Counterfeit Currency Detection Through Deep Convolutional Generative Adversarial Network

Salman Jan[1], Fara Gul[2], Mohammad Riyaz Belgaum[3],
Shahid Kamal[4], Afaq Ahmad[5], Muhammad Bilal[6], Atif Khan[7]
Faculty of Computer Studies, Arab Open University – Bahrain, A'ali, Kingdom of Bahrain[1, 3]
Bacha Khan University, Charsadda, Pakistan[2]
Center for Advanced Analytics-CoE for Artificial Intelligence-Faculty of Computing and Informatics, Multimedia University, Cyberjaya, 63100, Selangor, Malaysia[1, 4]
Department of Computer Science, Institute of Management Sciences, Peshawar, Pakistan[5]
Department of Computer Science, Islamia College University, Peshawar, Pakistan[6, 7]

***Abstract*—Worldwide, individuals, businesses, and economies are being affected by counterfeit currency significantly. Numerous models generate content that mimics the original, and existing solutions fall short in detecting the difference between real and fake. This study presents a detection system using three deep learning models: Deep Convolutional Generative Adversarial Network (DCGAN), Convolutional Neural Network (CNN), and Fully Connected Neural Network (FCNN). The proposed study also identifies patterns that contribute to real and fake currency when the models are trained on the data. After training the models, the proposed solution receives an accuracy of 95 per cent, an F1 Score of 0.957, 0.95 as precision, and 0.954 as recall. This study further carries out a comprehensive analysis of existing models and compares them with the proposed solution to determine the effectiveness of the solution and further recommend its implementation in real-world applications. The proposed solution contributes to the widespread adoption of the application across smart devices and further ensures a robust solution for the detection of counterfeit money.**

Keywords*—CNN; counterfeit; DCGAN; Fake Money; FCNN; fraud detection

I. Introduction

Counterfeiting pertains to the unlawful replication of a specific object, notably the currency of its original form. The repercussions of counterfeit currency can be detrimental to an economy, causing an upsurge in prices, fostering black market activities, influencing trade, business transactions, and administrative operations [1]. Currency counterfeiting persistently poses a formidable challenge to the financial systems of nations [2]. It involves the illicit replication of the official currency, hence lacking the authorization of the government, and poses a substantial menace to the global economy [3]. The production of counterfeit currency, also referred to as counterfeit money, is universally illegal since it transpires without the sanction of the central bank or the governing authority. The history of counterfeit currency traces back to antiquity, emerging nearly simultaneously with the inception of currency itself. It stands as one of the world's oldest illicit professions, even predating Lydian coins. The Lydian Stater, which predated the fall of the Lydian Empire to the Persian Empire, represented the inaugural instance of an officially issued coin by a government in recorded history [4]. Counterfeit coins, known as Fourree, were crafted by amalgamating base metals with pure gold or silver.

Modern approaches to discern genuine from counterfeit currency primarily rely on advanced image processing techniques. These methods encompass image acquisition, edge detection, feature extraction, image segmentation, and decision-making processes. Noteworthy security features include watermarks, concealed images, security threads, and optically variable inks [5]. However, the primary limitation of these approaches lies in their suboptimal detection efficiency, particularly regarding feature extraction [6]. To surmount this challenge, deep learning methodologies have emerged as compelling solutions. These techniques deploy multi-layer neural networks to facilitate the detection of counterfeit currency. While increasing the layers in neural networks can lead to greater complexity and higher error risks, convolutional neural networks (CNNs) offer a promising alternative [7]. Unlike fully connected layers, CNNs use filters that focus on important aspects of input data, scanning across the entire input data space to extract relevant features for specific tasks. CNNs are known for their power and efficiency, especially compared to traditional deep neural networks. In today's technologically advanced world, it has become easier to produce counterfeit currency without legal authorization, significantly impacting a nation's economy. The Malaysian Ringgit (MYR), issued by Bank Negara Malaysia (BNM), is particularly vulnerable to counterfeiting, especially in denominations of MYR 1, MYR 5, MYR 10, MYR 20, MYR 50, and MYR 100. In the field of computer science, many machine learning algorithms have been proposed for image processing. These methods detect and recognize currency notes by analyzing specific attributes such as color, shape, paper width, and image filtering.

In this study, three deep learning models were employed to develop an effective counterfeit currency detection system: Convolutional Neural Network (CNN), Fully Connected Neural Network (FCNN), and Deep Convolutional Generative Adversarial Network (DCGAN). CNNs are widely recognized for their ability to process and analyze images by automatically extracting meaningful features through multiple layers, making them as potential for visual recognition tasks. FCNNs complement this process by utilizing fully connected layers to perform accurate classification based on the features extracted from the input data. To further enhance detection performance, the study incorporates DCGAN, an advanced deep learning framework within the field of generative artificial intelligence. DCGAN consists of two interconnected components: a Generator and a Discriminator. The Generator learns the underlying patterns of genuine currency notes and produces realistic synthetic samples, while the Discriminator evaluates these samples and distinguishes between authentic and generated data. Through this adversarial learning process, the model becomes highly effective at identifying subtle characteristics of counterfeit currency, leading to improved detection accuracy and robustness.

A. Motivations and Research Gap

The problem of counterfeit money continues to pose a challenge and threat in the economic world. Traditional methods of counterfeit detection, such as manual inspection and simple image processing techniques, have proven inadequate in keeping up with the sophisticated techniques employed by counterfeiters [8]. This research aims to fill the gap by leveraging advanced deep learning techniques to enhance the detection accuracy and reliability of counterfeit currency identification. Specifically, the existing challenges and gaps that our research addresses include:

- Inefficiency of Traditional Methods: Traditional methods of counterfeit detection are labor-intensive and prone to errors, particularly in the case of high-quality counterfeits.
- Lack of Robustness in Existing Models: Previous models lack the robustness required to detect subtle variations and sophisticated counterfeiting techniques.
- Integration of Security Features: While some methods incorporate security features, they fail to ensure the integrity and traceability of detection results.
- DCGAN was selected because access to diverse counterfeit currency samples is limited. The generator produces synthetic counterfeit-like variations, while the discriminator learns to distinguish subtle visual differences between genuine and generated samples. This adversarial training exposes the discriminator to a broader range of counterfeit patterns than conventional supervised training alone. CNN and FCNN were included as baseline discriminative models for comparison.

