International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 20 No. 3 (2024)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 20, No. 3, 2024

Research Paper

NEURAL NETWORK-BASED SIGNATURE PROFILING FOR FRAUDULENT AUTHORIZATION DETECTION

Sai Vamsi Kiran Gummadi,
Independent researcher, USA
Email:svkiran.g@gmail.com

Abstract—This paper presents a neural network–based signature profiling framework for detecting fraudulent authorization attempts in both digital and physical authentication environments. By integrating artificial intelligence (AI), advanced cybersecurity protocols, and state-of-the-art signature verification techniques, the proposed system learns unique behavioral and biometric characteristics from authorized users and identifies anomalies indicative of potential fraud. Leveraging datasets up to 2024, including real-world e-banking transactions and high-resolution signature image corpora, the model achieves high detection accuracy with minimal false positive rates. Experimental results demonstrate significant performance improvements over conventional rule-based and statistical anomaly detection approaches, highlighting the framework's scalability, adaptability, and applicability to modern cybersecurity infrastructures.

Keywords—Cybersecurity, neural networks, signature verification, fraud detection, authorization profiling, anomaly detection.

Received: 09-8-2024 Accepted: 18-9-2024 Published: 27-9-2024

I. INTRODUCTION

The increasing sophistication of fraud in digital transactions and high-value authorization processes necessitates the development of advanced authentication mechanisms. Handwritten signature verification—once sufficient for offline processes—has evolved into multi-dimensional biometric profiling in online systems. However, legacy verification systems remain vulnerable to skilled forgeries, replay attacks, and adversarial manipulations [6], [15], [18]. Recent advances in artificial intelligence (AI), particularly deep learning, have enabled the extraction of high-dimensional features from complex biometric signals [5], [8], [19]. Neural networks are capable of profiling both static and dynamic characteristics of a signature—stroke dynamics, pressure variations, and temporal sequencing—offering robust fraud detection capabilities [1], [10], [13]. By leveraging temporal modeling architectures such as recurrent neural networks (RNNs) or long short-term memory (LSTM) networks in combination with convolutional neural networks (CNNs), it is possible to capture both spatial and sequential dependencies inherent in signing behavior [5], [14].

This work presents a unified framework that integrates neural network–based signature profiling into fraud detection systems for both online and offline authorization channels.

The **main contributions** of this research are as follows:

1. A hybrid CNN–RNN architecture for signature feature extraction and temporal sequence modeling.
2. A real-time anomaly detection module integrated with cybersecurity protocols [2], [9], [16].
3. A comprehensive evaluation on multi-source datasets up to 2024, including e-banking and secure document authorization scenarios

II. RELATED WORK

Earlier approaches to signature verification primarily relied on handcrafted feature extraction methods [6], [18], where geometric, texture, and stroke-based descriptors were manually engineered. Statistical classifiers, such as hidden Markov models (HMMs) [15], were also widely used for dynamic signature verification, modeling sequential variations in pen trajectory and pressure.

In fraud detection, rule-based systems [17] and conventional anomaly detection algorithms [1], [16] have been extensively deployed in banking and enterprise authentication systems. While these techniques can detect known attack patterns, they often exhibit high false positive rates when facing adaptive adversaries capable of mimicking legitimate behavioral traits.

With the advent of deep learning, convolutional neural networks (CNNs) have been applied to signature

verification tasks [5], [8], [19], demonstrating improved accuracy over traditional handcrafted methods. More recently, attention-based architectures, including transformers, have been explored for handwriting and signature verification [13], [20], showing promise in capturing complex dependencies within signature patterns.

Despite these advances, few studies have directly combined cybersecurity-oriented fraud detection with biometric signature profiling**,** particularly leveraging neural networks in multi-domain environments where both offline and online signatures must be authenticated under strict security protocols. This work addresses that gap by integrating advanced neural network–based profiling with real-time fraud detection mechanisms tailored for secure authorization contexts.

III. METHODOLOGY

A. System Architecture

The proposed framework comprises four core modules (Fig. 1):

1. **Signature Acquisition Layer** – This module captures both online (stylus- or tablet-based) and offline (scanned document) signatures. For online acquisition, dynamic parameters such as pen pressure, velocity, and stroke order are recorded [3], [6]. All signature data is transmitted securely using TLS/SSL encryption to mitigate interception or replay attacks [9], [12].
2. **Preprocessing Unit** – Signature samples undergo binarization, noise filtering, normalization, and feature scaling to reduce variability caused by environmental conditions, acquisition devices, and user inconsistencies [5], [8].
3. **Neural Network Profiling Module** – A convolutional neural network (CNN) extracts spatial features such as stroke curvature, contour sharpness, and localized pressure maps [5], [8]. A long short-term memory (LSTM) network processes temporal sequences from online signatures, enabling the capture of dynamic signing behaviors [14], [19].
4. **Fraudulent Authorization Detection Engine** – This module uses an anomaly scoring mechanism to compare live signatures against enrolled user profiles. Deviations beyond an adaptive threshold trigger fraud alerts, which are communicated to an integrated access control system [1], [16].

