnsu.2020.001653.

[21] W.C. Su, Z.P. Lu, Z.X. Wang, "Preserving the dignity of elders' choices:

A conceptual model of autonomous behavior in the use of digital technologies for older adults," Library Forum, (8), 86 - 95, 2021.

[22] Y.L. Wang, L. Z., "Analysing the influencing factors and countermeasures of the digital divide among the elderly in the digital age," Journalism Probe, 9, 126 - 128, 2021.

[23] F. Lin, A study of the digital generation gap in Chinese families in the context of ageing, Shenzhen University, 2018.

[24] X. Xu, The impact of the internet on the continued socialization of older people, Dongbei University of Finance and Economics, 2013.

[25] W.P. Zhang, J.H. Fan, "The construction of a social support system for the digital divide in old age," Scientific Research on Aging, 7(2), 63 - 70, 2019.

[26] Z.C. Du, "Revisiting the adherence to a positive view of gerontological education — and discussing the social de-personalization of the individual, life education," The Seniors University, 5, 22 - 26, 2009.

[27] C.X. Huang, "Status, challenges and countermeasures of the digital divide in old age," People's Forum, (29), 126 - 128, 2020.

[28] B. Lin, "Difficulties and priorities in the governance of digital poverty among the elderly," People's Forum, (29), 129 - 131, 2020.

[29] B. Yang, D.C. Jin, "The digital divide in the elderly: Manifestations, motivations, and paths to bridging," Central States Journal, (12), 74 - 80, 2021.

[30] A.H. Maslow, Maslow's humanistic philosophy, Jilin Publishing Group Co., Ltd.: 35 - 38, 160 - 168, 2013.

[31] B. Fogg, "A behavior model for persuasive design," in Proceedings of the 4th International Conference on Persuasive Technology, ACM, Claremont California USA: 1 - 7, 2009, doi:10.1145/1541948.1541999.

[32] H.L. Zhu, "Integrating technology in China to help the elderly: A paradigm shift," Communication of IIMA, 3, 95 - 106, 2015.

Advances in Science, Technology and Engineering Systems Journal Vol. 9, No. 4, 102-109 (2024)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

Energy Management Policy and Strategies in ASEAN

Wai Yie Leong[1*], Yuan Zhi Leong [2], Wai San Leong [2]

[1]*INTI International University, Persiaran Perdana BBN Putra Nilai, 71800 Nilai, Negeri Sembilan, Malaysia*

[2]*Schneider Electric Singapore, 50 Kallang Avenue, Kallang, Singapore*

ARTICLE INFO

Article history:
Received: 30 June, 2024
Revised: 11 August, 2024
Accepted: 14 August, 2024
Online: 20 August, 2024

Keywords:
Energy Efficiency
ASEAN
Energy Infrastructure
Renewable Energy

ABSTRACT

This research analyses the challenges faced by ASEAN countries in managing its energy efficiencies and resources due to rapid economic growth, increasing energy demand, and diverse energy infrastructures across member states. This paper explores the energy management policies and strategies within the ASEAN region, focusing on the integration of energy efficiency measures, renewable energy initiatives, and cross-border energy trade. This paper analyse the region's progress towards its sustainable energy goals, the role of policy frameworks, and the impact of regional collaboration. Key challenges such as energy security, affordability, and environmental sustainability are examined, alongside opportunities for innovation in energy technologies and policy reforms. The findings highlight the importance of a cohesive energy management strategy that balances the diverse needs of ASEAN member states while advancing the region's transition towards a low-carbon future. This paper provides policy recommendations aimed at enhancing ASEAN's energy resilience and supporting its sustainable development goals.

1. Introduction

The ASEAN region's energy demand is growing significantly and rapidly as a result of urbanisation and economic advancement. The ASEAN region's reliance on fossil fuels, volatile geopolitics, and challenges associated with climate change make it vulnerable to energy supply vulnerabilities.

Consequently, member countries of ASEAN have been working together to develop and implement energy management policies that promote economic development, environmental sustainability, and energy security. The specifics of each ASEAN Member State's (AMS) energy efficiency (EE) and activities are shown in Figure 1. Remarkably, in the 2030s, Brunei, Singapore and Thailand, declared their intention to cut their Energy Intensity (EI) by 45%, 35%, and 30% [1]. Over the years, AMS has demonstrated a considerable reduction in energy intensity from 2005-2020 and the projected of energy Sumption to 2040 is shown in Figure 2.

*Corresponding Authors: Wai Yie Leong INTI International University, Emails: waiyie@gmail.com

In order to improve energy security, regional collaboration is emphasised in the ASEAN energy policy. Member nations cooperate to reduce supply disruptions and guarantee a steady supply of energy for their expanding economies by encouraging cross-border and international energy trade, international networkings, and energy resource sharing (Table I).

The ASEAN energy strategy encourages collaboration on energy-related projects, experience-sharing, financing access, and alliances with foreign organisations, development agencies, and other countries. The energy-related concerns is strengthened by this international cooperation.

The ASEAN energy strategy demonstrates a cooperative dedication to tackling the region's energy-related issues. The strategy lays the groundwork for member nations to collaborate on energy resources management and create a sustainable energy Future by fostering energy security, resource sustainability, and better economic growth. ASEAN Energy Statistics Leaflet (AESL) 2023 provides comprehensive visualised snapshots of the energy landscape in ASEAN. These include primary energy supply, final

https://dx.doi.org/10.25046/aj090411

energy consumption, electricity, renewable energy, energy-gender, and other energy-related indicators as shown in Figure 3.

2. Literature Review

The heterogeneous region of ASEAN has different energy needs, resources, and obstacles. In light of economic growth and urbanisation, there is an increasing need for energy, making it imperative to create and execute efficient energy management strategies in order to guarantee energy security, sustainability, and resilience. In order to better understand the literature and research on energy management policy in ASEAN, this review will focus on some of the major obstacles, frameworks for policy, and possible solutions.

Challenges in Energy Management: The vast array of problems posed by ASEAN's heterogeneous energy landscape is noteworthy. Coal, oil, and natural gas are examples of fossil fuels that continue to be major energy sources. These fuels raise difficulties with energy security and the environment. In addition, the region is vulnerable to price changes and geopolitical issues due to its reliance on imported fossil fuels. The necessity of developing sustainable energy sources and diversifying the energy mix is highlighted by this circumstance.

Energy Policies and Frameworks: The ASEAN Plan of Action for Energy Cooperation, or APAEC, is the cornerstone of the region's energy policy framework. In order to promote energy security, affordability, accessibility, and sustainability, APAEC was founded in 2016. It emphasises how important regional collaboration is to resolving energy-related problems, advancing energy trade within ASEAN, and encouraging energy technology knowledge transfer.

Development of Renewable Energy: As a result of its ability to improve energy security and lessen its negative effects on the environment, renewable energy policies have become more popular among ASEAN members. According to research [2], government initiatives on feed-in tariffs (FiT), incentives, and schemes could facilitate renewable energy technology on wind energy and solar power.

Initiatives for Energy Efficiency: ASEAN's energy management plans has been increasing energy efficiency. Studies [3] have demonstrated that energy efficiency initiatives aimed at families and businesses have resulted in significant energy savings as shown in Figure 4. These programmes include the creation of energy-efficient appliances, the implementation of best practices, and technological advancements.

Policy Coordination and Implementation: A number of studies highlight how crucial it is for ASEAN member nations to coordinate their policies to guarantee the successful application of energy management plans. Mechanisms to improve energy security and foster economic cooperation have been suggested, including cross-border energy commerce and harmonising energy norms. Policy coordination presents a number of issues that call for constant attention, especially when considering the disparities in national capacities and priorities.

The literature also suggests potential paths that may influence ASEAN's energy management laws. It has been proposed that the resilience and sustainability of energy systems can be improved by exploring energy technologies like energy storage systems and smart grids. The shift to low-carbon energy systems can also be facilitated by matching energy policies with global climate commitments like the Paris Agreement.

The analysis highlights the intricacy of ASEAN's energy management policies, involving issues with environmental sustainability, energy security, and policy coherence. It is encouraging to see how far the region has come in creating renewable energy sources and energy-saving techniques. However, to guarantee a safe, sustainable, and resilient energy future,

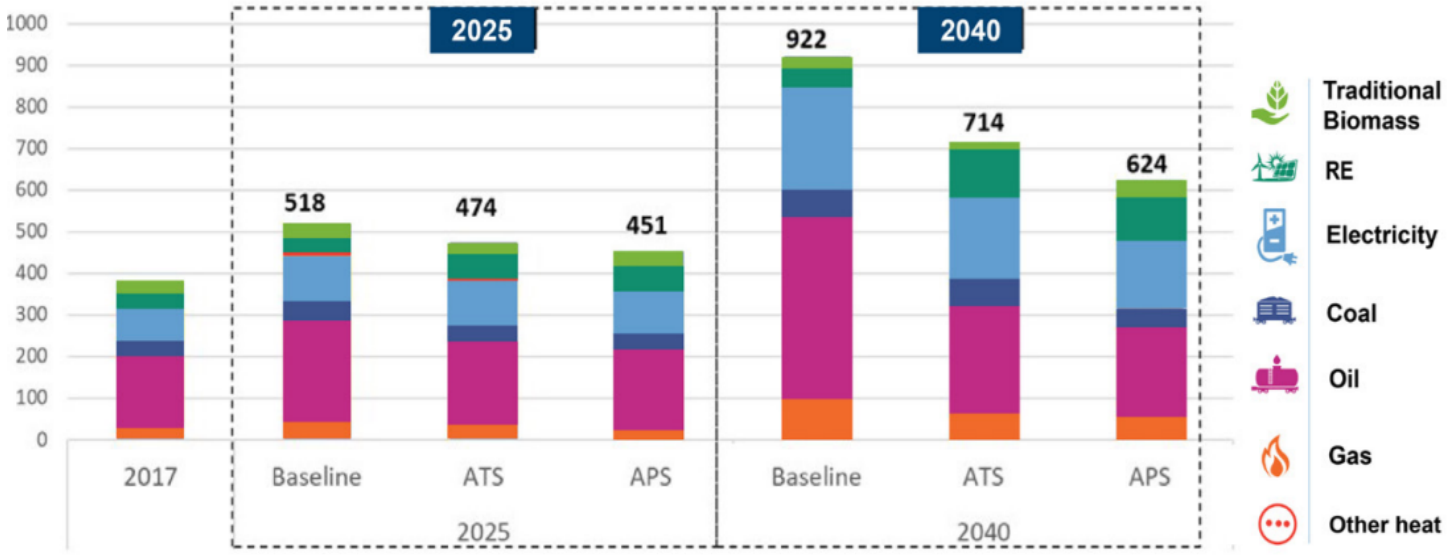


Figure 1. The projected ASEAN energy consumption based on 6th ASEAN Energy Outlook

cooperation must continue along with the development of novel tactics and changes to legislation [4].

3. Energy Efficiency Policy

The ASEAN region has a wealth of undeveloped renewable resources, but for now, fossil fuels control the majority of the energy systems in the area. ASEAN members aim to attain Net-Zero emissions by 2050 or later in order to combat climate change.

A. Singapore: The country has put in place a number of energy-saving initiatives:

- Energy Conservation Act mandates that major energy users increase their energy efficiency achievement and share on the energy consumption.
- Energy Efficiency National Partnership (EENP) initiative promotes the energy management strategies and energy savings objectives among organisations.
- Building designs and technology that are energy-efficient are promoted by the Green Mark certification programme.

B. Malaysia: The country has implemented energy efficiency policies such as the Energy Efficiency and Conservation Act, which attempts to increase energy efficiency in a number of industries.

- Projects and efforts pertaining to energy efficiency are supported by the Energy Efficiency and Conservation Fund.
- The programme called Malaysian Building Integrated Photovoltaic (MBIPV) promotes the integration of solar energy into buildings.

C. Thailand: The country's energy-saving initiatives include: Encouraging energy-efficient buildings and industry under the Energy Conservation Promotion Act.

- The plan encourages the use of energy-saving technologies and establishes goals for reducing energy intensity.
- Private investment in energy efficiency initiatives is encouraged by the Energy Performance Contracting (EPC) programme.

C. Indonesia: The country has implemented many energy efficiency programmes, such as the National Energy Policy, which endeavours to enhance energy efficiency while lowering energy intensity.

- The primary objective of the Energy Conservation Master Plan is to conserve energy in several sectors, including buildings, transportation, and industry.
- Building capacity and energy efficiency projects are supported by the Energy Efficiency and Conservation Programme.

D. Vietnam: The country has implemented many energy efficiency efforts, including:

- National Energy Efficiency Programme, which promotes energy-saving measures for public and industrial sectors.
- Energy Efficiency and Conservation Law creates energy labelling regulations and standards for energy-related equipment.
- Energy-efficient building designs are encouraged by the Green Building Certification programme.

E. Philippines: The country has enacted several energy-efficient laws, such as the Energy Efficiency and Conservation Act, to encourage energy-efficient technologies in buildings, industry, and transportation.

- The Energy Efficiency and Conservation Roadmap delineates objectives related to energy efficiency and provides a framework for accomplishing them.
- Programme implementation for energy efficiency is managed by the Energy Efficiency and Conservation Division of the Department of Energy.

G. Brunei: The energy-efficiency initiatives include:

- The National Energy White Paper lays out plans for enhancing energy-efficiency and advancing renewable energy.
- Targets for lowering energy use and advancing energy-efficient technologies are outlined in the Energy Efficiency Master Plan.

H.Vietnam, Cambodia, Myanmar, and Laos increase energy efficiency with assistance from partners and international organisations. Developing energy-efficient building rules, encouraging energy-efficient lighting, and spreading awareness of energy conservation are some of its endeavours.

It is imperative to acknowledge that these synopses offer a broad outline of energy efficiency regulations in every nation, as illustrated in Figure 3. These policies' efficacy is contingent upon a number of variables, including public participation, enforcement, and implementation. It is advised to consult government and professional energy related organisations for the information.

4. Strategies for Energy Management Policy in ASEAN

Diversification of Energy Sources: Changing your energy sources is one of the main tactics. Risks to energy security are increased by ASEAN's significant reliance on fossil fuels. These hazards can be reduced by encouraging the development and use of renewable energy sources, such as solar, wind, hydro, and geothermal. Figure illustrates energy and greenhouse gas emissions in ASEAN.

