International Journal of Electrical and Computer Engineering (IJECE)
Vol. 15, No. 6, December 2025, pp. 5804~5814
ISSN: 2088-8708, DOI: 10.11591/ijece.v15i6.pp5804-5814

Hybrid artificial intelligence approach to counterfeit currency detection

Monther Tarawneh
Department of Information Technology, Faculty of Information Technology and Communications, Tafila Technical University, Tafila, Jordan

Article Info

Article history:

Received May 15, 2025
Revised Jul 29, 2025
Accepted Sep 16, 2025

Keywords:

Artificial intelligence
Convolutional neural network
Counterfeit detection
Fraud detection
Generative adversarial network
Long short-term memory networks

ABSTRACT

The use of physical money continues, posing ongoing challenges in the form of counterfeit money. This problem not only poses a threat to economic stability but also undermines confidence in the financial systems in use. Traditional methods such as manual inspections and testing of security features have become ineffective in detecting advanced counterfeiting techniques on an ongoing basis. This study proposes a hybrid model that harnesses the power of artificial intelligence, combining convolutional neural networks (CNNs), long short-term memory networks (LSTMs), and support vector machines (SVMs) for counterfeit detection. The proposed model leverages the diverse strengths of a number of artificial intelligence techniques, combining the ability to detect counterfeiting, analyze visual aspects, and sequences of banknotes. The proposed model was tested using real Jordanian currency sets of different denominations and datasets generated using generative adversarial networks (GANs). The results showed that the model was able to detect counterfeiting with high accuracy of 98.6%. and minimal errors compared to other methods. This outstanding performance demonstrates the benefits of integrating artificial intelligence (AI) technologies and that there is room for development and solutions that can keep up with advanced counterfeiting strategies. The study demonstrates the importance of integrating AI in maintaining the integrity of physical currency transactions.

Corresponding Author:

Monther Tarawneh
Department of Information Technology, Faculty of Information Technology and Communications, Tafila Technical University
Tafila, Jordan
Email: smtarawneh@ttu.edu.jo

1. INTRODUCTION

Counterfeit money is one of the most serious problems facing the world. It poses a threat to the security and stability of financial organizations, which leads to mistrust in financial institutions and causes economic distress. Counterfeit money is a currency that has been issued or minted outside the legal framework and without government supervision, and the purpose of those who work with it is to deceive people and build wealth in an illegal way [1]. Despite being illegal, it has continued to develop with the development of technology and has become a fraudulent means of making wealth easily.

While the world is gradually shifting towards digital currencies [2], this may take a long time and physical currency will still be used in daily transactions, especially since most of the economy is based on cash. Due to the rising cost of living and the need for cash, counterfeit currencies have become an increasingly tempting and easy target for counterfeiters [3]. Counterfeit currencies can no longer be detected

using traditional methods such as manual inspection, ultraviolet examinations, and checking security features, they are failed to catch sophisticated fraud which leads to unexpected number of false negative [4], also insufficient to keep up with the modern technologies that counterfeiters are currently using.

There is a need for more accurate and reliable counterfeit detection systems. Artificial intelligence offers solutions to various aspects of life from cultural, economic, industrial, medical, and others [5]–[9] and can be a radical solution to this challenge. AI and deep learning techniques such as convolutional neural networks (CNNs), deep neural networks (DNNs), and generative adversarial networks (GANs) can distinguish complex patterns and characteristics in currency and thus detect counterfeits with greater accuracy and efficiency than traditional methods. In addition, AI tools have the ability to learn over time new fraud techniques [10]. These tools are designed based of the idea of self-learning over time to improve their accuracy as new data appear. This self-learning ability makes them powerful against new counterfeiting techniques without the need for reprograming or manual update. While AI predictions depend on data quality, there is increasing confidence in AI's ability to enhance accuracy in detecting counterfeit currency. As a result, there is investment by financial firms in these tools to strengthen their detection systems against smart fraud methods [11].

Most recent research has used AI techniques independently for forgery detection. For example, CNNs are used to extract visual features, while long short-term memory networks (LSTMs) are used to analyze sequences. GANs are also used to augment data volume. While we agree that these methods are effective, they have some limitations when used alone: CNNs may face challenges in handling unseen forgeries, incomplete sequences may mislead LSTMs, and GAN-based training may be insufficient if the dataset is biased toward a particular class. Few researchers combine these techniques into a single forgery detection model. Therefore, a hybrid model is proposed to fill this gap.

This study proposes a hybrid deep learning model for accurate counterfeit currency detection. The proposed model combines the advantages of convolutional neural networks (CNNs), long short-term memory networks (LSTMs), and support vector machines (SVMs), augmented by generative adversarial networks (GANs). This model aims to integrate spatial and sequential learning capabilities with synthetic data generation to improve detection performance. This research aims to study and evaluate artificial intelligence techniques for counterfeit currency detection. The proposed model addresses current gaps in counterfeit currency detection by improving generalization and robustness under realistic conditions. The study also explores real-world applications of the model, such as banks and ATMs, and discusses its ability to detect counterfeit currency instantly. The integration of artificial intelligence enhances accurate counterfeit currency detection and develops a more consistent tool for preventing fraud and securing physical cash transactions, thereby protecting the economy. The rest of the paper is organized into literature review, methodology, result and discussion, and conclusion at the end.

