Scientific Journal of University of Benghazi

SJUOB (2025) 38 (2) Applied Sciences: Mohammed. et . al, 73 – 93
www.sjuob.uob.edu.ly

Developing and Evaluating an Explainable Deep Learning–Based User Interface for Libyan Currency Authentication.

Mohammed Masoud Mohammed[1]*, Aeman.I.G.Masbah[2], Mansaf M. Elmansori[2]

1. Department of Computer Science, Faculty of Science, Derna University, Libya.

2. Department of Computer, College of Technical Sciences - Derna, Libya.

DOI: 10.37376/sjuob.v38i2 | Received:15/09/2025 | Accepted:21/11/2025 | Publishing: 23/12/2025

ABSTRACT

The problem of counterfeit currency production and distribution is increasing, driven by technological advancements, particularly the development of advanced printing machines. The ongoing issue of counterfeit currency poses a significant threat to the national economy, necessitating the creation of an effective detection system. In light of this problem, this study proposes an intelligent system for identifying and detecting counterfeit Libyan currency. This system relies on deep learning techniques. Our proposed model is based on the EfficientNet-B4 controlled architecture, which seeks to optimize computing power and accuracy. In this study, the dataset was prepared and preprocessed using Gaussian filtering to reduce noise and normalize. The general framework developed here consists of two stages: The first stage is an intelligent filter that attempts to exclude any banknotes or images that are not Libyan currency, ensuring that only data related to Libyan banknotes is transmitted to the second stage of the model. The second stage is the core of the study, as it will determine whether Libyan currency is authentic or counterfeit. To improve the transparency of the model and enhance the understanding of its results, Grad-CAM software was used to generate heat maps that clearly show the banknote regions that contributed most to the model's decision-making. To demonstrate the system's usability, a mock-up user interface was designed to illustrate the system's analysis and provide a practical environment. The results demonstrated good classification performance, consistently exceeding 90%, demonstrating how the proposed approach can be effectively applied to these models in practical situations. The findings of this research provide a practical framework to help financial institutions mitigate counterfeiting as part of the relevant compliance objectives that will determine the security of the monetary system.

KEYWORDS: Libyan Currency, Counterfeit Detection, Image Classification, Deep Learning, Efficientnet-B4, Heatmap Visualization, Grad-CAM, User Interface.

Corresponding Author: Mohammed Masoud Mohammed, *mohammed.bwshnaty@gmail.com*

 ISSN: Online 2790-1637, Print 2790-1629
National Library of Libya, Legal number: 154/2018

1.INTRODUCTION

In today's continually evolving world, technology is changing at an unprecedented rate that causes an unimaginable degree of change in our lives and work. While these advancements have undoubtedly enhanced convenience, they have also created opportunities for various forms of misuse. The most notable is counterfeiting banknotes. Counterfeiting is not a new concern; it has existed for generations. However, new technologies increase the liabilities associated with counterfeiting. While measures have improved a lot in terms of increased security features in different denominations, and overall banknote security has improved, the skill of counterfeiting has also improved in a way that makes it difficult to differentiate between genuine and fake notes [1]. This problem is especially prevalent in countries that are politically and economically unstable. In these situations, without proper regulatory scrutiny, a burgeoning black market has spread counterfeit currency, which invariably threatens the financial system and undermines public confidence in the national currency. Moreover, it has economic implications, as the effects of currency forgery also present significant security and social challenges by disrupting the functioning of markets, obstructing normal operations for businesses, and increasing the workload of financial and security actors [2]. Paper money is still widely used in everyday transactions, even with the numerous solutions that have been put forth to lessen dependency on actual cash, such as smart cards, magnetic cards, and electronic payment systems. Because of this reliance on cash, counterfeiters continue to have opportunities to take advantage of the system. Therefore, we desperately need a reliable system that can differentiate between real and fake banknotes based on their visual characteristics [3-4]. When dealing with high-quality counterfeit copies, traditional verification methods such as visual inspection and ultraviolet (UV) analysis have proven ineffective. The situation requires the use of modern technology tools to provide more reliable and permanent alternatives for fraud detection. Counterfeit detectors are often available in banks, and these devices are not easily accessible to the general public. Given these limitations, the field needs a more accessible and user-friendly way to develop public confidence in currencies[5]. In that aspect, advanced technology in encompassing methods based on deep learning has demonstrated potential, most notably in image studies and with the identified subtle visual cues not easily observed by humans. The aim of this study is to devise an intelligent system that can detect and recognize authentic or counterfeit Libyan paper currency using current technology without using complicated or costly instruments. This study is accomplished by determining if any discrepancies or divergences are identified, which hints that the currency is counterfeit. Its ability to detect counterfeit bills accurately, quickly, and at low cost is of great value to banks, agencies of government, businesses, and the general public. Last, but not least, it is also an original way to keep up with technical advancements while utilizing sophisticated computational mechanisms for the benefit of the economy of Libya.

1.1.Deep Learning in Image Classification:

Deep Learning (DL) is a growing form of machine learning (ML), a form of artificial intelligence (AI), as shown in Figure 1. DL is built on multi-layer or "deep" neural networks (DNNs). This form of machine learning has become a game-changing technology in computer vision, notably with image classification [6].

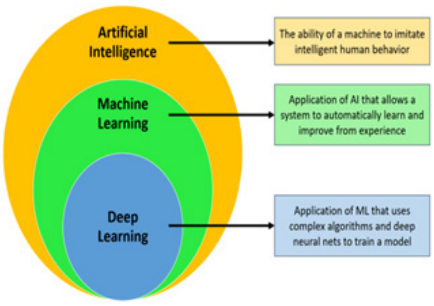

Figure (1): Relationship between AI, ML and DL

Consequently, deep learning is an algorithmically based on the structural and functional organization of the neural model of the human brain, wherein computational mod-

els can automatically extract, represent, and comprehend the high-dimensional and complex framework that composes large amounts of unstructured visual data [7].

Deep neural networks (DNN) are a form of artificial neural networks (ANN) characterized by a layering of neuron-like processing units, in which each layer produces more abstract feature representations through the nonlinear transformation of inputs. In order to classify images at the input layer, the deep neural network learns from the raw picture data, the pixel intensity value. The input layer learns pixel intensity value, and the hidden layers transform that value through pooling, activation functions, and convolutions to reduce or improve useful, discriminative features and meaningful learning features. Structure and parts develop into higher-level features (ex, shapes) from the low-level features (ex, textures, edges) learned in the first layer to the features learned in the hidden layers. The output layer will relate those higher-level features, low-level features, and potential objects from the predefined categories and give you the final classification. Figure 2 shows the internal structure of both ANN and DNN [8-9].

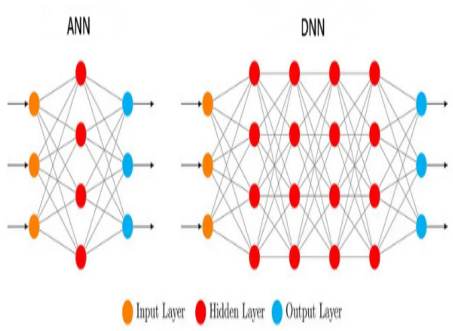

Figure (2): ANN and DNN structure.