Improved Energy Economy: Enhancing energy efficiency is yet another essential tactic. Energy-efficient measures can be implemented by member states in a variety of sectors, such as buildings, transportation, and industries. This entails using cutting-edge technologies, encouraging energy-efficient behaviours, and upholding energy efficiency regulations.

Cross-Border Energy Trade: Energy security and dependability can be improved by facilitating cross-border energy trade and linkages among member states. By constructing infrastructure for

the transmission of natural gas and electricity, this tactic enables excess energy in one nation to satisfy demand in another. These kinds of partnerships can reduce energy waste and maximise the use of resources.

Technology Innovation and Research: It is imperative to allocate resources towards technology innovation and research. Grid stability and energy management can be enhanced by developments in smart grids, energy saving and storage, and decentralised energy systems. To speed up technical advancements, ASEAN member states might encourage cooperation between academic institutions and business sectors.

Policy Coordination and Harmonisation: The prosperity of the area depends on member governments coordinating their energy policies. Fair competition can be encouraged and level playing fields can be created by harmonising norms, laws, and incentives. To enable cross-border trading of renewable energy, governance rules and key indicator targets for renewable energy can be aligned.

Building Human capability through Training Programmes and Educational Initiatives: Effective policy implementation depends on raising public awareness and fostering human capability. Increasing public knowledge of sustainable methods and energy saving can also encourage behavioural changes and advance energy management objectives.

The solutions presented in this paper provide a way forward for a sustainable, and safe energy, based on the energy issues that ASEAN is currently confronting. Through the adoption of strategies such as energy source diversification, efficiency enhancements, cross-border cooperation, technological innovation, and policy coordination, ASEAN can steer clear of obstacles to achieving its energy objectives and simultaneously support worldwide endeavours to tackle climate change and promote sustainable development [5].

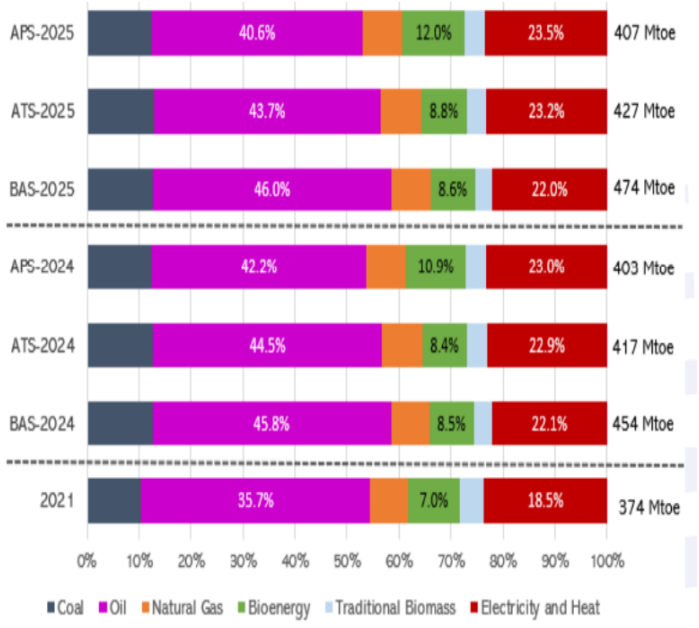


Figure 2: ASEAN energy demand 2024-2025 projection by fuel

Table I: Energy related pledges by committed by ASEAN countries

Pledge's Name	Targets	Countries
Global Renewable and Energy Efficiency pledge	Tripling the global's renewable energy generation capacity to at least 11,000 GW by 2030 and doubling the global average annual rate of energy efficiency improvement from 2% to over 4% per year until 2030	Brunei Darussalam, Malaysia, Singapore, Thailand
Global cooling pledge	Reduce cooling -related emission by a minimum of 68%to 2022 levels by 2050.	Brunei Darussalam, Cambodia, Singapore, Thailand, Vietnam
Declaration by Hydrogen and Derivatives	Mutual recognition of certification for renewable and hydrogen	Malaysia, Singapore

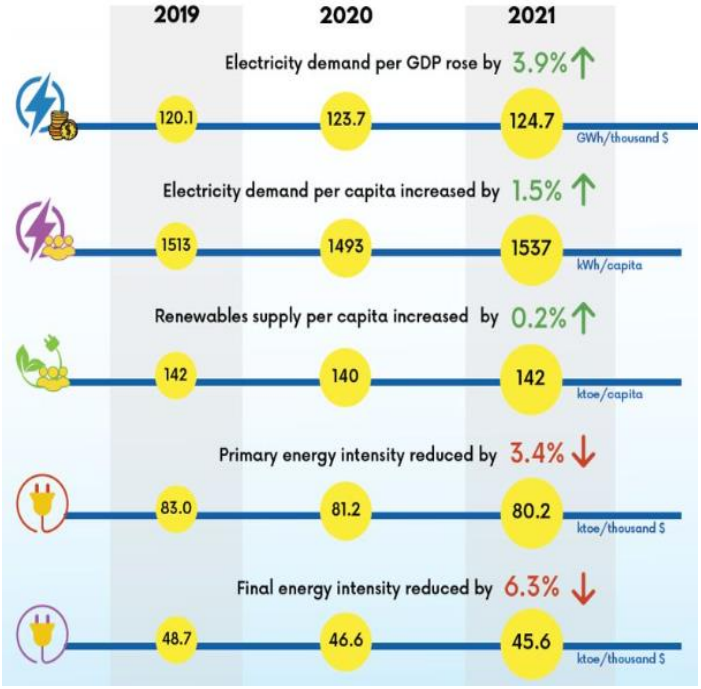


Figure 3: Primary energy supply, final energy consumption, electricity, renewable energy, energy-gender, and other energy-related indicators.

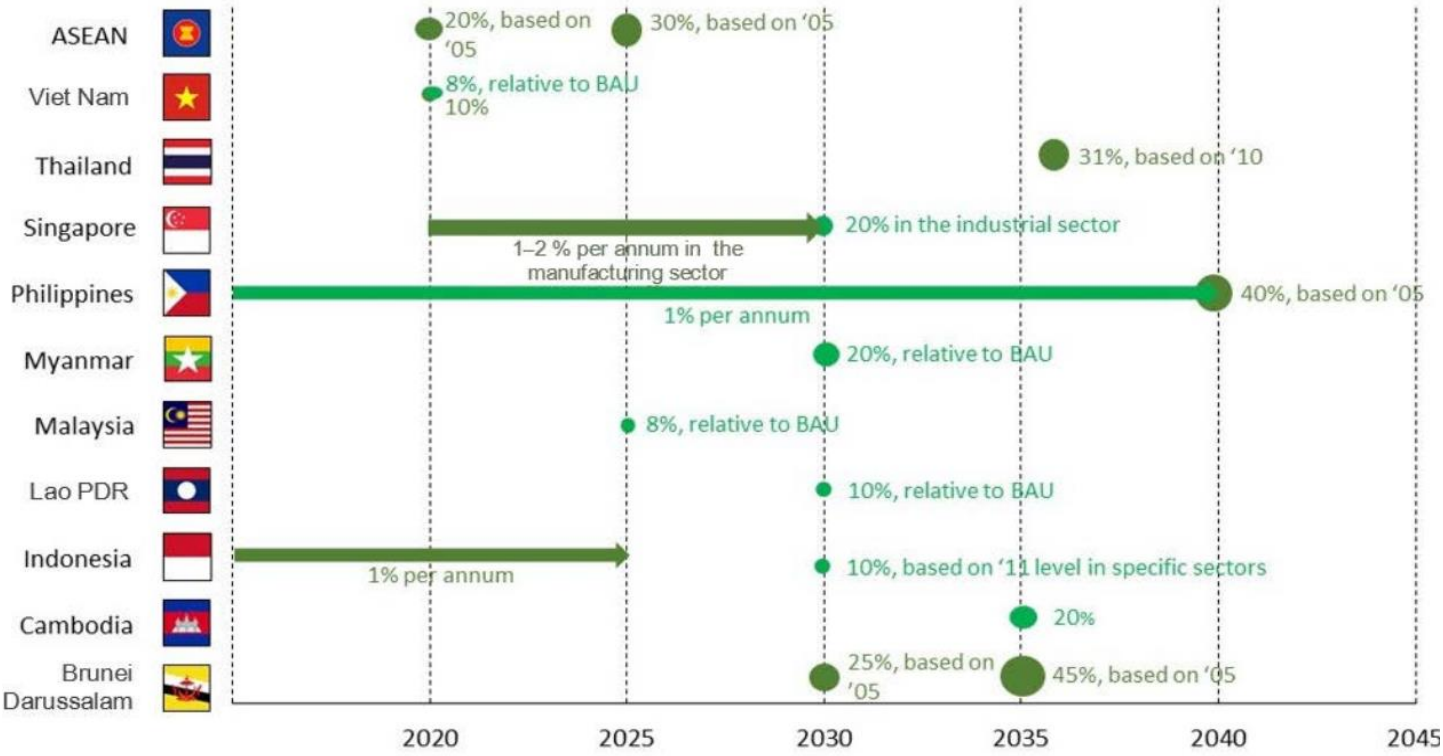


Figure 4: The ASEAN energy intensity (EI) and per capita total final energy consumption (TFC) [5]

5. ASEAN energy efficiency and policy Collaboration

Future prospects for efficient energy management in ASEAN are quite promising [6]. The region is witnessing economic expansion, urbanisation, and rising energy consumption. Consequently, there are multiple opportunities where energy efficiency and management initiatives might provide significant advantages (Table II):

A. The expansion of renewable energy: The ASEAN nations have an abundance of geothermal, hydro, wind, and solar energy resources. Increased utilisation of these resources offers a significant chance to improve energy security, lessen dependency on fuels, and reduce the climate change impacts [7, 8]. Infrastructure for renewable energy on wind turbines and solar energy, can draw investments, diversify the energy mix, and create jobs.

B. Smart Grid Implementation: ASEAN's energy management could undergo a radical change with the implementation of smart grid technologies. Demand response programmes, improved grid stability, optimal energy flow, and real-time monitoring and management of energy distribution are all made possible by smart grids [9]. Smart networks can decrease transmission and distribution losses and increase energy efficiency by incorporating renewable energy sources and strengthening system resilience.

C. Energy Efficiency in Buildings: An important portion of ASEAN's energy consumption comes from the building sector. Significant energy savings can be achieved by enforcing energy-efficient building rules, encouraging green building designs, and implementing technology like energy-efficient heating, cooling, and lighting systems [10]. Another big opportunity is to retrofit existing buildings with energy-efficient systems, as shown in Figure 4.

D. Industrial Energy Efficiency: ASEAN's energy-intensive sectors stand to gain from increased energy efficiency. Energy consumption and production costs can be decreased by using waste heat recovery, energy-efficient machinery, advanced manufacturing techniques, and process optimization [11]. Governments can use legislation and capacity-building initiatives to encourage industries to embrace best practices and technologies.

E. Electric Mobility and Transportation: The need for transportation grows along with urbanization [12]. One way to cut greenhouse gas emissions and lessen reliance on imported fossil fuels is to support public transit, establish infrastructure for EV charging, and promote electric vehicles (EVs). A sustainable transportation industry may be facilitated by the combination of renewable energy sources with electric mobility.

F. Energy Storage Solutions: The intermittency issues with renewable energy sources can be resolved by integrating energy storage technologies like batteries and pumped hydro storage [13]. In the end, energy storage contributes to a more dependable and resilient energy system by improving grid stability, facilitating the integration of renewable energy sources, and supporting demand-side management initiatives.

Country	Reference Document	EE Target
BN	Energy White Paper 2014	• 45% reduction of EI in 2035 compared to 2005 level
KH	Cambodia EE Plan	• 20% reduction of TFEC in 2035 compared to BAU
ID	National Energy Policy	• 1% reduction of EI per year until 2025 • 15% reduction of TFEC in each household and commercial sectors by 2025 compared to BAU
LA	National EE Policy 2016	• 10% reduction of TFEC in 2030 compared to BAU
MY	National EE Action Plan	• 8% reduction in electricity consumption in 2025 compared to 2016 level
MM	National EE&C Policy	• 20% reduction of electricity consumption in 2030 compared to BAU
PH	EE Roadmap for the Philippines, 2017-2020	• 40% reduction of EI in 2040 compared to 2005 level • 1% reduction of TFEC per year until 2040 compared to BAU
SG	Sustainable Singapore Blueprint	• 35% reduction of EI in 2030 compared to 2005 level
TH	Thai EE Policy 2015	• 30% of EI reduction in 2036 compared to 2010 level
VN	National Target Program for EE&C	• 5-7% EI reduction in TFEC in 2025 compared to 2019 level

Figure 5: ASEAN National Target on Energy Efficiency

	Malaysia	Indonesia	Philippines	Thailand	Vietnam	Singapore
Latest RE policy	MyRER 2035	National Energy Roadmap	Sectoral Energy Plan & Roadmap	Power Development Plan	Power Development Plan	Singapore's Energy Story
Year of latest RE policy	2020	2017	2017	2019	2019	2019
Overall RE targets	31% RE installed capacity by 2025, 40% by 2035	RE installed capacity by 45 GW by 2025, 168 GW by 2050, 31% of national primary energy supply in 2050	RE installed capacity of 20 GW by 2040	33% RE installed capacity by 2037 with RE mix as following • Solar 6 GW • Biomass 5.57 GW • Wind 3 GW • Hydropower 3.3 GW • Biogas 0.6 GW • MSW 0.5 GW	32% RE installed capacity by 2030, 45% by 2050	At least 2 GW of solar by 2030, and energy storage deployment target of 200 MW post 2025

Figure 6: Overview of key ASEAN countries' renewable energy share targets [1]

G. Cross-Border Energy commerce: By connecting the ASEAN nations, cross-border energy commerce may improve energy security and maximise the use of energy resources [14]. Building cross-border transmission lines collaboratively can facilitate the pooling of excess energy and act as a safety net against supply interruptions as shown in Figure 6.

H. Energy and Digitalization Data Analytics: In energy management, digital technology and data analytics have the potential to revolutionise the field [15]. Adoption of sensors, Internet of Things (IoT) devices, and data analytics platforms can facilitate data-driven decision-making for increased energy efficiency, predictive repair of equipment, and real-time monitoring of energy consumption [16].