2. LITERATURE REVIEW

Counterfeiting is not a new issue in the economic world. It has been around since the beginning of currency use and is monitored and dealt with by traditional methods such as manual inspection, ultraviolet scanning, and the use of security features such as watermarks and holograms. These methods have been effective in detecting counterfeit currency and have been widely adopted [12]. However, several disadvantages have emerged that have reduced their use, such as the level of accuracy and reliability. Manual inspections take a long time, while relying solely on the experience and skill of the audit. Additionally, skilled counterfeiters have surpassed these methods, and they have become no obstacle to them.

Early neural networks were simple in their learning abilities due to the lack of computational power and data availability [13]. The revolution in computational power and the availability of big data have opened the door to AI advancements, propelling the field into a new era of innovation and capability. These developments have significantly accelerated AI computations, enabling more sophisticated models and applications [14]. Advanced technologies lunch the power of artificial intelligence and deep learning to process vast amounts of data and learn complex patterns. Artificial intelligence introduces innovative approaches in various industries such as healthcare [15], [16], finance [17], [18], agriculture [19], security and autonomous systems [5]. As technology becomes more powerful, and AI methods become more efficient, deep learning has introduced innovative methods for detecting counterfeit currency [20]. These methods improve detection accuracy by analyzing a greater number of features, even spectral signatures and complex patterns that cannot be seen with the eyes. The use of deep learning has transformed the detection process to adaptable, fast and accurate methodologies.

Deep learning is a subsection of machine learning. Deep learning uses of deep neural networks that consist of multiple layers [21]. A deep neural network has an input layer, one or more hidden layers, and an output layer. Each layer contains nodes (neurons) that are fully connected to all nodes in the adjacent layers.

This structure help network to learn complex patterns through sequential layers, predict output variables based on the learned representation [22]. The DNN model and its applications are shown in Figure 1.

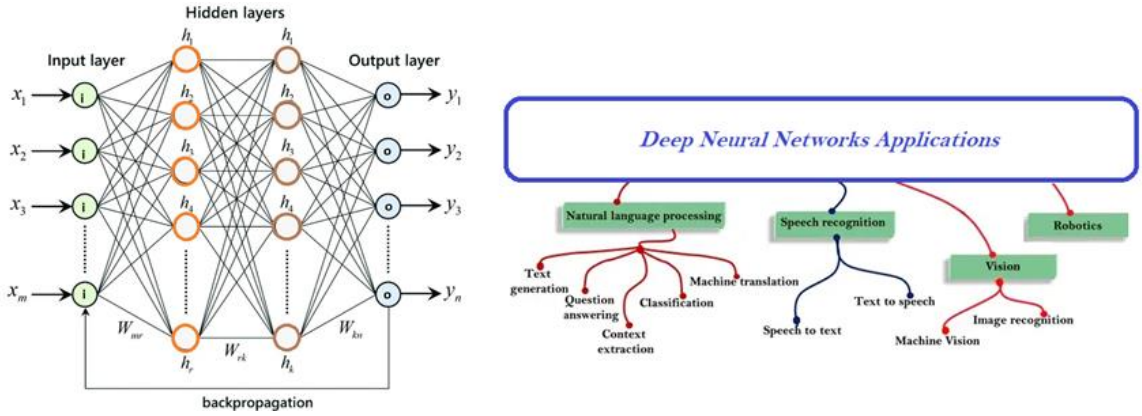

Figure 1. DNN architecture and its real-world applications [23]

The initial application of technology in counterfeit currency detection was rooted in image processing and pattern recognition techniques. These methods involved scanning currency notes to identify missing or altered features, such as color, size, lines, and textures. By analyzing these physical attributes [24], [25], these systems aimed to detect any discrepancies that could indicate a counterfeit note. Although effective to some extent, these methods were limited in their ability to adapt to more sophisticated counterfeiting techniques as they relied on predefined patterns and manual feature extraction. Furthermore, researchers merged these techniques with machine learning [26], [27] to improve their performance and increase accuracy. By using machine learning algorithms, the systems could learn from data and automatically detect more complex patterns, reducing human error and increasing the detection process in real-time.

Convolutional neural networks (CNNs) are most effective in image recognition due to its ability to analyze currency features. It is a multilayer deep learning neural network; they have multiple layers that extract features and train classifiers. CNNs utilize hierarchical representations to extract key topological features and features from currency images. CNNs manipulate pixels through various layers, this will capture features from complex and high-dimensional data. It has been implemented by researchers to detect fake in different currency such as Indian [28], [29], Euro [30], Jordanian [31], Bangladesh [25] and other currency [32]–[34].

CNN has been combined with other models. Researchers implement a system that combine CNN with LSTM networks that adapt to new counterfeiting methods as they appear [3], [35], [36]. However, this integration has some limitation in term of complexity, time, and need more training. Also, CNN combined with SVM, where CNN used for feature extraction from currency images followed by classifications by SVM [37]. The study shows good improvement in detecting fake currency and proves that the accuracy increased by integrating CNN with other models.

Generative adversarial networks (GANs) used to generate artificial images for currency, which used to train deep learning models to improve fake detection [38]. It allows AI tools to learn and comprehend differences between real and fake currency. Also, help to digest challenges of limited availability of counterfeit samples. However, this may increase the counterfeit problem and pose ethical and legal issues. Additionally, the generated images could not be that realistic and mislead the results accuracy.

