IJSSR
International Journal of Social Service and Research

Vol. 6, No. 4, April 2026
e-ISSN: 2807-8691 | *p*-ISSN: 2807-839X

A Hybrid Cryptographic and Biometric Framework for Real-Time Signer Verification in Digital Signing Systems

Farah Yulianti
President University, Indonesia
Email: farah.yulianti@president.ac.id

ABSTRACT

Digital document signing systems are widely adopted to support legally binding electronic transactions by ensuring practicality, integrity, authenticity, and non-repudiation in electronic workflows. Current digital signing platforms rely on public key Infrastructure (PKI) combined with secondary verification mechanisms such as one-time password (OTP) delivered via email, SMS, or messaging applications to strengthen signer authentication. While OTP mechanisms provides additional account level security, they primarily verify control over a communication channel and do not guarantee the individual performing the signing action is physically present or intentional participation of the signer at the time of document execution. This limitation creates potential vulnerabilities in cases of communication channel compromise. This paper investigated the security limitations of OTP based signer verification in digital signing environments and proposes a hybrid framework that integrates cryptographic signatures, OTP verification, and gesture-based facial liveness detection. The objective is to bind the signing action to real-time human presence while preserving the integrity guarantees of PKI. The results indicate that while OTP only verification maintains high usability, it is vulnerable under simulated channel-compromise conditions. Biometric liveness detection reduces presentation attack success, and the hybrid configuration demonstrates improved resistance to unauthorized signing compared with OTP only verification. These findings suggest that integrating lightweight biometric liveness detection into digital signing workflows can enhance identity assurance without replacing existing PKI infrastructure. This paper contributes to the discussion on strengthening signer legitimacy in electronic document execution through multi-layer identity verification.

Keywords: Digital document signing; Public Key Infrastructure (PKI); One-Time Password (OTP)

INTRODUCTION

Digital signatures play a critical role in modern electronic transactions by enabling legally binding agreements without requiring physical presences. Through cryptographic mechanisms such as hashing algorithms and public key infrastructure (PKI). Digital signatures ensure the integrity, authenticity, and non-repudiation of electronic documents (Maulana et al., 2025; Zhao, 2023; Zou et al., 2025). These mechanisms prevent unauthorized modification after signing and allow the identity of the signer to be reliably verified. As a result, digital signatures are fundamental to legal, financial, and governmental processes (Hassan & Alqahtani, 2025; Tullis, 2024; Tullis et al., 2024), where they enhance security, promote trust, and support widespread adoption of secure digital communication and electronic workflows (Singh & Kumar, 2025).

In practice however, digital signing systems must also address the challenge of reliably authenticating the signer. Most mainstream digital signing platforms implement a two-stage verification model (Bartłomiejczyk, 2024; Sharma, 2023; Subagja, 2025). First, the document is cryptographically signed using a private key associated with the signer's account, ensuring integrity and non-repudiation. Second, the signer's identity is verified using out-of-band

authentication mechanisms such as one-time passwords (OTP) sent via email, SMS, or messaging services. This approach is widely adopted due to its low implementation cost, ease of deployment, and user familiarity (Jarecki et al., 2021; Reynolds et al., 2020).

Despite the widespread use, OTP based mechanisms primarily verify control over an account, rather than the physical presence or intentional presence of the human signer. If an attacker gains access to user's email account, phone number, or messaging applications, a situation that has disproportionately affected vulnerable groups such as older adults and individuals with lower level of formal education in certain regions observed, the attacker may successfully complete OTP verification without being the legitimate signer. Recent security analyses indicate that OTP based authentication remains vulnerable to range of attacks (Khairnar et al., 2023; Lei et al., 2021; Yu et al., 2022), including phishing, bomb attacks (Denial of Service on SMS, email, and other messaging applications), malware, and delegated access scenarios, particularly in the context of high value digital transactions.

This limitation becomes more severe in digital signing environments. The presence of a valid cryptographic signature combined with a successfully entered OTP may still fail to guarantee that the legitimate individual consciously reviewed, understood, and authorized the signing action. As a result, while OTP based verification provide an additional layer of security, they do not fully address the requirements of strong identity assurance at the moment of signing (Kirvan et al., 2025; Li et al., 2025).

Biometric verification has been proposed as complementary solution to strengthen identity assurance. Facial biometrics are especially used because they can be implemented using cameras without specialized hardware. However, static facial recognition alone is vulnerable to spoofing attacks using photos or videos. To mitigate this risk, liveness detection techniques need to be implemented alongside to confirm that a real, live human is interacting with the system (George & Marcel, 2025; Technology, 2023).

