CNN-Canny-Based Signature Scrutiny Verification Techniques in Banking Applications

Noor Fadel [1,*], Bayadir A. Al-Himyari [1], Hiba Al-Khafaji [2], and Safaa S. Mohammed [2]

[1] Cyber Security, College of Information Technology, University of Babylon, Hilla, Iraq
[2] Software, College of Information Technology, University of Babylon, Hilla, Iraq
Email: noor.fadel@uobabylon.edu.iq (N.F.); sci.bayadir.abbas@uobabylon.edu.iq (B.A.A.-H.); hibamj.alkhafaji@uobabylon.edu.iq (H.A.-K.); safaa.almarshidy@uobabylon.edu.iq (S.S.M.)
*Corresponding author

***Abstract*—Ensuring the security of financial transactions and protecting official signatures on financial documents have always been a priority for individuals and international banks. Bank checks play a crucial role in global financial exchanges, with a vast number processed daily. However, signature forgery poses significant risks, leading to identity theft, financial losses, and reputational damage for both financial institutions and customers. Fraudulent transactions impact a bank's financial stability and erode consumer trust. Therefore, there is an urgent need for innovative solutions to enhance security and prevent signature-related fraud. This study proposes an automated signature verification system for bank checks, leveraging advancements in image processing and deep learning. Our approach begins with the acquisition of a customer's handwritten signature from check leaves. The main new idea in our method is using the Canny edge detection filter in the layers of the convolutional network instead of the usual Convolutional Neural Network (CNN) filters. This hybrid approach enhances feature extraction by focusing on critical signature contours, improving classification accuracy. Experimental results show that our CNN-Canny hybrid model reaches 98.8% accuracy, which is better than the 95.1% accuracy of traditional CNN methods. These findings highlight the potential of edge-aware deep learning techniques in strengthening security measures.**

***Keywords*—Canny filter, Convolutional Neural Network (CNN), banking transactions, fake signature, signature detection, deep learning, CNN-Canny**

I. Introduction

In the contemporary day, where technology links us in unprecedented ways, safeguarding the security and reliability of financial transactions is essential. Banks and financial institutions are essential for protecting our money and assets; nonetheless, they always encounter threats from individuals attempting to exploit weaknesses for personal benefit. A significant issue is signature forgery, a fraudulent technique that can result in illegal access to funds and illicit acts [1].

Manuscript received April 18, 2025; revised May 16, 2025; accepted June 19, 2025; published November 25, 2025.

Signatures have historically functioned as a principal method of authentication in banking transactions. They offer a distinctive identity for individuals, validating their consent and authority for diverse financial transactions, including withdrawals, payments, and transfers. Nevertheless, conventional signature verification systems, typically dependent on manual examination by banking specialists, are prone to human error and tampering. As technology advances, the methods employed by fraudsters also progress, requiring increasingly stringent and dependable systems for signature verification [2].

Image processing has always been very important because it enters into many health applications such as detecting diseases, educational or social applications such as Non-destructive testing [3]. Signature verification is considered a non-destructive test and others, so dealing with the concept of image processing is very important, especially in detecting forgery or other sensitive matters [4].

Canny filter detection is a vital image processing technique that gives good results in edge detection and is widely used [5].

In the modern banking environment, digital advances have shifted from being optional to essential for financial firms. This transition is propelled by the necessity to maintain competitiveness in a fluctuating market and satisfy changing client expectations [6]. Artificial Intelligence (AI) serves as a crucial catalyst for digital revolutions in banking, driving disruptive innovations across various channels, services, and strategies [7].

The application of AI in banking encompasses several areas, including front-office improvements like voice assistants and biometrics, as well as middle and back-office operations such as anti-fraud risk assessment and credit underwriting utilizing smart contract frameworks. Projected cost savings from AI implementation in banks are estimated to attain $447 billion by the year 2023, with over 80% of US banks acknowledging its advantages. Nonetheless, the incorporation of AI in banking introduces complex obstacles in addition to potential. Historically, AI concentrated on automating credit processes; however, its capabilities have broadened to

optimize internal operations and improve managing client relationships [8].

