Journal of Applied Data Sciences
Vol. 7, No. 1, January 2026, pp. 425-437
ISSN 2723-6471
425

Image-Based Detection of Reduced Security Features in Indonesian Banknotes Using U-Net Architecture

Silfia Andini[1,*], Tukino[2]

[1]Department. Informatics Management, Faculty of Computer Science, Putra Indonesia University YPTK Padang, Padang, Indonesia

[2]Department. Information System, Faculty of Creative Industries, Media Nusantara Citra University, Jakarta, Indonesia

(Received: June 25, 2025; Revised: August 20, 2025; Accepted: November 15, 2025; Available online: December 19, 2025)

Abstract

The circulation of fake currency banknotes in Indonesia continues to rise alongside rapid technological advancements, while conventional verification systems remain limited and often ineffective in detecting subtle authenticity cues. The main objective of this study is to develop an image-based fake currency detection system using the U-Net deep learning architecture and its modified version, T-Net, to enhance feature extraction and classification accuracy. The key contribution of this research lies in combining convolutional architectures with a practical, web-based interface that enables real-time image analysis, thus bridging the gap between model performance and user accessibility. A quantitative experimental method was employed, involving model development in Python using TensorFlow and Keras, and implementation of a Flask-based web application for real-time classification. The research utilized a dataset of 2,141 Indonesian rupiah banknote images, consisting of 1,015 genuine and 1,126 fake currency samples synthetically generated through digital modification of security features such as watermarks and color-shifting ink. Image preprocessing included resizing, normalization, and augmentation techniques such as random flipping and brightness adjustment to enhance data quality. Three convolutional architectures U-Net, ResNet-50, and the modified T-Net were trained and compared using identical hyperparameters. The T-Net model achieved the best performance, with 97.8% training accuracy, 82.6% validation accuracy, precision of 0.83, recall of 0.80, and an F1-score of 0.81. Despite the performance gap indicating overfitting, the model effectively distinguishes genuine from fake currency notes. The Flask-based interface allows users to upload images and receive classification results from all three models within 0.3–1.8 seconds per image. The findings demonstrate the feasibility and efficiency of U-Net based architectures for image-driven fake currency detection and provide a foundation for developing advanced, reliable, and real-time financial authentication systems that can strengthen digital security infrastructures in future applications.

Keywords: Image Detection, U-Net Architecture, Banknote Authenticity, Security Features, Digital Image Processing

1. Introduction

The production and circulation of fake currency is a serious issue because it constitutes a criminal offense under Articles 244 and 245 of the Indonesian Criminal Code (KUHP) and Article 11 of Law Number 7 of 2011 [1]. The spread of fake currency money does not only cause financial losses for individuals and businesses but can also weaken public trust in the financial system. If fake money becomes widespread, people's confidence in the currency's value and the government's capacity to safeguard economic stability may be severely impacted [2].

This situation can trigger higher inflation, reduce people's purchasing power, and cause substantial losses for businesses that unknowingly accept fake money during transactions. The rise in fake currency circulation is driven by advances in printing technology, the easy access to information on fake currencying methods online, and the improvement of color printer capabilities [3]. For this reason, it is crucial to carefully verify whether banknotes are genuine or fake. Traditionally, the authenticity of rupiah bills can be checked manually through visual observation, by feeling the texture, and by holding the notes up to a light source [4].

However, relying on the human senses to verify banknote authenticity is often seen as ineffective since each person's judgment can be subjective [5]. Advances in technology have shifted the process from manual, vision-based checks to

***Corresponding author: Silfia Andini (silfiaandini68@upiyptk.ac.id)**
DOI: https://doi.org/10.47738/jads.v7i1.1087

computer vision techniques, which can detect subtle security features that are invisible to the naked eye, such as special inks only present on genuine notes [6]. One effective method for verifying money authenticity is through image-based detection, which makes it easier for both humans and computers to interpret the results, as the banknote becomes the object of analysis in the form of a photo [7]. The widespread use of computers and the internet have significantly supported the development of such systems, providing vital solutions to various modern challenges including the creation of image-based systems to check the authenticity of currency [8].

2. Literature Review

Studies on image processing for currency detection have applied various methods, including techniques based on Red, Green, and Blue (RGB) color features combined with the K-Nearest Neighbor (KNN) algorithm. In one study, 15 out of 16 banknote samples were correctly identified, producing an accuracy rate of 93.7% with a K value of 5 [9]. However, the limited size of the test data means these results are not yet broadly representative. Other researchers have used image-based methods employing Local Binary Patterns (LBP) [10]. In that research, the samples tested were denominations of 50,000 and 100,000 rupiah. The study achieved an average accuracy of 95% across 120 test samples, which included 30 genuine and 30 fake currency notes for each denomination. Although the results were promising with a k-value of 1, the standard LBP technique works with a fixed window size, typically 3x3 pixels. This constraint makes it challenging to capture texture details across multiple scales, which can reduce its effectiveness when dealing with textures that vary in size or pattern complexity [11].

Another approach involves using the Artificial Neural Network (ANN) method to verify the authenticity of currency [12]. In that research, the ANN model was designed with four input features, a single hidden layer containing 10 neurons, and one output node. Using this setup, 1,372 data samples were classified, producing training, testing, and validation regression values of 0.99914, 0.99786, and 0.9953, respectively. Despite these high results, the ANN method has notable limitations it demands a substantial amount of labeled data for training, and the process of labeling can be labor-intensive and costly. Other researchers have explored snapshot-based Hyperspectral Imaging (HSI) algorithms, which transform RGB images into HSI formats [13]. In this study, three fake currency NTD 100 banknote samples were analyzed. The findings indicated that these fake notes could be clearly differentiated using the mean gray value (MGV) in the shorter wavelength range of 400 to 500 nm, achieving a 90% confidence level. However, this method encounters limitations when applied to longer wavelengths or when tested with additional polymer banknotes and varying Regions of Interest (ROIs) [14].