In context, convolutional Neural Networks (CNNs) are a subclass of Deep Neural Networks (DNNs) for especially efficient and scalable processing of grid-structured data [10], typically digital image data. CNNs are designed with convolutional layers that can exploit spatial hierarchies of features and are really useful in many application areas in computer vision. The convolutional layer can be thought of as a multi-channel global filter inspired by human vision that is arranged to enter information through areas of special perception that break down the processing requirements of visual stimuli by hierarchically filtering increasingly complex stimuli [11]. A common CNN for image classification is typically built with three layers in mind:

-Convolutional Layer:

This applies a group of filters (kernels) to the image to determine low-level image features such as edges, corners, and textures while maintaining relationships between pixels spatially. A convolution is a mathematical operation that takes two inputs: one is an image matrix, and the other is a kernel or a filter.

-It will process an image matrix of size h × w × d with a filter size of

-The output size will then be, (Figure 3)[12].

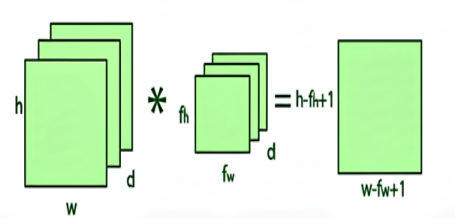

Figure (3): Image matrix multiplies kernel or filter matrix

-Pooling Layer: To decrease feature map spatial dimensions to reduce the computational cost, as well as increase invariance to small translations. Common pooling methods include max pooling and average pooling, (figure 4)[13].

 ISSN: Online 2790-1637, Print 2790-1629
National Library of Libya, Legal number: 154/2018

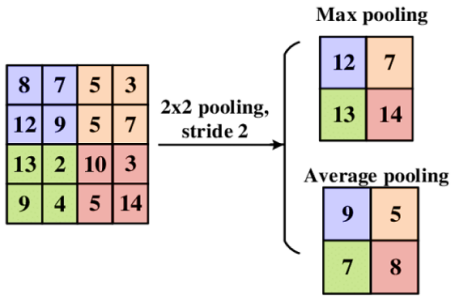

Figure (4): Illustration of max 2×2 pooling with a stride, comparing with the outputs of max pooling and average pooling

-Fully Connected Layer: This layer will flatten the feature maps into a vector and have fully connected (dense) connections to arrive at where we produce the final classification output. In fake note detection, this layer provides the final output probabilities of whether a note is "real" or "fake," applying an activation function such as the SoftMax or sigmoid. As shown in Figure 5, the CNN process converts the feature map matrix into vector representations, joins features, and applies activation functions like SoftMax or sigmoid to classify outputs. This integrated approach allows for robust hierarchical feature representations, crucial in complex visual recognition tasks like counterfeit currency detection [14].

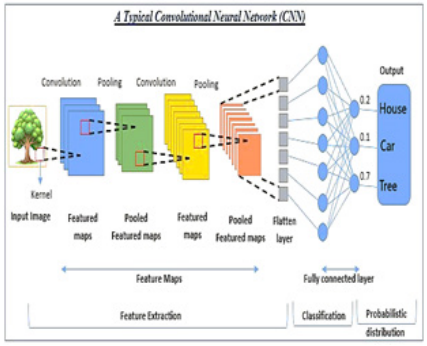

Figure (5): Workflow of convolutional, pooling, and fully connected layers.

1.2.Transfer Learning:

Transfer learning is a method of deep learning that improves model performance on small datasets by reusing knowledge from extensive datasets. This approach overcomes the limitations of deep learning, which often require large volumes of high-quality labeled data, by reusing knowledge from similar tasks with fewer data points [15]. In addition, transfer learning involves freezing initial layers of a pretrained model and retraining later layers to adapt to new domains. Fine-tuning allows for better refinement of task-specific features. Transfer learning offers advantages like shorter training time, better performance on smaller data sets, and lower computational costs, making it suitable for medical image analysis, fraud detection, and counterfeit currency detection. The EfficientNetB4 architecture is chosen for transfer learning [16].EfficientNetB4 is a mid-tier model with advanced accuracy and moderate resource usage cost, pre-trained on the ImageNet dataset. It uses transfer learning to improve classification accuracy and generalization, enhancing automated counterfeit currency detection[17].

1.3. Explainable Deep Learning:

Deep learning has achieved a tremendous level of accuracy on computer vision tasks, yet the advanced complexity of deep neural networks makes them "black boxes", clouding transparency and interpretability. Interpretable AI research also identifies this "black box" characteristic as the most important barrier to actualizing deployments of deep learning in high-stakes domains. As a remedy to this issue, Explainable AI (XAI) techniques have been developed to make model decisions and outcomes more comprehensible [18]. There are a multitude of XAI techniques, and commonly used methods include Gradient-weighted Class Activation Mapping (Grad-CAM) and heatmap visualizations, which can shed light on the inner workings of convolutional neural networks (CNNs) and demonstrate what areas of an image were most pertinent to predicting the final outcome [19].Grad-CAM operates on the premise of utilizing the gradients of class scores for the target class flowing into the last convolutional layers to create a coarse localization map that highlights where in the image is discriminative to the prediction of the model [20]. It allows researchers and

practitioners to observe where the model focuses its attention during classification, creating a kind of interface between high accuracy and the need for interpretability in their use of deep learning[21].

While Grad-CAM is a solid approach to conveying important information, as shown in Figure 6, heatmap visualizations can provide an easy-to-understand color-coded representation of those regions. Warmer colors (e.g., red and orange) indicate areas of high contribution by the model, while cooler colors (e.g., blue) denote areas of lower contribution [22]. In deep learning applications like counterfeit currency detection, heatmap visualizations allow us to grade whether the model is using appropriate security features (e.g., holograms, watermarks, or micro-texts) versus making predictions based on a background that might be incidental [23]. Integrating the predictive capabilities of deep learning methods through Grad-CAM, along with heatmap visualization of decision areas, brings researchers the best of both worlds. It provides the justification of the analytical ability of the assumptions relied upon while conveying the sort of transparency needed for validation and trustworthiness. This combination is not limited to supporting debugging and error analysis; it allows for obtaining evidence for claims, aiding the credibility of AI systems that are deployed in sensitive areas such as finance or security [24].