Detecting forged signatures is a vital task in document security and identity verification. Convolutional Neural Networks (CNNs) offer a powerful ability to extract complex visual patterns in handwritten signatures. When combined with a Canny filter, feature quality is enhanced by highlighting the subtle edges and boundaries that distinguish authentic signatures from forgeries. This architecture enables the model to focus on the distinctive details in the signature's linear structure, increasing classification efficiency. This strategy effectively contributes to improving detection accuracy and reducing the error rate in biometric systems.

In the following sections, we will present the competitive works in the second part of the research and also examine more thoroughly the methodologies used in this research, exploring the techniques used for signature analysis, implementation details, and image processing using CNN and Canny detection in the third section. Additionally, we will discuss the findings of our research methodology and the impact of employing edge detection technology with the Canny filter, with the aim of contributing to ongoing efforts to enhance the resilience of banking systems and protect customers' interest's world.

II. Literature Review

By leveraging AI techniques. The paper introduces it seeks to enhance the efficiency and accuracy of signature scrutiny. This paper uses image processing and machine learning to automate bank cheque signature verification. First, collect customers' handwritten signatures from cheque leaves. Methodology includes grayscale binarization, using Optical Character Recognition (OCR) and Line sweep signature detection, and SNN classification [9].

Image capture, pre-processing, extraction, and recognition in the autonomous bank cheque processing system are covered. It describes the automatic data extraction system's steps. It examines automated bank cheque processing concerns at several stages. The paper introduces advanced automatic bank cheque image processing methods. Examples of bank cheque image fields and subcategories, benchmark datasets, and the best algorithms are shown. Also covered are automatic cheque processing products. This assessment examines remaining field issues. Hidden Markov Model-Multi-Layer Perceptron (HMM-MLP) showed 95.5% date recognition accuracy and multilayer feed-forward neural network 97.31% payee name identification accuracy. In the courteous and legal amount system, DNN has 98.5%-digit recognition, MLP 93.2%, and Modified Quadratic Discriminant Function (MQDF) 97.04%. Support Vector Machine (SVM) classifiers and deep learning-based CNNs had 99.13% and 99.14% accuracy for signature and handwritten numeric character recognition, respectively [10].

The signature verification can be done online or offline, based on Geometric measures using a TensorFlow Python libraries [11].

This study compares machine learning algorithms for handwritten signature verification using 2011 International Conference on Document Analysis and Recognition (ICDAR). Signature and Center of Excellence for Document Analysis and Recognition (CEDAR) datasets is a well-known research institution in this field and offers popular signature databases. The inquiry includes preprocessing, CNN architecture feature extraction, and optimization. After rigorous evaluation, the best models are classified using supervised Machine Learning (ML) algorithms including linear SVM, random forest, logistic regression, and polynomial SVM. Results show that the Adam-optimized VGG16 design meets performance metrics. This study shows that ML methods can improve signature verification efficiency and accuracy, providing a robust document authentication solution [12].

Handwritten Signature Classification [13]: In the classification process, employed a variety of feature extraction models coupled with supervised learning algorithms. These models were meticulously selected to ensure optimal performance in discerning patterns within the data. His arsenal included Logistic Regression, Random Forest, Linear SVM, Radial Basis Function (RBF) SVM, Sigmoid SVM, and Poly SVM.

III. Materials and Methods

This research aims to develop a system for processing images of bank customer signatures using an accurate hybrid of the Canny filter and convolutional network techniques. Canny filters are typically used in the image pre-processing phase, but in the proposed method, they are used as the main filter in the convolutional network layers used. The goal is to integrate the Canny filter as a layer within the neural network. The Canny filter can be included as a dedicated layer within the CNN architecture, acting as a feature extraction layer.

The main goal of the proposed method is to:

- Accurately extract edges: The Canny filter helps identify the fine lines and details of the signature, facilitating structural comparison between authentic and forged signatures.
- Noise reduction: Removes unimportant details such as shadows or ink variations, focusing the neural network on the shape of the signature itself.
- Learning enhancement: Instead of processing the raw image, a more accurate representation of the signature can be fed to the CNN, enhancing performance.

