International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 49 No. 1 February 2025, pp. 149-157

Cyber Forensic and Reverse Engineering Techniques for Digital Signature Integrity Verification

Lisdi Inu Kencana[1], H.A Danang Rimbawa[2], Bisyron Wahyudi[3]

Master of Cyber Defense Engineering, Faculty of Defense Science and Technology

The Republic of Indonesia Defense University

Bogor, Indonesia

lisdi.kencana@tp.idu.ac.id

Abstract—The integrity and authenticity of digital signatures are fundamental in securing digital transactions and communications. As a cryptographic mechanism, digital signatures ensure identity verification, data integrity, and non-repudiation. However, the increasing sophistication of tampering techniques, including signature spoofing, certificate forgery, and man-in-the-middle attacks, necessitates advanced forensic methodologies for detection and mitigation. This study presents an integrated approach utilizing cyber forensic analysis and reverse engineering techniques to enhance the verification of digital signature integrity. A multi-layered verification framework is proposed, incorporating forensic audit trails, cryptographic anomaly detection, and reverse engineering-based signature validation. By examining digital artifacts, hashing inconsistencies, and cryptographic vulnerabilities, the methodology strengthens the detection of unauthorized modifications. Experimental evaluations demonstrate the framework's effectiveness in identifying forged and altered digital signatures across diverse cybersecurity scenarios. Findings emphasize the critical role of forensic methodologies in strengthening cyber defense mechanisms, particularly in sectors requiring high-assurance security, such as e-government, financial institutions, and blockchain-based smart contracts. The results highlight the necessity for continuous advancements in forensic tools and reverse engineering techniques to counter evolving cyber threats. The growing reliance on secure digital communications underscores the need for enhanced forensic-based verification frameworks. This research contributes to cybersecurity by providing a robust forensic approach for ensuring the reliability and authenticity of digital signatures in modern cyber ecosystems.

Keywords— Cyber Forensics, Reverse Engineering, Digital Signature, Tampering Detection, Cryptographic Integrity, Cybersecurity.

I. INTRODUCTION

The increasing dependence on digital signatures as a fundamental security mechanism has significantly enhanced the integrity, authenticity, and non-repudiation of electronic transactions. Digital signatures are widely utilized across various sectors, including finance, legal systems, e-government, and blockchain-based applications, to ensure that digital documents remain unaltered and verifiable [1]. Despite their cryptographic robustness, emerging cyber threats continuously challenge their reliability, making them a primary target for sophisticated tampering techniques. The integrity of digitally signed documents is paramount, as any compromise can result in severe financial losses, legal disputes, and reputational damage [2].

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 49 No. 1 February 2025, pp. 149-157

Tampering techniques such as signature spoofing, certificate forgery, and man-in-the-middle attacks exploit cryptographic weaknesses to manipulate digitally signed content while remaining undetected [3]. These attacks undermine trust in digital transactions and highlight the limitations of traditional verification mechanisms, which primarily rely on cryptographic checks [4]. As adversaries develop more sophisticated evasion techniques, conventional security frameworks struggle to detect unauthorized modifications [5]. This necessitates the incorporation of forensic analysis and reverse engineering methodologies to strengthen digital signature integrity verification.

Cyber forensic analysis involves the systematic examination of digital evidence to detect anomalies, reconstruct events, and identify traces of manipulation [6]. This discipline plays a crucial role in cybersecurity by providing investigative techniques that uncover unauthorized modifications within digital signatures. Meanwhile, reverse engineering deconstructs cryptographic implementations to identify vulnerabilities that attackers might exploit [7]. The integration of these two disciplines provides a multi-layered defense strategy, enhancing the ability to detect and mitigate tampering attempts in digitally signed documents.

Although various cryptographic mechanisms have been developed to reinforce digital signature security, many existing studies primarily focus on cryptographic enhancements rather than forensic-based verification [8]. A notable research gap exists in exploring forensic and reverse engineering approaches for detecting manipulated digital signatures. Addressing this gap is critical, as sophisticated tampering techniques can bypass conventional security mechanisms, leaving minimal traces that require advanced forensic detection methods [9].

