Journal of Theoretical and Applied Information Technology
15th March 2024. Vol.102. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AI DRIVEN GAME THEORY OPTIMIZED GENERATIVE CNN-LSTMMETHOD FOR FAKE CURRENCY DETECTION

MS.K. SWEETY[1], DR. M.NAGALAKSHMI[2], MS.RAHAMA SALMAN[3], DR GANTA JACOB VICTOR[4], ASLAM ABDULLAH M[5], PROF. TS.DR.YOUSEF A.BAKER EL-EBIARY[6]

[1]M.Tech Scholar, Department of CSE, Marri Laxman Reddy Institute of Technology and Management, Dundigal, Hyderabad- 500043
[2]Associate Professor, Department of CSE, Marri Laxman Reddy Institute of Technology and Management, Dundigal, Hyderabad- 500043.
[3]Lecturer, Department of Information Technology and Security, College of Computer Science & Information Technology ,Jazan University, Jazan,KSA.
[4]Associate Professor, Dept. of Computer Science and Engineering, Koneru Lakhmaiah Education Foundation
Green fields; Vaddeswaram, Guntur District 522302, Andhra Pradesh.
[5]Associate Professor, School of Chemical Engineering, Vellore Institute of Technology, Vellore, India
[6]Faculty of Informatics and Computing, UniSZA University, Malaysia.

[1]k.sweety0178@gmail.com, [2]nagalakshmi1706@gmail.com, [3]rabdol@jazanu.edu.sa,
[4]jacob.victor@kluniversity.in,[5]aslamabdullah.m@vit.ac.in, [6]yousefelebiary@unisza.edu.my

ABSTRACT

Imitation money, or fake cash, is a serious danger to global financial systems' reliability and security. Such currency items are made illegally with the intention of misleading people, organizations, and governments. Identifying counterfeit money is essential for a number of reasons, chief among them being the preservation of trust between the currency as well as banking systems. Fake money may upset economic stability, cause financial losses for people and enterprises, and destroy trust within the monetary system. Consequently, there may be a decrease of GDP and a rise in living costs. The effective operation of a nation's economy depends on the detection of counterfeit currency as it protects the integrity of a country's currency, prevents fraud, and preserves the safety of money transactions. The most advanced strategy for preventing counterfeit money is the AI-driven Game Theory Optimized Generative CNN-LSTM technique for Fake Currency Identification. The ongoing issue of counterfeiting calls for sophisticated and flexible solutions. This approach integrates the use of Generative Adversarial Networks (GANs) using game theory optimization, Long Short-Term Memory (LSTM) networks for temporal pattern recognition, as well as Convolutional Neural Networks (CNNs) for feature extraction. The device that discriminates has to attempt to separate synthetic pictures of counterfeit cash produced by the GAN from real banknotes. The technique is extremely accurate and flexible when it comes to identifying fake money. It offers greater possibilities that might improve safety within banking environments and other areas. The proposed framework is implemented in python. The proposed Game Theory Optimized Generative CNN-LSTMMethod shows better accuracy with 98.9% when compared with SVM, AlexNet, and Linear Discriminant Analysis.

Keywords: *Convolutional Neural Network (CNN); Fake Currency; Generative Adversarial Network (GAN); Game Theory Optimization;Long Short-Term Memory (LSTM).*

1. INTRODUCTION

The creation of duplicate cash that is counterfeit or manufactured without the state's or government's legal license is fraudulent. Counterfeit currency have become more prevalent in Indian market, as the technology evolves[1].During recent times, 4.6% counterfeit Indian currency was detected in RBI, while 95.4% in other banks[2].Circulation of fake currency is increasing at an alarming rate every year, which is of great concern. Identifying counterfeit currency is a matter of national importance because of the adverse impact that it has on the economy. It diminishes the value of currency notecausing inflation, which makes markets unstable and

hinders trade. These days, counterfeit currency notes are so flawless that it is nearly impossible to distinguish them apart from genuine currency notes. Almost every feature of the original currency, with the exception of a few, may now be imitated easily. Manually checking every currency in a transaction takes a lot of time, is messy, and increases the risk of ripping of currency. Normal citizens are the ones who are most impacted by fake currency since it is very difficult to recognise them and they are transferred from one hand to another very easily. "Fake Note Detector Machine" is the primary tool that is currently accessible for common citizens to detect counterfeit currency, which is available only in banks and not everyone can access[3].The State-owned bank of Pakistan uses a public relations effort including an application for mobile devices that detects fake cash in an effort to assist the public. A knowledge about the security features of the currency may assist some in spotting fake currency, however, illiterate people cannot find the difference between a fake and real currency. In addition, these features are challenging to detect with the human eye or by touching[1].

The rate at which automated money detection techniques and frameworks are being developed is concerning. Numerous industries, such as banking, rail ticket windows, retail stores, and changing currencies services, depend on reliable and affordable fake money detection systems. Banknotes are used in financial transactions. The availability of counterfeit currency on the global market has substantially increased. Fake currency is a major issue in many businesses. The prevalence of fake currency have an adverse impact on the nation's financial sector[4], [5].As image processing advances, new methods of spotting counterfeit money are being created by examining certain security elements including watermarks, concealed pictures, safety threads, along with dynamically changeable inks. It is crucial to take out the particular data with the money picture and select the best image processing technique to get the desired outcome.The basic steps of an image processing method are to obtain the image, find the edges, and convert the image to grayscale, feature extraction, image segmentation and generating. The shortcomings of this method like less detection accuracy and difficulty in extracting security features made this system inefficient[6].Watermarks, holographic patterns, safety threads, and anti-copier designs, and other characteristics are examples of anti-counterfeit techniques that are now being utilized to stop banknotes imitation in general. Due to the abundance of fake currency in circulation and the complexity of the detection methods, which use a variety of detecting sensors, including magnetic, infrared (IR), and ultraviolet (UV)sensors, it is challenging to regularly check for counterfeit notes. Because of this, it is challenging for average users to detect fake currency[7]. There are approaches based on traditional computer vision techniques that aim to overcome this challenge and provide alternate options like, using nearest neighbour interpolation, evolutionary algorithms, fuzzy systems, and histogram equalisation. However, the primary issue with these systems is their limited capacity and low accuracy.

Recognising the currency notes is difficult for those who are visually impaired. Therefore, it is necessary to develop a smartphone application that can identify Indian currencies. To aid in the identification for those who are blind, the Reserve Bank of India has added identification marks based on intaglio printing on banknotes worth Rs. 100 and more. But yet, blind people have trouble distinguishing between different denominations of cash. Client-server architecture is used by the majority of smartphone applications for cash detection; the image is processed via the cloud, which lengthens processing times and necessitates internet access.[8].Since forgery techniques constantly advance in technology, it is getting more difficult to confirm a currency's authenticity. Only RGB (red, green and blue) colour combinations may be seen by the human eye. In contrast, far-infrared (FIR) and ultraviolet (UV) rays of any wavelength can be detected via hyperspectral imaging (HSI).Since UV light and digital signatures are faster and simpler means of detecting fake currency, HSI is not frequently employed in the field of counterfeit currency detection[9], [10]. Since HSI employs spectral data taken from the picture of the phony cash, it can detect fake money even in its presence of safety mechanisms, but with a reduced and more challenging pace. Therefore, this may provide an unique and possibly more reliable method of recognizing currencies like coins and

old banknotes that do not include security features[11].Many techniques for identifying counterfeit money were first presented years ago. Most outdated processes are still done by hand, that's not only time-consuming, costly, and incorrect but also impractical. Further research is being conducted; however, it won't help to lessen the losses resulting from fraud. Artificial intelligence (AI) has been utilized in the banking sector to identify counterfeit cash using machine learning as well as data mining. [12], [13].