This paper argues that digital signing systems should move beyond OTP centric verification models and incorporate real-time biometric liveness detection directly in the signing action. By binding cryptographic signatures to live human presence, digital signing workflows can achieve stronger identity assurance without relying solely on external communication channels.

The objective of this work is not to replace PKI or OTP mechanisms, but to analyze their limitations and motivate a hybrid approach within the system. This paper makes several contributions: first, it provides an analysis of the limitations of OTP-based signer verification in digital signing workflows. Second, it introduces a hybrid cryptographic and biometric system model for digital document signing. Lastly, it discusses gesture-based facial liveness detection as a lightweight, deployable enhancement to improve security.

METHOD

This study described the experiment with a controlled, comparative experimental design to evaluate identity assurance at signing time under three verification configurations: (A) OTP-only, (B) biometric liveness-only, and (C) hybrid OTP + biometric liveness.

Study Design and Objectives

The experiments are designed to answer the following questions:

1. How effectively does OTP-only verification resist unauthorized signing under channel-compromise conditions?
2. How effectively does biometric liveness focused verification reduce presentation attacks?
3. Does hybrid OTP + biometric liveness improve identity assurance compared with OTP-only verification?

The primary hypothesis of this study is that the hybrid OTP + biometric liveness configuration will produce a significantly lower False Acceptance Rate (FAR) under adversarial scenarios compared with the OTP only configuration.

This hypothesis is based on the assumption that the two verification mechanisms mitigate different attack vectors and therefore provide complementary security benefits.

Experimental Design

A controlled comparative design was used with three verification configurations:

1. Configuration A: OTP only
2. Configuration B: Biometric Liveness Only
3. Configuration C: OTP + Biometric Liveness

Each configuration was tested under four threat scenarios: legitimate user, photo spoofing, video replay, and OTP channel compromise. Each scenario was repeated across multiple trials to ensure statistical reliability. Thirty legitimate participants and five designated adversarial participants were recruited for this controlled experiment. Each legitimate participant performed five signing attempts per verification configuration. The five adversarial participants performed channel-compromise simulations against OTP-based configurations and presentation attacks (photo and video replay) against biometric-based configurations, including combined attack scenarios under the hybrid model.

Evaluation Metrics

For each configuration scenario group, confusion matrix terms were computed as follows:

- True Acceptance Rate (TAR): Legitimate signings successfully completed [8]

$$TAR = \frac{TP}{TP + FN}\ x\ 100$$

- False Acceptance Rate (FAR): Unauthorized signings incorrectly accepted [8]

$$FAR = \frac{FP}{FP + TN}\ x\ 100$$

- Verification Failure Rate: Legitimate attempts rejected due to system limitations

$$VFR = \frac{FN}{TP + FN}\ x\ 100$$

- Signing Completion Time: Time from initiation to successful signature. Average completion time (seconds) was computed per group.

If a denominator was zero, the metric was reported as undefined (N/A) rather than imputed. These metrics allow direct comparison between OTP based and biometric based verification models.

The False Acceptance Rate (FAR) is used as the primary security metric because it directly measures the likelihood of unauthorized signing, which represents the main threat in digital signing systems.

True Acceptance Rate (TAR) and Verification Failure Rate (VFR) are included to evaluate usability and system reliability trade-offs.

Data Collection and Analysis

Each verification configuration was tested across all threat scenarios. Multiple signing attempts were conducted per scenario to reduce randomness and observe consistency.

Collected data included:

1. Verification Configuration
2. Threat Scenario
3. OTP/Liveness/Signature status
4. Completion Time and Failure Reason
5. Actor label (legitimate_user or attacker)
6. Outcome label (accepted or rejected) based on configuration acceptance logic.

Ethical Considerations

No raw biometric data were retained beyond runtime verification events. Facial data was processed in real time solely for liveness detection and discarded immediately afterward. Stored records were limited to experiment outcomes and metadata required for security evaluation. All participants were informed of the verification procedures and consented to participation.

RESULTS AND DISCUSSION

Dataset Composition and Attempt Distribution

This section reports the number of attempts collected per configuration scenario pair to establish statistical context before percentage interpretation.

Table 1 Number of Signing Attempts per Configuration and Scenario

ɔnfiguration	**Legitimate Attempts**	**Photo Spoof Attempts**	**Video Replay Attempts**	**ΓP Compromise Attempts**
P only				
ɛness Only				
ɔrid				

Source: Primary data obtained from the researcher's experimental results

Total legitimate attempts: 450

Total adversarial attempts: 100

All configurations were evaluated under controlled and repeatable conditions.

