International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 05 | May - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Digital Signature Verification using Deep Learning.

P. Kamakshi Thai[*1], E.Kavitha[*2],B.Saahith[*3], P.Sanjana[*4]
[1]Assistant Professor of Department of CSE (AI & ML) of ACE Engineering College, India.
[2],[3],[4]Students of Department of CSE (AI & ML) of ACE Engineering College, India.

ABSTRACT

Digital signature verification plays a vital role in bank and finance system security. The research suggests a deep learning approach to identify signatures as authentic by comparing them with an original reference signature. This approach examines the signature to verify its authenticity, deeming it verified if highly similar to the reference, and unverified else. The model suggested utilizes deep learning methods for feature extraction and accuracy enhancement. The aim is to present a secure and effective solution for digital signature verification.

INTRODUCTION

Digital signatures are essential to provide security in banking and financial systems. This work utilizes deep learning to verify signatures automatically by comparing every input with a reference stored to identify authenticity. Deep learning improves the accuracy of verification by extracting important features like shape, style, and stroke pattern. The final aim is to create a secure and trustworthy signature verification system for practical applications.

LITERATURE REVIEW

1. Digital Signature Based on ISRSAC

This article introduces a secure digital signature scheme based on ISRSAC, an improved RSA with a more complicated modulus. It accommodates standard, proxy, and multi-signatures (sequential and broadcasting) and is based on the SM3 hash function. The scheme is more secure than regular RSA and is supported by theoretical proof.

2.Fast Verification of Signatures With Shared ECQV Implicit Certificates

The paper offers two solutions that speed up digital signature verification via shared ECQV implicit certificates in vehicle communications. One approach is based on reusing shared certificate information, and the other on combined public key extraction and batch verification. These solutions minimize computation and offer up to 5× performance gains

3.Investigating the Common Authorship of Signatures by Off-Line Automatic Signature Verification Without the Use of Reference Signatures

The work describes three techniques for checking the common authorship of offline signatures without reference signatures. They involve methods based on similarity score matrices, feature-distance matrices, and complexity-based classification.

With publicly available signature databases, the suggested methods are compared with human assessors and proven to be more effective in determining if a collection of signatures has the same author.

4.EfficientSmall-Batch Verification and Identification Scheme With Invalid Signatures in VANETs

The article suggests a cost-effective small-batch verification and identification scheme for Vehicular Ad Hoc Networks (VANETs) to minimize the delay in identifying and verifying invalid digital signatures. It presents an optimization model that dynamically splits incoming signatures into optimal small-batches according to past error rates. The scheme incorporates exponentiation techniques to quickly identify invalid signatures, which drastically minimizes computational time.

5.A Secure Digital Signature Scheme for Deep Learning-Based Semantic Communication Systems

The paper proposes a secure digital signature scheme for semantic communication systems based on deep learning, integrating semantic features, RF fingerprints, and reconfigurable intelligent surfaces (RIS) to create dynamic keys. This improves message integrity and is resistant to attacks such as replay, tampering, and forgery. Results of experiments indicate robust security: performance with insignificant reduction in system efficiency.

6.A Privacy-Preserving Handwritten Signature Verification Method Using Combinational Features and Secure KNN

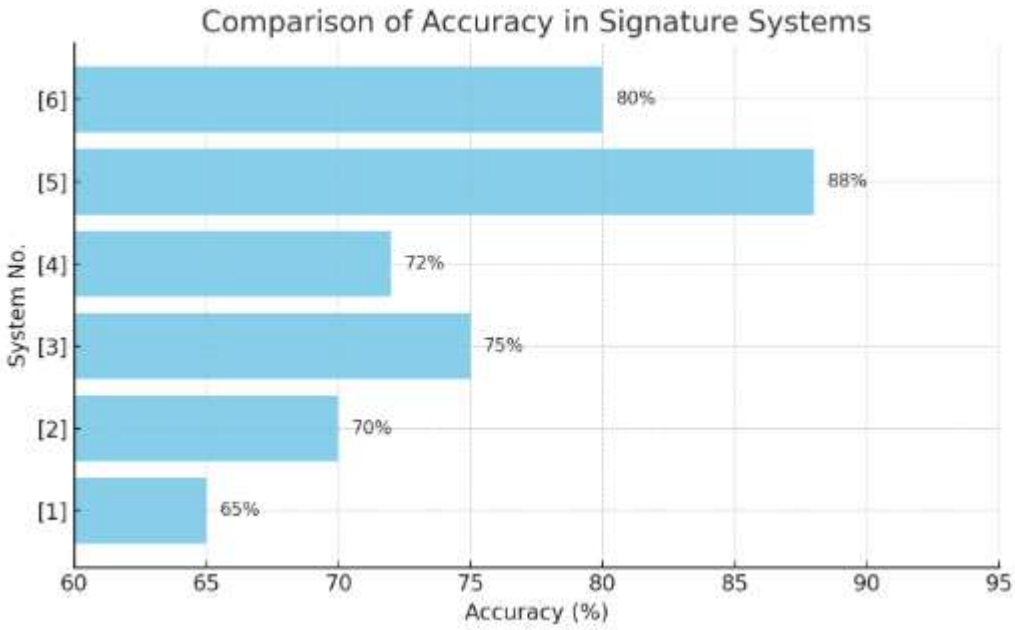
The article introduces a privacy-preserving dynamic handwritten signature verification approach based on combinational global and regional features, which is specifically designed for use on mobile devices. It utilizes secure k-nearest neighbors (KNN) for safeguarding user information in cloud environments without compromising verification accuracy. The approach is tested on SG-NOTE and MCYT-100 databases and yields better performance compared to the current methods.

