SIGNSECURE : HANDWRITTEN SIGNATURE VERIFICATION

Rutuja Sangole
Department of Computer Engineering, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, Maharashtra ,India
rutuja.sangole@cumminscollege.edu.in

Renuka Narkhede
Department of Computer Engineering, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, Maharashtra ,India
renuka.narkhede@cumminscollege.edu.in

Sakshee Poradwar
Department of Computer Engineering, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, Maharashtra ,India
sakshee.poradwar@cumminscollege.edu.in

Shalvi Dangre
Department of Computer Engineering, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, Maharashtra ,India
shalvi.dangre@cumminscollege.edu.in

Vaishnavi Kulkarni
Department of Computer Engineering, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, Maharashtra ,India
vaishnavi.kulkarni@cumminscollege.edu.in

Achal Thakare
Department of Computer Engineering, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, Maharashtra ,India
achal.thakare@cumminscollege.edu.in

Minakshi Getkar
Department of Computer Engineering, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, Maharashtra ,India
minakshi.getkar@cumminscollege.edu.in

Abstract— **In many educational institutions, hostel wardens rely on manually signed leave applications, making it difficult to verify whether the handwritten signature of the Head of Department (HOD) is genuine or forged. This project addresses that challenge by developing an automated Handwritten Signature Verification System using a Convolutional Neural Network (CNN) based Siamese architecture. The system analyzes and compares signature patterns to accurately distinguish between authentic and forged signatures.To ensure security and integrity, all signature data is encrypted, and verification results are stored on a blockchain ledger, making records tamper-proof and auditable. The complete solution is deployed on AWS cloud, enabling scalable access and reliable performance. With future plans to integrate quantum-secure encryption, this system aims to provide a robust, trustworthy, and technologically advanced method of signature verification in academic and administrative environments.**

I. INTRODUCTION

In educational institutions, handwritten signatures continue to play a vital role in authorizing official documents such as student leave applications, attendance records, and administrative approvals. Hostel wardens, in particular, rely heavily on handwritten signatures from the Head of Department (HOD) to grant permission for students to leave campus. Despite the widespread use of digital technologies, this manual process remains vulnerable to errors, forgery, and misuse. Verifying the authenticity of handwritten signatures through visual inspection alone is both time-consuming and unreliable, especially when wardens are not familiar with the exact signature style of every HOD.

Signature forgery is a serious concern, as forged approvals can lead to unauthorized leaves, security risks, and administrative inconsistencies. Traditional verification methods depend entirely on human judgment, which is subjective and prone to mistakes. As the number of students and administrative transactions increases, the need for an automated, accurate, and secure signature verification mechanism becomes essential. This necessity has motivated the development of intelligent systems capable of analyzing handwritten signatures using machine learning techniques.

Recent advancements in deep learning, particularly Convolutional Neural Networks (CNNs), have shown remarkable success in image-based pattern recognition tasks. A Siamese CNN architecture is especially effective for signature verification because it focuses on comparing pairs of signatures rather than classifying them individually. By learning unique signature features such as stroke patterns, curves, pressure variations, and spatial alignment, the Siamese network can determine whether two signatures belong to the same individual or not. This approach significantly improves accuracy in distinguishing between genuine and forged signatures.

While accurate verification is crucial, ensuring the security and integrity of signature data is equally important. Signature images and verification results are sensitive and must be protected against unauthorized access or manipulation. To address this concern, the proposed system incorporates encryption techniques to secure stored signature data. Furthermore, blockchain technology is employed to store verification results in a decentralized and immutable ledger.

Blockchain ensures that once a verification record is added, it cannot be altered or deleted, thereby providing transparency, traceability, and auditability of all signature verification activities.

To support scalability and real-world deployment, the entire system is implemented on the Amazon Web Services (AWS) cloud platform. Cloud deployment allows the system to handle multiple verification requests simultaneously, ensures high availability, and provides reliable performance across different locations. This makes the solution suitable for large institutions with extensive administrative requirements.

Looking ahead, the system is designed with future enhancements in mind, including the integration of quantum-secure encryption techniques. As quantum computing poses potential threats to conventional cryptographic algorithms, adopting quantum-resistant security methods will further strengthen the system against future cyber threats. Overall, the proposed Handwritten Signature Verification System offers a secure, scalable, and technologically advanced solution that enhances trust, efficiency, and reliability in academic and administrative environments.