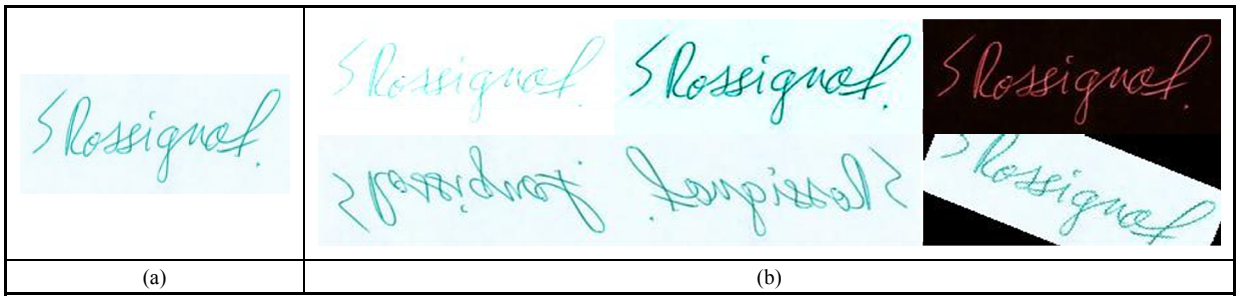
The dataset used in the proposed method consists of handwritten signature datasets for verification, containing 1000 patterns of authentic and forged signatures from 30 individuals. Each individual has five authentic signatures they created themselves and five forged signatures created by someone else, available on the Kaggle website https://www.kaggle.com/datasets/divyanshrai/handwritten-signatures.

A. Pre-processing

To build an efficient and highly accurate model, it is necessary to feed the network with a mix of diverse signatures. Because the real-life signature process is already somewhat variable for the same person, it was necessary to use an augmentation process to increase its size and diversity. Data augmentation techniques were applied to create several images with specific properties, such as:

- Rotation with a range of 20.
- Transformation with a width and height offset of 0.2.
- Random cropping with a range of 20.
- Adding a horizontal reflection blur with a range of 0.2.

Fig. 1 shows the augmentation process to increase its size and diversity for signature images.



(a) (b)

Fig. 1. Image augmentation process. (a) Original input signature; (b) Augmented signatures.

B. Model Creating CNN-Canny

We first applied the convolutional neural network algorithm to a set of signature images. It went through three stages: pre-processing, training, and finally testing. Subsequently, a CNN model is defined that includes 3 convolutional layers utilizing Canny and difference filters (32, 64, 128), 3 pooling layers using max pooling, and 2 dense layers: the first layer has 128 output classes with the ReLU activation function, while the second layer has one output class with the "sigmoid" activation function; dropout (0.2) is also included for regularization. Finally, the model is set up using the Adam optimizer, a binary cross-entropy loss function for binary classification, and accuracy to measure performance, preparing it for training over a set number of epochs (for 2). After the model for CNN-Canny was built, the training steps began. Fig. 2 illustrates all processes.

After training, we must test the model to measure its accuracy. We use different signature images and apply the read function to extract the feature, feed it to the CNN-Canny model, and print the classification result if it's real or forged.

It is worth mentioning that the proposed method worked on creating a hybrid vector from the values resulting from applying the CNN with a Canny filter in the same three layers, so the proposed method gave greater reliability and accuracy. Algorithm 1 shows the algorithm followed in this research.

The input image shows a simple signature consisting of horizontal, vertical, and diagonal lines. The first layer of each filter focuses on different features (edges, corners, etc.). Notice that some filters interact with horizontal parts and some with vertical parts. After pooling, image resolution decreases, but the main features remain. Image size decreases from 62×62 to 31×31 for each filter. Second layer: Detects more complex features. A combination of features from the first layer. Besides the 98.8 accuracy achieved by the proposed method, other evaluation metrics were also promising. Precision is 97.5%, recall is 95.2%, and finally, the F1-Score is 96.3%.