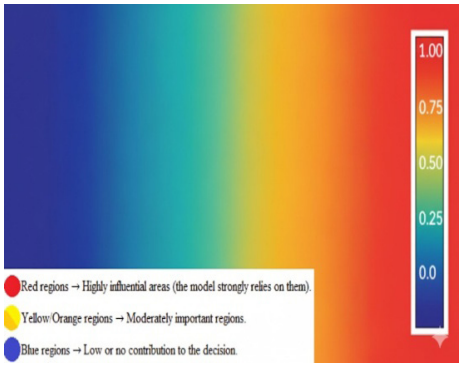

Figure (6): Attention heatmap

1.4. Security features of Libyan banknotes:

The official currency of Libya is the Libyan dinar (LYD). Like most modern currencies, the Central Bank of Libya has developed a range of security features in the banknotes to help avoid counterfeiting and maintain public trust and confidence in the currency system. The securities are the result of an ongoing process of technological innovation and the development of international standards for currency design and authentication. The security features are indicative of both technological and design aspects that serve to maintain the integrity of the national currency. The security design of the Libyan banknote incorporates a number of visible and hidden features that provide protection from counterfeiting and/or demonstrate authenticity. Visible anti-counterfeiting features include, but are not limited to, a dynamic color-shifting 3D holographic stripe, an engraved portrait, and a clear, translucent area, with colored gravure patterns also providing security and attractive visual features. Modern optical features such as optically variable ink (SPARK), fluorescent numbering, and monochromatic serial numbering offer significant layers of authentication in an optical method. Monochromatic serial numbering is identifiable with magnetic properties in order to enable unique identification for automated detection. Raised-intaglio printing can also enhance tactile-based identification and accessibility. An engraved gravure stripe also provides sufficiently micro-level textures that are extremely difficult to reproduce. In this research, an image processing approach and deep learning techniques are used to analyze these features and develop an intelligent system that is able to perform accurate discrimination of genuine Libyan banknotes compared to counterfeits and increase the reliability and automation of currency verification, as shown in Figure 7).

Figure (7): Basic features of Libyan security banknotes

2. METHODOLOGY

The methodology describes the study approach, data source, preprocessing steps, model design and training, and systematic evaluation procedures. It includes examples of the prototype user interface and system workflow. The systematic procedures ensure that every part of the project contributes to achieving a practical and accurate counterfeit detection system. The study includes statistical and visual performance measures, and the prototype user interface demonstrates how modules fit together in an organized flow. This study uses an applied experimental approach as the goal is to resolve a real-life issue (currency verification) with experimental training and evaluation of deep learning models for image classification, and using transfer learning to help reduce training complexity and resource consumption. EfficientNet-B4, the most current CNN model, was used as the core model due to its balance of accuracy versus computational efficiency.

2.1. System Architecture:

The proposed system employs a modular system where they are self-contained in a self-contained function to deliver the entire workflow. The proposed system in the figure below identifies five mains. The workflow highlights the various key stages planned in the overall design process: image preprocessing, building a CNN using EfficientNet-B4, training the model using the best hyperparameter setups, testing the model with statistical measurements of performance, and developing a prototype graphical user interface (UI) for end-users to interact with. The workflow demonstrates that the proposed system is reproducible, efficient, and scalable. These allow the proposed system to be adaptable for real-world deployment in individual and commercial use, as outlined in the following Figure (8). Research phases the proposed system, outlining five main axes.

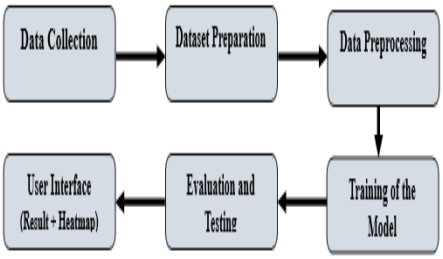

Figure (8): Diagram of the proposed system

2.2. Data Collection

The success of any deep learning system depends primarily on the quality and size of the dataset.

2.2.1. Data Sources:

The Libyan currency will be in denominations of 5, 10, and 20 dinars, and the images are collected from two types of sources:

-Real Currency: Well, provide brand new, clean samples of Libyan banknotes from an established source, preferably a commercial bank.

-Fake Currency: Obviously, obtaining real samples of fake currency is going to be exponentially more difficult, so it is really a case of attempting to simulate fake samples, emulated by digitally altering the images of the original currency to include the common characteristics of failures in the faking process.

2.2.2. Image Acquisition:

To ensure that the model operates under realistic circumstances, many devices and many shooting situations will be adopted to obtain images. Many modern smartphone cameras will be used to vary the lighting conditions (natural, artificial, or dim), shooting angles, shooting distance, and background type. Modern images of banknotes will include a transparent security zone, thus primarily highlighting the background features.

 ISSN: Online 2790-1637, Print 2790-1629
National Library of Libya, Legal number: 154/2018

Therefore, images are taken against either a white or black background, completely obscuring this area from the model so that it is distinct from the currency area. Thus, the model avoids this zone.

2.3. Data Preparation:

Data preparation processes, including data splitting and balancing, were used to ensure the reliability of the proposed model effects before using the datasets.

2.3.1. Data Splitting:

The proposed model will undergo rigorous data splitting to prevent overfitting and ensure reliable results. The dataset will be divided into three exclusive subsets, providing evaluation metrics from previously unexplored data, thereby providing an objective and reliable measure of results.

1.Training set: Approximately 70% of the data will come from the training set. Therefore, the model can use this data for parameter learning so that it can be trained.

2.Validation set: There will be approximately 20% of the data being used for the validation set, and the model will make use of this validation set to tune hyperparameters, observe convergence, and control for overfitting.

3.Test set: The remaining 10% will exclusively be used for final evaluation to provide an unbiased estimate of the performance of the model.

2.3.2. Data Balancing:

Class imbalance is a potential issue during the preparation of the dataset. Imbalance leads to bias with regard to the majority class, lowering sensitivity to the minority class. Balancing techniques include oversampling of the minority class, undersampling of the majority classes, or a hybrid of both, to achieve the most appropriate balance without sacrificing data diversity. Allora combination of these will assist in overcoming this limitation found in many real-world applications.

2.3.3. Dataset Description:

This study utilized two datasets for its research purpose: dataset 1 (Currency Verification) and dataset 2 (Authenticity Detection). The first dataset is used to determine if an image is a Libyan banknote, a filtering step before authenticity detection. If the input is not Libyan currency, such as a foreign currency banknote or non-currency image, it is filtered out of the classification pipeline. To make it clear, the division is shown in Table (1) as follows:

Table. (1): Distribution of the image verification dataset

Type of Image	Libyanbanknote	Not a Libyan currency
Total	1000	1000
Training = 70%	700	700
Validation=20%	200	200
Testing = 10%	100	100

Similarly, dataset 2 (Authenticity Detection) is a dataset of banknote images labeled as real or counterfeit, sourced from public and in-person sources. It was used for training and evaluating the model's performance to distinguish real banknotes from fake ones, enabling the model to distinguish between real and counterfeit banknotes. To make it clear, the division is shown in Tables (2) and (3) as follows:

Table. (2): Distribution of the real currency dataset

Type of Currency	20 LYD	10 LYD	5 LYD
Total	1500	1500	1500
Training= 70%	1050	1050	1050
Validation= 20%	300	300	300
Testing= 10%	150	150	150

Table. (3): Distribution of the fake currency dataset

Type of Currency	20 LYD	10 LYD	5 LYD
Total	1500	1500	1500
Training= 70%	1050	1050	1050
Validation= 20%	300	300	300
Testing= 10%	150	150	150

2.3.4. Data Preprocessing

Preprocessing is a significant part of guaranteeing that the input data we use for CNN is consistent, reduces noise, and remains representative. Before we input images into our model, they must have undergone some form of preprocessing to help standardize the images and improve their quality, as illustrated in Figure (9).

