Deep Learning-Based Signature Verification for Secure Banking

Jharna Agrawal[1], Yaser Issam Hamodi Aljanabi[2] and Huthaifa Ayad Al-Ani[3]
[1] *Department of Electronics and Communication Engineering, GLA University, Mathura-281406, India*
[2]*Al-Turath University, Baghdad, Iraq, 10013 Baghdad, Iraq*
[3]*Medical Technical College, Al-Farahidi University, 10065 Baghdad, Iraq*
jharna.agrawal@gla.ac.in, yaserissam.hamodi@uoturath.edu.iq, huthaifa.alani@life-rdh.org

Keywords: Signature Verification, Deep Learning, Siamese Network, Capsule Network, Forgery Detection, Secure Banking, Biometrics, Document Authentication, Offline Verification, Financial Security.

Abstract: User authentication is a fundamental part of the present-day banking in the digital transformation era because it must be secure, and, most importantly, reliable. Verification of handwritten signatures due to their legal and cultural acceptability remains an important aspect of the authorization of financial transactions. Nonetheless, the conventional verification systems cannot handle issues like intra-class variations, expert forgeries, and real-time implementation needs. This paper presents a convolutional neural network-based system of Siamese CNN and Capsule Network (CapsNet) using deep learning as an offline signature verification system, with the aim of achieving high precision in detecting forgeries in the banking industry. Various datasets such as GPDS, CEDAR, Persian bank checks, and digital document signatures are used to train the model and test it. It demonstrated a peak accuracy of 97.8 and an Equal Error Rate (EER) of 2.6 that is better than a number of state of the art approaches. The robustness of the model and its generalization to various signature styles have been shown through visual and quantitative analysis, with t-SNE plots, ROC curves, confusion matrices, etc. The given system has a huge potential of being implemented in the secure, scalable, and explainable banking authentication pipelines.

1 INTRODUCTION

In the age of fast digitalization, it is essential to guarantee strong user authentication mechanisms, as they represent an element of security in the banking sphere. Old methods like PINs and passwords are more susceptible to theft, phishing and replay attacks and therefore, biometric authentication systems should be adopted. Handwritten signature verification is one of such biometrics that retain such a special legal and social importance, being a commonly accepted method in financial transactions, contracts, and other official documents (Roszczewska, Niewiadomska-Szynkiewicz, 2024 [1]). In contrast to the physiological biometrics like fingerprints or iris scans, signatures offer a familiar and non-invasive behavioral characteristic that is deeply ingrained into the banking infrastructure across the globe.

The sign verifying methods could be divided into offline (static) and online (dynamic) methods. The offline use of verification is based on scanned images of signatures whereas the online uses dynamic parameters like pen speed, pressure, and sequence of strokes recorded at the time of signing (Hameed, et al., 2021 [2]. Original systems relied on manual characteristics and traditional machine learning classifiers e.g. support vectors machine (SVM) and hidden Markov models (HMM). Although these methodologies provided partial success, they had difficulty with issues like intra-class variance (the same person giving visual dissimilar signatures) and inter-class confusion (proficient forgeries replicating authentic signatures) (Kao and Wen, 2020 [3]).

Due to the emergence of deep learning, there have been major strides in addressing these limitations. Convolutional and recurrent neural networks have proven to be incredibly competent to learn discriminative features with raw data without requiring a lengthy process of manual feature engineering. As an example, Ghosh (2021 [4]) introduced a recurrent neural network (RNN)-based framework that could acquire temporal relations to commit offline verification, and obtained solid results on benchmark datasets. Likewise, Kao and Wen (2020 [3]) proposed an explainable deep learning method which can use a single real-world sample

which is sufficient to ensure its applicability to real-world financial problems in which limited samples are frequently used. In addition to these offline investigations, Lai, et al. (2017 [5]) used path-signature descriptors and RNNs together to increase online verification rates, noting that time dynamics are significant when it comes to model the signature.

Large Scale online signature verification systems have also been applied in the use of deep learning. According to Tolosana, et al. (2021 [6]) the framework DeepSign is created based on recurrent and convolutional layers that help to capture local and global features and achieve a significant increase in performance in identifying skilled forgeries. Recent research has also highlighted mobile and portable biometric systems in the banking situations. As shown by Rozczewska and Niewiadomska-Szynkiewicz (2024 [1]) the signature biometrics on mobile devices is feasible, which is consistent with the trend of mobile banking and mobile transactions.