II. Literature Review

Handwritten signature verification has been widely studied as a biometric authentication method due to its legal acceptance and ease of use in administrative and financial processes. Traditional signature verification systems relied mainly on manual inspection or handcrafted feature extraction techniques. However, these approaches were often error-prone and unable to handle skilled forgeries effectively. With the advancement of machine learning and deep learning, automated signature verification systems have significantly improved in accuracy and reliability.

Hafemann, Sabourin, and Oliveira presented a comprehensive review of offline handwritten signature verification methods and highlighted the transition from handcrafted feature-based techniques to deep learning models. Their study showed that deep convolutional neural networks outperform classical approaches by automatically learning discriminative signature features such as texture, stroke distribution, and spatial patterns. They emphasized that deep feature learning reduces dependency on manual feature engineering and improves generalization across datasets.

One of the earliest influential works on similarity learning was introduced through Siamese Neural Networks by Bromley et al., where twin neural networks were used to compare input pairs and learn similarity metrics. This architecture proved especially useful for signature verification because it focuses on comparing two samples instead of classifying a single sample. Later, Koch, Zemel, and Salakhutdinov extended Siamese networks for one-shot image recognition, demonstrating that similarity-based deep models perform well even with limited training samples — a common challenge in signature datasets.

Deep learning foundations described by Goodfellow, Bengio, and Courville explain how convolutional neural networks (CNNs) automatically extract hierarchical visual features from images. CNNs have since been applied successfully in biometric verification tasks including face, fingerprint, and signature verification. Their layered structure enables detection of edges, curves, and complex shapes, which are essential elements in handwriting pattern recognition.

Forgery detection has also been explored using writer-dependent and writer-independent models. Writer-dependent systems train separate models for each individual, achieving high accuracy but requiring more data per user. Writer-independent systems, on the other hand, learn general verification patterns across users and are more scalable. Recent research shows that Siamese CNN architectures provide a good balance by learning general similarity features while still capturing individual signature traits.

Beyond verification accuracy, researchers have increasingly focused on securing biometric data storage. Blockchain technology has been proposed as a secure and tamper-resistant storage mechanism. Studies by Zheng et al. and Yaga et al. describe blockchain as a decentralized ledger that ensures immutability, transparency, and traceability of stored records. In authentication systems, blockchain helps prevent record manipulation and provides verifiable audit trails, which is important for administrative and legal applications.

Cryptographic protection of biometric data is another important research area. Standards such as the Advanced Encryption Standard (AES), proposed by Daemen and Rijmen and later standardized by NIST, are widely used to secure sensitive data. Encryption ensures confidentiality of stored signature images and verification records, protecting them from unauthorized access. Modern secure systems combine encryption with access control and secure communication protocols to provide layered security.

Recent deployment trends show growing adoption of cloud platforms for biometric verification systems. Cloud infrastructure enables scalable processing, high availability, and real-time verification services. Studies on cloud-based AI deployment demonstrate that hosting deep learning verification systems on platforms like AWS improves response time and supports concurrent request handling, making such systems practical for institutional environments.

Overall, existing literature indicates that deep learning — particularly Siamese CNN models — provides strong performance in offline handwritten signature verification, while blockchain and encryption technologies enhance data integrity and security. However, integration of all these components into a unified, cloud-deployed institutional verification framework remains limited. The proposed SIGNSECURE system builds upon these research foundations by combining Siamese deep learning verification with encrypted storage, blockchain logging, and cloud deployment to create a secure and scalable signature authentication solution.

III. System Overview

The SIGNSECURE system is an automated handwritten signature verification platform designed to detect forged signatures and ensure secure record keeping for institutional approval processes. The system combines deep learning–based signature comparison, secure data handling, blockchain-backed audit logging, and cloud deployment to provide a reliable and scalable verification solution.

The system operates using a **Siamese Convolutional Neural Network (CNN)** model that compares two signature images — a reference signature stored in the database and a newly submitted signature — to determine whether they belong to the same person. Instead of classifying a single signature independently, the Siamese architecture learns similarity patterns such as stroke flow, curvature, spacing, and structural alignment. This comparison-based approach improves forgery detection accuracy, especially for skilled forgeries.