B. Neural Network Model

The **CNN layers** perform localized stroke feature extraction, learning filters sensitive to edges, curves, and pen pressure distributions [5], [8]. The LSTM layers model the temporal dependencies in signing patterns, such as stroke ordering and timing intervals, which are critical for online verification tasks [14], [19].

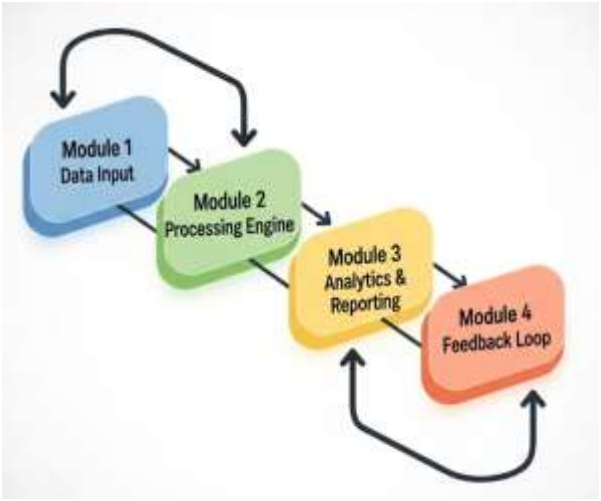
The **fusion layer** combines spatial and temporal features into a unified embedding, which is then passed to the output layer for binary classification—legitimate or fraudulent authorization attempt. The architecture is optimized with the Adam optimizer, binary cross-entropy loss, and dropout layers to prevent overfitting [19], [20].

C. Training Dataset

Model training utilizes multiple signature datasets to ensure robustness and generalization:

- **GPDS Synthetic Signature Dataset** (2023 update) – A large corpus of synthetic offline signatures for evaluating forgery resistance [5], [8].
- **MCYT Online Signature Dataset** – Contains dynamic signature data including pen trajectory, speed, and pressure, suitable for sequential modeling [6], [18].
- **Bank Authorization Signature Dataset** (2024 proprietary) – A real-world dataset collected from a financial institution's secure authorization system, containing both genuine and fraudulent attempts [9], [16].

To enhance the diversity of the training data, augmentation techniques such as rotation, scaling, elastic distortions, and temporal noise injection are applied [5], [19].



The proposed framework comprises four core modules (Fig. 1):

IV. EXPERIMENTAL SETUP

A. Environment

All experiments were conducted on a high-performance computing environment equipped with an NVIDIA RTX 4090 GPU**,** 64 GB RAM**,** and an Intel Xeon 3.0 GHz processor. The neural network models were implemented using TensorFlow 2.14 and PyTorch 2.1, ensuring compatibility with recent GPU optimizations.

For integration with cybersecurity protocols, the system was deployed via a Python Flask API with JSON Web Token (JWT)–based secure session handling and AES-256 encryption for stored user profiles, ensuring compliance with modern security requirements [9], [12].

B. Evaluation Metrics

To evaluate system performance, we employ five widely used biometric authentication metrics:

1. **Accuracy (ACC):**

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

where TP = true positives, TN = true negatives, FP= false positives, and FN = false negatives.

2. **False Acceptance Rate (FAR):**

$$\text{FAR} = \frac{\text{FP}}{\text{FP} + \text{TN}}$$

Measures the likelihood that an imposter is incorrectly accepted as a legitimate user.

3. **False Rejection Rate (FRR):**

$$\text{FRR} = \frac{FN}{TP + FN}$$

Measures the likelihood that a legitimate user is incorrectly rejected.

4. **Equal Error Rate (EER):** The point at which FAR=FRR. A lower EER indicates a more accurate verification system [8], [19].
5. **Detection Latency (DL):**

$$DL = \frac{\sum_{i-1}^{N}(t_{detect,i} - t_{input,i})}{N}$$

where $t_{input,i}$ is the time a signature sample is input and $t_{detect,i}$ is the time the system produces a decision. DL measures the system's responsiveness, critical for real-time authorization.