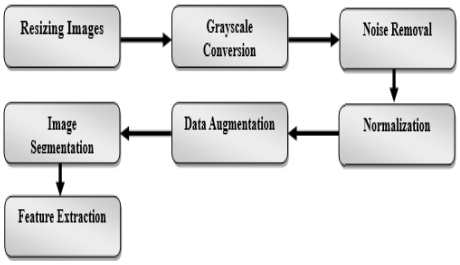

Figure (9): Diagram of data preprocessing operations.

1. Resizing Images: all images should be resized to 380 x 380 pixels to match the input size of EfficientNet-B4.

2. Grayscale Conversion: while the model can handle RGB input, converting to grayscale reduces complexity.

$I_{gray}(x,y)=0.299R+0.587G+0.114B$

3. Noise Removal: A Gaussian filter was used to demean the image:

$$G(x,y)=\frac{1}{2\pi\sigma^2}.e^{\frac{-(x^2+y^2)}{2\sigma^2}}$$

4. Normalization: The pixel values within all images will be scaled from the range [0-255] to the range [0-1]. This operation helps to speed up the model training process and provide a stable range of input. Pixel intensities were normalized to the range [0,1]

$$x'=\frac{x-min(x)}{max(x)\ -min(x)}$$

5. Data Augmentation: To synthetically enlarge the number of members and diversity in the dataset, random changes will be made to the images, which could include adding minor rotations, zooming in and out, and changing brightness. Random changes were used to enrich dataset variability: rotation (θ), zoom, brightness, and flips.

6.Image Segmentation: The study utilizes the Squeeze-and-Excitation (SE) Block for channel-wise feature recalibration in computer vision, enhancing robust segmentation and feature extraction in challenging situations. Figure (10) depicts the general scheme of the suggested segmentation.

(1). Holographic Stripe. (2). Protection. Portrait, Clear Window. (3). SPARK on Secondary Window. (4). Magnetic numbering. (5). Fluorescent numbering. (6). Tactile Emboss. (7). engraved Gravure stripe. (8). Relief writing. (9). The prominent engraved landmark. (10). The signature

Figure (10): Basic features of data Libyan security banknotes.

7. Feature Extraction Segmented regions are converted into numerical descriptors for machine learning models through a process known as feature extraction. Conventional techniques use features like texture or color histograms and modify them according to their dependability. Deep learning approaches, such as CNN models, with attention strategies like the Squeeze-and-Excitation (SE) Block, however, provide more reliable modifications, enabling networks to improve classification performance by increasing informative capabilities and decreasing uninformative ones. A summary of preprocessing methods and their benefits is shown in Table (4).

Table (4): Image preprocessing methods and benefits

Technique	Purpose	Effect
Resizing (380×380)	Uniform input for CNN	Standardization
Grayscale Conversion	Reduce computational cost	Simplicity
Gaussian Filtering	Reduce noise	Clarity
Normalization [0,1]	Improve convergence speed	Stability
Data Augmentation	Increase dataset size, reduce overfitting	Robustness
Image Segmentation	Highlight discriminative regions	Feature Enhancement

Table (4) outlines image preprocessing steps for CNNs, including resizing, grayscale conversion, Gaussian filtering, normalizing data to [0,1], and data augmentation and segmentation for robustness and discrimination among classes.

The pseudocode describing the preprocessing and augmentation pipeline is showed in Figure (11).

 ISSN: Online 2790-1637, Print 2790-1629
National Library of Libya, Legal number: 154/2018

```
preprocess_pipeline = Preprocessing)
   resize‹(380 ‹380) =
   grayscale = True‹
gaussian_filter = {kernel_size: ‹{1.0 :amgis ‹5
   normalization‹[1 ‹0] =
   augmentation} =
      rotation: ‹±7
zoom_range: ‹1.1
      brightness: {alpha: {10 :ateb ‹1.1
‹{
   segmentation} =
otsu_threshold: True‹
adaptive_threshold: {block_size: {2 :C ‹31
{
(
```

Figure (11): Pseudocode for data preprocessing and augmentation pipeline.

2.4. Model Development and Training:

This is the important part of the investigation where we will be building the "brain" of the system.

2.4.1. Model Selection:

At the heart of the system, we are using a convolutional neural network (CNN). In order to accelerate the development process of the system and take advantage of the availability of powerful models trained on millions of images, we will follow a transfer learning approach. The model we have proposed to use is EfficientNet-B4 because of its high efficiency coupled with a small footprint, which we favor for future use in a smartphone application. EfficientNet-B4 is an efficient trade-off. It also uses a compound scaling process that jointly scales depth (d), width (w), and resolution (r):

$$d = \alpha^{\varphi}, w = \beta^{\varphi}, r = \gamma^{\varphi}$$

where φ is the scaling coefficient, and constants were selected from a grid search in a constrained resource relative to α, β, and γ.

2.4.2. Modified architecture for binary classification:

A pre-trained EfficientNet-B4 (trained on ImageNet) was used as a feature extractor, and a dropout layer and a final sigmoid output were added. The architecture is shown in Figure (12), The top layers were replaced by custom dense layers.

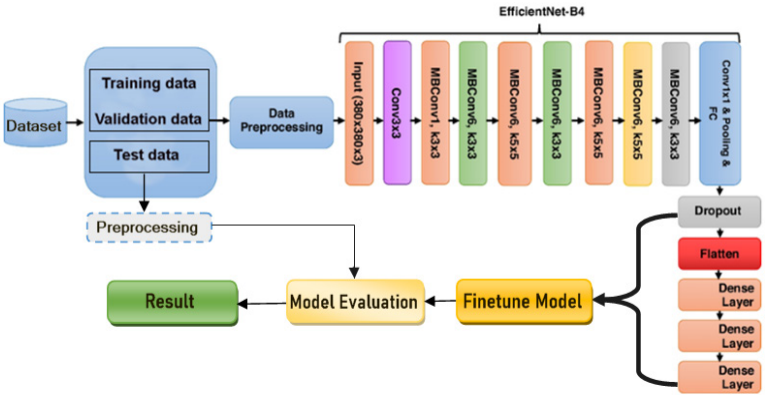

Figure (12): CNN model architecture (EfficientNet-B4 Modified for binary classification)

2.4.3. Training Process:

-Loss Function: The loss function that will be used is binary cross-entropy, which is the most commonly used loss function for binary classification problems. Binary cross-entropy was used:

$$L = -\left(\frac{1}{N}\right) \Sigma \left[y_i \log(\hat{y}_i) + (1 - y_i) \log(1 - \hat{y}_i) \right]$$

-Optimizer: The optimizer we will use is the Adam optimizer, because of the ability of the Adam optimizer to converge fast. Adam updates stage parameters with:

-First moment estimation : $mt = \beta^1 mt^{-1} + (1 - \beta^1) gt$

-Second moment estimation : $vt = \beta^2 vt^{-1} + (1 - \beta^2) gt^2$

-First trend bias correction: $\hat{m}_t = \frac{mt}{1 - \beta_1^t}$

-Second – direction bias correction:

$$\hat{v}t = \frac{vt}{1 - \beta^{2t}}$$

Base update: $\theta_{t+1} = \theta t - \frac{\alpha \hat{m} t}{\sqrt{\hat{v}t} + \varepsilon}$

AdamW improves generalization on vision models by decoupling weight decay from the gradient update.