B. Problem Statement

The presence of counterfeit currency causes negative impacts on the economy of the nation, which can lead to inflation and losses, both to the country and its people. In addition, this leads to distrust of the integrity of the currency, especially when conducting business. Upon careful analysis of the various methods that have been put in place to differentiate between the two, it becomes clear that traditional methods have been used before.

However, the counterfeiting technique has advanced to such a degree that the changes introduced into counterfeit notes escape detection through conventional machine learning methods. In this regard, in this study, deep learning algorithms have been employed on the basis that they can detect complex patterns in better ways. The problem is solved through the introduction of a strong system for counterfeit money detection. The proposed approach should be quite efficient to meet the needs of governments, financial organizations, companies, retailers, and even customers in distinguishing real currency from counterfeit currency. Consequently, the following noteworthy contributions have been made throughout the development of the proposed solution.

C. Contribution

This study proposed a framework for counterfeit currency detection which can help government agencies and banking sectors to distinguish genuine currency from counterfeit currency in an expedited manner. The contribution of this study is provided below:

- Novel Deep Learning Framework: This research presents an extensive framework for counterfeit currency detection based on advanced deep learning models such as DCGAN, CNN, and FCNN. Specifically, the DCGAN model performs better in recognizing counterfeit notes by capturing complex patterns that other models find hard to detect.
- Cross-Currency Applicability: The system proposed is not specific to any one currency. It has been effectively used to detect counterfeit Malaysian Ringgit (MYR) and Saudi Arabian Riyal (SAR). It can be extended to other currencies with minor adjustments in training.
- Performance Superiority: The proposed approach based on DCGAN achieves better accuracy, precision, recall, and F1 score compared to other existing methods, with 95.11% accuracy, 0.95 precision, 0.954 recall, and 0.957 F1 score. A comparative analysis with previous work clearly demonstrates the superiority of our method.
- Cost-Effective and Scalable: The framework is designed to be inexpensive and scalable, providing a robust solution for large-scale counterfeit detection and easy integration with smart devices and financial systems.

This research study is structured as follows: The study opens with a short overview of the work that was done in Section I. Section II offers an in-depth review of related work in the field and discusses its strengths and weaknesses. Section III shows how the authors addressed the gap as part of methodology. Section IV presents experiment settings followed with the experimental results and discussion drawn from all experiments using the proposed framework in Section V. Section VI presents a complete set of conclusions and recommendations and finally drafting the future work is presented in Section VII.

II. Related Work

The authors in [9] developed a system based on image processing techniques, utilizing OpenCV (CV2), Support Vector Machine (SVM) classifier, and other machine learning algorithms to extract image features. They compared these features with the genuine characteristics of banknotes. They effectively employed CNN to detect counterfeit currency.

An innovative approach to counterfeit currency detection using transfer learning was introduced by the authors in [10]. They employed AlexNet as a pre-trained model, consisting of convolutional layers, max-pooling layers, dropout layers, ReLU activations, and fully connected layers. To facilitate transfer learning, they removed the last three fully connected layers of AlexNet and adjusted it with weight and bias learning factors to extract latent features from currency images. Their training set was comprised of currency note images, augmented with 100 variations per image by altering the size and orientation, thereby increasing dataset diversity. The increased images were placed in folders according to the corresponding labels. The authors achieved average accuracy rates of 81.5% for genuine currency and 75% for counterfeit currency.

Kumar et al. [11] proposed a robust system for detection of counterfeit Indian rupee notes using ORB (Oriented FAST and Rotated BRIEF) and OpenCV's Brute Force matcher. Their system was based on digital image acquisition, grayscale conversion, edge detection, image segmentation and feature extraction. It has two modules, one is to extract security features and create database and other is to authenticate images from the test dataset. They achieved a significant average accuracy of 95.0% indicating the system is cost effective.

Pachon et al. [12] used artificial neural networks (ANNs) for banknote authentication. For their research they took data from specially created images for the purpose of improving currency classification accuracy with the help of Back Propagation algorithm. Their suggested procedure was image acquisition, conversion to grayscale, wavelet transformation, image segmentation, and classifier application. But they provided no details on implementation, results or average accuracy metrics.

In [13], Chandrappa et al. suggested a methodology for extracting critical information from the images of counterfeit money using bit plane slicing. This was done by decomposing 256 grayscale images into eight binary images, each representing different bit planes and applying edge detection techniques. They found that the sixth and seventh bit planes greatly improved edge and hidden element detection in the images. The methodology was implemented using image processing toolbox in MATLAB.

Teymournezhad et al. [14] proposed a system that combines image processing techniques and a deep learning network named GoogLeNet. The proposed work utilized the pre-trained GoogLeNet. It demonstrated high accuracy in detecting the security features of the genuine banknotes but low accuracy for the counterfeit samples. Image preprocessing steps consist of scaling, noise removal, sharpening, brightness adjustment, image segmentation and corner recognition. A 22-layer GoogLeNet was used for object recognition across a wide range of classes. The system was implemented in MATLAB R2018b on a Windows 7 platform.

Chowdhury et al. [15] proposed an automated authentication model using irregular color particles under UV light with UV ink as a security feature. The model achieved an accuracy of 96.3%. They used Region Proposal Network Stages (RPNs) to estimate quickly the regions of interest of different scales and aspect ratios.

Nur Farah et al. [16] used video spectral comparator (VSC), ATR-FTIR for chemical profiling and PCA for pattern recognition to differentiate genuine from counterfeit banknotes. Their methodology involved sample collection, physical and optical examinations, IR spectra acquisition, pattern recognition application, and PCA. However, their study lacked implementation, accuracy, and conclusive findings.

The authors in [17] used generative adversarial networks (GANs) for detecting fraudulent currency. GANs employed unsupervised learning to make supervised predictions, demonstrating high precision with an expanded image dataset. Their study included various deep learning models, achieving an accuracy rate of 80%. They highlighted the potential for enhancing accuracy with multi-class classifiers.

A standard currency identification system that makes use of edge detection, feature extraction, image segmentation, acquisition, grayscale transformation, and comparison was developed by Bandu et al. [18]. The research made use of CNN for pattern and image recognition, and suggested the use of SHA as an identifier for counterfeit currency depending on its physical characteristics. Nevertheless, the authors did not give system implementation and accuracy evaluation.