I. Green Finance and Investment: As green finance methods proliferate, funds for sustainable energy initiatives may be drawn to them. ASEAN nations may expedite the shift towards a sustainable and low-carbon energy future by endorsing investments in clean technology, energy-efficient infrastructure, and renewable energy.

J. International Collaboration and information Exchange: To speed up efforts to improve energy management and efficiency, ASEAN nations can take use of international partnerships and information exchange. Countries can adopt successful techniques and benefit from one other's experiences by exchanging best practices, lessons learned, and successful case studies [16, 17].

In general, there is a great deal of promise for improved energy security, job creation, economic growth, and environmental preservation in the ASEAN countries' future energy management and efficiency [18, 19]. Through deliberate utilisation of these opportunities, ASEAN nations can set the stage for a future in energy that is both sustainable and affluent [20, 21].

Table II: New and upcoming ASEAN energy policies based on 2023 regulations

Country	New Policy and Updates Announced in 2023
Brunei Darussalam	● Brunei Darussalam National Council on Climate Change (BNCCC) requires all greenhouse gas (GHG) emissions emitted by private and public sector facilities to be reported quarterly and annually. ● Brunei committed to cutting 20% of emissions compared to the business-as-usual scenario and moving towards net zero in 2050 through energy transition and forest conservation as stated under its 2030 Nationally Determined Contribution (NDC). ● The government plans to update their energy intensity reduction in 2024.
Cambodia	● Launched Power Development Master plan (PDP) 2022-2024, includes demand forecasts, generation expansion and a transmission and distribution plan. ● Increase renewable energy (RE) share and reduce fossil fuel energy share by 2040. ● Aims for a 21% coal power share of the total energy mix by 2030, down from an initially expected 40% in 2040. ● Cambodian government approved five new renewable projects that would generate 520 MW for the national power grid and aim to reduce CO2 emissions. ● Hydro and solar power generations spread throughout Cambodia, supporting the new PDP's targets of a capacity of 3,155 MW and 3,000 MW by 2040.
Indonesia	● Indonesia Minster of Energy and Mineral Resources (MEMR) issued Regulation Number 2 and the implementation of Carbon Capture and Storage (CCS) and Carbon Capture, Utilization and Storage (CCUS) in Upstream Oil and Gas Business Activities (MEMR Reg 2/2023). ● The MEMR Reg 2/2023 regulation covers technical, monetisation, operational, monitoring and measurement, reporting and verification (MRV) requirements, safety and environment and closure of CCS/CCUS activities. ● MMER Regulation Number 2/2024 to encourage rooftop solar by removing limits on capacity and increasing rooftop solar quota. ● Update Government Regulation Number 79 of 2014 concerning the National Energy Policy (NEP), targets and policies for energy and emissions in Indonesia for the period 2023-2060. ● Adjusted RE target from 23% to 17-19% by 2025.
Lao PDR	● In 2023, expanded RE generation as more clean emission technology is being implemented. ● National strategies on utilising hydrogen and ammonia for clean energy are being created.
Malaysia	● Launched policies in 2023 under National Energy Transition Roadmap (NETR). ● Low Carbon National Aspiration 2040 (LCNA 2040): set targets for energy transformation, reduce carbon emissions and lower coal power plants, increase RE power share, increase EE, adopts electric vehicles, increase the usage of public transport, increase carbon footprint tracking and sustainability reporting. ● Increase RE capacity from 40% in 2040 t o70% by 2050. More solar generation for government buildings and more RE trade with neighbouring countries.
Myanmar	● Ministry of Planning and Finance has exempted import taxes for solar generation technology. ● Incentives to increase energy investments in Myanmar.
Philippines	● Launched 2023 National Energy Efficiency and Conservation Plan (NEECP) and roadmap for the 2023-2050 period, aims for at least 30% emission reduction in the residential sector and 28% in utilities. ● Launched Fuel Conservation and Efficiency in Road Transport (FCERT) programs for higher fuel efficiency and electric vehicles (EVs)
Singapore	● Launched new emission standards for fossil-fuel- powered generation, to have at least 30% hydrogen ready to be used.

Thailand	● National Energy Policy Committee approved additional procurement of RE for 2022-2030. Increase the supply of RE, wind and solar generation in Thailand. ● Electricity Generating Authority of Thailand (EGAT) implemented a green tariff sandbox trial in 2023 for consumers to purchase RE easily. Full implementation in 2024. ● More EVs are being implemented on public transport. ● National Electric Vehicle Policy Committee extended the import fee exemption until the end of 2025, to attract domestic EV production in Thailand. ● Implemented Carbon Border Adjustment Mechanism (CBAM) certification in collaboration with the EU, to track and price carbon emissions for products to be able to be imported into the EU, effective from 2023 to 2025.
Vietnam	● Issued Directive No.20/CT-TTg to increase efforts for EE by reducing energy usage and using more energy efficient hardware. ● Vietnam's government approved National Energy Master Plan (NEMP) 2021- 2030m to achieve energy security, reduce carbon emission, target to reach net zero by 2050. ● Aspired to export RE by 2030, for 5000 to 10000 MW. ● Green hydrogen production is expected to increase to 200,000 tonnes annually by 2030 and 20 million tonnes by 3million tonnes in 2050.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] "ASEAN Energy in 2024: Key Insights about ASEAN Energy Landscape and Predictions in 2024," *ASEAN Centre for Energy*, 2024. URL: aseanenergy.org. (Accessed on 9 January 2024).

[2] ASEANPOST, "5 Energy Companies to Look out for in ASEAN," *ASEANPOST*, (Accessed on 9 January 2024). URL: https://theaseanpost.com/article/5-energy-companies-look-out-asean.

[3] "Energy: AEDS (ASEAN), IEA statistics (EU & Asia Pacific) Economics & Demographic: AEDS (ASEAN), APEC Statistics (Asia Pacific), WDI (EU)," (Accessed by July 2024).

[4] A.J.T.A.P. Gnanasagaran, "Renewable Energy Cooperation in ASEAN," *The ASEAN Post*, 2019. URL: https://theaseanpost.com/article/renewable-energy-cooperation-asean. (Accessed on 1 January 2024).

[5] Y. Liu, R. Noor, "Energy Efficiency in ASEAN: Trends and Financing Schemes," *ADBI Working Paper Series*, No. 1196, *Asian Development Bank Institute (ADBI)*, Tokyo, 2020.

[6] W.Y. Leong, R. Kumar, "5G Intelligent Transportation Systems for Smart Cities," *In Convergence of IoT, Blockchain, and Computational Intelligence in Smart Cities*, Edited by R. Kumar, V. Jain, W.Y. Leong, S. Teyarachakul, 1st Edition, *CRC Press*, 2023.

[7] W.Y. Leong, J.H. Chuah, B.T. Tee, *The Nine Pillars of Technologies for Industry 4.0*, *Institution of Engineering and Technology*, 2020.

[8] W.Y. Leong, *Human Machine Collaboration and Interaction for Smart Manufacturing: Automation, Robotics, Sensing, Artificial Intelligence, 5G, IoTs and Blockchain*, *Institution of Engineering and Technology*, Stevenage, United Kingdom, ISBN 1839534141, 2022.

[9] U. Mehrotra, W.Y. Leong, "NSEEAR: An Energy Adaptive Routing Protocol for Heterogeneous Wireless Sensor Networks," *2009 35th Annual Conference of IEEE Industrial Electronics*, Porto, Portugal, pp. 2647–2652, 2009, doi:10.1109/IECON.2009.5415255.

[10] W.Y. Leong, Y.Z. Leong, W.S. Leong, "Human-Machine Interaction in the Electric Vehicle Battery Industry," *2024 10th International Conference on Applied System Innovation (ICASI), IEEE*, pp. 69–71, 2024.

[11] W.Y. Leong, Y.Z. Leong, W.S. Leong, "Green Building Initiatives in ASEAN Countries," *2023 Asia Meeting on Environment and Electrical Engineering (EEE-AM)*, Hanoi, Vietnam, pp. 1–6, 2023.

[12] W.Y. Leong, *Medical Equipment Engineering: Design, Manufacture and Applications (Healthcare Technologies)*, *Institution of Engineering and Technology*, 2023.

[13] W. Lee, W. Liu, P.H. Chong, B.L. Tay, W.Y. Leong, "Design of Applications on Ultra-Wideband Real-Time Locating System," *2009 IEEE ASME International Conference on Advanced Intelligent Mechatronics*, 2009.

[14] W. Liu, E. Lupito, Y.L. Sum, B. Tay, W.Y. Leong, "Ultra Wideband Antenna for Real-Time Location System Application," *2009 35th Annual Conference of IEEE Industrial Electronics*, Porto, Portugal, pp. 2738–2742, 2009, doi:10.1109/IECON.2009.5415424.

[15] W.Y. Leong, J. Homer, "Implementing Nonlinear Algorithm in Multimicrophone Signal Processing," *2005 IEEE Workshop on Machine Learning for Signal Processing*, Mystic, CT, USA, pp. 33–39, 2005, doi:10.1109/MLSP.2005.1532870.

[16] W.Y. Leong, "Digital Technology for ASEAN Energy," *2023 International Conference on Circuit Power and Computing Technologies (ICCPCT)*, Kollam, India, pp. 1480–1486, 2023, doi:10.1109/ICCPCT58313.2023.10244806.

[17] W.Y. Leong, L.S. Heng, Y.Z. Leong, "Smart City Initiatives in Malaysia and Southeast Asia," *Proceedings of International Conference on Renewable Power Generation*, Shanghai, China, pp. 1143–1149, 2023.

[18] W.Y. Leong, L.S. Heng, Y.Z. Leong, "Malaysia Renewable Energy Policy and Its Impact on Regional Countries," *Proceedings of International Conference on Renewable Power Generation*, Shanghai, China, pp. 7–13, 2023.

[19] R. Kumar, V. Jain, W.Y. Leong, S. Teyarachakul, *Convergence of IoT, Blockchain, and Computational Intelligence in Smart Cities*, *CRC Press*, 2023.

[20] A. Arshad, M.A.M. Yajid, M. Daroonparvar, "Effect of Laser-Glazed Treatment on Thermal Cyclic Behavior of Plasma-Sprayed Lanthanum Zirconate/Yttria-Stabilized Zirconia Double Ceramic Layered on NiCoCrAlYTa-coated Inconel," *Journal of Thermal Spray Technology*, 2023, doi:10.1007/s11666-023-01662-7.

[21] R. Kumar, A.K. Kapil, V. Athavale, W.Y. Leong, A. Touzene, "The Catalyst for Clean and Green Energy Using Blockchain Technology," *In Modeling for Sustainable Development: A Multidisciplinary Approach*, Nova Science Publishers, Inc, pp. 23–39, 2023.

Advances in Science, Technology and Engineering Systems Journal Vol. 9, No. 4, 110-118 (2024)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

Assistive System for Collaborative Assembly Task using Augmented Reality

Woratida Sawangnamwong, Siam Charoenseang

Institute of Field Robotics, King Mongkut's University of Technology Thonburi, Bangkok 10140, Thailand

ARTICLE INFO

Article history:
Received: 24 June, 2024
Revised: 13 August,2024
Accepted: 14 August, 2024
Online: 27 August, 2024

Keywords:
Augmented reality
STEM education
Education robot

ABSTRACT

Augmented reality (AR) technology has been increasingly used in developing teaching materials with the aim of sparking more interest in technology (T) and engineering (E) among students in STEM education. In the proposed system, AR is integrated with an educational robot controlled by a KidBright microcontroller board, developed by the Educational Technology research team (EDT) at the National Electronics and Computer Technology Center in Thailand. Moreover, the KidBright program has been implemented over 2,200 Thai schools. To maximize the benefits of the KidBright program, the Assistive System for Collaborative Assembly Task using Augmented Reality (ASCAT-AR) was created with the objective of enabling students to learn and collaborate in assembling robots. Students will work in pairs to assemble robots using the system and learn about mechanics, sensors, and 3D-printed parts. The students were divided into two groups: Group A read the manual and assembled the robot independently, while Group B used the ASCAT-AR system. In addition, AR applications offer smooth graphic rendering at 44-60 frames per second. Evaluation result showed that Group B students had a higher average success rate than average success rate of Group A students. The results showed that users of the ASCAT-AR system were more motivated in learning and obtained more knowledge about robot technology and programming.

1. Introduction

STEM education is a method of teaching that focuses on science, technology, engineering, and mathematics. Students receive training and preparation for the necessary 21st-century skills needed for success in the modern world [1]. Based on Bloom's Taxonomy [2], the related skills are classified into three categories: cognitive skills as shown in Table 1, such as critical thinking and problem-solving; social and emotional skills, such as communication and collaboration; and technological skills, such as the ability to use digital tools and platforms [3].

Previous works have revealed gaps in the effectiveness of STEM education in preparing students. One significant gap is the shortage of teachers specializing in STEM fields. A case study published in the Journal of Science Education and Technology highlights the challenges faced by many schools, particularly those in low-income neighborhoods, in providing STEM instruction due to difficulties in recruiting qualified teachers [4], [5]. Another challenge lies in the insufficient professional development opportunities for STEM teachers, as some educators lack the essential skills and knowledge needed to seamlessly incorporate STEM teaching and learning [6]. One such gap is the absence of standards and frameworks for developing and implementing MR teaching tools in STEM education. Although there is a growing interest in using MR for educational purposes, [7] a study published in the Journal of Science Education and Technology indicated a lack of sufficient guidelines and frameworks to assist educators in creating and utilizing MR resources effectively [8]. Table 2 show a comparison of the technologies.