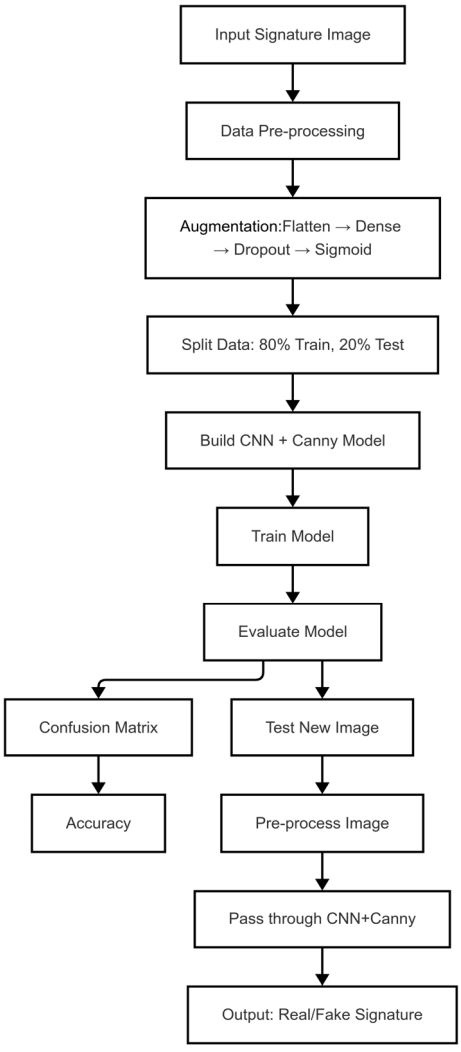


Fig. 2. Detecting real-fake signatures.

Algorithm 1: Algorithm for detecting fake signatures

Input: Image for signatures
Output: Binary classification result (Real or fake)

1. Data Preprocessing
   - Collect and structure signature image paths along with their corresponding class labels.
   - Convert the images to standardized NumPy array formats and resize them to a uniform resolution to ensure consistency across the dataset.
   - Encode categorical labels using a LabelEncoder.
2. Data Augmentation (Training Phase Only)
   - Employ the ImageDataGenerator API to perform real-time data augmentation, thereby increasing dataset diversity and enhancing generalization.
   - Apply augmentation techniques such as: Random rotations, Brightness variation, Random cropping, Horizontal scaling and flipping.

2. Model Architecture Design

Construct a deep learning architecture based on Convolutional Neural Networks (CNNs), enhanced with Canny edge filtering to emphasize signature contours and boundary features.

The model structure includes:

- Multiple Conv2D layers with BatchNormalization and MaxPooling2D to extract hierarchical visual features.
- Integration of a Canny-based filtered input, either as a separate channel or a fused feature map, to strengthen edge-aware representation.
- Fully connected (Dense) layers following a Flatten operation, including Dropout regularization to mitigate overfitting.
- A final output layer employing a sigmoid activation function for binary classification.

3. Model Evaluation and Inference
   - Quantitatively evaluate the model's performance using metrics such as accuracy, precision, recall, and F1-Score.
   - Employ a confusion matrix to analyze the classification errors and gain insights into model robustness.
   - Real-Time Signature Testing.

IV. Result and Discussion

It functions as a component of a hybrid architecture. A combination of learnable and fixed filters can be used, where some filters are set to be fixed (e.g., a Canny filter) and the rest are learnt during training. This approach takes advantage of both worlds: traditional knowledge and the adaptive capacity of the network.

A. First Convolutional Layer-Raw Features such as Edges and Corners

- Small filters (5×5) are applied to the image to extract features such as corners, straight lines, and initial details in the signature.
- Appearance: Multiple feature maps highlighting certain parts of the signature based on the filter used.
- Size: (H, W, num_filters), such as (64, 64, 32), we use 31 filters + filter Canny.

Output: A filtered image showing various features such as fine edges and more prominent areas of the signature. We need to make concatenate [conv1, canny1]. Fig. 3 shows the result of the first convolutional layer.

