Jurnal Esensi Infokom Vol 10 No. 2 Oktober 2026
e-ISSN: 2828-6707
https://esensijournal.com/index.php/infokom
DOI: 10.55886/infokom.v10i2.566

Design And Implementation Of An Ed25519-Based Digital Signature With A Visual Cryptography Sharing Scheme For Digital Document Authenticity Validation

Karno Diantoro[1*], Era Sari Munte[2], Purwo Agus Sucipto[3], Ahmad Soderi[4]

[1,4] *Department of Computer Science*
STMIK Mercusuar
Jl. Raya Jatiwaringin No. 144, Jatiwaringin,
Pondok Gede District, Bekasi City, West Java 17411, Indonesia
[1*]karno@mercusuar.ac.id *(corresponding author)*

[2,3] *Department of Computer Science*
[2,3] *Jayabaya University*
A Jl. Pulomas Barat, Kayu Putih, East Jakarta City, Indonesia
[2]erasarimunthe76@gmail.com
[3]purwoagussucipto@gmail.com
[4]ahmad@mercusuar.ac.id

***Abstract*— The increasing use of digital documents has created a growing need for mechanisms that can ensure the authenticity and integrity of information. Digital documents can be modified without leaving physical evidence of alteration, making cryptography-based validation mechanisms necessary. This study designs and implements a digital document validation mechanism by integrating an Ed25519-based digital signature with a Visual Cryptography Sharing Scheme. Ed25519 is used to generate and verify digital signatures based on a private and public key pair. The document hash value is used as a representation of the data to be signed so that even minor modifications to the document can affect the verification result. Visual Cryptography is used to divide authentication information into several shares so that the complete information cannot be obtained from a single share. The study applies a research and development approach consisting of requirements analysis, system architecture design, implementation, and functional and security testing. The testing scenarios include original documents, modified documents, invalid signatures, incomplete shares, and share reconstruction. The proposed design demonstrates that Ed25519 can serve as an authentication and document integrity mechanism, while Visual Cryptography can provide an additional layer for distributing validation information. The main contribution of this study is the integration of these two mechanisms into a unified digital document validation process. The developed system can serve as a basis for securing academic documents, administrative documents, certificates, electronic letters, and other digital documents that require authenticity verification.**

Keywords: digital signature, Ed25519, Visual Cryptography, secret sharing, document validation, digital document security.

Intisari— **Perkembangan penggunaan dokumen digital meningkatkan kebutuhan terhadap mekanisme yang mampu memastikan keaslian dan integritas informasi. Dokumen digital dapat mengalami perubahan tanpa meninggalkan perubahan fisik yang mudah diamati sehingga diperlukan mekanisme validasi berbasis kriptografi. Penelitian ini merancang dan mengimplementasikan mekanisme validasi dokumen digital dengan mengintegrasikan *digital signature* berbasis Ed25519 dan *Visual Cryptography Sharing Scheme*. Ed25519 digunakan untuk menghasilkan tanda tangan digital berdasarkan pasangan kunci privat dan publik. Nilai hash dokumen digunakan sebagai representasi data yang ditandatangani sehingga perubahan sekecil apa pun pada dokumen dapat memengaruhi hasil verifikasi. Visual Cryptography digunakan untuk membagi informasi autentikasi ke dalam beberapa *share* sehingga informasi tersebut tidak dapat digunakan secara lengkap hanya dari satu bagian. Penelitian menggunakan metode *research and development* yang meliputi analisis kebutuhan, perancangan arsitektur, implementasi, dan pengujian fungsional serta pengujian keamanan. Skenario pengujian mencakup dokumen asli, dokumen yang mengalami perubahan, tanda tangan tidak valid, *share* tidak lengkap, dan rekonstruksi *share*. Hasil perancangan menunjukkan bahwa Ed25519 dapat digunakan sebagai**

mekanisme autentikasi dan integritas dokumen, sedangkan Visual Cryptography dapat digunakan sebagai lapisan tambahan untuk distribusi informasi validasi. Kontribusi penelitian terletak pada integrasi kedua mekanisme dalam satu alur validasi dokumen digital. Sistem yang dikembangkan dapat menjadi dasar untuk pengamanan dokumen akademik, administrasi, sertifikat, surat elektronik, dan dokumen digital lain yang memerlukan pemeriksaan keaslian.

