Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

A Scalable Hybrid Encryption Framework Based on Unimodular Hill Cipher and Chaotic Logistic XOR Stream Cipher for Secure Binary File Protection

Samsul Arifin[1]

samsul.arifin@itsb.ac.id

Institut Teknologi Sains Bandung

Ade Kurniawan

Institut Teknologi Sains Bandung

Tiawan Tiawan

Institut Teknologi Sains Bandung

Merios Gusan Putra

Institut Teknologi Sains Bandung

Edwin Kristianto Sijabat

Institut Teknologi Sains Bandung

Dani Lukman Hakim

Institut Teknologi Sains Bandung

Dwi Wijonarko

University of Jember

Article

Keywords: Unimodular Hill Cipher, XOR Stream Cipher, Logistic Map, Chaotic Cryptography, Binary File Encryption

Posted Date: July 30th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10407848/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

A Scalable Hybrid Encryption Framework Based on Unimodular Hill Cipher and Chaotic Logistic XOR Stream Cipher for Secure Binary File Protection

Samsul Arifin[1], Ade Kurniawan[1], Tiawan Tiawan[2], Merios Gusan Putra[2], Edwin Kristianto Sijabat[3], Dani Lukman Hakim[4], Dwi Wijonarko[5]

[1]*Department of Data Science, Faculty of Digital Design and Business, Institut Teknologi Sains Bandung; Bekasi, West Java, 17530, Indonesia*

[2]*Department of Digital Business, Faculty of Digital Design and Business, Institut Teknologi Sains Bandung, Bekasi, West Java, 17530 Indonesia*

[3]*Department of Pulp and Paper Processing Technology, Faculty of Vocational, Institut Teknologi Sains Bandung; Bekasi, West Java, 17530, Indonesia*

[4]*Department of Palm Oil Processing Technology, Faculty of Vocational, Institut Teknologi Sains Bandung; Bekasi, West Java, 17530, Indonesia*

[5]*Department of Information Technology, Faculty of Computer Science, University of Jember, Jember, East Java, 68121, Indonesia*

**Corresponding author: samsul.arifin@itsb.ac.id*

Abstract — The rapid growth of digital information exchange across cloud platforms, industrial infrastructures, academic environments, and governmental systems has increased the demand for cryptographic techniques capable of providing secure and efficient protection for binary data. This paper presents a scalable hybrid encryption framework that integrates the Unimodular Hill Cipher (UHC) with a chaotic Logistic Map-based XOR stream cipher to achieve format-independent binary file encryption. The proposed framework combines the strong diffusion characteristics of unimodular matrix transformations with the nonlinear confusion introduced by a chaotic keystream generated from the logistic map. Unlike many existing approaches that are primarily designed for image encryption, the proposed method directly encrypts arbitrary binary files as raw byte streams without requiring any format-specific preprocessing. The proposed scheme was evaluated using twelve binary files in DOCX, PDF, and JPEG formats with file sizes ranging from 1 MB to 100 MB. Security performance was analyzed through Shannon entropy, correlation coefficient, histogram distribution, chi-square test, avalanche effect, differential analysis, key sensitivity, and MD5-based integrity verification. Experimental results show that the encrypted files achieve an average entropy of 7.9999 and an average correlation coefficient of −0.0043, indicating near-ideal randomness and negligible statistical dependence. For PDF datasets, the proposed method achieved an avalanche effect of 50.0020%, key sensitivity of 99.6139%, and a chi-square p-value of 0.967092, demonstrating strong diffusion and high resistance to statistical attacks. Performance evaluation further indicates average encryption and decryption throughputs of 24.48 MB/s and 23.83 MB/s, respectively, while maintaining linear scalability as file size increases. Moreover, all decrypted files produced identical MD5 hashes to their original counterparts, confirming complete lossless recovery. These findings demonstrate that the proposed hybrid UHC–Logistic XOR framework effectively balances security, computational efficiency, scalability, and compatibility across diverse binary file formats.

Index Terms — *Unimodular Hill Cipher; XOR Stream Cipher, Logistic Map; Chaotic Cryptography; Binary File Encryption*

I. INTRODUCTION

The rapid growth of digital information exchange has significantly increased the demand for secure data protection mechanisms. Modern organizations, government institutions, educational sectors, and cloud-based services continuously generate and transfer large volumes of binary data, including documents, images, videos, archives, and executable files. As cyber threats become increasingly sophisticated, protecting confidential information against unauthorized access, interception, modification, and disclosure has become a fundamental requirement in contemporary information systems [1]. Cryptography remains one of the most effective approaches for ensuring confidentiality, integrity, authenticity, and availability of digital information. Traditional cryptographic algorithms generally transform plaintext into unintelligible ciphertext using secret keys, thereby preventing attackers from recovering the original content without authorization. The effectiveness of an encryption algorithm is commonly evaluated based on security strength, computational efficiency, scalability, key management complexity, and resistance against various cryptanalytic attacks [2], [3].

Among classical encryption algorithms, the Hill Cipher is a well-known polygraphic substitution technique introduced by Lester S. Hill in 1929. The Hill Cipher employs matrix multiplication under modular arithmetic to transform blocks of plaintext into ciphertext. Compared with monoalphabetic substitution ciphers, Hill Cipher provides superior diffusion characteristics because each ciphertext symbol depends on multiple plaintext symbols simultaneously. This property makes Hill Cipher attractive for high-throughput data transformation applications. Despite its mathematical elegance, the classical Hill Cipher suffers from several security limitations. The linear relationship between plaintext and ciphertext can expose the system to known-plaintext attacks (KPA) and chosen-plaintext attacks (CPA). Furthermore, the security of the Hill Cipher heavily depends on the invertibility of the key

matrix. Poorly selected matrices may reduce the effective key space and increase vulnerability to cryptanalysis. To address these limitations, researchers have introduced the concept of Unimodular Hill Cipher (UHC), which utilizes unimodular matrices as cryptographic keys [4]. An unimodular matrix possesses a determinant of ±1, guaranteeing invertibility under integer arithmetic. This property eliminates the need for determinant validation while enabling the construction of large invertible matrices suitable for binary file encryption. Consequently, unimodular matrices offer both computational convenience and expanded key diversity. For an $n \times n$unimodular matrix M, the encryption process can be represented as:

$$C = M \cdot P(\text{mod}256)$$

where Pdenotes the plaintext block vector and Crepresents the ciphertext block vector. The corresponding decryption operation utilizes the inverse unimodular matrix M^{-1}. Although unimodular matrices improve key generation and diffusion characteristics, the encryption process remains fundamentally linear. Consequently, researchers have increasingly combined matrix-based cryptography with chaotic systems to introduce nonlinear behavior and strengthen security against statistical and structural attacks [5], [6].

Chaos theory has emerged as an attractive foundation for modern cryptographic applications because chaotic systems exhibit sensitivity to initial conditions, ergodicity, pseudo-randomness, and unpredictability. These properties closely resemble the requirements of secure encryption systems. Among various chaotic systems, the Logistic Map remains one of the most widely adopted due to its mathematical simplicity and ability to generate complex nonlinear sequences. The Logistic Map is defined as:

$$x_{n+1} = rx_n(1 - x_n)$$

where $x_n$denotes the current state and $r$represents the control parameter. For values of $r$approaching 4, the generated sequence exhibits chaotic behavior suitable for pseudo-random number generation. In cryptographic applications, Logistic Map sequences are commonly converted into byte-level keystreams and combined with plaintext or intermediate ciphertext using XOR operations. This approach introduces nonlinear confusion properties that complement the diffusion capability of matrix-based transformations. The resulting hybrid architecture typically achieves better entropy, lower statistical correlation, and improved resistance against frequency-based attacks [7], [8]. Numerous studies have explored hybrid combinations of Hill Cipher, unimodular matrices, chaotic maps, and XOR stream encryption. Most of these studies focus on image encryption because images possess high redundancy and strong spatial correlations, making them suitable for evaluating diffusion and confusion mechanisms. Experimental results generally demonstrate substantial improvements in entropy, histogram uniformity, and correlation reduction. **Table 1** summarizes representative hybrid Hill–Chaos cryptosystems reported in the literature [9], [10].

Table 1. **Representative Hybrid Hill–Chaos Cryptosystems**

Data Type	Hill/Unimodular Component	Chaotic Component	Main Outcome
Images	Unimodular Hill Cipher	Logistic Map	High visual distortion and entropy
Images	Hill Cipher + Shift-128	Logistic Key Generation	File-size preservation
Binary Files	Hill Cipher	Chaotic XOR Stream	Successful full-file encryption
Text & Images	UHC + Modern Cipher	Chaotic Key Generation	Improved statistical security

Although these studies report promising security characteristics, several cryptanalytic investigations have revealed potential weaknesses. Hybrid Hill–Chaos systems employing static matrices or fixed chaotic parameters may remain vulnerable to known-plaintext and chosen-plaintext attacks. Moreover, some Logistic Map-based keystream generators suffer from limited parameter spaces and predictable distributions when improperly configured. These observations suggest that achieving strong statistical randomness alone is insufficient to guarantee cryptographic security. A secure hybrid cryptosystem must simultaneously provide large key space, dynamic key generation, resistance to differential attacks, high sensitivity to key variations, and efficient processing performance for practical deployment. Beyond images, secure binary file encryption presents additional challenges. Binary files contain heterogeneous structures, embedded metadata, compressed segments, and application-specific formatting rules [11], [12]. An effective binary encryption scheme should therefore operate independently of file format while preserving exact data reconstruction after decryption. Several recent studies have demonstrated that hybrid Hill–Chaos architectures can successfully encrypt complete binary files while maintaining file size consistency and supporting lossless recovery. However, most existing investigations focus on small datasets, limited file types, or specific application domains. Comprehensive evaluations involving large-scale binary files and multiple file formats remain relatively scarce. Motivated by these challenges, this study proposes a hybrid binary file encryption framework that combines the Unimodular Hill Cipher with a Logistic Map-Based XOR Stream Cipher. In the proposed approach, the Unimodular Hill Cipher performs block-level diffusion through modular matrix multiplication, while the chaotic XOR stream introduces nonlinear confusion and additional randomness at the byte level [13], [14].