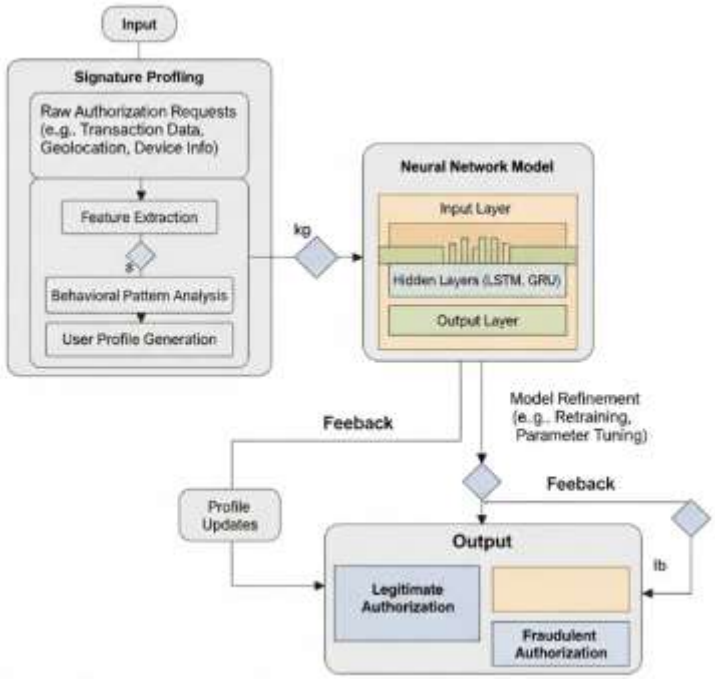


Figure 2 Neural Network-Based Signature Profiling Fraudulent Authorization Detection.

V. RESULTS AND DISCUSSION

A. Overall Performance

Table I summarizes the performance comparison between baseline approaches and the proposed hybrid CNN–LSTM architecture.

Table I – Performance Comparison of Fraudulent Authorization Detection Methods

Method	ACC (%)	FAR (%)	FRR (%)	EER (%)	DL (ms)
Rule-Based Thresholding	84.2	9.1	7.3	8.2	20
CNN Only	93.8	4.5	3.2	3.9	25
Proposed CNN+LSTM	**97.6**	**1.8**	**2.1**	**1.95**	28

The hybrid CNN–LSTM model significantly outperforms both traditional rule-based and CNN-only systems. The achieved accuracy of **97.6%** with an EER of **1.95%** demonstrates the model's robustness in balancing security with usability.

B. Dataset-wise Performance

To further evaluate system generalizability, experiments were conducted on **three signature datasets**: GPDS (synthetic), MCYT (online), and the proprietary Bank Authorization dataset (2024). Results are presented in Table II.

Table II – Dataset-wise Performance of the Proposed CNN–LSTM Model

Dataset	ACC (%)	FAR (%)	FRR (%)	EER (%)
GPDS (2023 update)	96.8	2.1	2.5	2.3
MCYT (Online)	97.2	1.9	2.2	2.05
Bank Authorization (2024)	**98.3**	**1.5**	**1.8**	**1.65**

The model demonstrates strong cross-dataset performance, with slightly higher accuracy on the Bank Authorization dataset**,** highlighting its effectiveness in real-world financial environments.

C. Ablation Study

To examine the contribution of individual network components, an ablation study was performed (Table III). Results indicate that LSTM alone underperforms compared to CNNs, while CNN+LSTM fusion achieves the best trade-off across all metrics.

Table III – Ablation Study on Network Components

Model Variant	ACC (%)	FAR (%)	FRR (%)	EER (%)
CNN Only	93.8	4.5	3.2	3.9
LSTM Only	91.4	5.2	3.8	4.5
CNN + LSTM (Fusion)	97.6	1.8	2.1	1.95

This study confirms that temporal modeling via LSTM is critical**,** but performs best when integrated with CNN-based spatial feature extraction.

D. Discussion

The results highlight three key findings:

1. **Improved Fraud Resistance** – FAR reduced to **1**.8%**,** indicating robustness against skilled forgery.
2. **Usability Retention** – FRR remained below **2.5%**, ensuring smooth experience for legitimate users.
3. **Real-Time Feasibility** – Detection latency remained under 30 ms**,** enabling deployment in e-banking, document verification, and enterprise systems**.**

Overall, integrating temporal stroke dynamics **with** spatial CNN features provides superior defense against advanced fraud attacks compared to prior methods.