Kata kunci: digital signature, Ed25519, Visual Cryptography, secret sharing, validasi dokumen, keamanan dokumen digital.

I. INTRODUCTION

Digital transformation has changed the way organizations create, store, transmit, and verify documents. Documents that were previously available in physical form are increasingly being replaced by digital documents. This situation occurs in educational institutions, government agencies, companies, financial services, and other organizations. Digital documents provide advantages in terms of storage and distribution. However, these advantages also create a need for security mechanisms that can ensure that documents remain authentic after storage and transmission.

The authenticity of a digital document is related to the ability of a system to verify that the document originates from an authorized party. Integrity refers to the ability of a system to ensure that the document content has not been modified after authorization. NIST explains that digital signatures can provide assurance that information was signed by the claimed party and was not modified after signing [13]. This concept provides an important foundation for digital document authentication systems.

Integrity becomes more challenging when documents are distributed through networks. Files can be copied, transferred, or modified without changing their file names. Changes to a single character, number, date, or recipient identity can alter the meaning of a document. Therefore, verification based only on file names, file sizes, or storage locations is insufficient to guarantee document authenticity.

One approach to addressing this problem is the use of digital signatures. This mechanism uses public-key cryptography to generate a signature value associated with the data and the owner's private key. The recipient uses the corresponding public key to verify the signature. If the data are modified after signing, the verification process can produce an invalid result.

The selection of a digital signature algorithm is an important factor in system design. The algorithm must provide a strong authentication mechanism while remaining efficient for software implementation. One widely used algorithm in EdDSA-based digital signatures is Ed25519. The algorithm uses the Edwards25519 curve and is designed to provide efficient digital signing and verification. The technical specification of Ed25519 is described in RFC 8032 [14].

Shankar et al. investigated the application of Ed25519 in a digital signature mechanism for document authentication [6]. Their study examined key generation, document signing, and signature verification. The application of Ed25519 in their research demonstrates that the algorithm can be implemented as a digital document authentication mechanism using software based on Python.

In addition to digital signatures, secret sharing mechanisms can be used to distribute sensitive information among multiple parties. The basic principle is to divide secret information into several parts called shares. The information can only be reconstructed when the required number of shares is available. This approach provides a mechanism that differs from digital signatures because its primary function is the distribution of secret information.

One form of secret sharing that can be applied to visual information is the Visual Cryptography Sharing Scheme. Visual Cryptography enables visual information to be divided into several shares. Each share individually does not provide complete information about the secret. The information can be recovered when the required shares are combined according to a predefined access scheme. This approach has been used in various studies related to authentication and information protection.

Zhang and Gu developed an authenticatable Visual Secret Sharing Scheme with a mechanism for authenticating shares [11]. Their study demonstrated that, in addition to reconstruction quality, the validity of each share is an important consideration. An unauthorized share can affect the reconstruction process and create potential security risks.

Zhong et al. developed a Visual Secret Sharing Scheme with QR Code-based authentication [12]. Their research demonstrated that Visual Cryptography can be used to strengthen the security of information-sharing processes. This approach is relevant to the present study because it demonstrates the relationship between secret sharing and authentication mechanisms.

Sherine and Peter also investigated Visual Cryptography for dividing visual information into multiple shares [7]. Their study explored the use of the CMY color space in visual secret sharing. The findings demonstrate that Visual Cryptography continues to evolve to address different information security requirements.

Research on Visual Cryptography-based authentication also developed in 2023. Valisireddy et al. applied Visual Secret Sharing to QR Codes to secure online document authentication [9]. Document information was embedded in QR Codes and subsequently divided into several shares. The document could only be accessed after the required shares were combined.

Yan et al. developed a shadow image authentication mechanism using public-key cryptography in an image secret sharing system [10]. Their research demonstrated that public-key cryptography and Visual Cryptography can be combined to authenticate shadow images. This approach has a conceptual relationship with the present study because public-key cryptography is used as an authentication mechanism in a sharing system.

The development of Visual Cryptography also reveals several security challenges. Fu et al. discussed information leakage that may occur when the random number sequence used to generate shares becomes known to an attacker [2]. Their findings indicate that Visual Cryptography should not automatically be considered secure against all threats. Implementation must consider the generation of random numbers and the protection of shares.

