NTU Journal of Engineering and Technology (2024) 3 (3) : 36-45
DOI: https://doi.org/10.56286/ntujet.v3i3.944

IRAQI Academic Scientific Journals

P-ISSN: 2788-9971 E-ISSN: 2788-998X
NTU Journal of Engineering and Technology
Available online at: https://journals.ntu.edu.iq/index.php/NTU-JET/index

Advanced Methods for Identifying Counterfeit Currency: Using Deep Learning and Machine Learning

Nama'a M. Z. Hamed[1], Fadwa Al Azzo[2]
1. Computer Engineering Department, North Technical University, Mosul, Iraq, 2. Computer Engineering Department, North Technical University, Mosul, Iraq

Article Informations

Received: 01-04- 2024,
Revised: 10-07-2024,
Accepted: 19-09-2024,
Published online: 26-09-2024

Corresponding author:
Name: Nama'a M. Z. Hamed
Affiliation : North Technical University
Email: *nmaa.manhal@ntu.edu.iq*

Key Words:
Counterfeit currency detection,
Machine Learning,
Deep Learning,
Iraqi Dinar,
Security Features,
advanced Techniques.

A B S T R A C T

Counterfeiting is a serious threat to economies because sophisticated counterfeit banknotes are becoming increasingly difficult to identify through conventional verification techniques, thanks to advancements in printing technology. In this work, we offer a thorough investigation of sophisticated methods for detecting counterfeit money that make use of deep learning and machine learning approaches. Using machine learning algorithms like Random Forest, Decision Tree Classifier, XGBoost, CatBoost, and Support Vector Machine (SVM) in addition to deep learning techniques like Convolutional Neural Networks (CNNs), VGG16, MobileNetV2, and InceptionV3, we examine the security characteristics of Iraqi dinar banknotes and build robust models. All of the models in our results had high accuracy rates, with CNN, CatBoost, and SVM showing particularly strong performance. These results demonstrate how effective cutting-edge technical solutions are in thwarting the dangers posed by counterfeit money, protecting national economies and reducing losses. Sustaining the security of international financial systems and keeping ahead of evolving counterfeiting strategies need ongoing study and development in this area.

Introduction

Modern society is experiencing a surge in counterfeit money due to major technology advancements; these can range from shoddy banknotes to intricately designed imitations. Even with the increasing number of online and electronic transactions, many people still find that actual banknotes are important. Furthermore, because governments can track the source of cash, electronic payment systems offer greater security and are vital in the battle against counterfeiting. It's critical to recognize and differentiate real banknotes from counterfeit ones. Comparing manual verification techniques to automated ones reveals that they are inefficient and slow. Contemporary printing methods yield banknotes with intricate details that could be hard for people to notice. More complex detection techniques are required since, despite the existence of UV recognition technology, it is not enough to combat sophisticated counterfeiting strategies [1].

Several image recognition-based identification technologies have been developed to examine banknotes for color, design features and specific data to ensure accurate authentication. In Iraq, the official currency is the dinar and the banknotes are in several denominations, namely fifty thousand dinars, twenty-five thousand dinars, ten thousand dinars, five thousand dinars, one thousand five hundred, and finally two hundred and fifty dinars [2].

The issue of counterfeit money circulating in many monetary systems is a serious threat to the economies and value of the currencies in those countries. The ability of counterfeiters to copy coins with frightening precision thanks to technological improvements has made it challenging to distinguish between real and fake money. Modern editing software and sophisticated printers are frequently used to create counterfeit money that is frequently identical to real notes. The global problem of legitimate currency becoming more and more muddled with counterfeit currency is pervasive [3].

In order to increase public knowledge of the security risks related to banknotes, central banks use a variety of direct-to-consumer and institutional marketing techniques. The goal of initiatives like smartphone applications for detecting counterfeit currencies and television commercials is to inform people about the dangers [4]. But a lot of people have trouble telling the difference between real and fraudulent money, especially those with low literacy skills. Some people handling cash in public places might not notice security elements. Furthermore, the identification of traits associated with counterfeit money might be made more difficult by torn, soiled, or damaged banknotes [5].

In order to increase public knowledge of the security risks related to banknotes, central banks use a variety of direct-to-consumer and institutional marketing techniques. The goal of initiatives like smartphone applications for detecting counterfeit currencies and television commercials is to inform people about the dangers. But a lot of people have trouble telling the difference between real and fraudulent money, especially those with low literacy skills. Some people handling cash in public places might not notice security elements. Furthermore, the identification of traits associated with counterfeit money might be made more difficult by torn, soiled, or damaged banknotes [5].

Produced without a valid government or state license, counterfeit money is meant to seem like real money in order to trick people. It is prohibited to produce or use since it is regarded as a type of fraud or counterfeiting. Innovative approaches have been put forth to address this issue, such as topic-based segment creation systems that effectively gather pertinent data [6]. Due to deep learning's superior performance in image classification tasks, convolutional neural networks (CNNs) in particular have gained widespread traction. An automatic solution is available when counterfeit currency is detected in real-time with accuracy thanks to a deep CNN model that was trained on a variety of banknote datasets [7].

The widespread occurrence of fake money presents difficulties for a number of industries, such as retail, banking, and currency exchange services. The increase in the creation of counterfeit notes can be ascribed to technological improvements like copy machines and scanners, which make it more difficult for the human eye to discern between real and false notes. Thus, strengthening banknote security features and installing counterfeit detection systems at ATMs and banks are essential steps [8].