-Performance Metrics: Accuracy will be primarily monitored during training.

-Hyperparameters: The table (5) indicates that the configurations for the training set were based on a Batch Size of 32, as this achieved a balance of stability and computational efficiencies, and 30 Epochs, which allowed ample learning to occur and to mitigate overfitting. The Adam optimizer was selected for quicker convergence, and to ensure stable updates, while Binary Cross-Entropy was selected as the loss function, given that the task is a binary classification task.

Table (5): Training hyperparameters

Parameter	Value
Batch Size	32
Epochs	30
Optimizer	Adam
Loss Function	Binary Cross-Entropy

2.5. Model Evaluation

To assess the model's efficacy, a suite of performance indicators based on the confusion matrix will be deployed after assessing the model on the test dataset.

1.Accuracy: The portion of correct classifications over total samples.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Where TP: True Positi.

FP: False Positive

TN: True Negative.

FN: False Negative.

2.Precision: Of all of the banknotes that the model classified as "Fake", what percentages were correct? (It was possible).

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

3.Recall/Sensitivity: Of all the real "fake" banknotes, what percentage did the model detect? (It was important that no counterfeit coins were missed).

$$Recall = \frac{TP}{TP + FN}$$

4.F1-Score: The harmonic mean between precision and recall, it is an overall indicator of a model's performance.

$$F1 = 2 . \frac{Precision\ Recall}{Precision + Recall}$$

5.Confusion Matrix:

Table (6) shows the confusion matrix parameters used to evaluate the performance of the proposed deep learning model, including true positive (TP), false positive (FP), true negative (TN), and false negative (FN). These metrics form the basis for calculating accuracy, precision,

recall, and F1 score.

Table (6): Confusion matrix parameters

		Actual	
		Real	Fake
Predicted	Real	TP	FP
	Fake	FN	TN

TP=∑(ytrue=1 ∧ ypred=1)

FP=∑(ytrue=0 ∧ ypred=1)

TN=∑(ytrue=0 ∧ ypred=0)

FN=∑(ytrue=1 ∧ ypred=0)

Where,

-True Positive (TP) is an image that is labeled with an Original Banknote that is predicted as a Real Banknote.

-False Positive (FP) is an image ed as "Fake Banknote" that is predicted as " Real Banknote."

-False Negative (FN) is an image labeled with a Real Banknote that is predicted as a Fake Banknote.

-True Negative (TN) is an image labeled with "Fake Banknote" that is predicted as a Fake banknote.

6. ROC and AUC

To evaluate the efficacy of the proposed CNN-based banknote authentication system further, Receiver Operating Characteristic (ROC) curves were employed. Receiver Operating Characteristic (ROC) Curve: A ROC curve is a graphical representation that shows the trade-off between True Positive Rate (TPR, also called Recall or Sensitivity) and False Positive Rate (FPR) at multiple

$$TPR = \frac{TP}{TP + FN} FPR = \frac{FP}{FP + TN}$$

In the ROC plot:

• X-axis (FPR): Proportion of real banknotes classified incorrectly as counterfeit.

• Y-axis (TPR): Proportion of counterfeit banknotes correctly classified as counterfeit

6.1.Area Under the Curve (AUC):

The AUC is a single scalar that summarizes the classifier's performance at all thresholds. The AUC is the area under the ROC curve. AUC values are in the range of [0, 1]:

AUC = ∫[0, 1] TPR(FPR) d(FPR)

AUC value interpretation:

• AUC = 1.0 → Perfect classifier (best case)

• 0.9 ≤ AUC < 1.0 → Excellent classification performance

• 0.8 ≤ AUC < 0.9 → Good classification performance

• 0.7 ≤ AUC < 0.8 → Acceptable classification performance

• 0.5 ≤ AUC < 0.7 → Poor classification performance (similar to random guessing)

• AUC = 0.5 → model has performance equivalent to random chance

• 0.5 ≤ AUC < 0.7 → Poor classification performance (similar to random guessing)

• AUC = 0.5 → The model has performance equivalent to random chance.

ROC curves allow a greater degree of scrutiny of the classifier beyond a simple number of overall accuracy measures. In the counterfeiting realm of banknote detection:

• A high TPR means fakes will not be missed.

• A low FPR means real banknotes will not be marked as fake.

Thus, the ROC-AUC analysis provides a reasonable balance between the model's ability to be sensitive to counterfeit notes and its integrity in marking real notes.

6.2.User Interface Design (Prototype)

A prototype user interface will be developed using the Tkinter library in Python in order to create a straightforward method of utilizing the proposed model. The user interface will be preliminary and scalable in the future. The user will be able to upload a photo from their studio or take one directly from their camera and pass it to the model to make a prediction on the currency denomination (genuine or counterfeit). The user interface will also include an additional button to show a heatmap, the focus areas, which show the decision-making focus areas, and would further improve interpretability. The prototype is not the final destination; it is the start of the process that allows one to develop a fully integrated user interface

for an eventual commercial or institutional effort. The prototype was created using Tkinter. The main system interface, as shown in Figure 13, is as follows:

Figure (13): Main operational interface of the Libyan currency detector

6.2.1.Functional Components

Table 7 shows the most important components of the system and their functions.

Table (7): Functional Components

Component	Function
Select Images	The user can upload an image of Libyan currency to be verified.
Predict	The system will then use the pre-trained deep learning model to predict if the currency is real or fake.
Heatmap	The user can visualize the saliency/heatmap that displays the most salient regions in the model's class label decision; this will allow the user to have explainable AI.
Clear	The current image and results from this previous prediction are removed, enabling the user to start over.
Camera	The user is able to capture an image for immediate verification.
Exit	The user can exit the application.
Previous/Next	Allows you to navigate through multiple uploaded images.
Result section	Shows the output of the prediction and initially prompts the user to select an image before producing any results.

2.7. Workflow Flowchart:

To better visualize the sequential operations of the system, a workflow flowchart was developed. It outlines the steps from image acquisition to classification. The pipeline includes image-preprocessing, augmentation, model training, and evaluation, as illustrated in Figure 14. The workflow integrates all modules:

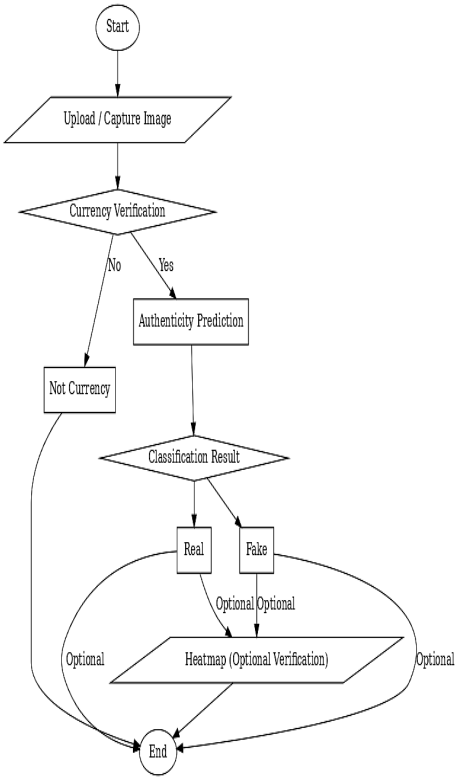

Figure (14): Flowchart of the complete system

2.8. Tools and Techniques Used

2.8.1. Hardware Specification:

Table 8 shows the hardware specifications used in implementing and evaluating the proposed system.