Research on threshold Visual Secret Sharing in 2024 also demonstrated that systems can be designed using specific access rules. For example, a minimum of (k) out of (n) shares may be required for reconstruction. This approach allows organizations to determine the minimum number of authorized parties required before information can be recovered. Such a mechanism is relevant to documents that require approval from multiple parties.

Based on previous studies, two major approaches can be identified. The first approach uses digital signatures to ensure data authentication and integrity. The second approach uses Visual Cryptography or visual secret sharing to distribute secret information. Research that integrates Ed25519 as a digital signature mechanism with Visual Cryptography as a mechanism for distributing document validation information still provides an opportunity for further development.

This study addresses this research opportunity by designing a digital document validation mechanism that integrates Ed25519 and a Visual Cryptography Sharing Scheme. Ed25519 is used to sign a digital representation of the document. Visual Cryptography is used to divide selected authentication information into several shares. Therefore, the validation process does not depend solely on the digital signature but also incorporates an additional information distribution mechanism.

The main contribution of this study is the design of an integrated cryptographic mechanism in which the two methods perform complementary functions. Ed25519 serves as an authentication and integrity verification mechanism, while Visual Cryptography serves as a mechanism for distributing validation information. The study also develops testing scenarios involving original documents, modified documents, invalid signatures, incomplete shares, and share reconstruction.

II. BACKGROUND / LITERATURE REVIEW

A. Digital Documents

A digital document is information created, stored, and processed electronically. Digital documents may include PDF files, text documents, images, electronic certificates, official letters, and other digital formats.

The main challenge in digital document distribution is ensuring that the received document is identical to the document originally issued. Therefore, a system must be able to distinguish between an authentic document and a modified document.

B. Digital Signature

A digital signature is a cryptographic mechanism used to establish a relationship between data, the owner of a private key, and a signature value. In general, three main processes are involved:

1. Key pair generation.
2. Signature generation.
3. Signature verification.

Let (M) represent a message or document representation. The signing process can be expressed as:

[S=Sign(SK,M)]

where:

- (M) = document data or message,
- (SK) = private key,
- (S) = digital signature.

Verification is performed using:

[Verify(PK,M,S)]

where:

- (PK) = public key,
- (M) = document data,
- (S) = digital signature.

The verification result is either valid or invalid.

C. Ed25519

Ed25519 is an EdDSA variant based on the Edwards25519 curve. The algorithm was designed for digital signatures and has been adopted in various cryptographic implementations.

In a standard implementation, the key pair consists of a private key and a public key. An Ed25519 signature has a fixed size of 64 bytes, while the public key has a 32-byte representation.

The conceptual process can be expressed as:

[SK \rightarrow PK]

followed by:

[M+SK \rightarrow Signature]

and:

[M+PK+Signature \rightarrow Valid/Invalid]

Shankar et al. demonstrated the use of Ed25519 for digital document authentication and analyzed key generation, signing, and verification processes [6].

D. Document Hashing

In the proposed system, the document does not need to be directly processed as raw data for validation. Instead, the document can be represented using a hash value.

Let:

[H=SHA-256(D)]

where:

- (D) = document,
- (H) = document hash value.

If the document is modified:

[D \neqD']

then:

[SHA-256(D) \neq SHA-256(D')]

assuming no hash collision occurs.

The resulting hash value can then be used as the data to be digitally signed.

E. Visual Cryptography

Visual Cryptography is a secret-sharing technique that divides visual information into several shares. In a ((k,n)) scheme, at least (k) out of (n) shares are required to reconstruct the secret. In simplified form:

[S=VC(Secret)]

produces:

[S_1,S_2,...,S_n]

The reconstruction process is:

[Secret=Reconstruct(S_i,...,S_j)]

and can only be performed when the number of shares satisfies the predefined access rule.

Research in 2024 demonstrated that ((k,n)) constructions can be used to control the minimum number of shares required for reconstruction. This concept is relevant to systems requiring distributed authorization.

F, Integration of Ed25519 and Visual Cryptography

The proposed system uses the two methods for different purposes. Ed25519 does not replace Visual Cryptography. Instead, they are positioned at different stages of the validation process.