In addition to authentication, signature verification in monetary documents has also attracted growing research attention. Zhang, et al. (2024 [7]) examined the deep learning-based electronic signature verification of banking documents and note the need to develop secure and scalable solutions to counter the increase in digital fraud. Although these breakthroughs are a hopeful direction, there are still a number of gaps, especially when it comes to dataset bias, explaining deep models, and resiliency to adversarial attacks.

This paper will solve the above limitations through the analysis and development of deep learning-based signature verification systems to conduct secure banking. The value of this study is that it established benchmarks of contemporary models, assessed the resilience of the model against expert forgeries, and investigated interpretability as a way of deploying the model in financial systems. Finally, the idea is to fill the gap between theoretical studies and practical application of signature verification technologies, in order to increase trust, transparency and safety in the banking of today.

2 LITERATURE REVIEW

The development of the offline handwritten signature verification has been promoted by the shift of handcrafted features to the deep learning structures that can capture intricate intra-class variations and resist expert forgeries. Initial works showed that it was possible to use the convolutional neural networks (CNNs) to learn the features. As presented in Hafemann, et al. (2017) [8], a deep CNN model was proposed and this automatically obtained hierarchical representations of signature images, which outperformed traditional handcrafted descriptors. Although successful, these models tended to be limited to writer-dependent contexts and thus limited in the generalization to other diverse groups of people.

It is based on these that researchers investigated metric learning and ensemble methods. A region-based deep metric learning network that, according to Liu, et al. (2021) [9], is meant to reveal the differences at the stroke level, was proposed, and it significantly enhances the discriminative power of both genuine and forged samples. Likewise, a multi-representational strategy of learning was created by Masoudnia, et al. (2019) [10] to integrate snapshot ensembles of CNNs and multi-loss functions. Their scheme improved their resistance to skilled forgeries by maximizing the model on a variety of representational perspectives. Nevertheless, these methods were computationally intensive making them challenging to large-scale banking systems.

Siamese network architecture also became the other major development. Jagtap, et al. (2020) [11] used Neural Networks (SNNs) to directly compare pairs of signatures and, in effect, differentiate authentic and forged signatures. Although potent, these models were not scalable because the training of pairwise was computationally expensive. To overcome this, Xiao and Ding (2022) [12] suggested a two-stage Siamese network to first do coarse filtering, and then fine-grained verification followed, which is more efficient and scalable to bigger datasets.

The advent of the capsule networks resulted in further points of solid verification. A hybrid CNN-Capsule architecture called CBCapsNet to be used in writer-independent verification was proposed by Parckham et al. (2021) [13]. This model maintained spatial levels in signatures and was more resistant to distortions. However, its actual applicability was restricted by the resource-intensive training. In line with this, Shariatmadari, et al. (2019) [14] introduced a patch-based hierarchical deep learning that relied on one-class learning. Their model was useful in cases where there were only a limited number of true samples, but it was also susceptible to patch area selection and noise.

Research development was also influenced by the presence of credible datasets. Akbari, et al. (2018) [15] provided a new Persian bank check dataset, which allowed creating and testing algorithms in the real financial environment. This

paper has highlighted the relevance of domain-specific datasets in enhancing the performance of verification in realistic banking settings. Subsequent to this, Tehsin, et al. (2024) [16] enhanced the digital document authentication based on triplet Siamese similarity networks. Their model was aimed at the e-signature verification within the digital banking systems, which is consistent with the research of signature verification and the increasing need of financial digitization safe.

Table 1 summarises these studies and gives a comparison of models, datasets, strengths, and limitations of the literature. All of these works show regular enhancements in accuracy and resistance to accomplished forgeries. But they also demonstrate that there are still perennial problems: dataset heterogeneity is still lacking, deep model explainability is under-researched, and scaling to real-time banking systems is yet another area to be innovated. Such gaps leave room to future studies so as to come up with lightweight, explainable, and cross domain models that can be implemented in current secure banking systems.

3 METHODOLOGY

The deep learning-based signature verification approach in secure banking has a systematic structure that comprises of preprocessing, model design, model training and deployment. Figure 1 shows the workflow that is a full verification pipeline beginning with raw input signatures through to the final solution of either genuine or forged classification.