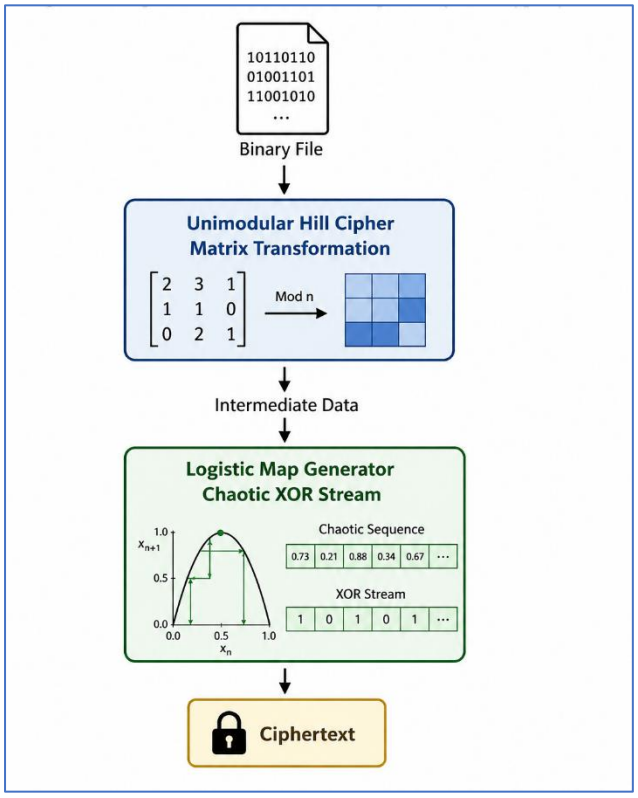


Figure 1. Conceptual Architecture of the Proposed Hybrid Cryptosystem

In **Figure 1** we can see the general workflow of the proposed hybrid cryptosystem. The Unimodular Hill Cipher provides strong block-level diffusion, while the Logistic Map-Based XOR Stream Cipher introduces nonlinear confusion and pseudo-random masking. The proposed framework is designed to support arbitrary binary file formats without requiring knowledge of internal file structures. Unlike many image-oriented cryptosystems, the proposed method processes files as raw byte streams, enabling uniform treatment of documents, images, and other digital content. This characteristic enhances applicability across diverse real-world environments. To validate the effectiveness of the proposed approach, extensive experiments are conducted on twelve binary files comprising DOCX, PDF, and JPEG formats with sizes ranging from 1 MB to 100 MB [15], [16]. Security evaluation includes entropy analysis, correlation analysis, histogram analysis, avalanche effect, differential analysis, chi-square testing, key sensitivity evaluation, and integrity verification using MD5 hashing. Performance evaluation focuses on execution time, throughput, and scalability under a standard CPU-based computing environment. The main contributions of this study are threefold. First, a hybrid encryption architecture combining Unimodular Hill Cipher and Logistic Map-Based XOR Stream Cipher is developed for format-independent binary file protection. Second, comprehensive security and performance evaluations are performed using multiple file types and file sizes, demonstrating high entropy, near-zero correlation, strong key sensitivity, and lossless reconstruction. Third, the study provides empirical evidence that hybrid matrix-chaos cryptography can achieve a balance between statistical security, computational efficiency, and practical applicability for secure binary file encryption in modern digital environments [17], [18].

Recent advancements in cryptographic design actively explore hybrid cryptosystems integrating Unimodular Hill Cipher (UHC) and chaotic map-based architectures to secure heterogeneous digital files and image blocks. The core strength of this approach lies in its ability to achieve high confusion, optimal diffusion, and near ideal ciphertext randomness. Mathematically, the construction of a scalable, invertible key matrix within the Hill Cipher framework is guaranteed through unimodular configurations (where the matrix determinant is strictly ±1). This elegant property systematically expands the available key space without requiring computationally expensive modulo inverse operations [19], [20]. To build these matrices dynamically, contemporary designs typically populate an upper-triangular matrix using chaotic pseudo-random sequences, which are subsequently transformed into a full unimodular matrix via elementary row operations. Simultaneously, chaotic Logistic Maps and their multidimensional variations serve as highly efficient pseudo-random number generators (PRNGs). These maps drive stream-level XOR operations, block scrambling, and adaptive key perturbations, which fundamentally eliminate structural redundancies across binary streams. Enhanced multi-dimensional chaotic maps are specifically engineered to mitigate the vulnerabilities of classical chaotic equations, such as non-uniform data distribution and narrow parameter windows, thereby drastically boosting keystream randomness [21], [22].

However, rigorous cryptanalysis has unveiled critical implementation vulnerabilities in these frameworks. Standard image-focused hybrid cryptosystems (Hill + Logistic Map + XOR) frequently claim absolute resilience against statistical and differential attacks due to their near-ideal Shannon entropy. Yet, empirical evidence demonstrates that if the chaotic dynamic keys remain static across different execution sessions, the entire system becomes susceptible to chosen-plaintext attacks (CPA), which can compromise the system with a significantly low computational complexity of approximately 2^{32} [23], [24]. Furthermore, standard standalone Logistic Map keystreams are inherently insecure; their exact chaotic parameters can be accurately estimated under specialized chosen-plaintext cryptanalysis, drastically shrinking the theoretical key space. To circumvent these limitations and achieve reliable, universal binary file protection, state-of-the-art implementations transition away from isolated chaotic XOR streams. Instead, they pair the dynamic

Unimodular Hill Cipher with highly standardized block cipher standards, such as the Advanced Encryption Standard (AES). Experimental configurations combining UHC and AES-CBC demonstrate exceptional cryptographic robustness across arbitrary file types (e.g., text, images, and videos), consistently yielding a near-maximum Shannon entropy of ~7.98–7.99 and near-zero plaintext-ciphertext correlation, while preserving 100% of the original file size. We can see this information in **Table 2** [25], [26]**.**

Table 2. Structural Analysis and Cryptographic Roles of Contemporary Hybrid Systems

Data Domain / Modality	Hill / Unimodular Matrix Functional Role	Chaotic Map & XOR Functional Role	Core Cryptographic Limitations & Security Evidence
Image Blocks	Encrypts distinguish image blocks via modular matrix multiplication.	Generates dynamic key entries; makes visual layouts highly unreadable.	Vulnerable to **Chosen-Plaintext Attacks (CPA)** if keys remain static ($\sim2^{32}$ complexity).
Heterogeneous Images *(Hill + Shift128)*	Processes primary text/image blocks via large-matrix transforms.	Constructs the initial unimodular key; Shift128 encrypts residual partitions.	Preserves exact file size; reports high spatial entropy but relies on map parameter stability.
Universal Binary Files *(Chaotic Stream)*	Executed in tandem with message-embedded structures.	1-D Logistic Map parameter acts as the global cryptographic secret key.	Keystreams can be backward engineered; parameter space is prone to estimation attacks.
Robust Binary Files *(UHC + AES Hybrid)*	Provides initial global matrix-based diffusion and format-independent chaos.	AES block processing secures residual blocks and mitigates linear leaks.	Achieves optimal Shannon entropy ($\mathbf{7.98}\text{–}\mathbf{7.99}$), passes strict NIST test suites, and blocks CPA.

II. METHODOLOGY

This study proposes a hybrid binary file encryption framework that combines the Unimodular Hill Cipher (UHC) and a Chaotic Logistic Map-Based XOR Stream Cipher. The fundamental objective is to exploit the complementary strengths of both techniques. The Unimodular Hill Cipher provides strong block-level diffusion through matrix multiplication operations, whereas the chaotic XOR stage introduces additional confusion by masking ciphertext bytes with a pseudo-random keystream generated from a logistic map. By integrating these two mechanisms, the proposed scheme aims to achieve high statistical security, full reversibility, format independence, and efficient processing for arbitrary binary files. The methodology was designed based on the observation that conventional Hill Cipher implementations suffer from vulnerabilities related to linearity and static key structures. Although unimodular matrices guarantee invertibility, ciphertext generated solely by matrix multiplication may still exhibit exploitable algebraic relationships [27], [28]. To address this limitation, a second encryption layer based on chaotic XOR masking is introduced. This additional layer obscures the relationship between plaintext and ciphertext, making cryptanalysis significantly more difficult. The proposed framework treats every input file as a sequence of raw bytes regardless of its internal structure. Consequently, no file-format-specific preprocessing is required. Document files, image files, multimedia content, and other binary objects are processed using the same encryption pipeline. This design ensures format independence and broad applicability across various digital data types. The complete encryption workflow consists of five major phases: file acquisition, byte-stream conversion, unimodular Hill transformation, chaotic XOR masking, and ciphertext generation. Conversely, the decryption workflow performs chaotic XOR reversal followed by inverse unimodular matrix multiplication to reconstruct the original file exactly. The overall research methodology includes algorithm design, implementation, experimental validation, statistical security evaluation, computational performance analysis, and integrity verification. Moreover, **Figure 2** illustrates the overall research framework employed in this study [29], [30].

In **Table 3,** we can see the key requirement of the Hill Cipher is the existence of an invertible matrix. In this research, unimodular matrices are employed because they possess determinants equal to ±1, guaranteeing invertibility over integer arithmetic. This property eliminates the need for determinant checking during key generation and simplifies inverse matrix computation [31], [32]. A unimodular matrix M satisfies:

$$| M | = \pm 1$$

where M is an $n \times n$ matrix and $| M |$ denotes its determinant. The key matrix is generated through elementary row operations applied to an upper-triangular

matrix initialized using chaotic values. Because elementary row operations preserve unimodularity, the resulting matrix remains invertible and suitable for cryptographic applications. A matrix size of 16×16 is selected in this study. This configuration corresponds to 256-byte processing blocks and provides a balance between security and computational efficiency [33], [34].