Confusion Matrix Summary

Table 2 Confusion Matrix Outcomes per Configurations

Configuration	**Scenario**	**TP**	**FN**	**FP**	**TN**
OTP only	Legitimate	150	0	-	-
OTP only	P Compromised Channel	-	-	25	0
Liveness Only	Legitimate	147	3	-	-
Liveness Only	Photo Spoof	-	-	0	25
Liveness Only	Video Replay	-	-	2	23

Configuration	Scenario	TP	FN	FP	TN
Hybrid	Legitimate	146	4	-	-
Hybrid	? Compromised Channel + Liveness Spoof Attempts	-	-	1	24

Source: Primary data derived from the experimental confusion matrix analysis

Performance Metrics

Table 3 Security and Usability Metrics

Configuration	TAR (%)	VFR (%)	FAR (%)	Attack Type
OTP only	100	0	100	TP Compromised Channel
Liveness Only	98	2	(Photo Spoofing) 3 (Video Replay) 4% (Combined)	All Spoof Attacks
Hybrid	97.33	2.67	4	TP Compromised Channel + Liveness Spoof Attempts

Source: Primary data based on system performance metric calculations

Comparative Security Analysis

Table 4 Relative Security Under OTP Compromise

Configuration	FAR Under OTP Compromised Channel	Relative Reduction vs OTP only method
OTP only	100%	-
Hybrid	4%	96% Reduction

Sourch: Primary data from comparative security analysis results

The results indicate a substantial reduction in unauthorized signing probability under channel-compromise conditions. Hybrid authentication reduces the false acceptance rate under OTP-compromised channel attacks from 100% to 4%, representing a 96% relative reduction compared to OTP-only authentication.

Security vs Usability Trade-Off

Table 5 Overall Comparison

Configuration	ntity Assurance Strength	Attack Resistance	Usability (TAR)
OTP only	Low Under Channel Compromise	Very Weak	Very High
Liveness Only	Moderate	Strong against photos, moderate against video	High
Hybrid	Highest	Strongest	High

Source: Primary data from overall system evaluation results

Statistical Significance Analysis

To assess whether the observed reduction in false acceptance rates between the OTP-only and Hybrid configurations is statistically significant, Fisher's exact test was applied to the 2×2 contingency table of adversarial acceptance outcomes. Fisher's exact test was selected because of the categorical outcome structure and the presence of small cell counts, including a zero-frequency cell in the OTP-only rejection category. Unlike the chi-square test, Fisher's exact test does not rely on large-sample approximations and is therefore appropriate for this dataset.

Under OTP-compromise conditions, the OTP-only configuration accepted 25 of 25 adversarial attempts, whereas the Hybrid configuration accepted 1 of 25 attempts. Fisher's exact test indicates a statistically significant difference between configurations (two-sided $p = 4.11 \times 10^{-13}$), confirming that the Hybrid model significantly reduces unauthorized signing acceptance compared with OTP-only under simulated channel compromise.

Key Observations

1. OTP Only verification demonstrates significant vulnerability under channel compromise (FAR = 100%)
2. Liveness Only verification eliminates static photo attacks (FAR = 0%) and limits video replay (8%)
3. Hybrid verification reduces unauthorized signing to 4% under OTP compromise
4. Hybrid model introduces a minimal but measurable usability trade-off (TAR decreases from 100% to 97.33%)

The results statistically support the hypothesis that combining channel possession verification with real-time biometric presence verification significantly improves identity assurance during digital signing.

This study was conducted in a controlled experimental environment with a limited number of participants and predefined spoofing scenarios. Results may vary under real-world deployment conditions, including diverse lighting environments, demographic variation, and more advanced deepfake techniques. Future research should expand participant diversity and evaluate additional adversarial models.

CONCLUSION

This paper examined identity assurance limitations in contemporary digital signing systems and evaluated the impact of integrating biometric liveness detection into the signing workflow. The findings highlight an important distinction between verifying possession of credentials and verifying the presence of the legitimate signer at the moment of document execution. The experimental results indicate that OTP based verification, while highly usable, remains vulnerable when communication channels are compromised. Biometric liveness verification reduces the success rate of presentation attacks, particularly static photo-based spoofing, though it introduces a modest usability trade-off. The hybrid OTP and liveness configuration demonstrates stronger resistance to unauthorized signing attempts compared with OTP-only verification, suggesting that combining independent verification factors enhances overall identity assurance. From a system design perspective, the integration of biometric liveness does not replace cryptographic guarantees provided by PKI but complements them by addressing a separate dimension of signer legitimacy. By requiring