Research published in the Journal of Science Education and Technology highlights the scarcity of mixed reality (MR) integration in STEM curricula. Rather than fully integrating mixed reality (MR) into the curriculum, some STEM instructors use it sporadically, which may reduce its effectiveness in teaching [9], [10]. Thailand has placed significant emphasis on STEM education and is committed to developing a more skilled and innovative workforce [11] The STEM education curriculum has been previously introduced and studied in Thailand[12], with initiatives focusing on curriculum development, digital media production, implementation in classrooms, and teacher training [13] The challenge is that students demonstrate low engagement in STEM disciplines. This lack of interest can hinder the effectiveness of STEM education and the development of a skilled future

*Corresponding Author: Siam Charoenseang, King Mongkut's University of Technology Thonburi, siam.cha@kmutt.ac.th

workforce [14]. Recently, robotics competitions have been organized in Thailand to motivate students' interest and creativity in robotics. In line with these efforts, schools have developed STEM education curricula that allow students to engage with technology. Although there is research on the design and implementation of MR learning games for robot assembly, there are still gaps in the teaching of technology and engineering subjects in STEM education. To enhance skills in robotics technology, this research project has developed an Assistive System for Collaborative Assembly Task using Augmented Reality (ASCAT-AR). This proposed system enables students to learn about the components and begin assembling a robot. The project implements augmented reality (AR) technology to captivate students' interests and relate their learning to future career opportunities.

Table 1: The Revised Taxonomy (2001) [4]

1.Remember	This level is about recalling information, such as facts, definitions, and concepts.
2.Understand	This level is about understanding the meaning of information, such as being able to explain it in your own words or apply it to new situations.
3.Apply	This level is about using information to solve problems or complete tasks.
4.Analyze	This level is about breaking down information into its component parts and understanding how they relate to each other.
5.Evaluate	This level is about making judgments about the value or worth of information.
6.Create	This level is about putting information together in new and original ways.

Table 2: XR Technology Comparison [9]

Features	AR	VR	MR
Definition	Limited interaction with virtual objects	Natural interaction with virtual objects	Natural interaction with both real and virtual objects
Hardware	Headset or smartphone	Headset required	Headset required
Applications	Navigation, wayfinding, product visualization, gaming	Gaming, entertainment, education, training	Gaming, entertainment, design, manufacturing, education, training

This research aims to develop an innovative educational tool to assist students in learning technology and engineering concepts within STEM education. AR technology is utilized within this system, and the educational robot is designed to be interfaced with Microsoft HoloLens 2 devices.

2. Proposed System

This research aims to create an innovative educational tool that can motivate students to understand STEM contents through robot assembly and control. Augmented reality (AR) technology is incorporated into this system to enhance the learning experience. The system overview, demonstrated in Figure 1, shows how users can use hand gestures to interact with a 3D model, manipulate its motion, and access information. Once the robot assembly is completed, the Microsoft HoloLens 2 provides a user interface for controlling the robot.

2.1. System Overview

The system overview depicted in Figure 1 illustrates that users can assemble an educational robot and utilize hand gesture recognition to rotate, move, zoom in, and zoom out a 3D prototype. The display is viewed through the Microsoft HoloLens 2. Once the educational robot is fully assembled, the system will show model a user interface and a window for simple programming, which is used to control the educational robot.

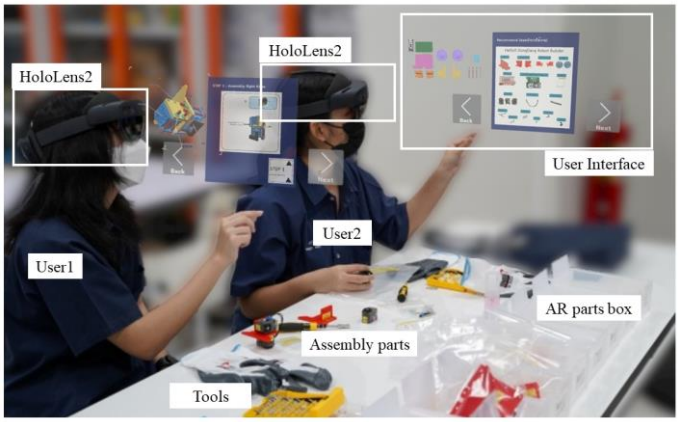


Figure 1: System Overview

2.2. System Configuration

The system operates through two primary processes: constructing the robot and controlling it. Figure 2 provides an overview of the involved steps. Initially, students are required to assemble the components of the educational robot. They can then write basic code to manage the robot using Microsoft HoloLens 2. Communication with the robot is conducted via a MQTT protocol. All instructions for building and controlling the robot are displayed directly on the Microsoft HoloLens 2.

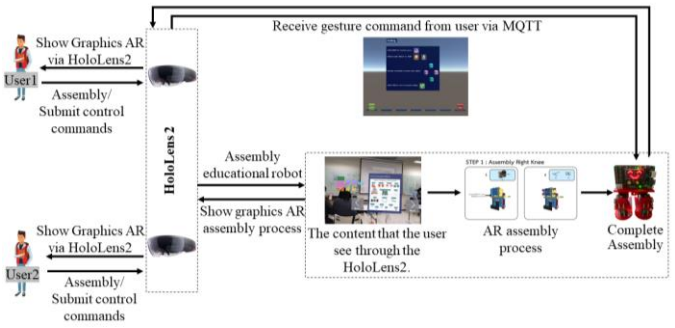


Figure 2: System Configuration

2.3. Mechanical Design and Implementations

The Otto platform was effectively used in a robotics engineering class at MIT, demonstrating its suitability for educational purposes [15]. The education robot is based on the Otto DIY Ninja robot, which is an open-source robot designed to teach programming, mechanics, electronics, design, the internet of things, and artificial intelligence [16]. It was selected as the foundation for the project because of its well-designed, affordable nature that is suitable for Thai schools. Several modifications were made to the Otto DIY Ninja design to align it more closely with Thai curriculum and teaching style. The robot is a low-cost, user-friendly, and educationally rich tool that can be used to teach various STEM concepts to students in Thailand.

The education robot in this research was designed using the SolidWorks program for 3D modeling robot parts. The robot has circular feet for walking and wheels for fast movement. The wheel was designed to allow the robot to walk on its feet or move on wheels. The robot's head is designed to accommodate the KidBright microcontroller board, OpenCM9.04 for operating the DYNAMIXEL XL-320 and a battery pack. The robot's legs can be folded and are designed to support two DYNAMIXEL XL-320s on each side. The component parts of the robot that will be used for 3D printing are shown in Figure 3. The foot part of the robot is shown in Figure 4, and the robot's head with the control board is shown in Figure 5.

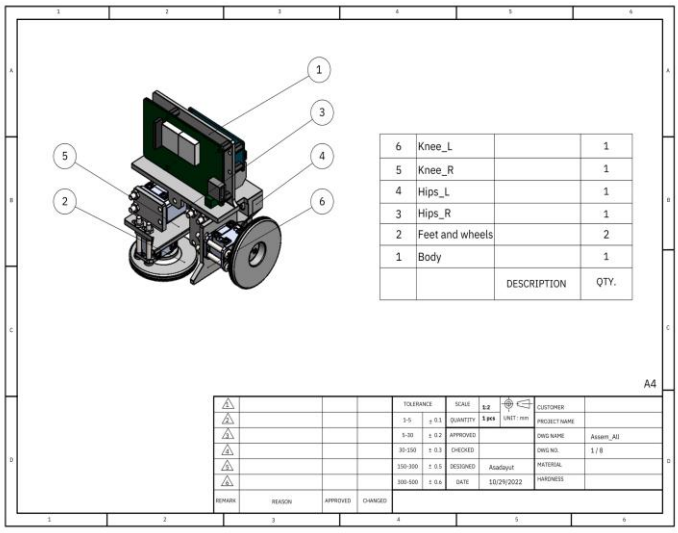


Figure 3: Robot design

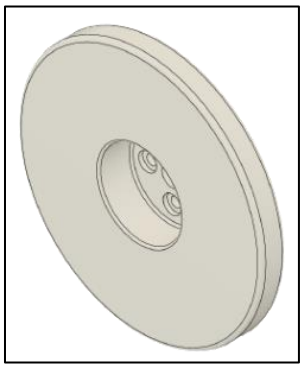


Figure 4: Wheel part

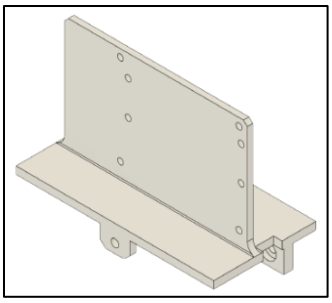


Figure 5: Head part

The assembled robot is set to the walk mode by default as shown in Figure 6. In this mode, the robot can move forward, backward, turning left, and turning right. Additionally, the robot can be switched to the wheel mode as shown in Figure 7, where it can move using its wheels. Even in wheel mode, the robot retains the ability to move forward, backward, turn left, and turn right.

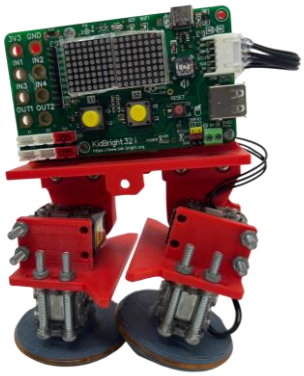


Figure 6: Walk mode configuration

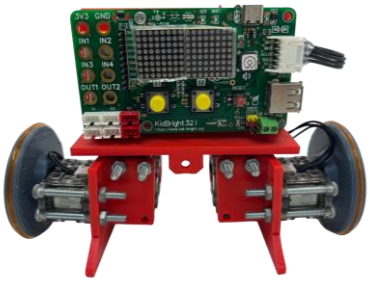


Figure 7: Wheel mode configuration

2.4. Electronic Design and Implementations

The KidBright microcontroller board was developed by the educational technology research team (EDT) at the National Electronics and Computer Technology Center (NECTEC), Thailand. It has been implemented over 2,200 schools across the country, promoting STEM learning on a wide scale. The board, based on the ESP32 microcontroller, enables device-to-device connectivity with internet of things feature and supports the integration of various external sensor modules via the I2C communication port. Figure 8 shows the connections of the KidBright board, the OpenCM9.04 controller, and the four DYNAMIXEL XL-320 servo motors. The KidBright microcontroller board offers a user-friendly interface,

affordability, and IoT capabilities, making it an asset for educational robots, suitable for both in-class learning and remote-control applications.

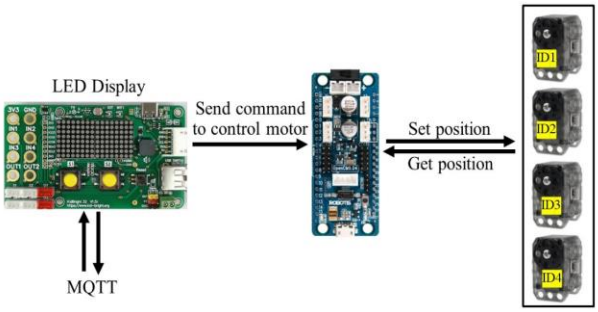


Figure 8: Microcontroller connection diagram

Figure 9 shows the OpenCM9.04 microcontroller and battery pack while Figure 10 displays the circuit battery charging design. The OpenCM9.04 is a microcontroller board used for controlling the DYNAMIXEL XL-320 motors. The battery pack supplies power to both the OpenCM9.04 and the DYNAMIXEL XL-320 motors. These components are essential for the education robot as they provide the necessary power for control the robot's movement.

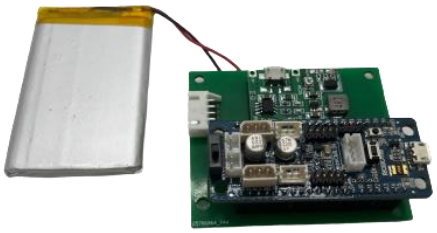


Figure 9: Battery charger and OpenCM 9.04 board

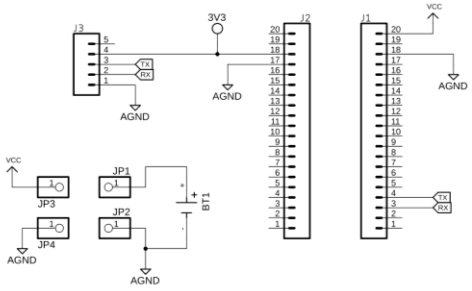


Figure 10: Battery charging and OpenCM 9.04 circuit design

2.5. Software Design and Implementations

2.5.1. Education Robot

The robot control program is divided into two parts. The KidBright program part: This part is used to as display graphics on screen and sends and receives data through the MQTT protocol. The KidBright board receives the robot's commands from the user. The OpenCM9.04 program part: This part is connected to the KidBright board using the I2C communication protocol. It is used to control the position of the DYNAMIXEL XL-320 motors to move to the received position by using the C++ programming language. The MQTT protocol is a lightweight messaging protocol that is well-suited for IoT applications. It is used to send and receive messages between devices over a network. The MQTT protocol is used in the education robot to send and receive commands between the KidBright board and the Microsoft HoloLens 2. The robot can be controlled by the user with two modes, which are wheel mode and walk mode as shown in Figure 11 and Figure 12, respectively.

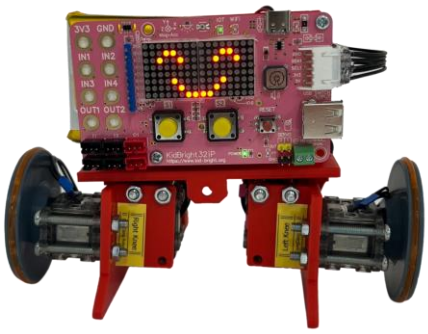


Figure 11: Wheel mode with display

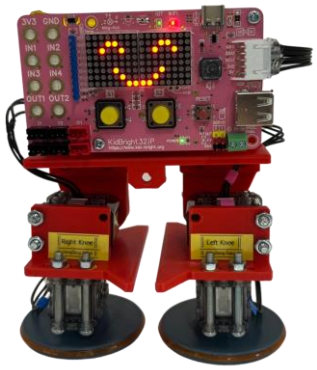


Figure 12: Walk mode with display

2.5.2. Robot Assembly Procedures

The assembly instructions for this research were modeled after LEGO's format, catering to a young audience. They were crafted to be intuitive, and accommodating users who may have no prior experience in robot assembly. These instructions utilize a 2D graphical format with distinct images and directional arrows to guide users through the assembly steps. Figure 13, the first page of the instructions, introduces the robot's parts along with a count of the pieces and components required for assembly. Subsequently, Figure 14 shows the detail of the initial step for the assembly, focusing on constructing the left knee, It is divided into two sub-steps. The guide follows a systematic structure, with each step clearly labeled and numbered. These instructions are a crucial component of the educational robot kit, facilitating the assembly process and enriching the user's understanding of the robot's various parts and components.