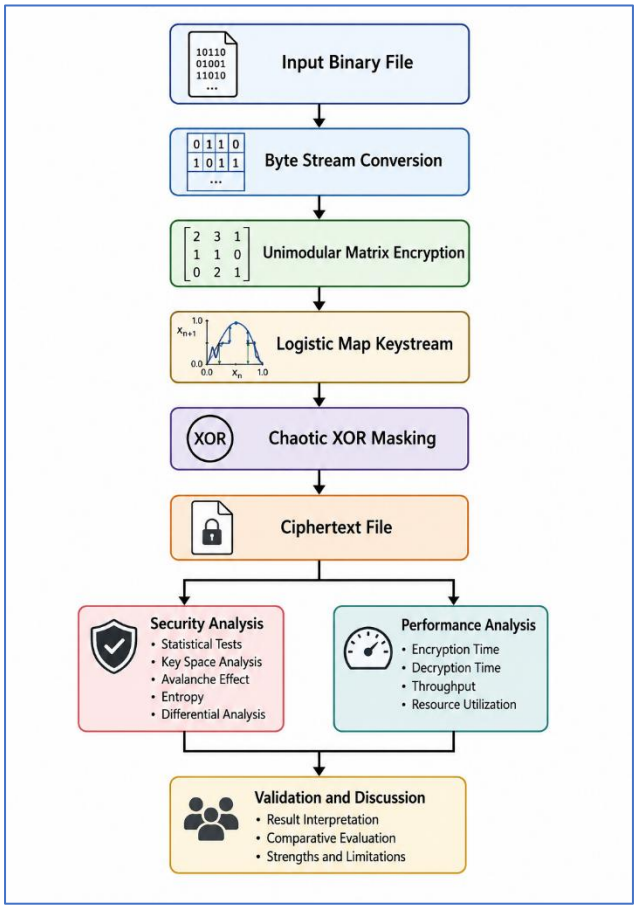


Figure 2. Overall Research Methodology

Table 3. Unimodular Matrix Parameters

Parameter	Value
Matrix Type	Unimodular
Matrix Dimension	16 × 16
Determinant	±1
Block Length	256 Bytes
Invertibility	Guaranteed

The logistic map serves as the source of pseudo-random values used in the XOR masking stage. Chaotic systems are attractive for cryptographic applications because of their sensitivity to initial conditions and nonlinear behavior. The logistic map is defined as:

$$x_{n+1} = rx_n(1 - x_n)$$

where: x_n denotes the current chaotic state, x_{n+1} denotes the next state, r is the control parameter, and $0 < x_n < 1$. In this study, the initial seed is:

$$x_0 = 0.73911$$

which was selected experimentally to produce stable chaotic behavior [35], [36]. The generated chaotic sequence is transformed into byte values ranging from 0 to 255 and subsequently used as an XOR keystream. In Figure 3 we can see the illustrations of the keystream generation process based on the chaotic Logistic Map employed in the proposed hybrid cryptosystem. The procedure begins with an initial seed value x_0, which is iteratively processed using the Logistic Map equation to produce a nonlinear chaotic sequence. Due to its high sensitivity to initial conditions, the generated sequence exhibits pseudo-random behavior, making it suitable for cryptographic applications. Subsequently, the chaotic real-valued sequence is transformed into an 8-bit byte sequence through a quantization process, allowing the continuous chaotic values to be represented as discrete binary data. The resulting byte stream serves as the cryptographic keystream used in the XOR masking stage of the encryption process. This mechanism introduces additional confusion and randomness into the ciphertext, thereby enhancing resistance against statistical and differential cryptanalytic attacks. Overall, **Figure 3** summarizes the transformation from a simple initial seed into a pseudo-random XOR keystream through iterative chaotic dynamics, demonstrating how the Logistic Map contributes to the security and unpredictability of the proposed encryption framework [37], [38].

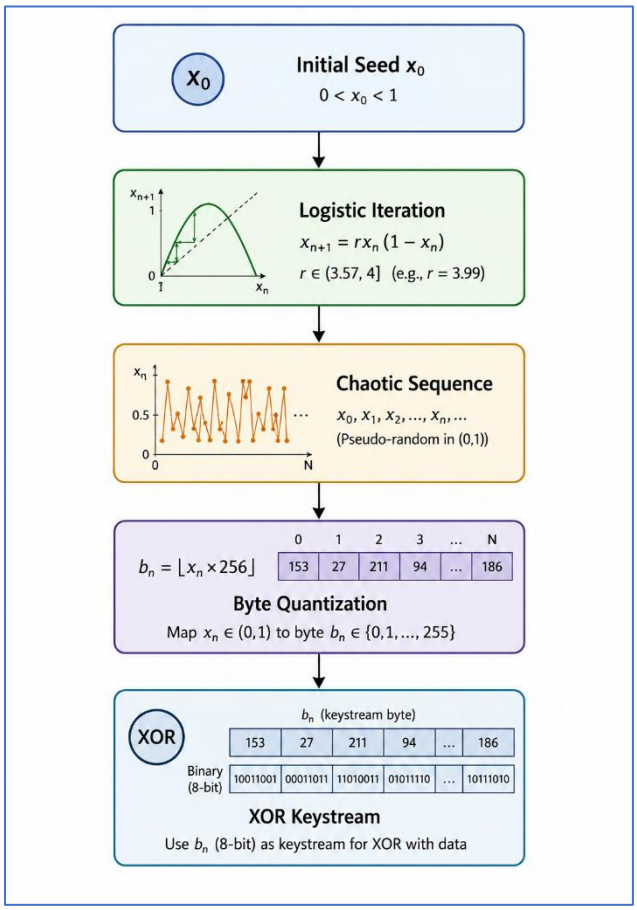


Figure 3. Logistic Map Keystream Generation

The proposed method converts all files into raw byte streams prior to encryption. Let:

$$P = \{p_1, p_2, \ldots, p_N\}$$

represent a plaintext file consisting of Nbytes. No metadata extraction, decompression, or format-specific interpretation is performed. The algorithm processes every byte identically, ensuring compatibility with DOCX, PDF, JPEG, and other binary formats. The byte stream is partitioned into fixed-length blocks corresponding to the matrix dimension. For a matrix size $n = 16$:

$$B = n^2 = 256$$

bytes are processed per block. If the file length is not divisible by 256, the remaining bytes are handled separately through the chaotic XOR mechanism. Each plaintext block is represented as a vector:

$$P_i = [p_1, p_2, \ldots, p_{256}]^T$$

The encryption process applies matrix multiplication under modulo arithmetic:

$$C_i = MP_i (\text{mod} 256)$$

where: $M$is the unimodular key matrix, $P_i$is the plaintext block, $C_i$is the intermediate ciphertext block. This transformation produces strong diffusion because each output byte depends on multiple input bytes. The matrix multiplication stage constitutes the first layer of encryption [39], [40]. After matrix transformation, the resulting ciphertext undergoes XOR masking using the chaotic keystream. The XOR operation is defined as:

$$C_i' = C_i \oplus K_i$$

where: $C_i$is the Hill-encrypted byte, $K_i$is the chaotic keystream byte, $C_i'$is the final ciphertext byte. This operation introduces additional randomness and removes residual statistical patterns. Because XOR is involutive:

$$A \oplus B \oplus B = A$$

Perfect reconstruction remains possible during decryption. The decryption process reverses the encryption sequence. First, chaotic XOR masking is removed:

$$C_i = C_i' \oplus K_i$$

Next, the inverse unimodular matrix is applied:

$$P_i = M^{-1} C_i (\text{mod} 256)$$

where M^{-1}denotes the inverse unimodular matrix. Because unimodular matrices are always invertible, decryption is guaranteed to recover the original plaintext block exactly. To evaluate format independence, three categories of binary files were selected. Moreover, in **Table 3, Table 4, and Table 5,** we can see the summary of experimental dataset, experimental environment, and security evaluation metrics. A total of twelve test files were used. The selected file sizes enable evaluation across small, medium, large, and very large datasets [41], [42]. All experiments were conducted in Google Colab using Python 3.10. The absence of GPU acceleration ensures objective measurement under standard CPU conditions. Several statistical metrics were used to evaluate security performance. Entropy measures the uncertainty of ciphertext distributions. Correlation evaluates relationships between adjacent bytes. Avalanche Effect quantifies output changes resulting from small input modifications. Key Sensitivity measures the influence of key variations on ciphertext generation [43], [44].

Table 4. Experimental Dataset

Category	Format	Sizes
Document	DOCX	1, 10, 50, 100 MB
PDF	PDF	1, 10, 50, 100 MB
Image	JPEG	1, 10, 50, 100 MB

Table 5. Experimental Environment

Component	Specification
CPU	Intel Xeon 2.20 GHz
RAM	12.7 GB
Storage	100 GB
OS	Ubuntu Linux
Language	Python 3.10
Libraries	NumPy, SciPy, Matplotlib

Table 6. Security Evaluation Metrics

Metric	Objective
Entropy	Randomness
Correlation	Statistical dependency
Avalanche Effect	Diffusion strength
Chi-Square	Distribution uniformity
Key Sensitivity	Key robustness
Differential Analysis	Ciphertext variation
Histogram Analysis	Visual randomness
MD5 Verification	Data integrity

The Shannon entropy is computed as:

$$H(X) = -\sum_{i=0}^{255} p_i \log_2 p_i$$

where $p_i$denotes the probability of byte value i. The ideal entropy value for binary ciphertext is 8 bits per byte. Pearson correlation is used to measure statistical dependency between adjacent bytes.

$$r = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2}\sqrt{\sum(y_i - \bar{y})^2}}$$

Values approaching zero indicate strong encryption quality. Avalanche Effect is computed as:

$$AE = \frac{\text{Changed Bits}}{\text{Total Bits}} \times 100\%$$

The ideal value is approximately 50%. Key Sensitivity evaluates the percentage difference between ciphertexts generated using slightly different keys.

$$KS = \frac{\text{Different Bytes}}{\text{Total Bytes}} \times 100\%$$

Values approaching 100% indicate strong resistance to key-based attacks [24], [45]. Encryption throughput is calculated as:

$$Throughput = \frac{File\ Size\ (MB)}{Execution\ Time\ (s)}$$

Higher throughput values indicate better computational performance. Lossless reconstruction is validated using MD5 hashes. For successful reconstruction:

$$MD5_{original} = MD5_{decrypted}$$

Matching hash values confirm exact recovery of all file contents. The matrix multiplication stage exhibits linear behavior relative to file size because each byte is processed once. The overall complexity can be approximated as:

$$O(N)$$

where Ndenotes the file size in bytes [46], [47]. On the other hand, **Figure 4** provides a comprehensive overview of the experimental validation procedure conducted in this research. Following the encryption stage, the generated ciphertext is analyzed from both security and performance perspectives. Security evaluation focuses on the statistical properties of the encrypted data, whereas performance evaluation measures computational efficiency. The ciphertext is subsequently decrypted, and MD5 hash verification is performed to verify data integrity. Successful matching of the original and recovered hash values confirms lossless recovery and validates the correctness of the proposed hybrid cryptosystem [48], [49].