Blockchain technology has been used to detect counterfeit currencies, as its core properties such as decentralization and immutability can be used to combat counterfeiting and increase confidence in their verification. Blockchain technology can be employed to record, track, and verify the serial number of currencies in real time, preventing unregistered funds from entering the financial system [1], [2]. In addition to serial numbers, cryptographic tags can be placed and secure databases can be used to automate the verification of currencies before they enter the financial system using blockchain-based smart contract technology [3]. To reduce the risk of currency counterfeiting, the concept of using digital currencies and making them an alternative to physical currencies emerged, and blockchain applications were employed to create digital currencies. Blockchain was enhanced by integrating it with artificial intelligence to analyze data and predict any illegal activity in the field of currency trading [3]–[5].

There are studies that have used recurrent neural networks to detect counterfeiting by tracking the serial numbers on circulating currency [39]. They identify any irregularities in the sequence of serial numbers and have proven effective in identifying potential counterfeiting activities and enhancing the security of currency circulation. To power both the image recognition abilities of CNNs and the sequential data processing powers of recurrent neural networks (RNNs), a hybrid model has been implemented that integrates CNN with RNN, providing a more comprehensive solution for counterfeit detection [40], [41].

AI is a crucial element in improving financial security by providing tools that can detect fraudulent activities in real-time. AI-based systems are used in banks and financial services to secure transactions, authenticate currency, and stop the circulation of fake money. There are increasing number of studies that use AI in finance and focus on fraud detection, especially counterfeit currency detection. Deep learning approaches provide a strong solution to the ongoing counterfeiters methods. However, ongoing activities of counterfeits tactics require continuous effort to develop new frameworks to prevent fraud and increase accuracy in detecting fake currency.

3. METHOD

To develop a model to detect counterfeit currency regardless of its type, it is necessary to combine the capabilities of different AI algorithms into a single model. The proposed model is a hybrid model that combines CNNs, LSTMs, GANs, and SVMs. Figure 2 shows the steps of the proposed model. This model improves accuracy by processing all aspects of the original and sequential images to detect counterfeiting.

To understand the multiple aspects of counterfeit detection, the new model was chosen as a combination of CNN, LSTM, GAN, and SVM. CNNs are better suited for analyzing banknote images due to their ability to learn spatial patterns and image features. LSTMs have proven their ability to model sequential dependencies and identify irregular patterns in number sequences, making them suitable for processing serial numbers. Due to the lack of legal tender for counterfeit currency, GANs were used to generate realistic images of counterfeit currency for sufficient training. SVMs, on the other hand, have the potential to handle high-dimensional data and provide robust decision boundaries.

Figure 2 shows the main components of the model and step by step of the proposed models. It includes:

a. Dataset: a collection of image images of Jordanian banknotes (1,5,10,20, 50) from Kaggle. The dataset contains 7312 images (5473 real+1839 GAN-generated).
b. Image preprocessing: number of operations applied on the images before processing it: resized to 224×224 pixels, contrast adjustment, rotation, flipping, scaling, and cropping.
c. Serial Number: extract a 10-digit sequence numbers as input for LSTM.
d. GNA: to get good training and have diversity in the dataset, DCGAN used to generate realistic fake currency images.
e. Feature extraction: CNN used three convolutional blocks (32, 64, 128 filters), ReLU activations, and max pooling. Features flattened and processed via dense layers with dropout.
f. LSTM: LSTM sequence model with 64 units employed to analyze serial numbers before ReLU-activated dense layer.
g. Fusion and Classification: linear SVM (C=1, tolerance=1e-3) used to classify the output of integrated CNN and LSTM.
h. Model training: Adam optimizer used to train the model (0.5 dropout for CNN, 0.2 for LSTM), batch size of 32, and 50 epochs. Early stopping used to avoid overfitting.
i. Performance evaluation: the proposed model evaluated using accuracy, precision, recall, F1-score, and AUC.

The above steps of the research procedure are explained in more detail in separate coming sub sections.

3.1. Dataset

The dataset used in this study downloaded from Kaggle [42] is a collection of balanced high-quality images featuring banknotes Jordanian Dinar (JD): 1, 5, 10, 20, and 50 JDs. It includes new editions of 1, 20, and 50 JDs banknotes. This dataset contains 5473 images and designed for the development and evaluation of machine learning models for automatic currency recognition and denomination classification tasks. Table 1 shows the number of samples for each Jordanian Dinar (JD) denomination, and Figure 3 shows genuine and counterfeit 1JD.

Serial numbers recorded from banknotes sets to detect irregular sequence and recognize counterfeit currency through irregularities in circulation patterns. Also, GANs were used to create synthetic counterfeit banknotes to enhance model's ability to detect forgeries. We must be aware that the samples generated GANs may be used by malicious individuals to produce counterfeit currency that is close to the real currency, so this must be controlled. Therefore, in this research, we adhere to ethical guidelines regarding the use of GANs.