B. ReLU Activation Layer Features without Negative Values

The ReLU function is applied to the feature maps to remove negative values, helping to make the network more stable. Hear the shape same as the previous feature maps, but without negative values. Output is the same as the feature maps, but with negative values removed, enhancing the contrast of the lines.

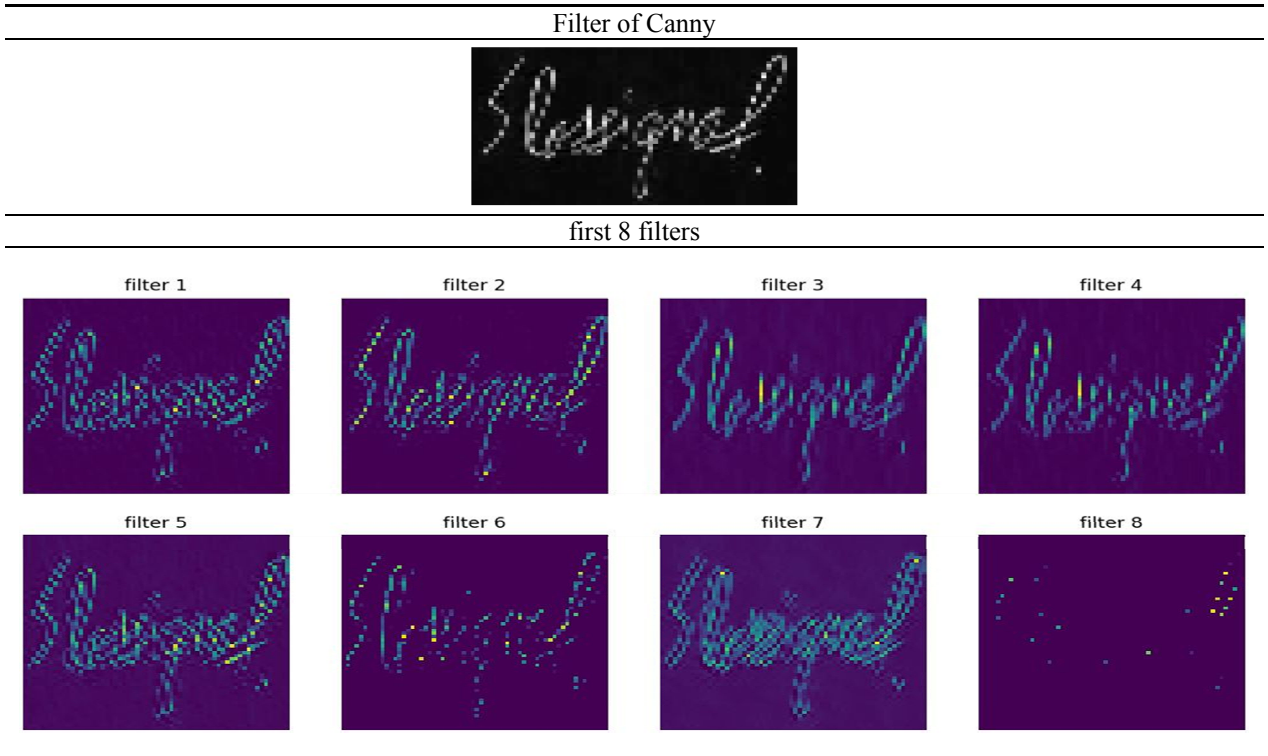


Fig .3. First convolutional layer-raw features.

C. Pooling Layer—A Smaller Version that Retains the Strongest Features

The dimensions of the feature maps are reduced using pooling. Max Pooling, which helps extract the most important features and reduce the data size. Here the shape is a smaller image containing only the essential features. Output is a smaller image that retains only the strongest lines and most distinctive areas of the signature. Fig. 4 shows the result of the pooling layer.

D. Second Convolutional Layer—Advanced

Patterns such as curves. Another set of filters is applied, but this time to extract more complex features, such as curvatures and fine details in the signature. Hear the shape has new feature maps focused on more complex patterns. Output images showing advanced details of the signature, such as the line pattern and curvatures. Also make concatenate [conv2, canny2].

