VOL. 11. NO. 4 MAY 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v11i4.7728

JITK (JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER)

ENHANCED QR CODE BASED DIGITAL SIGNATURES FOR SECURE DOCUMENT MANAGEMENT TOWARD SUSTAINABLE GREEN INVESTMENT

Bagas Dwi Yulianto[1*]; Wisnu Wendanto[2]

Department of Informatics[1]
Department of Software Engineering[2]
Universitas Pignatelli Triputra, Surakarta, Indonesia[1,2]
www.upitra.ac.id[1,2]
bagas19.yulianto@gmail.com[*], wwendanto9@gmail.com

(*) Corresponding Author
(Responsible for the Quality of Paper Content)

Abstract— *This study proposes a secure QR Code–based digital signature framework to support paperless legal document management and sustainable green investment. The method integrates SHA-256 hashing and enhanced Multi-Factor RSA encryption, combined with a block-based hexadecimal processing approach to improve computational efficiency while maintaining strong cryptographic security. The generated encrypted signature is embedded into a QR Code, enabling real-time document verification through decryption and hash comparison. The main contribution of this study lies in the integration of optimized Multi-Factor RSA with QR-based authentication, providing both high security and practical verification capability within a unified system. Experimental results demonstrate successful authentication across all test cases, with robust performance under image distortions such as rotation, sharpening, Poisson noise, and Gaussian noise. The proposed method achieves an average Avalanche Effect of 85.78%, indicating strong diffusion and resistance to cryptographic attacks. Furthermore, a sustainability assessment involving 100 authorized respondents from education, corporate, and government sectors produced average scores above 4.0 across green computing, legal reliability, technology adoption, and digital security dimensions. These findings confirm that the proposed framework enhances digital document security while supporting environmentally sustainable and legally compliant paperless transformation.*

Keywords: *Paperless System, QR Code Authentication, Sustainability Impact Assessment.*

Intisari— *Penelitian ini mengusulkan suatu kerangka tanda tangan digital berbasis Kode QR yang aman untuk mendukung pengelolaan dokumen yang legal tanpa kertas serta investasi hijau berkelanjutan. Metode yang digunakan mengintegrasikan fungsi hash SHA-256 dan enkripsi Multi-Factor RSA yang ditingkatkan, dikombinasikan dengan pendekatan pemrosesan berbasis blok dalam format heksadesimal untuk meningkatkan efisiensi komputasi tanpa mengurangi kekuatan keamanan kriptografi. Tanda tangan terenkripsi yang dihasilkan kemudian disematkan ke dalam QR Code, sehingga memungkinkan proses verifikasi dokumen secara real-time melalui dekripsi dan perbandingan nilai hash. Kontribusi utama penelitian ini terletak pada integrasi Multi-Factor RSA yang dioptimalkan dengan autentikasi berbasis QR, yang memberikan tingkat keamanan tinggi sekaligus kemampuan verifikasi yang praktis dalam satu sistem terpadu. Hasil eksperimen menunjukkan keberhasilan autentikasi pada seluruh skenario pengujian, dengan kinerja yang tetap andal terhadap berbagai distorsi citra seperti rotasi, penajaman, noise Poisson, dan noise Gaussian. Metode yang diusulkan mencapai nilai rata-rata Avalanche Effect sebesar 85,78%, yang menunjukkan tingkat difusi yang tinggi serta ketahanan terhadap serangan kriptografi. Selain itu, evaluasi keberlanjutan yang melibatkan 100 responden yang memiliki kewenangan dari sektor pendidikan, korporasi,*

JITK (JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER)
VOL. 11. NO. 4 MAY 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v11i4.7728

dan pemerintahan menghasilkan skor rata-rata di atas 4,0 pada dimensi green computing, keandalan hukum, adopsi teknologi, dan keamanan digital. Temuan ini menegaskan bahwa kerangka yang dikembangkan mampu meningkatkan keamanan dokumen digital sekaligus mendukung transformasi tanpa kertas yang ramah lingkungan dan sesuai dengan ketentuan hukum.

***Kata Kunci**: Sistem Tanpa Kertas, Otentikasi Kode QR, Penilaian Dampak Keberlanjutan*

INTRODUCTION

Excessive paper consumption contributes to environmental threat, including deforestation and increased carbon emissions [1]. Paper waste, which is difficult to decompose, further contributes to pollution problems. Moreover, the paper production process itself requires significant amounts of energy that damage ecosystems. In a business context, reliance on physical paper also increases operational costs and reduces work efficiency [2]. These conditions demand concrete solutions to mitigate negative impacts while supporting sustainability.

The adoption of a paperless system has emerged as a strategic approach to minimizing resource consumption while improving administrative performance [3]. By replacing physical documentation with digital workflows, institutions can reduce operational costs, improve information accessibility, and enhance traceability. This transition supports broader digital transformation initiatives and aligns with sustainability objectives centered on efficiency and responsible resource management [4]. Beyond environmental benefits, paperless systems improve productivity and transparency across both public and private sectors through streamlined collaboration and secure data management [5]. With digital document management tools and secure cloud-based storage, administrative tasks can be completed more efficiently, with improved traceability and reduced risk of data loss. This technological shift also enables faster information retrieval and streamlined collaboration among stakeholders, leading to more effective decision-making processes. Beyond operational advantages, adopting paperless systems contributes to the development of a modern, environmentally aware economy by promoting sustainable practices and reducing waste generation.