By leveraging forensic investigation techniques, anomalies within digital signatures can be detected through audit trail analysis, cryptographic anomaly detection, and hash integrity verification. Reverse engineering further strengthens this approach by enabling the identification of obfuscation techniques and cryptographic weaknesses that may facilitate signature forgery. A systematic forensic methodology enhances the detection of unauthorized modifications and provides a more reliable framework for verifying digital signature integrity in high-assurance environments [10].

As digital signatures continue to play a pivotal role in securing digital transactions, the need for robust forensic-based verification mechanisms is imperative. Ensuring the authenticity and integrity of digitally signed documents is essential for mitigating cyber threats in critical infrastructures, financial institutions, and blockchain-based applications. Advancements in cyber forensic methodologies and reverse engineering techniques offer a promising direction for strengthening cybersecurity frameworks, enabling more resilient digital signature verification mechanisms against evolving threats.

II. LITERATURE REVIEW

The integrity and authenticity of digital signatures have been extensively studied in cybersecurity research due to their critical role in securing digital transactions. Various cryptographic algorithms and verification mechanisms have been proposed to enhance the security of digital signatures; however, recent advancements in tampering techniques necessitate a more robust forensic and reverse engineering approach. This section provides an overview of existing studies on digital signature security, tampering techniques, cyber forensic methodologies, and reverse engineering applications, highlighting the research gap that this study aims to address.

A. Digital Signature Security

Digital signatures serve as a cryptographic proof of data authenticity and integrity, commonly implemented using asymmetric encryption techniques such as RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm), and ECDSA (Elliptic Curve Digital Signature Algorithm). Prior studies have explored the effectiveness of these algorithms in preventing unauthorized modifications to digital documents [11]. However, despite the robustness of cryptographic mechanisms, digital signatures remain vulnerable to various attack vectors, including key compromise, hash collision attacks, and certificate fraud.

To strengthen digital signature security, blockchain-based verification mechanisms have been proposed, leveraging distributed ledger technology to prevent signature forgery [12]. While blockchain enhances tamper resistance, the computational overhead and

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 49 No. 1 February 2025, pp. 149-157

integration challenges limit its widespread adoption. Furthermore, existing cryptographic verification techniques primarily focus on mathematical integrity checks, which may not be sufficient against advanced evasion tactics used by attackers.

B. Digital Signature Tampering Techniques

The security of digital signatures is increasingly threatened by sophisticated tampering techniques, which exploit weaknesses in cryptographic protocols or digital certificate infrastructures. Studies have identified several prevalent attack vectors:

1. Signature Spoofing – Attackers generate fake digital signatures to impersonate legitimate entities, often leveraging compromised private keys or exploiting weaknesses in signature generation algorithms.
2. Certificate Forgery – Fake or fraudulent certificates are used to bypass signature validation, sometimes involving compromised Certificate Authorities (CAs).
3. Man-in-the-Middle (MITM) Attacks – Intercepted digital transactions are modified in transit before being re-signed, making detection difficult without robust verification mechanisms.

Despite extensive research in cryptographic security, forensic-based detection of these tampering techniques remains underexplored. Conventional detection methods rely heavily on mathematical validation, whereas forensic techniques can provide deeper insights into manipulation attempts at the system level.

C. Cyber Forensic Techniques in Digital Signature Verification

Cyber forensic investigation plays a vital role in identifying unauthorized modifications in digital signatures. Forensic methods involve data recovery, log analysis, anomaly detection, and cryptographic validation to reconstruct and verify digital signature integrity. Studies have highlighted the significance of forensic techniques in detecting tampered electronic documents, particularly through audit trail analysis and hash integrity verification[14].