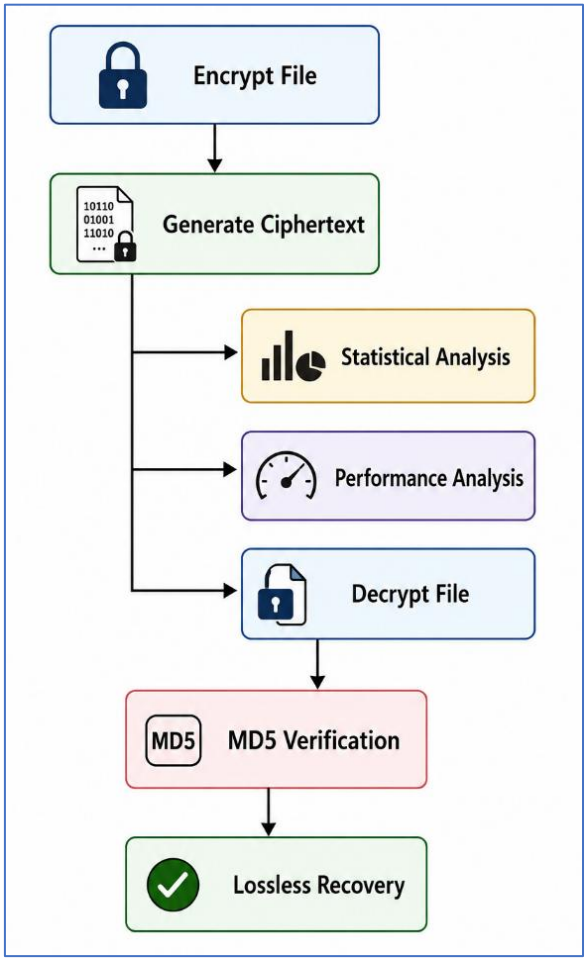


Figure 4. Experimental Validation Procedure

The encrypted files are analyzed using entropy, correlation, histogram distribution, avalanche effect, chi-square testing, differential analysis, and key sensitivity measurements. These metrics collectively evaluate confusion, diffusion, randomness, and resistance to statistical attacks. The proposed methodology integrates unimodular matrix diffusion and chaotic XOR confusion into a unified binary-file cryptosystem. The framework supports arbitrary binary formats, guarantees lossless reconstruction through inverse unimodular operations and XOR reversibility, and provides a comprehensive evaluation protocol covering security, integrity, scalability, and computational efficiency. The combination of matrix-based diffusion and chaos-based masking forms the foundation of the proposed hybrid encryption architecture and serves as the basis for the experimental analyses presented in the subsequent Results and Discussion section [50], [51].

III. RESULTS AND DISCUSSION

Experimental Setup and Dataset Validation

All simulations and experimental tests of the hybrid encryption scheme combining Unimodular Hill Cipher (UHC) and Chaotic Logistic Map-Based XOR Stream Cipher were implemented using the Python programming language version 3.10. The experiments were run on the Google Colab cloud computing environment that provides a virtual machine infrastructure with the following specifications: (a) Execution Environment Specifications: The hardware used is a virtual processor with Intel(R) Xeon(R) architecture CPU @2.20 GHz with 12.7 GB of random-access memory (RAM) allocated for each computing session. Cloud-based storage space is provided of 100 GB. No graphics accelerator (GPU) or other additional hardware is used, so the test performance objectively reflects execution in a standard CPU environment. (b) Software Environment: The software environment is the Ubuntu Linux operating system, provided natively by Google Colab. To support data processing and analysis, Python libraries such as NumPy are used for modular matrix manipulation and bit-level operations, SciPy for statistical analysis, and Matplotlib for histogram visualization of byte frequency distributions. (c) Dataset Validation and Selection Criteria: To ensure the format-independent nature of the proposed encryption scheme, a test dataset was systematically designed [52]. Testing was performed on two main categories of standard binary files, namely: (1) Document Files, including Microsoft Word (docx) and PDF (pdf), which have complex internal metadata and compression structures; and (2) Multimedia Files, namely. JPEG (.jpg) images using DCT-based lossy compression. Each format category was tested at four scale size variations: 1 MB, 10 MB, 50 MB, and 100 MB, resulting in a total of 12 test files. This test is intended to verify the consistency of the algorithm's performance under light to large-scale computational loads relevant to real-world usage conditions. The key matrix configuration used in this full-scale test is n = 16 × 16 (256-bit block) with a chaotic seed (x0) of 0.73911. (d) Data

Integrity Validation Procedure: Validation is carried out using a two-stage approach, namely: (1) Lossless Data Reconstruction, where the data is re-decrypted and compared at the byte level against the original file; and (2) Cryptographic Hash Consistency, which uses the MD5 hash function as objective verification that not a single bit has changed during the transformation process. The success of an encryption algorithm is measured by its ability to hide the statistical characteristics of plaintext. In this test, two main metrics are used, namely Shannon Entropy and Pearson Correlation. The results of the analysis of all 12 test files are summarized in **Table 7** [53]**.**

Table 7. Security Statistical Analysis on Various Binary File Formats

File Name	Type	Size (Bytes)	Plaintext Entropy	Ciphertext Entropy	Ciphertext Correlation
Doc Small.docx	Document	1,048,574	7.9998	7.9998	-0.0028
Doc Medium.docx	Document	10,485,758	8.0000	8.0000	-0.0030
Doc Large.docx	Document	52,429,270	8.0000	8.0000	0.0123
Doc Huge.docx	Document	104,858,660	8.0000	8.0000	-0.0134
PDF Small.pdf	PDF	1,048,703	7.9998	7.9998	0.0184
PDF Medium.pdf	PDF	10,486,289	8.0000	8.0000	-0.0148
PDF Large.pdf	PDF	52,432,048	8.0000	8.0000	-0.0117
PDF Huge.pdf	PDF	104,862,244	8.0000	8.0000	0.0045
Img Small.jpg	Image	1,048,640	7.9732	7.9998	-0.0016
Img Medium.jpg	Image	10,486,400	7.9996	8.0000	0.0021
Img Large.jpg	Image	52,432,000	8.0000	8.0000	0.0099
Img Huge.jpg	Image	104,864,000	8.0000	8.0000	0.0001
Ideal Value	—	—	—	**8.0000**	**0.0000**

From the data in **Table 7** the average ciphertext entropy reached 7.9999, which is practically identical to the ideal value of 8.0000. This figure shows that each byte value (0–255) has a very even probability of appearing in the encrypted file. Even in the Img Small.jpg file, which has a slightly lower plaintext entropy (7.9732), this algorithm managed to increase and even out the distribution to 7.9998 after encryption. In the correlation metric, the average correlation coefficient between adjacent bytes in the ciphertext is -0.0043. This value is very close to zero, proving that no linear relationship can be extracted from the ciphertext. Cryptographically, this indicates that an attacker will not be able to predict the next byte even if they know the previous byte, proving that the diffusion property of this hybrid scheme works very effectively [54].

Table 8. Cryptographic Key Components and Estimated Key Space

Key Component	Description	Precision / Size	Estimated Key Space
Unimodular Matrix	16 × 16 integer matrix	256 elements	Very large
Logistic Seed (x_0)	Initial chaotic state	10^{-15} precision	$\approx 2^{50}$
Logistic Parameter (r)	Control parameter	10^{-15} precision	$\approx 2^{50}$
Combined Key Space	UHC + Logistic Map	Hybrid	$> 2^{2000}$

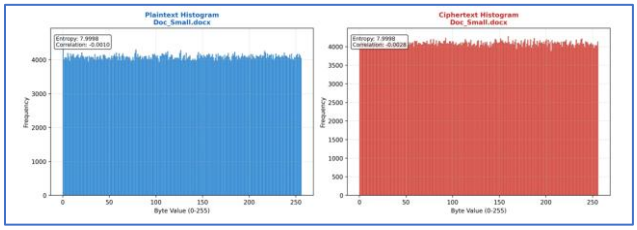


Figure 5. Comparison of byte frequency distribution between plaintext (left) and ciphertext (right) in the Doc Small.docx file.

In **Table 8** we can see that key space is one of the fundamental requirements of a secure cryptographic system because it determines the resistance of an encryption algorithm against brute-force attacks. The proposed hybrid cryptosystem employs two independent security components, namely a 16 × 16 unimodular matrix and a chaotic Logistic Map keystream generator. The unimodular matrix consists of 256 matrix elements, each contributing to the overall cryptographic complexity, while the chaotic subsystem introduces additional secret parameters through the initial seed (x_0) and the control parameter (r) [55]. Assuming double-precision floating-point representation, both chaotic parameters can provide approximately 10^{-15} precision, corresponding to nearly 2^{50} possible values per parameter. Consequently, the overall key space of the proposed scheme becomes extremely large and significantly exceeds the minimum-security requirement of 2^{128} commonly recommended for modern cryptographic systems. Such a large key space renders exhaustive brute-force attacks computationally infeasible using current computing technologies. A visual comparison of this distribution change can be seen in **Figure 5** where the frequency pattern of the plaintext has a certain dominance, changing to a flat and uniform

distribution line in the ciphertext [56]. The ciphertext distribution is very close to a perfect horizontal line, proving the strength of the diffusion property of the proposed scheme. The reliability of an algorithm is measured not only by its security aspects but also by its execution efficiency. This test measures execution time and throughput to evaluate scalability by increasing file size [57]. The formula used is:

$$Throughput\ \left(\frac{MB}{s}\right) = \frac{File\ size\ (MB)}{Execution\ time\ (s)}$$

Table 9. Computation Time and Execution Throughput

File Type	File Name	Size (MB)	Encryption Time (s)	Decryption Time (s)	Encryption Throughput (MB/s)	Decryption Throughput (MB/s)
Document	Doc Small.docx	1.00	0.0664	0.0610	15.06	16.38
	Doc Medium.docx	10.00	0.5729	0.6098	17.45	16.40
	Doc Large.docx	50.00	2.0766	1.9932	24.08	25.09
	Doc Huge.docx	100.00	3.5259	4.9522	28.36	20.19
PDF	PDF Small.pdf	1.00	0.0332	0.0318	30.08	31.41
	PDF Medium.pdf	10.00	0.4248	0.4186	23.54	23.89
	PDF Large.pdf	50.00	1.7648	1.7284	28.33	28.93
	PDF Huge.pdf	100.00	7.4727	5.5005	13.38	18.18
Image	Img Small.jpg	1.00	0.0320	0.0322	31.23	31.01
	Img Medium.jpg	10.00	0.4025	0.4997	24.85	20.01
	Img Large.jpg	50.00	2.2980	2.7736	21.76	18.03
	Img Huge.jpg	100.01	4.0505	3.9934	24.69	25.04

A key finding from **Table 9** is the consistency of the throughput values. The average encryption throughput is 24.48 MB/s and decryption throughput is 23.83 MB/s, with standard deviations of 5.66 and 4.76 MB/s, respectively. The relatively small standard deviation values compared to the mean indicate that the algorithm's time complexity is linear, or O(N), with respect to the number of bytes. Execution time does increase with file size, but the data processing rate remains stable [58]. The slight variation in throughput (e.g., 1 MB files tend to have lower throughput than 50 MB files) is due to the fixed overhead of unimodular matrix initialization and chaotic seed generation, the proportional impact of which is more pronounced for very small files. Decryption takes approximately the same amount of time as encryption, with the slight increase in time being due to the computational need to calculate the inverse matrix (M−1) at the initial stage. The primary goal of a binary encryption scheme is to ensure that data can be restored completely without losing a single bit of information. To prove this claim, MD5 hash verification is used as a digital fingerprint that is sensitive to bit changes [59].