Nasayreh et al. [19] used different CNN architectures for identification of fake Jordanian bank notes and obtained competitive levels of accuracy using optimized AlexNet and GoogleNet models. The modifications in VGG16 resulted in maximum accuracy of 99.88%. Their approach can be implemented in automated payment systems and mobile currency checking. Aulia et al. [20] showed the recognition and classification of paper currency for Saudi Arabian Riyal denominations using Geometric Template Matching and Grayscale Template Matching techniques.

III. Methodology

This section presents the proposed methodology for detection of counterfeit currency, as shown in Fig. 1. The proposed framework is composed of the following components:

- Dataset
- Generator
- Latent Space
- Discriminator
- Fine-tuning

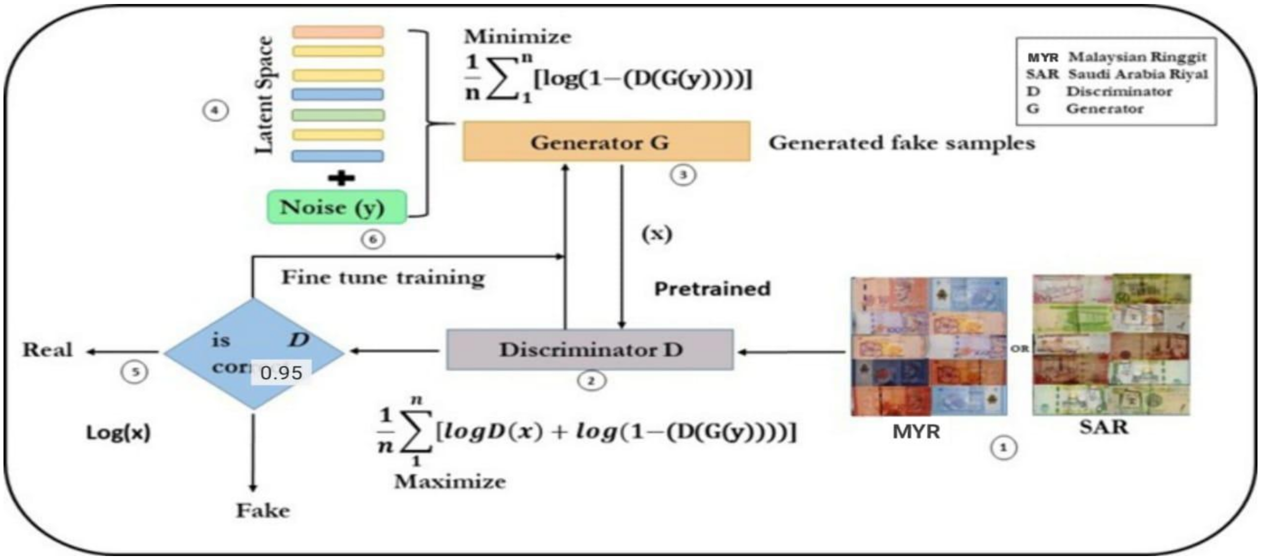

Fig. 1. Proposed framework for counterfeit currency detection using DCGAN.

A. Dataset

In this model, the system is designed to accept input data in the form of Malaysian Ringgit (MYR) and Saudi Arabian Riyal (SAR) currency notes. The dataset used in this study consisted of 15,148 images of Malaysian Ringgit (MYR) and Saudi Arabian Riyal (SAR) currency notes, including both genuine and counterfeit samples. The genuine images were taken using a phone, while counterfeit samples were generated using the generative component of the DCGAN. All images were resized to 128 × 128 pixels and converted to RGB format before training. The dataset was divided into 80% training data and 20% testing data, with 20% of the training portion used for validation. The class-wise distribution of genuine and counterfeit images should also be reported. However, it is important to note that this system can be adapted to verify the authenticity of currency notes from any denomination if it undergoes proper training with an adequate dataset. The flexibility of this solution allows for its application to various currencies by ensuring the model receives appropriate training. It's worth noting that there is no access to individuals involved in the production of counterfeit currency. Hence, an artificial function is employed to generate simulated counterfeit currency samples. These synthetic samples are utilized as representations of counterfeit currency notes and are generated by a dedicated algorithmic generator.

B. Generator

The framework employs the DCGAN model, originally proposed by Radford et al. [21], which has shown remarkable capabilities in generating realistic data samples and improving classification tasks. The DCGAN generator component generates fake samples by using latent space. A generator uses a mathematical formula and gives input in the digital form of the currency. The fake samples produced by the Generator are sent to Discriminator.

C. Latent Space

The latent space is like a database in which currency notes along with some noises are added in the digital form. With latent space, the generator gives output in the digital form of the currency. In this way, we have real and fake currency.

D. Discriminator

The discriminator's main function is to evaluate whether a currency sample, generated by a dedicated generator, is genuine or counterfeit. This is achieved through a training process where the discriminator learns to distinguish between real and fake currency notes. The system works accurately when the discriminator correctly identifies a genuine note as real and a counterfeit note as fake. If the discriminator incorrectly classifies a genuine note as counterfeit, corrective measures are taken to improve its performance. This fine-tuning process aims to enhance the discriminator's accuracy in differentiating between real and fake currency. The goal is to minimize the probability of the generator's output being mistaken while maximizing the discriminator's accuracy. In practice, the discriminator should aim for a probability of 1 when assessing genuine notes, indicating a correct decision. Conversely, a probability of 0 indicates an incorrect judgment. Therefore, the objective is to reduce the number of such erroneous classifications.

E. Fine-Tuning

Fine-tuning is a critical step in transfer learning, involving the adaptation of pre-trained model weights to new data instances. When the discriminator incorrectly identifies genuine currency as counterfeit, it indicates an error in its decision-making. To address this, a fine-tuning process is initiated to improve the discriminator's accuracy. This corrective procedure enhances the discriminator's ability to accurately distinguish between authentic and counterfeit currency notes, thereby increasing its overall proficiency.