In challenges involving currency detection, deep learning models—particularly CNNs—have demonstrated encouraging results, obviating the necessity for human feature extraction. Deep learning techniques have the ability to recognize counterfeit currency notes accurately because there are about 180 different currencies in the world, each with specific security features and sizes. Techniques for augmenting data, like color analysis and image enhancement, help cash detection algorithms become even more accurate [9].

The study attempts to address the serious threat that counterfeiting poses to Iraq's economy and stability by predicting counterfeit Iraqi cash using machine learning, deep learning, and transfer learning. It intends to use machine learning algorithms to examine characteristics and trends in both real and counterfeit Iraqi cash. To improve detection accuracy, deep learning—specifically, CNNs—will be used to automatically extract pertinent features from cash photos. In order to reduce the amount of extensive training data required, transfer learning will also be investigated as a means of adapting pre-trained models for Iraqi currency prediction. The study's overall goal is to

create a reliable system for identifying counterfeit Iraqi cash in real time, protecting the nation's financial stability and minimizing losses.

Related Works

The authors of [10] suggest utilizing a supervised machine learning algorithm to identify fake banknotes, attempting to tackle the difficulties caused by the pervasiveness of printing technologies and replication techniques. The movement of money, whether it be virtual or actual, gives bad people the chance to sabotage the financial system's regular operations. The creation of counterfeit money has a big effect on a country's economy and people's quality of life. Their research aims to overcome the drawbacks of conventional methods by utilizing machine learning techniques to improve counterfeit detection. They show through simulation results that our suggested machine learning model performs better than conventional methods, offering more accuracy in detecting counterfeit money. They hope to lessen the negative impact of fake notes on the financial system and the overall economy by utilizing cutting-edge algorithms, which will ultimately benefit society as a whole.

Researchers in [11] aimed to authenticate cash samples using both conventional methods and modern machine learning techniques. Leveraging image processing combined with machine learning, a false-identity detection success rate of 99.9% was achieved for paper currency. The research proposed employing K-Nearest Neighbors (KNN) followed by image processing for counterfeit money identification due to KNN's accuracy, especially with small datasets. By compiling accurate currency attribute data into a banknote authentication dataset, advanced computational and mathematical methodologies were applied. Through AI algorithms and image processing, high accuracy in data extraction was achieved. Results showed competitive performance of KNN alongside other techniques, with detection accuracies of Convolutional Neural Network (CNN): 67.88%, Support Vector Machine (SVM): 75.91%, and KNN: 72.26%, demonstrating the effectiveness of the proposed method in identifying counterfeit currency.

Authers in [12] addresses the pressing issue of counterfeit currency by proposing a system that utilizes deep learning techniques for detection. With the proliferation of advanced printing equipment, counterfeit notes have become a significant concern in the industry. Previous methods based on image processing, while effective, were limited in efficiency and time-consuming. Our system aims to overcome these challenges by leveraging deep learning to accurately detect counterfeit Indian currency notes. By utilizing the TensorFlow framework and its high-level API Keras, the model creation process is simplified, resulting in a less time-consuming and highly accurate solution. The results demonstrate promising confidence scores for both real and fake currency denominations, indicating the effectiveness of the proposed approach in identifying counterfeit notes.

Researchers in [13] examines the growing risk of counterfeit money, which is made possible by developments in color printing technology. Print businesses were the only places that could manufacture counterfeit notes, but these days, anyone can duplicate money that looks just like real money using a simple laser printer. The study uses machine learning algorithms like KNN and Support Vector Machine in conjunction with image processing techniques like image comparison, segmentation, edge detection, feature extraction, and grayscale conversion to address this problem. These techniques are used to distinguish between genuine and counterfeit money, providing useful resources for studies intended to slow the spread of counterfeit money.

This research in [14] addresses the growing prevalence of counterfeit money by proposing a deep learning-based approach for cash recognition. Conventional technologies that use hardware and image processing methods have not shown to be effective in detecting counterfeit money. By examining photographs of currency, the suggested method uses a deep convolutional neural network to identify counterfeit notes. The network acquires distinct features for the real-time identification of counterfeit currency by training it on a dataset that represents 2000 different types of currency notes. The deep CNN model provides excellent accuracy in detecting counterfeit currencies and does away with the requirement for manual feature extraction. To improve the accuracy of money recognition, a number of methods are also investigated, such as the African Buffalo Optimization Approach (ABO), generative adversarial networks (GAN), convolutional neural networks, recurrent neural networks (RNN), and classical neural networks. Findings indicate that the suggested buffalo optimization strategy outperformed conventional techniques like KNN and SVM, obtaining a specificity of 98.92% and sensitivity of 96.8%.

Reference [15] discusses Afghanistan's counterfeit currency problem, which has a big effect on the country's economy and presents difficulties for banks and other businesses. These organizations have access to authentication machines, but the general public does not have access to them. The research fills this vacuum by suggesting an image processing technique that analyses particular security characteristics to identify fake Afghan banknotes. First and second-order statistical features were extracted from the input photos, and the WEKA machine learning program was used to build the models. Random Forest, PART, and Naïve Bayes algorithms were then used for classification. The outcomes show that the suggested strategy is

successful in thwarting counterfeit money, with the Random Forest algorithm achieving an amazing 99% accuracy rate in identifying phone Afghan banknotes.

Researchers in [16] presents a novel method for identifying counterfeit banknotes using the support vector machine (SVM) technique. SVM is quite good at classifying banknotes as genuine or fake based on information taken from pictures, especially when it comes to pattern classification. The experiment's outcomes show that the SVM model outperformed the Perceptron model, which had an accuracy of 98.36%, with an accuracy of 99.55%. This novel algorithm provides a promising way to identify fake money in financial systems.