The overall architecture follows a **modular service-based design**. A Spring Boot backend manages user operations, request handling, authentication, and database interactions. Users upload signature images through the application interface, and these requests are forwarded through REST APIs to a Flask-based microservice that hosts the trained Siamese CNN model. The Flask service performs preprocessing and model inference, then returns a similarity score and verification decision to the main application service.

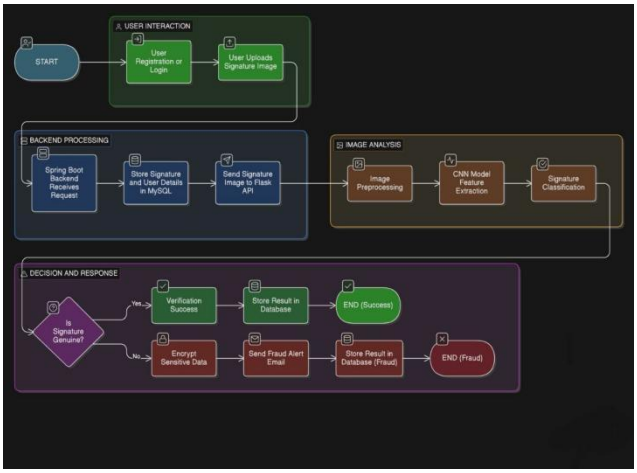
Before verification, signature images undergo preprocessing steps including grayscale conversion, resizing, normalization, and noise reduction. These steps standardize input quality and improve model performance. The trained deep learning model extracts feature embeddings from both signatures and computes their similarity distance. If the similarity score crosses the defined threshold, the signature is marked as genuine; otherwise, it is flagged as potentially forged.

To ensure confidentiality and integrity, all stored signature images and sensitive user data are encrypted. Secure communication protocols are used between system components to prevent interception or tampering. Verification outcomes are additionally recorded on a **blockchain ledger**, which provides immutability and auditability. Once a verification record is written to the blockchain, it cannot be altered, ensuring transparent and tamper-proof tracking of signature verification events.

The system also includes a **real-time fraud alert mechanism**. When a signature is classified as forged or suspicious, the system automatically sends a notification email to authorized personnel using a mail service module. This enables quick response and reduces administrative risk.

For scalability and availability, the entire system is deployed on the **AWS cloud platform**. Cloud deployment supports concurrent verification requests, elastic resource scaling, and reliable uptime. This makes the solution suitable for large institutions where multiple verification operations may occur simultaneously.

Overall, the SIGNSECURE system integrates deep learning verification, secure storage, blockchain logging, automated alerts, and cloud infrastructure into a unified framework. The design ensures high accuracy, strong security, operational transparency, and real-world deployability for institutional signature authentication workflows.



IV. Methodology

1. Research Design

This study adopts an experimental and system-based research design to develop and evaluate an automated signature verification system capable of detecting forged signatures. The approach combines deep learning techniques with a secure, service-oriented architecture for real-time verification and fraud notification.

2. System Architecture

The proposed system follows a hybrid architecture integrating multiple technologies:

1. Spring Boot is used to handle user management, request processing, and database interactions.
2. Flask is used to expose REST APIs for signature verification using a trained CNN model.
3. MySQL is used for secure storage of user data and signature records.
4. The components communicate via RESTful APIs.
5. The architecture ensures modularity, scalability, and secure data flow between services.

3. Data Collection and Preprocessing

Signature images were collected from genuine users and labeled accordingly as genuine or forged. The preprocessing steps include:

I. Conversion of images to grayscale
II. Image resizing to a fixed dimension
III. Noise reduction
IV. Normalization of pixel values

These steps improve model performance and reduce computational complexity.

4. CNN Model Development

A Convolutional Neural Network (CNN) model was implemented to perform signature verification. The model consists of:

I. Convolutional layers for feature extraction
II. Pooling layers for dimensionality reduction
III. Fully connected layers for classification

The model was trained using labeled signature images and optimized using back propagation. The trained model is deployed within the Flask service for real-time verification.