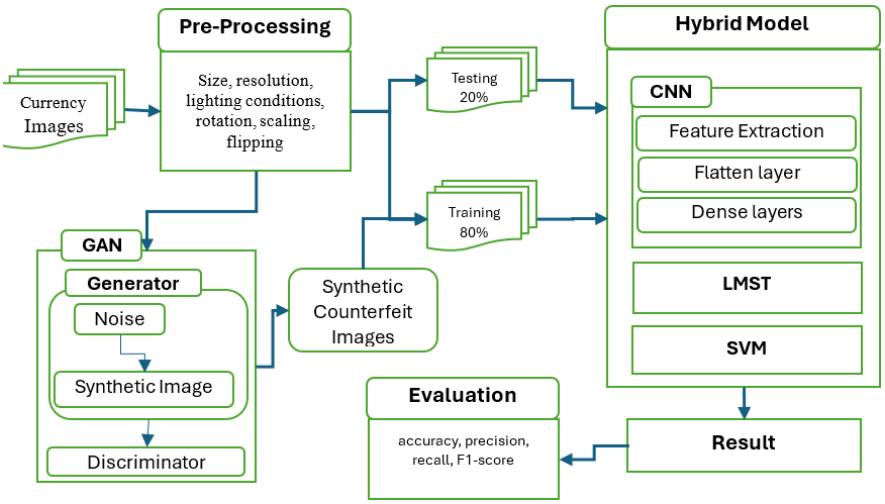

Figure 3. workflow of the hybrid counterfeit detection model

Table 1. Number of samples for each Jordanian Dinar (JD) denomination

Notes (JD)	Numbers
50	1178
20	1225
10	867
5	108
1	1123

Figure 3. Sample of genuine (left) and counterfeit (right) 1 JD banknote

3.2. Preprocessing

To obtain high-quality images and extract features, the banknote images were standardized in terms of size (224,224,3), resolution, and lighting conditions to be used by deep learning models. The dataset contains images of Jordanian currency with different backgrounds and conditions to add complexity to the data and simulate real conditions. It includes images of folded or partially hidden banknotes. This is very important to improve the model's ability to detect counterfeit currency in various conditions. This was done using noise reduction, contrast adjustment, and grayscale transformation applications.

Preprocessing was conducted to ensure the quality of the banknote images as well as to meet the requirements of the deep learning model. Priority was given to interpreting contrast because it reveals essential visual features for distinguishing counterfeiting, such as edges and patterns. This is due to the lack of lighting, and this modification made it possible to identify them during feature extraction in the CNN. Some images may contain unwanted artifacts that hinder the model during the training process. Therefore, noise reduction was employed to enhance the clarity of the images, and the model then concentrates on significant features instead of noise. Other preprocessing techniques were employed to improve the generalizability and reliability of the model under different conditions, such as grayscale transformation, rotation, gradient, and reflection. Different views were created to facilitate the modelling of the model from different angles and positions of the currency. Preprocessing techniques that increase complexity and require a computational problem were avoided.

To ensure that the model works realistically and prevent overfitting, some techniques such as rotation, scaling, clippings, and flipping were applied to the images, this create new images with different situations and ensure that the training is more than memorizing specific features. The number of images increase from 5473 to 7312. As for the serial number, it was cleaned and formatted to ensure consistent input for analysis by the LSTM model. To minimize the risk of overfitting, dropout layers were added to the model. Furthermore, complex models were penalized, and the simplest solutions were taken. To create a balanced dataset, and to ensure that there is no overfitting for certain types of data, real samples were combined with those produced by GANs. This ensures that the model's ability is enhanced by using the samples produced by GANsz.

3.3. Implementation

The banknotes images will be loaded into CNN model to extract features to capture all features that are important for Counterfeit detection. The CNN integrated with LSTM to analyze the pattern of serial numbers and identify irregular patterns. Then the extracted features classified by SVM as real or counterfeit. GANs used to create realistic fake images, which were used to augment the training dataset. The CNN model is implemented with four main layers:

a. Convolutional layers: The model starts with a series of convolutional layers designed to capture local features such as edges, textures, shapes, and patterns in the input images. These layers are responsible for learning low-level and high-level image features that are essential for detecting intricate differences between real and counterfeit banknotes.
b. Max pooling layers: After each convolutional layer, a max pooling layer reduces the spatial dimensions of the extracted feature maps. This down sampling allows the model to focus on the most important features. The computational complexity was reduced, while maintaining the most important features from the image.
c. Flatten layer: Once the model has selected and refined the important visual features using its specialized layers, it needs to simplify this information for further processing. This is done by flattening the complex 2D feature maps into a simple straight line—a 1D vector. This step is crucial because it transforms the processed image data into a simpler form that the next part of the network, which does the actual classification, can easily work with
d. After transforming the complex data into a single, straight line (the flattened feature vector), it enters a dense layer packed with 512 tiny processing stations. ReLU activation function help to focus on the most useful features among all features.

Next, this prepared data moves to another dense layer, which focused solely on making one crucial decision: is the banknote real or counterfeit? It does this through a single unit equipped with a sigmoid activation function, which squeezes the incoming data into a range between 0 and 1. This method allows the model to make sense of banknote images in a sophisticated way, ultimately providing a probability that acts much like a confidence score on whether the banknote is genuine or fake.

CNN integrated with LSTM (network is used to analyze banknote serial numbers of length 1-10. The serial numbers on the banknotes are processed using an LSTM layer with 64 modules. The input shape parameter is fed to the LSTM layer to determine the structure of the input sequence. To capture nonlinear relationships, a fully connected dense layer containing 128 and ReLU activation units were added.