Despite these advantages, it also introduces new challenges, especially in the management of official documents that demand strong guarantees of authenticity, integrity, and confidentiality [6]. Official documents often require validation mechanisms that ensure non-repudiation and tamper resistance, which traditional digital storage alone cannot guarantee. The absence of a verifiable authentication process may lead to security vulnerabilities, such as data manipulation, unauthorized access, or digital forgery. Therefore, the implementation of advanced cryptographic mechanisms becomes essential to maintain trust and compliance in digital document management [7]. Addressing these challenges requires a comprehensive approach that merges cryptographic security with verifiable identity authentication to achieve both technical and legal reliability in digital workflows.

To overcome these challenges, this research integrates a digital signature framework based on Multi-Factor RSA encryption [8] combined with SHA-256 hashing, which together serve as the foundation for secure QR Code generation. The Multi-Factor RSA algorithm enhances traditional RSA encryption by introducing additional prime factors during key generation [9], thereby strengthening cryptographic complexity and resistance to brute-force attacks. Meanwhile, the SHA-256 hashing algorithm ensures document integrity by generating a unique and irreversible digital signature for each file [10]. When combined, these two techniques establish a robust two-layer verification model SHA-256 guarantees that the content remains unchanged, while Multi-Factor RSA authenticates the digital ownership and encryption validity.

Additionally, embedding the encrypted digital signature into a QR Code provides a practical and efficient mechanism for real-time verification and validation. QR Codes function as portable cryptographic tokens that encapsulate encrypted metadata such as document hashes, timestamps, and authorized user credentials [11]. This design allows users to verify document authenticity simply by scanning the QR Code, which triggers a decryption process that confirms whether the embedded hash corresponds to the original data. The combination of SHA-256, Multi-Factor RSA, and QR Code-based encoding ensures that paperless document systems maintain both technological reliability and legal compliance. Beyond strengthening security, the implementation of this system directly supports green investment objectives by transforming conventional

VOL. 11. NO. 4 MAY 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v11i4.7728
JITK (JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER)

operational workflows into fully digital, paperless processes. The reduction in physical document usage contributes to lower resource consumption, decreased carbon emissions, and minimized administrative waste. From an Environmental, Social, and Governance (ESG) perspective, the system aligns with environmental goals through paper reduction, supports social accountability by ensuring transparent and verifiable documentation, and enhances governance through secure and auditable digital authentication mechanisms. Consequently, this hybrid cryptographic approach not only improves document security and operational efficiency but also reinforces the scalability and sustainability of digital transformation initiatives aligned with ESG-driven green investment strategies [12].

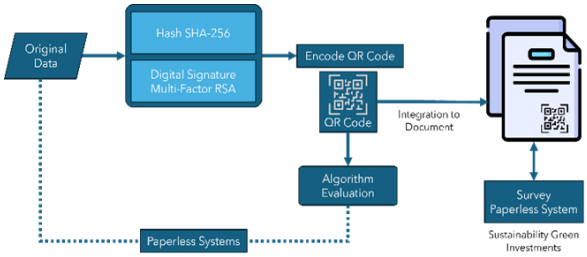
Previous studies serve as references and supporting evidence for this research, outlining the effectiveness of various cryptographic approaches in digital signature systems. Rapolu et al. (2022) utilized SHA-256 combined with RSA and AES to ensure image authentication and detect modifications [13]. Pangan et al. (2022) applied RSA-based QR Codes for secure user and administrator verification [14]. Yulianto et al. (2022) proposed a multi-layer digital signature scheme integrating SHA-256, 3DES, and DSA to validate digital certificates. [15].

Subsequent studies further reinforce this research. Putra et al. (2023) implemented signcryption using Multi-Factor RSA to enhance file security through combined signing and encryption processes [16]. Raman et al. (2024) employed QR Codes in a digital signature system, demonstrating superior performance compared to conventional methods while ensuring verification of the developed system [17]. Barron et al. (2025) focused on preventing Quishing or QR Code forgery by applying cryptographic techniques as a security mechanism for QR Codes [18]. Although these studies confirm the reliability of hashing, encryption, and QR-based verification techniques, they generally focus on individual components or layered approaches without optimizing computational efficiency or integrating these mechanisms into a unified, QR-based digital signature framework.

Based on the limitations of previous studies, main research gaps are the absence of an integrated framework that combines hashing, encryption, and QR-based verification into a single system, and the lack of optimization techniques to improve computational efficiency in Multi-Factor RSA. To address these gaps, this study proposes a QR Code–based digital signature framework that integrates SHA-256 hashing with enhanced Multi-Factor RSA using a block-based hexadecimal processing approach. This innovation ensures that the transition toward paperless systems can be carried out securely and in alignment with the principles of sustainable green investment [19].

