Dwi Wijonarko

Paper AUHCAES_Dadan [13Jun2026]_ToC

Hiliriset UNEJ-ITSB - Tahun 2

Document Details

Submission ID
trn:oid:::3618:145350937

Submission Date
Jul 11, 2026, 9:44 AM GMT+7

Download Date
Jul 11, 2026, 9:51 AM GMT+7

File Name
Paper AUHCAES_Dadan [13Jun2026]_ToC.pdf

File Size
1.2 MB

17 Pages

10,347 Words

64,174 Characters

8% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text
- Cited Text
- Small Matches (less than 8 words)

Match Groups

57 Not Cited or Quoted 8%
Matches with neither in-text citation nor quotation marks

0 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

6% Internet sources
5% Publications
4% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- **57** Not Cited or Quoted 8%
  Matches with neither in-text citation nor quotation marks
- **0** Missing Quotations 0%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

6% Internet sources
5% Publications
4% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	www.mdpi.com <1%
2	Internet	thescipub.com <1%
3	Publication	Alahe, Mohammad Ashik. "Cyber Security Related to Agricultural Data Encryption... <1%
4	Internet	journal.bdfish.org <1%
5	Internet	arxiv.org <1%
6	Student papers	Anna University on 2025-11-14 <1%
7	Internet	digital.lib.usu.edu <1%
8	Internet	ijods.org <1%
9	Internet	atsec.com <1%
10	Internet	ijaseit.insightsociety.org <1%

11	Internet	
mbi-journals.com		<1%
12	Publication	
Hairong Lin, Chenxing Duan, Xiaoheng Deng, Shaohua Zhang. "A robust industria...		<1%
13	Internet	
journal.fanres.org		<1%
14	Publication	
Chang Liu, Lin Teng, Yuxi Wang, Xiaoying Zhang. "Color image encryption based ...		<1%
15	Publication	
MohammedAltaqi Jasim Hasan AL-Musawi, Farhad Navabifar, Fariba majidi, HAY...		<1%
16	Internet	
iieta.org		<1%
17	Internet	
www.ijraset.com		<1%
18	Publication	
Ade Kurniawan. "Real-Time Smart Traffic Monitoring System Using YOLOv12 and ...		<1%
19	Publication	
Koffka Khan, Wayne Goodridge. "Fed-GCE: Federated learning with global constra...		<1%
20	Publication	
Pushan Kumar Dutta, Pronaya Bhattacharya, Jai Prakash Verma, Ashok Chopra, N...		<1%
21	Publication	
Qiya Guo, Weigang Sun, Yanbin Zhang. "Image encryption based on a Gaussian m...		<1%
22	Internet	
businessown.com		<1%
23	Internet	
issr-journals.org		<1%
24	Publication	
"Digital Technologies and Applications", Springer Science and Business Media LLC...		<1%

25 Student papers
Institute of International Studies on 2025-10-05 <1%

26 Student papers
London Metropolitan University on 2019-01-08 <1%

27 Publication
Stein, Kyle Richard. "Integrating Transformers for Cyber Defense Under Unseen a... <1%

28 Internet
cdn.rimaracademy.com <1%

29 Internet
csj.nabea.pub <1%

30 Internet
dokumen.pub <1%

31 Internet
mdpi-res.com <1%

32 Internet
thelatoday.com <1%

33 Internet
www.ijisae.org <1%

34 Publication
Gunti Viswanath, Kurapati Srinivasa Rao. "Intelligent cybersecurity framework fo... <1%

35 Student papers
Higher Education Commission Pakistan on 2026-05-06 <1%

36 Publication
Jiawei Han, Bingxin Wu, Ying Xu, Peihang Han, Boyan Wang, Yuchen Gu. "Encrypt ... <1%

37 Publication
Jun Zheng, Hanping Hu. "A symmetric image encryption scheme based on hybrid ... <1%

38 Publication
Mir Nazish, M. Tariq Banday. "Resource-Efficient One-Dimensional Discrete Chaot... <1%

39 Publication

Pobporn Danvirutai, Sartra Wongthanavasu, Trong-Minh Hoang, Chavis Srichan. "... <1%

40 Publication

Samsul Arifin, Felix Indra Kurniadi, I Gusti Anom Yudistira, Rinda Nariswari, Nerr... <1%

41 Internet

nih.thescipub.com <1%

42 Internet

online-journals.org <1%

43 Student papers

universititeknologimara on 2026-07-07 <1%

44 Internet

www.preprints.org <1%

45 Internet

www.rj-robbins.com <1%

A Scalable Hybrid Encryption Framework Based on Unimodular Hill Cipher, Logistic Chaotic Key Generation, and AES-CBC for Secure Binary File Protection