Using the ML method It took a lot of work and intensive testing to determine whether fraudulent cash could be identified using Support Vector Machines (SVM)[14]. To predict fraud currencies, supervised and unsupervised algorithms were also used[15], [16]. The categorization approach is the most often applied methodology for detecting unauthorized financial transactions. [17]–[19].The Deep Learning methodology has demonstrated remarkable efficacy in resolving practical problems, where the complexity and number of layers decrease as data volume grows. As a result, deep learning isoften regarded as one of the predominant technologies incomputing[4], [5].Convolutional neural networks (CNNs) used in deep learning (DL) have beaten traditional machine learning methods and even humans in categorization challenges. CNNs were recently employed in certain present initiatives towards money authentication along with fake identification having excellent outcomes[20].The deep CNN model eliminates the need for manual feature extraction, as deep learning algorithms have showed remarkable performance in such tasks. Using the given dataset for training, the model improves its ability to spot counterfeit currency notes[21].In medical to banking, artificial intelligence (AI) has revolutionized a number of industries through its introduction and implementation. The creation of reliable and effective techniques for identifying counterfeit money notes is crucial for financial safety and preventing counterfeiting efforts. The identification of counterfeit cash is a crucial endeavor since it may have serious consequences for society and the economy.In this framework, a novel approach that utilizes AI-powered Game Theory optimization methods in combination using Generative Convolutional Neural Networks (CNN) along with Long Short-Term Memory networks (LSTM) to transform the field of counterfeit cash identification.

This novel approach helps to preserve the integrity of cash circulation and protect financial institutions while also improving the precision and effectiveness of identifying counterfeit currency.The majority of conventional methods for detecting counterfeit money have relied on governed by rules and heuristic based algorithms. Although somewhat successful, these techniques frequently fall short of the ever-changing tactics used by counterfeiters.On the other hand, AI-powered system takes a comprehensive and flexible strategy, enabling to identify a variety of counterfeit cash variants, such as those with progressively more intricate patterns and characteristics. Generative LSTM networks for sequence modeling and Convolutional Neural Networks (CNNs) to feed feature extraction are the foundations of this methodology. Together, these parts examine minute characteristics and trends in currency notes, giving the system an unmatched level of precision in identifying real from fake money. Moreover, the use on Game Theory optimization, an advanced technique which enhances the ability to make choices of the framework and minimizes false positives along with false negatives. AI-driven Generative CNN-LSTM technique for fake cash detection, which is tailored for Game Theory, has a significant potential effect. By offering a resilient and flexible approach which might be used on different platforms along with real-time applications, this is anticipated to improve the overall safety of banking systems, safeguard both customers and businesses from fake currency, and help preserve the health of the economy. It will go into further detail about the approach's details in the parts that follow, outlining its methodology, technological foundations, and benefits over more conventional counterfeit detection techniques.

The following were the key contributions for this paper:

- This research provides a novel approach that combines Long Short-Term Memory networks (LSTM) using Generative Convolutional Neural Networks (CNN) for the detection of

counterfeit currency. The outcome is a high-performing combination among image feature extraction as well as sequence modelling.

- This combination improves detection accuracy by enabling the model to catch minute visual characteristics including temporal patterns in money notes.An important development is the application of optimization techniques from Game Theory.
- The framework's method for making decisions is improved by utilizing the ideas of game theory, which lowers the frequency for false positives as well as false negatives.
- This implies because the method is extremely precise and flexible enough to adjust to changing counterfeit tactics. Because of its platform-independence, the suggested solution is adaptable and usable with a range of systems and equipment.

The remaining portions of this paper are organized as follows: Section 2 lists relevant works, while Section 3 concentrates on the problem statement; Section 4 shows the suggested Game Theory Optimized Generative CNN-LSTM method for detecting counterfeit currency; Section 5 displays findings from the evaluations; and Section 6 provides conclusion and future work of the concluded paper.

2. RELATED WORKS

Mohan and Veeramani [6]suggested a method to identify the fake currencies that are so prevalent in the Indian Market. According to this method, through isolating safety threads characteristics from a money note, fake cash may be identified. To detect counterfeit money, the most popular method—transfer learning with Alex net—is employed. Convolutional, max pooling, dropout, ReLU activations and fully connected layers make up Alex net. Transfer learning's three layers are adjusted to meet the proposed criteria.This method achieved a mean accuracy of 81.5% and 75% for original and fake currencies respectively. The drawback of this method is that pre-processing steps were not taken to avoid the noise in the captured images of the currencies, and the other attributes like the money's surface was not considered for effective counterfeit currency detection.Ali et al.[1]proposed a method to identifycounterfeit currencies using a highly innovative and powerful model Generative Adversarial Networks (GAN). It is employed to separate original data items from generated ones and identify generative imitation samples. This generating network along with the discriminator network are the two modules used by GANs, an intriguing kind of neural network system. To develop a Discriminator Neural Network, data is taken from the training set and generated data.The damage caused byeach Discriminator's network functions are modified throughout training. After training, the model can distinguish between counterfeit andgenuine notes, that are 80% accurate.The discriminator component of GANs serves as a sorting system for identifying the images. DeepMoney can be examined onnew generative models as they are developed in the machine learning field to produce better and more potent outcomes.

This method resulted in low accuracy rate without the use of enhancedMulticlassclassifiers. The design and quality of counterfeit money may differ greatly. It might be difficult for algorithms trained on one kind of money to apply to another. Yildiz et al.[4]proposed a deep learning technique to detect counterfeit currencies.The objective is to fine-tune the pre-trained Convolutional Neural Networks (CNN) in order to provide an effective and precise method for determining the authenticity of the currencies.Database or dataset collection is the first stage in currency detection through image processing. The final three layers of the pre-trained AlexNet were replaced as the initial stage of fine tuning. To enhance the capacity for non-linear problem solving, a Rectified Linear Unit (ReLU) layer was included.The fully connected layer, the Softmax layer and the classification output layer are used in place of the fine tuning in order to retrain Google Net to categorise new images.The first layer of the CNN VGG16 correlated each image with the input layer.It is likely to claim that currency recognition is incredibly accurate, but failed to implement in real-time.Zhang et al.(2019)proposed a method to recognise currencies using Deep Learning.

By removing the currency characteristics layer by layer, CNN is utilized as a monetary detection model to increase the reliability of the experimental results. To begin with, money photos must be gathered within the training data set. Additionally, the trial results must be analyzed. Sorting the data, selecting the currency pictures that best suit the experiment's requirements, and adding the selected picture to the data set are all necessary steps before training the model. This Multilayer Perceptron (MLP) layers receives the training data, uses them to extract features, classifies the currencies based on those characteristics, and finally recognizes the currency to train the model. The volume and diversity of annotated datasets including examples of authentic and fake. Pham et al.[7] proposed a method using visible-light image captured by smartphone camera to detect counterfeit currenciesbased on Deep Learning Technique. The first fake currency detection algorithm developed based on CNN that makes use of visible-light images captured using smartphone cameras. Compared to older methods that take pictures of currency using many sensors, that's more beneficial. To lessen the undesired impact of the backdrop on the reliability of detection, the CNN is fed the nearby Region of Interest (also known as ROI) around the centre of the coin as inputs rather than the full picture. The Class Activation Mapping (CAM) approach is used to search the ROIs for the currency traits that are most crucial for distinguishing between genuine and counterfeit cash.Of all the CNN architectures, ResNet18 provided high accuracy with a rate of 96%. When compared to actual money notes, imitation currency samples are rather uncommon. This disparity in class could bias model predictions and reduce the precision of detection.