COMPARISON TABLE

S. NO	Title	Authors	Year	Methodology	Strengths
1.	Digital Signature Based on ISRSAC	Teng Yang1, Yanshuo Zhang2 , Song Xiao1,*, Yimin Zhao1	2021	The article presents a safer version of digital signatures employing an enhanced RSA technique known as ISRSAC.	This new approach is more difficult to crack than standard RSA, and therefore digital signatures are safer.
2.	Fast Verification of Signatures With Shared ECQV Implicit Certificates	Hee-Yong Kwon and Mun-Kyu Lee	2019	The paper suggests two efficient signature verification techniques based on common ECQV implicit certificates to accelerate batch verification in bandwidth-constrained	The suggested techniques minimize signature verification time by up to 5× over conventional methods.

				systems such as vehicular networks.	
3.	Investigating the Common Authorship of Signatures by Off-Line Automatic Signature Verification Without Reference Signatures	Moises Diaz , Member, IEEE, Miguel A. Ferrer , Soodamani Ramalingam , and Richard Gues	2020	Three machine learning techniques verify whether offline signatures are from the same individual without reference samples.	The techniques, particularly with complexity analysis, perform better than human intuition.
4.	Efficient Small-Batch Verification and Identification Scheme With Invalid Signatures in VANETs	Zhenhua Liu, MinYingying Ding, and Baocang Wangg Yuan	2021	The paper employs a clever approach to divide and verify message signatures in small groups to accelerate the process in vehicle networks.	The technique makes checking signatures significantly quicker, reducing delays by a maximum of 50%, and performs effectively even when there are numerous incorrect messages in vehicle networks.
5.	A Secure Digital Signature Scheme for Deep Learning-Based Semantic Communication Systems	ZHIHUA XIA 1, TIANJIAO SHI1, NEAL N. XIONG 2, XINGMING SUN, AND BYEUNGWOO JEON	2022	The article establishes a digital signature system that utilizes AI-derived meaning, device ID, and wireless channel characteristics to authenticate communication.	The system ensures effective security against attacks such as forgery and tampering without compromising on communication speed
6.	A Privacy-Preserving Handwritten Signature Verification Method Using Combinational Features and Secure KNN	Qianlong Sun, Guoshun Nan, Tianyi Li, Huici Wu, Zhou Zhong, Xiaofeng Tao	2018	The article suggests a secure handwritten signature verification technique based on combined global and regional features with privacy protection via secure kNN.	Built a trainable agent with TensorFlow and started reinforcement learning (RL) integration for browser-based applications

Comparison graph:



RESEARCH GAPS

1.Digital Signature Based on ISRSAC

Enhances cryptographic security but does not account for real-world signature variation or employ AI.

2.Fast Verification of Signatures With Shared ECQV Implicit Certificates

Optimized for digital certificates, but not for biometric or handwritten signature verification.

3. Investigating the Common Authorship of Signatures by Off-Line Automatic Signature Verification Without Reference Signatures

Not practically applicable in strict identity systems and does not employ deep learning for feature extraction

4. Efficient Small-Batch Verification and Identification Scheme With Invalid Signatures in VANETs

Targets communication systems, excluding handwritten signatures and deep feature learning.

5.A Secure Digital Signature Scheme for Deep Learning-Based Semantic Communication Systems

Deals with deep learning for semantic messages, inappropriate for image-based signature verification.

6. A Privacy-Preserving Handwritten Signature Verification Method Using Combinational Features and Secure KNN

Relies on handcrafted features and classical techniques; doesn't have an end-to-end deep learning mechanism.

PROPOSED SYSTEM

The method under consideration employs deep learning to authenticate digital signatures by matching them with a reference signature. It processes the signature image and extracts key features using a trained Convolution Neural Network first. The features are then compared with the reference stored to determine authenticity. When the similarity is high, the signature is indicated as verified; otherwise, it is rejected. This method decreases manual labor and improves accuracy. It is particularly valuable in secure settings such as banking and financial institutions.

Conclusion

This work suggests system employs deep learning to verify digital signatures with high accuracy and security. It compares each input signature against a reference stored and establishes authenticity while detecting forgeries. This minimizes human error and accelerates verification. The model picks out key features like shape, stroke, and style to enhance decision-making. It is structured to be solid even on commodity hardware, hence suitable for actual deployment. It solves increasing worries of fraud for banking and finance. It promotes trust in digital transactions. Automated, the procedure becomes scalable and efficient. It helps in safe identity verification. In general, it provides an up-to-date, solid means of signature validation.

REFERENCES

[1] M. Thangavel and P. Varalakshmi**,** "Improved secure RSA cryptosystem for data confidentiality in cloud," *International Journal of Information Systems and Change Management*, vol. 9, no. 4, 2017, pp. 261–277

[2]H.-Y. Kwon and M.-K. Lee, "Fast Verification of Signatures With Shared ECQV Implicit Certificates," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 4680–4694, May 2019.

[3]M. Diaz, M. A. Ferrer, S. Ramalingam, and R. Guest, "Investigating the Common Authorship of Signatures by Off-Line Automatic Signature Verification Without the Use of Reference Signatures," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 487–497, 2020.

[4]Z. Liu, M. Yuan, Y. Ding, and B. Wang, "Efficient Small-Batch Verification and Identification Scheme With Invalid Signatures in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 12, pp. 12836–12846, Dec. 2021.

[5] Q. Sun, G. Nan, T. Li, H. Wu, Z. Zhong, and X. Tao**,** "A Secure Digital Signature Scheme for Deep Learning-Based Semantic Communication Systems," *IEEE Wireless Communications Letters*, 2025.

[6] D. S. Guru, K. S. Manjunatha, S. Manjunath, and M. T. Somashekara, Interval valued symbolic representation of writer dependent features for online signature veri cation, Expert Syst. Appl., vol. 80, pp. 232243, Sep. 2017.