E. Fully Connected Layer

The extracted features are converted into a vector and sent to the classification layers for decision-making. Here the shape is a numerical vector representing the signature characteristics, which can be used to identify or classify the signature. Output: A set of numbers representing the user's signature based on the extracted features. Final vector shape for the signature in Figs. 3 and 4 is: (1, 14, 14, 16).

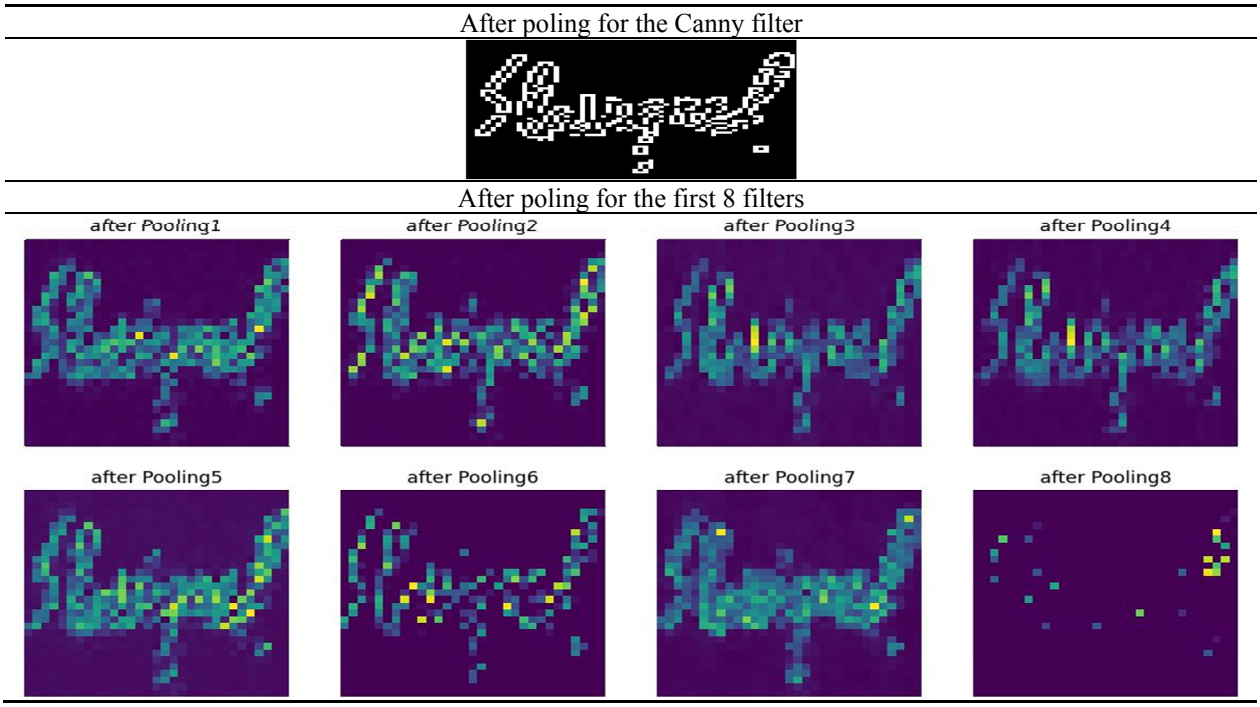


Fig. 4. The result of the pooling layer.

F. Output Layer

The final decision is made, whether to classify the signature (e.g., real or fake) or compare it with other signatures. CNN-Canny hybrid model achieves 98.8% accuracy, outperforming traditional CNN-based methods, which achieved 95.1% accuracy. These findings highlight the potential of edge-aware deep learning techniques in strengthening security measures.

In our proposed approach, the Canny edge detection filter plays a vital role in highlighting signature contours by detecting regions of high-intensity gradients. The performance of the Canny filter heavily relies on the appropriate selection of the low and high thresholds. These thresholds define the sensitivity of the filter to gradient changes and, consequently, to edge preservation or suppression.