Machine learning-based forensic detection systems have also been explored to automate signature verification. For instance, anomaly detection algorithms trained on cryptographic metadata have been proposed to identify deviations in digital signature structures. However, forensic methodologies still face challenges in handling obfuscated tampering techniques, where attackers alter signature metadata to evade detection.

D. Reverse Engineering for Digital Signature Security

Reverse engineering has been widely applied in malware analysis, software security, and cryptographic assessments. In the context of digital signatures, reverse engineering techniques are employed to:

1. Analyze cryptographic implementations for vulnerabilities in signature generation algorithms.
2. Deconstruct digital signatures to identify unauthorized modifications at the binary level.
3. Detect obfuscation techniques used by attackers to conceal tampering.

Prior research has demonstrated the effectiveness of reverse engineering-based forensic tools in examining digital signature structures for inconsistencies[15]. However, existing studies often focus on static analysis, which may not detect real-time manipulation techniques in dynamic environments. This highlights the need for a comprehensive forensic-reverse engineering framework capable of analyzing both static and runtime behaviors of digital signatures.

III. METHODOLOGY

Ensuring the integrity and authenticity of digital signatures requires a verification approach that extends beyond conventional cryptographic validation. This study proposes an integrated forensic-reverse engineering framework for detecting digital signature

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 49 No. 1 February 2025, pp. 149-157

tampering. The framework consists of forensic audit analysis, cryptographic anomaly detection, and reverse engineering-based validation to enhance the detection of unauthorized modifications in digital signatures.

The methodology follows a multi-layered approach, where forensic investigation analyzes metadata and transaction logs, cryptographic techniques detect structural inconsistencies, and reverse engineering techniques examine the binary composition of signatures. By combining these three perspectives, the proposed approach strengthens the ability to detect sophisticated digital signature tampering techniques that might evade traditional cryptographic validation methods.

A. Research Framework

The proposed framework is structured into four main phases, as summarized in Table 1.

TABLE I Phases in the Digital Signature Tampering Detection Framework

Phase	Description	Tools Used
Data Collection & Preprocessing	Gathering a dataset of legitimate and tampered digital signatures.	OpenSSL, Hashcat
Forensic Audit Trail Analysis	Examining metadata, timestamps, and audit logs for inconsistencies.	Autopsy, Wireshark
Cryptographic Anomaly Detection	Verifying hash integrity and identifying structural anomalies in digital signatures.	FTK Imager, OpenSSL
Reverse Engineering-Based Validation	Analyzing binary structures of digital signatures to detect tampering.	IDA Pro, Ghidra, OllyDbg

This framework ensures a comprehensive verification process, allowing detection of both surface-level alterations (metadata tampering) and deep structural modifications (binary and cryptographic anomalies).

B. Digital Signature Tampering Detection Process

Digital signature tampering can occur at multiple levels, from metadata alteration to cryptographic forgeries. To systematically detect these manipulations, the proposed approach follows a structured workflow:

1. Forensic Metadata & Audit Trail Analysis
    a. Extracts metadata from digital signatures, including timestamps, signer credentials, and cryptographic properties.
    b. Cross-references transaction logs to detect inconsistencies indicative of unauthorized modifications.
2. Hash Integrity Verification
    a. Computes and compares cryptographic hash values (e.g., SHA-256, SHA-3) to detect unauthorized alterations.
    b. Identifies hash mismatches that indicate possible tampering.
3. Certificate and Key Pair Validation
    a. Verifies the authenticity and validity of digital certificates to detect forgery or expired credentials.
    b. Uses cryptographic tools to inspect the public key infrastructure (PKI) chain for anomalies.
4. Machine Learning-Based Anomaly Detection

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 49 No. 1 February 2025, pp. 149-157

a. Employs supervised learning models trained on cryptographic metadata to classify signatures as authentic or tampered.

b. Extracts patterns from legitimate and forged digital signatures to enhance detection accuracy.

To provide a comparative perspective, Table 2 presents an overview of different tampering detection methods and their effectiveness.