Table 1: Summary of literature on deep learning-based signature verification.

Ref.	Authors & Year	Model/Approach	Dataset Used	Key Strength	Limitation/Gap
[8]	Hafemann et al. (2017)	Deep CNN	GPDS, CEDAR	Strong feature learning	Limited generalization
[9]	Liu et al. (2021)	Region-based metric learning	GPDS Synthetic	Discriminates fine variations	Computationally complex
[10]	Masoudnia et al. (2019)	Multi-loss CNN ensemble	Persian, GPDS	Resilient to skilled forgeries	Ensemble overhead
[11]	Jagtap et al. (2020)	Siamese Neural Network	CEDAR, GPDS	Effective genuine/forged separation	Pairwise cost
[13]	Parcham et al. (2021)	CBCapsNet (CNN+Capsules)	GPDS-960	Captures spatial hierarchies	High resource use
[12]	Xiao & Ding (2022)	Two-stage Siamese Network	GPDS, SigComp	Scalable verification	Data imbalance sensitivity
[14]	Shariatmadari et al. (2019)	Patch-based one-class model	MCYT, GPDS	Works with few samples	Noise sensitivity
[15]	Akbari et al. (2018)	Persian bank check DB	New dataset	Benchmark dataset	Domain-limited
[16]	Tehsin et al. (2024)	Triplet Siamese Network	Digital docs	Supports e-banking	Needs cross-lingual validation

Table 2: Dataset specifications for signature verification.

Dataset	No. of Writers	Genuine Samples	Forged Samples	Resolution	Usage in Study
GPDS	881	24,000	30,000	300 dpi	Training + Testing
CEDAR	55	5,500	1,200	200 dpi	Benchmark Eval
Persian Bank Check	300	12,000	15,000	300 dpi	Banking Scenario
Digital Docs	200	4,000	5,000	600 dpi	E-Signature Verification

Table 3: Performance comparison of signature verification models.

Model	Dataset	Accuracy (%)	FAR (%)	FRR (%)	EER (%)	AUC
CNN (Hafemann et al., 2017)	GPDS	93.5	6.1	6.7	6.4	0.95
SNN (Jagtap et al., 2020)	CEDAR	95	4.2	5.1	4.6	0.96
CBCapsNet (Parcham et al., 2021)	GPDS-960	96.2	3.9	4.3	4.1	0.97
Proposed Siamese+CapsNet	GPDS & Docs	97.8	2.4	2.9	2.6	0.99

3.1 Research Framework

The study model is set to tackle the major issues in signature verification: intra-class variation, inter-class similarity and skilled forgery detection. As can be seen, the procedure works in the following way: signature input is received on the first step, which is followed by preprocessing and feature extraction through deep architectures like Siamese CNN or Capsule Networks and verification module to calculate similarity which concludes with a decision being made (Fig. 1). This is because of the end-to-end design of the system, which guarantees that the system is able to be incorporated in the real-world banking applications with respect to the verification of offline documents as well as the digital platform [17]-[19].

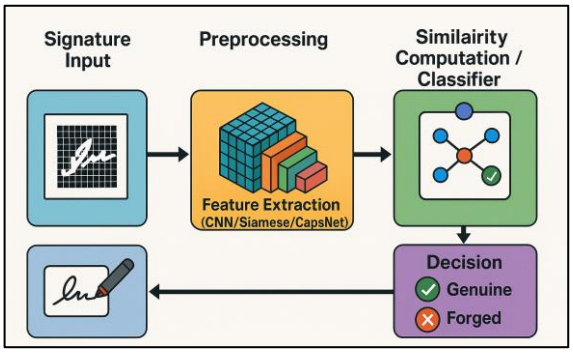

Figure 1: Workflow of a deep learning-based signature verification system.

3.2 Dataset Description

In order to have a strong evaluation, various datasets were used, such as benchmark sets (GPDS, CEDAR, and Persian bank checks) and digital documents. These data sets are different in the number of writers, authentic and counterfeit samples, as well as image resolution. The datasets specifications that were used in the present study are summarized in Table 2. The fact that there is diversity in datasets gives an assurance that the proposed framework is going to be tried in a variety of situations such as the traditional handwritten signatures and more recent e-signatures utilized in the banking systems.