This study contributes to the field in several aspects. First, it introduces an optimized Multi-Factor RSA mechanism that enhances computational efficiency through block-based hexadecimal processing. Second, it develops a unified QR Code–based authentication model that enables real-time verification of digital documents. Third, it evaluates the proposed system from both cryptographic performance and sustainability perspectives, demonstrating its applicability in supporting secure and environmentally sustainable paperless document management.

MATERIALS AND METHODS



Source: (Research Results, 2025)

Figure 1. Research Method

As illustrated in Figure 1, this research is structured into three primary stages. The first stage involves the development of a Paperless System that generates a QR-based digital signature through the combined use of SHA-256 hashing and Multi-Factor RSA encryption, which is subsequently embedded into legally valid digital documents. The second stage focuses on testing and evaluation, where the proposed algorithm and method are assessed in terms of performance, authentication, and verification to ensure system reliability and accuracy. The final stage encompasses a paperless system survey, which is conducted to analyze the system's contribution to sustainable green investment, emphasizing its potential environmental and operational benefits.

A. Paperless System

The system was developed as a web-based application architecture to ensure accessibility,

VOL. 11. NO. 4 MAY 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v11i4.7728

scalability, and secure data management [20]. The implementation utilizes PHP for server-side processing, integrated with a MySQL database for storing document metadata and verification records. The system is deployed on a web server environment and supports QR Code generation and scanning modules for real-time verification. A web-based framework enables users to interact with the system seamlessly through standard browsers without requiring additional installations, thereby enhancing usability and deployment efficiency. Moreover, this architecture facilitates centralized control and maintenance, ensuring that updates, authentication processes, and data integrity can be managed consistently across all user endpoints.

B. Cryptographic Processing

The QR Code generation process is implemented using PHP-based cryptographic operations that employ the SHA-256 hashing algorithm followed by encryption through the Multi-Factor RSA scheme [21]. Multi-Factor RSA, also known as multi-prime RSA, extends conventional RSA by using more than two prime factors in modulus generation. In this study, the Multi-Factor RSA utilizes three prime numbers (p, q, r) to construct the modulus n extending the conventional two-prime RSA model. The private key is generated accordingly through modular inverse computation. This approach increases factorization complexity while maintaining computational efficiency through optimized modular exponentiation.

This research proposes an enhanced Multi-Factor RSA that utilizes a block-based modular encryption process to improve computational efficiency. The SHA-256 hash output, represented in hexadecimal format, is divided into fixed-size blocks of 1 hex characters and directly converted into decimal values prior to encryption. This approach eliminates the need for ASCII conversion, reducing computational overhead while preserving data integrity and cryptographic strength. For instance, a generated hash segment such as (A0B2C3…F) is divided into a block (A, 0, B, 2, C, 3, …, F) and then directly converted into pure decimal values before undergoing Multi-Factor RSA encryption. This approach significantly reduces processing time while maintaining cryptographic strength and data integrity.

Finally, the combination of these cryptographic methods constitutes the token embedded within the QR Code, which is directly integrated into the corresponding legal document. The data utilized for token generation include the authorized issuer's name combined with a timestamp recorded now of tokenization. This mechanism ensures that each QR Code is uniquely bound to the document's identity, enabling secure verification, traceability, and authenticity.

C. Algorithm Evaluation

The initial evaluation of the proposed method was conducted through encryption and decryption processes, where the generated token when scanned must accurately reproduce the authorized assignment or letter data. This output is validated by comparing the hash obtained from the decryption process, thereby confirming the authenticity of the digital signature through verification process. Subsequently, a verification test was performed on the modified QR Code using the Mean Squared Error (MSE) metric to assess its validity [22].

The image distortion experiments, including rotation, sharpening, Poisson noise, and Gaussian noise, were conducted using MATLAB to ensure controlled and consistent evaluation conditions. Each modified QR Code was then scanned and verified using the developed system to confirm its readability and authentication validity. In addition, the Avalanche Effect was analyzed to measure the sensitivity of the proposed cryptographic method, as even minimal changes in input should result in significant variations in the ciphertext, indicating strong cryptographic performance [23].

$$MSE = \frac{\sum_{x=1}^{n}(O_x - M_x)^2}{n} \quad (1)$$

Equation (1) represents the computation of the MSE, which quantifies the difference between the original and modified QR Code images. In this equation, Ox denotes the original pixel value, Mx denotes the modified pixel value, and n represents the total number of pixels. The squared difference between each corresponding pixel pair is summed and divided by n, providing an objective measure of the distortion introduced during QR Code modification.

$$AE = \frac{d}{n} \times 100\% \quad (2)$$

Equation (2) is used to calculate the Avalanche Effect, which measures the sensitivity of the encryption algorithm to small changes in the input. In this equation, d represents the number of differing blocks between two ciphertexts generated from slightly different inputs, while n denotes the

VOL. 11. NO. 4 MAY 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v11i4.7728
JITK (JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER)

total number of encrypted blocks. A higher value indicates stronger diffusion characteristics, meaning that even minimal alterations in the plaintext produce significant changes in the ciphertext, thereby ensuring robust cryptographic performance.