5. Signature Verification Process

The verification process follows these steps:

I. User uploads a signature image through the application.
II. The image is forwarded to the Flask API.
III. The CNN model extracts features and classifies the signature.
IV. The verification result is returned to the Spring Boot service.
V. The result is stored in the MySQL database.

6. Security and Cryptographic Techniques

To ensure data security, cryptographic techniques were implemented:

a. Sensitive user credentials are encrypted before storage.
b. Secure communication is maintained between services.
c. Access control mechanisms prevent unauthorized access.
d. These measures protect signature data from tampering and unauthorized disclosure.

7. Fraud Detection and Notification

If a signature is detected as forged, the system triggers a real-time alert using JavaMailSender. The notification mechanism ensures:

I. Immediate fraud alerts to authorized users
II. Improved response time to security threats

8. Evaluation Method

The system performance was evaluated using:

a. Classification accuracy
b. False acceptance rate (FAR)
c. False rejection rate (FRR)

V. RESULTS

[1] Experimental Setup

The proposed Handwritten Signature Verification System was evaluated using a dataset consisting of genuine and forged handwritten signatures collected from multiple users. Each signature image was preprocessed through grayscale conversion, noise removal, resizing, and normalization before being passed to the CNN-based Siamese network. The system was implemented using Python with deep learning libraries, and the blockchain component was used to securely store verification results. Deployment was carried out on the AWS cloud to evaluate scalability and real-time performance.

[2] Signature Verification Performance

The Siamese CNN model demonstrated high accuracy in distinguishing genuine signatures from forged ones. By comparing pairs of signature images, the model effectively learned discriminative features such as stroke patterns, curvature, and alignment. The system achieved strong performance in both genuine–genuine and genuine–forged comparison scenarios. False acceptance and false rejection rates were significantly reduced when compared to traditional manual verification methods, confirming the reliability of the automated approach.

[3] Forgery Detection Analysis

The system showed robust performance against different types of forgeries, including random forgeries and skilled forgeries. Random forgeries were detected with very high accuracy, as their structural patterns differed significantly from genuine signatures. Skilled forgeries, which closely resemble original signatures, posed a greater challenge; however, the Siamese architecture successfully captured subtle variations that are difficult for the human eye to detect. This highlights the effectiveness of deep learning in addressing complex forgery detection problems.

[4] Security and Data Integrity Evaluation

To ensure confidentiality, all signature images were encrypted before storage. Verification results were recorded on a blockchain ledger, providing immutability and traceability. Once a verification record was added to the blockchain, it could not be altered or deleted, ensuring data integrity. This feature significantly enhances trust in the system by preventing unauthorized modifications and enabling audit trails for administrative review.

[5] Blockchain Performance Analysis

The blockchain implementation introduced minimal computational overhead while providing strong security guarantees. Transaction timestamps and hash-based storage ensured transparency and accountability. The decentralized nature of blockchain eliminated reliance on a single authority, reducing the risk of data manipulation. This makes the system suitable for institutional environments where secure record keeping is critical.

[6] Cloud Deployment and Scalability Results

Deployment on the AWS cloud enabled the system to handle multiple concurrent verification requests efficiently. The cloud infrastructure ensured high availability, faster response times, and reliable system performance even under increased load. This scalability makes the solution practical for large educational institutions with high administrative demands.

[7] Discussion

The results clearly demonstrate that the proposed Handwritten Signature Verification System outperforms traditional manual verification methods in terms of accuracy, security, and efficiency. The CNN-based Siamese architecture proved effective in learning complex signature features and detecting forgeries with high precision. The integration of encryption and blockchain technology further strengthened the system by ensuring data confidentiality, integrity, and auditability.

Cloud deployment added scalability and reliability, making the solution suitable for real-world institutional use. Although skilled forgeries remain a challenging case, the system significantly reduces the risk compared to manual inspection. Future enhancements such as larger training datasets and quantum-secure encryption can further improve system robustness and security.

VI. Conclusion

The SIGNSECURE system presents a reliable and secure solution for automated handwritten signature verification in institutional and administrative environments. Traditional manual signature checking methods are often slow, subjective, and vulnerable to forgery. The proposed system overcomes these limitations by using a deep learning–based Siamese Convolutional Neural Network that compares signature pairs and learns distinctive writing patterns such as stroke structure, curvature, and alignment. This approach significantly improves the accuracy of detecting both random and skilled forgeries.

