An Explainable Cyber-Forensic Framework for Handwritten Signature Verification Using Behavioural Biometrics, Pressure-Sensitive Acquisition, and Secure Metadata Analysis

Dr. Bhanu Prakash[1], Dr. Sowmya Ramachandrachar[2]
[1]*Msc student, National Forensic Sciences University, Gandhinagar, Gujarat. Corresponding author.*
[2]*Msc student, National Forensic Sciences University, Gandhinagar, Gujarat.*
doi.org/10.64643/IJIRTV12I11-198683-459

***Abstract* — The digitization of handwritten documents has transformed signature forgery into a complex cyber-forensic challenge involving image manipulation, replay attacks, and identity fraud. Conventional verification approaches, including purely visual examination and black-box machine learning models, often lack scalability, transparency, or legal defensibility. This study proposes an explainable cyber-forensic framework that integrates behavioural biometric analysis, pressure-sensitive input devices, and secure document metadata examination for handwritten signature verification. Each decision is explicitly linked to observable forensic features such as writing movement, stroke behaviour, pressure dynamics, and document integrity indicators. By combining explainable cybersecurity techniques with classical forensic document examination principles, the framework enables scalable deployment while preserving interpretability and evidentiary robustness suitable for judicial and regulatory environments.**

Keywords: **Cyber forensics; explainable security; handwritten signature verification; behavioural biometrics; document integrity**

I. INTRODUCTION

Handwritten signatures remain a widely accepted means of authentication in banking, legal, healthcare, and governmental systems. Despite advances in cryptographic authentication, handwritten signatures persist due to long-standing legal recognition and operational convenience. In modern workflows, however, these signatures are routinely digitized, stored, transmitted, and reused, exposing them to cyber-enabled manipulation.

Most cybersecurity mechanisms focus on protecting digital credentials and cryptographic signatures, while handwritten signatures embedded in digital documents receive limited forensic scrutiny. When verification relies solely on visual similarity or automated similarity scores, forged signatures—particularly those created through image reuse or artificial intelligence—may evade detection. This limitation necessitates a framework that is scalable, explainable, and legally defensible, integrating forensic reasoning with cybersecurity controls.

II. SIGNATURES AS EXPLAINABLE BEHAVIOURAL BIOMETRICS

Handwritten signatures constitute behavioural biometric evidence, reflecting neuromuscular coordination, motor memory, and habitual writing patterns. A defining characteristic of behavioural biometrics is natural intra-writer variation; genuine signatures are never identical across executions.

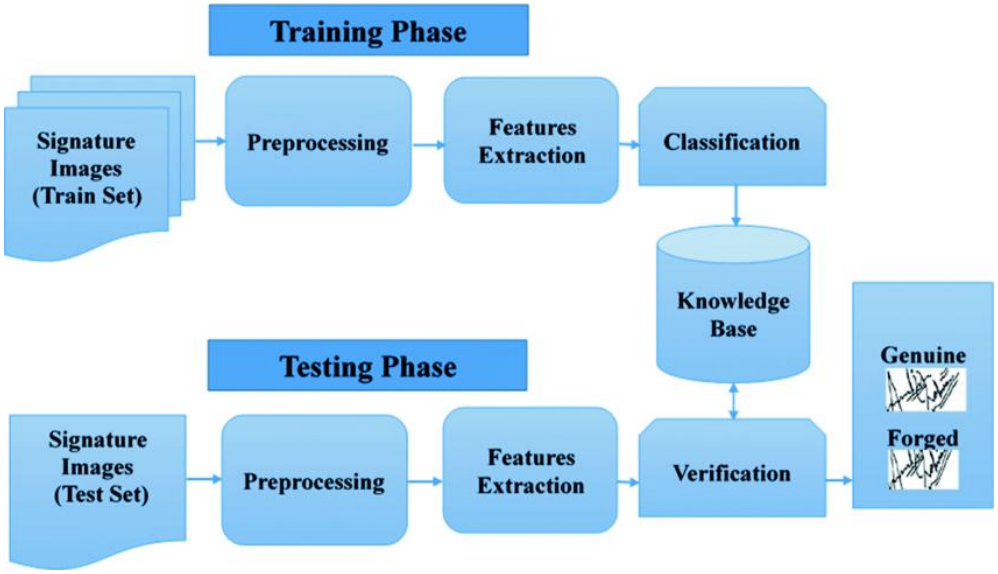
From a cyber-forensic standpoint, this variability is advantageous. Near-exact similarity may indicate replay attacks, tracing, or digital manipulation. Authenticity assessment must therefore prioritize behavioural consistency over superficial resemblance, with explainability remaining central for forensic and judicial acceptance.