Pachon et al. [20]recommended a method to detect fake currencies using deep learning. The money should be stored in a dark room with little to no light. To emphasize the important security aspects, an ultraviolet (UV) light having an average frequency of 365 nm is shone on the currency. Each of these elements are recorded using a video camera and transmitted through an integrated device. CNN is then supplied the image and is tasked with determining the legitimacy of the cash. Transfer-Learning (TL) is then employed for training the models using the suggested technique. The dataset was divided into three groups, and the four already trained architectures were chosen: AlexNet,SqueezeNet, ResNet18, as well as InceptionV3.In contrast with different models, AlexNet's models have a slower convergence rate during transfer learning, which is consistent with SqueezeNet's models. Monitoring actual money notes, the management of actual money notes may give rise to concerns regarding privacy and security, irrespective of the motivation over the dataset collection. It is crucial to use caution while handling and storing such data. Veeramsetty et al. [8]suggested a platform-neutral application that uses deep learning to recognize Indian money. For usage in online and mobile apps, an innovative small Convolutional Neural Network (CNN) architecture is developed to recognize Indian currencies efficiently. The CNN model has been trained, verified, and tested using a newly created dataset of Indian currencies. Such CNN-based mobile and internet applications will use the recognized money note as the basis for their written and audio output. TensorFlow is used to generate the suggested model, which is then improved by selecting the ideal hyperparameter values and assessed utilizing transfer learning towards popular CNN designs. The accuracy rate obtained through the proposed methodology is 87.5%.It might be difficult to support several languages and localizations, particularly for apps that serve a broad Indian user base.It may be quite difficult to make an application available to users suffering disabilities, including those who have vision problems.

The majority of current fake cash detection techniques rely on basic criteria and algorithms based on rules, both of which have a number of drawbacks. These techniques usually fail to keep up with the constantly changing strategies used by counterfeiters, which causes missing counterfeit notes along with a rise in false positives that annoy genuine users. They fail to be as strong when managing the various patterns and values of banknotes, as well as not as effective of handling minute counterfeit variants. Furthermore, the system's dependence of classical approaches limits their adaptability and implementation in different situations. There is a research gap in this area because there isn't a complete and flexible solution which makes use of advanced technologies, like artificial intelligence, deep learning, and based on information methods, to get around these constraints and offer a more precise, independent of platforms, and fast method of detecting counterfeit currency. In order to protect banks, insurance companies, and customers from the widespread danger of counterfeit cash, a new strategy is required to address the constant difficulties offered by counterfeiters. This novel

technique has the ability to transform the fake money detection environment and greatly improve the reliability and safety of money transfers globally by utilizing advanced technologies and creative approaches.

3. PROBLEM STATEMENT

The issue this study attempts to solve is how to detect the counterfeit currency that is so common in today's markets. Counterfeit currency is such a curse to the society, resulting in number of negative impacts like decline in the value of real money, price inflation as a consequence of an unjustified artificial expansion of the money supply, and a decline in the social acceptance of paper money.Counterfeit banknotes aregetting increasingly common over time. Real and phoney bank notes are differentiated using systematic approaches employing bank noteauthentication. Currently, a vast array of applications is accessible, including automated teller machines, check-out lanes, businesses that exchange money, motels and banks.The current techniques to identify counterfeit money are frequently struggling with accuracy, cost,time requirementsandalso, they are not readily available to the general public[20].This paper proposes novel deep learning algorithms that uses Generative CNN-LSTM, optimized using game theory to address these issues.

4. PROPOSED GAME THEORY OPTIMIZED GENERATIVE CNN-LSTMMETHOD FOR FAKE CURRENCY DETECTION

The process for detecting counterfeit cash that is being provided starts with the vital phase of data collecting, which includes photos of real banknotes as well as artificial counterfeit images. The model is trained using these data sources as its basis, which enables it to load up on the minute distinctions between real and fake banknotes. The fundamental component of this method is the combination of two innovative technologies: the Convolutional Neural Network (CNN) performs feature extraction from real and fake images, whereas the Generative Adversarial Network (GAN) generates images of counterfeit currency that are thoroughly meant to simulate real banknotes. The model is able to comprehend and recognize complex spatial aspects because to this combination.Moreover, the analysis gains a temporal element from the Long Short-Term Memory (LSTM) network, which makes it possible to identify complex patterns and connections in banknote picture series. An exclusive aspect of this approach is game theory optimization, which assures the very realistic pictures of counterfeit money that are created, hence improving the generator's performance while rendering it very difficult for the discriminator to distinguish between real and fake notes. In the end, the model combines information obtained by CNN, LSTM, and GAN to provide a thorough comprehension of the currency pictures.It uses these collected insights to identify whether a picture is a genuine currency or a fake one. This results in a reliable and flexible approach for detecting counterfeit cash, which has significant consequences for improving the banking system's security. Fig 1 Shows the overall methodology diagram for proposed Game Theory Optimized Generative CNN-LSTM Model for fake currency detection.

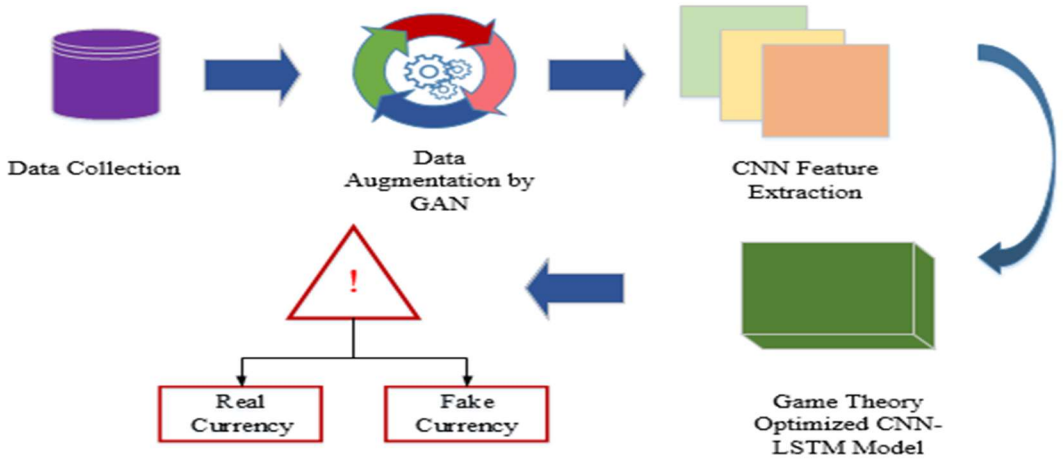

Fig 1: Proposed Game Theory Optimized Generative CNN-LSTM Model For Fake Currency Detection

4.1 Data Collection

The dataset is obtained from the website Kaggle[22], containing 4002 images of Indian currency in all denominations, that are valid since 2020. The dataset includes photossnapped using the Redmi Note 5 Pro and images that were downloaded from the Google images page.The dataset contains three directories namely, train, andtestwhich were very useful in classifying the images of the Indian currencies.Banned notes worth 1000 and 500 rupees are not included in this collection.