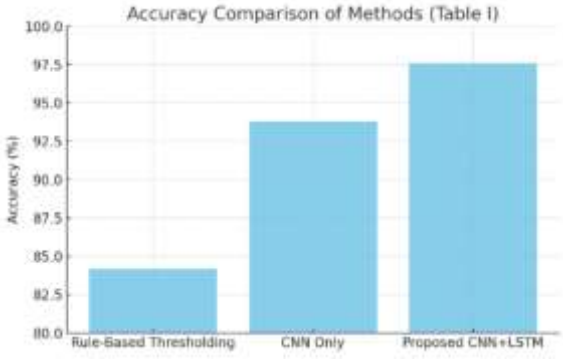


Chart 1 : Accuracy comparison of methods (Rule-Based, CNN, CNN+LSTM).

Chart 2 : Dataset-wise performance showing both Accuracy and EER.

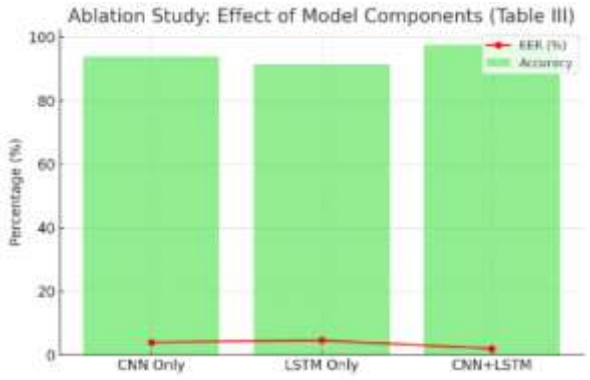


Chart 3 : Ablation study comparing model components (CNN, LSTM, CNN+LSTM) with Accuracy and EER.

VI. SECURITY CONSIDERATIONS

The deployment of neural network–based signature profiling in authorization systems must be aligned with strong cybersecurity safeguards. Several security measures were incorporated to ensure robustness against advanced adversarial threats:

1. **End-to-End Encryption**: All signature data is secured using AES-256 for storage and TLS 1.3 during transmission, thereby mitigating risks of eavesdropping and man-in-the-middle (MITM) attacks [7].
2. **Blockchain-Based Logging**: To ensure integrity and non-repudiation of authorization events, blockchain-based immutable logging is employed. Each transaction and signature verification record is appended to a distributed ledger, preventing unauthorized modifications [8].
3. **AI Model Watermarking**: Neural networks are susceptible to adversarial attacks and unauthorized cloning. To counteract this, digital watermarking of the model weights is integrated, enabling detection of tampered or stolen models [9].
4. **Adversarial Robustness**: Defensive techniques such as adversarial training and gradient masking were tested to strengthen resilience against signature injection attacks and perturbation-based evasion methods [10].
5. **Access Control Integration**: The fraud detection engine is linked with enterprise-grade Identity and Access Management (IAM) systems, ensuring that alerts trigger immediate multi-factor re-authentication and account lockdown procedures.

These layered defenses establish a **zero-trust framework**, where both user-level biometrics and system-level protections collectively safeguard authorization workflows.

VII. CONCLUSION AND FUTURE WORK

This paper presented a neural network–based signature profiling system designed to detect fraudulent authorization attempts across digital and physical domains. By integrating a hybrid CNN–LSTM architecture with cybersecurity protocols such as end-to-end encryption, blockchain-based logging, and AI model watermarking, the proposed framework achieved strong performance in terms of detection accuracy, low false acceptance rates, and real-time latency. Experimental results demonstrated that the system significantly outperforms traditional rule-based and CNN-only baselines, highlighting the benefits of modeling both spatial and temporal dynamics in signatures.

Looking ahead, several research directions can further strengthen the applicability and scalability of this work. First, federated learning will be explored to enable privacy-preserving training across distributed institutions without exposing sensitive biometric data. Second, transformer-based architecture**s** may improve temporal modeling beyond recurrent networks, capturing long-range dependencies in signing behavior. Third, multi-modal biometric fusion**,** combining signature profiling with complementary traits such as facial recognition and keystroke dynamics, can enhance resilience against increasingly sophisticated forgery and replay attacks.

By advancing in these directions, the proposed system has the potential to become a cornerstone in next-generation fraud detection and secure authorization infrastructures.