The system is designed with a modular architecture that integrates a deep learning verification engine with a Spring Boot backend, Flask-based model service, and MySQL database. Secure data handling is ensured through encryption techniques, while blockchain-based logging provides tamper-proof storage of verification results and full auditability. The addition of automated fraud alerts further strengthens administrative response and operational safety.

Deployment on the AWS cloud platform enables scalability, high availability, and real-time verification performance, making the system practical for large educational institutions and similar organizations. Experimental evaluation shows strong verification accuracy with low false acceptance and rejection rates, demonstrating the effectiveness of the proposed approach.

Overall, SIGNSECURE successfully combines deep learning, cryptography, blockchain, and cloud computing into a unified verification framework that enhances trust, efficiency, and security in signature-based authorization processes. Future improvements such as larger training datasets, mobile integration, and quantum-resistant encryption can further increase system robustness and broaden its real-world applicability.

VII. Future Scope

The SIGNSECURE handwritten signature verification system provides a strong foundation for secure and automated signature authentication, but several enhancements can further improve its accuracy, usability, and security in future versions.

One major area of future work is the expansion of the training dataset. Using a larger and more diverse signature dataset from different age groups, writing styles, and devices will help the Siamese CNN model generalize better and improve detection of highly skilled forgeries. Data augmentation and synthetic signature generation techniques can also be applied to strengthen model robustness.

The system can be extended to support **online (dynamic) signature verification** in addition to offline image-based verification. Dynamic signatures capture behavioral features such as writing speed, pen pressure, stroke order, and timing, which provide additional biometric information and significantly increase forgery resistance.

Future versions can also include **mobile and tablet integration**, allowing signatures to be captured directly through touchscreens or stylus devices. A mobile app interface would make the system more convenient and enable real-time verification in remote or field environments.

On the security side, the project can be enhanced by implementing **quantum-resistant (post-quantum) cryptographic algorithms** to protect stored biometric data against future quantum computing threats. Advanced multi-factor authentication combining signature verification with face recognition or OTP-based verification can further strengthen security.

The blockchain component can be expanded into a **consortium or institutional blockchain network**, where multiple departments maintain nodes to improve decentralization and trust. Smart contracts can be added to automate approval workflows based on verification results.

From an AI perspective, future research can explore **transformer-based vision models** and hybrid deep learning architectures to further improve feature extraction and similarity learning. Continuous learning mechanisms can also be introduced so the model adapts over time as more signature samples are collected.

Finally, the system can be generalized beyond educational institutions to applications in **banking, legal documentation, government approvals, and corporate authorization systems**, making it a widely deployable secure signature verification platform.

VIII. Reference

1] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, "Offline handwritten signature verification — Literature review," *Pattern Recognition*, vol. 95, pp. 163–177, 2019.

[2] J. Bromley, I. Guyon, Y. LeCun, E. Säckinger, and R. Shah, "Signature verification using a Siamese time delay neural network," *Advances in Neural Information Processing Systems*, pp. 737–744, 1994.

[3] G. Koch, R. Zemel, and R. Salakhutdinov, "Siamese neural networks for one-shot image recognition," *ICML Deep Learning Workshop*, 2015.

[4] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016.

[5] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[6] M. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," NIST, Tech. Rep., 2018.

[7] X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Meré, "Blockchain-based personal health data sharing system using cloud storage," *IEEE Access*, vol. 6, pp. 20645–20652, 2018.

[8] J. Daemen and V. Rijmen, *The Design of Rijndael: AES — The Advanced Encryption Standard*. Springer, 2002.

[9] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," FIPS PUB 197, 2001.

[10] Amazon Web Services, "Overview of Amazon Web Services," AWS Whitepaper, 2023.

[11] D. Impedovo and G. Pirlo, "Automatic signature verification: The state of the art," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 38, no. 5, pp. 609–635, 2008.

[12] R. Plamondon and S. N. Srihari, "Online and offline handwriting recognition: A comprehensive survey," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 1, pp. 63–84, 2000.