IV. Experimental Settings

To provide a comprehensive understanding of the methodology and facilitate reproducibility, a detailed information about the models and settings employed in the proposed work are presented. The DCGAN model architecture consists of two main components: the Generator and the

Discriminator. The Generator starts with a 100-dimensional noise vector as input. It includes a dense layer with 128 units, utilizing ReLU activation and batch normalization to stabilize the learning process. This is followed by upsampling layers, which are paired with Conv2DTranspose layers. These layers have filters of sizes 128, 64, and 32, with a kernel size of 5x5, strides of 2x2, and 'same' padding, all using ReLU activation. The last layer of the Generator is a Conv2DTranspose layer which generates the output as RGB images of size 128x128x3, with a 5x5 kernel, 1x1 strides, 'same' padding, and tanh activation. After each Conv2DTranspose layer, dropout layers with rate 0.3 are used to prevent overfitting.

The Discriminator on the other hand takes as input 128x128x3 RGB images. It consists of Conv2D layers with filter sizes of 32, 64 and 128. Kernel size is 5x5, stride is 2x2 and padding is 'same'. These layers use LeakyReLU activation with a slope of $\alpha=0.2$ which allows a small gradient when the unit is not active. After each Conv2D layer, the research added a dropout layer with a rate of 0.3 to further regularize the model. Finally, the Discriminator ends with a dense layer with 1 unit and sigmoid activation to output the probability of the input image being real or fake. For training, the model is run for 10 epochs with a batch size of 128. The research uses the Adam optimizer with learning rate 0.0002 and decay rate $\beta=0.5$. The Generator and Discriminator are using binary cross entropy for their loss functions. The loss functions tell your model what to learn.

A. Test Bed Environment

This study focuses on the experimental setup for training a DCGAN. The training was carried out on a GPU based machine at the Cyber Security and Technological Convergence department, Malaysian Institute of Information Technology, University Kuala Lumpur. The architecture used Keras with TensorFlow as a backend. The Keras library was used with several components such as dense layers, the dropout technique, activation functions, and flatten options. The dense layer was employed to tune the filters to detect the various attributes of the currency notes under examination.

The dropout method helped to reduce overfitting and remove extraneous features that did not add to the proper labeling and the real look of the notes. The “ReLU" activation function was chosen and it was responsible for clipping the input values in the range of 0 to 1. The datasets consisted of the real and counterfeit currency samples which were used to train DCGAN, CNN, and FCNN. The DCGAN framework consisted of two simple components, the Discriminator (D) and the Generator (G). These components were trained with a learning rate of 0.0002. Specifically, the training process is to update the discriminator, then update the generator twice. In this way the discriminator was prevented from minimal loss.

The results of the learning process were generated and well documented. A specific hardware and software environment was required for the development of the proposed framework. The primary memory capacity used in this study was 16 GB with GPU-supported hardware, including the NVIDIA P100 Kernel. All the experiments were performed on the Linux Operating System. With a minimum system configuration of Intel(R) Xeon(R) processor with a clock speed of 0.82 GHz to 1.59 GHz, 2 cores, and 16 GB memory, the experiments are reproducible.

B. Training of Deep Learning Models

During the training of the models, the dataset was divided into three separate datasets: a training set, a validation set, and a test set. The details are provided as follows:

1) Training set: It is the first dataset, used to train the model to learn the complex features of real currency notes in each iterative step. This immersive training allows the model to make accurate predictions when faced with totally new, never-before-seen data. In this work, the dataset is split into 80% training set and 20% test set.

2) Validation set: The validation set is a subset of the training set that is set aside from the training set during each epoch of training. During the training, the model is validated with data from this set. The division of training and validation data enables the model to learn from training data and test the model on the validation set. Importantly, this validation process provides insights that can be used to tune the hyperparameters. The model then classifies and evaluates each input of the validation set during training based on the acquired knowledge of the training set. In this work, 20% of the training data is used as the validation data.

3) Test set: After training and validating the models, they can be applied to predict results for the data of the test set. The 20% test set, not to be used in the training or validation set, is held for the final evaluation of the model. The test set should preferably have no labels and serve as an unbiased evaluation of the predictive ability of the model. The training and validation sets, however, are annotated, making it easier for the model to learn.

V. Results and Discussion

This section presents details of classification results obtained after training deep learning models on real and fake currency notes. The following subsections outline the various performance indicators of the employed models.

A. Performance Analysis of Employed Models

Metrics used in performance evaluation include accuracy, recall, precision, and F1 scores. These measures are critical in measuring the efficiency of different deep learning models used in the study. The study involves the exploration of different parameters that will help in converging to get accurate results. The normal confusion matrix is composed of four categories that include false negative, false positive, true positive, and true negative. In this particular study, “positive" refers to fake currency, whereas “negative" refers to the real currency. For the DCGAN model that analyzed 15,148 images, there were two categories under consideration – positive and negative. Conversely, in the Positive case, the predicted negative instances amounted to 350, with 7,802 predicted positive instances. Notably, DCGAN exhibited the most favorable results among all models.

The CNN model also processed 15,148 samples, however, the negative case resulted in 5,800 predicted negative currency notes and 1,696 predicted positive instances. In the positive case, there were 1,648 instances of predicted negative currency notes and 6,004 predicted positive instances. Finally, examining the

FCNN model, with the same dataset of 15,148 samples, the negative case yielded 5,528 predicted negative currency notes and 2,757 predicted positive instances. In the positive case, the predicted negative instances totaled 2,535, with 4,328 predicted positive instances.

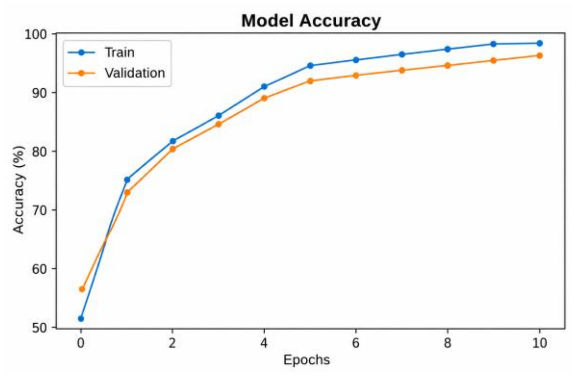

Fig. 2. Accuracy of the DCGAN model.

Fig. 2 shows the trend of the model's accuracy for the DCGAN model. The blue line represents the training trend, while the orange line shows validation accuracy. The figure shows that both the training and validation accuracies are improving with each epoch and finally reach 95%.