The hybrid model was trained with a supervised learning approach. The CNN and LSTM networks optimized using Adam optimizer, while SVM used linear kernel for final classification. A combination of dropout and early stopping techniques was employed to avoid overfitting and ensure effective training.

In order to get the best performance of the hybrid model, the hyperparameters of the algorithms included in the model were modified. For the CNN, different filter sizes and numbers were tested and the best performance was achieved using 3x3, 32 and 64 filters in the first two layers, followed by 128 in the deeper layers. ReLU activation is used due to its ability to handle nonlinearity, and reduce spatial dimensions without losing important features, max pooling is used with a pool size of 2x2. Also, grid search determined an optimal learning rate of 0.0001, and a dropout rate of 0.5 in the fully connected layers, which avoids overfitting. For LSTM, the best number of hidden units was 64 and 10 length units were concatenated to fit the structure of the sequence data. A dropout rate of 0.2 was used to avoid the overfitting problem. To ensure adaptive and efficient learning, Adam optimizer was used with a learning rate of 0.001. To obtain efficient and accurate classification, a linear SVM kernel was used. The optimal value of the regularization parameter (C) was 1 with a tolerance of 1e-3 to ensure fast convergence and balanced accuracy. Many experiments were conducted to choose these hyperparameters to ensure the efficient performance of the hybrid model.

4. RESULTS AND DISCUSSION

A variety of metrics utilized to evaluate the performance of the proposed model, including accuracy, precision, recall, F1-score, and the confusion matrix. To ensure the reliability of the model, it was trained and assessed on both genuine data (Jordanian banknotes) and GAN-generated counterfeit data, several conditions considered for recognizing genuine and counterfeit banknotes to provide a comprehensive environment for evaluating model performance on diverse inputs.

The implementation was implemented in Colab environment using Python libraries. In this research, a hybrid system was implementer by integrating CNN for feature extraction, LSTM for sequential pattern recognition (currency serial numbers), and SVM for classification of currency as fake or genuine. This method enables the model to analyze visual features from currency and the patterns of sequential serial numbers, improving its accuracy. To provide sufficient data for model learning in the training and accurate evaluation on hidden data, the dataset was split into 80% for training and 20% for testing. The results of the proposed model (CNN-LSTM-SVM) were very remarkable, reaching an accuracy of 98.6%, which proves the model's ability to accurately distinguish between counterfeit and genuine currency in most situations. The computational efficiency and resource requirements for the hybrid model were tested and compared to individual requirements for CNN, LSTM and SVM. Despite the higher resource requirements expected for the model integrating CNN, LSTM, and SVM, the hybrid model demonstrated strong performance and accuracy in the results, resulting in its computational cost.

The combination of CNN, LSTM, and SVM substantially enhanced the model's capability to deal with both spatial and sequential data. Table 2 provides a comparison between the proposed model and other models tested on the same dataset, highlighting the superior performance of the CNN-LSTM-SVM approach.

Table 2. Comparison between the proposed model and other models

Model	Precision	Recall	F1-Score	Accuracy
CNN	95.40%	95.20%	95.30%	95.00%
CNN-LSTM	96.50%	96.30%	96.40%	96.20%
CNN-GAN	95.00%	94.50%	94.70%	94.80%
CNN-LSTM-SVM	***98.80%***	***98.30%***	***98.50%***	***98.60%***
CNN-CAM	96.60%	96.40%	96.50%	96.00%
CNN-GRU	95.80%	95.60%	95.70%	95.70%
CNN-RNN	94.50%	94.00%	94.30%	94.20%
CNN-Transformer	97.30%	97.00%	97.10%	97.10%

The result shows the effectiveness of combining the classification accuracy of SVM and feature recognition of CNN. The high accuracy of the models, close to 100%, indicates that there is room for improvement of the system and further improvement of accuracy. However, this depends on the size of the available data and its diversity. As well as the quality of the images available in different conditions and angles. In addition to reaching the appropriate settings for the model. All this may guarantee results with excellent accuracy in detecting forgery.

Figure 4 shows the ROC curve of the performance of the proposed hybrid model. The calculated area under the curve (AUC) of 0.92 shows that the model has the ability to distinguish between genuine and counterfeit money. This result confirms the results listed in Table 2 that the proposed hybrid model outperforms other methods in most metrics including accuracy, precision, recall, and F1 score. The training and validation lose depicted in Figure 5 shows the efficiency of the model with low overfitting. We notice that the training loss decreases from about 0.6 to less than 0.2, which is related to the training accuracy as the model becomes more confident in its predictions. The validation loss decreases from 0.6 to about 0.25. This confirms that the model's ability to generalize improves with each epoch. The convergence of the training and validation loss values towards the following epochs proves that the model is not overfitting.

The proposed model demonstrated good performance in distinguishing between counterfeit and genuine banknotes. The combination of CNN, LSTM and SVM AI techniques had a significant impact on the effectiveness of the model. This is expected as the model combines the features of CNN in distinguishing between fine visual features that are important in distinguishing between counterfeit and genuine banknotes and the features of LSTM in dealing with sequential patterns in serial numbers, giving the ability to track banknotes and identify the culprit. When the model was tested on counterfeit banknotes created by GAN, its performance was satisfactory with an accuracy of 98.6%. The model demonstrated a slight increase in false negatives due to the presence of some counterfeit banknotes that are close to real banknotes and cannot be distinguished by visual inspection. Also, false positives where genuine notes could be classified as counterfeit. This brings about the need for research and development to improve detection accuracy. Both False positive and false negative pose a challenge for the financial systems and allow counterfeit currency to

be used. This will reduce the trust in the detection system and return us to the manual verification processes. The proposed model, which integrates CNN, LSTM and SVM, significantly reduces false negatives by performing a comprehensive analysis of visual and sequential features. The AUC score demonstrates the model's ability to effectively balance trade-offs.