The 2D manual is implemented as a user interface (UI) on the display of Microsoft HoloLens 2. The UI on Microsoft HoloLens 2 is in a 3D format. 3D models can be scaled, rotated, or moved. These models can be animated to form an animation loop of the assembly process. Figure 15 shows Next and Back UI buttons for the next step or to go back to the previous step when the wrong assembly occurs. Assembly figure and description can be shown in Figure 16. The UI was developed using the Unity game engine.

The UI was designed to be easy to use and understand, even for users with no prior experience with 3D applications.

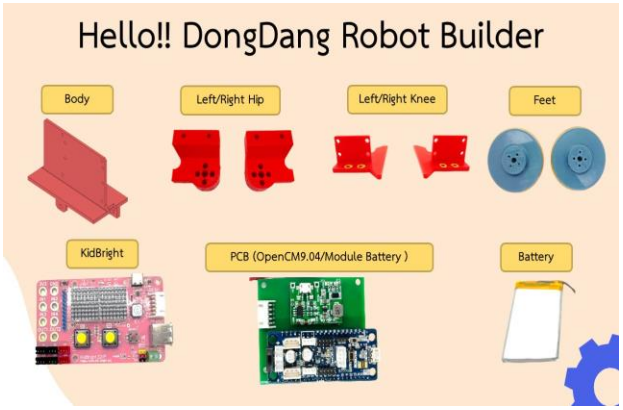


Figure 13: Introduction page of robot parts

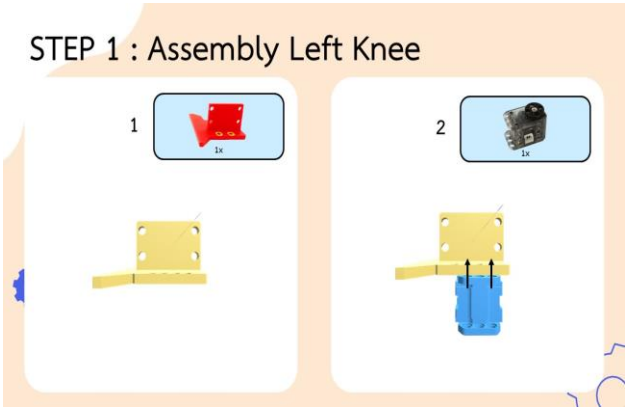


Figure 14: Assembly manual

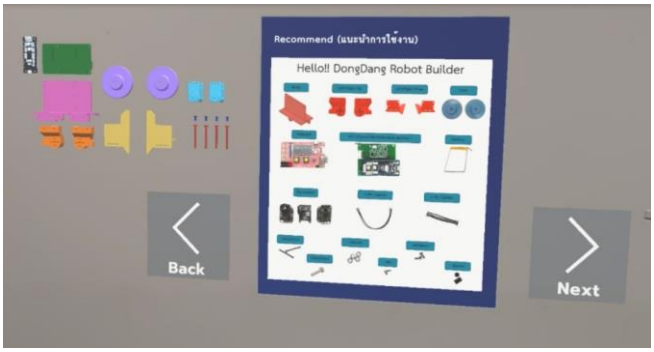


Figure 15: 3D introduction of robot parts via Microsoft HoloLens 2

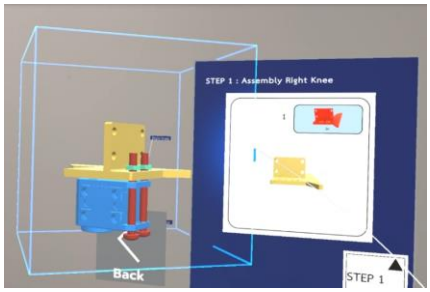


Figure 16: 3D guide for robot assembly via Microsoft HoloLens 2

3. System Implementations

3.1. Assembly System

Figure 17 shows the state diagram of ASCAT-AR system. First, the user launches the ASCAT-AR application. The application presents a window showing details of the modeled robot's components, as well as the models of necessary tools and equipment. Next, the user follows the on-screen guide to assemble the robot. This interactive guide will lead the user through the assembly process, from step one to step eight. AR highlights the exact location of each tool required for the current step, and enhances the ease of the assembly process. After completing the assembly, the application offers a choice of reassembling the robot or proceeding to program its controller. At this step, the user can verify each step of the assembly to ensure the completion. Once the assembly is confirmed to be completely correct, the application moves to a display window for robot control programming.

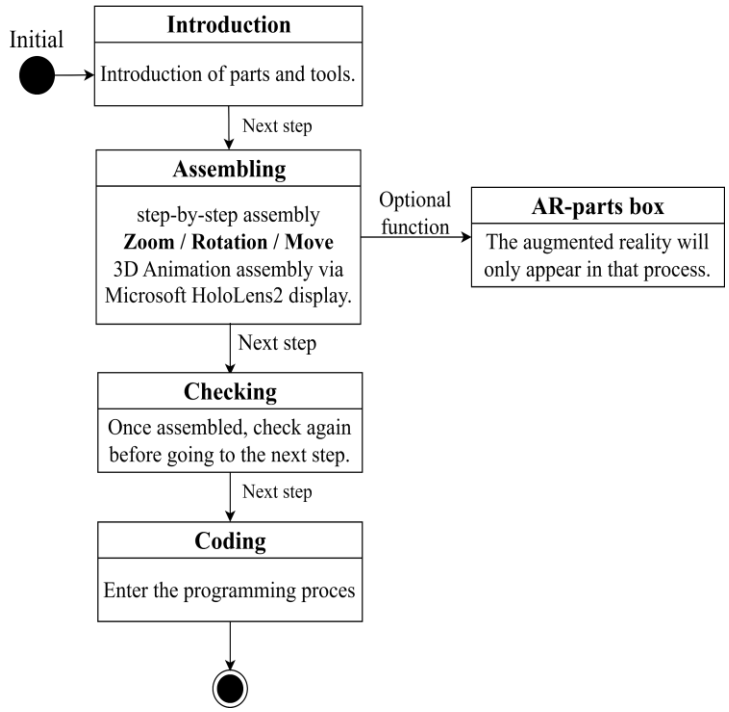


Figure 17: State diagram of proposed system

Figure 18 shows the sequences of assembly process. Each step must be completed before the next step can be proceeded. However, some robot modules can be assembled independently from the others.

3.2. Blockly System and Robot Control

Figure 19 shows the code using block or Blockly, an open-source visual programming language. Blockly allows users to write code using a visual block-based interface. Blockly is based on the prototype concept from Google's Blockly [14] and is designed to be easy to use and intuitive. This makes Blockly an excellent tool for teaching programming concepts to children and other beginners. Blockly lets beginners build programs fast and easily with visual blocks. Blockly is also flexible and can be used to create many kinds of programs [17]. Overall, Blockly is a powerful and user-friendly visual programming language that has become a popular choice for both teaching and development.

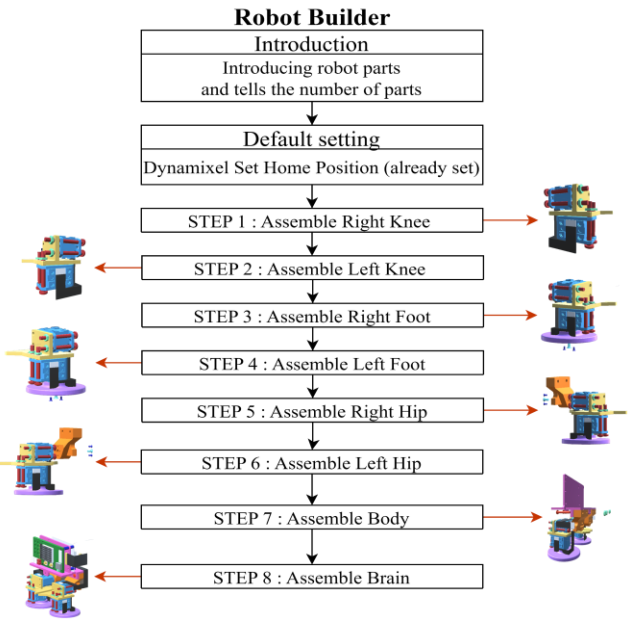


Figure 18: Robot assembly steps

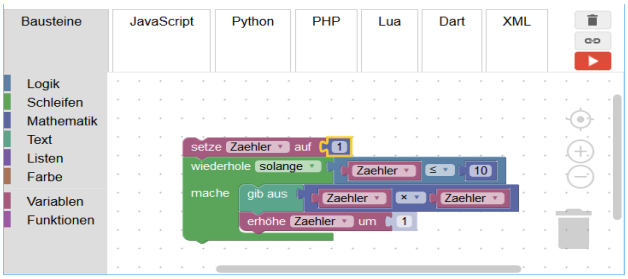


Figure 19: Google's Blockly demo [17]

The command set designed for ASCAT-AR system includes the following command buttons, which are MQTT connection button, robot transformation button, movement command buttons (front, back, left, and right), run the command button, as shown in Figure 20. These movement command buttons are used to control the movement of the robot. When the user presses a movement command button, it will create a command block in scene. When the command block appears, the user can pick it up and sort it into any available position. The programming window allows only 5 command blocks at one time as shown in Figure 21. Once the command is in the correct position, the user presses the run button to send the command to the robot. The instruction set is designed to be simple to use. This makes the instruction set a valuable tool for controlling the movement of the robot.

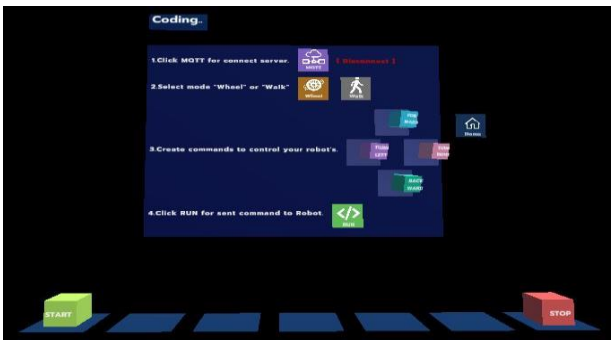


Figure 20: Robot control interface

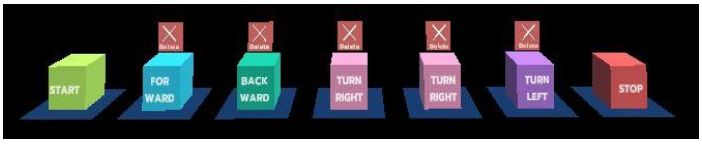


Figure 21: Samples of command blocks

The state diagram of robot control in Figure 22 describes the process of sending the robot command to the education robot. First, the user connects to the MQTT server by clicking the MQTT button on the screen. The user can select the working mode of the robot after the proposed application is connected with the MQTT server. There are two operational modes which are wheel mode and walk mode. In wheel mode, the robot moves like a car. In walk mode, the robot moves like a human walk. The user can select the Front, Back, Left, Right, and Turn commands to move the robot in the desired direction. Once the user completes the block coding, the Run button can be clicked to send the robot commands. As shown in Figure 23, the robot moves accordingly to the selected commands given by the user.

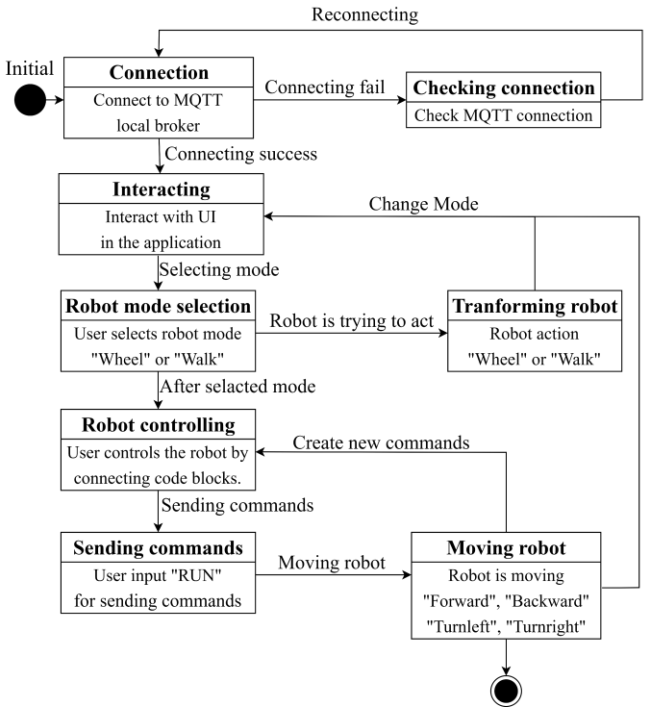


Figure 22: State diagram of Blockly-based robot control

Figure 23: Users send robot commands to the real robot via HoloLens 2

4. Experimental Results

The experimental results of this research cover system performance, usability, and values for specific tasks. System performance shows rendering frame rate of the ASCAT-AR system program on Microsoft HoloLens 2. Usability tests cover the evaluation of user's satisfaction, ability to learn, and ease of learning. Values for specific tasks are evaluated from data records of the assembly times, success rates, and error rates.

4.1. Population and Requirement

The number of users in the system are 24 persons who are high school students in Thailand. The students were divided into two groups to compare between the uses of the ASCAT-AR system and the assembly manual.

4.2. Evaluation Tools

4.2.1. Robot assembly record form

This form aims to collect the amount of time that the students spent on robot assembly. It can record the time spent, the point of assembly failure, and the time it takes to fix the wrong position, and the number of errors.

4.2.2. Pre-questionnaire and post-questionnaire

The pre-questionnaire and post-questionnaire forms include general questions about user background, experience, and suggestions for improving the system, as well as questions about values for specific tasks and evaluation of satisfaction on proposed system.

4.2.3. Satisfaction questionnaire

The satisfaction form aims to collect feedback on user's satisfaction about the provided content and system performance of the ASCAT-AR system.

4.2.4. Comparative assessment form

This assessment form was applied for both experimental sets to compare motivation and system differences.

4.3. Procedure of Experiment

The experimental sets were established for Thai high school students aged 13-18 years who have some or no experience in engineering. The experimental sets provide the users about practical experience in robot assembly and the use of Microsoft HoloLens 2 headset.