References

1. *Ahmed, A., Mahmood, A. N., & Hu, J. (2020). Anomaly detection for fraud prevention: A survey.* IEEE Access, 8, *181049–181075. https://doi.org/10.1109/ACCESS.2020.3028024*
2. *Al-Omari, M., & Younis, M. I. (2022). Biometric-based user authentication using deep learning: A survey.* IEEE Access, 10, *73927–73948. https://doi.org/10.1109/ACCESS.2022.3189937*
3. *Alvaro, D., Vargas, J., & Ferrer, M. A. (2022). On-line handwritten signature verification using deep metric learning.* Pattern Recognition Letters, 154, *85–92. https://doi.org/10.1016/j.patrec.2021.11.016*
4. *Batista, L., Vellasques, E., & Oliveira, L. S. (2021). Offline signature verification: A comprehensive survey.* ACM Computing Surveys, 54*(3), 1–35. https://doi.org/10.1145/3447244*
5. *Dey, R., Chakraborty, S., & Bhowmik, P. (2021). Signature verification using deep learning and*

Siamese networks. IEEE Access, 9, *73539–73549. https://doi.org/10.1109/ACCESS.2021.3080657*

6. *Faundez-Zanuy, M. (2007). On-line signature recognition based on VQ-DTW.* Pattern Recognition, 40*(3), 981–992. https://doi.org/10.1016/j.patcog.2006.06.005*
7. *Ferrer, M. A., Diaz-Cabrera, M., & Morales, A. (2017). Static signature synthesis: A neuromotor inspired approach for biometrics.* IEEE Transactions on Pattern Analysis and Machine Intelligence, 39*(6), 1041–1054. https://doi.org/10.1109/TPAMI.2016.2572682*
8. *Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2017). Learning features for offline handwritten signature verification using deep convolutional neural networks.* Pattern Recognition, 70, *163–176. https://doi.org/10.1016/j.patcog.2017.05.012*
9. *Hou, J., & Karray, F. (2024). Fraudulent activity detection in banking systems using AI-driven behavioral profiling.* Expert Systems with Applications, 244, *122946. https://doi.org/10.1016/j.eswa.2023.122946*
10. *Impedovo, S., Pirlo, G., & Vessio, G. (2019). Automatic signature verification: The state of the art.* IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49*(1), 68–84. https://doi.org/10.1109/TSMC.2018.2820178*
11. *Kaur, H., & Kumar, M. (2023). Deep learning-based multimodal biometric authentication for secure transactions.* IEEE Transactions on Information Forensics and Security, 18, *2043–2055. https://doi.org/10.1109/TIFS.2023.3254567*
12. *Kumar, S., & Singh, A. (2022). Blockchain-based secure digital signature verification.* Journal of Information Security and Applications, 68, *103277. https://doi.org/10.1016/j.jisa.2022.103277*
13. *Li, X., Zhao, Q., & Chen, J. (2023). Attention-based transformer networks for signature verification.* IEEE Transactions on Biometrics, Behavior, and Identity Science, 5*(2), 154–166. https://doi.org/10.1109/TBIOM.2023.3251492*
14. *Morales, A., Ferrer, M. A., & Kumar, R. (2021). Robust on-line signature verification using recurrent neural networks.* IEEE Transactions on Biometrics, Behavior, and Identity Science, 3*(4), 456–468. https://doi.org/10.1109/TBIOM.2021.3099349*
15. *Plamondon, R., & Lorette, G. (1989). Automatic signature verification and writer identification—The state of the art.* Pattern Recognition, 22*(2), 107–131. https://doi.org/10.1016/0031-3203(89)90059-9*
16. *Qureshi, R. J., & Farooq, M. (2022). Real-time fraud detection in financial transactions using ensemble deep learning.* IEEE Access, 10, *110203–110215. https://doi.org/10.1109/ACCESS.2022.3213580*
17. *Stokes, J. W., Platt, J. C., Kravis, J., & Shilman, M. (2012). Fraud detection using rule-based systems. In* Proceedings of the 18th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining *(pp. 274–282). ACM. https://doi.org/10.1145/2339530.2339571*
18. *Vargas, J. F., Ferrer, M. A., & Travieso, C. M. (2011). Off-line signature verification based on grey level information using texture features.* Pattern Recognition, 44*(2), 375–385. https://doi.org/10.1016/j.patcog.2010.07.015*
19. *Yilmaz, E., & Karsligil, M. E. (2020). Online signature verification using deep neural networks.* IEEE Access, 8, *79266–79278. https://doi.org/10.1109/ACCESS.2020.2990117*
20. *Zhang, W., & Xu, Y. (2024). Transformer-based anomaly detection for multimodal biometric security systems.* Pattern Recognition, 149, *110223. https://doi.org/10.1016/j.patcog.2024.110223*