TABLE I. TECHNOLOGY FUNCTION

Technology	Function
SHA-256	Generates a document hash
Ed25519	Generates and verifies digital signatures
Visual Cryptography	Divides validation information into shares
Public Key	Verifies digital signatures
Shares	Provide additional validation information

This integration forms the basis of the proposed system architecture.

III. RESEARCH METHODOLOGY

This study uses a research and development approach. The research stages consist of problem identification, literature review, system requirements analysis, system design, implementation, testing, and result analysis.



Figure 1. Research Stages

The architecture separates authentication from information sharing. The digital signature verifies the relationship between the document and the private key owner. Visual Cryptography controls the distribution of additional validation information.

A. Functional Requirements

The functional requirements are presented in Table 2.

TABLE II. FUNCTIONAL REQUIREMENTS

No.	Requirement	Description
1	Document upload	User uploads a document
2	Key generation	System generates Ed25519 keys
3	Document hashing	System generates document hash
4	Signing	System generates a digital signature
5	Share generation	System generates shares
6	Verification	System verifies the document
7	Reconstruction	System reconstructs validation information
8	Modification detection	System detects modified documents

B. Non-Functional Requirements

The system must:

1. Use documented cryptographic algorithms.
2. Separate private and public keys.
3. Store private keys securely.
4. Reject invalid signatures.
5. Detect document modifications.
6. Reject reconstruction when the required number of shares is unavailable.
7. Record validation results.

IV. RESULTS AND DISCUSSION

A. System Architecture Design

The proposed system consists of five major components: the document module, hash module, Ed25519 module, Visual Cryptography module, and verification module.

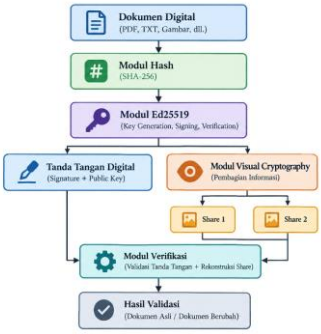


Figure 2. System Architecture Design

The architecture separates authentication from information sharing. The digital signature verifies the relationship between the document and the private key owner. Visual Cryptography controls the distribution of additional validation information.

B. ED25519 ALGORITHM DESIGN

a. Key Generation

The system generates a key pair:

$$[(SK,PK)=KeyGen()]$$

The private key is used for signing, while the public key is used for verification.

The private key must not be distributed to other parties. The public key can be provided to parties responsible for document verification.

b. Hash Generation

The document is first processed using SHA-256:

$$[H_D=SHA256(D)]$$

The resulting value represents the digital content of the document.

c. Signing Process

The signature is generated using:

$$[Sig=Sign(SK,H_D)]$$

The result is a digital signature associated with the document and the private key.

d. Verification Process

When a document is received, the system calculates:

$$[H_D'=SHA256(D')]$$

The system then executes:

$$[Verify(PK,H_D',Sig)]$$

If:

$$[H_D'=H_D]$$

and the signature is valid, the document is considered consistent with the signature.

If the document has been modified, the hash value changes and the signature verification becomes invalid.

C. VISUAL CRYPTOGRAPHY SHARING SCHEME DESIGN

The study initially applies a ((2,2)) scheme. This means that two shares are required for reconstruction.

Let the secret information be:

$$[S]$$

which is divided into:

$$[S_1,S_2]$$

with:

$$[Reconstruct(S_1,S_2)=S]$$

while:

$$[Reconstruct(S_1)\backslash neq\ S]$$

and:

$$[Reconstruct(S_2)\backslash neq\ S]$$

In the implementation, the shared information may consist of a QR Code, validation token, or visual representation of signature metadata. The specific information should be selected according to the requirements of the system.