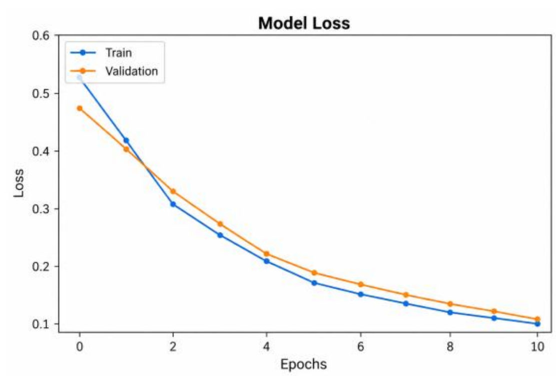

Fig. 3. Loss of the DCGAN model.

Fig. 3 represents the loss function of the model. It is clear from the graph that the loss of training and validation is decreasing after each epoch. Overall, the models represent a good fit.

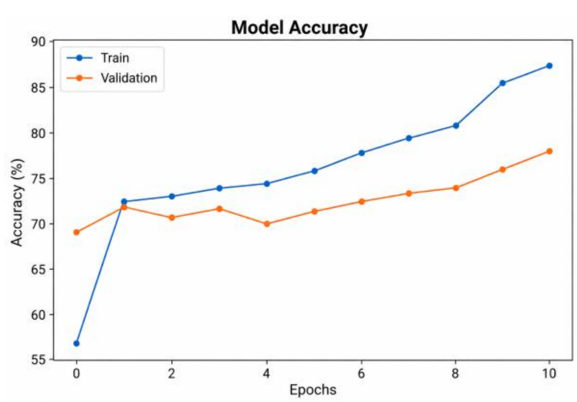

Fig. 4. Accuracy of the CNN model.

Fig. 4 represents the accuracy of CNN model in detecting the Counterfeit currency. It is evident from the above trend that validation accuracy is not improving as training accuracy does. Validation accuracy starts from 70% and after fluctuation reaches to 77%.

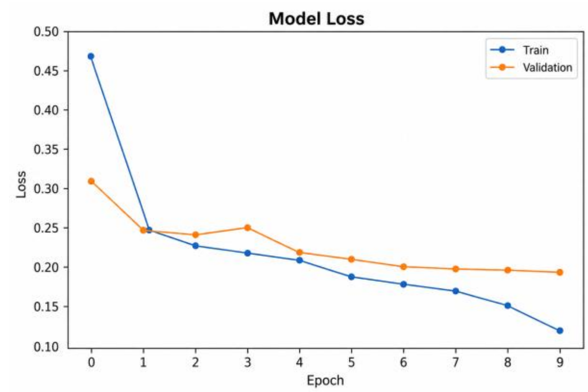

Fig. 5. Loss of the CNN model.

Fig. 5 shows the loss of CNN model. The training loss is constantly decreasing and reaches to 0.1 while validation loss is not decreasing as such. Overall, the model does not reflect a good fit.

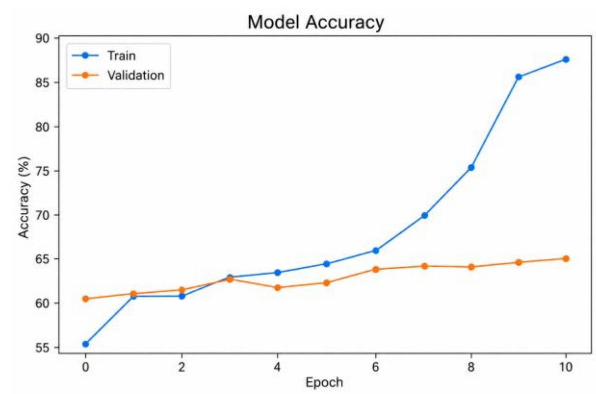

Fig. 6. Accuracy of the FCNN model.

Fig. 6 represents the accuracy trend of FCNN model. The trend indicates that training accuracy is improving with each epoch, however, the validation accuracy is not improving as such.

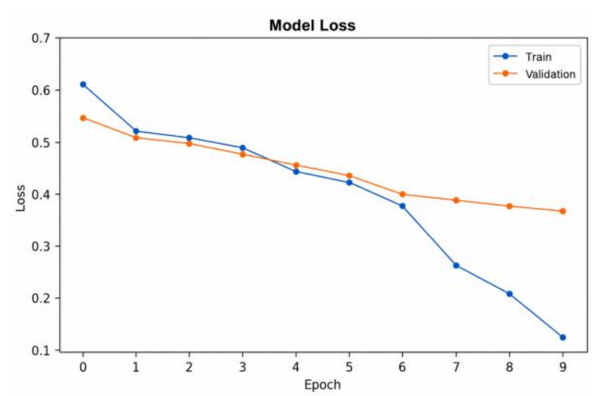

Fig. 7. Loss of the FCNN model.

Fig. 7 shows the loss function of FCNN. The training loss is decreasing constantly and reaches to 0.1 from 0.6. On the other hand, validation loss initially decreased and then remained stagnant. Overall, the mode seems to be overfitting.

The confusion matrix for DCGAN, CNN and FCNN is provided in Table I.

TABLE I. CONFUSION MATRIX OF THE DCGAN, CNN AND FCNN MODELS.

Model	Cases	Predicted Negative	Predicted Positive
DCGAN	Negative Cases	6606	390
	Positive Cases	350	7802
CNN	Negative Cases	5800	1696
	Positive Cases	1648	6004
FCNN	Negative Cases	5528	2757
	Positive Cases	2535	4328

The results of employing the state-of-the-art deep learning approaches to classify real and fake currency is depicted in Fig. 8.

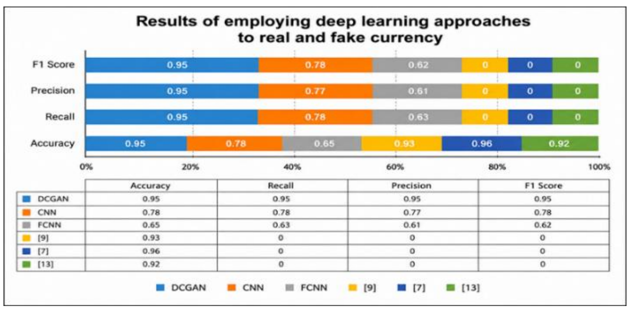

Fig. 8. Results of deep learning approaches to detect genuine currency.