In [17] The suggested method entails utilizing MATLAB software to extract several features—such as security threads, bleed lines, edges, forms, textures, colors, and fluorescence—from the notes. For feature extraction and analysis, a supervised learning model—more precisely, the support vector machine (SVM)—is used. Using the SVM classifier, the system compares the extracted statistical features with those kept in a MAT file. Other techniques, including the black box algorithm, are also tested. The suggested method makes it easy to distinguish between real and false notes quickly and is fast to put into practice. An analysis of the system's performance demonstrates that SVM outperforms genetic bee colony (GBC) and support vector classifier (SVC) methods in terms of accuracy, precision, and F-score. Specifically, the proposed SVM model achieves an accuracy, precision, and F-score of 99.9%, demonstrating its effectiveness in detecting counterfeit currency.

Iraqi Dinar Security Features

The dinar currency in Figure (1) has a number of security measures in place to prevent counterfeiting and guarantee its legitimacy. Among these elements is the metallic printing on the upper left corner of the banknote, which adds an elusive shiny quality. The security thread, which is positioned at the upper middle area of the currency to increase its resistance to counterfeit reproduction, is another notable security element. The left side of the banknote also has a horse head watermark incorporated into it, which adds a distinctive and detailed detail that is difficult to duplicate. Additionally, the lower left portion of the money has a color-changing symbol that adds another degree of protection against unauthorized copying. Last but not least, the notes have an ultraviolet feature that, when exposed to ultraviolet light, glows to indicate the value of the denomination. This feature acts as a reliable means of authentication in the middle of the note. When taken as a whole, these security measures help to reduce the dangers of counterfeiting and protect the integrity of the dinar money.

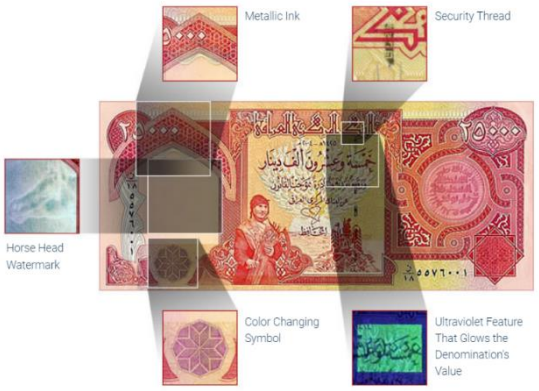


Figure 1. Iraqi Dinar Security Features

METHODOLOGY

The Model in Figure (2) describes a thorough method for creating and implementing machine learning models for the categorization of banknotes as authentic or fraudulent. It starts with a thorough overview of the dataset, stressing the importance of these models in financial security and the binary classification problem. The development of several deep learning models is then covered, including Convolutional Neural Networks (CNNs) like VGG16, MobileNetV2, and InceptionV3, each of which is designed to make use of pre-trained architectures for feature extraction and classification.

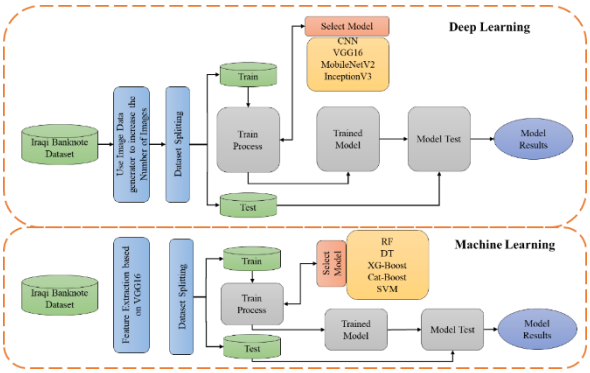


Figure 2. Complete Model Block Diagram

The article also discusses the feature extraction procedure based on the VGG16 model, which entails preparing datasets for training and testing, preprocessing picture data, and extracting features via transfer learning. It also covers the application of machine learning algorithms, each of which is set up with particular parameters for classification tasks, including Random Forest, Decision Tree Classifier, XGBoost, CatBoost, and Support Vector Machine (SVM).

Dataset Description

The data that is presented in Table (1) shows how banknotes are classified into real and fake categories. The training set consists of 1087 actual banknote instances and 558 false banknote instances. There are 272 banknotes in the testing set, 140 of which are genuine and 132 of which have been determined to be fraudulent. It looks like we have a binary classification problem here, and the objective is to create a model that can reliably identify real banknotes from fake ones. Financial institutions and law enforcement organizations need these models to stop counterfeiting. Researchers may train models that recognize patterns and characteristics of real currency by using machine learning techniques and algorithms. This will help identify counterfeit banknotes. With the ultimate goal of improving security measures inside the banking and financial sectors, this dataset offers a fundamental basis for creating and assessing such models.

Table 1. Dataset Size

Train	Real	Fake
1087	558	529
Test	Real	Fake
272	140	132

Convolutional Neural Network Implementation

A convolutional neural network (CNN) in Figure (3), a deep learning architecture that is frequently used for image classification tasks, is the model that is being described. It consists of multiple layers intended for processing and feature extraction from input images:

First, learnable filters are used to convolve input pictures using convolutional layers (Conv2D). The first Conv2D layer operates on images with 64x64 pixel dimensions and three color channels (RGB), using 32 filters of varying sizes. These filters identify a range of characteristics from the input photos, including patterns, textures, and edges. By setting negative pixel values to zero, activation functions—more especially, Rectified Linear Units (ReLU)—introduce non-linearity into the model.