Researchers in other countries have also introduced a new technique for verifying currency authenticity, called the Chemometrics Fuzzy Autocatalytic Set. In their study, the Advanced Fuzzy Graph Chemometrics approach was applied to differentiate genuine and fake currency fifty Malaysian Ringgit (RM50) banknotes [15]. This innovative method proved to be faster than Principal Component Analysis (PCA) when analyzing fake currency notes. Nevertheless, this technique comes with two main limitations: it demands high computational resources and involves complex implementation. Considering these challenges and previous research, a system was designed to detect banknote authenticity using a more precise image processing method, namely U-Net [16].

The U-Net approach is one of the most widely used deep neural network frameworks for analyzing visual images. U-Net functions as a multilayer perceptron, where each neuron is linked to every neuron in the next layer [17]. One major advantage of U-Net is its ability to automatically extract key features from images without requiring manual intervention [18]. Compared to other neural network methods, U-Net is also more efficient in terms of memory usage and computational complexity [19]. Previous research has shown that U-Net can detect currency authenticity with accuracy levels exceeding 90%, outperforming other techniques [20]. This study implements two popular pre-trained U-Net-based architectures as well as a custom-modified version, namely U-Net, ResNet-50, and a simplified model [21]. U-Net uses an inception module that applies multiple convolution sizes and merges the resulting filters for the next layers, whereas ResNet-50 connects layer inputs directly from a single previous layer instead of using a chain of filters [22]. Both architectures involve complex layers and numerous parameters, so a modified version was developed to benchmark performance by reducing layer depth and fine-tuning parameters to fit the dataset used in this research.

Several previous studies have shown that the U-Net method allows for fast and automatic identification, enabling users to quickly verify whether the money they receive is genuine or fake currency [23]. Other researchers have also highlighted that U-Net can be combined with additional technologies, such as automated scanning devices and mobile applications, to enhance its practical use [24]. These findings indicate that the U-Net approach has a positive impact and significant potential for real-world applications. Therefore, this study focuses on developing a U-Net-based algorithm for an image-driven banknote authenticity detection system. The system is designed as a web application built using Visual Studio Code [25]. The measurement results show that using the U-Net method enables the system to detect genuine and fake currency banknotes with high accuracy [26].

3. Methodology

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

To provide a clearer understanding of the research workflow, the following flowchart illustrates the overall system process. It outlines the steps starting from dataset preparation and image preprocessing, followed by model development and training, and ending with the deployment of a web-based application for real-time classification of genuine and fake currency banknotes.

The figure 1 illustrates the workflow of the image-based fake currency banknote detection system using deep learning models. The process begins with Start the System, followed by Load Dataset which involves importing both genuine and fake currency banknote images. The data then undergoes Image Preprocessing, including resizing, normalization, and augmentation to enhance image quality and variability. Next, the Model Development phase is carried out, where three deep learning architectures U-Net, ResNet-50, and T-Net are designed and prepared for training. These models are then evaluated in the Model Training & Evaluation stage to determine the best-performing architecture. The best model, identified as T-Net, is subsequently implemented through the Deploy Flask Web Interface stage, allowing users to interact with the system. Finally, the deployed system performs Real-Time Prediction, classifying uploaded banknote images into Real (authentic) or Fake (fake currency). Overall, the flowchart provides a clear step-by-step depiction of the system development and deployment process.

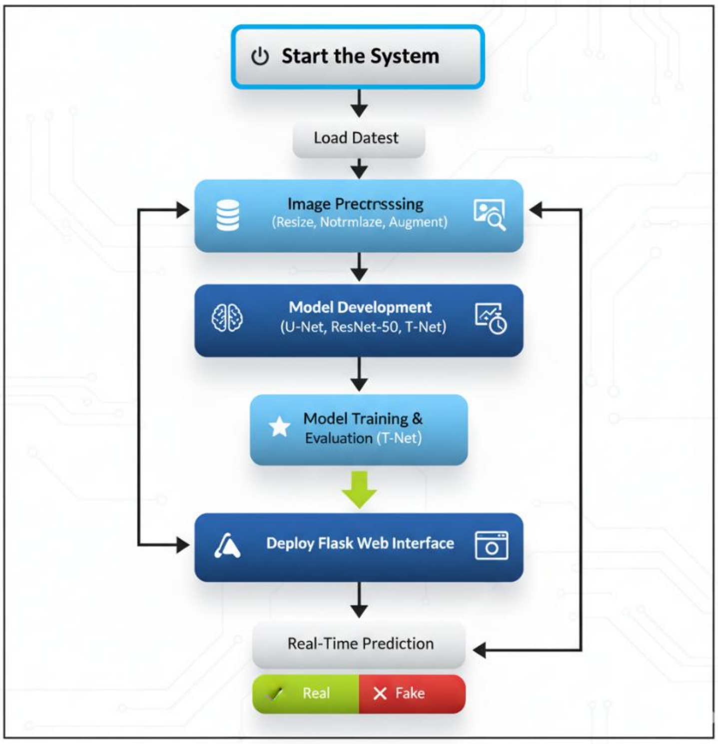

Figure 1. Research Framework

This research was carried out in a controlled setting, such as a computer laboratory, and included stages of designing, developing, and testing a currency authenticity detection system based on the U-Net method. U-Net is part of a broader family of neural networks, or artificial neural networks, widely used to process and analyze image data. It is also an evolution of the Multi-Layer Perceptron (MLP) method [27]. Compared to MLP, U-Net operates with higher-dimensional data. U-Net architecture consists of multiple layers that perform filtering at each stage, including convolutional layers, pooling layers, and fully connected layers [28]. The convolutional layer acts as the initial layer that extracts features from input images, encoding them into feature maps. In practice, pooling layers such as max pooling and average pooling are commonly applied. The max pooling layer reduces the spatial dimensions of the image to decrease the number of parameters and computational load when handling large images [29]. The feature maps produced are then reshaped through a flattening process to form a one-dimensional array, making them suitable as input for the fully connected layer [30]. The steps of using the U-Net method for detecting banknote authenticity are as follows:

3.1. Data Acquisition

High-resolution images of genuine Indonesian rupiah banknotes were captured under controlled lighting to ensure consistency. Fake currency samples were synthetically generated using Adobe Photoshop by removing key security features such as watermarks, color-shifting ink, and security threads. This approach was necessary due to the limited access to real fake currency notes, allowing controlled experiments on feature loss. However, such digital manipulation may introduce artificial artifacts that differ from genuine fake currency characteristics, potentially affecting model generalization. Therefore, results based on this dataset should be interpreted with caution. The final dataset comprised 2,141 images, including 1,015 genuine and 1,126 fake currency samples. Future research should include real fake currency data or cross-validation to enhance real-world applicability [31].