Typically, a high/low ratio between 2:1 and 3:1 is recommended in edge detection applications. Based on experimental tuning for our dataset, we found that a low threshold of 50 and a high threshold of 150 (3:1 ratio) yielded the most consistent results in isolating signature strokes from the background.

A lower ratio (<2:1) increases sensitivity, which may lead to false positives, particularly with noisy or low-quality scans. A higher ratio (>3:1) improves precision but risks missing finer stroke edges, which are essential in signature verification. Thus, an adaptive threshold tuning mechanism or fixed thresholds calibrated to the dataset characteristics ensures optimal performance.

The Canny filter was selected over alternative edge detectors (such as Sobel, Prewitt, or Laplacian) due to several key advantages such as:

Noise Suppression, Canny uses Gaussian smoothing, reducing sensitivity to high-frequency noise that is common in scanned or photographed signatures. Edge Localization, it provides superior localization of edges due to the use of non-maximum suppression and dual thresholding. These qualities make Canny especially suitable for preserving critical shape features of

signatures that are essential for forgery detection.

Combining Canny with deep feature enhancement layers in the CNN compensates for Canny's failure cases by learning edge representations.

Regarding the time taken for the proposed method, the total time was 1 m 7 s. The time per step was approximately 45 ms to 55 ms per step.

Divided each epoch into 9 data batches, resulting in a total of 9 steps per cycle. Therefore, the approximate time per epoch was between 0.4 s and 0.5 s.

- Accuracy: The model maintained a stable accuracy of 0.9884 (98.8%) across all recent cycles.
- Loss: Approximately 0.2061 to 0.2078—a low and stable value.
- val_loss: Approximately 0.0064 to 0.0145.
- Loss and val_loss are small, indicating no overfitting.
- Training yields excellent performance (low loss and high accuracy). Testing yields excellent performance time, taking 23 ms for each signature.

Other evaluation criteria were also satisfactory. Precision is 97.5%, recall is 95.2%, and the F1-Score is 96.3%.

Most of the above research used deep learning methods for their high classification efficiency, but our method relied on hybrid filters combining both Canny and convolutional network filters in each layer. Table I illustrates a comparison between the proposed approach and previously employed techniques by researchers, along with the accuracy of their results.

TABLE I. COMPARISON OF THE PROPOSED METHOD WITH RELATED WORKS

Ref.	Technique Used	Accuracy
[9]	OCR and Linesweep, classification using CNN	90
[11]	CNN	90–94
[12]	VGG-16	99
	CNN	94.37
Proposed system	Hybrid CNN-Canny	98.8

V. CONCLUSION

This study introduced an advanced signature verification system specifically designed for banking transactions, leveraging a Convolutional Neural Network (CNN) enhanced through a hybrid layer integration approach. A central innovation in our methodology was the incorporation of the Canny edge detection filter within the convolutional architecture. This integration significantly improved the model's ability to extract fine-grained, contour-based signature features, thereby enhancing its capability to distinguish between genuine and forged signatures.

Extensive experimentation demonstrated the model's high accuracy and robustness, surpassing conventional CNN-based methods by capitalizing on the edge-preserving characteristics of the Canny filter. This enhancement enabled the network to focus more effectively on critical structural features while suppressing irrelevant noise, thereby improving classification performance. Furthermore, the application of data augmentation and regularization techniques mitigated overfitting and improved the model's generalizability across varied signature styles.

One of the primary challenges addressed in this work was the integration of the non-learnable Canny filter into the trainable CNN framework. To overcome this, a dual-channel approach was employed, wherein one channel processed raw input through the Canny filter and the other through standard convolutional layers. The feature maps generated by both channels were subsequently fused to form a unified representation, combining the strengths of both traditional and adaptive filtering.

The proposed model achieved a classification accuracy of 98.8%, with a precision of 97.5%, recall of 95.2%, and an F1-Score of 96.3%. These results indicate that the CNN-Canny hybrid approach offers a reliable and efficient solution for signature verification in financial environments. By enhancing the accuracy of forgery detection, the system contributes to stronger fraud prevention mechanisms and bolsters the integrity of digital banking transactions.