Max Pooling Layers (MaxPooling2D) are added after the Conv2D layers in order to minimize spatial dimensions and manage overfitting. Using the maximum value from each region and down sampling the data, max pooling works on small sections of the feature maps. This model reduces the feature map dimensions by performing max-pooling with a pool size of (2, 2).

To convert the multi-dimensional feature maps into a one-dimensional vector, a flatten layer is added after the convolutional and max-pooling layers. Feeding the data into Dense Layers (completely connected layers), the next parts of the model, requires this step.

To acquire high-level representations of the features that the convolutional layers extracted, two Dense Layers are incorporated. ReLU activation is used in the first dense layer, which has 128 units and makes it easier to identify complicated patterns in the data. With a sigmoid activation function, the single unit that makes up the second dense layer. This last layer, which outputs the likelihood that the input image belongs to the positive class (class 1), is commonly used in binary classification problems.

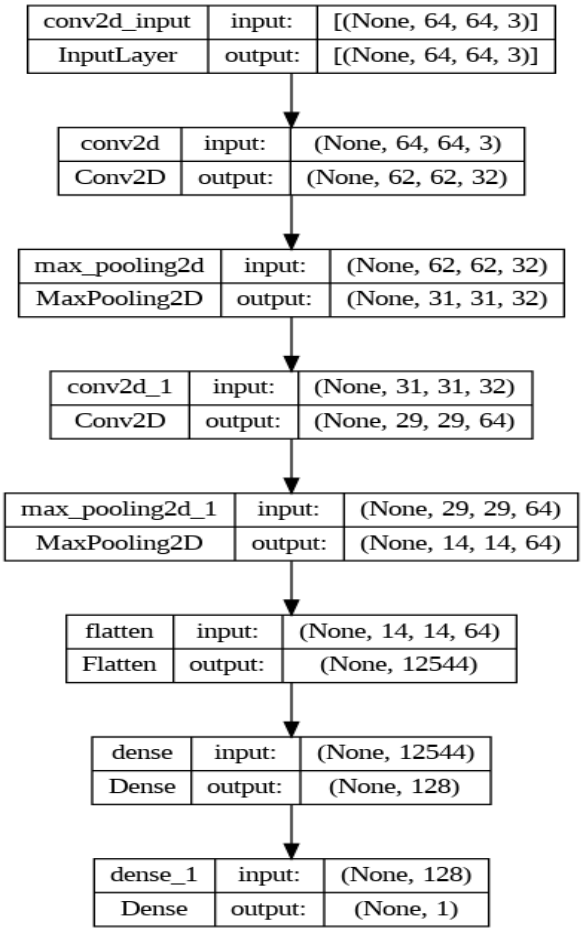


Figure 3. Convolutional Neural Network Design

All things considered, this CNN architecture successfully extracts hierarchical features from input photos, producing a model that can correctly predict results in image classification tasks. Convolutional and dense layers work together to teach the model how to identify patterns and use the retrieved features to inform decisions.

VGG16 Model Implantation

The presented model in Figure (4) employs a transfer learning methodology, making use of the VGG16 architecture that has been pre-trained on the ImageNet dataset. The 16-layer VGG16 convolutional neural network, which is mostly made up of pooling and convolutional layers, is renowned for its simplicity and depth. We may use the VGG16

model as a feature extractor by setting {include_top=False}, which excludes the fully linked layers at the top of the model. The input shape is defined as (224, 224, 3), which complies with the VGG16 model's input size. A Sequential model is built on top of the VGG16 base, with the first step being the Flatten layer, which converts the multi-dimensional feature maps into a one-dimensional vector. The input for later layers is this representation that has been flattened. In order to learn high-level features from the recovered VGG16 features, a Dense layer with 128 units and ReLU activation is added after the Flatten layer. After that, a Dropout layer is added with a dropout rate of 0.5 to promote robustness and generalization by randomly deactivating neurons during training and prevent overfitting. The output layer for binary classification tasks is a Dense layer with a single unit and sigmoid activation that is appended at the end. Its function is to estimate the likelihood that the input will belong to the positive class.

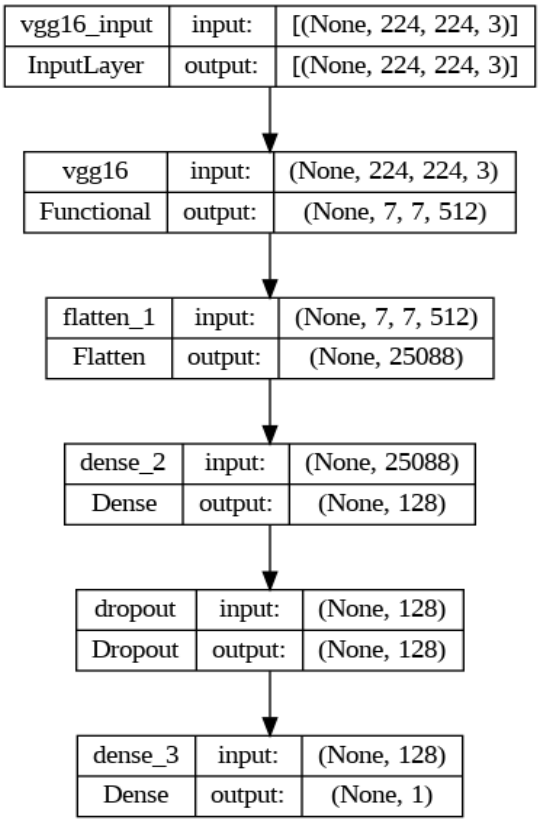


Figure 4. VGG16 Modified Model

In conclusion, this model applies a custom classifier on top of the pre-trained VGG16 network to modify the network for certain classification tasks. This allows for the extraction of significant characteristics from input photos. This strategy is especially helpful when dealing with little amounts of data since it makes advantage of the expertise acquired from training on massive datasets like ImageNet.