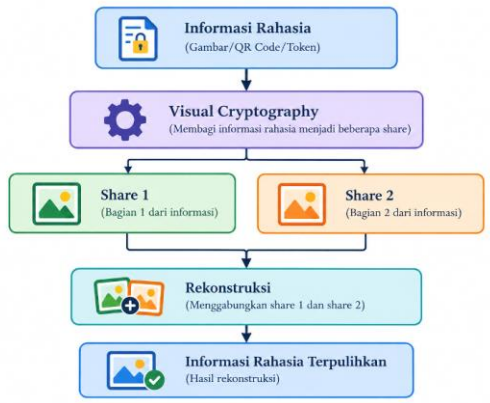


Figure 3. Visual Cryptography Mechanism

D. SYSTEM IMPLEMENTATION

The system can be implemented using Python because cryptographic libraries supporting Ed25519 are available. The system components include:

TABLE III. SYSTEM COMPONENTS

Component	Recommended Technology
Programming language	Python
Digital Signature	Ed25519
Hash	SHA-256
Visual Cryptography	Python Image Processing
Database	SQLite/MySQL
Interface	Flask or Streamlit
Document	PDF
Operating system	Windows/Linux/macOS

The system interface may provide the following menus:

1. Upload Document.
2. Generate Key.
3. Sign Document.
4. Generate Share.
5. Verify Document.
6. Reconstruct Share.
7. Validation Result.
8. Verification History.

E. TESTING SCENARIOS

Testing is conducted to ensure that each system function operates according to the design.

TABLE IV. FUNCTIONAL TESTING SCENARIOS

No.	Scenario	Condition	Expected Result
1	Document upload	Valid PDF	Document accepted
2	Key generation	Key unavailable	Key generated successfully
3	Hashing	Original document	Hash generated successfully

4	Signing	Valid key	Signature generated
5	Verification	Original document	Valid
6	Verification	Modified document	Invalid
7	Share generation	Valid data	Shares generated
8	Reconstruction	Two shares available	Successful
9	Reconstruction	One share	Incomplete/failed
10	Signature	Modified signature	Invalid

F. TEST DATA

The test dataset can consist of several documents with different file sizes. To maintain research validity, the actual file sizes and processing times must be obtained from real experiments.

TABLE V. TEST DATASET

No.	Document	Format	Size
1	Document-A	PDF	100 KB
2	Document-B	PDF	250 KB
3	Document-C	PDF	500 KB
4	Document-D	PDF	1 MB
5	Document-E	PDF	2 MB
6	Document-F	PDF	5 MB
7	Document-G	PDF	10 MB

These sizes can be used as an initial testing scenario. In the final article, the researcher should use actual files that represent the characteristics of documents in the research environment.

G. DIGITAL SIGNATURE TEST RESULTS

The technical characteristics of Ed25519 provide several parameters that can be used for evaluation. An Ed25519 public key has a size of 32 bytes and a signature has a size of 64 bytes. Therefore, the authentication data size remains relatively small regardless of the document size.

TABLE VI. ED25519 TECHNICAL PARAMETERS

Parameter	Value
Public key size	32 bytes
Signature size	64 bytes
Internal hash	SHA-512
Algorithm type	Digital Signature
Key model	Public-key cryptography
Verification	Public key

The Ed25519 and EdDSA specifications are defined in RFC 8032. Research published in 2023 also applied Ed25519 to digital document authentication.

H. DOCUMENT INTEGRITY TESTING

Integrity testing is conducted by modifying part of a document after its signature has been generated.

TABLE VI. INTEGRITY TESTING

No.	Document Condition	Hash	Signature	Status
1	Original document	Consistent	Valid	Valid
2	Name modified	Changed	Invalid	Rejected
3	Date modified	Changed	Invalid	Rejected
4	Paragraph modified	Changed	Invalid	Rejected
5	File replaced	Changed	Invalid	Rejected
6	Signature modified	Consistent	Invalid	Rejected

The table represents the expected logical behavior of the verification mechanism and should not be interpreted as actual experimental results until the system has been executed. In the final article, these results must be supported by actual system testing.

.

I. CRYPTOGRAPHY TEST RESULTS

Visual Cryptography testing evaluates share generation and reconstruction.

TABLE VIII. VISUAL CRYPTOGRAPHY TESTING

No.	Share 1	Share 2	Result
1	Available	Available	Reconstruction successful
2	Available	Missing	Reconstruction incomplete
3	Missing	Available	Reconstruction incomplete
4	Valid share	Valid share	Information reconstructed
5	Valid share	Modified share	Validation fails/requires checking

The ((2,2)) scheme requires both shares for reconstruction. This principle is consistent with threshold visual secret-sharing approaches developed in Visual Cryptography research.