Importantly, the hybrid architecture incorporated both fixed (Canny-based) and trainable filters, benefiting from domain knowledge while retaining the learning flexibility of neural networks. This balanced approach provides a foundation for future advancements.

Looking ahead, potential extensions of this work may include the integration of transformer-based architectures or multi-modal biometric systems to further enhance accuracy, scalability, and real-world adaptability. The trained model is lightweight and suitable for deployment via frameworks such as TensorFlow Lite, supporting cross-platform compatibility. The system can be embedded into real-time signature verification pipelines or mobile banking applications, with support for both cloud-based APIs and on-device inference, offering versatile deployment options for financial institutions.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Noor Fadel contributed by selecting the methodology, applying it with the fourth researcher, and including the work's main idea. The academic writing of the research was for Bayadir A. Al-Himyari, and the linguistic review was for Hiba Al-Khafaji. All authors had approved the final version.

REFERENCES

[1] U. Akhundjanov, B. Soliyev, N. Juraev *et al*. "Off-line handwritten signature verification based on machine learning," in *Proc. E3S Web of Conferences, EDP Sciences*, vol. 508, 03011, 2024.

[2] S. D. Bhavani and R. K. Bharathi, "A multi-dimensional review on handwritten signature verification: strengths and gaps," *Multimedia Tools and Applications*, vol. 83, pp. 2853–2894, 2023.
[3] N. Fadel, I. K. Abbood, and H. Q. Gheni, "Best classification of continuous data based on hybrid decision tree," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 10, no. 1s, pp. 388–392, 2022.
[4] N. F. Hussain, W. Al-Hameed, and M. K. Ahmed, "Non destructive testing for detection abnormal object in the X-ray images," *Journal of Physics: Conference Series*, vol. 1660, no. 1, 012104, 2020.
[5] N. Fadel and E. I. A. Kareem, "Detecting hand gestures using machine learning techniques," *Ingenierie des Systemes d'Information*, vol. 27, no. 6, pp. 957–965, 2022.
[6] B. A. Eren, "Determinants of customer satisfaction in chatbot use: evidence from a banking application in Turkey," *International Journal of Bank Marketing*, vol. 2, no. 39, pp. 294–331, 2021.
[7] M. Dobrescu and E. M. Dobrescu, "Artificial Intelligence (AI)-the technology that shapes the world," *Global Economic Observer*, vol. 6, no. 2, pp. 71–81, 2018.
[8] E. Digalaki. (2022). The impact of artificial intelligence in the banking sector—how AI is being used in 2022. *Business Insider*. [Online]. Available: https://www.businessinsider.com/ai-in-banking-report?r=US&IR
[9] D. Tuteja, R. Dhand, M. Reineu *et al*. "Automated signature verification in bank cheque processing using Siamese and convolutional neural networks," in *Proc*. *2024 First International Conference on Electronics, Communication and Signal Processing (ICECSP) IEEE*, 2024, pp. 1–6.
[10] N. Thakur, D. Ghai, and S. Kumar, "Automatic imagery bank cheque data extraction based on machine learning approaches: A comprehensive survey," *Multimedia Tools and Applications*, vol. 82, no. 20, pp. 30543–30598, 2023.
[11] A. A. Lakshmi, G. S. Reddy, M. S. Reddy, and N. Kathirisetty, "Offline signature forgery detection based on geometric measures using tensorflow model," in *Proc*. *2024 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC)*, 2024, pp. 1–7.
[12] T. Akter, M. S. Akter, T. Mahmud *et al*. "Evaluating the performance of machine learning models in handwritten signature verification," in *Proc*. *2024 Asia Pacific Conference on Innovation in Technology (APCIT)*, 2024, pp. 1–6.
[13] Y. B. Hamdan and A. Sathesh, "Construction of statistical SVM based recognition model for handwritten character recognition," *Journal of Information Technology and Digital World*, vol. 3, no. 2, pp. 92–107, 2021.