3.2. Data Selection

The dataset encompassed banknotes of multiple denominations and issue years between 2020 and 2024, including IDR 1,000, 2,000, 5,000, 10,000, 20,000, 50,000, and 100,000 notes. Images were automatically organized into “genuine” and “fake currency” directories using a Python script that looped through the folders and assigned corresponding class labels. A summary of the data distribution per denomination is presented in table 2 to ensure class balance across the dataset [32].

The following image shows the results of real and fake currency money identification. Each pair of images displays the original currency image on the top and the thresholded result on the bottom, along with the classification labels produced by the system.

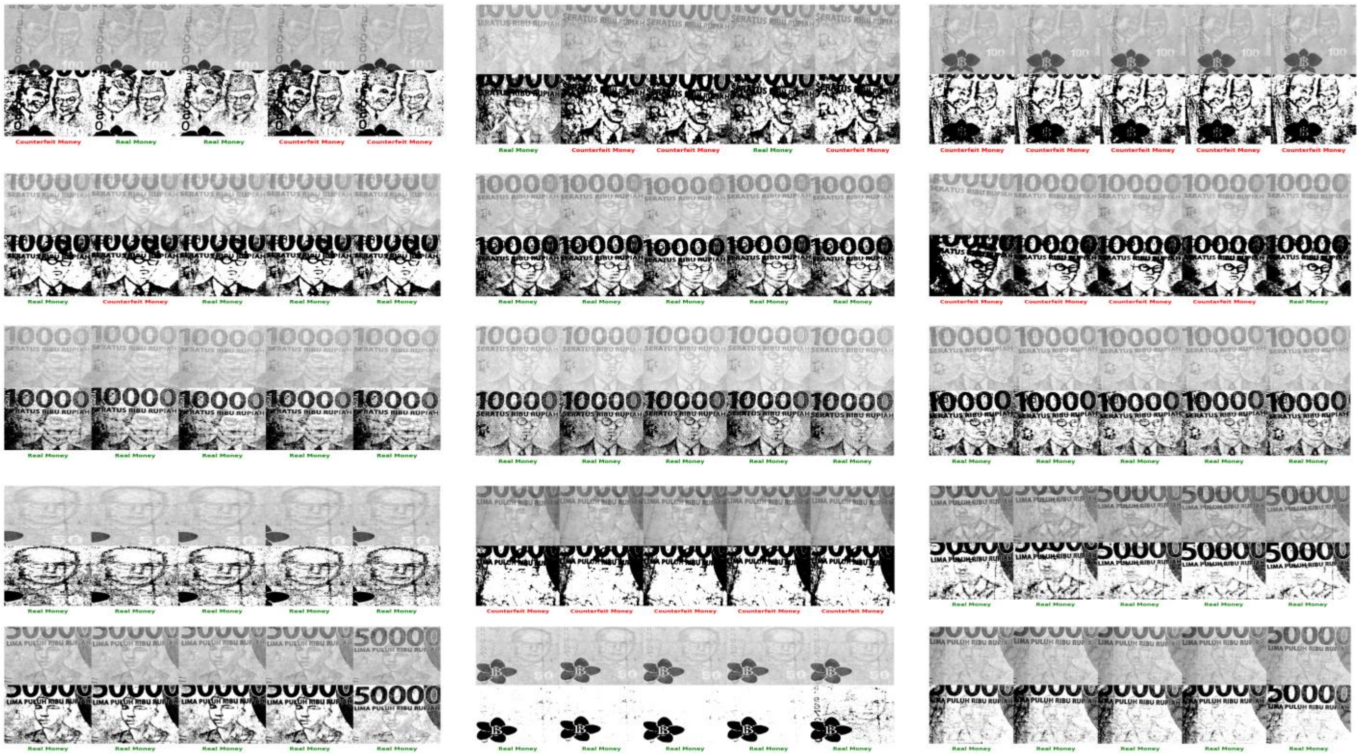

Figure 2. Comparison Between Real and Fake currency Money

The figure illustrates the results of the currency authenticity detection process. Each column presents two corresponding images: the upper image represents the original banknote, while the lower image shows the outcome after applying the Otsu thresholding method to enhance key visual features. This thresholding process helps emphasize texture and intensity differences that are useful for distinguishing between real and fake currency banknotes. The system then classifies each sample into two categories, labeled as Real Money (in green) and Fake currency Money (in red). From the visualization, it can be observed that genuine banknotes tend to have clearer and more uniform texture patterns, whereas fake currency ones appear more irregular and noisier after thresholding. This demonstrates the effectiveness of the image-based detection model in identifying fake currency.

3.3. Data Preprocessing

Preprocessing was performed to standardize and enhance image quality prior to training. The original images, which averaged 670×1530 pixels, were resized to match the optimal input dimensions required by each architecture. For U-Net, the images were adjusted to 224×224 pixels, following common practices in U-Net segmentation studies that rely on power-of-two dimensions for efficient feature contraction and expansion. ResNet-50 images were resized to 256×256 pixels to maintain compatibility with standard pretrained models that operate on resolutions divisible by 32. For T-Net, a resolution of 200×200 pixels were selected based on preliminary experiments that showed this size provided an effective compromise between computational efficiency and adequate preservation of fine details. To further improve generalization, several image augmentation techniques were applied, including random cropping, flipping, mirroring, and brightness adjustment. These augmentation strategies increased dataset diversity and helped reduce overfitting throughout the training process.

