International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 02 | Feb - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

DeepSign – Intelligent Signature Verification and Fraud Detection

Prof.D.S.Katkade
Department of Information Technology,
K. K. Wagh Polytechnic, Nashik.
Tejaswini Dadaji Raundal,
Department of Information Technology,
K. K. Wagh Polytechnic, Nashik.
Nehali Rajaram Bharati,
Department of Information Technology,
K. K. Wagh Polytechnic, Nashik.
Mohini Pandurang Pawar
Department of Information Technology,
K. K. Wagh Polytechnic, Nashik.

Abstract

Signature verification plays a vital role in banking, legal documentation, and digital authentication systems. The increasing number of forgery cases has created a strong demand for automated and intelligent verification mechanisms. This paper presents DeepSign, a hybrid system that combines traditional machine learning and advanced deep learning techniques to accurately distinguish between genuine and forged signatures. Handcrafted features such as HOG, LBP, and GLCM are extracted and classified using SVM and Random Forest. Deep CNN architectures such as ResNet, VGG, and Inception are employed for automatic feature learning. Autoencoders are used for anomaly detection. The hybrid approach improves robustness, scalability, and detection accuracy.

Keywords

Signature Verification, Forgery Detection, Machine Learning, Deep Learning, SVM, Random Forest, CNN, Autoencoder, Fraud Detection.

1. Introduction

Signature verification is one of the most trusted methods for personal identification in financial, legal, and official transactions. Unlike passwords or PINs, signatures are unique to individuals, making them a reliable form of authentication. However, with the rise of forgery and fraud in banking and administrative sectors, detecting fake signatures has become essential to prevent identity theft and financial losses.

Manual verification by experts is time-consuming, subjective, and error-prone. Moreover, genuine signatures of the same person may vary due to writing conditions, while skilled forgers can create imitations that closely resemble the original. This makes fake signature detection a challenging task.

To solve this, the proposed system uses **Machine Learning (ML) and Deep Learning (DL) algorithms**. Handcrafted features like HOG, LBP, and GLCM are extracted for traditional ML models such as SVM and Random Forest, while deep CNN architectures (ResNet, VGG, Inception) automatically learn complex patterns from raw images. A hybrid approach combining both ensures high accuracy, efficiency, and robustness.

The dataset is taken from **Kaggle and GPDS signature datasets**, which provide a large number of genuine and forged samples. The system has practical applications in **banks, government offices, and digital platforms**, where it can automate and strengthen authentication processes.

Thus, **Fake Signature Detection using Machine Learning** offers a secure, intelligent, and scalable solution to combat forgery and ensure trust in identity verification.

2. Problem Statement

Forgery of signatures is a growing security concern in financial institutions, government offices, and digital authentication systems, leading to fraud, financial loss, and identity theft. Manual verification by experts is time-consuming, inconsistent, and prone to human error, especially when dealing with large volumes of documents. The challenge lies in accurately distinguishing between genuine and forged signatures, as even genuine signatures of the same person may vary in style, pressure, or speed, while skilled forgeries can closely mimic original signatures. Therefore, there is a pressing need for an automated, intelligent, and scalable system that can reliably detect forged signatures using advanced machine learning and deep learning algorithms, ensuring higher accuracy, efficiency, and security in real-world applications.

3. Literature Survey

Title: Offline Handwritten Signature Verification using Hidden Markov Models
Authors: Justinoetal.(2000)
This paper proposed the use of Hidden Markov Models (HMMs) for offline handwritten signature verification. The study demonstrated that HMMs could effectively classify simple forgeries but struggled with highly skilled forgeries. The research laid an early foundation for probabilistic modeling in signature verification.

Title: Signature Verification using Handcrafted Features and Support Vector Machines
Authors: Rivardetal.(2013)
This study explored the use of feature extraction techniques like Histogram of Oriented Gradients (HOG) and Local Binary Patterns (LBP), combined with Support Vector Machines (SVM) for classification. The results showed good accuracy on small and medium datasets, proving handcrafted features effective for baseline signature verification.

Title: Learning Features for Offline Signature Verification Using Deep Convolutional Neural Networks
Authors: Hafemannetal.(2017)
The authors introduced Convolutional Neural Networks (CNNs) for signature verification, where the model automatically learned discriminative features from raw signature images. CNNs achieved higher accuracy than traditional handcrafted methods and showed strong adaptability across different datasets.

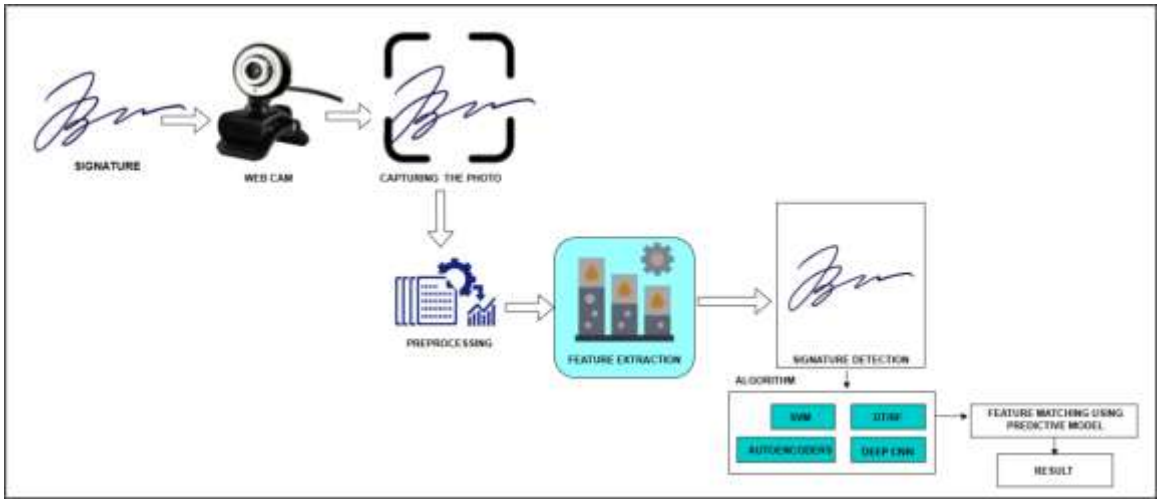
Title: Hybrid Approaches for Signature Verification using Machine Learning and Deep Learning
Authors: Deyeal.(2017)
This paper presented a hybrid system that combined handcrafted feature extraction with deep learning models to improve robustness. The hybrid model balanced computational efficiency with high classification accuracy, making it suitable for real-world scenarios where both performance and interpretability are required.