B. Real-Time Complexity Analysis of the Proposed Approach

The proposed counterfeit currency detection framework leverages DCGAN, CNN, and FCNN. The real-time performance of these models is influenced by several factors, including the model's architecture, the size of the dataset, and the computational resources available.

1) DCGAN Complexity:

a) Training complexity: The DCGAN architecture consists of a Generator and a Discriminator, both of which are optimized concurrently during training. The time complexity of training the model depends on the size of the input image (n), the number of layers (L), and the number of parameters in each layer. Given that backpropagation is performed for both the Generator and Discriminator in each epoch, the overall training complexity can be approximated as O(2×n×L).

b) Inference complexity: During inference (real-time detection), the complexity is significantly reduced since only the Discriminator is used to classify an image as genuine or counterfeit. For a DCGAN with L layers, the inference complexity is approximately O(n×L), making it feasible for real-time applications.

2) CNN and FCNN complexity:

a) CNN complexity: CNNs rely on convolutional operations that have a time complexity of O(k×n2×m2), where k is the size of the filter, n×n is the size of the input image, and m×m is the size of the output feature map. While training a CNN is computationally expensive, involving multiple convolutional and pooling layers, inference complexity is relatively low. This makes CNNs suitable for real-time detection scenarios).

b) FCNN complexity: FCNN models, with their fully connected layers, have a time complexity of O(n2×L), where n is the number of neurons in the layer and L is the number of layers. While FCNNs offer high accuracy, they may be less efficient than CNNs and DCGANs in terms of real-time performance due to the fully connected layers, which introduce higher computational demands.

3) Real-time feasibility: For real-time applications, the key factor is inference time. DCGAN's Discriminator, once trained, has a low inference complexity, which makes it well-suited for real-time currency detection. CNNs also offer efficient inference with low latency, though FCNNs may introduce slightly higher inference times due to their dense architecture.

4) Overall real-time performance: While training deep learning models like DCGAN, CNN, and FCNN can be computationally intensive, the real-time complexity for detection (inference) is significantly lower. DCGAN, in particular, offers a balance between accuracy and efficiency, with real-time classification complexity at O(n2×L), making it ideal for deployment in environments where rapid and accurate counterfeit detection is required. As mentioned earlier, the research conducted experiments using a system configuration consisting of an NVIDIA P100 GPU, 16 GB of memory, and an Intel Xeon processor.

Given the DCGAN model's architecture and the number of image samples (15,148), the training time for the DCGAN model was approximately 3-4 hours for 10 epochs with a batch size of 128.

C. Model Accuracy

The experimental results demonstrated that DCGAN obtained a highest accuracy of 95% in detecting counterfeit currency. The accuracy rate is determined using Eq. (1):

$$Accuracy = \frac{Number of correctly identified samples}{Total number of samples} \quad (1)$$

The accuracies of various models employed are presented in Fig. 9.

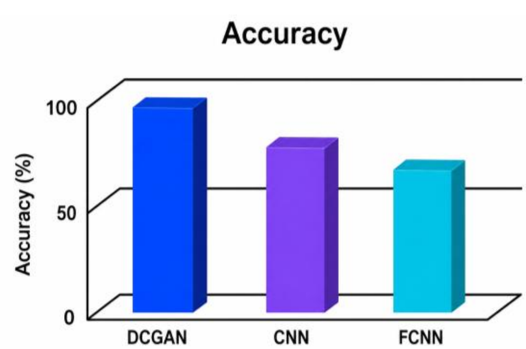

Fig. 9. Accuracy obtained by various models.

D. Recall

The recall metric is employed to measure the performance of the algorithm for recognizing the positives, as illustrated by Eq. (2). The True Positives (TP) refer to the total number of cases which were correctly predicted by the model to be positive (counterfeit currency), while the False Negatives (FN) denote those cases which have been wrongly recognized as negatives (genuine currency).

$$\text{Recall} = \frac{TP}{TP+FN} \tag{2}$$

Recall obtained by different models is presented in Fig. 10. It is evident that DCGAN surpassed other models in terms of recall.

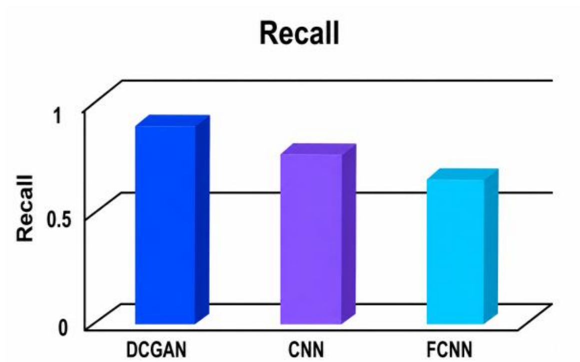

Fig. 10. Recall obtained by various models.

E. Precision

This is the measure that is used to determine the precision of the model's positive predictions, as seen in Eq. (3). The measure is used to find the fraction of true positive predictions among all the positive predictions made by the model. True Positive (TP) is the number of correct positive predictions and False Positive (FP) is the number of wrong positive predictions, where the model predicted a positive outcome (counterfeit currency), but the actual outcome was negative (genuine currency).

$$Precision = \frac{TP}{TP+FP} \tag{3}$$

The Precision obtained by different models is presented in Fig. 11. It is evident that DCGAN surpassed other models in terms of precision.

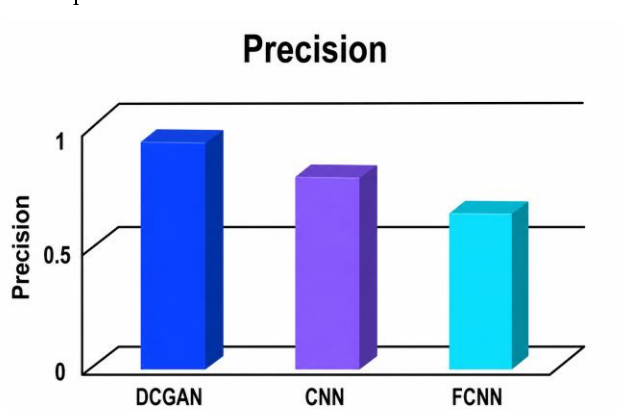

Fig. 11. Precision obtained by various models.