Table (8): Hardware Specification

Component	Specification
Processor	Intel i3 2GHz
RAM	4 GB
Storage	512 GB HDD

2.8.2. Software Specification:

Table 9 presents the software specifications employed in the development and testing of the proposed system.

 ISSN: Online 2790-1637, Print 2790-1629
National Library of Libya, Legal number: 154/2018

Table (9): Software Specification

Software	Specification
Operating System	Windows 10
Programming Language	Python 3.10
IDE (Integrated Development Environment)	VS Code
Libraries	TensorFlow, Keras, OpenCV, Scikit-learn, Numpy, Pandas, Seaborn
Model training environment	Google Colaboratory
Storing and managing data	Google Drive (cloud storage)

3.RESULTS AND EVALUATION

3.1. Model 1: Currency VS. Not Currency:

The first stage required classifying if a banknote image belonged to Libyan currency or not. The EfficientNet-B4 model was trained and evaluated on Dataset 1. The EfficientNet model has a compound scaling and optimized architecture, which aided in high levels of accuracy when detecting Libyan banknotes. The model's overall performance, evaluated based on performance measures, is synthesized below:

3.1.1. Training Performance:

Figure 15 (Training Performance) shows the change in accuracy and loss during the training process. It can be seen that the model performance improved significantly from the outset (after 0 epochs) with training accuracy increasing to 100% and training loss (1.1565e-04) and a validation accuracy of 98.76% after the 5th epoch. From that time onwards performance stabilization occurred, and performance was maintained at a high-performance level for both groups of subjects. In relation to the loss—

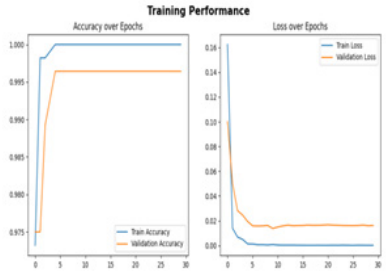

Figure (15): Training & validation accuracy and loss curves for Model 1

3.1.2. Confusion Matrix:

Figure 16 and Table 10 provide the confusion matrix, which indicates the model was able to correctly classify all samples at 100%. Therefore, the model correctly identified both currency and non-currency without any false positives or false negatives. The results show that the model was distinguished between the two categories effectively and has shown the ability to generalize well.

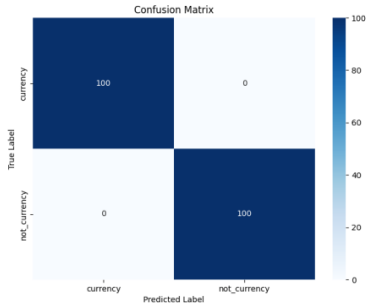

Figure (16): Confusion matrixfor Model 1

Table (10): Confusion Matrix Results for Model 1

		Actual	
		Real	Fake
Predicted	Currency	TP= 100	FP= 0
	Not Currency	FN= 0	TN= 100

3.1.3. Performanc Metrics:

The model highlighted in Table 11 demonstrated accuracy equal to 100% for each of the four performance statistics of accuracy, precision, recall, and F1 rate. The model with zero error was able to classify the samples into currency and non-currency classes with no class error and indicated high class discrimination ability. All total averages (Macro Avg + Weighted Avg) were also equal to 100% accuracy, which indicated the model achieved strict accuracy across the entire data set. These values were calculated from Table 10 stemming from the confusion matrix.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} = \frac{100 + 100}{100 + 100 + 0 + 0} = 1.0(100\%)$$

$$Precision = \frac{TP}{TP + FP} = \frac{100}{100 + 0} = 1.0(100\%)$$

 ISSN: Online 2790-1637, Print 2790-1629
National Library of Libya, Legal number: 154/2018

$$Recall = \frac{TP}{TP + FN} = \frac{100}{100 + 0} = 1.0(100\%)$$

$$F1 = 2.\frac{Precision.Recall}{Precision + Recall} = 2.\frac{1.0}{1.0 + 1.0} = 1.0(100\%)$$

Table (11): Performance metrics for Model 1

Class	Precision	Recall	F1-score	Support
Currency	1.00	1.00	1.00	100
Not Currency	1.00	1.00	1.00	100
Accuracy			1.00	200
Macro Avg	1.00	1.00	1.00	200
Weighted Avg	1.00	1.00	1.00	200

3.1.4. ROC Curve and AUC Analysis:

The ROC curve in Figure 17 extends the illustration of the model's performance in class discrimination appropriately, as the AUC (area under the curve) reached its maximum value of 1.0, signifying perfect classification performance with no classified error. The blue line has shown that the true positive rate (TPR) was continually high across all false positive rates, which suggests that the model's strength was in being able to optimally balance sensitivity and specificity. TPR and FPR calculated as:

$$TPR = \frac{TP}{TP + FN} = \frac{100}{100 + 0} = 1.0\ (100\%)$$

$$FPR = \frac{FP}{FP + TN} = \frac{0}{0 + 100} = 0$$

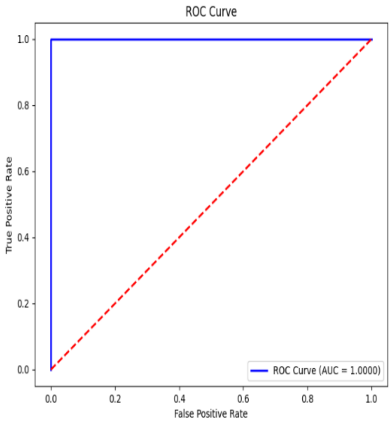

Figure (17): ROC Curve& AUC for Model 1

3.2. Model 2: Real VS. Fake Classification

3.2.1. Training Performance for Model 2:

Figure (18) presents the training and validation performance metrics from the proposed model as it was supplied with genuine and counterfeit currency. The left plot shows the accuracy plots over several training epochs, where it was clear that the training accuracy climbed steadily to nearly 90% while the validation accuracy settled downwards at 88%. This would imply that the model generalizes well and there was no blatant overfitting. The right plot presents the loss values for training and validation. Here, the training loss fell steadily below 0.25, and the validation loss settled down at approximately 0.30 after about the fifteenth epoch, which shows that the model was still learning. Overall, the take-home message was that the model can distinguish between genuine currency and counterfeit currency reliably after only a number of training epochs, and it has also demonstrated strong and consistent performance in doing so.