Volunteers were divided into two groups to avoid the memorization of operation flow and provided AR contents. The ASCAT-AR system was tested with 12 students while the other 12 students used the assembly manual. There were pre- and post-questionnaires to collect the students' knowledge and interest about the robot and the opinions on the experiment.

In Figure 24, students, who have no experience about robot assembly, are divided into two groups. The experiment consists of the following steps:

Step 1: Students need to complete a preliminary questionnaire.

Step 2: Both groups were asked to assemble the robot with different tools. The aim of this exercise is to provide experience about engineering tools and AR technology for students. The expected learning outcome is that both groups of students can complete the robot assembly and control the robot's movement.

Step 3: After completion of robot assembly and robot control, each group of students was asked to answer a post questionnaire testing.

Step 4: Students, who worked with ASCAT-AR system, need to complete the satisfaction questionnaire.

During experiments were conducted, researchers also observed the students' behaviors and reactions and interviewed the students regarding their experiences on using the ASCAT-AR system and the instruction manual.

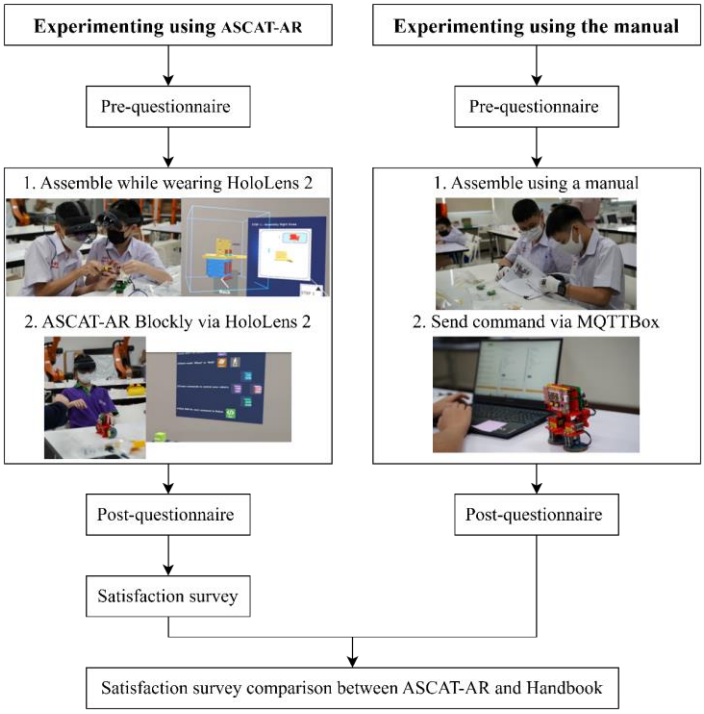


Figure 24: Experiment process flow

4.4. Experimental Results

The study was designed to evaluate the effectiveness of the ASCAT-AR system in enhancing student learning in STEM education, particularly in robot assembly task. The participants were 24 high school students aged 13-18 from Thailand, who had no prior experience with robotics. The study investigated two learning tools, which are the ASCAT-AR system utilizing augmented reality guidance via the Microsoft HoloLens 2 and the traditional 2D printed manual.

Data were collected using a combination of observation forms, questionnaires, and system logs. During the assembly phase, completion times, error rates, and task success rates were recorded for each participant. Pre- and post-experiment questionnaires were conducted to assess all participants' knowledge about educational robot assembly and movement control, and their satisfaction on the learning process.

The collected data were analyzed using statistical methods to compare the performance of the two groups. Assembly times were averaged, and error rates were calculated as percentages of incorrect assembly steps.

4.4.1. System Performance

AR contents are rendered on the Microsoft HoloLens 2 devices with a reasonable frame rate. The system delivers a smooth and responsive graphics to enhance the user's experience. Figure 25 shows that the application can render at frame rates of 44-60 FPS with a resolution of 1440x936 pixels per eye.

Figure 25: Frame rates of ASCAT-AR system

4.4.2. Usability

The comparative evaluations from learners, who used the ASCAT-AR system and used instruction manual to assemble and control robot, were conducted to assess system benefits, ease of use, ease of learning, and user satisfaction. Each aspect was rated on a 5-point Likert's scale (1=lowest, 5=highest) by 24 participants.

Table 3: Results of satisfaction survey comparing between the uses of ASCAT-AR system and instruction manual

Learnability	**ASCAT-AR**	**Manual**
I can learn about more parts of the robot.	3.67	4.08
I can perform cooperative task in assembling robots.	4.42	4.75
I want to complete the final robot assembly.	4.83	4.75
I think it took a long time after using this learning tool.	3.58	3.5
Easiness of control		
I find it difficult, and I want to quit.	2.25	2.67
Satisfaction		
I am interested and would like to learn more.	4.17	4.58
How much motivation does the system provide for me to build a robot?	4.17	3.92

Table 3 shows the results of the satisfaction survey comparing the uses of ASCAT-AR system and instruction manual. Scores of learnability shows that the use of ASCAT-AR system can motivate and help the users to assemble robots more successfully than the use of instruction manual. Scores of easiness of control identifies that the use of ASCAT-AR system slightly more difficult than the use of instruction manual since users were just using Microsoft HoloLens 2 for the first time. Finally, users think that the ASCAT-AR system can motivate and help them to assemble and control robot.

4.4.3. Values for Specific Task

To collect the feedback from the experiments, the users were scheduled to perform the task within 2 hours for both of the uses of ASCAT-AR system and instruction manual. Table 4 shows the minimum, maximum, and average of user's robot assembly time for both cases.

Table 4: Time spent on task completion

Groups	**Min time**	**Max time**	**Average time**
ASCAT-AR	0:49:47	1:53:56	1:12:24
Manual	0:59:39	1:40:35	1:18:12

In Figure 26, task completion rate (TSR) is a performance chart used to measure usability and show the percentage of task completion in each step and the system effectiveness of helping users to achieve their goals. The success of the task can be influenced by factors such as user interaction with the interface, overall user experiences, and user motivation. Students using the ASCAT-AR system had a constant percentage success rate from assembly step 1 to final assembly step 8, ranging from 75% to 100%. The results show that students, who used ASCAT-AR system, had a better success rate during step 1 and step 2 than the ones who used the instruction manual with success rate of 33% in task 1.

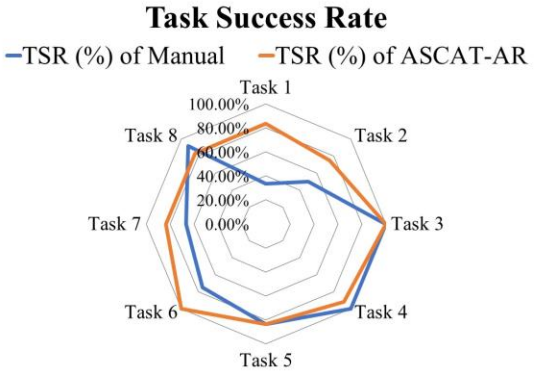


Figure 26: Robot assembly success rate chart

Comparing error rates, students using the ASCAT-AR system assisted robot assembly system had fewer errors than those assembling robots manually. The robot assembly assisted system had a prototype model that could be rotated 360 degrees for a detailed and accurate view of the assembly position, unlike the 2D figures in the manual.

5. Conclusions and Discussions

This research focuses on the development of an ASCAT-AR system using AR technology. Augmented Reality has been developed and applied in various industries, such as education, medicine, tourism, industry, entertainment, and etc [18]. AR technology has the potential to improve the learning experience. It can help the learner to better understand and remember educational content because it allows users to be engaged in learning, which may lead to generate creative teaching methods and better educational outcomes [19]. Currently, efforts and focus on promoting STEM curricula in Thailand have been found, and it has also been found that some teachers have limited knowledge of STEM education and lack of capability of how to integrate STEM into their teaching practices [20]. The proposed system provides AR content that is utilized to comply with the STEM curriculum integrating multiple various subjects. The goal is to equip students with knowledge and understanding of technology and engineering,

enhance their collaborative skills, and foster their interests in applying this competency for future careers. The system specifically helps the development of collaborative skills by engaging students in a collaborative robot assembly task. The system's core hardware consists of the Microsoft HoloLens 2 device and an educational robot. The ASCAT-AR system displays 3D model data and animations to help students explore structures and components in augmented reality. The system is designed with a user-friendly interface that makes it accessible to non-engineering students. The application and the robot can interact in real time, enhancing learning and creating a robot control experience. The study found that students who used ASCAT-AR system were more motivated to complete the robot assembly than the ones who used the manual. Times spent on task completion of two student groups are slightly different. These results may depend on the learning ability of each student. In addition, visualization of 3D models from the ASCAT-AR system assists the user to know the positions of robot parts and sequence of robot assembly more clearly. This increases the success rate of robot assembly.

The evaluation covered all three aspects: system performance, usability, and values for specific tasks. The evaluation results demonstrated that the ASCAT-AR system can increase the user's interests in learning to gain more knowledge and skill about robot technology and programming. Additionally, the robot was found to be easy to control using the ASCAT-AR system. The proposed system not only aids in teaching the users how to program and control the robot but also enhances their understanding of technological concepts and fostering their creativity and collaboration skills.

Furthermore, the improved 3D object detection can improve the current system performance in order to help the user to assemble the robot more easily. The system can be applied to other learning subjects to give users a visualization of the concept.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

We would like to acknowledge the funding from the Program Management Unit for Human Resources & Institutional Development, Research and Innovation (PMU-B)'s AI for All 1-2 projects and the Thailand Science Research and Innovation's Fundamental Fund for research financial supports, and the Human-Computer Interface Lab and Institute of Field Robotics for supporting the facilities and hardware used in this research.

References

[1] B.E. Penprase, "STEM Education for the 21st Century," *Springer International Publishing*, 2020, doi:10.1007/978-3-030-41633-1.

[2] P. Armstrong, "Bloom's Taxonomy," *Vanderbilt University Center for Teaching*, 2010.

[3] B. Bai, H. Song, "21st Century Skills Development through Inquiry-Based Learning: From Theory to Practice," *Asia Pacific Journal of Education*, **38**(4):584–586, 2018, doi:10.1080/02188791.2018.1452348.

[4] A.L.W., K.D.R., A.P.W., C.K.A., R. Mayer, P.P.R., J. Raths, W.M.C., "A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives," 2001.

[5] World Economic Forum, "Schools of the Future: Defining New Models of Education for the Fourth Industrial Revolution," *World Economic Forum Reports*, January 2020.

[6] S. Wachira, L. Deborah, "HANUSCIN and CHATREE FAIKHAMTA Perceptions of In-service Teachers toward Teaching STEM in Thailand," *Asia-Pacific Forum on Science Learning and Teaching*, **18**(2):1, 2017.

[7] J. Garzón, J. Pavón, S. Baldiris, "Systematic Review and Meta-analysis of Augmented Reality in Educational Settings," *Virtual Reality*, **23**(4):447–459, 2019, doi:10.1007/s10055-019-00379-9.

[8] C.E. Hughes, C.B. Stapleton, D.E. Hughes, E.M. Smith, "Mixed Reality in Education, Entertainment, and Training," *IEEE Computer Graphics and Applications*, **25**(6):24–30, 2005, doi:10.1109/MCG.2005.139.

[9] O.B., Gleb; I., "VR vs AR vs MR: Differences and Real-Life Applications," *RubyGarage*, 2020.

[10] T.L. Hutner, V. Sampson, L. Chu, C.L. Baze, R.H. Crawford, "A Case Study of Science Teachers' Goal Conflicts Arising when Integrating Engineering into Science Classes," *Science Education*, **106**(1):88–118, 2022, doi:10.1002/sce.21690.

[11] A. Koolnapadol, P. Nokkaew, P. Tuksino, "The Study of STEM Education Management Connecting the Context of Science Teachers in the School of Extension for Educational Opportunities in the Central Region of Thailand," *International Journal of Science and Innovative Technology*, **2**(June):121–130, 2019.

[12] F.N. Promboon, K.K. Finley, "The Evolution and Current Status of STEM Education in Thailand: Policy Directions and Recommendations," *STEM Education in the Nation: Policies, Practices, and Trends*, Springer Singapore, pp. 423–459, 2018, doi:10.1007/978-981-10-7857-6_17.

[13] S. Sutaphan, C. Yuenyong, "STEM Education Teaching Approach: Inquiry from the Context Based," *Journal of Physics: Conference Series*, **1340**(1):012003, 2019, doi:10.1088/1742-6596/1340/1/012003.

[14] Suriyabutr, J. Williams, "Integrated STEM Education in Thai Secondary Schools: Challenges and Addressing of Challenges," *Journal of Physics: Conference Series*, **1957**(1):012025, 2021, doi:10.1088/1742-6596/1957/1/012025.

[15] E.B. Olson, "Otto: A Low-Cost Robotics Platform for Research and Education," 2001.

[16] O. DIY, "Build Your Own Robot Like a Ninja," *Brno, Czech*, 2021.

[17] G.D. Group, "Try Blockly," *Google*, 2021.

[18] F. Eishita, K. Stanley, "The Impact on Player Experience in Augmented Reality Outdoor Games of Different Noise Models," *Entertainment Computing*, **27**:2018, doi: 10.1016/j.entcom.2018.04.006.

[19] M. Brizar, D. Kažović, "Potential Implementation of Augmented Reality Technology in Education," *2023 46th MIPRO ICT and Electronics Convention (MIPRO)*, pp. 608–612, 2023, doi:10.23919/MIPRO57284.2023.10159865.

[20] S. Pitiporntapin, P. Chantara, W. Srikoom, P. Nuangchalerm, L.M. Hines, "Enhancing Thai In-service Teachers' Perceptions of STEM Education with Tablet-based Professional Development," *Asian Social Science*, **14**(10):13, 2018, doi:10.5539/ass.v14n10p13.