4.2 Data Augmentation

The dataset must contain avarious collection of real currency and fake currency samples. The very inventive and potent generative model known as Generative Adversarial Networks (GANs) is employed to produce fake samples that have resemblance to the actual notes. The greatest level of reliability may be achieved in distinguishing between real and counterfeit money using GANs. GANs, or generative adversarial networks, are incredibly intriguing neural network structures made up of two modules: the component that discriminates as well as the module that generates. Several encouraging results were achieved after applying GANs on the dataset. The discriminative method D determines the probability whether any data gathered by generator M is either created by G or is derived using training data, whereas the generative model creates fictitious currency samples. The generative model G's loss as well as energy functions may be expressed mathematically as eqn. (1).

$$\mathrm{GL} = \frac{1}{n}\sum_{1}^{n}[\log\left(1-\left(D\left(G(y)\right)\right)\right)] \quad (1)$$

Additionally, the discriminator's loss function may be written as in eqn. (2).

$$\mathrm{DL} = \frac{1}{n}\sum_{1}^{n}[logD(x) + \log\left(1-\left(D\left(G(y)\right)\right)\right)] \quad (2)$$

In this case, x stands for the currency from the data, y for the generator's sample, and G for the generator and D for the discriminator.

Eqn. (3) outlines how both the discriminator and the generator are trained with the objective reduce the loss function.

$$min_{tt}max_{D}L(G,D) = E\big(x - P_{data}(x)\big)\big[\log\big(D(x)\big)\big] + E\big(z - P_{latent}(z)\big)[\log\Big(1-D\big(G(z)\big)\Big)] \quad (3)$$

Where, $E\ [log\ (\big(D(x)\big))]$ represents the sample's log-likelihood, D makes an attempt to distinguish the created sample from the real sample. The expected log-likelihood of D given a sample that was generated by G is represented by the second term in the equation.The expectation of the generator that a sample it generates will trick the discriminator is represented by $(1 - D(G(z)))$. As a result, the discriminator and the generator are set up in the GAN as a minmax framework.

4.3 Generative CNN-LSTM Model

The objective of the feature retrieval module is to extract the descriptive feature parts from the paper banknote sample. For this case, features are extracted using a CNN. Color, size, shape, and perceptible characteristics are a few of the distinctive characteristics that CNN regularly uses to recognize banknotes. A supervised version for the CNN algorithm is utilized for extracting the CNN feature. The CNN has input, hidden, then output layers. In the CNN model, the subsampling procedures layer along with the convolution layer both have been referred by the term the feature extractor layer. The image of a money note is composed of several local characteristics that are detected by the convolutional layers. These characteristics include the identification mark, safety threads, copper and broad golden strip, among many additional safety features. Particularly intricate features may be picked up by the filters when the image passes through every layer. To obtain the regional feature, the input of every neuron within the convolution layer of neurons is connected with the locally susceptible area located in the layers beneath it. The suggested Game Theory Optimized Generative CNN-LSTM Model's overall architectural diagram is displayed in Fig. 2.

Journal of Theoretical and Applied Information Technology
15th March 2024. Vol.102. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

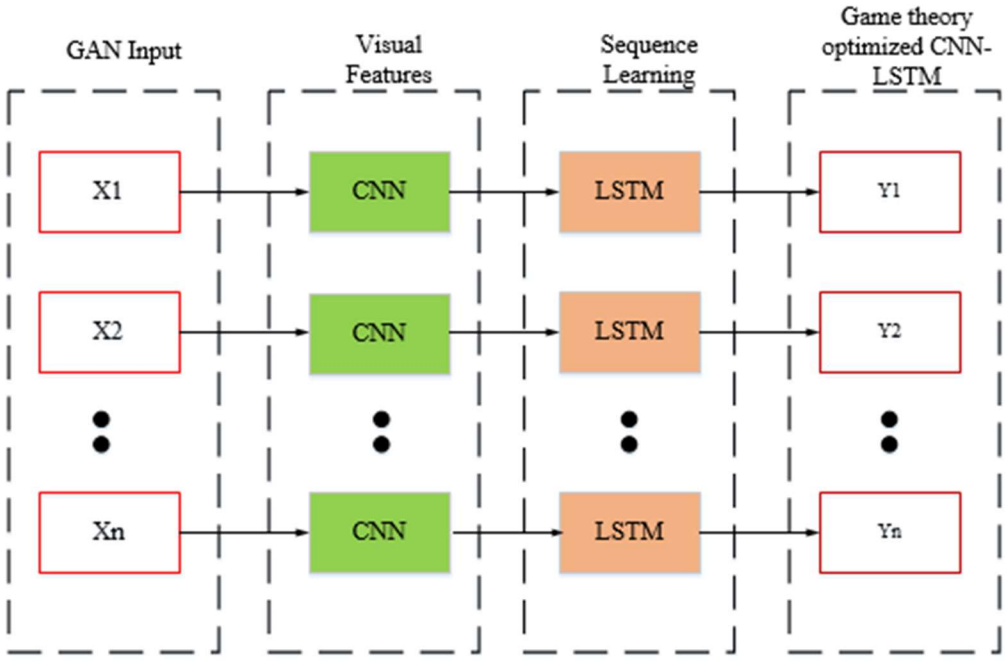

Fig 2: Architecture Diagram For Proposed Game Theory Optimized Generative CNN-LSTM Model

ReLU stands for Rectifier Unit, which is the most often utilized activation function to feed CNN neurons' outputs. CNN usually extracts top-level characteristics from the last output layer of the model. Additionally, the CNN algorithm models usually use two-dimensional (2-D) convolution filters to analyze RGB and grayscale pictures. A CNN processes the input of a currency note picture in the first step Convolutional layers, pooling layers, along with activation functions are used by CNNs to recognize and extract relevant details from pictures of currency notes. A collection of map features which depict the visual data on the currency note are the stage's outputs. The main elements and functions of an CNN algorithm to feature extraction towards the identification of counterfeit cash are as follows:

4.3.1 Convolutional Layer

This type of layer applies several filters upon the input picture in order to carry out the convolution process. Certain characteristics, including edges, corners, or surfaces, are detected by each filter. In order to recognize appropriate patterns on money notes, the filters are acquired during the training phase. The mathematical expression shown below eqn. (4) may be used to illustrate the basic operation of a convolutional layer Feature maps are produced by performing convolution, often known as cross-correlation, among an input image (I) as well as a collection of learnable filters (L).

$$(M) = I * L \quad (4)$$

Here, this convolution operation is denoted by "*". Structures and characteristics found in the input picture that the filter has identified are captured by the feature map.

4.3.2 Activation Function (ReLU)

The feature maps are subjected, element-by-element, to an activation function subsequent to convolution. One popular activation function is the Rectified Linear Unit, has the following eqn. (5).

$$R'(x) = max(0, x) \quad (5)$$

Considering the derivative for the function R(x), the statement "R'(x) = max (0, x)" provides a piecewise function. According to the value of x, the derivative R'(x) in this expression takes on several values. R'(x) equals x if x is bigger or less equal to 0. R'(x) equals 0 if x is

below 0. In order to assist the network, recognize intricate patterns, this function adds non-linearity.