Title: Offline Signature Verification using Deep CNN Architectures
Authors: Khalajzadehetal.(2018)
This research compared deep CNN architectures such as VGG, ResNet, and Inception for detecting forged signatures.

The study demonstrated that deep CNNs could identify subtle differences between genuine and forged samples, providing high accuracy and scalability for large datasets.

4. Proposed Methodology

The proposed methodology for fake signature detection involves a sequence of steps starting from data collection to final classification. First, the input signature images are preprocessed to enhance quality and remove noise. Next, features are extracted using both handcrafted techniques and deep learning models. These features are then fed into machine learning and deep learning classifiers to distinguish between genuine and forged signatures. Finally, the system outputs the classification result, which can be integrated into a real-time verification application.



5. Applications

1) Banking Sector – For automated verification of signatures on cheques, loan forms, and account-related documents to prevent financial fraud.

2) Legal Institutions – To authenticate signatures on contracts, agreements, and affidavits, reducing disputes and forgery cases.

3) Government Offices – For verifying signatures on official certificates, identity documents, and approvals to ensure authenticity.

4) Educational Institutions – To validate signatures on mark sheets, certificates, and administrative documents, ensuring credibility.

5) Corporate Sector – For employee verification, HR records, and contract approvals to safeguard organizational data and transactions.

6) Forensic Departments – Assisting experts in criminal investigations by providing automated and reliable signature verification tools.

7) Insurance Companies – To detect fraudulent claims by verifying policyholder signatures on claim forms and agreements.

8) E-Governance & Digital Services – For secure online signature verification in e-signatures and digital authentication platforms.

9) Healthcare Sector – To validate signatures on patient consent forms, prescriptions, and medical records, ensuring legal compliance.

10) General Public / Consumers – Providing trust and security in personal financial transactions, property deals, and documentation requiring authentication.

6. Advantages

- High accuracy detection
- Reduced human error
- Fast processing speed
- Robust against skilled forgeries
- Scalable for large datasets
- Hybrid model efficiency
- Improved security and fraud prevention
- Real-time verification capability
- Cost-effective solution
- Adaptable to different signature styles

7. Future Enhancements

In the future, the fake signature detection system can be enhanced in several ways to improve accuracy and usability. Advanced deep learning models like **CNNs with attention mechanisms** or **Siamese networks** can be used for better feature learning. The system can also be extended to support **multi-language or multilingual signatures**, handle **different signature styles and formats**, and detect **partial forgeries**. Real-time verification using **mobile applications** or cloud-based deployment can make the system more accessible. Additionally, integrating **biometric authentication** or **blockchain-based verification** can increase security and reliability for sensitive applications such as banking or legal documents.

8. Conclusion

DeepSign provides an intelligent and scalable framework for signature verification using hybrid machine learning and deep learning techniques. The system enhances security, reduces fraud risk, and ensures reliable authentication for modern digital applications.

9. References

Cherri Ishikawa; Jeff Allen U.Marasigan Cloud-based signature validation using CNN inception-Resnet architecture, IEEE 12th International conference on Humanoid, 2020.

F. Noor, A. E. Mohamed, F. A. Ahmed, and S. K. Taha, □Offline handwritten signa ture recognition using convolutional neural network approach,□ in 2020International Conference on Computing, Networking, Telecommunications & Engineering Sciences Applications (CoNTESA), pp. 51□57, IEEE, 2020.

J. A. Lopes, B. Baptista, N. Lavado, and M. Mendes, □Offline handwritten signature verification using deep neural networks,□ Energies, vol. 15, no. 20, p. 7611, 2022.

J. Poddar, V. Parikh, and S. K. Bharti, □Offline signature recognition and forgery detection using deep learning,□ Procedia Computer Science, vol. 170, pp. 610□617, 2020.

O. Tarek and A. Atia, □Forensic handwritten signature identification using deep learning,□ in 2022 IEEE 9th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), pp. 185□190, IEEE, 2022.

P.William Implementation of Hand Written based Signature Verification Technology using Deep Learning, International conference on intelligent engineering and management,2023 IEEE.

S.Bonde, P. Narwade, and R. Sawant, □Offline signature verification using convo lutional neural network,□ in 2020 6th International Conference on Signal Processing and Communication (ICSC), pp. 119□127, IEEE, 2020.

T. Venkat Narayana Rao, R. Balasubramanian, and K. S. Seshan, Real-Time Handwritten Signature Verification using CNN and Siamese Network, International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), IEEE-2019.

Y. Gupta, S. Kulkarni, and P. Jain, □Handwritten signature verification using trans fer learning and data augmentation,□ in Proceedings of International Conference on Intelligent Cyber-Physical

P. Singh, P. Verma, and N. Singh, □Offline Signature Verification: An Application of GLCM Features in Machine Learning,□□Ann. Data Sci., no. 0123456789, 2021, doi: 10.1007/s40745-021-00343-y.