real-time human interaction in addition to channel possession and cryptographic key use, the hybrid model increases the complexity of adversarial attacks and reduces reliance on a single verification mechanism. The experiment in this paper was conducted in a controlled experimental setting with a limited participant pool and predefined attack scenarios. Future research should examine larger and more diverse user populations, evaluate advanced spoofing techniques such as deepfake-based attacks, and assess long-term usability in real-world deployments. Further investigation into privacy considerations and implementation constraints is also recommended. Thus, embedding biometric liveness detection into digital signing workflows represents a practical enhancement to existing verification models and provides a structured approach to strengthening identity assurance in electronic document execution systems.

REFERENCES

Bartłomiejczyk, M. (2024). *Analysis of attacks on SMS OTP-based authentication*. CORE.

George, A., & Marcel, S. (2025). *Deep learning models for robust facial liveness detection*. arXiv.

Hassan, M., & Alqahtani, A. (2025). Digital signatures and their legal significance. *Edelweiss Applied Science and Technology*, *9*(1), 52–64.

Jarecki, S., Jubur, M., Krawczyk, H., Saxena, N., & Shirvanian, M. (2021). Two-factor password-authenticated key exchange with end-to-end security. *ACM Transactions on Privacy and Security (TOPS)*, *24*(3), 1–37. https://doi.org/10.1145/3446807

Khairnar, S., Gite, S., Kotecha, K., & Thepade, S. D. (2023). Face liveness detection using artificial intelligence techniques: A systematic literature review and future directions. *Big Data and Cognitive Computing*, *7*(1), 37. https://doi.org/10.3390/bdcc7010037

Kirvan, G., Reese, A., & Lumburovska, M. (2025). One time password (OTP) solution for two factor authentication. *Journal of Computer Science and Security Practices*.

Lei, Z., Nan, Y., Fratantonio, Y., & Bianchi, A. (2021). On the insecurity of SMS one-time password messages against local attackers in modern mobile devices. *Network and Distributed Systems Security (NDSS) Symposium 2021*. https://doi.org/10.14722/ndss.2021.24078

Li, J., Zhang, Y., & Chen, X. (2025). A high-performance adaptive fusion network for face anti-spoofing detection. *Scientific Reports*, *15*. https://doi.org/10.1038/s41598-025-21461-0

Maulana, F., Hendra, Y., Sakinah, P., Eirlangga, Y. S., & Ayun, A. Q. (2025). Efektivitas dan kelemahan autentikasi berbasis web menggunakan one-time password (OTP) dalam mencegah akses tidak sah. *Informatika Journal*.

Reynolds, J., Samarin, N., Barnes, J., Judd, T., Mason, J., Bailey, M., & Egelman, S. (2020). Empirical measurement of systemic 2FA usability. *29th USENIX Security Symposium (USENIX Security 20)*, 127–143.

Sharma, D. (2023). A survey on face presentation attack detection mechanisms. *Sensors*.

Singh, R., & Kumar, P. (2025). OTP security in wallet systems: A vulnerability assessment. *International Journal of Innovative Research in Science and Society*, *5*(3), 45–56.

Subagja, B. (2025). Minimizing face spoofing attacks with liveness detection. *Pertanika Journal*.

Technology, N. I. of S. and. (2023). *Digital Signature Standard (DSS) (FIPS PUB 186-5)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.186-5

Tullis, C. (2024). Public Key Infrastructure: Implementing High-Trust Electronic Signatures. In *World Bank Digital Transformation White Paper Series*. World Bank.

Tullis, C., Constantine, N., & Cooper, A. (2024). Electronic Signatures: Enabling Trusted Digital Transformation. In *World Bank Digital Transformation White Paper Series*. World Bank.

Yu, Z., Qin, Y., Li, X., Zhao, C., Lei, Z., & Zhao, G. (2022). Deep learning for face anti-spoofing: A survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *45*(5), 5609–5631. https://doi.org/10.1109/TPAMI.2022.3189326

Zhao, S. (2023). Security Vulnerabilities of Popular Multifactor Authentication Methods and a Remedy. *Journal of Network & Information Security*, *11*(1).

Zou, F., Zhang, Z., & Hu, Y. (2025). OTP-Hunter: An App-based Fuzzing Framework to Discover One Time Password Vulnerabilities. *IEEE Transactions on Dependable and Secure Computing*. https://doi.org/10.1109/TDSC.2025.3000000