D. Sustainability Impact Assessment

The assessment was conducted involving 100 respondents from diverse professional backgrounds, all of whom were either currently holding or had previously held official positions within their respective institutions. This selection criterion ensures that each participant possessed legal authority to perform document signing, thereby reinforcing the study's focus on authentic and authorized digital signatures. The surveyed institutions were categorized into three sectors: education, corporate, and government, providing a representative overview of digital document authentication practices across multiple organizational domains.

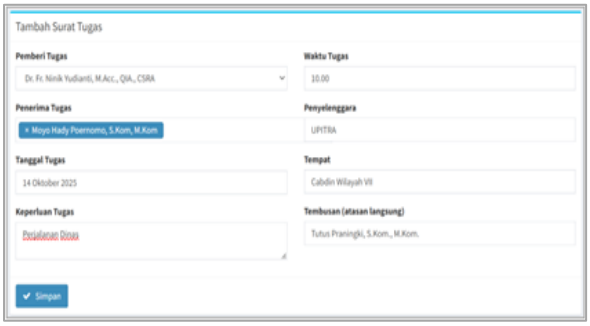
The survey assessment was conducted based on four key aspects that support sustainable green investment. The first aspect, green computing, evaluates how the implementation of a paperless system contributes to reducing global carbon emissions and mitigating environmental impacts. The second aspect, legal document, examines the ability of digital signatures to serve as legally recognized instruments for official correspondence and task authorization. The third aspect, technology, focuses on the system's role in promoting modern digital transformation and its applicability across different institutional sectors. Finally, the fourth aspect, digital security, assesses the reliability and robustness of the system in ensuring data protection and maintaining integrity when digital signatures are applied.

RESULTS AND DISCUSSION

In this section, we present and discuss the results and findings obtained from the implementation of the proposed framework as outlined in Figure 1.

A. Paperless System

Figure 2 illustrates the interface of the paperless system during the digital signature creation process, where users are required to complete all the provided data fields. The entered information, including the name of the authorized officer or document issuer and the timestamp now of signature generation, serves as the primary input for the QR Code process. These parameters are securely processed through the integrated cryptographic functions to ensure that each generated QR Code represents a unique and verifiable digital identity for the document.



Source: (Research Results, 2025)
Figure 2. Adding the Digital Signature Interface

Source: (Research Results, 2025)
Figure 3. Interface of QR Code Data

Figure 3 illustrates the QR Code generated as a digital signature token, automatically produced by the system after the encryption and hashing processes. Each QR Code represents a unique cryptographic identity derived from key document parameters such as the authorized signer's name, timestamp, and verification data. This design ensures that every digital signature is distinct, tamper-resistant, and securely bound to its associated document. The QR Code serves not only as a compact digital seal but also as an authentication mechanism that can be validated in real time through the decryption and hash comparison process.

Figure 4 demonstrates how the generated QR Code is integrated into the digital document, showcasing seamless system interoperability between encryption, document management, and user access. Users can authenticate the document by scanning the code, which retrieves and validates the encrypted data against its stored hash values.

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 11. NO. 4 MAY 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v11i4.7728

Source: (Research Results, 2025)
Figure 4. Example of Integrated Document

Figure 5 illustrates the verification results obtained through the QR Code scanning process. The verification mechanism is performed by decrypting the encoded token and comparing the resulting output with the corresponding SHA-256 hash value. If the decrypted data produce the same hash value as the original record, the system confirms the signature as valid. As shown on the left side of the figure, a valid result appears when the decrypted information successfully matches the SHA-256 hash generated during the initial signature creation process. In this condition, the system displays the complete set of encrypted information associated with the digital signature, including the authorized signer's identity and the timestamp used during token generation. Conversely, the right side of the figure demonstrates an invalid result, which occurs when the decrypted output fails to match the expected hash value. Such a mismatch indicates that the data may have been modified, corrupted, or generated from an unauthorized source, thereby confirming that the digital signature cannot be authenticated.

Source: (Research Results, 2025)
Figure 5. QR Code Verification Valid & Invalid

B. Cryptographic Processing

Table 1. Cryptographic Processing into QR Code (Digital Signature)

No	Complete Data	Hash SHA-256	Multi-Factor RSA	QR Code
1	Dr. Fr. Ninik Yudianti, M.Acc., QIA., CSRA; Monday, 13 October 2025 00:27:25; Moyo Hady Poernomo, S.Kom, M.Kom; Perjalanan Dinas	856be00b3ab5187b3e3052ff1865af9040e880c516267fa0a35a021783ce3ec0	02d78d832c000083b1be83d701028583b12cb100d7083c3c01028dd7be3cdb0040002c0202006cd7018d088d853cbe00beb1d7be0008018502b16c2cb12c6c00	
2	Thomas Ambar Prihastomo, S.S., M.Sc; Monday, 13 October 2025 15:11:42; Benedictus Herry Suharto, S.T., M.T.; Pendampingan Prof John	2250bf21a5aa9ca1ae3d96fc34e0abe5d4fa89fc6f90dbd79ff3f38e2a15ade0	0808d700833c0801bed7bebedb6cbe01be2cb19ddb8d3c6cb1402c00be832cd79d403cbe02db3c6c8d3cdb009d839d85db3c3cb13cb1022c08be01d7be9d2c00	
3	Neil Semuel Rupidara, S.E., M.Sc., Ph.D.; Monday, 13 October 2025 15:21:52; Remon Gunanta, S.Pd., M.Si.; SAP Update License	be3e05e0d0dc7239e46470aed2c228b3cbd49c8238d2624958cbc9fc8d428583	0883b1b18d08b108dbdbb101be02020801d7b1db6c02852c2c01026c856cbe839d010800856c023c83d72cdb9db1020102d79d83836c3c01d79d852c3cdbdbd7	
4	Neil Semuel Rupidara, S.E., M.Sc., Ph.D.; Monday, 13 October 2025 15:24:04; Moyo Hady Poernomo, S.Kom, M.Kom; Pelatihan Office 2021	be3e05e0d0dc7239e46470aed2c228b3cbd49c8238d2624958cbc9fc8d428583	832cb12c00d72c009d009d6c8508b1db2c408d408500be2c9d086c08080283b16c839d40db6c0208b1029d088d0840dbd7026c836cdb3c6c029d400802d702b1	