4.3.3 Pooling Layer (Max Pooling)

Feature maps are down sampled using pooling layers, which lowers their spatial dimensions. Max pooling, for instance, may be expressed as follows in eqn. (6).

$$O(a,c) = max(R'(a,c)) \quad (6)$$

Where, O (a, c) the equivalent place in the pooling layer's output, is given the maximum value. It picks the highest value from a set of neighbouring values.Pooling preserves the most important properties while removing less important data, which contributes to the network's translational invariance.CNNs often have several convolutional layers with ever more complicated filters. Gradually, abstract characteristics are extracted by each layer.Fully Connected Layers, determine the last predictions upon the currency note's legitimacy, the flattening feature maps are run across fully connected layers following feature extraction.

4.3.4 Long Short-Term MemoryApproach

In the fields like deep learning as well as artificial intelligence, RNN (recurrent neural network) architectures with Long Short-Term Memory (LSTM) have become more prominent. It is especially made to overcome the shortcomings of conventional RNNs in handling disappearing or expanding gradient issues and capturing long-range interdependence. Within the area of fake currency detection, generative long short-term memory (LSTM) networks are essential because they can model temporal sequences of data and identify patterns which simple images alone could miss. A kind of recurrent neural network (RNN) called an LSTM network is made to identify long-term relationships in sequential data.LSTM networks' main characteristics and parts are Memory Cells, Gates, State Maintenance, and Activation Functions. These algorithms can analyze a series of observations or properties taken from a money note within its context of detecting fake currency.The essential component within an LSTM network is the LSTM cell. It is made up of several gates, including the cell state (e), forget gate (r), output gate (u), as well as input gate (n). The information flow inside the cell is controlled by these gates.The input gate (n) selects the new data that will be added to the cell state. It considers the hidden state from before (h(t-1)) and the current input (x(t)). The input gate formula is expressed in eqn. (7).

$$n(x) = \sigma(G\_i * [d(x-1), t(x)] + k\_i) \quad (7)$$

Where,n(x) denotes the output of the input gate; the activation function of the sigmoid is represented by σ.The input gate's weight matrix is denoted by G_i.Concatenating the prior hidden state with the current input is represented by the expression $[d(x-1), t(x)]$.

Forget gate (r) makes the decision about which data that the previous state of the cell (e(x-1)) must be ignored or lost. The formula for calculating it is denoted in eqn. (8).

$$r(x) = \sigma\,(G\_r * [d(x-1), t(x)] + k\_r) \quad (8)$$

Cell State Update (e) the input and forget gates are used to update the cell state (e(x)). It considers which data to save from the previous state $(f(t) * c(t-1))$ while controlling the transmission of information and updating with new information$(i(X) * tand(G_e * [d(x-1), t(x)] + k_e))$. Eqn. (9) is the formula for updating the cell state.

$$e(x) = r(x) * e(x-1) + i(x) * tand(G\_e * [d(x-1), t(x)] + k\_e) \quad (9)$$

Output Gate (u), this gate determines the value of the following hidden state (d(x))in eqn. (10).

$$u(x) = G\_u * [d(x-1), t(x)] + k\_u \quad (10)$$

Hidden State (d), the output of the LSTM cell, which is affected by both the cell's state as well as the output gate, is known as the hidden state (d(x)). The formula to compute it is denoted in eqn. (11).

$$d(x) = u(x) * tand(e(x)) \quad (11)$$

LSTM networks acquire their feature maps following feature extraction. The patterns of sequence and temporal relationships seen in the features are to be modelled by the LSTM. This enables the network to take into account the features' temporal evolution, making it very helpful for identifying counterfeit money that could have variable or changing properties. After processing the series of feature maps, the LSTM network learns to identify patterns and variances that point to fake money. The LSTM cells preserve hidden states that extract pertinent data from prior feature maps, allowing the framework to distinguish between temporal along with spatial complexities.

4.3.5 Game Theory Optimization

The Game Theory Optimised Generative CNN-LSTM approach for Fake Currency Detection relies heavily upon game theory optimisation. This simplifies the Generative Adversarial Network (GAN) training phase easier. In this procedure, both the discriminator and the generator play a game of strategy to enhance the generator's capacity to produce remarkably accurate counterfeit banknote images. Finding a Nash equilibrium—a situation in which neither party had a desire to alter its approach unilaterallyis the fundamental goal of the concept of game theory. The two participants within this adversarial game within the setting of the GAN consist of the discriminator along with the generator. Generator (G) First the generator's approach aims to produce representations of counterfeit money which are as accurate as reasonable. Its goal is to produce extremely realistic-looking counterfeit banknotes in order to maximise the likelihood of deceiving the discriminator. The discriminator uses precise image classification to distinguish between authentic and counterfeit cash. It attempts to classify the photos as accurately as possible. Finding an equilibrium among the generator's loss (the ability to produce counterfeit money) along with the discriminator's loss (the ability to recognise counterfeit money) represents the game's objective function in eqn. (12).

$$F(A,I) = -E[log(I(x))] - E[log(1 - I(A(z)))] \quad (12)$$

When evaluating actual banknotes (x), the discriminator's loss is measured by $E[log(I(x))]$. E [log (1 - I(A(z)))] is the discriminator's loss while evaluating fake banknotes issued by the generator (A(z)). By increasing the second term, the generator hopes to reduce F(A, I) and make it harder to enable the discriminator to differentiate the counterfeit banknotes that are created.To identify the Nash equilibrium, both the discriminator and the generator are updated repeatedly during the training phase. The discriminator gets better at telling real money from false, whereas the generator adjusts its approach to produce counterfeit that is more accurate. Extremely effective counterfeit detection is the result of this ongoing advancement.

5. RESULTS AND DISCUSSION

The AI-powered Game Theory Optimized Generative CNN-LSTM technique for Fake Currency Detection has been proven to be incredibly effective at accurately and versatilely detecting counterfeit currency. This approach has achieved innovative outcomes within a beneficial combination of Generative Adversarial Networks (GANs) for strategic game optimization, Long Short-Term Memory (LSTM) networks during temporal pattern recognition, and Convolutional Neural Networks (CNNs) to feed feature extraction. It establishes an innovative standard within the field of money authentication with its capacity to distinguish even the smallest changes between real and fake money, regardless of the face of developing counterfeiting tactics. The created counterfeit cash is extremely convincing due to the Nash equilibrium reached by game theory optimization, making it progressively harder to tell apart from real banknotes.Thus, the novel way to counterfeit currency identification provides a strong and dependable solution that might significantly improve safety in monetary and banking systems. The proposed framework is implemented in python.

5.1 Performance Evaluation

For comparison the SVM, Alexnet and Linear Discriminant Analysis methods performance is compared with the proposed Game Theory Optimized Generative CNN-LSTMmodel. Precision, recall, F1-score, and accuracy were utilized as evaluation criteria for comparison. The

model was evaluated using these parameters are shown below:

Accuracy

A frequently used indicator to assess the effectiveness of categorization tasks. is accuracy. The accuracy is computed by dividing the total number of predicts by the number of right predictions. It is described using an eqn. (13).

$$Accuracy = \frac{RN+RP}{RP+AP+RN+AN} \quad (13)$$

Where, 'RN' means true negative ;'RP' means true positive ; 'AP' means false positive ; 'RN' means true negative; 'AN' means false negative.