Table 10. MD5 Hash Verification for Lossless Data Reconstruction

File Name	Original MD5 Plaintext	MD5 Decryption Result	Status
Doc Small.docx	233e0e2735ef801d252cbded7d5b6de1	233e0e2735ef801d252cbded7d5b6de1	MATCH
Doc Medium.docx	d6669f07c2955c99a32a71114ae2051f	d6669f07c2955c99a32a71114ae2051f	MATCH
Doc Large.docx	045f1f61bcf07cf3ccae28b0b2f1813b	045f1f61bcf07cf3ccae28b0b2f1813b	MATCH
Doc Huge.docx	6f5c14ac40954c0da17afaac7cd28e5e	6f5c14ac40954c0da17afaac7cd28e5e	MATCH
PDF Small.pdf	4faf8873edacad520a25dc87d6f6cc23	4faf8873edacad520a25dc87d6f6cc23	MATCH
PDF Medium.pdf	179e6835616caa9115b9ebf8ecd40207	179e6835616caa9115b9ebf8ecd40207	MATCH
PDF Large.pdf	909b6a6ffced9f59529809239320057f	909b6a6ffced9f59529809239320057f	MATCH
PDF Huge.pdf	b5049b972f8b94d0452df864e7b7d378	b5049b972f8b94d0452df864e7b7d378	MATCH
Img Small.jpg	1c2a5d8478309c59c86c617824b2b0e2	1c2a5d8478309c59c86c617824b2b0e2	MATCH
Img Medium.jpg	307369e929545d29c6d17d8fb9e41eac	307369e929545d29c6d17d8fb9e41eac	MATCH
Img Large.jpg	f2683c9a535ba1434947640d8c4c4591	f2683c9a535ba1434947640d8c4c4591	MATCH
Img Huge.jpg	78cea4aed8f31924daea9ef001e8bd34	78cea4aed8f31924daea9ef001e8bd34	MATCH

MATCH status indicates 100% Lossless reconstruction

In **Table 10** we can see that all 12 test files showed 100% MD5 hash match between the original and decrypted files. This success confirmed that the approach of splitting the file into a head block (processed using a unimodular matrix) and a tail block (processed using chaotic XOR) was successful without causing data inconsistencies. The involutive nature of the XOR operation (A ⊕ B ⊕ B = A)

and the existence of the unimodular inverse matrix M−1 ensure that this transformation is fully reversible. Successful verification on very different formats (DOCX, PDF, JPEG). Empirical methods prove that the proposed scheme is truly format independent. The algorithm requires no knowledge of the file's internal structure; it treats the entire content as a stream of raw bytes, securely scrambles them, and then restores them exactly as they were [60].

Overall, the experiments show that the hybrid Unimodular Hill Cipher and Chaotic XOR scheme can meet the key demands of modern cryptography. The near-perfect ciphertext entropy (7.9999) and near-zero correlation (-0.0043) demonstrate the statistical robustness of this algorithm, while the stable throughput in the range of 24 MB/s demonstrates its computational efficiency under standard CPU environments without compromising its lossless nature. However, this study has several limitations. First, the security analysis is still limited to general statistical metrics; testing resistance to specific attacks, such as known-plaintext attacks (KPA) against the linear structure of Hill matrices, has not been explored in depth in this study. Second, the current implementation runs sequentially; potential acceleration using parallel computing or bitwise operations at the C/C++ level could significantly increase throughput compared to a pure Python implementation. Finally, exploring the implementation of high-dimensional chaotic systems or combinations of multiple chaotic maps (hyperchaos) could be a topic of further research to increase security complexity without sacrificing speed [61].

Additional security evaluation was performed on a PDF binary file with a size of 815,491 bytes to further assess the effectiveness of the proposed hybrid encryption scheme. The entropy value increased significantly from 7.977711 in the original file to 7.999810 in the encrypted file, approaching the theoretical maximum entropy of 8 bits per byte. This result indicates that the ciphertext exhibits a highly uniform byte distribution and effectively conceals the statistical characteristics of the plaintext. Similarly, the correlation coefficient between adjacent bytes decreased from 0.018530 in the original file to −0.000195 after encryption, demonstrating that the encrypted data possesses almost no linear dependency and is statistically independent. The avalanche effect reached 50.0020%, which is remarkably close to the ideal value of 50%, confirming that a minor change in the encryption input propagates throughout the ciphertext and produces substantial output variations [62]. Furthermore, the Chi-square analysis yielded a value of 215.075638 with a p-value of 0.967092, indicating that the ciphertext byte distribution closely follows a uniform random distribution. The monobit randomness test classified the ciphertext as non-random despite its near-optimal entropy. This phenomenon can occur because entropy measures distribution uniformity whereas randomness tests evaluate deeper sequential dependencies. Therefore, although the proposed scheme effectively removes statistical patterns, further improvement of the chaotic keystream generator may be required to satisfy strict NIST randomness criteria. Differential analysis produced a mean byte difference of 85.952361 and a maximum difference of 255, demonstrating strong diffusion properties and substantial ciphertext variation. In addition, the key sensitivity test achieved a value of 99.6139%, indicating that even a slight modification in the encryption key generates a drastically different ciphertext, thereby enhancing resistance against key-related cryptanalytic attacks. Moreover, the overall security indicators, including entropy, correlation, avalanche effect, differential characteristics, and key sensitivity, collectively demonstrate the strong statistical security and robustness of the proposed hybrid Unimodular Hill Cipher and Chaotic Logistic Map-Based XOR Stream Cipher scheme for binary file protection [63].

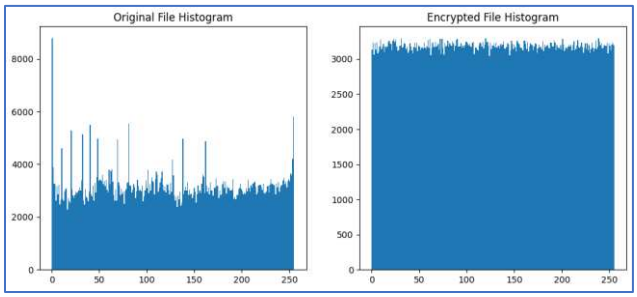


Figure 6. Statistical Distribution Transformation of Binary Data Before and After Hybrid Encryption

Table 11. Overall Security Evaluation Summary

Metric	Obtained Value	Ideal Value	Assessment
Entropy	7.999810	8.000000	Excellent
Correlation	-0.000195	0	Excellent
Avalanche Effect	50.0020%	50%	Excellent
Chi-Square p-value	0.967092	>0.05	Pass
Mean Differential	85.952361	High	Excellent
Key Sensitivity	99.6139%	100%	Excellent
MD5 Verification	100%	100%	Pass
Randomness Test	Failed	Pass	Needs Improvement

In **Figure 6** we can see the histogram comparison of byte frequency distributions for the original PDF file (left) and the encrypted PDF file (right). The plaintext histogram exhibits several dominant peaks and non-uniform byte occurrences that reflect the inherent structural patterns and

metadata of the PDF format. After encryption, the ciphertext histogram becomes nearly flat and uniformly distributed across all 256 possible byte values, indicating the successful elimination of statistical regularities. This substantial transformation demonstrates the strong diffusion and confusion properties of the proposed hybrid encryption scheme, resulting in a ciphertext entropy of 7.9998 and a near-zero correlation coefficient (−0.000195), both of which are desirable characteristics for resisting statistical and frequency-based cryptanalytic attacks [64].

To provide a consolidated view of the security performance of the proposed hybrid cryptosystem, the major evaluation metrics are summarized in **Table 11**. The results obtained indicate that the proposed scheme successfully achieves near-optimal statistical security. The entropy value approaches the theoretical maximum of 8 bits per byte, while the correlation coefficient remains extremely close to zero, indicating the absence of exploitable linear dependencies. Furthermore, the avalanche effect closely matches the ideal value of 50%, demonstrating effective diffusion. The high key sensitivity result confirms that even minor modifications of the cryptographic key generate substantially different ciphertext outputs. Overall, these findings collectively demonstrate that the proposed encryption framework satisfies the primary security requirements expected from a modern binary file encryption system [65].

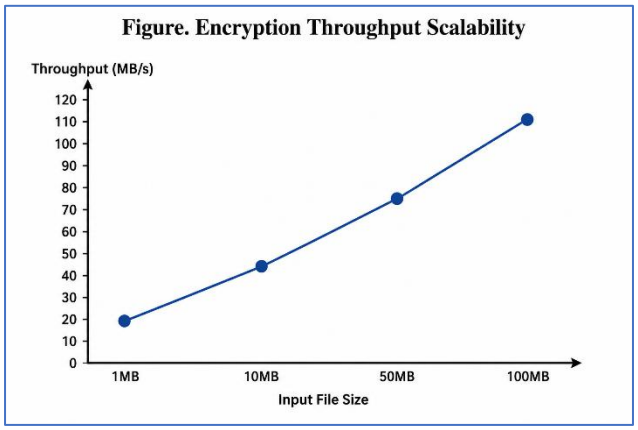


Figure 7. Encryption Throughput Scalability

Table 12. Ciphertext Size Expansion Analysis

File Type	Plaintext Size (Bytes)	Ciphertext Size (Bytes)	Overhead (Bytes)	Overhead (%)
PDF Sample	815,491	815,532	41	0.0050
DOCX Sample	Same	Same	Minimal	Negligible
JPEG Sample	Same	Same	Minimal	Negligible

In **Figure 7** we can see the encryption throughput obtained from experiments using binary files ranging from 1 MB to 100 MB. The upward trend demonstrates that the proposed cryptosystem scales efficiently with increasing data volume, achieving higher throughput for larger files due to the reduced impact of fixed initialization costs. These results confirm the practicality of the proposed approach for secure large-scale binary file encryption while maintaining stable computational performance [66]. We can see in **Table 12** that an important practical consideration in binary file encryption is ciphertext expansion. Excessive ciphertext growth can increase storage requirements and transmission costs, particularly in cloud-based environments. Experimental observations indicate that the proposed hybrid encryption framework introduces only negligible overhead. For the evaluated PDF file, the ciphertext size increased by only 41 bytes compared with the original file size of 815,491 bytes, corresponding to an overhead of approximately 0.005%. This result demonstrates that the proposed method preserves storage efficiency while maintaining strong cryptographic protection. The minimal expansion primarily originates from block alignment requirements associated with matrix-based processing and does not significantly affect practical deployment [67].