No	Complete Data	Hash SHA-256	Multi-Factor RSA	QR Code
5	Johannes Christianto Hartono, S.Pd.; Monday, 13 October 2025 15:31:02; Bagas Dwi Yulianto, S.Kom., M.Kom.; Licensing Office 2021	f2c47c923aa921fc7 dde60d3c6d33f805 d4daefc165f06548e 66b7f90219fbe1	3c086c40856cdb08b1bebedb0801 3c6c859d9d2c8d009db16c8d9db1 b13c0200d79d409dbe2c3c6c018d d73c008dd740022c8d8d83853cdb 000801db3c832c01	

Source: (Research Results, 2025)

Table I presents the results of the hashing and encryption processes, which together generate the QR Code used as a digital signature for official documents. The table summarizes the transformation of input data such as the authorized officer's name and timestamp into the corresponding SHA-256 hash, followed by encryption using the Multi-Factor RSA algorithm. The resulting encrypted values are then encoded into a QR Code, ensuring secure, unique, and verifiable digital identification for each document within the paperless system.

C. Algorithm Evaluation

Table 2. QR Code Authentication

No	QR Code	Hash SHA-256	Decryption Process	Validity
1		856be00b3ab5187b3e3052ff1865af904 0e880c516267fa0a35a021783ce3ec0	856be00b3ab5187b3e3052ff1865af904 0e880c516267fa0a35a021783ce3ec0	Valid
2		2250bf21a5aa9ca1ae3d96fc34e0abe5d 4fa89fc6f90dbd79ff3f38e2a15ade0	2250bf21a5aa9ca1ae3d96fc34e0abe5d 4fa89fc6f90dbd79ff3f38e2a15ade0	Valid
3		be3e05e0d0dc7239e46470aed2c228b3 cbd49c8238d2624958cbc9fc8d428583	be3e05e0d0dc7239e46470aed2c228b3 cbd49c8238d2624958cbc9fc8d428583	Valid
4		be3e05e0d0dc7239e46470aed2c228b3 cbd49c8238d2624958cbc9fc8d428583	be3e05e0d0dc7239e46470aed2c228b3 cbd49c8238d2624958cbc9fc8d428583	Valid
5		f2c47c923aa921fc7dde60d3c6d33f805d 4daefc165f06548e66b7f90219fbe1	f2c47c923aa921fc7dde60d3c6d33f805d 4daefc165f06548e66b7f90219fbe1	Valid

Source: (Research Results, 2025)

Table 2 presents the verification results, showing that each scanned token or digital signature was decrypted and compared to its original hash value. When the decrypted output matched the corresponding hash, the signature was confirmed as valid and authenticated. The findings demonstrate that all tested data were successfully reconstructed to their original hash values, confirming the reliability of the proposed cryptographic framework. This result indicates a 100% authentication accuracy, which is consistent with the expected behavior of hash-based verification systems. Compared to previous studies such as Rapolu et al. (2022) [13] and Yulianto et al. (2022) [15], which also reported successful authentication using multi-layer cryptographic approaches, the proposed method achieves similar reliability while offering a more integrated and efficient QR-based verification mechanism. This suggests that the combination of SHA-256 and enhanced Multi-Factor RSA can maintain strong

VOL. 11. NO. 4 MAY 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v11i4.7728

integrity guarantees without increasing system complexity.

Source: (Research Results, 2025)

Figure 6. QR Code Robustness Testing Under Image Distortions (Rotate, Sharpen, Poisson, Gaussian)

Figure 6 illustrates the modified QR Codes generated using MATLAB through several image alteration techniques, including rotation, sharpening, Poisson noise, and Gaussian noise with a variance of 0.5 [24]. These modifications were implemented to assess the robustness and stability of the proposed QR Code–based digital signature when subjected to different types of image distortions. The evaluation aims to ensure that the QR Code maintains its readability and data integrity despite potential visual or environmental degradation.