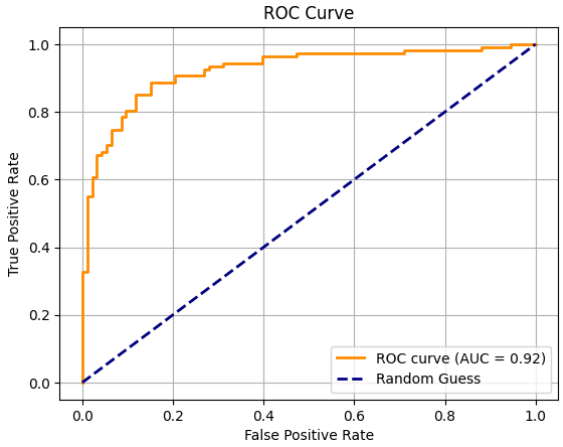

Figure 4. ROC curve of the proposed hybrid model

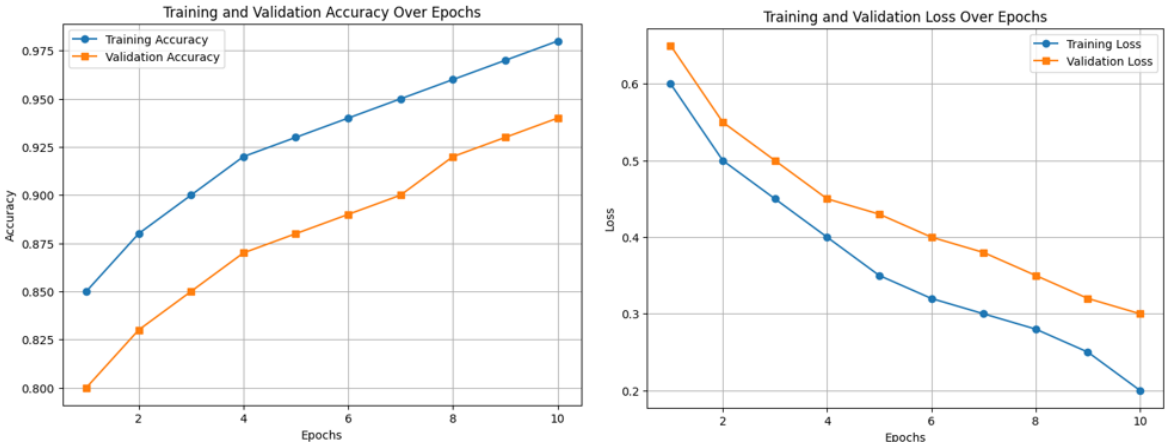

Figure 5. Training and validation accuracy and loss of the proposed hybrid model over 10 epochs

The proposed model shows better accuracy and can be considered applicable to real-world applications such as ATMs, banknote counting machines and sales points. However, relying solely on image quality and serial numbers poses some limitations when working in uncontrolled environments, such as damaged banknotes. While the use of GANs reduces reliance on large datasets, their use also carries some risks. Therefore, explainable artificial intelligence (XAI) should be employed to help investigate anomalies. This model is scalable to include other algorithms to combat counterfeiting worldwide. Also, it needs to be integrated with a banknote scanning system and a central database for further updating and training the model and enabling it to detect counterfeit currency in real time before accepting deposit or dispensing cash. The findings of this study demonstrate the ability of Hybrid model to improve the accuracy over single methods. This research contributes to the digital security in the finance systems.

5. CONCLUSION

Counterfeit currency has become a problem all over the world, as traditional methods have become inaccurate in detecting counterfeit banknotes, so technology has been employed in this regard, especially machine learning and artificial intelligence methods. This study proposes an effective artificial intelligence-based method for detecting counterfeit currency.

The new proposed hybrid model utilizes more than one artificial intelligence technique to utilize the strengths of each and find a comprehensive solution to counterfeit currency. It merges CNNs, LSTMs, GANs, and SVMs. The CNN-LSTM-SVM model demonstrated outstanding performance, achieving an impressive 98% accuracy in detecting counterfeit currency compared to previous models. CNN-based models achieved accuracy rates ranging from 93% to 95%, while CNN-LSTM methods achieved slightly higher accuracy rates of 96.2%. The proposed model combines the strengths of feature extraction (CNN), sequence learning (LSTM), classification robustness (SVM), and GAN-based boosting. Also, it is capable of working in different situations, granted by synthetic data generated by generative adversarial networks with its scalability. Research and development should continue to handle the growth of counterfeiting methods, with a critical need to continue develop artificial intelligence models and training methodologies.

There is a need to continue developing counterfeit detection technologies. The main focus should be on integrating AI algorithms to improve detection methods. The model should also be tested on different currencies from different countries in order to participate in the fight against counterfeit money on a larger scale. The robustness and reliability of the system can also be improved by incorporating advanced transformer models and real-time detection. This study paves the way for innovation in financial security, supporting economic stability and enhancing confidence in global financial systems. The results showed the effectiveness of this hybrid model, and with proper settings and increasing data and diversity, the model will be more powerful and accurate in detecting counterfeit currencies.