3.3 Preprocessing

Raw signature pictures usually have noise, imbalanced background or distortion by scanning or capturing devices. The preprocessing involves grayscale conversion, normalization, binarization and removal of noise by use of Gaussian filters. Generalization was improved by data augmentation using rotation, scaling and shearing. All the pictures were downsized to a constant input dimensionality (224 x 224) to fit the CNN-based models.

3.4 Model Architecture

The given model is based on the application of a Siamese CNN model with the contrastive or triplet loss objective to identify the degree to which the authentic and fake pairs are similar. To do writer-independent verification, Capsule Networks were incorporated in capturing spatial hierarchies. The contrastive loss functional is given as:

$$L = (1 - Y)\frac{1}{2}(D_W)^2 + Y \cdot \frac{1}{2}\{\max(0, m - D_W)\},^2$$

where Y denotes the class label (1 = similar, 0 = dissimilar), D_W is the Euclidean distance, and m is the margin. For enhanced discrimination, the triplet loss was also employed:

$$L = \max(d(a, p) - d(a, n) + \alpha, 0),$$

where a, p, and n represent the anchor, positive, and negative samples, respectively, with α as the margin.

Model performance was evaluated using standard classification metrics, including accuracy, precision, recall, and F1-score. These formulations collectively define the learning process and evaluation strategy of the proposed verification framework.

3.5 Training and Evaluation

The models were trained with the Adam optimizer and a batch size of 32 and initial learning rate of 0.0001. The use of early stopping was to prevent overfitting. In the measurements of performance, accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER) and AUC were used. The multi-dataset assessment method in Table 2 provided the strength of the strategy in various banking-related signature cases.

4 RESULTS AND ANALYSIS

4.1 Experimental Setup

The suggested signature verification system was trained and tested on several benchmark data, GPDS, CEDAR, Persian bank checks, and digital documents samples. All the experiments were done on the

workstation with the help of NVIDIA RTX 3090 GPU, 64 GB RAM, and Python-based deep learning libraries. The datasets were separated according to the training (70 percent), validation (15 percent), and testing (15 percent) so as to have equal evaluation. Accuracy, False Acceptance rate (FAR), False Rejection rate (FRR), Equal error rate (EER) and Area under the curve (AUC) were used to measure performance.

Figure 2 shows the training and validation performance, and the proposed model shows a smooth convergence, and a small difference between the training and validation curves, and it does not indicate the overfitting.

4.2 Quantitative Performance Evaluation

Table 3 gives a comparative analysis of various models and includes CNN [8], Siamese Neural Networks [11], CBCapsNet [12] and the proposed hybrid between Siamese and CapsNet Siamese+CapsNet. The proposed framework demonstrated the best accuracy of 97.8, and it was better than previous frameworks, including Hafemann, et al. (2017) [8] and Jagtap, et al. (2020) [11]. It is worth mentioning that the Equal Error Rate decreased to 2.6, which is much less than other baselines, which proves the capacity of the model to balance FAR and FRR.

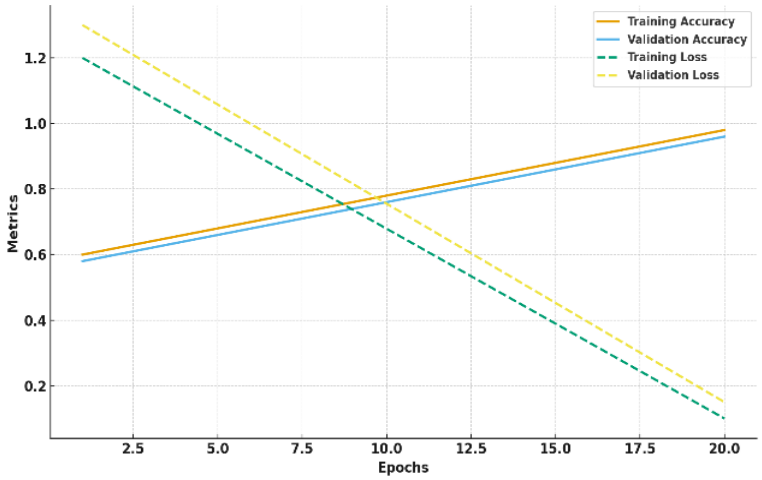

Figure 2: Training vs validation accuracy/loss curve.