Table 3. QR Code Robustness Evaluation

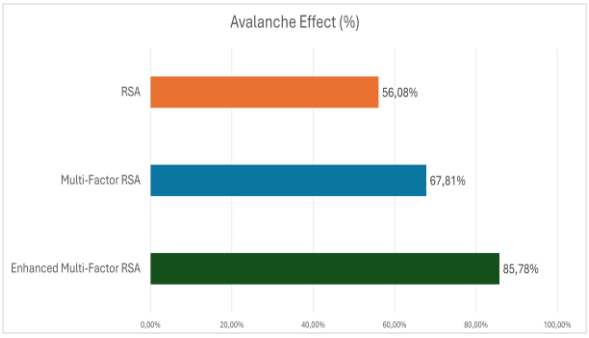
No	QR Code	Modification	MSE	Validity
1		Rotate 180°	25963.0836	Valid
		Sharpening 100	583.6408	Valid
		Poisson	47.1862	Valid
		Gaussian 0.5	7266.4895	Valid
2		Rotate 180°	25654.7870	Valid
		Sharpening 100	573.2542	Valid
		Poisson	46.6516	Valid
		Gaussian 0.5	7383.8254	Valid
3		Rotate 180°	25582.6327	Valid
		Sharpening 100	585.4136	Valid
		Poisson	45.9257	Valid
		Gaussian 0.5	7482.7588	Valid
4		Rotate 180°	25836.9127	Valid
		Sharpening 100	592.2454	Valid
		Poisson	48.0508	Valid
		Gaussian 0.5	7100.8291	Valid
5		Rotate 180°	25685.6168	Valid
		Sharpening 100	584.3644	Valid
		Poisson	46.3859	Valid
		Gaussian 0.5	7440.7373	Valid

Source: (Research Results, 2025)

Table 3 presents the outcomes of the QR Code robustness testing, revealing that all applied modifications including rotation, sharpening, and noise addition had no impact on the readability or integrity of the QR Code. The encoded information remained completely recoverable and verifiable, validating the method's effectiveness under various distortion conditions. These findings confirm the strong resilience and structural stability of the generated QR Code, as all modified images

VOL. 11. NO. 4 MAY 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v11i4.7728
JITK (JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER)

remained readable and valid despite significant distortion levels. The relatively high MSE values, particularly under rotation and Gaussian noise, indicate substantial pixel-level differences; however, they do not affect the decoding capability of the QR Code. This demonstrates that the proposed method is robust against common image degradations, aligning with findings from Barron and Sharma (2025) [18], who emphasized the importance of distortion-resistant QR-based authentication. The results highlight that structural redundancy in QR encoding effectively preserves embedded cryptographic information even under adverse conditions.

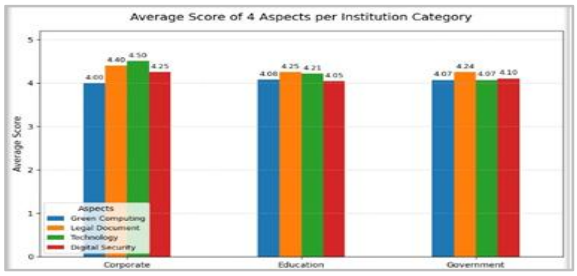


Source: (Research Results, 2025)
Figure 7. The Comparison of Avalanche Effect

Figure 7 presents the average Avalanche Effect derived from the evaluation results. Compared to the 50% diffusion benchmark reported by Verma and Sharma (2020) [25], a comparative analysis demonstrates the effectiveness of the proposed enhancement. The conventional RSA algorithm produced an Avalanche Effect of 56.08%, while the standard Multi-Factor RSA achieved 67.81%. In contrast, the proposed Enhanced Multi-Factor RSA reached 85.78%, representing a substantial improvement in diffusion performance.

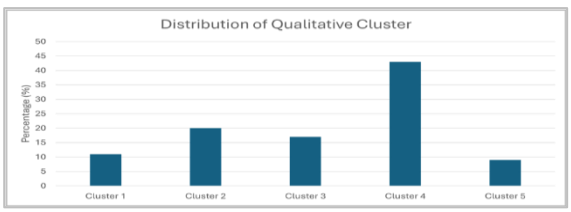
The high diffusion level is achieved through the integration of SHA-256 hashing and Enhanced Multi-Factor RSA, which significantly increases the sensitivity of the ciphertext to small input variations. The proposed method substantially outperforms conventional RSA and standard Multi-Factor RSA. This improvement indicates stronger resistance to differential attacks and enhanced randomness in ciphertext generation. The result confirms that the proposed block-based hexadecimal processing contributes not only to efficiency but also to improved cryptographic diffusion.

D. Sustainability Impact Assessment



Source: (Research Results, 2025)
Figure 8. Average Score All Instutition

Figure 8 illustrates that the average score across all institutional categories exceeds 4.0, indicating that the proposed paperless system effectively promotes positive transformation toward sustainable green investment practices. Within the corporate sector, the technology aspect achieved the highest rating, reflecting the system's capability to drive modernization and its applicability across various organizational operations. Conversely, in the education and government sectors, the legal document aspect scored the highest, emphasizing strong confidence in the system's ability to generate legally recognized digital signatures for official correspondence and administrative documentation. These findings demonstrate the proposed framework's adaptability and practical relevance across different institutional sectors. The consistently high scores (above 4.0) indicate strong user acceptance, particularly in legal reliability and technology adoption. However, the variation across sectors suggests that organizational readiness and digital maturity may influence perceived effectiveness. Compared to previous studies on digital signature adoption, which often focus solely on technical validation, this study extends the evaluation by incorporating sustainability and user perception dimensions. This highlights the broader impact of the proposed system, not only in enhancing security but also in supporting environmentally sustainable digital transformation.