Precision

A classification model's positive predictions are evaluated using a measure called precision. When false positive mistakes are expensive or undesired, it is especially crucial. To compute precision, use the formula below (14).

$$Precision = \frac{RP}{TP+F} \quad (14)$$

Where, 'RP' represents true positive and 'FP' represents false positive.

Recall

Recall, sometimes referred to as sensitivities or real-positive rate, is a statistic used to evaluate a classification model's capacity to accurately identify every relevant occurrence of a given class. The following eqn. (15) is used to calculate recall.

$$Recall = \frac{RP}{RP+A} \quad (15)$$

F1 Score

The F1 score is a statistic that combines accuracy and recall to give a fair evaluation of the effectiveness of a classification model. It is especially helpful when you're trying to balance reducing inaccurate results (precision) and avoiding false negatives (recall) while maintaining accuracy. Eqn. (16), which calculates the F1 score, is as follows.

$$F1\ score = 2 * \frac{Precision*Recall}{Precision+Re} \quad (16)$$

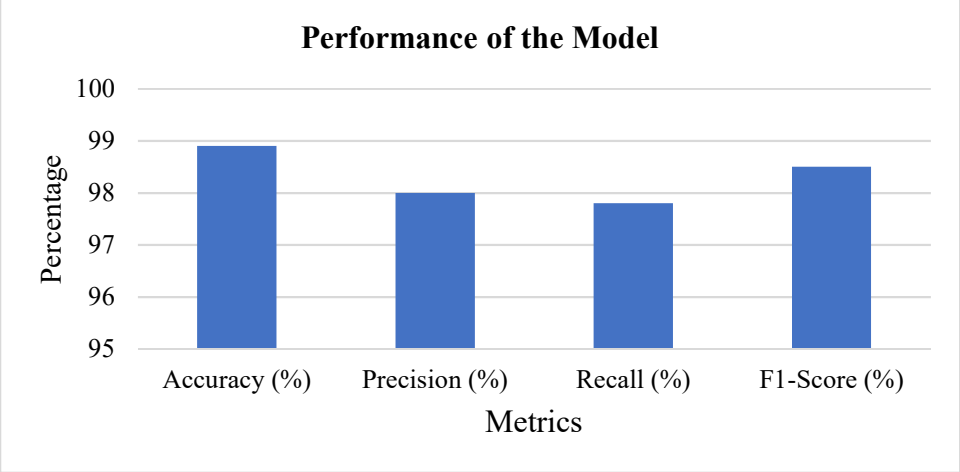

Fig 3:Performance Of The Proposed Game Theory Optimized Generative CNN-LSTM Model

An overview of the performance metrics for the "Proposed Game Theory Optimized Generative CNN-LSTM Model" is shown in the Fig 3. With an incredible 98.9% accuracy rate, the model was able to classify nearly all the data points correctly. Additionally, it showed a high accuracy of 98%, indicating that 98 percent of the times the model was correct when it predicted a favorable result. Moreover, the model achieved a recall of 97.8%, indicating that it correctly recognized 97.8% of the dataset's real positive events. The model's overall performance in classifying tasks is shown by its F1-Score of 98.5%, which reflects this great equilibrium between precision and recall.

Table 1: Performance Metrics Of Game Theory Optimized Generative CNN-LSTM Model With Existing Methods

Method	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
AlexNet[23]	87.74	86	88	85
SVM[24]	94	93	92	90
Linear Discriminant Analysis[25]	98.1	96	94	95
Proposed Game Theory Optimized Generative CNN-LSTM Model	98.9	98	97.8	98.5

The Table 1 provides an overview that compares the various techniques for identifying counterfeit money. Considering an accuracy of 87.74%, recall of 88%, precision of 86%, and F1 Score of 85%, the "AlexNet" approach was successful. Considering an accuracy of 94%, precision of 93%, recall of 92%, and an F1 Score of 90%, the "SVM" approach showed better results. "Linear Discriminant Analysis" outperformed the other techniques, achieving 98.1% accuracy, 96% precision, 94% recall, and a 95% F1 Score. With an astonishing F1 Score of 98.5%, accuracy of 98.9%, precision of 98%, along with recall of 97.8%, the "Proposed Game Theory Optimized Generative CNN-LSTM Model" beat all other approaches, though. With a high degree of accuracy (98.9%), precision (98%), recall (97.8%), F1 Score (98.5%), and overall efficiency, the suggested Model which relies upon Game Theory Optimized Generative CNN-LSTM stands out to be a particularly efficient method for detecting fake currency. It is a promising option for such applications.

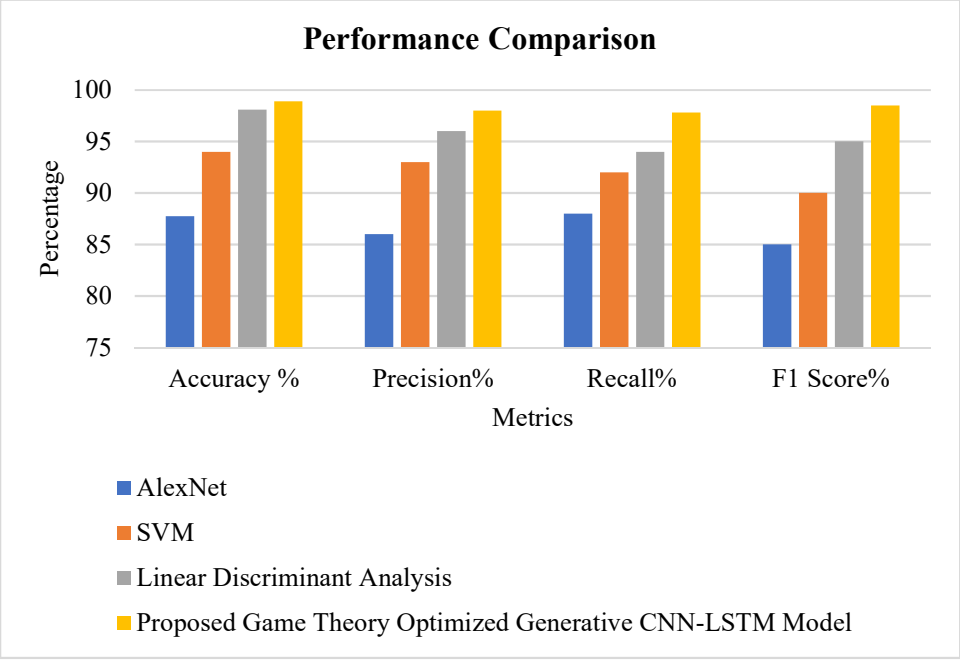

Fig 4: Graphical Depiction Of The Performance Metrics Of Proposed Game Theory Optimized Generative CNN-LSTM Model With Existing Approaches

The Fig 4 compares several techniques for identifying counterfeit cash. With an amazing 98.9% accuracy, 98% precision, 97.8% recall, and a remarkable F1 Score of 98.5%, the " recommended Game Theory Optimized Generative CNN-LSTM Model" is clearly the best performance. This approach, which utilizes Game Theory Optimized Generative CNN-LSTM, performs exceptionally well and is the best option for detecting counterfeit money since it has exceptional accuracy, precision, recall, along with overall efficiency.