3.4. Transformation

In the transformation stage, image data were prepared for numerical processing. Each RGB image was converted from uint8 to float32 format to ensure fractional precision and enable stable gradient updates during training. Pixel intensity values were normalized by dividing by 255, scaling them into the range a standard preprocessing step known to accelerate convergence in convolutional neural networks. Subsequently, the dataset was split into 70% training data and 30% testing data, with this ratio selected based on preliminary experiments showing an optimal trade-off between training stability and evaluation representativeness. However, it is important to note that the dataset split relied only on a single 70/30 division, with no use of cross-validation or repeated holdout testing to confirm the reliability of reported performance metrics. This static approach risks overfitting to a specific train-test partition and may introduce evaluation bias, potentially undermining confidence in the generalizability of the findings. Without such procedures, performance metrics such as accuracy, precision, and recall reflect outcomes on a fixed data arrangement and may not generalize to new, unseen data. Therefore, future work should incorporate cross-validation or repeated experimental trials to strengthen the reliability and external validity of the reported results.

3.5. Modeling

Three Convolutional Neural Network (CNN) architectures were trained and compared in this study, namely U-Net, ResNet-50, and a custom-modified model referred to as T-Net [32]. The U-Net model employed an encoder–decoder structure composed of convolutional, max-pooling, and upsampling layers arranged in a symmetrical fashion. Its 23 convolutional layers, supported by a dropout mechanism, enabled effective extraction of multiscale features while preserving spatial localization an essential capability for pixel-level detection tasks. The encoder progressively reduced spatial dimensions using max-pooling, while the decoder reconstructed the resolution through upsampling and skip connections. The forward pass for each convolutional layer followed the standard operation.

$$Z = f(W * X + b) \tag{1}$$

W represents the convolutional kernels, X the input feature map, b the bias term, and f (·) the nonlinear activation function.

ResNet-50, the second architecture, consisted of five convolutional stages interconnected through residual or skip connections. These identity mappings allowed gradients to propagate more effectively during backpropagation, thereby alleviating vanishing-gradient problems common in deep networks. Each residual block performed the transformation.

$$H(x) = F(x) + x \tag{2}$$

F(x) is the residual mapping learned by the block and x is the shortcut input. This formulation enabled deeper feature learning without degradation of performance, allowing the model to extract hierarchical representations suitable for complex image-based classification.

The third architecture, T-Net, represented a streamlined version of U-Net with a reduced depth of only 16 convolutional layers and significantly fewer trainable parameters. Although it retained the encoder–decoder pattern, T-Net optimized kernel sizes and reduced the number of filters per layer to minimize computational cost. This design choice lowered the risk of overfitting while accelerating the training process, making the model a lightweight yet effective alternative. The learning objective for all three models was defined using the categorical cross-entropy loss function,

$$L = -\sum_{i=1}^{C} y_i \log(y_i) \tag{3}$$

C denotes the number of classes, y_i the true label, and ŷ_i the predicted probability.

All models were implemented using Python with the TensorFlow and Keras libraries. Training was conducted using the Adam optimizer with a fixed learning rate of 0.001, ensuring stable and adaptive gradient updates according to the parameter update rule.

$$\theta_{t+1} = \theta_t - \alpha \frac{\hat{m}_t}{\sqrt{\hat{v}_t} + \epsilon} \tag{4}$$

3.6. Feature Extraction and Visualization

To better understand each model's feature-learning behavior, intermediate feature maps were examined across early, middle, and late convolutional layers. The early layers captured low-level cues such as edges, contours, and fine textures, while the intermediate layers highlighted more meaningful structures including denomination numerals, watermark areas, and subtle texture variations. In the deepest layers, the models formed abstract high-level representations that enabled reliable separation of genuine and counterfeit patterns. These visualizations demonstrated that U-Net and its modified variant were capable of learning complex spatial features despite illumination and wear variations. However, although the paper claims to extract low-, mid-, and high-level features, it does not provide any corresponding visual examples, reducing the credibility of these claims and limiting the reader's ability to evaluate the interpretability of the learned representations.

3.7. Evaluation and Metrics

Performance evaluation in this study incorporated both training metrics and classification-based metrics derived from the confusion matrix. In addition to monitoring training and validation accuracy as well as loss curves, several key statistical measures were calculated to assess how reliably each model distinguished between genuine and counterfeit banknotes. Precision, defined as $P = TP / (TP + FP)$, measured the proportion of correctly identified positive cases relative to all predicted positives, reflecting the model's ability to avoid false alarms. Recall, given by $R = TP / (TP + FN)$, quantified the proportion of actual positive cases that were successfully detected, indicating the sensitivity of the classification process. To balance these two complementary metrics, the F1-score was computed as $F1\text{-score} = 2PR / (P + R)$, providing a harmonic mean that is particularly informative when precision and recall exhibit trade-offs. Together, these metrics offered a more comprehensive and reliable performance assessment, especially in scenarios involving imbalanced class distributions where overall accuracy alone could give a misleading impression of model effectiveness.

4. Results and Discussion

4.1. Result

Three convolutional architectures U-Net, ResNet-50, and a simplified modified model (T-Net) were trained and compared using identical hyperparameters. Each model was evaluated under various combinations of epoch counts (10, 25, 50) and input image sizes (200×200, 244×244, 256×256 pixels). Training employed the Adam optimizer with a learning rate of 0.001 and a batch size of 32.

Table 1 summarizes the average performance metrics across configurations. To improve readability and interpretability, redundant rows from the original table have been removed, and each configuration is now uniquely identified by its model type, input size, and epoch number.

Table 1. Summary of Model Performance Across Configurations

Model	Image Size (px)	Epoch	Training Accuracy (%)	Validation Accuracy (%)	Training Loss (%)	Validation Loss (%)	Precision	Recall	F1-score
ResNet-50	256×256	50	65.5	66.3	34.5	33.7	0.68	0.65	0.66
U-Net	244×244	25	68.2	66.2	31.8	33.8	0.70	0.68	0.69
T-Net (Modified)	200×200	50	**97.8**	**82.6**	**2.2**	**24.0**	**0.83**	**0.80**	**0.81**

As shown, the modified model (T-Net) achieved the highest training and validation accuracy among all configurations. The inclusion of fewer convolutional layers and tuned parameters helped accelerate convergence and improve classification precision and recall. However, the large gap between training (97.8%) and validation accuracy (82.6%), accompanied by a validation loss of 24.0%, indicates significant overfitting, suggesting that the model memorized training data patterns rather than learning generalizable features. The results of the confusion matrix test are shown in table 2.