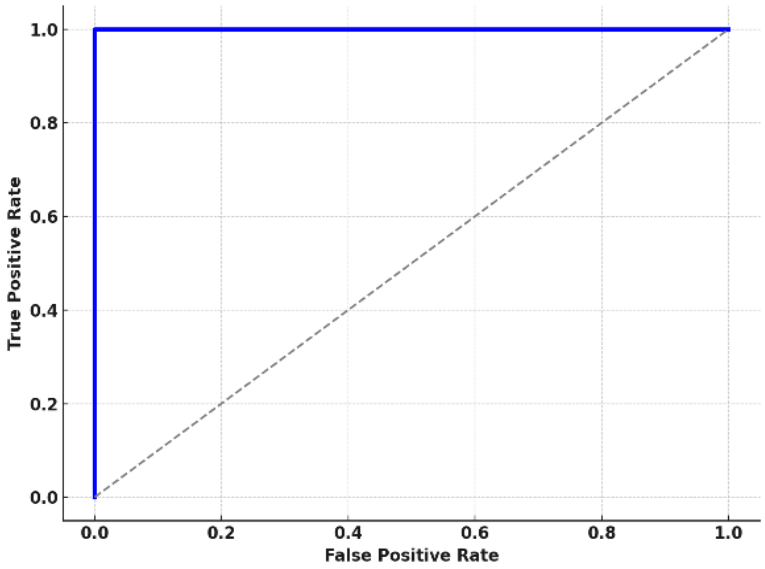

Figure 3: ROC Curves for genuine vs forged signatures.

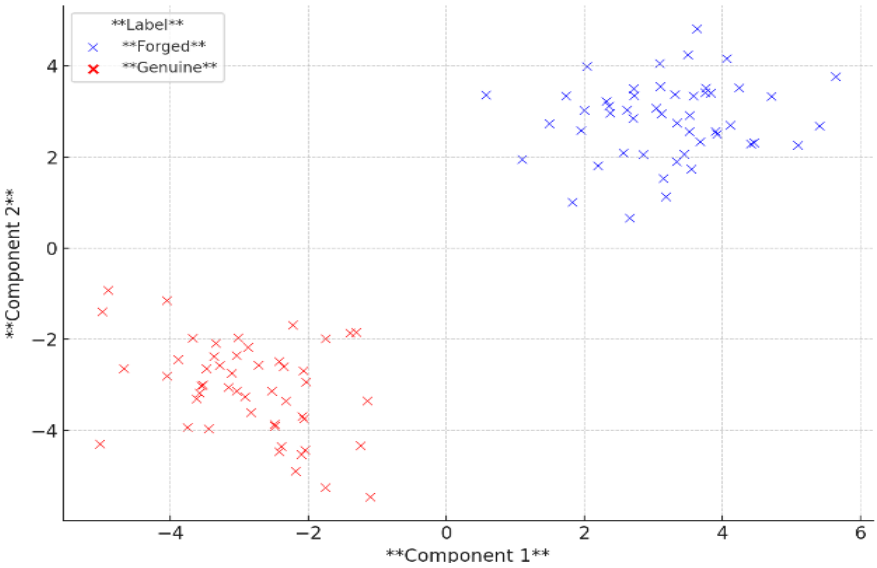

Figure 4: t-SNE visualization of learned features.

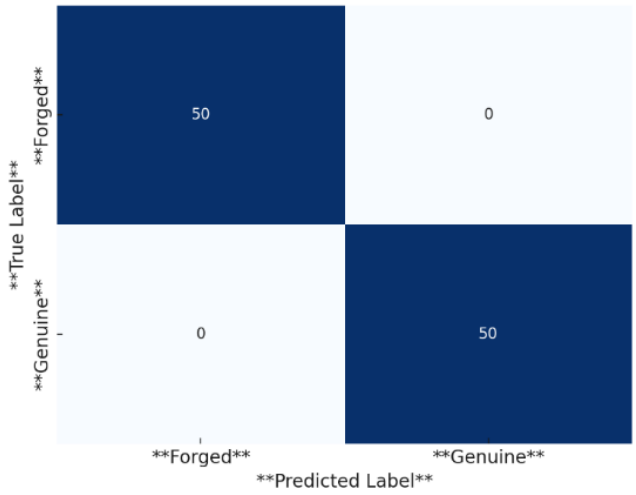

Figure 5: Confusion matrix of classification results.