FUNDING INFORMATION

Authors declare that there is no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Monther Tarawneh	✓	✓			✓	✓			✓	✓				

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that there is no conflict of interest regarding the publication of this paper.

DATA AVAILABILITY

The used dataset is available on Kaggle and can be accessed at:
https://www.kaggle.com/datasets/halabilbesei/jordanianbanknotesold-and-new-edition
The data contains images of various Jordanian currencies, which were used for the training and evaluation of the proposed model.

REFERENCES

[1] A. Saida, M. S. A. Baig, C. Sreedhar, M. Ramesh, R. Spoorti, and K. Kaveri, "Detection of counterfeit currency," in *Emerging Trends in IoT and Computing Technologies*, CRC Press, 2024, pp. 6–11.
[2] S. K. Panda, A. Sathya, and S. Das, "Bitcoin: Beginning of the cryptocurrency era," in *Recent Advances in Blockchain Technology: Real-World Applications*, Springer, 2023, pp. 25–58.
[3] M. SWEETY and M. R. SALMAN, "AI driven game theory optimized generative CNN-LSTM method for fake currency detection," *Journal of Theoretical and Applied Information Technology*, vol. 102, 2024.
[4] A. T. G. Tapeh and M. Z. Naser, "Artificial intelligence, machine learning, and deep learning in structural engineering: a scientometrics review of trends and best practices," *Archives of Computational Methods in Engineering*, vol. 30, no. 1, pp. 115–159, 2023, doi: 10.1007/s11831-022-09793-w.
[5] M. Tarawneh, F. AlZyoud, and Y. Sharrab, "Artificial intelligence traffic analysis framework for smart cities," in *Science and Information Conference*, 2023, pp. 699–711.