F. F1-Score

F1-score is widely used to evaluate performance of machine learning classifiers including those used for natural language processing applications and search engine algorithms among others [14]. The F1 score is calculated to find a balance between recall and precision. Mathematically F1 Score is calculated using Eq. (4):

$$F1 - Score = 2\frac{(Pr\,ecision \times Re\,call)}{(Pr\,ecision + Re\,call)} \tag{4}$$

The F1-score obtained by different models is depicted in Fig. 12. The results showed that DCGAN outperformed other models in terms of F1-score.

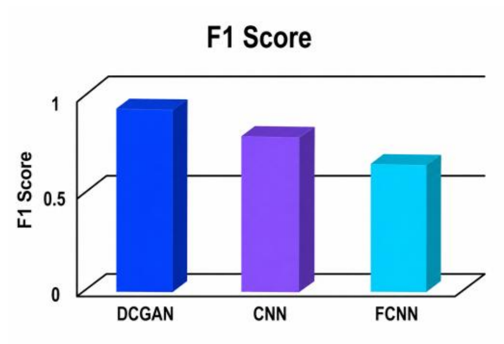

Fig. 12. F1-Score obtained by various models.

G. Comparison with Baseline Methods

To benchmark the performance of our proposed DCGAN-based approach, this research compared the results with those reported in the study by [14], which also employed GAN for counterfeit currency detection. The comparison is summarized in Table II, highlighting the superior performance of our method in terms of accuracy, precision, recall, and F1-score.

TABLE II. COMPARISON WITH BASELINE METHODS

Method	Accuracy	Precision	Recall	F1-score
Proposed DCGAN	0.951	0.950	0.954	0.957
Ref. [10]	0.815 / 0.750*	NR	NR	NR
Ref. [11]	0.950	NR	NR	NR
Ref. [15]	0.963	NR	NR	NR
Ref. [17]	0.800	NR	NR	NR
Ref. [19]	0.9988	NR	NR	NR

NR: Not reported. *Ref. [10] reported 81.5% accuracy for genuine and 75.0% for counterfeit notes.

H. Limitations of Proposed Framework

The proposed framework shows significant improvements in the detection of counterfeit currency, but has the following limitations:

1) Potential vulnerabilities to adversarial attacks: Deep learning models, e.g. DCGAN, are vulnerable to adversarial attacks. The system can be fooled by slight modifications to counterfeit notes. Future work should study how to defend the model against such attacks.

2) Requirement for large and diverse datasets: The performance of the proposed framework depends on the availability of large and diverse datasets. The dataset utilized for this research is extensive yet not exhaustive of all counterfeit currencies. The dataset can be expanded to include a wider range of counterfeit samples which may increase the performance of the model.

3) Lack of component-wise ablation analysis: The proposed framework combines synthetic image generation, discriminator-based classification, and image preprocessing. However, the present evaluation reports the performance of the complete framework and does not separately measure the contribution of each component. Therefore, the individual impact of synthetic sample generation, discriminator learning, and preprocessing remains a limitation of the current study. Future work will include an ablation study to evaluate each component independently.

4) Lack of repeated experimental trials: The reported results were obtained from a single controlled experimental run. Although the same dataset, training parameters, and computing environment were used for all models, repeated trials with different random seeds were not conducted. Therefore, the absence of mean values, standard deviations, confidence intervals, and statistical significance testing is acknowledged as a limitation. Future work will include multiple independent runs to assess the consistency and statistical reliability of the results.

5) Limited evaluation under real-world imaging conditions: The proposed framework was evaluated using a single dataset under controlled experimental conditions. Its robustness under variations such as lighting changes, camera differences, image rotation, occlusion, damaged banknotes, blur, and noise was not independently assessed. Therefore, the practical generalizability of the framework remains limited. Future work will evaluate the model under diverse real-world image acquisition conditions.

6) Absence of deployment performance metrics: Although the proposed framework has potential for smart-device and real-time deployment, the current study does not report practical deployment metrics such as inference time, model size, parameter count, FLOPs, memory consumption, or CPU/GPU latency. Therefore, real-time and smart-device suitability cannot yet be fully confirmed. Future work will evaluate these metrics on embedded and mobile computing platforms.

7) Absence of qualitative misclassification analysis: The current evaluation reports aggregate performance metrics and confusion matrices but does not include qualitative examples of false-positive and false-negative predictions. Consequently, the specific visual conditions that lead to classification errors, such as blur, poor lighting, occlusion, damaged notes, or visually similar counterfeit features, were not examined. Future work will include representative misclassified samples and a detailed analysis of common failure patterns.

8) Unverified real-time and smart-device deployment: The present study evaluates classification performance but does not measure deployment-related factors such as inference time, model size, parameter count, FLOPs, memory usage, or CPU/GPU latency. Therefore, the suitability of the proposed framework for real-time and smart-device deployment has not yet been experimentally confirmed. Future work will assess these metrics on mobile and embedded platforms.

9) Real-world implementation challenges: Limitations of computational resources and integration of the system with existing financial infrastructures. These practical considerations need to be well assessed to ensure smooth deployment and operation.

10) Deployment claims beyond experimental validation: The proposed framework was evaluated in a controlled experimental environment and was not tested within financial institutions, real-world transaction settings, embedded devices, or end-user environments. Therefore, claims regarding immediate deployment should be interpreted cautiously. The findings demonstrate the potential of the framework for counterfeit currency detection, while practical adoption requires further validation under operational conditions.

VI. Conclusion

Existing solutions for counterfeit money detection have been proved ineffective due to the skillful manipulation of miscreants. This study presents different techniques and methods employed for the detection and identification of counterfeit currency. In addition, it provides a new framework with deep learning models such as DCGAN, CNN, and FCNN. Deep learning methods are preferred due to their ability to find complex relationships in the input data. The primary aim is to train these deep learning models to rightfully classify real and fake currency notes. The endgame is embedded in apps on smart devices for wider deployment. The effectiveness of the system is confirmed in terms of various metrics like accuracy, precision, recall, and F1-score and its flexibility is demonstrated at a low cost by comparing the various models used to assess the efficiency of the study. The results demonstrated that DCGAN outperformed the rest of the models employed in this study and achieved 95% accuracy, 0.95 precision, 0.954 recall, and 0.957 F1-score. The confusion matrix also showed that DCGAN correctly classified 7,802 counterfeit samples and 6,606 genuine samples, outperforming both CNN and FCNN.