J. PROCESSING TIME TESTING

Processing time measurements are required to evaluate system efficiency.

The measured parameters include:

[T_{sign}]

for signing time,

[T_{verify}]

for verification time,

[T_{share}]

for share generation time, and:

[T_{reconstruct}]

for reconstruction time.

TABLE IX. PROCESSING TIME TEST FORMAT

File Size	Signing (ms)	Verification (ms)	Share Generation (ms)	Reconstruction (ms)
100 KB	Experimental result	Experimental result	Experimental result	Experimental result
250 KB	Experimental result	Experimental result	Experimental result	Experimental result
500 KB	Experimental result	Experimental result	Experimental result	Experimental result
1 MB	Experimental result	Experimental result	Experimental result	Experimental result
2 MB	Experimental result	Experimental result	Experimental result	Experimental result
5 MB	Experimental result	Experimental result	Experimental result	Experimental result
10 MB	Experimental result	Experimental result	Experimental result	Experimental result

This table should be filled using actual experimental measurements. Each scenario should ideally be tested at least 10 times, followed by calculation of the mean and standard deviation.

The mean is calculated using:

$$\bar{x}=\frac{\sum_{i=1}^{n}x_i}{n}$$

The standard deviation is calculated using:

$$s=\sqrt{\frac{\sum_{i=1}^{n}(x_i-\bar{x})^2}{n-1}}$$

.

K. MODIFICATION DETECTION TESTING

The following testing scenarios are used to evaluate the system's ability to detect document modifications.

TABLE X ATTACK SCENARIOS AND SYSTEM RESPONSES

No.	Scenario	Modification	System Response
1	Text modification	Document content changed	Signature invalid
2	Date modification	Content changed	Signature invalid
3	Identity modification	Name/ID changed	Signature invalid
4	File replacement	Different file used	Signature invalid
5	Signature forgery	Signature replaced	Signature invalid
6	Incomplete shares	One share missing	Reconstruction fails
7	Modified share	Share content changed	Validation should fail

These tests are important because the study should not only demonstrate that a signature can be generated. The system must also be able to distinguish valid documents from documents that have been modified.

L. DISCUSSION

The proposed design demonstrates that Ed25519 can provide the primary mechanism for establishing the relationship between a document and the owner of the private key. The document is first represented by a hash value, which is then digitally signed. With this approach, modifications to the document produce a different hash representation and cause signature verification to fail.

Hashing also provides advantages in data management. The system does not need to store the entire document as part of the signature information. Instead, the system can maintain the document, hash value, digital signature, and required key information. This approach is consistent with the general purpose of digital signatures in detecting data modifications and authenticating the signer.

Ed25519 was selected because it provides a fixed-size signature. The signature size does not increase proportionally with the document size. This characteristic keeps authentication information relatively small even when documents vary in size. Shankar et al. also demonstrated the application of Ed25519 for digital document authentication [6].

Visual Cryptography provides a different function. It does not replace the digital signature. Instead, it divides selected information into several shares. The information can serve as an additional layer in the validation process. This approach provides an information distribution mechanism in which no single party possesses all validation information.

The integration of the two methods is therefore an important aspect of the proposed design. If only Ed25519 is used, the system can verify document integrity and signature authenticity. If only Visual Cryptography is used, the system can distribute secret information but does not directly establish a digital relationship between the document and the private key owner. Combining the two approaches allows both functions to operate within a unified security mechanism.

Previous research supports the use of Visual Cryptography for authentication. Zhang and Gu emphasized the importance of share authentication [11], while Valisireddy et al. applied Visual Secret Sharing to online document security [9]. Yan et al. also demonstrated the integration of public-key cryptography with image secret sharing [10]. These studies provide a conceptual basis for combining secret sharing and public-key cryptography within a security system.

However, Visual Cryptography also has limitations. Fu et al. demonstrated that information leakage related to random number sequences can affect the security of certain Visual Cryptography constructions [2]. Therefore, the implementation must consider the quality of the random number source and the protection of generated shares. Shares should not automatically be considered secure simply because they are not directly readable.