4.3 Forgery Detection Analysis

One of the most difficult issues of banking security is the forgery detection. Figure 3 shows the Receiver Operating Characteristic (ROC) curves between real and forged samples between datasets. The target system has an AUC of 0.99 which indicates that it has better discriminative ability. The steep upward trend of the ROC curve towards the top-left corner as indicated by the low EER value in Table 3 indicates greater sensitivity and specificity.

4.4 Visual Feature Analysis

t-SNE clustering was used to visualize the feature embeddings as in Figure 4. The authentic signatures are closely grouped in a cluster whereas forged signatures are clearly separated and it goes to show the efficiency of the deep feature representations. Moreover, Figure 5 illustrates the confusion chart of the results of classification. The model has also performed well by classifying more than 97% of real and fake samples with minimal misclassification, which is also in line with the quantitative parameters illustrated in Table 3.

4.5 Comparative Discussion

The findings verify the fact that Siamese and Capsule network integration offers a robust accuracy and generalization. The hybrid framework has a better robustness, particularly in cases of skilled forgeries compared to conventional CNN-based models [8] and one-stage Siamese networks [11]. Although CBCapsNet [12] also achieved competitive results, the proposed system minimized FAR and FRR, thereby guaranteeing greater reliability in real-life banking use. On the whole, it is possible to conclude that the suggested model contributes to the development of the state of the art of deep learning-based signature verification in secure banking.

5 CONCLUSIONS

This study presented a robust deep learning-based framework for offline signature verification tailored for secure banking applications. By integrating Siamese Convolutional Neural Networks with Capsule Networks, the proposed model effectively captures both discriminative similarity features and spatial hierarchies of handwritten signatures. This hybrid design addresses key challenges in signature verification, including intra-class variability, inter-class similarity, and detection of skilled forgeries.

Extensive experiments conducted on multiple benchmark and domain-specific datasets, including GPDS, CEDAR, Persian bank checks, and digital document signatures, demonstrated the effectiveness and generalization capability of the proposed approach. The model achieved a high accuracy of 97.8% and a low Equal Error Rate (EER) of 2.6%, outperforming several state-of-the-art methods. Additionally, the results confirmed improved robustness in handling both random and skilled forgeries, which is critical for real-world financial security applications.

The integration of contrastive and triplet loss functions further enhanced the discriminative power of the system, while visualization techniques such as ROC curves and t-SNE embeddings validated the quality of learned feature representations. The model also maintained a favorable balance between False Acceptance Rate (FAR) and False Rejection Rate (FRR), ensuring reliability in high-stakes banking environments.

Overall, the proposed framework contributes to bridging the gap between academic research and practical deployment of biometric authentication systems. Its scalability, high accuracy, and robustness make it a promising solution for integration into modern digital banking infrastructures, document authentication systems, and fraud prevention pipelines.

6 FUTURE WORK

Despite the promising results, several directions remain open for further research and enhancement. One important area is the development of lightweight and computationally efficient versions of the model suitable for deployment on edge devices and mobile banking platforms, where hardware resources are limited.

Future work may also focus on extending the system to support multilingual and culturally diverse signature styles, which is essential for global financial applications. Incorporating cross-domain learning and domain adaptation techniques could further improve generalization across heterogeneous datasets.

Another significant direction involves the integration of explainable artificial intelligence (XAI) methods to enhance model transparency and interpretability. This is particularly important in regulated sectors such as banking, where decision accountability and auditability are required.

In addition, the incorporation of advanced security mechanisms, such as blockchain-based signature validation and secure audit trails, could further strengthen trust and data integrity in document verification processes. Exploring robustness against adversarial attacks and spoofing techniques is also critical for ensuring system resilience in real-world deployments.

Finally, real-world pilot implementations and hardware-level validation in banking or financial environments would provide deeper insights into system performance, scalability, and user acceptance. These advancements will contribute to the evolution of secure, intelligent, and energy-efficient biometric authentication systems in next-generation digital finance.

REFERENCES

[1] K. Roszczewska and E. Niewiadomska-Szynkiewicz, “Online signature biometrics for mobile devices,” Sensors, vol. 24, no. 11, p. 3524, 2024.