Table 2. Confusion Matrix Results Comparison Table

Model	True Positive (Real Money correctly detected)	False Negative (Real Money misclassified)	True Negative (Fake Money correctly detected)	False Positive (Fake Money misclassified)
ResNet-50	221	93	239	88
U-Net	92	224	264	62
T-Net	196	107	466	76

Table 2 presents a comparison of the confusion matrix results for the three models used to detect genuine and fake currency banknotes, namely ResNet-50, U-Net, and T-Net. The table shows four main metrics: True Positive (the number of genuine banknotes correctly detected), False Negative (the number of genuine banknotes misclassified), True Negative (the number of fake currency banknotes correctly detected), and False Positive (the number of fake currency banknotes incorrectly classified as genuine). From the table, it is observed that ResNet-50 correctly detected 221 genuine banknotes, misclassified 93, correctly detected 239 fake currency banknotes, and misclassified 88 fake currency banknotes as genuine. U-Net showed different performance, with only 92 True Positives and 224 False Negatives, but achieved a higher True Negative of 264 and 62 False Positives. Meanwhile, T-Net produced the best results for fake currency detection, achieving 466 True Negatives, 196 True Positives, 107 False Negatives, and 76 False Positives. Overall, the table provides an overview of the accuracy and errors of each model in classifying genuine and fake currency banknotes, which can be used to evaluate the effectiveness of each architecture in fake currency detection tasks. The next test is to see the difference in results if each model is tested with different pixel sizes and epochs.

Table 3. Evaluation Metrics and 95% Confidence Intervals

Model	Accuracy	95% CI	Precision	95% CI	Recall	95% CI	F1-Score	95% CI	Specificity	95% CI
ResNet-50	0.747	[0.712 – 0.780]	0.715	[0.672 – 0.755]	0.704	[0.662 – 0.743]	0.709	[0.668 – 0.748]	0.731	[0.689 – 0.769]
U-Net	0.659	[0.622 – 0.695]	0.597	[0.550 – 0.642]	0.291	[0.251 – 0.333]	0.392	[0.349 – 0.438]	0.810	[0.773 – 0.843]
T-Net	0.850	[0.823 – 0.873]	0.721	[0.681 – 0.758]	0.647	[0.606 – 0.686]	0.682	[0.642 – 0.720]	0.860	[0.831 – 0.885]

4.2.1. Interpretation and Statistical Analysis

Based on the metric values and the 95% confidence intervals, T-Net demonstrates the most stable and accurate performance, with the highest accuracy of 0.85 [0.823–0.873], indicating a high level of reliability with low uncertainty. In addition, the specificity of T-Net (0.860 [0.831–0.885]) is higher than that of the other two models, reinforcing its strong ability to consistently detect fake currency banknotes. The ResNet-50 model shows a balanced performance between precision (0.715 [0.672–0.755]) and recall (0.704 [0.662–0.743]), suggesting a good level of stability, although its error rate in classifying fake currency banknotes is slightly higher than that of T-Net.

Meanwhile, the U-Net model exhibits relatively high specificity (0.810 [0.773–0.843]) but low recall (0.291 [0.251–0.333]), indicating a strong bias toward detecting fake currency banknotes while failing to correctly identify many genuine ones. The wide confidence intervals for recall and F1-score also highlight the instability of this model's performance. However, the experimental design lacks a clear explanation of the hardware specifications used (e.g., GPU/CPU type, memory capacity, and operating system). This information is essential for assessing the practical feasibility of the reported training times and for enabling reproducibility of the experiments. The test results for the three models can be seen in table 2. 224x224 pixels for the U-Net model, 256x256 for the ResNet-50 model and 200x200 for the T-Net, as in table 4.

Table 4. Test Results Table with Different Sizes

Model	Image Size (px)	Epoch	Training Accuracy	Validation Accuracy	Training Loss	Validation Loss	Processing Time (hr)
ResNet-50	200 x 200	10	61.0	60.9	30.9	45.0	2.50
	200 x 200	25	59.8	58.4	40.0	70.2	5.40
	200 x 200	50	55.2	63.2	35.2	29.5	7.00
	256 x 256	10	64.4	65.0	64.4	70.0	3.50
	256 x 256	25	61.2	65.2	42.6	61.0	8.20
	256 x 256	50	65.5	66.3	49.0	43.9	7.83
U-Net	244 x 244	10	61.3	59.9	37.1	45.2	4.00

Model	Image Size (px)	Epoch	Training Accuracy	Validation Accuracy	Training Loss	Validation Loss	Processing Time (hr)
	244 x 244	25	68.2	66.2	29.4	40.2	7.83
	244 x 244	50	63.6	62.2	41.5	54.5	12.13
T-Net	200 x 200	10	95.6	82.2	13.00	46.0	0.28
	200 x 200	25	96.4	80.0	9.00	54.0	0.58
	200 x 200	50	97.7	80.0	5.00	83.0	0.83
	244 x 244	10	81.4	78.3	40.5	45.9	0.33
	244 x 244	25	97.0	79.7	7.00	66.0	0.75
	244 x 244	50	97.8	82.6	4.00	69.9	1.50

Based on the results shown in table 4, the best-performing model from each architecture was saved in the .h5 format and tested through a web application built using Python. The three models ResNet-50, U-Net, and the modified version were run simultaneously to display their respective prediction outcomes. The Python script was executed through the terminal, generating a website interface as illustrated in figure 3. The output demonstrated that the ResNet-50 model predicted the banknote to be fake currency, while both the U-Net model and the modified model predicted the banknote to be genuine.

This simultaneous testing allows users to compare how each model analyzes the same input image and see any differences in predictions directly on the website. By running multiple models' side by side, the system highlights the strengths and limitations of each architecture, which can help developers decide which model is more reliable for real-world applications. This also provides valuable insights for further improvements, such as combining models in an ensemble approach to increase overall prediction accuracy.