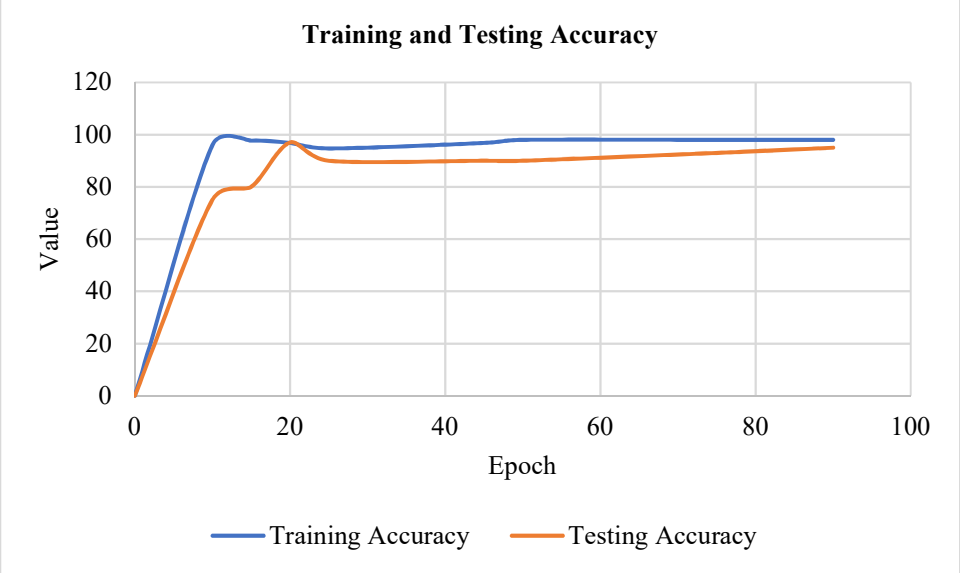

Fig 5:Graphical Depiction For Training And Testing Accuracy Of Proposed Game Theory Optimized Generative Cnn-Lstm Method

The Fig 5 shows a Game Theory Optimized Generative CNN-LSTM approach's training and testing accuracy towards the identification of counterfeit cash. The training accuracy is initially set at 0%, which denotes a lack of learning. The training and testing accuracy levels of the framework both gradually rise during training, demonstrating the model's capacity to recognize patterns and provide precise predictions. Approaches such as Game Theory Optimized Generative CNN-LSTM show notable gains, with testing accuracy of 95% and training accuracy of 98%. This shows that the properties needed for detecting phony cash have been effectively obtained and adapted by the model. The Game Theory Optimized Generative CNN-LSTM approach is an appropriate selection for this application because to its consistent and significant rise in testing accuracy, which shows its durability and usefulness in successfully recognizing fake cash.

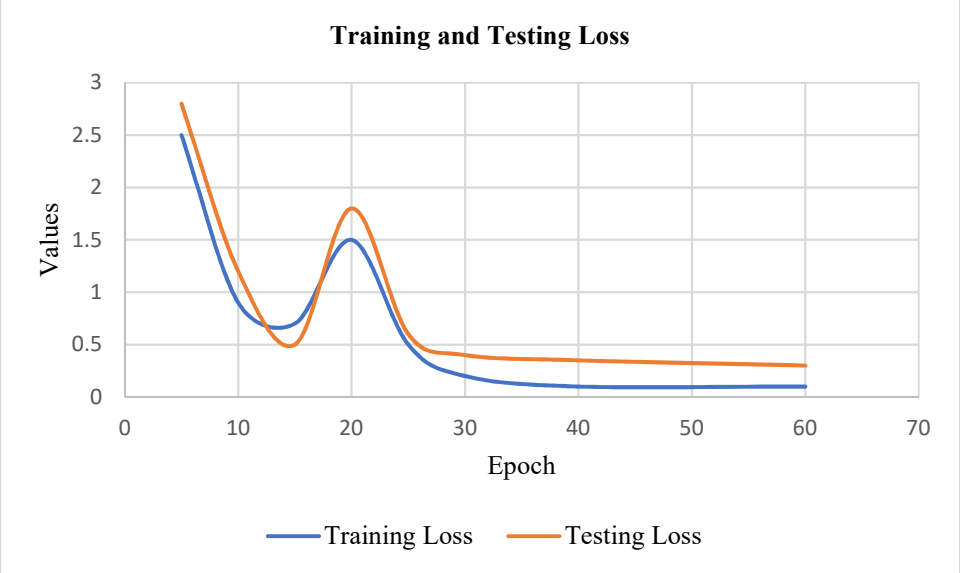

Fig 6:Graphical Depiction For Training And Testing Loss Of Proposed Game Theory Optimized Generative CNN-LSTM Method

The training and testing loss values in the Game Theory Optimized Generative CNN-LSTM approach used to identify counterfeit cash are shown in the Fig 6. The framework has to be performed better because its initial training and testing loss levels have been very high. On the other hand, the loss values gradually drop as the framework is utilized, indicating an effective process of learning. The decreasing loss values seen in both training and testing indicate that the Game Theory Optimized Generative CNN-LSTM approach is improving in terms of reducing mistakes and correctly classifying instances of phony cash. These loss curves' contraction to low values suggests the model is picking up new information and generalizing successfully. Overall, this shows that the Game Theory Optimized Generative CNN-LSTM approach is improving its performance for the identification of phony cash significantly, demonstrating its capacity for real time applications.

5.2 Discussion

The process of detecting counterfeit money begins with gathering data, which includes photos of real banknotes as well as artificial counterfeits. These data sources serve as the basis for training the model so that it might pick up on the minute characteristics that set authentic banknotes apart from counterfeit ones. This approach is based on combining innovative technologies: the Convolutional Neural Network (CNN) gathers features from actual and imitation money to ensure the algorithm can identify fine spatial details, whereas the Generative Adversarial Network (GAN) painstakingly creates counterfeit currency images that closely resemble genuine ones. A temporal component is further added by the Long Short-Term Memory (LSTM) network, which can recognize detailed correlations and patterns in currency picture patterns. The game-theoretical optimization is a unique feature that promises the counterfeit graphics created are extremely realistic, making it difficult for the discriminator to distinguish among genuine and false notes. The model combines knowledge obtained through CNN, LSTM, as well as GAN to provide a thorough comprehension of banknote pictures. It makes use of this information to determine if a picture depicts a real banknote or a fake one, providing a flexible and reliable way to improve safety within the financial sector.

6. CONCLUSION AND FUTURE SCOPE

A novel approach to the problem of detecting counterfeit cash involves the AI-driven Game Theory Optimized Generative CNN-LSTM technique for Fake cash Detection. By utilizing a variety of innovative technology, this technique takes a comprehensive approach to the issue and

achieves remarkable accuracy and flexibility. With the use of game theory optimization, Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and Generative Adversarial Networks (GANs) are integrated to create a potent tool for differentiating real banknotes from fake ones. It might greatly improve the safety of transactions involving cash and banking systems.The technique's comprehensive approach, which combines temporal and geographical analysis, results in unmatched accuracy in the identification of counterfeit money. Since of its versatility, the model is over time since it keeps working even when counterfeiters come up with new methods. It supports the reliability and safety within the monetary system by accurately identifying counterfeit money. This technique may be used for current time fraudulent cash detection in a variety of industries, such as retail, banking, and ATM networks.