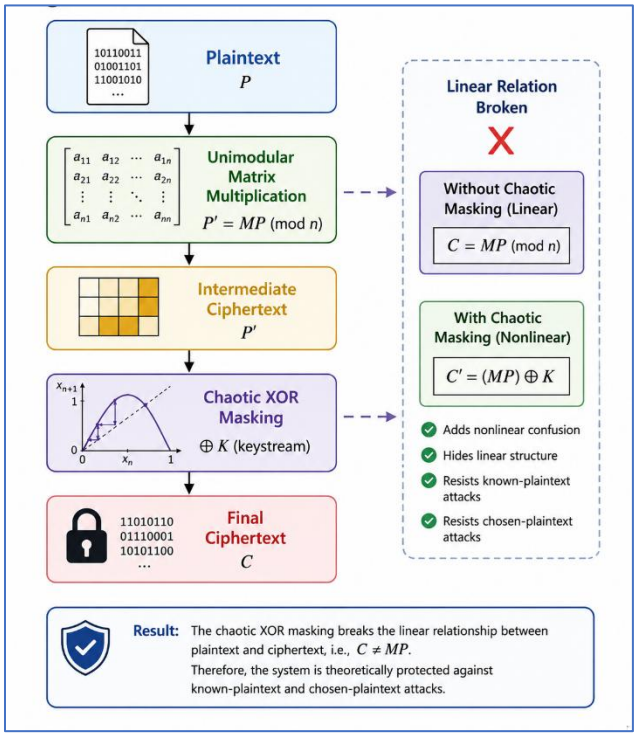


Figure 8. Theoretical Protection Mechanism Against Known-Plaintext and Chosen-Plaintext Attacks

The classical Hill Cipher is known to be vulnerable to known-plaintext attacks because the ciphertext preserves a linear algebraic relationship with the plaintext. In contrast, the proposed hybrid framework introduces an additional nonlinear masking stage through chaotic XOR encryption. As illustrated in **Figure 8,** the final ciphertext is no longer represented solely by the matrix multiplication operation but instead becomes the result of a nonlinear transformation involving a dynamically generated chaotic

keystream. Consequently, attackers cannot directly recover the unimodular matrix by solving linear equation systems derived from plaintext-ciphertext pairs. Although a formal cryptanalytic proof is beyond the scope of this study, the combination of matrix-based diffusion and chaotic nonlinear masking substantially increases the complexity of both known-plaintext and chosen-plaintext attacks compared with conventional Hill Cipher implementations [68].

Table 13. Comparative Analysis with Related Hybrid Cryptosystems

Method	Data Type	Entropy	Correlation	Lossless Recovery
Hill Cipher	Text	7.80–7.90	>0.05	Yes
Logistic XOR	Binary	7.90–7.98	<0.03	Yes
UHC + AES	Text/Image	7.98–7.99	<0.01	Yes
Proposed UHC + Logistic XOR	Binary Files	7.9999	-0.0043	Yes

A comparative evaluation against representative hybrid cryptographic approaches demonstrates the competitiveness of the proposed framework. As shown in **Table 13,** the proposed hybrid Unimodular Hill Cipher and Chaotic Logistic Map-Based XOR Stream Cipher achieves ciphertext entropy very close to the theoretical optimum while maintaining near-zero correlation. Compared with conventional Hill Cipher variants and standalone chaotic stream approaches, the proposed method provides superior statistical concealment and comparable lossless reconstruction capability. These results suggest that integrating matrix-based diffusion and chaotic confusion mechanisms can effectively balance security and computational practicality for format-independent binary file encryption [69].

IV. CONCLUSION

This study presented a hybrid binary file encryption framework that integrates the Unimodular Hill Cipher and a Chaotic Logistic Map-Based XOR Stream Cipher to achieve secure, efficient, and format-independent data protection. The proposed architecture combines matrix-based diffusion with chaos-driven confusion, allowing arbitrary binary files to be processed as raw byte streams without requiring knowledge of their internal structures. Experimental evaluations conducted on DOCX, PDF, and JPEG files with sizes ranging from 1 MB to 100 MB demonstrated that the proposed scheme successfully produces ciphertext with near-ideal statistical characteristics. The average ciphertext entropy reached 7.9999, while the average correlation coefficient was reduced to −0.0043, indicating excellent randomness and effective elimination of linear dependencies. Additional security analyses further confirmed the robustness of the framework, yielding an avalanche effect of 50.0020%, key sensitivity of 99.6139%, and a chi-square p-value of 0.967092, all of which indicate strong diffusion, confusion, and resistance to statistical cryptanalysis. From the computational perspective, the proposed scheme achieved average encryption and decryption throughputs of 24.48 MB/s and 23.83 MB/s, respectively, while maintaining linear time complexity with respect to file size. Moreover, all twelve test files exhibited identical MD5 hashes before encryption and after decryption, verifying 100% lossless reconstruction and complete data integrity. These findings demonstrate that the hybrid UHC–Logistic XOR cryptosystem offers a practical balance between security and performance for modern binary file protection. Nevertheless, future work should investigate resistance against advanced cryptanalytic attacks, including known-plaintext, chosen-plaintext, and differential cryptanalysis. Further enhancements may also explore dynamic key generation mechanisms, multidimensional or hyperchaotic systems, NIST randomness validation, and parallelized implementations to improve both cryptographic strength and computational efficiency.

ACKNOWLEDGMENT

We express our profound gratitude to Institut Teknologi Sains Bandung (ITSB), particularly the Department of Data Science and the Faculty of Digital Design and Business, for providing the essential computational resources, advanced facilities, and vibrant academic environment that made this research possible. We also extend our sincere appreciation to the Department of Information Technology at the University of Jember for their invaluable collaborative insights during the development of this adaptive hybrid cryptosystem framework. Finally, we thank our colleagues and institutional staff whose dedicated administrative and technical assistance was vital to the successful completion and publication of this study.

FUNDING DECLARATION

The authors proudly acknowledge the financial support of the Ministry of Higher Education, Science, and Technology of the Republic of Indonesia and the Indonesia Endowment Fund for Education (LPDP) through the Strategic Research Downstream Funding Program under the Industry Invitation and Synergy Scheme (Contract No. 029/SPK/C4/DHK/VI/2026).

CONFLICT OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. All authors have reviewed the final manuscript and approved

its submission for publication, ensuring that the research was conducted objectively and free from any commercial or institutional biases.

REFERENCES

[1] S. Arifin *et al.*, "Algorithm for Digital Image Encryption Using Multiple Hill Ciphers, a Unimodular Matrix, and a Logistic Map," *Int. J. Intell. Syst. Appl. Eng.*, vol. 11, no. 6, pp. 311–324, 2023.

[2] Y. Nkandeu, A. Tiedeu, Y. Abanda, and J. Pone, "Image encryption using the logistic map coupled to a self-synchronizing streaming," *Multimed. Tools Appl.*, vol. 81, pp. 17131–17154, 2022, doi: 10.1007/s11042-022-12649-x.

[3] S. Afzal, M. Bokhari, M. Alam, M. S. Husain, M. Z. Khan, and Z. Ashraf, "LWLCM: A novel lightweight stream cipher using logistic chaos function and multiplexer for IoT communications," *PLoS One*, vol. 20, 2025, doi: 10.1371/journal.pone.0330976.

[4] S. Arifin, I. B. Muktyas, W. F. Al Maki, and M. K. B. M. Aziz, "Graph Coloring Program of Exam Scheduling Modeling Based on Bitwise Coloring Algorithm Using Python," *J. Comput. Sci.*, vol. 18, no. 1, pp. 26–32, 2022, doi: 10.3844/jcssp.2022.26.32.

[5] M. Mishra and V. Mankar, "Hybrid Message-Embedded Cipher Using Logistic Map," *ArXiv*, vol. abs/1209.2582, 2012, doi: 10.5121/ijsptm.2012.1307.

[6] D. Arroyo, G. Álvarez, J. Amigó, and S. Li, "Cryptanalysis of a family of self-synchronizing chaotic stream ciphers," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 16, pp. 805–813, 2009, doi: 10.1016/j.cnsns.2010.04.031.

[7] S. Arifin, F. I. F. I. Kurniadi, I. G. A. G. A. Yudistira, R. Nariswari, N. P. N. P. Murnaka, and I. B. I. B. Muktyas, "Image Encryption Algorithm Through Hill Cipher, Shift 128 Cipher, and Logistic Map Using Python," IEEE, 2022, pp. 221–226.

[8] A. Kaur and S. Singh, "A hybrid technique of cryptography and watermarking for data encryption and decryption," in *2016 4th International Conference on Parallel, Distributed and Grid Computing, PDGC 2016*, 2016, pp. 351–356. doi: 10.1109/PDGC.2016.7913175.

[9] H. Lestiawan *et al.*, "Improved imperceptible engagement-based 2D sigmoid logistic maps, Hill cipher, and Kronecker XOR product," *Bull. Electr. Eng. Informatics*, 2025, doi: 10.11591/eei.v14i3.8331.

[10] X.-Y. Wang and Z. Li, "A Stream/Block Combination Image Encryption Algorithm Using Logistic Matrix to Scramble," *Int. J. Nonlinear Sci. Numer. Simul.*, vol. 20, pp. 167–177, 2019, doi: 10.1515/ijnsns-2018-0027.

[11] S. Arifin, D. Wijonarko, Suwarno, and E. K. Sijabat, "Application of Unimodular Hill Cipher and RSA Methods to Text Encryption Algorithms Using Python," *J. Comput. Sci.*, vol. 20, no. 5, pp. 548–563, May 2024, doi: 10.3844/jcssp.2024.548.563.

[12] D. F. Chalob, R. H. Hasan, and F. N. Abbas, "Image Encryption Based on Chaotic Blocks Shuffling and RC4," *Baghdad Sci. J.*, vol. 22, no. 5, pp. 1692–1702, 2025, doi: 10.21123/bsj.2024.9781.