Advances in Science, Technology and Engineering Systems Journal Vol. 9, No. 1, 7-12 (2025)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology 2024-25

ASTESJ

ISSN: 2415 6698

Evaluation of Physicochemical Stability in Extemporaneous Omeprazole-Based Preparations

Ezri Cruz-Pérez[1,2], José Locia-Espinoza[1,2], Joel Jahaziel Díaz-Vallejo[1,2,3], Magda Olivia Pérez-Vásquez[1,2], Luis Morales de la Vega[1], Luz Irene Pascual-Mathey*[1,2],

[1]*Facultad de Química Farmacéutica Biológica, Universidad Veracruzana, Xalapa, 91000, Veracruz, México*

[2]*Maestría en Farmacia Clínica, Universidad Veracruzana, Xalapa, 91000, Veracruz, México*

[3]*Centro de Alta Especialidad "Dr. Rafael Lucio", Xalapa, 91020, Veracruz, México*

ARTICLE INFO

Article history:
Received: 20 November, 2024
Revised: 18 December, 2024
Accepted: 19 December, 2024
Online: 19 January, 2025

Keywords:
Omeprazole
Stability
Extemporaneous preparation

ABSTRACT

Extemporaneous omeprazole-based preparations are commonly used in hospitals; however, there are no validated studies about physicochemical stability. This study aimed to determine if temperature, luminosity, and the type of diluent affect the stability of omeprazole in the extemporaneous preparation. For stability, the methodology validated previously by our group was used. The 2k experimental design included Temperature (25ºC and 35ºC) and Luminosity (covered by light and 400 Lx) variables. Diluents were evaluated at five levels: 1) Citric acid + polyethylene glycol solution, 2) Polyethylene glycol solution, 3) Physiological saline solution, 4) Citric acid + polyethylene glycol solution + physiological saline solution, and 5) Polyethylene glycol solution + physiological saline solution. Minitab 18 software was used for data analysis, and the degradation kinetics were determined by linear regression. The optimal condition for physicochemical stability was a temperature of 25ºC covered by light (OM1-3h 49', OM2-3h 2', SSF-5h 8', OM1SSF-2h 27', OM2SSF-6h 23'). The diluent based on physiological saline solution provided more than five hours of shelf-life, and more than six hours, the diluent based on OM2 + SSF. However, the best option is physiological saline solution, considering the accessibility of the diluent. In conclusion, environmental conditions should be considered in extemporaneous omeprazole-based preparation since they are affected by temperature, luminosity, and type of diluent. Assessing shelf-life prior to administration is necessary to provide a safe and effective drug, avoiding the occurrence of side effects in patients.

1. Introduction

Omeprazole (OMZ) is one of the most widely used drugs in hospitals, increasing its use every year. However, the indiscriminate use of extemporaneous omeprazole-based preparations represents a health risk. Up to 73% of patients who receive omeprazole do not require it, and 38% of these have shown adverse effects, which can prolong their hospital stay [1], [2].

The requirements for evaluating stability are indicated in the NOM-073 "Stability of drugs and medicines, as well as herbal remedies" for determining the shelf-life of medicines as marketed by the pharmaceutical industry [3]. However, in the case of extemporaneous drugs, there is no national regulation; the shelf-life should be determined by the conditions in which the extemporaneous preparation is made. Proper preservation is a prerequisite to maintaining the pharmacological and therapeutic properties. Therefore, it is important to improve safety since it can decrease effectiveness and modify safety due to the toxicity of degradation products [4].

Moreover, information on the stability and storage conditions of extemporaneous preparations is limited since pharmacovigilance is not a common practice in our country. In addition, generally, the unit in charge of performing such activity

*Corresponding Author: Luz Irene Pascual Mathey, Facultad de Química Farmacéutica Biológica, Universidad Veracruzana, Xalapa, C.P. 91000, Veracruz, México, +522281251392, lupascual@uv.mx

https://dx.doi.org/10.25046/aj100102

is the nursing. This can lead to errors, such as inadequate formulation, microbial contamination, concentration, and wrong dose calculation. Therefore, it is essential to evaluate the stability of the drug prior to its administration to patients to avoid the risk of adverse effects or toxicity [5].

The main conditions to retain the physicochemical stability and the microbiological properties within the quality specifications established in the formulation during its shelf-life and throughout storage time, are temperature, humidity, luminosity, and type of diluent [4], [6], [7]. Such variables can accelerate the degradation kinetics of active ingredients and alter their efficacy and safety [2], [3].

The shelf-life of a drug is measured by the concentration of the active ingredient, which should be < 10% of the total dose indicated on the product label. A percentage greater than 10% pointed out that the drug is losing effectiveness. Also, the degradation products could cause adverse or toxic effects on the patients [3], [5], [8], [9], [10], [11].

The 2k design systematizes and reduces the variables to simplify the procedure and evaluates the main effects and their interactions [12]. In 2k factorial designs, the 2 represents the two levels at which each variable is tested, identified as low (-) and high (+). The k represents each of the independent variables. The design (2*2) performs four different experiments; the variables are identified with the letters A and B, and the interaction between these two variables is identified with AB [13], [14].

Additionally, photosensitive drugs need to be kept covered by light due to their characteristics [11]. Those indications are usually mentioned in the package insert or technical data sheet. All photosensitive drugs should be kept in appropriate containers (protected from light) to avoid deterioration, both in the pharmaceutical services and the hospitalization units. Many of them are packaged by the pharmaceutical industry (in topaz glass ampoules) to protect them from light. If this does not occur, they should always be kept in the original package or wrapped in aluminum foil or other opaque paper [11].

In the internal medicine area of a tertiary care hospital in the state of Veracruz, a medication preparation service has been available since 2014, which has allowed a decrease in the adverse effects associated with medication (dosage, preparation, among others). However, there are no stability studies on extemporaneous preparations. Therefore, this study aimed to determine whether the factors of temperature, luminosity, and type of diluent are associated with the stability of omeprazole in extemporaneous preparations.

2. Methods

An experimental study was carried out in the Pharmaceutical Technology Laboratory of the School of Pharmaceutical Biological Chemistry, Universidad Veracruzana, Mexico.

The experimental steps carried out in this study are described in Figure 1.

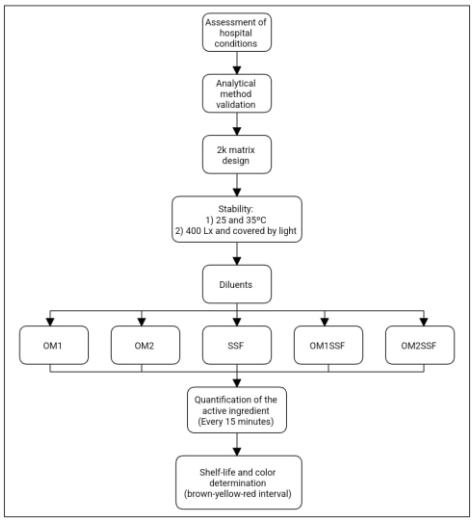


Figure 1: The flowchart summarizes the experimental design used in this study

2.1. Reagents:

The hospital provided two intravenous omeprazole trademarks (OMZ1 lot T18J487 and OMZ2 lot OM18I15). The OMZ reference standard was purchased from Sigma-Aldrich, purity 99.6%, lot LRAC0716, with the supplier's certificate of analysis.

2.2. Analytical equipment:

- UV Spectrophotometer, Beckman, model DU-7000.

- Stove, RIOS Rocha, model HS-33 adapted with 400Lx LED lamp.

2.3. Matrix of 2^k desing:

In this study a factorial design was used, since in each trial or complete replication of the experiment all possible combinations of factor levels were investigated [15]. Factorial designs produce more adequate experiments, since each observation provides information on all factors. Thus, the response to any factor observed under different conditions indicates whether the factors act independently on the experimental units. Interaction between factors occurs when their action is not independent [16].

The independent variables evaluated were Temperature, Luminosity, and Type of diluent. The dependent variable was the shelf-life. We performed a 2^k design to determine the association of factors involved in the stability of the active agent [13], [14]. Analyses were repeated ten times until the concentration of the active in the extemporaneous preparation decreased by more than 10 percent. Temperature includes 25 and 35 degrees Celsius (ºC). Luminosity includes covered by light and 400 Luxes (Lx). The diluent was evaluated at five levels, described in the next section. The variables and their levels are shown in Table 1.

The conditions used in this study were according to standards. The temperature of 25ºC is the optimal for the preparation and storage of non-thermolabile drugs. The second temperature was selected after reviewing the areas of administration of the extemporaneous preparations, with the maximum temperature at

35ºC. Concerning the luminosity, 400 Lx is what a standard hospital lamp provides.

Table 1. Factors and levels included in the 2^k desing.

Factors	Levels	
	Low (-)	High (+)
Temperature	25ºC	35ºC
Luminosity	Covered by light	400 Lx

Lx= luxes.

The proposed design (2^k) defines a total of 4 tests for each evaluation. The combinations used in each test are presented in Table 2.

Table 2. Matrix of 2^k desing

Test	Temperature	Luminosity
1	(-) 25ºC	(-) Covered by light
2	(+) 35ºC	(-) Covered by light
3	(-) 25ºC	(+) 400 Lx
4	(+) 35ºC	(+) 400 Lx

Lx= luxes.

For each diluent, a four-test assay matrix was assigned. The diluent preparation is shown below:

Diluents:

-SSF: Intravenous OMZ diluted with Physiological Saline Solution 0.9%.

-OM1: Intravenous OMZ diluted with its diluent (Solution with Citric Acid + Polyethylene Glycol).

-OM2: Intravenous OMZ diluted with its diluent (Polyethylene glycol solution).

-OM1SSF: Intravenous OMZ diluted with OM1 + SSF (50:50).

-OM2SSF: Intravenous OMZ diluted with OM2 + SSF (50:50).

SSF, OM1, and OM2 are commercial diluents that the hospital provides and used in the internal medicine area. The manufacturers did not indicate the OM1 and OM2 diluent concentrations. A matrix of two hundred determinations was performed considering the design matrix (4 tests), the diluents (5), and the ten sampling times.

Quantification method (Validation and quantification):

The OMZ quantification was previously reported and validated by our working group [17].

Stability:

Physicochemical stability (quantification of OMZ) was performed at the conditions of 25°C ± 2°C and 35°C ± 2°C, with a lamp providing 400 Lx. Samples prepared with the diluents were analyzed each 15 min until the concentration of OMZ decreased > 10% [3].

Color determination

The method was obtained from the analysis 0181 "Solution color" described in the United Mexican States Pharmacopoeia (2014). It is based on the visual color of the sample (in solution) against reference standards in a specific color range under established conditions [18].

The color presented in the sample, will be within the brown-yellow-red interval. A solution is considered colorless if its appearance is the same as that of the water or solvent used to reconstitute it (not more intense than the reference solution B9)

Preparation of standard solutions:

Solutions were prepared as indicated in Annex II of the FEUM "Preparation of reference solutions."

Procedure:

We prepared reference solutions in 10 mL tubes of equal diameters. Then, we transfer 5 mL of the sample of omeprazole preparation to a 10 mL test tube of equal diameter to those of the reference solutions. Compare the sample with the reference solutions in a horizontal plane separated from each other by 3 cm on a white background with indirect light.

3. Results and discussion

Shelf-life

The results of the stability of the drug OMZ in its different extemporaneous preparations are shown in Table 3 and Figure 2, where the shelf-life times (time in hours to reach 10% degradation of the active principle) are presented.

Regarding shelf-life, the optimal condition is covered by light at 25°C (Test 1). According to the literature, this condition prevents the degradation of the active ingredients [19], [20].

The diluents with the best shelf-life times (obtained in all the conditions evaluated) were SSF and OM2SSF (Table 3 and Figure 2).

Table 3. Shelf-life times (hours).

Tests	Diluents				
	OM1	OM2	SSF	OM1SSF	OM2SSF
1	3h 49'	3h 2'	5h 8'	2h 27'	6h 23'
2	01h 4'	01h 16'	02h 25'	01h 10'	01h 22'
3	01h 57'	01h 57'	01h 48'	01h 48'	02h 20'
4	01h 4'	01h 15'	02h 19'	02h 00'	01h 6'

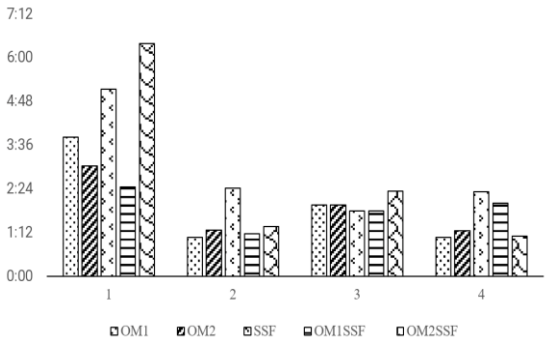


Figure 2. The graph shows the shelf-life of the different conditions (Tests identified from 1 - 4, see Table 2) and the diluents evaluated.

The above results differ from those reported in the Stabilis 4.0 page, which indicates shelf-life times of 6 hours with 5% glucose solution covered by light, without considering the temperature. The values closest to those previously reported are those obtained

for preparations with OM2SSF diluent (06h 23), followed by the preparation with SSF diluent (05h 08) of shelf-life, both at conditions of 25°C and covered by light. The literature indicates that preparations with the SSF-based diluent presents a shelf-life of 12 hours. However, the present study shows lower shelf-life times than previously reported. Those results allow us to point out that it is necessary to verify the shelf-life times reported in the literature and check the operating conditions of each institution center.

In the tertiary hospital where extemporaneous preparations of OMZ are prepared, the shelf-life used is four hours, according to the information indicated in the inserts (at room temperature <no more than 30°C> covered by light).

Concerning the results obtained in this study, the stability conditions recommended by the manufacturers in the insert were not met. For OM1 (diluent with citric acid and polyethylene glycol), under the conditions of 25°C and covered by light, a shelf-life of 03h 49 hours was obtained. For the OM2 solution (diluent with polyethylene glycol), a shelf-life of 03h 02 hours was obtained. On the other hand, the conditions of 35°C and 400 Lx (OM1 and OM2) showed a shelf-life above two hours for both solutions without completing the shelf-life mentioned in the insert.

Figure 3 shows the predictions obtained using the Arrhenius method for the 30°C condition of the diluents of solutions OM1 and OM2, where the comparison with the temperatures of 25°C (circle) and 35°C (triangle), both covered by light, can be seen. The red line on the Y axis indicates 90% of the active; the X axis indicates the time marked on the label of the two drugs (4 hours).