VII. Future Work

For further refinement of performance, it is recommended to retrain the models on new instances on a regular basis to further improve the performance and reduce false positives. Note: This study has been addressed for specific currency notes (MYR & SAR) while the proposed system can be applied on different country currency notes provided with ample model training and tuning of parameters. Other future directions could also be:

- Exploring the possible implementation of other security features like watermarking and holograms into the detection framework.
- Extending the framework to other currencies other than MYR and SAR and evaluate the generalizability and applicability around the world.

- Exploring transfer learning and domain adaptation methods to improve the model performance with limited new data instances.

REFERENCES

[1] C. D. Widagdo and H. Firmansyah, "The Impact of Counterfeit Money Circulation on Monetary Stability and The Role of Bank Indonesia in Handling It," *Awang Long Law Review,* vol. 7, no. 2, pp. 333-339, 2025.

[2] A. Mukundan, Y.-M. Tsao, W.-M. Cheng, F.-C. Lin, and H.-C. Wang, "Automatic counterfeit currency detection using a novel snapshot hyperspectral imaging algorithm," *Sensors,* vol. 23, no. 4, p. 2026, 2023.

[3] R. E. McKinney Jr, L. P. Shao, D. C. Rosenlieb Jr, and D. H. Shao, "Counterfeiting in cryptocurrency: An emerging problem," in *Handbook of Digital Currency*: Elsevier, 2024, pp. 169-183.

[4] Walker, "Money and financial technology (FinTech) history," *Int'l Law.,* vol. 56, p. 227, 2023.

[5] F. Niaz, J. Zhang, Y. Zheng, M. Khalid, and A. Niaz, "mm-cur: A novel ubiquitous, contact-free, and location-aware counterfeit currency detection in bundles using millimeter-wave sensor," *ACM Transactions on Sensor Networks,* vol. 20, no. 6, pp. 1-26, 2024.

[6] G. Yu and Z. Luo, "Financial fraud detection using a hybrid deep belief network and quantum optimization approach," *Discover Applied Sciences,* vol. 7, no. 5, p. 454, 2025.

[7] S. Sultana, I. Yasmin, M. J. Patwary, M. A. S. Bhuiyan, I. Salam, and M. H. Miraz, "Generating cgan-based synthetic dermoscopy images and classifying with deep lightweight cnn," in *2023 International Conference on Computing, Networking, Telecommunications & Engineering Sciences Applications (CoNTESA)*, 2023: IEEE, pp. 90-95.

[8] U. Sadyk, R. Baimukashev, and C. Turan, "State-of-the-Art Review of Deep Learning Methods in Fake Banknote Recognition Problem," *International Journal of Advanced Computer Science & Applications,* vol. 15, no. 1, 2024.

[9] A. A. Noor and N. I. R. Ruhaiyem, "Detecting counterfeit currencies using image processing techniques and artificial intelligence," in *AIP Conference Proceedings*, 2025, vol. 3282, no. 1: AIP Publishing LLC, p. 030006.

[10] S. Mathe, J. Kannamma, E. Narmada, C. Rampilla, and S. N. Rehmathunnisa, "Identification of Counterfeit Currency Using Image Processing and Deep Learning," in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2024: IEEE, pp. 1-7.

[11] D. Kumar and S. Chauhan, "Indian fake Currency Detection using computer vision," *International Research Journal of Engineering and Technology,* vol. 7, no. 5, pp. 2870-2874, 2020.

[12] C. G. Pachon, D. M. Ballesteros, and D. Renza, "An efficient deep learning model using network pruning for fake banknote recognition," *Expert Systems with Applications,* vol. 233, p. 120961, 2023.

[13] S. Chandrappa, P. Chandra Shekar, P. Chaya, L. Dharmanna, and M. Guruprasad, "Machine learning algorithms for identifying fake currencies," *SN Computer Science,* vol. 4, no. 4, p. 368, 2023.

[14] K. Teymournezhad, H. Azgomi, and A. Asghari, "Detection of counterfeit banknotes by security components based on image processing and GoogLeNet deep learning network," *Signal, Image and Video Processing,* vol. 16, no. 6, pp. 1505-1513, 2022.

[15] A. A. Chowdhury, A. Das, D. Karmaker, and K. K. S. Hoque, "Evaluation of Deep Learning models on UV ink: a Fake Money detection scheme with RPN," in *Proceedings of the 2nd international conference on computing advancements*, 2022, pp. 67-74.

[16] N. F. D. Ajid *et al.*, "Counterfeit one hundred Malaysian ringgit banknotes discrimination using chemical imaging inspection and pattern recognition," *Australian Journal of Forensic Sciences,* vol. 54, no. 5, pp. 695-709, 2022.

[17] F. Antonius, J. Ramu, P. Sasikala, J. Sekhar, and S. S. C. Mary, "DeepCyberDetect: hybrid AI for counterfeit currency detection with GAN-CNN-RNN using African Buffalo optimization," *International Journal of Advanced Computer Science and Applications,* vol. 14, no. 7, 2023.

[18] S. C. D. Bandu, M. Kakileti, S. S. Jannu Soloman, and N. Baydeti, "Indian fake currency detection using image processing and machine learning," *International Journal of Information Technology,* vol. 16, no. 8, pp. 4953-4966, 2024.

[19] A. Nasayreh *et al.*, "Jordanian banknote data recognition: A CNN-based approach with attention mechanism," *Journal of King Saud University-Computer and Information Sciences,* vol. 36, no. 4, p. 102038, 2024.

[20] S. Aulia and A. Rusdinar, "Geometric and grayscale template matching for Saudi Arabian riyal paper currency recognition," *International Journal of Electrical and Computer Engineering (IJECE),* vol. 8, no. 6, pp. 4230-4238, 2018.

[21] A. Radford, L. Metz, and S. Chintala, "Unsupervised representation learning with deep convolutional generative adversarial networks," arXiv preprint arXiv:1511.06434, 2015.