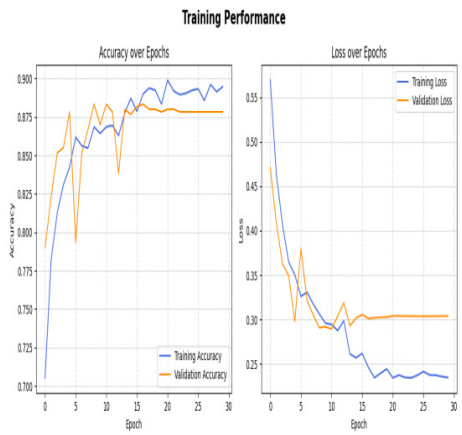

Figure (18): Training & validation accuracy and loss curves for Model 2

3.2.2. Confusion matrixfor model 2:

Figure (19) and Table (12) the confusion matrix incorporates the measures of performance for the proposed model tested on the test dataset, including 150 genuine samples and 150 counterfeit samples. The model had correctly classified 141 genuine notes; meanwhile, there were 142 counterfeit notes being correctly classified as the positive tie. This also corresponded with the model misclassifying only nine genuine notes as counterfeit, while misclassifying eight counterfeit notes as genuine notes. Overall, these results suggest that the model is quite robust in categorizing real from fake currency, as well as the high level of precision/recall for both classes. The lower count of misclassifications implies strong reliability and that this model can be practically applied to real-world applications that identify counterfeit currency.

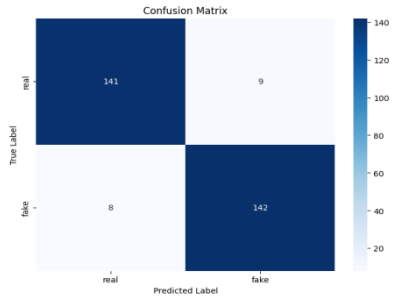

Figure (19): Confusion matrixfor Model 2

Table (12): Confusion Matrix Results for Model 2

		Actual	
		Real	Fake
Predicted	Real	TP= 141	FP= 9
	Fake	FN= 8	TN= 142

3.2.3. Performance metrics for model 2:

The confusion matrix describes the success of the proposed model on the test dataset of 300 samples (150 real and 150 fake). As indicated by the confusion matrix, the model successfully predicted 141 real notes and 142 fake notes with only (9 + 8 = 17) misclassifications, as shown in Table 13. Using the proposed model's results, the evaluation metrics were calculated as:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} = \frac{141 + 142}{141 + 142 + 9 + 8} = 0.943$$

$$Precision = \frac{TP}{TP + FP} = \frac{141}{141 + 8} = 0.9463$$

$$Recall = \frac{TP}{TP + FN} = \frac{141}{141 + 9} = 0.9400$$

$$F1 = 2.\frac{Precision.Recall}{Precision + Recall} = 2.\frac{0.8905}{1.8863} = 0.9431$$

The abovementioned results have demonstrated that the model had an overall accuracy of 94.33% with equal precision and recall in both classes; it presented the potential to accurately detect authentic versus counterfeit currency.

3.2.4. ROC Curve Analysis:

The ROC shows the relationship between TPR (True Positive Rate) and FPR (False Positive Rate) of the proposed model that the confusion matrix results yielded, with TPR calculated as:

Table (13): Performance metrics for Model 2

Class	Precision	Recall	F1-score	Support
Real	0.9463	0.9400	0.9431	150
Fake	0.9404	0.9467	0.9435	150
Accuracy			0.9433	300
Macro Avg	0.9434	0.9433	0.9433	300
Weighted Avg	0.9434	0.9433	0.9433	300

$$TPR = \frac{TP}{TP + FN} = \frac{141}{141 + 8} = 0.9493$$

Moreover, FPR calculated as:

$$FPR = \frac{FP}{FP + TN} = \frac{9}{9 + 142} = 0{,}0596$$

As seen on the ROC curve (Figure 20), the model continued to demonstrate an extremely strong separation of real versus fake classes, as evidenced by the AUC of 0.9493. This also provided reassurance of the capacity of the model to clearly delineate classes, as when the AUC values are close to 1.0, this means correspondingly few false positives occur, and there was quite a bit of classification capability in the model.

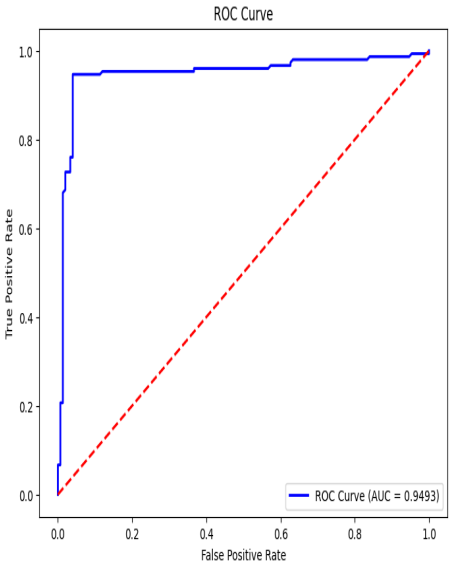

Figure (20): ROC Curve& AUC for Model 2

While the developed model resulted in a reasonable classification accuracy of approximately 94%, this amount did not reach a 100% perfect score based on various technical and transfer factors, which are discussed below. Initially, it could not reach maximum accuracy and performance curves due to several factors related to the data composition and the complex nature of the new Libyan banknote.

The training images were different in aspects of lighting, resolution, and capture angles and had polymer substrate-induced reflections, which made the fine details less clear and caused distortion. Also, the new banknote has security features that are highly complex, including a transparent window, a holographic stripe with a 3D component, and SPARK technology with variable reflectance. These attributes produce dynamic visual patterns that models simply cannot learn consistently. Also, an inconsistent ratio of genuine to counterfeit banknotes can skew the learning and subsequently impact the AUC value.

In contrast, some authors using controlled data with fixed angles and constant illumination reported accuracy as high as 100%, such as [25] on Colombian currency

using ResNet18. For studies with real and variable data, accuracy ranged from 85% to 94%, such as the results of [26] using Jordanian currency. The position of the result in this study is attributed to the fact that modern Libyan polymer banknotes contain transparent areas and three-dimensional elements, as noted by [27], which add complexity by acting as optical elements. Furthermore, under realistic data capture conditions, variation typically reduces generalization only slightly compared to controlled data, as noted by [28]. Overall, achieving around 94% accuracy is commendable and realistic and indicates the existing structural and optical complexity of modern polymer banknotes and the difficulty of producing a complete model of all their security features in a learning framework.

3.3.User Interface Evaluation:

The user interface of the proposed system was constructed with ease of use and ease of operation in mind. As shown in the Figures 21, we used an interface that allows the users to upload images, predict, and return the results without excessive barriers. For example, the system accurately reported that the uploaded image was not Libyan currency and presented a clear, simple error.

This feedback facilitates ease of use by helping the user operate effectively without misleading the user into bad interactions with the system. For Libyan banknotes, the system will tell you whether your inputs are genuine or counterfeit, along with the confidence attached to the prediction. For example, if the prediction results show 90%, the banknote is expected to be either genuine (or counterfeit, depending on the denomination). However, a confidence score of 70% does not simply mean belief that the banknote is "70% counterfeit"; it simply is a measure of the probability of the banknote belonging to the denomination that was predicted. This probabilistic feedback is important for transparency purposes and can help the user make their decisions with more confidence when operating the system.