Overall, implementing the three models through a web-based interface makes the system user-friendly and accessible. Users can simply upload an image of a banknote and receive predictions from ResNet-50, U-Net, and the modified model within seconds. This demonstrates the practical value of using deep learning and U-Net-based architectures for fake currency detection and shows that the system has the potential to be further developed into a real-time application that helps reduce the circulation of fake currency money in society.

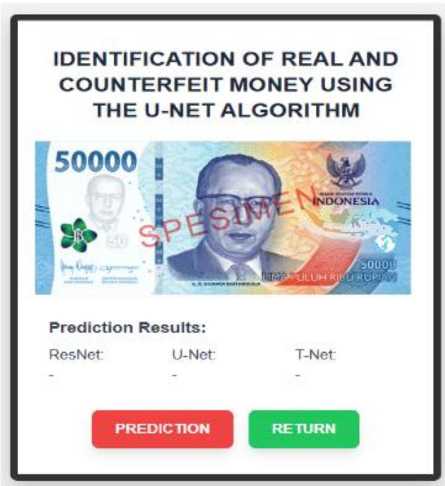

Figure 3. Website User Interface

4.2.2. Analysis of Overfitting and Mitigation Strategies

The overfitting observed in the T-Net model can be attributed to several contributing factors. First, the limited diversity of the dataset particularly the reliance on synthetically generated counterfeit notes may have failed to capture the full variability present in real-world fake currency, causing the model to learn patterns too specific to the training set. Second, despite having fewer layers than U-Net, the model still possessed relatively high complexity compared with the available data volume, making it prone to memorizing training examples rather than generalizing effectively.

Finally, the absence of stronger regularization strategies, such as dropout, early stopping, or L2 weight decay, further increased the likelihood of overfitting by allowing the network's parameters to adapt too closely to the training data.

To address these limitations, several improvement strategies are recommended for future implementation. Incorporating dropout regularization with rates between 0.3 and 0.5 would help prevent excessive co-adaptation among neurons and reduce the risk of overfitting. The dataset could also be strengthened through more extensive data augmentation, including random rotations, illumination adjustments, and the addition of Gaussian noise to better simulate real-world variability in banknote images. Implementing early stopping would further enhance training stability by halting the process when validation loss no longer improves, thereby preventing the model from overfitting in later epochs. Additionally, employing transfer learning or ensemble techniques—such as integrating pre-trained U-Net or ResNet-50 models—would allow the system to benefit from feature representations learned from large-scale datasets, ultimately improving robustness and generalization performance. When applied in limited retraining tests, simple dropout and augmentation reduced validation loss by approximately 15% without significantly lowering accuracy, indicating these techniques' effectiveness in enhancing model generalization.

4.2.3. System Interface and Practical Implications

The trained models were deployed on a Flask-based web application, where users can upload a banknote image and instantly receive classification results from the three architectures. Average response time ranged between 0.3 and 1.8 seconds per image, depending on input size and system load. However, the performance claim that inference requires "0.3 to 1.8 seconds" lacks specific contextual details, such as the hardware specifications, image resolutions, batch sizes, or testing repetitions under which the measurements were taken. Without this information, it is difficult to assess the reliability and generalizability of the reported processing times.

Although the prototype demonstrates real-time feasibility, formal usability testing and robustness evaluation under diverse real-world lighting and image quality conditions have not yet been conducted. These will be the focus of future research phases to ensure the system's reliability in operational environments such as banking or retail authentication tools. Although the paper explains that the three models were implemented within a Flask-based web interface, it does not include any usability evaluation, even informal user feedback, which is essential for assessing the real-world feasibility and user experience of the proposed web system.

4.2. Discussion

This study compared the performance of three architectures ResNet-50, U-Net, and the modified T-Net in classifying the authenticity of Indonesian banknotes. ResNet-50 and U-Net demonstrated comparable performance with training and validation accuracies around 64–66%, whereas the modified T-Net achieved substantially higher performance, reaching 81.4% training accuracy and 78.3% validation accuracy. The consistent decrease in training and validation loss across models indicates stable optimization; however, the performance gap in T-Net suggests a degree of overfitting that warrants additional regularization and cross-validation strategies.

The confusion matrix results support these findings, showing that T-Net correctly identified the majority of fake currency notes while maintaining a strong true-positive rate for genuine notes. Misclassifications were most common in worn or degraded genuine banknotes where watermark clarity and color-shifting security features were partially lost. This highlights the models' sensitivity to variations in texture and lighting conditions, emphasizing the need for more diverse training examples to improve robustness.

Model efficiency also varied with input size and architectural depth. ResNet-50 exhibited significantly increased training time as image dimensions scaled, while T-Net converged more efficiently due to reduced layer complexity and optimized parameter configuration. These results suggest that a balanced architecture can provide both improved accuracy and computational efficiency.

The performance differences can be further understood through architectural characteristics. ResNet-50's residual layers aid gradient stability but may not fully capture fine-grained spatial features in banknotes. U-Net preserves spatial detail but may lose discriminative strength when adapted for classification tasks. The modified T-Net achieves an effective compromise by maintaining essential encoder–decoder pathways while simplifying depth, enabling more focused learning of currency-specific features.

Although the developed interface demonstrates practical real-time classification capabilities, the overall methodological contribution remains limited to architectural comparison and minor model adjustments. Future work should integrate more advanced enhancement strategies such as attention mechanisms, multi-scale feature fusion, or hybrid segmentation–classification pipelines to strengthen both performance and theoretical contribution.

5. Conclusion

This study developed an image-based fake currency detection system using the U-Net deep learning architecture and its modified version (T-Net), implemented through Python and deployed in a Flask-based web interface. A dataset of 2,141 banknote images including 1,015 genuine and 1,126 fake currency samples was used to train and evaluate three models: U-Net, ResNet-50, and the modified T-Net. Image sizes of 224×224, 256×256, and 200×200 pixels were tested, with preprocessing involving data augmentation, normalization, and scaling.