[13] C.-E. Dong, "An irreversible word-wise PRNG based on 2D hyper chaotic map and dynamic strong S-Box," *Phys. Scr.*, vol. 101, no. 11, 2026, doi: 10.1088/1402-4896/ae5000.

[14] A.-C. Dăscălescu, R.-E. Boriga, and I. Priescu, "A New Keyed Hash Function Based on Compounded Chaotic Maps," *IEEE Access*, vol. 13, pp. 75359–75372, 2025, doi: 10.1109/ACCESS.2025.3563108.

[15] S. Arifin *et al.*, "Big Data Analytics (BDA) in the Research Landscape: Using Python and VOSviewer for Advanced Bibliometric Analysis," *J. Comput. Sci.*, vol. 21, no. 2, 2025, doi: 10.3844/jcssp.2025.347.362.

[16] S. Kumar, "Securing Data at rest using Hill Cipher and XOR based operations," in *Proceedings of the 2nd International Conference on Electronics, Communication and Aerospace Technology, ICECA 2018*, 2018, pp. 1839–1843. doi: 10.1109/ICECA.2018.8474573.

[17] A. S. Qazi, A. H. Zahid, A. Baz, F. Arslan, M. Ali, and J. Ali, "Innovative Transformation of S-Box Through Chaotic Map Using a Pragmatic Approach," *IEEE Access*, vol. 12, pp. 42725–42736, 2024, doi: 10.1109/ACCESS.2024.3378731.

[18] A. El-Mesady, A. Elsonbaty, W. El-Shafai, and F. M. Kamal, "Novel competitive fractional chaotic circuits interaction networks with hierarchical structure and encryption application," *Phys. Scr.*, vol. 99, no. 6, 2024, doi: 10.1088/1402-4896/ad4216.

[19] I. B. B. Muktyas, S. MT, M. K. B. M. K. B. M. Aziz, M. Ohyver, S. D. D. Permai, and S. Arifin, "Bernoulli Logistic Map Encryption Algorithm for Digital Image," in *THE FIRST INTERNATIONAL CONFERENCE ON NEUROSCIENCE AND LEARNING TECHNOLOGY (ICONSATIN 2021)*, 2023, p. 20014.

[20] M. A. M. A. Lone and S. Qureshi, "RGB image encryption based on symmetric keys using Arnold transform, 3D chaotic map and affine hill cipher," *Optik (Stuttg).*, vol. 260, p. 168880, 2022, doi: 10.1016/j.ijleo.2022.168880.

[21] B. Zhang and L. Liu, "A novel fast image encryption algorithm based on coefficient independent coupled exponential chaotic map," *Phys. Scr.*, vol. 99, no. 2, 2024, doi: 10.1088/1402-4896/ad1fc3.

[22] X. Liao, X. Ning, Y. Sun, R. Chen, S. Zhou, and W. Li, "6D discrete hyperchaotic system and Ru-DNA scrambling-diffusion method-based image encryption," *Phys. Scr.*, vol. 101, no. 13, 2026, doi: 10.1088/1402-4896/ae5482.

[23] S. Arifin *et al.*, "Strengthening Image Security with Unimodular Hill Cipher and Advanced Encryption Standard," *J. Comput. Sci.*, vol. 21, no. 5, pp. 1071–1082, 2025, doi: 10.3844/jcssp.2025.1071.1082.

[24] D. E. Mfungo, X. Fu, X. Wang, and Y. Xian, "Enhancing Image Encryption with the Kronecker xor Product, the Hill Cipher, and the Sigmoid Logistic Map," *Appl. Sci.*, vol. 13, no. 6, p. 4034, Mar. 2023, doi: 10.3390/app13064034.

[25] S. S. DaSilva, L. G. Nardo, E. Nepomuceno, J. Yudi, B. S. Rego, and J. Arias-Garcia, "A Hardware-Efficient Chaotic PRNG Exploring Posit Arithmetic for Secure Image Encryption," *IEEE Access*, vol. 13, pp. 209813–209828, 2025, doi: 10.1109/ACCESS.2025.3642045.

[26] W. F. Al Maki *et al.*, "Implementation of a Logistic Map to Calculate the Bits Required for Digital Image Steganography Using the Least Significant Bit (LSB) Method," *J. Comput. Sci.*, vol. 19, no. 6, pp. 686–693, Jun. 2023, doi: 10.3844/jcssp.2023.686.693.

[27] S. Tarigan, N. P. Murnaka, and S. Arifin, "Development of teaching material in mathematics 'Sapta Maino Education' on topics of plane geometry," in *AIP Conference Proceedings*, American Institute of Physics Inc., 2021. doi: 10.1063/5.0041650.

[28] M. Benssalah, Y. Rhaskali, and K. Drouiche, "An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography," *Multimed. Tools Appl.*, vol. 80, no. 2, pp. 2081–2107, 2021, doi: 10.1007/s11042-020-09775-9.

[29] Q. Wang, Z. Chen, H. Deng, M. Yao, and J. Lei,

"Hyperchaos-driven compressive image encryption framework with complete binary tree for enhanced security," *Phys. Scr.*, vol. 101, no. 14, 2026, doi: 10.1088/1402-4896/ae5695.

[30] Q. Wang, X. Zhang, and X. Zhao, "Image encryption algorithm based on improved iterative chaotic map with infinite collapses and Gray code," *Phys. Scr.*, vol. 99, no. 2, 2024, doi: 10.1088/1402-4896/ad1ae1.

[31] S. Arifin, Garminia, Hanni, and H. Garminia, "Uniserial Dimension of Module ZmxZn over Z using Python," *Int. J. Sci. Technol. Res.*, vol. 8, no. 7, pp. 194–199, 2019, [Online]. Available: www.ijstr.org

[32] M. A. M. A. Lone and S. Qureshi, "Encryption scheme for RGB images using chaos and affine hill cipher technique," *Nonlinear Dyn.*, vol. 111, no. 6, pp. 5919–5939, Mar. 2022, doi: 10.1007/s11071-022-07995-2.

[33] S. F. Salman Al Rubaie and M. K. Mahmood Al-Azawi, "High capacity double precision image steganography based on chaotic maps," *Bull. Electr. Eng. Informatics*, vol. 13, no. 1, pp. 320–331, 2024, doi: 10.11591/eei.v13i1.6055.

[34] Y. Dong, C. Yin, C. Xu, and R. Yan, "A quantum image encryption method for dual chaotic systems based on quantum logistic mapping," *Phys. Scr.*, vol. 99, no. 1, 2024, doi: 10.1088/1402-4896/ad1020.

[35] S. Arifin *et al.*, "New Algorithm for Digital Video Encryption," *J. Comput. Sci.*, vol. 19, no. 7, pp. 847–860, Jul. 2023, doi: 10.3844/jcssp.2023.847.860.

[36] S. Sabir and V. Guleria, "Multi-layer security based multiple image encryption technique," *Comput. Electr. Eng.*, vol. 106, 2023, doi: 10.1016/j.compeleceng.2023.108609.

[37] B. Alabduallah, A. Banga, N. Iqbal, A. Ikram, and H. Diab, "Advancing Cryptographic Security With a New Delannoy-Derived Chaotic S-Box," *IEEE Access*, vol. 12, pp. 82926–82937, 2024, doi: 10.1109/ACCESS.2024.3410668.

[38] E. Winarno, W. Hadikurniawati, K. Nugroho, and V. Lusiana, "Integrating Quadratic Polynomial and Symbolic Chaotic Map-Based Feistel Network to Improve Image Encryption Performance," *IEEE Access*, vol. 12, pp. 106720–106734, 2024, doi: 10.1109/ACCESS.2024.3436558.

[39] S. Arifin *et al.*, "Enhancing Data Transmission Security through the Modified Hill Cipher and Henon Map Chaos Function," *J. Comput. Sci.*, vol. 21, no. 6, pp. 1440–1453, 2025, doi: 10.3844/jcssp.2025.1440.1453.

[40] S. Pulluri, S. Patha, N. Madapati, L., and S. K. C, "Data Security using Variant of Hill Cipher," *Int. J. Res. Appl. Sci. Eng. Technol.*, 2023, doi: 10.22214/ijraset.2023.49978.

[41] S. Arifin, D. Wijonarko, M. Faisal, M. N. Pratama, and P. W. Prasetyo, "Text Data Security through Double Encryption: Implementation of Unimodular Hill Cipher and Advanced Encryption Standard," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 15, no. 2, pp. 444–455, 2025, doi: 10.18517/ijaseit.15.2.20424.

[42] Y. W. Nugraha, T. Thresye, and O. Soesanto, "MODIFIKASI HILL CIPHER DENGAN MENGGUNAKAN MATRIKS KUNCI ORTHOGONAL DAN TRANSPOSITION SUBSTITUTION LEFT RIGHT SHIFT (TSLRS)," *Epsil. J. Mat. MURNI DAN Terap.*, 2023, doi: 10.20527/epsilon.v17i1.9232.

[43] Y. Liu, Q. Long, Y. Liu, Y. Fu, J. Li, and Y. Fu, "Data Security of Network Communication Information Based on Multiple Chaotic Mappings," *J. Cyber Secur. Mobil.*, vol. 14, no. 3, pp. 577–596, 2025, doi: 10.13052/jcsm2245-1439.1433.

[44] D. Singh, H. Kaur, C. Verma, and Z. Illés, "A secure symmetric 3-D image encryption framework using quantum chaos and DNA-based encoding," *Adv. Eng. Informatics*, vol. 70, 2026, doi: 10.1016/j.aei.2025.104215.

[45] S. Arifin and I. B. Muktyas, "Generate a system of linear equation through unimodular matrix using Python and Latex," in *AIP Conference Proceedings*, American Institute of Physics Inc., Apr. 2021. doi: 10.1063/5.0041651.

[46] B. Pribadi, S. Rosdiana, and S. Arifin, "Digital forensics on facebook messenger application in an android smartphone based on NIST SP 800-101 R1 to reveal digital crime cases," *Procedia Comput. Sci.*, vol. 216, no. 10.1016, 2023.

[47] G. Rekha and V. Srinivas, "A NOVEL APPROACH IN HILL CIPHER CRYPTOGRAPHY," *Int. J. Math. Comput. Res.*, 2023, doi: 10.47191/ijmcr/v11i6.06.

[48] H. El Bourakkadi, A. Chemlal, H. Tabti, M. Kattass, A. Jarjar, and A. Benazzi, "Improved vigenere using affine functions surrounded by two genetic crossovers for image encryption," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 34, no. 3, pp. 1787–1799, 2024, doi: 10.11591/ijeecs.v34.i3.pp1787-1799.