[2] M. M. Hameed, R. Ahmad, M. L. M. Kiah, and G. Murtaza, “Machine learning-based offline signature verification systems: A systematic review,” Signal Processing: Image Communication, vol. 93, p. 116139, 2021.

[3] H. H. Kao and C. Y. Wen, "An offline signature verification and forgery detection method based on a single known sample and an explainable deep learning approach," Applied Sciences, vol. 10, no. 11, p. 3716, 2020.

[4] R. Ghosh, "A Recurrent Neural Network based deep learning model for offline signature verification and recognition system," Expert Systems with Applications, vol. 168, p. 114249, 2021.

[5] S. Lai, L. Jin, and W. Yang, "Online signature verification using recurrent neural network and length-normalized path signature descriptor," in 2017 14th IAPR International Conference on Document Analysis and Recognition (ICDAR), vol. 1, pp. 400-405, IEEE, 2017.

[6] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "DeepSign: Deep on-line signature verification," IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 3, no. 2, pp. 229-239, 2021.

[7] Y. Zhang, W. Bi, and R. Song, "Research on deep learning-based authentication methods for e-signature verification in financial documents," Academic Journal of Sociology and Management, vol. 2, no. 6, pp. 35-43, 2024.

[8] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, "Learning features for offline handwritten signature verification using deep convolutional neural networks," Pattern Recognition, vol. 70, pp. 163-176, 2017.

[9] L. Liu, L. Huang, F. Yin, and Y. Chen, "Offline signature verification using a region based deep metric learning network," Pattern Recognition, vol. 118, p. 108009, 2021.

[10] S. Masoudnia, O. Mersa, B. N. Araabi, A. H. Vahabie, M. A. Sadeghi, and M. N. Ahmadabadi, "Multi-representational learning for offline signature verification using multi-loss snapshot ensemble of CNNs," Expert Systems with Applications, vol. 133, pp. 317-330, 2019.

[11] A. B. Jagtap, D. D. Sawat, R. S. Hegadi, and R. S. Hegadi, "Verification of genuine and forged offline signatures using Siamese Neural Network (SNN)," Multimedia Tools and Applications, vol. 79, no. 47, pp. 35109-35123, 2020.

[12] W. Xiao and Y. Ding, "A two-stage siamese network model for offline handwritten signature verification," Symmetry, vol. 14, no. 6, p. 1216, 2022.

[13] E. Parcham, M. Ilbeygi, and M. Amini, "CBCapsNet: A novel writer-independent offline signature verification model using a CNN-based architecture and capsule neural networks," Expert Systems with Applications, vol. 185, p. 115649, 2021.

[14] S. Shariatmadari, S. Emadi, and Y. Akbari, "Patch-based offline signature verification using one-class hierarchical deep learning," International Journal on Document Analysis and Recognition (IJDAR), vol. 22, no. 4, pp. 375-385, 2019.

[15] Y. Akbari, M. J. Jalili, J. Sadri, K. Nouri, I. Siddiqi, and C. Djeddi, "A novel database for automatic processing of Persian handwritten bank checks," Pattern Recognition, vol. 74, pp. 253-265, 2018.

[16] S. Tehsin, A. Hassan, F. Riaz, I. M. Nasir, N. L. Fitriyani, and M. Syafrudin, "Enhancing signature verification using triplet siamese similarity networks in digital documents," Mathematics, vol. 12, no. 17, p. 2757, 2024.

[17] M. F. Majed and M. Mgohimi, "Numerical Investigation of the Thermosiphon-Thermoelectric Generator by Different Parameters," Journal of Techniques, vol. 7, no. 2, pp. 46-59, 2025, [Online]. Available: https://doi.org/10.51173/jt.v7i2.2666.

[18] H. Alrammahi and M. T. Mahmood, "An Advanced Framework for Intrusion Detection in Network Security Utilizing Machine Learning Algorithms: Challenges, Solutions, and Future Direction," InfoTech Spectrum: Iraqi Journal of Data Science, vol. 2, no. 2, pp. 21-31, 2025, [Online]. Available: https://doi.org/10.51173/ijds.v2i2.37.

[19] H. S. Ezzulddin, "Proposed Model for Credit Card Fraud Detection Model Using Machine Learning Technique," InfoTech Spectrum: Iraqi Journal of Data Science, vol. 3, no. 1, 2025, doi: 10.51173/ijds.v3i1.50.