Source: (Research Results, 2025)
Figure 9. Qualitative Cluster

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 11. NO. 4 MAY 2026
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v11i4.7728

Figure 9 presents the qualitative feedback from respondents, grouped into five thematic clusters reflecting perceptions of the proposed system's impact and applicability. The first cluster (11%) suggests that the legally recognized digital correspondence mechanism can be extended to other categories of legal documents, broadening its practical implementation. The second cluster (20%) underscores that digital signatures hold strong potential for legal adoption across diverse operational and administrative contexts. The third cluster (17%) demonstrates substantial support for green investment initiatives, highlighting the system's role in improving institutional efficiency while promoting environmental sustainability.

The fourth and most significant cluster (43%) reveals that digital signatures effectively minimize paper consumption without compromising legal validity, showcasing the system's ability to integrate ecological responsibility with operational reliability. Meanwhile, the fifth cluster (9%) emphasizes encouragement for continued digital transformation within institutions to further reduce paper dependency.

CONCLUSION

This study proposes a QR Code–based digital signature framework that integrates SHA-256 hashing with enhanced Multi-Factor RSA to enable secure and practical paperless document management. The main contribution is a unified cryptographic and QR-based verification model that supports real-time authentication while improving computational efficiency through block-based hexadecimal processing. The effectiveness of the approach is evidenced by consistent authentication accuracy (100%), strong cryptographic diffusion (85.78% Avalanche Effect), and stable QR Code readability under various image distortions. In addition, user evaluation results with average scores above 4.0 indicate that the system is not only technically reliable but also practically applicable in supporting secure and environmentally sustainable digital transformation. However, This study is limited to controlled experimental conditions and has not been validated in large-scale real-world deployments. Future work may focus on evaluating system scalability under high transaction volumes and integrating advanced verification technologies to further enhance robustness and interoperability.

REFERENCE

[1] A. Santoro, F. Piras, and Q. Yu, "Spatial Analysis of Deforestation in Indonesia in the Period 1950–2017 and the Role of Protected Areas," *Biodivers Conserv*, Jul. 2023, doi: 10.1007/s10531-023-02679-8.

[2] L. B. Kringelum, J. N. Kristiansen, and A. N. Gjerding, "Business Model Implications of Industry Path Dependency," *Journal of Business Models*, vol. 9, no. 1, pp. 20–28, Mar. 2021, doi: 10.5278/jbm.v9i1.5866.

[3] K. Moustafa, P. J. García, F. El Khoury, and S. Pierre, "From Seller Screens to Buyer Screens: Toward a Smart Digital Receipt Solution for Sustainability and Greenhouse Gas Mitigation by Million Tons," *Digital Society*, vol. 2, no. 3, p. 53, Nov. 2023, doi: 10.1007/s44206-023-00078-8.

[4] Y. Yin, J. Hussain, Q. Gou, and J. Wang, "Green Economic Growth and Environment: Unveiling the Role of Environmental Policy and Cleaner Energy in G-7 Countries," *Clean Technol Environ Policy*, vol. 26, no. 12, pp. 4137–4156, Dec. 2024, doi: 10.1007/s10098-024-02824-z.

[5] S. J. Rashid, "Empowering Paperless Workflows: Networked UDC-Based EDMS for Enhanced Efficiency and Data Security," *NTU Journal of Engineering and Technology*, vol. 3, no. 4, pp. 1–6, Dec. 2024, doi: 10.56286/ntujet.v3i4.919.

[6] R. A. Khan and S. A. Lone, "A Comprehensive Study of Document Security System, Open Issues and Challenges," *Multimed Tools Appl*, vol. 80, no. 5, pp. 7039–7061, Feb. 2021, doi: 10.1007/s11042-020-10061-x.

[7] J. Chandrashekhara, A. V B, P. H, and R. B. R, "A Comprehensive Study on Digital Signature," *International Journal of Innovative Research in Computer Science and Technology*, vol. 9, no. 3, pp. 43–47, May 2021, doi: 10.21276/ijircst.2021.9.3.7.

[8] A. Dash, A. Sarkar, A. Chatterjee, S. Darshana, M. Pandey, and R. K. Barik, "Multi-Factor Analysis of RSA Based on Variations in Primes Used for Modulus Generation," in *2023 3rd International Conference on Innovative Sustainable Computational Technologies (CISCT)*, Sep. 2023, pp. 1–6. doi: 10.1109/CISCT57197.2023.10351432.

[9] R. S. Ganesh and D. K. Venkataramana, "Optimized Digital Signature Algorithm with Multi-Prime RSA," *International Journal of*

Scientific Research and Technology, Mar. 2025, doi: 10.5281/zenodo.15078329.