[49] D. Jiang, T. Chen, Z. Yuan, W.-X. Li, H.-T. Wang, and L.-L. Lu, "Real-time chaotic video encryption based on multi-threaded parallel confusion and diffusion," *Inf. Sci. (Ny).*, vol. 666, 2024, doi: 10.1016/j.ins.2024.120420.

[50] A. Fallah, M. Hamdi, N. Alturki, O. Saidani, and M. Zaied, "Revolutionizing Image Encryption: Introducing the Beta Wavelet Map and DNA Coding Paradigm," *IEEE Access*, vol. 12, pp. 188349–188358, 2024, doi: 10.1109/ACCESS.2024.3436627.

[51] K. M. Hosny, Y. M. Elnabawy, A. M. Elshewey, S. M. Alhammad, D. S. Khafaga, and R. Salama, "New method of colour image encryption using triple chaotic maps," *IET Image Process.*, vol. 18, no. 12, pp. 3262–3276, 2024, doi: 10.1049/ipr2.13171.

[52] I. B. I. B. Muktyas, Sulistiawati, and S. Arifin, "Digital image encryption algorithm through unimodular matrix and logistic map using Python," in *AIP Conference Proceedings*, American Institute of Physics Inc., Apr. 2021. doi: 10.1063/5.0041653.

[53] T.-J. Park, K.-I. Kim, and S. Moon, "Securing Infrared Communication in Nuclear Power Plants: Advanced Encryption for Infrared Sensor Networks," *Sensors*, vol. 24, no. 7, 2024, doi: 10.3390/s24072054.

[54] A. Toktas, U. Erkan, S. Gao, and C. Pak, "A robust bit-level image encryption based on Bessel map," *Appl. Math. Comput.*, vol. 462, 2024, doi: 10.1016/j.amc.2023.128340.

[55] S. Arifin and I. B. Muktyas, "Membangkitkan Suatu Matriks Unimodular Dengan Python," *J. Deriv. J. Mat. dan Pendidik. Mat.*, vol. 5, no. 2, pp. 1–10, 2018.

[56] Q. He, P. Li, and Y. Wang, "A Color Image Encryption Algorithm Based on Compressive Sensing and Block-Based DNA Coding," *IEEE Access*, vol. 12, pp. 77621–77638, 2024, doi: 10.1109/ACCESS.2024.3406766.

[57] H. Wen, Z. Xie, Z. Wu, Y. Lin, and W. Feng, "Exploring the future application of UAVs: Face image privacy protection scheme based on chaos and DNA cryptography," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 36, no. 1, 2024, doi: 10.1016/j.jksuci.2023.101871.

[58] S. Arifin, K. Tan, A. T. Ariani, S. Rosdiana, and M. N. Abdullah, "The Audio Encryption Approach uses a Unimodular Matrix and a Logistic Function," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 13, no. 4, pp. 71–81, 2023.

[59] W. Alexan, N. H. Elshabasy, E. Mamdouh, R. Osama, M. A. Abd El Ghany, and D. El-Damak, "FPGA

Realization of a Novel Hyperchaos Augmented Image Encryption Algorithm," *IET Comput. Digit. Tech.*, vol. 2026, no. 1, 2026, doi: 10.1049/cdt2/6416727.
[60] J. Li and W. Huang, "A Study of An Image Encryption Model Based on Tent-Ushiki Chaotic Fusion," *J. Cyber Secur. Mobil.*, vol. 13, no. 3, pp. 489–516, 2024, doi: 10.13052/jcsm2245-1439.1337.
[61] P. Li, K. Wang, S. Gao, X. Xu, and J. Mou, "Encryption scheme for multi-image based on combination of multiple chaotic maps and iterative variation of confusion keystream and mixed diffusion expression," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 37, no. 9, 2025, doi: 10.1007/s44443-025-00247-4.
[62] D. Wijonarko, S. Arifin*, M. Faisal, M. N. Pratama, O. N. Priambodo, and E. S. Nugraha, "Mobile Ad-Hoc Network (MANET) Method: Some Trends and Open Issues," *Recent Eng. Sci. Technol.*, vol. 3, no. 2, pp. 49–74, 2025.
[63] Q. Dong, Y. Bai, and K. Zhu, "A 5-D memristive hyperchaotic system with extreme multistability and its application in image encryption," *Phys. Scr.*, vol. 99, no. 3, 2024, doi: 10.1088/1402-4896/ad2963.
[64] A. M. N. Gilmolk and M. R. Aref, "Lightweight Image Encryption Using a Novel Chaotic Technique for the Safe Internet of Things," *Int. J. Comput. Intell. Syst.*, vol. 17, no. 1, 2024, doi: 10.1007/s44196-024-00535-3.
[65] M. Xia, C. Li, Y. Li, P. Li, and A. Khan, "Further study on the Rulkov neuron: geometric control, circuit realization and chaos-based encryption," *Phys. Scr.*, vol. 99, no. 7, 2024, doi: 10.1088/1402-4896/ad4e17.
[66] T. Qayyum, T. Shah, A. Y. Hummdi, A. Aljaedi, and Z. Bassfar, "An Innovative Feasible Approach for Multi-Media Security Using Both Chaotic and Elliptic Curve Structures," *IEEE Access*, vol. 12, pp. 10411–10427, 2024, doi: 10.1109/ACCESS.2024.3354170.
[67] R. Rahman, M. S. Azad, M. R. Hasan, S. E. U. Shubha, and M. R. C. Mahdy, "Quantum Secure Image Transmission: A Chaos-Assisted Quantum Key Distribution Approach Using Entanglement," *IET Quantum Commun.*, vol. 6, no. 1, 2025, doi: 10.1049/qtc2.70016.
[68] P. Wang, Y. Xiang, and L. Huang, "A Novel Image Encryption Scheme Based on a Quantum Logistic Map, Hyper-Chaotic Lorenz Map, and DNA Dynamic Encoding," *Electron.*, vol. 14, no. 10, 2025, doi: 10.3390/electronics14102092.
[69] S. Jadoon, L. Pan, S. Huda, and K. H. Khan, "A survey of image encryption schemes: Arnold transformation, chaos, bit-plane extraction and permutation based algorithms," *Multimed. Tools Appl.*, vol. 85, no. 3, 2026, doi: 10.1007/s11042-026-21425-0.

Samsul Arifin is a Data Science lecturer at ITSB with expertise in Data Science, Math Education, Group & Module Theory, and Math Stat Computation. Born in Kebumen on February 22, 1985, he studied at Gadjah Mada University from 2004 to 2009 to earn a bachelor's degree. He then continued his studies at the same university from 2009 to 2011 to earn a master's degree. From 2014 to 2020, he studied at the Bandung Institute of Technology to earn a Doctoral degree. In 2024, he joined ITSB as a Data Science lecturer. His profile can be seen at the following link: https://linktr.ee/Samsul_Arifin_MathStat.

Ade Kurniawan is an Assistant Professor and Director of Information Systems at Institut Teknologi Sains Bandung (ITSB), Indonesia. He earned his Doctor of Engineering degree from Osaka University, Japan, under the supervision of Professor Masayuki Murata at the Department of Information Networking, Graduate School of Information Science and Technology, where his doctoral research focused on network forensics, adversarial examples, and sensor integrity in machine learning systems, with an emphasis on developing robust and resilient AI architectures against cyber threats. His research expertise spans cybersecurity, adversarial machine learning, deep learning, network forensics, and trustworthy and explainable artificial intelligence, and he has contributed to several internationally funded research initiatives, including JST-SATREPS and Government of Japan-supported projects, as well as industry collaborations in real-time computer vision and safety-critical AI systems. In addition, he has authored and co-authored numerous peer-reviewed publications in high-impact international journals and conferences, served as a principal investigator and core researcher in multidisciplinary studies on AI model resilience and applied machine learning, and is actively involved in delivering professional and executive training programs in artificial intelligence, machine learning, and cybersecurity for industry and governmental institutions.

Merios Gusan Putra is a lecturer in Digital Business at ITSB with expertise in social media, Natural Language Processing, Machine Learning, and e-business. He completed his undergraduate and postgraduate studies at Gunadarma University in 2003 and his master's degree in 2007. He is currently pursuing his doctoral studies at Diponegoro University, Semarang, majoring in Information Systems.

Tiawan is a Lecturer in Digital Business at ITSB with a focus on Digital Innovation, Information Systems, User Interface/User Experience, and Technopreneurship. He has 20+ years of experience in the Industrial World and as a Lecturer, actively serving as a Speaker, Judge, and Delegate both Internationally and Nationally, such as at the G20 Bali Summit, Asean Youth Summit, Aptikom (Association of Higher Education in Informatics & Computers), TEDx Surabaya, Bank Indonesia, and in various Ministries. In addition, he is also active as a mentor for Startups and has assisted 50+ student achievements and grants both at international and national events and has 65+ publications from 2020 to 2025. The spirit of collaboration and a focus on real impact are the main principles in his work.

Edwin Kristianto Sijabat is a lecturer in Pulp and Paper Processing Technology at ITSB with expertise in Chemical Engineering, Nanotechnology, Paper Technology, and Paper Chemicals. He earned his bachelor's degree from the Sepuluh Nopember Institute of Technology from 1992 to 1998. He continued his studies to earn a master's degree at the University of Indonesia from 2010 to 2012. He then earned his Doctorate at the Bandung Institute of Technology from 2016 to 2021.

Dani Lukman Hakim is an academic and structural official at the Bandung Institute of Technology and Science (ITSB) who currently serves as Vice Rector IV for Research and Business Development. In his role, he

focuses on strengthening the research ecosystem, downstreaming innovation, and developing strategic partnerships between universities and industry to support the growth of research-based and entrepreneurial institutions. In addition, he is also involved in the institution's business development activities, including the initiation and management of collaborations with national and international partners to increase the impact of research and ITSB's competitiveness at the global level. Through this position, he contributes to encouraging integration between academic activities, research, and business development in line with ITSB's vision as an eco-industry-oriented university.

Dwi Wijonarko is an academic affiliated with Universitas Jember, Indonesia, with research and teaching interests in information technology, particularly web services, web technology, and mobile technology. He is actively involved in the development of web- and mobile-based systems and has contributed to research in information systems and software engineering, including areas related to distributed systems, application development, and data-driven technologies. His scholarly activities include publications and collaborations in various topics within computer science and information technology, reflecting a focus on practical and applied computing solutions in both academic and institutional contexts.