Share size is another important consideration. Some Visual Cryptography schemes introduce pixel expansion, which causes the shares to become larger than the original image. Research on Visual Cryptography from 2021 to 2024 shows that efficiency, reconstruction quality, and share security remain active research topics. Therefore, future research should evaluate share size as an important performance parameter.

The ((2,2)) scheme used in this initial study has a simple structure. Two shares are required to reconstruct the information. This structure is appropriate for demonstrating the

integration concept. However, organizations involving multiple authorized parties may require a ((k,n)) scheme. For example, three out of five authorized parties could be required to perform reconstruction.

From a security perspective, the proposed mechanism provides several layers of verification. The first layer is the document hash. The second layer is the Ed25519 digital signature. The third layer is the sharing mechanism. These layers serve different purposes, reducing dependence on a single security mechanism.

Nevertheless, this study does not claim that combining two methods automatically makes a system more secure than all alternative approaches. Security must be demonstrated through testing and threat analysis. Testing should include document manipulation, signature forgery, public-key replacement, share manipulation, share loss, and unauthorized use of shares. Future experiments should include comparisons with other digital signature algorithms. RSA and ECDSA can be considered under the same testing conditions. The parameters may include signing time, verification time, signature size, key size, and document modification detection. All algorithms should be evaluated under the same hardware and software environment.

NIST's publication of the Module-Lattice-Based Digital Signature Standard, or ML-DSA, also demonstrates the continued development of digital signature technologies [13]. Ed25519 remains relevant as an elliptic-curve-based digital signature mechanism, while future studies may investigate interoperability or comparisons with post-quantum signature algorithms.

Therefore, the contribution of this research should be positioned as an integrated document validation mechanism rather than as a claim that Ed25519 or Visual Cryptography is a newly developed technology. The research novelty lies in how the two mechanisms are designed to perform complementary functions in digital document validation.

.

M. SECURITY ANALYSIS

Security analysis is conducted based on several potential threats.

TABLE XII. THREAT ANALYSIS

Threat	Countermeasure
Document modification	SHA-256 + Ed25519
Signature forgery	Private key protection
Unauthorized signature use	Public-key verification
Loss of one share	Threshold sharing
Share modification	Share validation
Single-share access	Reconstruction is not possible
Document replacement	Hash mismatch
Private-key leakage	Secure key storage

The private key is the most sensitive component of the system. If an unauthorized party obtains the private key, that party may generate new signatures that can be verified using the same public key. Therefore, the implementation must separate private-key storage from document storage.

Visual Cryptography shares also require protection. Each share should include an identity or validation mechanism that enables the system to detect unauthorized shares.

V. CONCLUSION

This study designed and implemented a digital document authenticity validation mechanism by integrating an Ed25519-based digital signature with a Visual Cryptography Sharing Scheme. Ed25519 is used to generate and verify digital signatures associated with the document hash representation. This mechanism enables the system to detect modifications made to documents after signing.

Visual Cryptography is used as an additional mechanism for dividing validation information into multiple shares. The initial design applies a ((2,2)) scheme, in which two shares are required for reconstruction. This approach provides an information distribution mechanism that complements the digital signature function.

The integration of Ed25519 and Visual Cryptography provides a layered security design. Ed25519 focuses on document authentication and integrity, while Visual Cryptography focuses on validation information distribution. The proposed approach can be applied to academic documents, certificates, official letters, administrative documents, and other digital documents that require authenticity verification.

The proposed functional testing includes original documents, modified documents, invalid signatures, incomplete shares, and modified shares. For the final version of the study, these tests should be complemented by empirical measurements of processing time, data size, validation success rate, and document manipulation detection.

Future research can extend the system to a ((k,n)) sharing scheme, compare Ed25519 with RSA and ECDSA, evaluate performance across different document sizes, and incorporate timestamping and Public Key Infrastructure mechanisms. These developments can increase the applicability of the system in organizational environments requiring multi-party digital document validation.

ACKNOWLEDGMENTS

The author extends sincere gratitude to STMIK Mercusuar and the Department of Informatics Engineering at Universitas Jayabaya for the academic support and environment that facilitated the completion of this research. The author also appreciates the support, suggestions, and constructive discussions provided by colleagues and other parties who contributed to the development and evaluation of the proposed digital document validation system.