[6] M. Tarawneh, H. AbdAlwahed, and F. AlZyoud, "Innovating project management: AI applications for success prediction and resource optimization," in *International Conference on Advances in Computing Research*, 2024, pp. 382–391.
[7] O. Tarawneh, M. Tarawneh, Y. Sharrab, and M. Husni, "Mushroom classification using machine-learning techniques," in *AIP Conference Proceedings*, 2023, p. 030003.
[8] L. Bordoni and F. Mele, *Artificial intelligence for cultural heritage*. Cambridge Scholars Publishing, 2016.
[9] Y. Qin, Z. Xu, X. Wang, and M. Skare, "Artificial intelligence and economic development: An evolutionary investigation and systematic review," *Journal of the Knowledge Economy*, vol. 15, pp. 1736–1770, 2024.
[10] 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, 2024.
[11] D. Gupta, N. K. Miryala, and A. Srivastava, "Leveraging artificial intelligence for countering financial crimes," *Journal ID*, vol. 2157, p. 178, 2023.
[12] O. Y. Rodionova and A. Pomerantsev, "NIR-based approach to counterfeit-drug detection," *TrAC Trends in Analytical Chemistry*, vol. 29, pp. 795–803, 2010.
[13] M. R. Meireles, P. E. Almeida, and M. G. Simões, "A comprehensive review for industrial applicability of artificial neural networks," *IEEE Transactions on Industrial Electronics*, vol. 50, pp. 585–601, 2003.
[14] S. Zhu, T. Yu, T. Xu, H. Chen, S. Dustdar, and S. Gigan, "Intelligent computing: the latest advances, challenges, and future," *Intelligent Computing*, vol. 2, p. 6, 2023.
[15] O. Tarawneh, M. Otair, M. Husni, H. Y. Abuaddous, M. Tarawneh, and M. A. Almomani, "Breast cancer classification using decision tree algorithms," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 4, pp. 676–680, 2022, doi: 10.14569/IJACSA.2022.0130478.
[16] M. Tarawneh and O. Embarak, "Hybrid approach for heart disease prediction using data mining techniques," *Lecture Notes on Data Engineering and Communications Technologies*, vol. 29, pp. 447–454, 2019, doi: 10.1007/978-3-030-12839-5_41.
[17] S. Tatineni and A. Mustyala, "Enhancing financial security: data science's role in risk management and fraud detection," *International Journal of Advancements in Computational Technology*, vol. 2, pp. 2583–8628, 2024.
[18] S. Koehler, N. Dhameliya, B. Patel, S. Kumar, and R. Anumandla, "AI-enhanced cryptocurrency trading algorithm for optimal investment strategies," *Asian Accounting and Auditing Advancement*, vol. 9, no. 1, 2018.
[19] Manas Wakchaure, B.K. Patle, and A.K. Mahindrakar, "Application of AI techniques and robotics in agriculture: A review," *Artificial Intelligence in the Life Sciences*, vol. 100057, 2023.
[20] M. Laavanya and V. Vijayaraghavan, "Real time fake currency note detection using deep learning," *International Journal of Engineering and Advanced Technology*, vol. 9, no. 1s5, pp. 95–98, 2019, doi: 10.35940/ijeat.a1007.1291s519.
[21] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, pp. 436–444, 2015.
[22] K. Ali, M. Alzaidi, D. Al-Fraihat, and A. M. Elamir, "Artificial intelligence: benefits, application, ethical issues, and organizational responses," 2023, pp. 685–702.
[23] D. Al-Fraihat, Y. Sharrab, F. Alzyoud, A. Qahmash, M. Tarawneh, and A. Maaita, "Speech recognition utilizing deep learning: A systematic review of the latest developments," *Human-centric Computing and Information Sciences*, vol. 14, 2024, doi: 10.22967/HCIS.2024.14.015.
[24] M. M. Alimushwan, A. Mohaimin, R. Islam, and S. Chowdhury, "Fake currency detection using image processing method," in *IOP Conference Series: Materials Science and Engineering*, 2016, p. 052047.
[25] Z. Ahmed, S. Yasmin, M. N. Islam, and R. U. Ahmed, "Image processing based feature extraction of Bangladeshi banknotes," in *The 8th International Conference on Software, Knowledge, Information Management and Applications (SKIMA 2014)*, 2014, pp. 1–8.
[26] S. C. D. Bandu, M. Kakileti, S. S. J. Soloman, and N. Baydeti, "Indian fake currency detection using image processing and machine learning," *International Journal of Information Technology*, pp. 1–14, 2024.
[27] A. Pathak, A. Chakraborty, M. Rahaman, T. S. Rafa, and U. Nayema, "Enhanced counterfeit detection of Bangladesh currency through convolutional neural networks: a deep learning approach," *International Journal of Innovative Research in Computer Science \& Technology*, vol. 12, pp. 10–20, 2024.
[28] R. Sumalatha, B. J. Reddy, and T. V. R. Reddy, "Identification of fake Indian currency using convolutional neural network," in *2022 6th International Conference on Computing Methodologies and Communication (ICCMC)*, 2022, pp. 1619–1623.
[29] J. D'cruz, M. Jose, M. Eldhose, and B. Jose, "Fake Indian currency detection using deep learning," *International Journal of Engineering Applied Sciences and Technology*, vol. 5, pp. 2143–2455, 2021.
[30] C. G. Pachón, D. M. Ballesteros, and D. Renza, "Fake banknote recognition using deep learning," *Applied Sciences*, vol. 11, p. 1281, 2021.
[31] A. Nasayreh, A. S. Jaradat, H. Gharaibeh, W. Dawaghreh, R. M. Al Mamlook, and Y. Alqudah, "Jordanian banknote data recognition: A CNN-based approach with attention mechanism," *Journal of King Saud University-Computer and Information Sciences*, vol. 36, p. 102038, 2024.
[32] M. Melaku, "Ethiopian currency detection and counterfeit verification using deep learning," Master Thesis, St. Mary's University, 2023.
[33] S. A. Naseem, A. Rehman, S. Z. Uddin, B. Khan, Z. Mehmood, and M. U. Nisa, "Counterfeit recognition of Pakistani currency," *KIET Journal of Computing and Information Sciences*, vol. 6, pp. 123–147, 2023.
[34] G. Behery, H. El-Hadidi, A. El-Harby, and T. A. Usamad, "Intelligent Libyan banknote recognition system," *International Research Journal of Engineering and Technology*, vol. 8, pp. 1668–1680, 2021.
[35] M. N. Hasan, R. N. Toma, A.-A. Nahid, M. M. Islam, and J.-M. Kim, "Electricity theft detection in smart grid systems: A CNN-LSTM based approach," *Energies*, vol. 12, p. 3310, 2019.
[36] 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, 2023.
[37] V. Kukreja, S. Mehta, S. Gupta, and A. Garg, "Financial foresight: predictive power of CNN-SVM in fake currency detection analysis," in *2024 5th International Conference for Emerging Technology (INCET)*, 2024, pp. 1–6.
[38] T. Ali, S. Jan, A. Alkhodre, M. Nauman, M. Amin, and M. S. Siddiqui, "DeepMoney: counterfeit money detection using generative adversarial networks," *PeerJ Computer Science*, vol. 5, p. e216, 2019.
[39] S. Kore, D. Mishra, I. Bhiogade, and D. Jituri, "Fake currency detection using recurrent neural networks (RNN)," *Journal For Basic Sciences*, vol. 23, no. 6, 2023.
[40] J. A. Nasir, O. S. Khan, and I. Varlamis, "Fake news detection: A hybrid CNN-RNN based deep learning approach," *International Journal of Information Management Data Insights*, vol. 1, no. 1, Apr. 2021, doi: 10.1016/j.jjimei.2020.100007.

[41] I. K. Sastrawan, I. P. A. Bayupati, and D. M. S. Arsa, "Detection of fake news using deep learning CNN–RNN based methods," *ICT Express*, vol. 8, pp. 396–408, 2022.
[42] H. Bilbesei, "Jordanian Banknotes (Old and New Edition)," Kaggle, 2023.

BIOGRAPHIES OF AUTHORS

Monther Tarawneh is an assistant professor in the Information Technology Department at Tafila Technical University, Jordan. He received his Ph.D. in Computing from the University of Sydney, Australia, in 2009. His research interests span a range of fields, including artificial intelligence, cybersecurity, mobile computing, and the internet of things (IoT). Dr. Tarawneh has extensive experience in academia, contributing to curriculum development, supervising graduate research, and publishing in reputable international journals and conferences. He is also actively involved in teaching advanced programming, simulation techniques, and data mining. He can be contacted at: mtarawneh@ttu.edu.jo.