4.4 MobileNetV2 Model Implantation

The model presented in Figure (5) is a transfer learning strategy that makes use of the MobileNetV2 architecture, a convolutional neural network that is lightweight and built for embedded and mobile vision applications. Pre-trained weights from the ImageNet dataset are imported into the MobileNetV2 model, but `include_top=False` is used to exclude the top (completely connected) layers. With this setup, MobileNetV2 can function as a feature extractor, extracting pertinent features from input photos.

The pre-trained layers in the underlying MobileNetV2 model are frozen by setting {layer.trainable = False} for each layer to avoid them from being modified during training and possibly losing important learned features. This guarantees that the task-specific data will only be used to train the custom classifier layers that are put on top.

The Sequential model is used to construct the custom classifier. One-dimensional feature vectors are produced by flattening the output of the MobileNetV2 base model. To learn high-level representations of the retrieved features, a thick layer with 128 units and ReLU activation is added. In order to reduce overfitting, dropout regularization is used at a rate of 0.5, deactivating neurons at random during training. The output layer is then completed with a dense layer that has a single unit and a sigmoid activation function. This layer is appropriate for binary classification tasks, where it predicts the likelihood that the input will belong to the positive class.

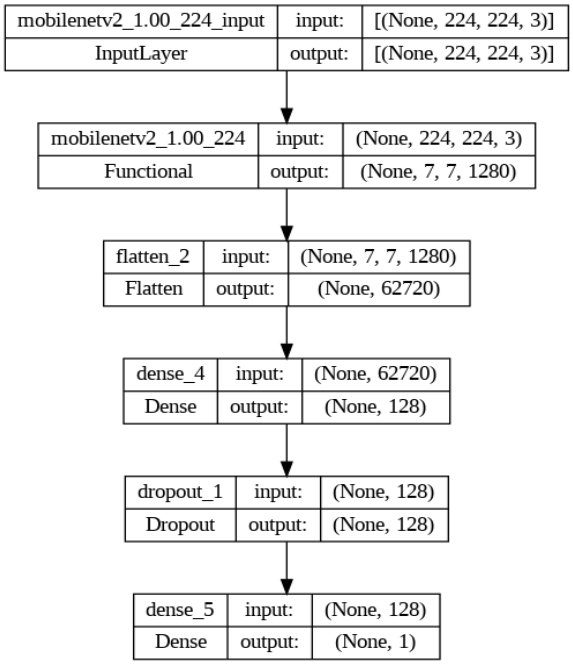


Figure 5. MobileNetV2 Modified Model

All things considered; this model makes use of MobileNetV2's potent feature extraction

capabilities to tailor the classifier to certain classification tasks. The model can function effectively with little training data by fine-tuning only the recently added layers, which makes it suitable for a variety of picture classification applications.

InceptionV3 Model Implantation

The model shown in Figure (6) uses a deep convolutional neural network called InceptionV3, which is optimized for image classification tasks. It is a transfer learning method. The fully connected layers at the top are excluded by setting `include_top=False}, and the InceptionV3 model is initialized with pre-trained weights from the ImageNet dataset. By using this technique, the InceptionV3 model may extract features from input photos and function as a feature extractor.

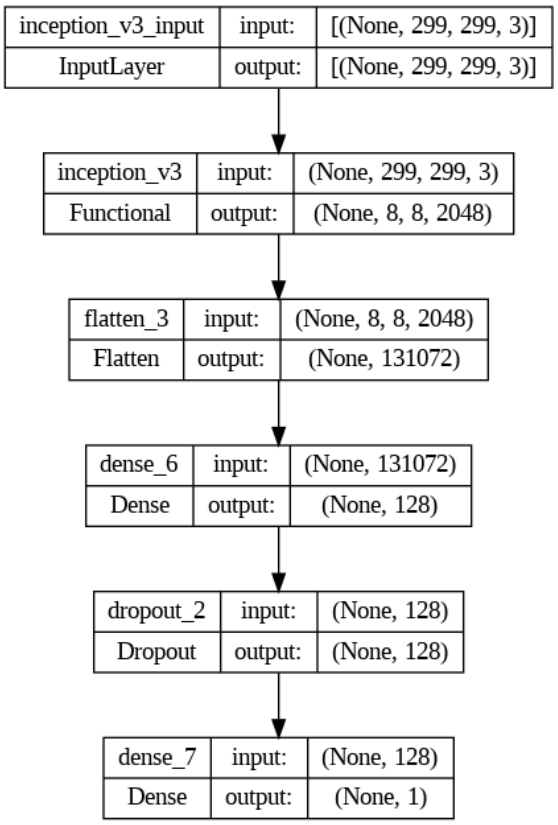


Figure 6. InceptionV3 Modified Model

The frozen InceptionV3 base is then used as the foundation for a bespoke classifier. After being flattened, the InceptionV3 model's output is fed into a dense layer with 128 units and ReLU activation to produce a one-dimensional feature vector. The retrieved features are mapped by this dense layer to higher-level representations appropriate for the current classification task. After the dense layer, a dropout layer with a dropout rate of 0.5 is added, randomly deactivating neurons during training to prevent overfitting. Lastly, the output layer consists of a dense layer with a single unit and sigmoid activation. This layer is appropriate for binary classification tasks, where it forecasts the likelihood that the input will belong to the positive class.