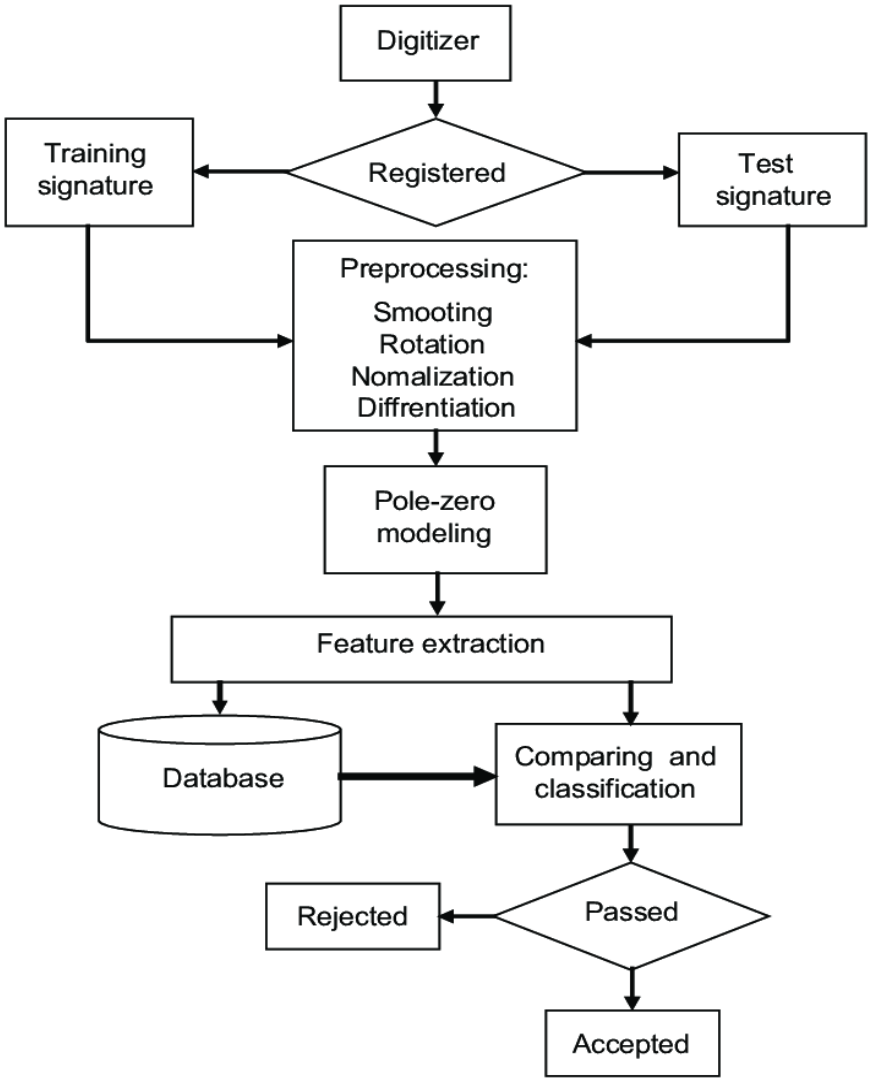
III. CYBER-ENABLED THREAT MODEL

Digitized handwritten signatures are vulnerable to multiple cyber-enabled attacks, including signature harvesting, cut-and-paste forgery, digital enhancement to conceal hesitation, replay of previously signed documents, and AI-assisted simulation. These attacks exploit systems that equate similarity with authenticity while neglecting behavioural and contextual evidence.

IV. INTEGRATED EXPLAINABLE CYBER-FORENSIC FRAMEWORK

The core contribution of this study is an integrated framework combining pressure-sensitive acquisition, behavioural biometric analysis, explainable cybersecurity decision logic, and secure document metadata examination. The overall architecture is illustrated in Figure 1.





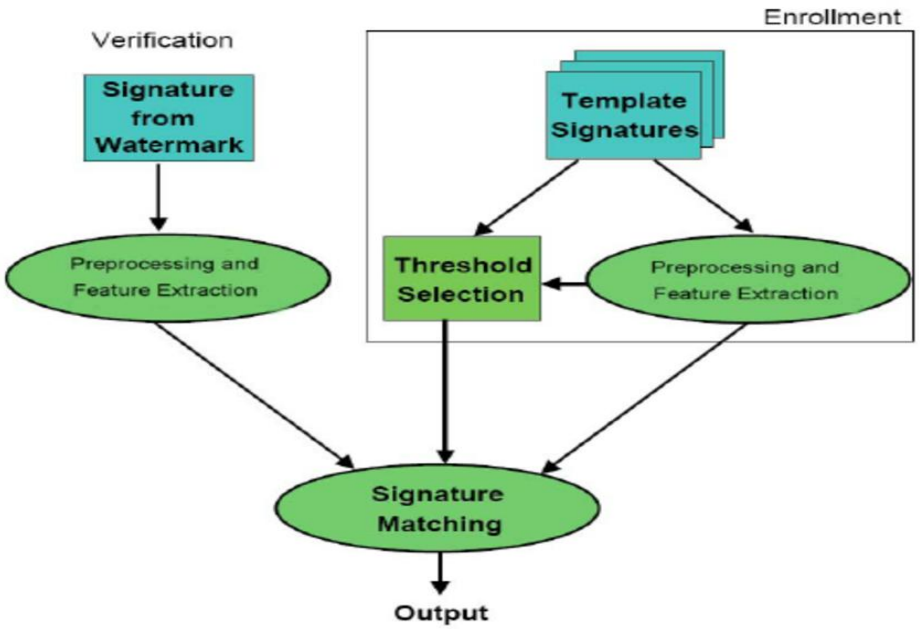


Figure 1. Integrated explainable cyber-forensic architecture for handwritten signature verification.