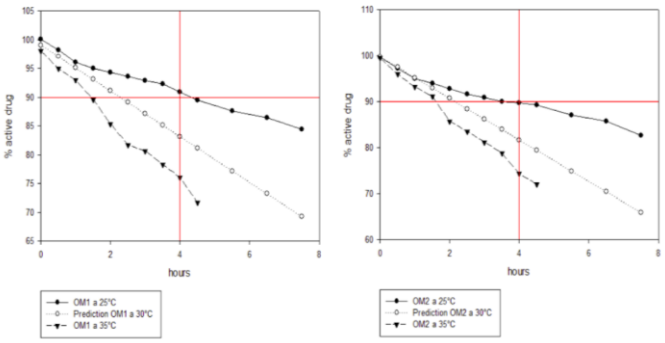


Figure 3. Predicted degradation of omeprazole at 30ºC (lines identified by white circles) compared to 25ºC (lines identified by black circles) and 35ºC (lines identified by triangles) with both diluents (OM1 and OM2). The intersection of the red lines determines the time of 4 hours concerning a concentration of 90% of the active ingredient.

Analysis of main effects (2^k design)

The original design proposed in this study is a 2^k, which considers the variables temperature and luminosity for each diluent analyzed. The results obtained for the main effects and interaction are reported below.

Regarding the analysis of the main effects (Figure 4), the impact of temperature on the shelf-life is more significant in the average variation of response compared to luminosity in the different tests with the diluents, except the SSF where the main effect is luminosity compared to temperature. The plots of the main effects corroborate the significance of each of the diluents tested.

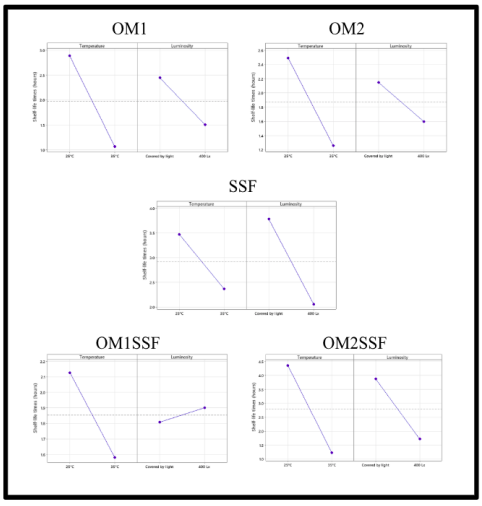


Figure 4: Plots of the main effects. Behavior of OMZ with temperature and luminosity factors in the different diluents.

Regarding the interaction effect, all the diluents present a possible interaction between temperature and luminosity. However, there is a complete interaction in the diluent OM1SSF, corroborated in the interaction graphs in Figure 5.

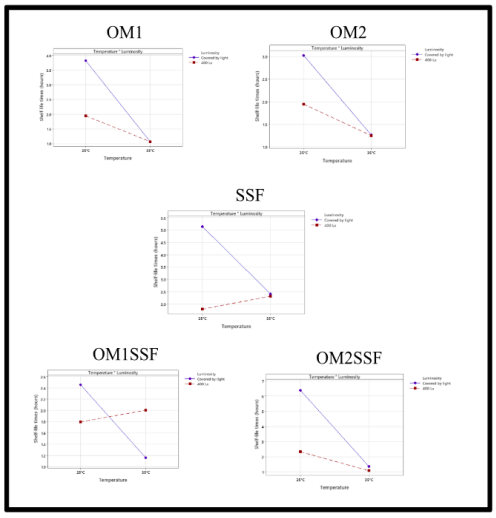


Figure 5. Interaction graphs. The behavior of OMZ concerning the interaction of temperature and humidity factors in the different diluents.

The SSF diluent is the best option for the extemporaneous preparation of OMZ, considering the luminosity, since it is the variable that most affects it. Those will provide better control of the preparation since it is easier to control the luminosity [11].

The diluent least affected by the main effects and by the interaction is the OM2SSF, presenting good shelf-life times. The difficulty of the preparation is the availability of the diluent polyethylene-glycol since its preparation is limited to the manufacturer's availability [7].

On the other hand, the diluent with the greatest variation was the OM1SSF, where temperature and luminosity decreased the shelf-life. This preparation presented the biggest interaction and the lowest shelf-life.

Solution color

Simultaneously to the quantification of the active ingredient, color determinations were made by comparison with standards. The results are presented in Figure 4.

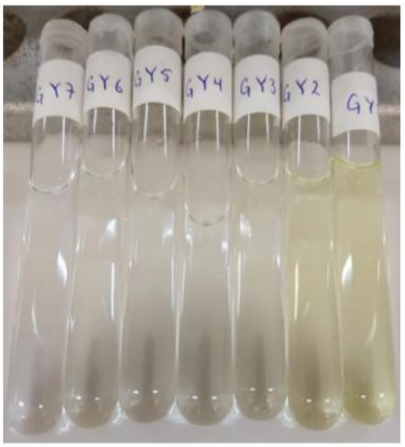


Figure 4. Color standards used for solution color testing. GY = color scale according to pharmacopoeia within the brown-yellow-red interval. GY1 represents the highest intensity.

Omeprazole is a photosensitive drug, so when exposed to light, it shows slight coloration, as evidenced in this test. Tables 4, 5, and 6 show the samples that presented coloration when exposed to 400 Lx. The coloration with the greater intensity was at 25ºC temperature. There were no visual differences between the diluents (OM1 versus OM2, and SSF versus OM2SSF) (Tables 4 and 5) except the OM1SSF mixture (Table 6), which exhibits a coloration that occurs at 25ºC with 400 Lx.

In this analysis, there is no direct relationship between the appearance of color in the preparation and the degradation of omeprazole. However, there is a direct relationship between the color appearance in the solution and the exposure to 400 Lx luminosity. These results suggested a decrease in the appearance of color in extemporaneous preparations of omeprazole intravenous solution.

One of the main limitations of this study is that stability studies could not be performed during storage time; however, the results indicate that pharmacovigilance studies applied to extemporaneous preparations are necessary to inform the nursing department about the correct conditioning of the extemporaneous preparation to provide a safe and effective drug, avoiding the occurrence of side effects in patients [5].

Table 4. Staining of the diluent solution OM1 and OM2.

	T0	T1	T2	T3	T4	T5	T6	T7	T8	T9
25°C – C/L	GY7	GY7	GY7	GY7	GY7	GY6	GY6	GY5	GY4	GY3
35°C – C/L	GY7	GY7	GY7	GY6	GY6	GY6	GY5	GY4	GY4	GY3
25°C – 400lx	GY7	GY7	GY6	GY6	GY4	GY3	GY3	GY2	GY2	GY2
35°C – 400lx	GY7	GY7	GY7	GY6	GY5	GY5	GY4	GY3	GY2	GY2

GY = color scale according to pharmacopoeia within the brown-yellow-red interval. GY1 represents the highest intensity. C/L = cover of light. No difference was observed between solutions OM1 and OM2.

Table 5. Staining of the diluent solution SSF and OM2SSF

	T0	T1	T2	T3	T4	T5	T6	T7	T8	T9
25°C – C/L	GY7	GY7	GY7	GY7	GY6	GY6	GY5	GY5	GY4	GY3
35°C – C/L	GY7	GY7	GY7	GY6	GY6	GY6	GY5	GY4	GY4	GY3
25°C – 400lx	GY7	GY7	GY6	GY6	GY4	GY3	GY3	GY2	GY2	GY2
35°C – 400lx	GY7	GY7	GY7	GY6	GY5	GY5	GY4	GY3	GY2	GY2

GY = color scale according to pharmacopoeia within the brown-yellow-red interval. GY1 represents the highest intensity. C/L = cover of light. No difference was observed between solutions SSF and OM2SSF.

Table 6. Staining of the diluent solution OM1SSF

	T0	T1	T2	T3	T4	T5	T6	T7	T8	T9
25°C – C/L	GY7	GY7	GY7	GY7	GY6	GY6	GY5	GY4	GY3	GY3
35°C – C/L	GY7	GY7	GY7	GY6	GY6	GY5	GY4	GY4	GY3	GY3
25°C – 400lx	GY7	GY6	GY6	GY6	GY3	GY3	GY2	GY2	GY2	GY2
35°C – 400lx	GY7	GY7	GY7	GY6	GY5	GY4	GY4	GY3	GY2	GY2

GY = color scale according to pharmacopoeia within the brown-yellow-red interval. GY1 represents the highest intensity. C/L = cover of light.

4. Conclusion

The stability of the extemporaneous preparation of OMZ - intravenous solution is affected by temperature, luminosity, and type of diluent. Temperature was the variable with the main impact on shelf-life, with the shelf-life at 25°C except for the SSF solution, whose effect was mainly due to luminosity. Regarding luminosity, the optimal condition is preparing extemporaneous solutions covered by light. The optimal diluent for the extemporaneous preparation of OMZ is based on a physiological saline solution due to its longer shelf-life and no commercial brand limitations for its preparation. Concerning the staining of solutions, it is necessary to protect Omeprazole preparations from light, regardless of the diluent used, to ensure the effectiveness and safety of the drug. These conditions are necessary for the good management of omeprazole in the hospital setting, for its suitability for clinical use, and to avoid ineffectiveness and toxic effects associated with its irrational use.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

The authors thank the Centro de Alta Especialidad “Dr. Rafael Lucio” for the support of this work.

References

[1] F. Carranza, “Seguridad del omeprazol: ¿es adecuada la duración de los tratamientos?” Farmacéuticos Comunitarios, **7(1)**: 5–9, 2015, DOI: https://doi.org/10.5672/fc.2173-9218.(2015/vol7).001.02.

[2] Castro, C. M. De Argila, A. Albillos, “Consideraciones prácticas en el manejo de los inhibidores de la bomba de protones,” Revista Española de Enfermedades Digestivas (Madrid), **108**: 145–153, 2016, http://scielo.isciii.es/pdf/diges/v108n3/es_revision.pdf.

[3] Secretaría de Salud, "NOM-073-SSA1-2005, Estabilidad de fármacos y medicamentos," **2005**, https://salud.gob.mx/unidades/cdi/nom/073ssa105.html.

[4] J. R. Falconer, K. J. Steadman, "Extemporaneously compounded medicines," Australian Prescriber, **40(1)**: 5–8, 2017, DOI: https://doi.org/10.18773/austprescr.2017.001.

[5] M. R. Mattos da Silva, D. L. Pereira, E. P. dos Santos, J. E. Ricci, "Preparation of extemporaneous oral liquid in the hospital pharmacy," Brazilian Journal of Pharmaceutical Sciences, **56**: e18358, 2020, DOI: https://doi.org/10.1590/s2175-97902019000418358.

[6] V. K. Yellepeddi, "Stability of extemporaneously prepared preservative-free prochlorperazine nasal spray," American Journal of Health-System Pharmacy, **75(1)**: e28–e35, 2018, DOI: https://doi.org/10.2146/ajhp160531.

[7] N. Barrueco, I. Escobar-Rodríguez, B. García-Díaz, M. E. Gil-Alegre, E. López-Lunar, M. G. Ventura Valares, "Estabilidad de medicamentos en la práctica clínica: de la seguridad a la eficiencia," Farmacia Hospitalaria, **37(3)**: 175–177, 2013, DOI: https://dx.doi.org/10.7399/FH.2013.37.3.587.

[8] M. Yu, J. Qian, D. Guo, L. Li, X. Liu, "Severe adverse reactions caused by omeprazole: A case report," Experimental and Therapeutic Medicine, **12(2)**: 1103–1106, 2016, DOI: https://doi.org/10.3892/etm.2016.344V.

[9] FEUM, "Suplemento para establecimientos dedicados a la venta y suministro de medicamentos y demás insumos para la salud," **6a. Edición**, 2019, México.

[10] E. Casaus, "Guía de buenas prácticas en la administración de medicamentos en servicios de farmacia hospitalaria," Farmacia Hospitalaria, **2024**, https://www.sefh.es/sefhpdfs/GuiaBPP_JUNIO_2014_VF.pdf.

[11] I. Sánchez, M. D. Nájera, A. Espuny, J. C. Titos, "Revisión de la estabilidad de los medicamentos fotosensibles," Farmacia Hospitalaria, **35(4)**: 204–215, 2011, DOI: https://doi.org/10.1016/j.farma.2010.05.005.

[12] A. Correa, P. Grima, X. Tort-Martorell, "Experimentation order with good properties for 2k factorial designs," Journal of Applied Statistics, **36(7)**: 743–754, 2009, DOI: https://doi.org/10.1080/02664760802499337.

[13] J. Lu, "On finite-population Bayesian inferences for 2k factorial designs with binary outcomes," Journal of Statistical Computation and Simulation, **89(5)**: 927–945, 2019, DOI: https://doi.org/10.1080/00949655.2019.1574793.

[14] P. Paengkoum, C. Yuangklang, S. Paengkoum, "Robust 2k factorial designs: non-normal symmetric distributions," Pakistan Journal of Statistics, **77(2555)**: 73–77, 2012, https://avesis.anadolu.edu.tr/yayin/5e5440d7-fa53-4f62-b152-d7f40e35d981/robust-2k-factorial-designs-non-normal-symmetric-distributions.

[15] D. Montgomery, "Diseño y análisis de experimentos," **2a. Edición**, Limusa Wiley, **2010**, México.

[16] L. Kuehl, "Diseño de Experimentos: Principios estadísticos para el diseño y análisis de investigaciones," **2a. Edición**, Thomson Learning, **2001**, España.

[17] E. Cruz, I. Camacho, J. Locia, L. I. Pascual, M. O. Pérez, J. J. Diaz, "Validation of a UV spectrophotometric method for quantification of Omeprazole using different types of diluents," IEEE International Conference on Engineering Veracruz (ICEV), **2023**, DOI: 10.1109/ICEV59168.2023.10329709.

[18] FEUM, "Métodos generales de análisis," **11a. Edición**, **2014**, México.

[19] Secretaría de Salud, "NORMA Oficial Mexicana NOM-249-SSA1-2010, Mezclas estériles: nutricionales y medicamentosas, e instalaciones para su preparación," **2010**, http://www.dof.gob.mx/normasOficiales/4327/salud/salud.htm.

[20] A. Tellez, "Modelo nacional de farmacia hospitalaria," Secretaría de Salud, **2009**, https://www.uaeh.edu.mx/investigacion/icsa/LI_UsoMedic/Ana_Tellez/modelo.pdf.