This model design adapts the classifier to particular classification problems while utilizing the robust feature extraction capabilities of the InceptionV3 model. The model can function effectively with little training data by fine-tuning only the recently added layers, which makes it suitable for a variety of picture classification applications.

Feature Extraction Based on VGG16 Model

This code snippet shows how to use transfer learning to create an image classification model using a pre-trained VGG16 model. It loads and preprocesses image data from a given directory first, dividing it into sets for testing and training. The VGG16 model is used as a feature extractor after being pretrained on ImageNet. To preserve learned features, the top layers are eliminated and the remaining layers are frozen. Using the updated VGG16 model, features are retrieved from the training and testing sets. Following their flattening and combination with the appropriate labels, these features are used to create training and testing datasets.

Lastly, CSV files containing the combined datasets are preserved for later use in model evaluation and training. All things considered, this procedure makes use of transfer learning to produce an efficient picture classification model with the least amount of data and computational resources needed.

Machine Learning Algorithm

These algorithms for machine learning cover a variety of methods for classification assignments. During training, Random Forest builds several decision trees and produces a forecast that is the class mode. To build a prediction model, the Decision Tree Classifier iteratively divides the dataset according to attribute values. Gradient boosting is used by XGBoost to iteratively improve decision trees' accuracy. CatBoost is designed to efficiently handle categorical data without requiring a lot of preprocessing. To identify data points, Support Vector Machine (SVM) builds hyperplanes in high-dimensional space. For repeatability, each algorithm is set up with a random state parameter, guaranteeing consistent outcomes over runs. Through a comparative analysis of their respective dataset performances, the optimal strategy for the particular classification problem can be determined.

Table 2. Machine Learning Algorithms Description

Algorithm	Description	
Random Forest	N-Estimatiom =100	Random State= 42
Decision Tree Classifier	-	Random State= 42
XG-Boost	-	Random State= 42
Cat-Boost	-	Random State= 42
Support Vector Machine	-	Random State= 42

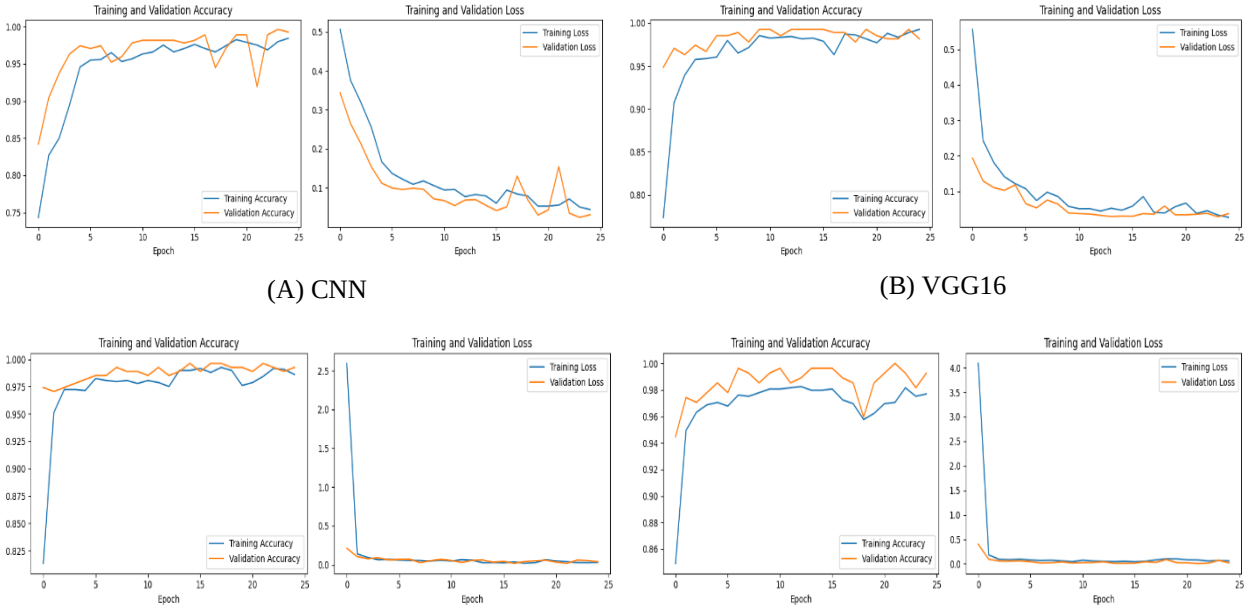
RESULTS

Deep Learning Results

The results in Table (3) from the evaluation of different models for classifying banknotes as real or fake indicate strong performance across the board. The Convolutional Neural Network (CNN) model achieves notably high accuracy, with a train accuracy of 98.44%, validation accuracy of 99.26%, and test accuracy of 99.26%, along with low corresponding loss values. Similarly, the VGG16, MobileNetV2, and InceptionV3 models also demonstrate high accuracy rates, with minor variations among them. VGG16 and MobileNetV2 exhibit slightly lower performance compared to CNN, with a train accuracy of 99.26% and validation/test accuracy of 98.16% for VGG16, and a train accuracy of 98.62% and validation/test accuracy of 99.26% for MobileNetV2. InceptionV3 performs admirably, with a train accuracy of 97.7% and consistent validation/test accuracy of 99.26%. Although InceptionV3's loss values are slightly higher than the others, indicating a slightly higher error rate during training and validation, all models demonstrate strong learning and generalization capabilities. Overall, these findings suggest that all models are well-equipped for accurately identifying real and fake banknotes, showcasing their effectiveness in contributing to security measures within the banking and financial sectors.