The architecture illustrates pressure-sensitive signature acquisition, behavioural biometric feature analysis, an explainable cybersecurity decision layer, and secure document metadata analysis, operating within a human-in-the-loop model to ensure interpretability, scalability, and legal robustness.

4.1 Pressure-Sensitive Signature Acquisition

Pressure-sensitive input devices capture dynamic parameters such as writing pressure, speed, acceleration, and stroke timing. These parameters provide high-resolution behavioural biometric data that are difficult to replicate using image-based forgery or replay techniques. Each parameter has direct forensic interpretability, strengthening evidentiary value.

4.2 Behavioural Feature Analysis

Captured data are examined using rule-based forensic criteria, including stroke continuity, writing rhythm, pressure distribution, and consistency of habitual letter formations. Rather than generating opaque similarity scores, the framework documents how each feature contributes to authenticity assessment.

4.3 Explainable Cybersecurity Decision Layer

An explainable decision layer aggregates behavioural observations into a structured forensic rationale. Each outcome—genuine, forged, or inconclusive—is accompanied by a traceable explanation linking specific features to the conclusion.

4.4 Secure Document Metadata Analysis

Secure metadata analysis examines contextual attributes such as creation and modification timestamps, device identifiers, cryptographic hashes, and access logs. Metadata findings serve as corroborative cyber-forensic evidence, supporting behavioural analysis without replacing handwriting examination.

4.5 Integrated Interpretive Outcome

Final conclusions are derived from cumulative evaluation of behavioural biometrics, pressure dynamics, and metadata integrity. Decisions are evidence-weighted, ensuring forensic rigor and legal defensibility.

V. DISCUSSION

The proposed framework balances scalability with interpretability by combining automated preprocessing and expert-guided evaluation. Unlike black-box systems, it enables transparent reasoning suitable for cybersecurity audits, forensic investigations, and judicial proceedings. The human-in-the-loop model reduces false acceptance rates and improves resistance to replay and AI-generated forgeries.

VI. APPLICATIONS

The framework is applicable in banking (cheque and loan fraud detection), e-governance (verification of

affidavits and property records), and healthcare and insurance (authentication of consent and medico-legal documents). In each domain, explainability enhances trust and regulatory compliance.

VII. LIMITATIONS AND FUTURE SCOPE

The framework requires specialized acquisition devices and expert oversight. Future work may focus on standardized deployment, secure integration with document management systems, and harmonization with explainable artificial intelligence models to further enhance scalability.

VIII. CONCLUSION

This study presents an explainable cyber-forensic framework that positions handwritten signature verification at the intersection of behavioural biometrics and cybersecurity. By integrating pressure-sensitive input devices, transparent decision logic, and secure document metadata analysis, the framework addresses modern cyber-enabled forgery threats while preserving interpretability and legal robustness. The approach provides a scalable and trustworthy solution for authenticating handwritten signatures in digital environments.

REFERENCES

[1] Huber RA, Headrick AM. *Handwriting identification: facts and fundamentals*. Boca Raton (FL): CRC Press; 1999.

[2] Ellen D. *The scientific examination of documents: methods and techniques*. 2nd ed. Boca Raton (FL): CRC Press; 2005.

[3] Hilton O. *Scientific examination of questioned documents*. New York (NY): Elsevier; 1982.

[4] Found B, Rogers D. The probative character of forensic handwriting examination. *Forensic Sci Int*. 2008;175(2–3):137–143.

[5] Srihari SN, Cha SH, Arora H, Lee S. Individuality of handwriting. *J Forensic Sci*. 2002;47(4):856–872.

[6] Kam M, Fielding G, Conn R. Writer identification by professional document examiners. *J Forensic Sci*. 1997;42(5):778–786.

[7] Jain AK, Ross A, Prabhakar S. An introduction to biometric recognition. *IEEE Trans Circuits Syst Video Technol*. 2004;14(1):4–20.

[8] Plamondon R, Srihari SN. Online and offline handwriting recognition: a comprehensive survey. *IEEE Trans Pattern Anal Mach Intell*. 2000;22(1):63–84.

[9] Casey E. *Digital evidence and computer crime*. 3rd ed. London (UK): Academic Press; 2011.

[10] Diaz M, Ferrer M, Morales A. Offline signature verification using convolutional neural networks. *Appl Sci*. 2020;10(11):3716.

[11] Hafemann LG, Oliveira LS, Sabourin R. Offline handwritten signature verification—literature review. *IEEE Trans Pattern Anal Mach Intell*. 2020;42(3):1–21.

[12] Tolosana R, Vera-Rodriguez R, Fierrez J, Morales A, Ortega-Garcia J. Deep learning for handwritten signature verification: a survey. *IEEE Access*. 2021;9:1–25.