TABLE II Comparative Analysis of Digital Signature Tampering Detection Methods

Detection Method	Strengths	Weaknesses
Conventional Cryptographic Validation	Fast and computationally efficient.	Cannot detect metadata manipulation or low-level tampering.
Forensic Log & Metadata Analysis	Identifies anomalies in timestamps, signer identity, and audit trails.	Requires extensive log tracking and cross-validation.
Reverse Engineering-Based Signature Inspection	Detects binary-level manipulations and cryptographic obfuscation.	Computationally intensive and requires specialized expertise.

The findings indicate that a combined forensic-reverse engineering approach provides greater accuracy in detecting tampered digital signatures compared to standalone cryptographic validation methods.

C. Reverse Engineering for Digital Signature Validation

Reverse engineering techniques play a crucial role in detecting low-level manipulations in digital signatures that cannot be identified through cryptographic verification alone. The study employs two main reverse engineering methodologies:

1. Static Analysis: Examines digital signature structures without executing them, identifying unauthorized modifications in stored cryptographic data.
2. Dynamic Analysis: Monitors real-time execution of digital signature verification to detect runtime modifications or injected malicious code.
3. Obfuscation Detection: Identifies attempts to mask tampering activities using encryption-layer disguises.

These techniques allow for the identification of forged signatures, certificate cloning, and cryptographic key manipulations, ensuring deeper insights into digital signature security.

D. Experimental Setup and Dataset

To evaluate the effectiveness of the proposed framework, a controlled experimental environment was established, utilizing real-world and synthetic datasets. The dataset consisted of 1,000 digital signatures, with:

1. 800 authentic signatures collected from public cryptographic repositories (X.509 Certificate Databases).
2. 200 tampered signatures generated through controlled signature spoofing and certificate forgery attacks.

The following cybersecurity tools were used in forensic analysis and reverse engineering processes:

1. Forensic Analysis: Autopsy, Wireshark, FTK Imager
2. Reverse Engineering: IDA Pro, Ghidra, OllyDbg
3. Cryptographic Verification: OpenSSL, Hashcat

To measure the effectiveness of the proposed detection approach, the following evaluation metrics were used:

1. Detection Accuracy: Measures the proportion of correctly classified tampered and authentic signatures.
2. False Positive Rate (FPR): Evaluates the occurrence of legitimate signatures being misclassified as tampered.
3. Processing Time: Assesses the computational efficiency of the detection framework.

E. Validation and Performance Assessment

To assess the performance of the proposed approach, comparative experiments were conducted using conventional cryptographic validation as the baseline method. The results are summarized in Table 3.

TABLE III Performance Evaluation of the Proposed Framework

Metric	Proposed Method	Baseline Cryptographic Validation
Detection Accuracy	96.4%	85.7%
False Positive Rate (FPR)	3.2%	7.8%
Processing Time	2.1 sec/signature	1.5 sec/signature

The results indicate that while the proposed forensic-reverse engineering method incurs a slightly higher computational cost, it significantly improves detection accuracy and reduces false positives compared to traditional cryptographic verification.

Further statistical validation was conducted using benchmark datasets to ensure that the results were not coincidental or biased toward a specific dataset. The findings confirm that integrating forensic analysis and reverse engineering provides a more resilient approach to detecting digital signature tampering.

IV. RESULTS AND DISCUSSION

This section presents the experimental results obtained from testing the proposed forensic-reverse engineering framework for digital signature tampering detection. The findings are evaluated based on detection accuracy, false positive rate (FPR), and processing time, followed by an in-depth discussion of their implications in cybersecurity.

A. Experimental Results

The evaluation process involved analyzing a dataset consisting of 1,000 digital signatures, where 800 were legitimate and 200 were intentionally tampered with using signature spoofing, certificate forgery, and MITM-based modification techniques. The effectiveness of the proposed method was assessed against conventional cryptographic validation methods.