Table 3. Deep Learning Accuracy and Loss

Model	Train Accuracy	Train Loss	Validation Accuracy	Validation Loss	Test Accuracy	Test Loss
CNN	0.9844	0.0445	0.9926	0.0311	0.9926	0.03110
VGG16	0.9926	0.0270	0.9816	0.0377	0.9816	0.03770
MobileNetV2	0.9862	0.0299	0.9926	0.0383	0.9926	0.03829
Inception V3	0.977	0.0588	0.9926	0.0211	0.9926	0.02106



(A) CNN (B) VGG16

(C) MobileNetV2 (D) Inception V3

Figure 6. Accuracy and Loss Analysis

Machine Learning Results

The analysis of machine learning algorithms for classifying banknotes as real or fake reveals varying levels of performance across different models. Random Forest achieves a commendable accuracy, precision, recall, and F1-score of 96%, indicating robust performance across all metrics. The Decision Tree Classifier, however, demonstrates slightly lower performance compared to Random Forest, with scores of 83% across all metrics. XGBoost stands out with exceptional performance, boasting an accuracy, precision, recall, and F1-score of 97%, showcasing its effectiveness in classification tasks. CatBoost emerges as the top-performing algorithm, achieving high scores of 98% across all metrics, indicating superior performance compared to other algorithms.

Similarly, Support Vector Machine (SVM) exhibits strong performance, closely aligning with CatBoost with an accuracy, precision, recall, and F1-score of 98%. Overall, CatBoost, SVM, and XGBoost emerge as the top-performing algorithms, demonstrating high accuracy and reliability in classifying banknotes, while Random Forest also proves to be a robust choice (See Figure 7).

Table 4. Machine Learning Evaluation Metric

Model	Accuracy	Precision	Recall	F1-Score
Random Forest	0.96	0.96	0.96	0.96
Decision Tree Classifier	0.83	0.83	0.83	0.83
XG-Boost	0.97	0.97	0.97	0.97
Cat-Boost	0.98	0.98	0.98	0.98
Support Vector Machine	0.98	0.98	0.98	0.98

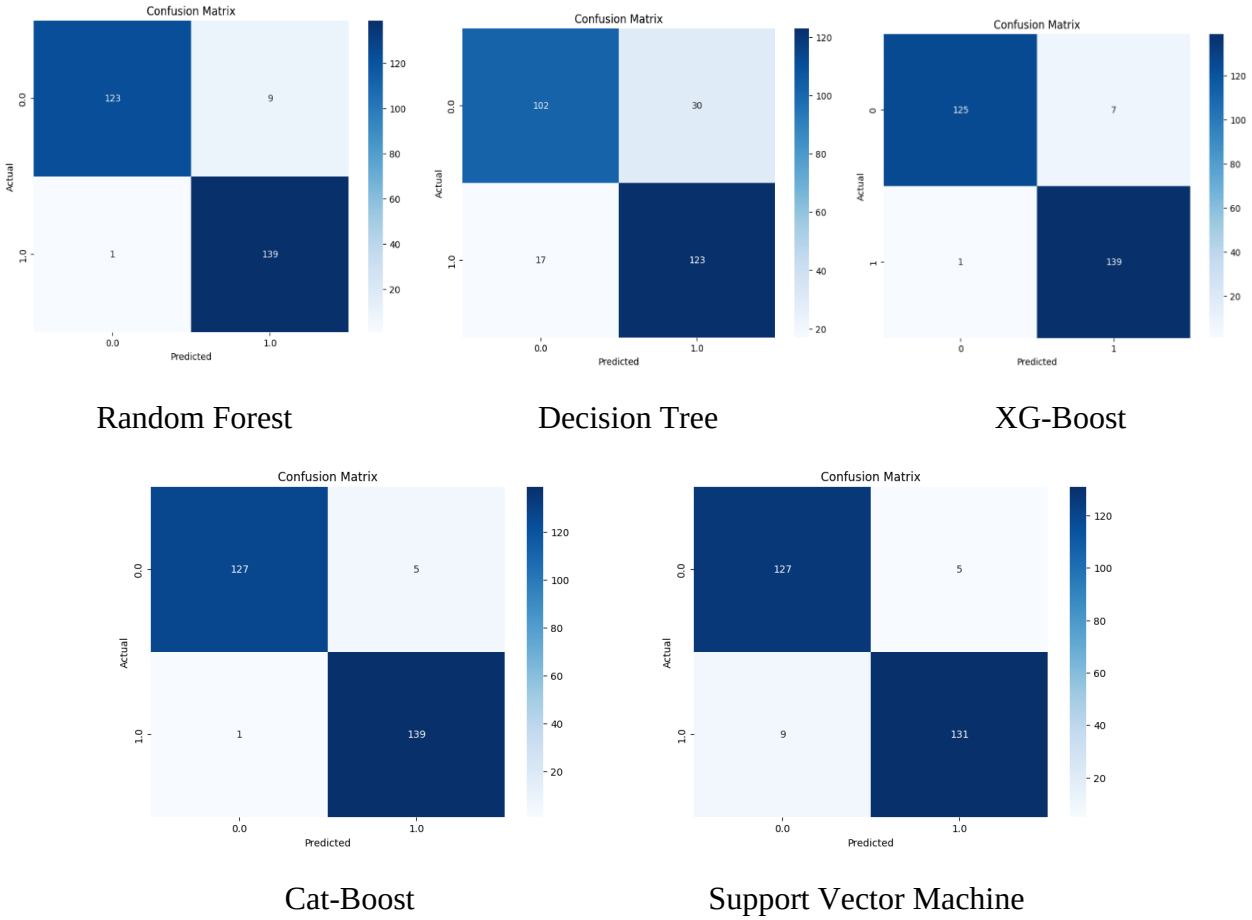


Figure 7. Machine Learning Algorithm Confusion Matrix

Conclusions

The increase in counterfeit money presents a serious risk to economies across the globe, thus protecting financial systems will require sophisticated detection and classification techniques. When it comes to recognizing complex counterfeit banknotes created using contemporary printing technology, traditional verification methods are frequently insufficient. Numerous image recognition-based identification solutions have been created in response to this difficulty, with an emphasis on ensuring correct authentication through the analysis of specific data, color, and design