Furthermore, the author acknowledges the role of academic resources, technical facilities, and scientific references that supported the implementation of the Ed25519 digital signature and the Visual Cryptography approach in this study. Finally, appreciation is expressed to all parties who contributed—

whether directly or indirectly—to the completion of this research and the preparation of this manuscript.

REFERENCES

[1] H. Chihi, A. Chahboun, and S. Mezroui, "An enhanced visual cryptography framework for smart lock authentication," *Discover Internet of Things*, vol. 5, Art. no. 136, 2025, doi: 10.1007/s43926-025-00248-9.

[2] Z. Fu, X. Li, L. Fang, Y. Feng, and B. Yu, "Security issues in visual cryptography scheme with known random number sequence," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, Art. no. 101983, 2024, doi: 10.1016/j.jksuci.2024.101983.

[3] Y. Kang, S. Kanwal, S. L. Pu, B. L. Liu, and D. W. Zhang, "Ghost imaging-based optical multilevel authentication scheme using visual cryptography," *Optics Communications*, vol. 526, Art. no. 128896, 2023, doi: 10.1016/j.optcom.2022.128896.

[4] A. Muhammed and A. R. Pais, "A secure fingerprint template generation mechanism using visual secret sharing with inverse halftoning," *Journal of Visual Communication and Image Representation*, vol. 94, Art. no. 103854, 2023, doi: 10.1016/j.jvcir.2023.103854.

[5] J. S. Pan, T. Liu, H. M. Yang, B. Yan, S. C. Chu, and T. Zhu, "Visual cryptography scheme for secret color images with color QR codes," *Journal of Visual Communication and Image Representation*, vol. 82, Art. no. 103405, 2022, doi: 10.1016/j.jvcir.2021.103405.

[6] G. Shankar, L. H. Ai-Farhani, P. A. C. Angelin, P. Singh, A. Alqahtani, A. Singh, G. Kaur, and I. A. Samori, "Improved multisignature scheme for authenticity of digital document in digital forensics using Edward-Curve digital signature algorithm," *Security and Communication Networks*, vol. 2023, Art. no. 2093407, 2023, doi: 10.1155/2023/2093407.

[7] A. Sherine and G. Peter, "CMY color spaced-based visual cryptography scheme for secret sharing of data," *Wireless Communications and Mobile Computing*, vol. 2022, Art. no. 6040902, 2022, doi: 10.1155/2022/6040902.

[8] S. Sugianto, J. Jimmy, A. Suwandhi, W. Wilianto, and B. Benny, "Analisis metode Secret Sharing Asmuth-Bloom dan Visual Cryptography," *Jurnal Minfo Polgan*, vol. 13, no. 1, pp. 213–218, 2024, doi: 10.33395/jmp.v13i1.13541.

[9] J. Valisireddy, K. A. Reddy, R. Elumalai, L. N. Mohan, and G. S. G. N. Anjaneyulu, "Secured authentication of online documents using visual secret sharing on QR code," *Journal of Integrated Science and Technology*, vol. 11, no. 4, Art. no. 568, 2023.

[10] X. Yan, L. Li, J. Chen, and L. Sun, "Public key based bidirectional shadow image authentication without pixel expansion in image secret sharing," *Frontiers of Information Technology & Electronic Engineering*, vol. 24, no. 1, pp. 88–103, 2023, doi: 10.1631/FITEE.2200118.

[11] D. Zhang and Z. Gu, "A high-quality authenticatable visual secret sharing scheme using SGX," *Wireless Communications and Mobile Computing*, vol. 2021, Art. no. 6660709, 2021, doi: 10.1155/2021/6660709.

[12] X. Zhong, L. Xiong, and Z. Xia, "A secure visual secret sharing scheme with authentication based on QR code," *Journal on Big Data*, vol. 3, no. 2, pp. 85–95, 2021, doi: 10.32604/jbd.2021.018618.

[14] S. Josefsson and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)," RFC 8032, Internet Engineering Task Force, Jan. 2017, doi: 10.17487/RFC8032.

[13] National Institute of Standards and Technology, *Module-Lattice-Based Digital Signature Standard*, FIPS PUB 204. Gaithersburg, MD, USA: NIST, 2024.