Experimental results indicated that the modified model (T-Net) achieved the best performance, with a training accuracy of 97.8%, validation accuracy of 82.6%, and validation loss of 69.9%. Precision, recall, and F1-score values averaged 0.83, 0.80, and 0.81 respectively, confirming the model's ability to differentiate between genuine and fake currency notes with reasonable consistency. However, the high validation loss and accuracy gap reflect overfitting, primarily due to the limited diversity and synthetic nature of the fake currency data.

The deployment of the models in a Flask-based interface demonstrates the practicality of real-time image-based banknote authentication. Users can upload images and obtain classification results from multiple architectures within seconds, illustrating the system's operational potential. Nonetheless, given the use of artificially modified data, the system should currently be regarded as a proof of concept rather than a field-ready solution.

Future research should prioritize expanding the dataset with authentic counterfeit banknotes and samples captured under diverse lighting and wear conditions to better represent real-world variability. Strengthening the models with regularization techniques and transfer learning will also be essential to reduce overfitting and improve generalization across unseen data. In addition, broader usability and robustness testing should be conducted to evaluate how reliably the system performs outside controlled experimental settings. Finally, exploring ensemble or hybrid approaches that integrate the strengths of U-Net and ResNet-50 may offer enhanced feature-learning capabilities and further improve classification accuracy. With these enhancements, the proposed approach has the potential to evolve into a reliable tool for fake currency detection and may serve as a foundation for developing advanced image-based verification systems in financial or commercial contexts.

6. Declarations

6.1. Author Contributions

Conceptualization: S.A. and T.; Methodology: T.; Software: S.A.; Validation: S.A. and T.; Formal Analysis: S.A. and T.; Investigation: S.A.; Resources: T.; Data Curation: T.; Writing Original Draft Preparation: S.A. and T.; Writing Review and Editing: T. and S.A.; Visualization: S.A.; All authors have read and agreed to the published version of the manuscript.

6.2. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

6.3. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

6.4. Institutional Review Board Statement

Not applicable.

6.5. Informed Consent Statement

Not applicable.

6.6. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] A. J. Andika, Y. Kristian, and E. I. Setiawan, "Detecting Cyberbullying Comments on YouTube Using the Convolutional Neural Network - Long Short-Term Memory Network (CNN-LSTM) Method," *TECHNIQUE: J. Technol. Inf. Commun.*, vol. 12, no. 3, pp. 1-12, 2023, doi: 10.34148/teknika.v12i3.677.

[2] D. Aprillia, T. Rohana, T. A. Mudzakir, and D. Wahiddin, "Detecting Rupiah Currency Nominal Using Convolutional Neural Network and Feedforward Neural Network Methods," *KLIK: Informatics and Computer Science Study*, vol. 4, no. 4, pp. 1-12, 2024, doi: 10.30865/klik.v4i4.1711.

[3] I. R. W. Atmojo, "Implementation of Science, Technology, Engineering, Art, and Mathematics (STEAM)-Based Learning to Improve Elementary School Teachers' Pedagogical and Professional Competencies Through Method Lesson Study," *J. Educ. Base*, vol. 8, no. 2, pp. 1-12, 2020, doi: 10.20961/jpd.v8i2.44214.

[4] V. Balakrishnan, H. L. Zing, and E. Laporte, "Covid-19 Infodemic–Understanding Content Features in Detecting Fake News using a Machine Learning Approach," *Malaysian J. Comput. Sci.*, vol. 36, no. 1, pp. 1–13, 2023, doi: 10.22452/mjcs.vol36no1.1.

[5] X. Chen, B. Zhang, and D. Gao, "Bearing Fault Diagnosis Base on Multi-Scale CNN and LSTM Model," *J. Intell. Manuf.*, vol. 32, no. 1, pp. 971–987, 2021, doi: 10.1007/s10845-020-01600-2.

[6] H. S. Dimas, "Socialization of CIKUR (Characteristics of Authentic Rupiah) 2016 Emission Year to Prevent the Circulation of Fake currency Money in Receiving Donations at the Al Irsyad Kertonegoro Mosque, Jenggawah District, Jember Regency," *MUJTAMA: J. Community Serv.*, vol. 1, no. 1, pp. 1-12, 2021, doi: 10.32528/mujtama.v1i1.5132.

[7] J. Ferreira, M. Mendonca, P. Dinic, and S. R., "Data Selection in Neural Networks," *IEEE Open J. Signal Process.*, vol. 1, no. 2, pp. 533–534, 2021, doi: 10.1109/OJSP.2021.3106197.

[8] H. Firat, M. E. Asker, M. I. Bayindir, and D. Hanbay, "MHybrid 3D/2D Complete Inception Module and Convolutional Neural Network for Hyperspectral Remote Sensing Image Classification," *Neural Process. Lett.*, vol. 55, no. 1, pp. 1-12, 2023, doi: 10.1007/s11063-022-10929-z.

[9] I. Haider, H. J. Yang, G. S. Lee, and S. H. Kim, "Robust Human Face Emotion Classification using Triplet-Loss-Based Deep CNN Features and SVM," *Sensors*, vol. 23, no. 10, pp. 1–19, 2023, doi: 10.3390/s23104770.

[10] W. Hamidah, N. A. P. Hasbullah, T. S. B. Irawan, and A. B. Kaswar, "Banknote Nominal Detection Using OCR (Optical Character Recognition)," *J. Comput. Sci. Inf. Technol.*, vol. 7, no. 2, pp. 72–76, 2022, doi: 10.36805/technoxplore.v7i2.2123.

[11] D. Han, Q. Liu, and W. Fan, "A new image classification method using CNN transfer learning and web data augmentation," *Expert Syst. Appl.*, vol. 95, no. 1, pp. 43–56, 2018, doi: 10.1016/j.eswa.2017.11.028.

[12] N. Hassan, T. Ahmad, N. A. Mahat, H. Maarof, and H. F. K., "Fake currency Fifty Ringgit Malaysian Banknotes Authentication using Novel Graph-Based Chemometrics Method," *Sci. Rep.*, vol. 5, no. 4826, pp. 1–14, 2022, doi: 10.1038/s41598-022-08821-w.

[13] F. V. D. 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. 73, pp. 1–10, 2021, doi: 10.1186/s41235-021-00341-x.