aspects. This study examined several methods for identifying counterfeit money, emphasizing the value of deep learning, machine learning, and transfer learning in raising detection accuracy. Significant progress has been made in accurately differentiating between real and fake banknotes through the use of deep learning techniques like Convolutional Neural Networks (CNNs), VGG16, MobileNetV2, and InceptionV3, in conjunction with machine learning algorithms like Random Forest, Decision Tree Classifier, XGBoost, CatBoost, and Support Vector Machine (SVM).

The methodology of the study comprised a thorough review of the security aspects of the Iraqi dinar as well as the application of strong machine learning and deep learning models for the detection of counterfeits. The findings showed that all models had good accuracy rates. CNN stood out for its deep learning capability, while CatBoost and SVM were the best machine learning algorithms. The results highlight how successful cutting-edge technical solutions are in thwarting the dangers posed by counterfeit money. Financial institutions and law enforcement agencies can improve their capacity to detect and reduce the spread of counterfeit banknotes, protecting the integrity of national economies and reducing financial losses, by utilizing machine learning and deep learning techniques. Sustaining the security of international financial systems and keeping ahead of evolving counterfeiting strategies depend on ongoing research and development in this area.

Acknowledgments. Authers would like to thank North Technical University for Support.

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. 2019, no. 9, pp. 1–21, 2019, doi: 10.7717/peerj-cs.216.

[2] A. A. Abbas, "An Image Processor Bill Acceptor for Iraqi Currency," *Al-Nahrain J. Sci.*, vol. 22, no. 2, pp. 78–86, 2019, doi: 10.22401/anjs.22.2.10.

[3] M. Beare, "Counterfeit Currency," *Encycl. Transnatl. Crime Justice*, 2013, doi: 10.4135/9781452218588.n32.

[4] H. de Heij, "Banknote design for retailers and public," *DNB Occas. Stud.*, vol. 8, no. 3, 2010.

[5] F. van der Horst, J. Snell, and J. Theeuwes, "Enhancing banknote authentication by guiding attention to security features and manipulating prevalence expectancy," *Cogn. Res. Princ. Implic.*, vol. 6, no. 1, p. 73, 2021, doi: 10.1186/s41235-021-00341-x.

[6] S. R. Gross, "Senior Researcher Kaitlin Jackson Roll," *Natl. Regist. Exonerations Sept.*, vol. 1, p. 2020, 2014.

[7] J. Posetti *et al.*, *JOURNALISM , ' FAKE NEWS ' & Handbook for Journalism Education and Training*. 2020.

[8] A. Rajee, R. Ahmed, and S. Humaira Sunzida, "A Project Report on Fake Currency Detection," no. May, pp. 0–40, 2023, doi: 10.13140/RG.2.2.21616.43526.

[9] C. G. Pachón, D. M. Ballesteros, and D. Renza, "Fake banknote recognition using deep learning," *Appl. Sci.*, vol. 11, no. 3, pp. 1–20, 2021, doi: 10.3390/app11031281.

[10] T. M. Beigh, J. Arivazagan, and V. P. Venkatesan, "COUNTERFEIT CURRENCY DETECTION," *J. Emerg. Technol. Innov. Res.*, vol. 10, no. 3, pp. 356–358, 2023.

[11] D. S. Kodati, D. M. Dhasaratham, V. Srikanth, and K. M. Reddy, "Detection of Fake Currency Using Machine Learning Models," *Int. J. Res. Sci. Eng.*, no. 41, pp. 31–38, 2023, doi: 10.55529/ijrise.41.31.38.

[12] P. D. P. Patil, G. Varma, S. Poojary, S. Sawant, and A. Sharma, "Counterfeit Currency Detection based on AI," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 4, pp. 3022–3027, 2022, doi: 10.22214/ijraset.2022.41980.

[13] P. S. Rao, "Counterfeit Currency Detection Using Machine Learning," *Interantional J. Sci. Res. Eng. Manag.*, vol. 07, no. 12, pp. 1–10, 2023, doi: 10.55041/ijsrem27717.

[14] F. Antonius, J. Ramu, P. Sasikala, J. C. Sekhar, and S. S. C. Mary, "DeepCyberDetect: Hybrid AI for Counterfeit Currency Detection with GAN-CNN-RNN using African Buffalo Optimization," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 7, pp. 651–662, 2023, doi: 10.14569/IJACSA.2023.0140772.

[15] H. Ashna and Z. Momand, "Applications of Machine Learning in Detecting Afghan Fake Banknotes," 2023.

[16] H. K. Easa, A. A. Saber, N. K. Hamid, and H. A. Saber, "Machine learning based approach for detection of fake banknotes using support vector machine," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 31, no. 2, pp. 1016–1022, 2023, doi: 10.11591/ijeecs.v31.i2.pp1016-1022.

[17] S. Shinde *et al.*, "Identification of fake currency using soft computing," *Multidiscip. Sci. J.*, vol. 6, no. 2, pp. 1–11, 2024, doi: 10.31893/multiscience.2024018.