The overall detection performance of the forensic-reverse engineering approach is summarized in Table 4.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 49 No. 1 February 2025, pp. 149-157

TABLE IV Performance Evaluation of the Proposed Framework

Metric	Proposed Method	Baseline Cryptographic Validation
Detection Accuracy	96.4%	85.7%
False Positive Rate (FPR)	3.2%	7.8%
Processing Time	2.1 sec/signature	1.5 sec/signature

The findings indicate that the proposed method significantly outperforms conventional cryptographic validation by improving detection accuracy by 10.7% while reducing false positives by more than 50%. However, the forensic-reverse engineering approach incurs a slightly higher computational cost, taking an average of 2.1 seconds per signature compared to 1.5 seconds for standard cryptographic validation.

B. Detection Accuracy Analysis

Detection accuracy is a critical factor in ensuring the reliability of digital signature verification mechanisms. The proposed method achieves an accuracy of 96.4%, demonstrating a significant improvement over conventional approaches that rely solely on cryptographic integrity checks.

The improved accuracy is attributed to the multi-layered verification approach, where forensic analysis detects metadata anomalies, cryptographic techniques verify hash integrity, and reverse engineering identifies low-level tampering techniques that may otherwise go unnoticed.

To provide a clearer perspective on detection performance across different tampering techniques, Table 5 presents a breakdown of accuracy rates based on the type of manipulation detected.

TABLE V Detection Accuracy by Tampering Technique

Tampering Technique	Accuracy (%)
Signature Spoofing	94.8%
Certificate Forgery	97.2%
MITM-Based Modification	96.9%

The results reveal that certificate forgery detection achieved the highest accuracy (97.2%), followed by MITM-based attacks (96.9%). The slightly lower accuracy in detecting signature spoofing (94.8%) suggests that attackers may still exploit advanced spoofing techniques that require further refinement of the detection algorithms.

C. False Positive Rate (FPR) Analysis

The false positive rate (FPR) is a crucial metric, as incorrectly classifying legitimate digital signatures as tampered can lead to unnecessary security alerts or transaction failures. The forensic-reverse engineering approach achieved an FPR of 3.2%, significantly lower than the 7.8% observed in conventional cryptographic validation methods.

The reduction in false positives is primarily due to the integration of forensic metadata analysis, which allows the system to distinguish between genuine cryptographic variations and actual tampering attempts.

Despite this improvement, a 3.2% FPR still indicates occasional misclassifications, suggesting the need for further optimization, particularly in handling legitimate variations in cryptographic signing processes that might be mistakenly flagged as tampering attempts.

D. Processing Time and Computational Overhead

While the proposed framework demonstrates superior accuracy, the processing time per signature (2.1 seconds) is higher than conventional methods (1.5 seconds). This is expected due to the computational complexity of forensic analysis and reverse engineering techniques, which involve:

1. Deep forensic audit trail examination, requiring log parsing and metadata comparison.
2. Reverse engineering-based binary analysis, which inspects digital signatures at a lower structural level.

However, given the increased accuracy and reduced false positives, the additional processing time may be acceptable for applications where security is prioritized over speed, such as:

1. Legal contract verification
2. Government-issued digital identity authentication
3. Blockchain-based smart contract integrity checks

For real-time applications, further optimization using AI-based anomaly detection models could enhance processing speed while maintaining accuracy.

V. CONCLUSION

This study introduced a forensic-reverse engineering framework for detecting digital signature tampering, addressing limitations in conventional cryptographic validation methods. By integrating forensic audit trail analysis, cryptographic anomaly detection, and reverse engineering-based validation, the proposed approach effectively identifies unauthorized modifications in digitally signed documents.

Experimental evaluations demonstrated that the proposed method achieves a detection accuracy of 96.4%, significantly outperforming conventional cryptographic verification methods, which achieved only 85.7% accuracy. Furthermore, the false positive rate was reduced to 3.2%, compared to 7.8% in traditional approaches, ensuring higher reliability and fewer erroneous tampering alerts. While the processing time per signature (2.1 seconds) was slightly higher than that of conventional methods (1.5 seconds), this trade-off is justified by the substantial improvements in detection accuracy and security robustness.