[10] J. C. Bañas and J. C. Mababa, "File Integrity Verifier Using Digital Signature Algorithm and SHA-256 with Memory-Mapping Technique," *International Journal of Computing Sciences Research*, vol. 7, pp. 2348–2357, Aug. 2023.

[11] T. Wellem, Y. Nataliani, and A. Iriani, "Academic Document Authentication using Elliptic Curve Digital Signature Algorithm and QR Code," *JOIV : International Journal on Informatics Visualization*, vol. 6, no. 3, pp. 667–675, Sep. 2022, doi: 10.30630/joiv.6.2.872.

[12] S. L. Andriati and D. A. Batubara, "The Validity of QR-Code Digital Signature in Contract Towards The Evidence Agenda In Civil Court," *Mahadi: Indonesia Journal of Law*, vol. 3, no. 2, pp. 95–102, Aug. 2024.

[13] R. T. Rapolu, M. K. Gopal, and G. A. E. S. Kumar, "A Secure Method for Image Signaturing using SHA-256, RSA, and Advanced Encryption Standard (AES)," in *2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, Apr. 2022, pp. 1–7. doi: 10.1109/ICDCECE53908.2022.9792989.

[14] A. M. S. Pangan, I. L. Lacuesta, R. C. Mabborang, and F. P. Ferrer, "Authenticating Data Transfer Using RSA-Generated QR Codes," *European Journal of Information Technologies and Computer Science*, vol. 2, no. 4, pp. 18–30, Aug. 2022, doi: 10.24018/compute.2022.2.4.73.

[15] B. D. Yulianto, L. Budi Handoko, E. H. Rachmawanto, Pujiono, and M. A. Soeleman, "Digital Certificate Authentication with Three-Level Cryptography (SHA-256, DSA, 3DES)," in *2022 International Seminar on Application for Technology of Information and Communication (iSemantic)*, Sep. 2022, pp. 343–350. doi: 10.1109/iSemantic55962.2022.9920404.

[16] T. S. Putra, M. A. Budiman, and S. Suwilo, "Signcryption Techniques For Digital File Security Using the RSA Multi-Factor Algorithm and the ESIGN Algorithm," in *2023 International Conference of Computer Science and Information Technology (ICOSNIKOM)*, Nov. 2023, pp. 1–6. doi: 10.1109/ICoSNIKOM60230.2023.10364520.

[17] R. Raman, V. Kumar, B. G. Pillai, D. Rabadiya, R. Divekar, and H. Vachharajani, "Implementing QR Code-Enabled Smart Documents: A Fusion of Distributed Databases and Digital Signatures," in *2024 Second International Conference on Data Science and Information System (ICDSIS)*, May 2024, pp. 1–5. doi: 10.1109/ICDSIS61070.2024.10594158.

[18] I. R. Barron and G. Sharma, "Quashing Quishing Attacks Using Self-Authenticating Dual-Modulated QR Codes," *IEEE Secur Priv*, pp. 2–10, Feb. 2025, doi: 10.1109/MSEC.2025.3530487.

[19] A. A. Santosa and F. Alamsjah, "The Drivers of a Digital Signature System Adoption: Evidence from Finance and Information System Departments," *Journal of Information Systems Engineering and Business Intelligence*, vol. 8, no. 1, pp. 80–90, Apr. 2022, doi: 10.20473/jisebi.8.1.80-90.

[20] Fitriyani, M. Nuzula, and C. L. Setiawati, "Development of an Integrated Web-Based Multi-User Application for Village Fund Usage Reporting Using CodeIgniter," *Jurnal Serambi Engineering*, vol. 10, no. 2, Mar. 2025.

[21] B. D. Yulianto and S. H. Hadi, "Verifikasi Quick Response Code dengan Vigenere Cipher dan Multi-Factor RSA," *Techno.Com*, vol. 24, no. 1, pp. 240–247, Feb. 2025, doi: 10.62411/tc.v24i1.12192.

[22] C. Manikandan, A. P. Rabinson, A. Devibala, M. Sivanesh, S. Karunyaa, and A. Rajesh, "Design of Image Encryption Technique Using MSE Approach," in *Applications and Techniques in Information Security*, V. S. Shankar Sriram, A. G. H., G. Li, and S. R. Pokhrel, Eds., Singapore: Springer Nature, 2025, pp. 95–106. doi: 10.1007/978-981-97-9743-1_7.

[23] J. Kaur and K. R. R. Kumar, "Analysis of Avalanche effect in Cryptographic Algorithms," in *2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Oct. 2022, pp. 1–4. doi: 10.1109/ICRITO56286.2022.9965127.

[24] A. Ghazdali, A. Hadri, A. Laghrib, and M. Nachaoui, "Poisson Noise and Gaussian Noise Separation Through Copula Theory," *Multimed Tools Appl*, vol. 83, no. 26, pp. 67927–67952, Aug. 2024, doi: 10.1007/s11042-023-17898-y.

[25] R. Verma and A. K. Sharma, "Cryptography: Avalanche effect of AES and RSA," *International Journal of Scientific and Research Publications (IJSRP)*, vol. 10, no. 4, p. p10013, Apr. 2020, doi: 10.29322/IJSRP.10.04.2020.p10013.