Figure (21): Screenshot of prediction operations for a Libyan banknote

3.4 .Grad-CAM Heatmap Visualization:

Grad-CAM heat maps were produced for each sample. Visual features of the banknotes from Libya (logo, product's color, design, etc.) were also significant.

The conditions of interpretation are analysis and are through any distributions of suspicious areas. In Figure 22, warm colors (red and yellow) represent the areas enhanced for the end user, add value to the banknotes that had the most amount of influence on predicting the outcome, and cool colors (blue and purple) represent negative influence. This method of interpretation increases the transparency of the model since they can see what the most essential features of the banknotes were in relation to classification, ultimately adding greater reliability and confidence in the detection framework being proposed.

Figure (22): Screenshots of a Heatmap of a Libyan Banknote

4.CONCLUSION

In conclusion, this study achieved its aim by developing an effective, as well as understandable, deep learning model for counterfeit banknote detection. The study based its contributions on principles from the EfficientNet-B4, the Grad-CAM visualization approach, and a basic prototype user interface to offer practical and technical contributions. While the study has a few notable limitations regarding the dataset and real-world data, the research provides a strong base for future work to build from and extend the work spawned from the study. Thus, this research not only contributes to the academic conversation of deep learning and fraud detection but also provides a direction for practice in the financial and commercial world. In future work, several potential research directions will enhance and expand the scope of the work presented in this paper. Expanding the dataset will ensure the highest possible system accuracy for developers. Furthermore, improving the user experience/UI of both mobile and web applications will create a cross-platform experience.

REFERENCES

1.Barbosa J, Martins H S R, da Silva A J S, NoratoH M G, Duarte, A R. Counterfeit banknote identification based on outlier detection methods. International Journal of Scientific Management and Tourism, 2024;10(2), 45–59. ISSN: 2386-8570.

2.Antonius F, Ramu J, Sasikala P, Sekhar JC, Mary S C. Deep Cyber Detect: Hybrid AI for Counterfeit Currency Detection with GAN-CNN-RNN using African Buffalo Optimization. International Journal of Advanced Computer Science and Applications, 2023;14(7).

3.Alshorman O, Omar K, Ahmad T. Banknotes counterfeit detection using convolutional neural networks with attention mechanisms: A case study on Jordanian currency. Journal of Imaging, 2024 ;10(2).

4.Pham T D, Lee Y W, Park C, Park K R. Deep Learning-Based Detection of Fake Multinational Banknotes in a Cross-Dataset Environment Utilizing Smartphone Cameras for Assisting Visually Impaired Individuals. Mathematics, 2022;10(9), 1616.

5.Van der Horst F, Snell J, Theeuwes J. Finding counterfeited banknotes: the roles of vision and touch. Cognitive Research: Principles and Implications,2020; 5, Article 40.

6.Alzubaidi L, Zhang J, Humaidi A J.. Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. J Big Data, 2021; 8, 53.

7.LeCun Y, Bengio Y. Hinton G. Deep learning. Nature, 2015; 521, 436–444 .

8.Waseem R, Zenghui W. Deep Convolutional Neural Networks for Image Classification: A Comprehensive Review. Neural Comput 2017; 29 (9): 2352–2449.

9.Krizhevsky A, Sutskever I, Hinton G. ImageNet classification with deep convolutional neural networks. In Proc. Advances in Neural Information Processing Systems, 2012; 25 1090–1098.

10.Gupta R., Singh S. Revolutionizing convolutional neural networks for enhanced currency security and fraud prevention. BPAS Journals. 2024; Vol.44 No. 3. P. 24900-24908.

11.Rangel C. A. survey on convolutional neural networks and their performance limitations in image recognition tasks. Journal of Sensors, 2024; 2797320.

O'Shea K, Nash R. An Introduction to Convolutional Neural Networks.2015; ArXiv, abs/1511.08458.

12.Albawi S, Mohammed T A,Al-Zawi S. "Understanding of a convolutional neural network," 2017 International Conference on Engineering and Technology (ICET), Antalya, Turkey, 2017, pp. 1-6, doi: 10.1109/ICEngTechnol.2017.8308186.

13.Ali T, Jan S, Alkhodre A, Nauman M, Amin M, Siddiqui MS. DeepMoney: counterfeit money detection using generative adversarial networks. PeerJ Comput Sci. 2019;5:e216.

14.Wang J, Perez L,Hays J. The effectiveness of data augmentation in image classification using deep learning. Convolutional Neural Networks in Image Processing,2020; 10(4), 450–460.

15.Zhang B, Chen L, Liu X, Zhao L. Practices and challenges of using GitHub Copilot: An empirical study. arXiv preprint arXiv, 2023; 2303.08733.

16.Tan M, Le Q. EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks. In Proceedings of the 36th International Conference on Machine Learning 2019 ;(Vol. 97, pp. 6105–6114). PMLR.

17.Longo L, Lapuschkin S, Seifert C. (Eds.).. Explainable Artificial Intelligence: Second World Conference, xAI 2024, Valletta, Malta, July, Proceedings, Part IV (Communications in Computer and Information Science, 2024;Vol. 2156).

18.Cheng Z, Wu Y, Li Y, Cai L, Ihnaini B . A Comprehensive Review of Explainable Artificial Intelligence (XAI) in Computer Vision. Sensors, 2025; 25(13), 4166.

19.Zhang H, Ogasawara K. Grad-CAM-Based Explainable Artificial Intelligence Related to Medical Text Processing. Bioengineering (Basel). 2023; 10(9):1070. Published 2023 Sep 10.

20.Chattopadhay A, Sarkar A, Howlader P, BalasubramanianV N. Grad-CAM++: Generalized gradient-based visual explanations for deep convolutional networks. IEEE Winter Conference on Applications of Computer Vision (WACV), 2018;839–847.

21.Chefer H, Gur S, Wolf L. Transformer interpretability beyond attention visualization. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR),2021; 782–791.

22.Samek W.Wiegand T.Müller K. "Explainable Artificial Intelligence: Understanding, Visualizing and Interpreting Deep Learning Models." ArXiv abs/1708.08296 2017: n. pag.

23.Selvaraju R. Cogswell M A, Das R. Vedantam D. BatraD. "Grad-CAM: Visual Explanations from Deep Networks via Gradient-Based Localization,; IEEE International Conference on Computer Vision (ICCV), Venice, Italy, 2017; pp. 618-626, doi: 10.1109/ICCV.2017.74.

24.Pachón, C G, Ballesteros, D M, Renza, D.. Fake banknote recognition using deep learning. Applied Sciences, 2021; 11(3), 1281.

25.Nasayreh A, Jaradat A S, Gharaibeh H, Dawaghreh W, Al Mamlook R M, Al-Na'amneh Q, Daoud M, Migdady H, Abualigah L. Jordanian banknote data recognition: A CNN-based approach with attention mechanism. Journal of King Saud University – Computer and Information Sciences, 2024; 36(4), 102038.

26.Rafiei A, Karimi A, Bodaghi M. Polymer banknotes: A review of materials, design, and printing. Sustainability, 2023; 15(4), 3736.

27.Lee J W. A survey on banknote recognition methods by various sensors. Sensors, 2017;17(11), 2627.