The Game Theory Optimized Generative CNN-LSTM approach powered by AI has a potential and wide future scope towards the identification of fake currency. This strategy can develop into real-time fraudulent cash detection systems as technology progresses, boosting security in a variety of commercial and banking environments. The technology may be broadly available to consumers by integrating it into mobile applications. Additionally, financial services can be strengthened against fake threats by using it widely in banks and other enterprises. Enhanced algorithmic models for producing even more realistic counterfeit money might result from ongoing studies and developments, pushing the technology to advance additionally. Expanding the use of this technique in ATM networks, retail stores, and banks can improve total financial safety on a bigger scale. Due to the concepts underpinning this method's cross-domain flexibility, it may be used to detect fraudulent objects in a variety of domains, from recognizing fake imagery to finding fake papers and products, hence increasing its usability and influence across a range of sectors. This approach is expected to be crucial in the future for protecting financial services and making the entire world a safer, more fraud-resistant place.

REFERENCES

[1] T. Ali, S. Jan, A. Alkhodre, M. Nauman, M. Amin, and M. S. Siddiqui, “DeepMoney: counterfeit money detection using generative adversarial networks,” *PeerJ Comput. Sci.*, vol. 5, p. e216, Sep. 2019, doi: 10.7717/peerj-cs.216.

[2] N. Gautam, R. K. Saud, and L. Bhandari, “Demonetisation in India and its Effect in Nepal,” *Sch. J.*, pp. 228–239, Dec. 2021, doi: 10.3126/scholars.v4i1.42482.

[3] K. S. Warke, R. Kanthi, D. Makadia, S. Mogarkar, and P. Pawar, “COUNTERFEIT CURRENCY DETECTION USING IMAGE PROCESSING,” vol. 9, no. 2, 2022.

[4] A. Yildiz, “Banknotes Counterfeit Detection Using Deep Transfer Learning Approach,” *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 5, pp. 8115–8122, Oct. 2020, doi: 10.30534/ijatcse/2020/172952020.

[5] Q. Zhang, W. Q. Yan, and M. Kankanhalli, “Overview of currency recognition using deep learning,” *J. Bank. Financ. Technol.*, vol. 3, no. 1, pp. 59–69, Apr. 2019, doi: 10.1007/s42786-018-00007-1.

[6] L. Mohan and V. Veeramani, “Real Time Fake Currency Note Detection using Deep Learning,” *Int. J. Eng. Adv. Technol.*, vol. 9, no. 1S5, pp. 95–98, Dec. 2019, doi: 10.35940/ijeat.A1007.1291S52019.

[7] T. D. Pham, C. Park, D. T. Nguyen, G. Batchuluun, and K. R. Park, “Deep Learning-Based Fake-Banknote Detection for the Visually Impaired People Using Visible-Light Images Captured by Smartphone Cameras,” *IEEE Access*, vol. 8, pp. 63144–63161, 2020, doi: 10.1109/ACCESS.2020.2984019.

[8] V. Veeramsetty, G. Singal, and T. Badal, “Coinnet: platform independent application to recognize Indian currency notes using deep learning techniques,” *Multimed. Tools Appl.*, vol. 79, no. 31–32, pp. 22569–22594, Aug. 2020, doi: 10.1007/s11042-020-09031-0.

[9] T. H. Chia and M. J. Levene, “Detection of counterfeit US paper money using intrinsic fluorescence lifetime,” *Opt. Express*, vol. 17, no. 24, p. 22054, Nov. 2009, doi: 10.1364/OE.17.022054.

[10] S. Baek, E. Choi, Y. Baek, and C. Lee, “Detection of counterfeit banknotes using multispectral images,” *Digit. Signal Process.*, vol. 78, pp. 294–304, Jul. 2018, doi: 10.1016/j.dsp.2018.03.015.

[11] S.-Y. Huang, A. Mukundan, Y.-M. Tsao, Y. Kim, F.-C. Lin, and H.-C. Wang, "Recent Advances in Counterfeit Art, Document, Photo, Hologram, and Currency Detection Using Hyperspectral Imaging," *Sensors*, vol. 22, no. 19, p. 7308, Sep. 2022, doi: 10.3390/s22197308.

[12] J. Chaquet-Ulldemolins, F.-J. Gimeno-Blanes, S. Moral-Rubio, S. Muñoz-Romero, and J.-L. Rojo-Álvarez, "On the Black-Box Challenge for Fraud Detection Using Machine Learning (II): Nonlinear Analysis through Interpretable Autoencoders," *Appl. Sci.*, vol. 12, no. 8, p. 3856, Apr. 2022, doi: 10.3390/app12083856.

[13] A. Da'u and N. Salim, "Recommendation system based on deep learning methods: a systematic review and new directions," *Artif. Intell. Rev.*, vol. 53, no. 4, pp. 2709–2748, Apr. 2020, doi: 10.1007/s10462-019-09744-1.

[14] S. Gopane and R. Kotecha, "Indian Counterfeit Banknote Detection Using Support Vector Machine," *SSRN Electron. J.*, 2020, doi: 10.2139/ssrn.3568724.

[15] D. Choi and K. Lee, "An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation," *Secur. Commun. Netw.*, vol. 2018, pp. 1–15, Sep. 2018, doi: 10.1155/2018/5483472.

[16] Y. Zeng and J. Tang, "RLC-GNN: An Improved Deep Architecture for Spatial-Based Graph Neural Network with Application to Fraud Detection," *Appl. Sci.*, vol. 11, no. 12, p. 5656, Jun. 2021, doi: 10.3390/app11125656.

[17] W. Hilal, S. A. Gadsden, and J. Yawney, "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances," *Expert Syst. Appl.*, vol. 193, p. 116429, May 2022, doi: 10.1016/j.eswa.2021.116429.

[18] M. N. Ashtiani and B. Raahemi, "Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review," *IEEE Access*, vol. 10, pp. 72504–72525, 2022, doi: 10.1109/ACCESS.2021.3096799.

[19] A. Ali *et al.*, "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review," *Appl. Sci.*, vol. 12, no. 19, p. 9637, Sep. 2022, doi: 10.3390/app12199637.

[20] C. G. Pachón, D. M. Ballesteros, and D. Renza, "Fake Banknote Recognition Using Deep Learning," *Appl. Sci.*, vol. 11, no. 3, p. 1281, Jan. 2021, doi: 10.3390/app11031281.

[21] K. Bhavsar, K. Jani, and R. Vanzara, "Indian Currency Recognition from Live Video Using Deep Learning," in *Computing Science, Communication and Security*, vol. 1235, N. Chaubey, S. Parikh, and K. Amin, Eds., in Communications in Computer and Information Science, vol. 1235. , Singapore: Springer Singapore, 2020, pp. 70–81. doi: 10.1007/978-981-15-6648-6_6.

[22] V. Mane, "Indian Currency Note images dataset 2020." Accessed: Nov. 07, 2023. [Online]. Available: https://www.kaggle.com/datasets/vishalmane109/indian-currency-note-images-dataset-2020

[23]. Vijayaraghavan Laavanya, "Real Time Fake Currency Note Detection using Deep Learning," *Int. J. Eng. Adv. Technol.*, vol. 9, no. 1S5, pp. 95–98, Dec. 2019, doi: 10.35940/ijeat.A1007.1291S52019.

[24] T. Yadav, "Evaluation of Machine Learning Algorithms for the Detection of Fake Bank Currency." Accessed: Nov. 07, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9377127/

[25] G. Shokeen, "Analysis of Counterfeit Currency Detection Techniques for Classification Model." Accessed: Nov. 07, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/8777704/