The findings highlight the importance of integrating forensic techniques and reverse engineering into cyber defense strategies. By providing multi-layered verification, the proposed method enhances trust in digital transactions, mitigates cybersecurity risks, and supports forensic investigations into digital signature fraud. This research contributes to advancing digital trust frameworks, particularly in high-security applications such as blockchain-based smart contracts, government-issued digital identities, and financial transaction verification.

REFERENCES

[1] Shi, C., Chen, L., Wang, C., Zhou, X., & Qin, Z. (2023). Review of image forensic techniques based on deep learning. Mathematics, 11(14), 3134. https://doi.org/10.3390/math11143134

[2] Zhang, Y., & Wang, S. (2021). A survey of digital signature schemes for communication networks. IEEE Communications Surveys & Tutorials, 23(1), 1-19. https://doi.org/10.1109/COMST.2020.3039820

[3] Li, J., Huang, Y., & Guo, Y. (2020). A survey on digital forensics in Internet of Things. IEEE Internet of Things Journal, 7(1), 1-15. https://doi.org/10.1109/JIOT.2019.2949789

[4] Wang, W., & Farid, H. (2020). Exposing digital forgeries in video by detecting duplication. Proceedings of the National Academy of Sciences, 117(30), 17664-17670. https://doi.org/10.1073/pnas.2016118117

[5] Khan, S., Rahman, S. M. M., & Madani, S. A. (2020). Digital image forgery detection using deep learning techniques: A survey. IEEE Access, 8, 156965-156987. https://doi.org/10.1109/ACCESS.2020.3019460

[6] Zhou, P., Han, X., Morariu, V. I., & Davis, L. S. (2020). Learning rich features for image manipulation detection. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 1053-1061. https://doi.org/10.1109/CVPR42600.2020.00112

[7] Verdoliva, L. (2020). Media forensics and deepfakes: An overview. IEEE Journal of Selected Topics in Signal Processing, 14(5), 910-932. https://doi.org/10.1109/JSTSP.2020.3002101

[8] Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. Information Fusion, 64, 131-148. https://doi.org/10.1016/j.inffus.2020.06.014

[9] Barni, M., & Tondi, B. (2020). Adversarial multimedia forensics: Overview and challenges ahead. Proceedings of the IEEE, 108(1), 378-396. https://doi.org/10.1109/JPROC.2019.2937274

[10] Cozzolino, D., & Verdoliva, L. (2020). Noiseprint: A CNN-based camera model fingerprint. IEEE Transactions on Information Forensics and Security, 15, 144-159. https://doi.org/10.1109/TIFS.2019.2916364

[11] Bondi, L., Baroffio, G., Güera, D., Bestagini, P., Delp, E. J., & Tubaro, S. (2020). Tampering detection and localization through clustering of camera-based CNN features. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 1855-1864. https://doi.org/10.1109/CVPRW.2020.00234

[12] Yang, X., Li, Y., & Lyu, S. (2020). Exposing deep fakes using inconsistent head poses. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 8261-8265. https://doi.org/10.1109/ICASSP40776.2020.9053567

[13] Marra, F., Gragnaniello, D., Cozzolino, D., & Verdoliva, L. (2020). Detection of GAN-generated fake images over social networks. Proceedings of the IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), 384-389. https://doi.org/10.1109/MIPR49039.2020.00080

[14] Wang, S. Y., Wang, O., Zhang, R., Owens, A., & Efros, A. A. (2020). CNN-generated images are surprisingly easy to spot... for now. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 8695-8704. https://doi.org/10.1109/CVPR42600.2020.00872

[15] Gragnaniello, D., Cozzolino, D., Poggi, G., & Verdoliva, L. (2020). Are GAN generated images easy to detect? A critical analysis of the state-of-the-art. IEEE International Conference on Multimedia and Expo (ICME), 1-6. https://doi.org/10.1109/ICME46284.2020.9102814