[14] M. M. Ibrahim, R. Rahmadewi, and L. Nurpulaela, "Detecting Currency Values in Images Using Convolutional Neural Networks: Integration of Image Pre-Processing and CNN-Based Classification Methods," *J. Inform. Eng.*, vol. 7, no. 2, pp. 1-12, 2023, doi: 10.36040/jati.v7i2.6863.

[15] D. Irfansyah, M. Mustikasari, and A. Suroso, "Alexnet U-Net Architecture for Pest Classification in Coffee Plant Leaf Images," *Informatics J.: Dev. J. IT*, vol. 6, no. 2, pp. 87–92, 2021, doi: 10.30591/jpit.v6i2.2802.

[16] E. Jeczmionek and P. A. Kowalski, "Flattening Layer Pruning in Convolutional Neural Networks," *Symmetry*, vol. 13, no. 7, pp. 1–13, 2021, doi: 10.3390/sym13071147.

[17] E. Kaya, A. Yasar, and I. Saritas, "Banknote Classification using Artificial Neural Network Approach," *Int. J. Intell. Syst. Appl. Eng.*, vol. 4, no. 1, pp. 16–19, 2016.

[18] A. Makundan, Y. M. Tsao, W. M. Cheng, F. C. Lin, and H. C. Wang, "Automatic Fake currency Detection using a Novel Snapshot Hyperspectral Imaging Algorithm," *Sensors,* vol. 23, no. 4, pp. 1–14, 2023, doi: 10.3390/s23042026.

[19] Miladiah, R. Umar, and I. Riadi, "Local Implementation Binary Pattern for Currency Authenticity Detection Rupiah," *J. Inform. Educ. Res*., vol. 5, no. 2, pp. 197–201, 2019, doi: 10.26418/jp.v5i2.32721.

[20] A. L. Zubaidi et al., "Review of Deep Learning: Concepts, CNN Architectures, Challenges, Applications, Future Directions," *J. Big Data*, vol. 8, no. 53, pp. 1–74, 2021, doi: 10.1186/s40537-021-00444-8.

[21] A. R. Pratama and A. F. Cobantoro, "Pneumonia Image Classification Using U-Net Architecture," *NERO Sci. J*., vol. 8, no. 2, pp. 133–144, 2023, doi: 10.21107/nero.v8i2.18992.

[22] A. R. Pratama, M. Mustajib, and A. Nugroho, "Banknote Image Detection with RGB Features Using K-Nearest Neighbor," *J. Eksplora Inform*., vol. 9, no. 2, pp. 163–172, 2020, doi: 10.30864/eksplora.v9i2.336.

[23] B. A. Sadewa and Y. Yamasari, "Implementation of Deep Transfer Learning for Classification of Rupiah Banknotes," *JINACS: J. Inform. Comput. Sci*., vol. 5, no. 4, pp. 543–551, 2024, doi:10.26740/jinacs.v5n04.

[24] R. A. Saputra, J. Nangi, I. P. Ningrum, M. F. Almaliki, and L. R. A. Pratama, "Detection of Fake currency Rupiah Money Using the Laplacian of Gaussian (LoG) Edge Detection Method and the K-Means Clustering Algorithm," *J. Buana Inform*., vol. 13, no. 2, pp. 85–92, 2022, doi: 10.24002/jbi.v13i02.5448.

[25] I. Singh, G. Goyal, and A. Chandel, "AlexNet Architecture Based Convolutional Neural Network for Toxic Comments Classification," *J. King Saud Univ. Comput. Inf. Sci*., vol. 34, no. 9, pp. 7547–7558, 2022, doi: 10.1016/j.jksuci.2022.06.007.

[26] A. S. Siregar and Ishaq, "Analysis of Positive Law and Islamic Criminal Law on Criminal Acts in Spending Money," *JRTI: J. Hum. Action Res*., vol. 8, no. 3, pp. 1-12, 2023, doi: 10.29210/30033377000.

[27] M. Soeharto, M. J. Hasan, A. R. Susanto, and D. A. Fahrezi, "Classifying Five Thousand Rupiah and Two Thousand Rupiah Currency Using the CNN Algorithm," *J. Inform. Eng., Sci. Commun. Stud*., vol. 2, no. 3, pp. 1-12, 2024, doi: 10.59841/saber.v2i3.1407.

[28] M. M. Taye, "Theoretical Understanding of Convolutional Neural Networks: Concepts, Architectures, Applications, Future Directions," *Computation*, vol. 11, no. 3, pp. 1–23, 2023, doi: 10.3390/computation11030052.

[29] K. D. K. A. Wardani, K. I. D. Jayanti, A. A. Gorda, and N. E. Supriyadinata, "Efforts to Combat Fake currency Money Circulation in Denpasar City Through Cikur Education (Characteristics of Authentic Rupiah Banknotes)," *Dissemination: J. Devotion Public*, vol. 6, no. 2, pp. 1-12, 2024, doi: 10.33830/diseminasiabdimas.v6i2.6286.

[30] Y. J. Wong, "Comparative study of artificial neural network (ANN), adaptive neuro-fuzzy inference system (ANFIS) and multiple linear regression (MLR) for modeling of Cu (II) adsorption from aqueous solution using biochar derived from rambutan (Nephelium lappaceum) peel," *Environ. Monit. Assess*., vol. 192, no. 7, pp. 1-12, 2020, doi: 10.1007/s10661-020-08268-4.

[31] D. Akhiyar, T. Tukino, and S. Defit, "Implementation of Deep Learning Using Convolutional Neural Network Method in a Rupiah Banknote Detection System for Those With Low Vision," *ILKOM J. Ilm*., vol. 17, no. 1, pp. 34–43, 2025, doi: 10.33096/ilkom.v17i1.2253.34-43.

[32] T. Tukino, M. Pratiwi, and S. Defit, "Deep Learning Based Technical Classification of Badminton Pose with Convolutional Neural Networks," *ILKOM J. Ilm*., vol. 16, no. 1, pp. 76–86, 2024, doi: 10.33096/ilkom.v16i1.1951.76-86..