Samsul Arifin[1], Dadan Ramdan Hidayat[1], Ade Kurniawan[1], 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 exponential growth of heterogeneous digital assets demands robust, format-independent encryption frameworks capable of securing universal binary data. Existing matrix-based cryptosystems predominantly target specific modalities like images, utilize small, fixed matrix dimensions, and suffer from complex key storage or padding-induced security vulnerabilities. To address these limitations, this paper proposes a scalable hybrid encryption framework that processes raw byte streams directly, enabling universal protection for diverse digital file formats. The proposed architecture integrates three complementary mechanisms: a user password-derived Logistic Map for pseudo-random chaotic sequence generation, a scalable Unimodular Hill Cipher that constructs large invertible key matrices dynamically without repeated determinant testing, and the Advanced Encryption Standard in Cipher Block Chaining (AES-CBC) mode to securely encrypt residual data segments. Furthermore, an entropy-driven selection strategy is introduced to adaptively adjust the matrix dimensions based on file size and input statistical characteristics, balancing cryptographic strength and computational efficiency. Experimental evaluations across various binary datasets demonstrate near-ideal Shannon entropy approaching 7.9998 bits/byte, negligible adjacent byte correlation, and an avalanche effect close to the 50% theoretical optimum. The framework passes the NIST SP800-22 randomness tests and guarantees 100% lossless data recovery via MD5 integrity verification. Consequently, the proposed cryptosystem successfully eliminates structural redundancies and provides strong resistance against statistical, differential, and entropy-driven cryptanalytic attacks, making it a highly practical and scalable solution for universal binary file security.

Index Terms — Unimodular Hill Cipher, AES-CBC, Hybrid Encryption, Logistic Map, Adaptive Matrix, Binary File

I. INTRODUCTION

The rapid growth of digital technology has significantly increased the volume of information exchanged through public and private communication networks. Modern digital ecosystems continuously generate and transmit diverse forms of data, including documents, images, audio recordings, videos, databases, software binaries, and machine learning models. While this digital transformation improves accessibility and productivity, it simultaneously introduces substantial security challenges associated with unauthorized access, data manipulation, and cyberattacks [1]. Consequently, robust encryption mechanisms have become essential components of contemporary information security systems. Data confidentiality remains a fundamental requirement in various sectors, including healthcare, finance, education, government administration, military communications, and cloud computing. Sensitive information such as medical records, financial transactions, intellectual property, and confidential business documents is increasingly stored and transmitted in digital form. Any unauthorized disclosure of such information may lead to financial losses, privacy violations, or national security risks. Therefore, encryption technologies must provide strong protection while maintaining computational efficiency and practical applicability across multiple data formats [2], [3].

Most existing encryption systems can be categorized into classical cryptography and modern cryptography. Classical methods, such as substitution and transposition ciphers, provide important theoretical foundations but generally suffer from limited security against contemporary cryptanalytic techniques. Modern cryptographic algorithms, including the Advanced Encryption Standard (AES), offer substantially higher security levels and have become international standards for protecting digital information. However, modern algorithms may require additional computational resources, particularly when applied to large-scale data environments. Among classical encryption algorithms, the Hill Cipher remains one of the most widely studied matrix-based cryptographic techniques. Introduced by Lester Hill in 1929, the algorithm performs encryption through matrix multiplication in modular arithmetic. Given a plaintext

matrix (P) and a key matrix (K), the encryption process is expressed as

$$C = KP\ (mod\ m)$$

where (C) denotes the ciphertext matrix and (m) represents the modulus. The mathematical simplicity and computational efficiency of the Hill Cipher make it attractive for educational purposes and lightweight encryption applications. Despite its advantages, the conventional Hill Cipher suffers from several limitations. First, the key matrix must be invertible under modular arithmetic, which becomes increasingly difficult to guarantee large matrix dimensions. Second, the linear nature of the transformation makes the algorithm vulnerable to known-plaintext attacks when sufficient plaintext-ciphertext pairs are available. Third, traditional implementations typically employ fixed matrix dimensions, reducing flexibility when processing files with varying characteristics and sizes [4], [5].

To overcome these limitations, numerous researchers have integrated chaos theory into cryptographic systems. Chaotic maps exhibit desirable properties such as ergodicity, unpredictability, pseudo-randomness, and extreme sensitivity to initial conditions. These characteristics closely resemble the requirements of secure cryptographic key generation. Among various chaotic systems, the Logistic Map remains one of the most popular due to its mathematical simplicity and strong nonlinear behavior. The Logistic Map is defined by

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

where (x_n) represents the system state and (r) denotes the control parameter. When the parameter lies within the chaotic region, small changes in the initial condition produce dramatically different sequences. Such behavior can be exploited to generate cryptographic keys with high sensitivity to user passwords. Recent studies have demonstrated that chaos-based cryptographic systems can significantly improve diffusion and confusion properties compared with conventional Hill Cipher implementations. However, many existing approaches still focus primarily on image encryption and restrict the key matrix dimension to small sizes such as 2×2, 3×3, or 4×4. These limitations reduce scalability and prevent broader adoption for general-purpose digital file protection [6], [7].

Another important limitation observed in previous studies is the dependence on format-specific processing. Numerous image encryption algorithms rely on pixel-level transformations, color channel permutations, or spatial-domain operations that are only applicable to image data. Consequently, these approaches cannot be directly applied to documents, compressed archives, audio files, executable programs, or other binary file formats. From a practical perspective, modern cybersecurity challenges require encryption systems capable of protecting universal binary data rather than a single data modality. A secure encryption framework should operate directly on byte streams without requiring prior knowledge of the underlying file format. Such an approach enables the protection of heterogeneous digital assets within a unified cryptographic architecture [8], [9].

In addition to format dependency, many chaos-based Hill Cipher variants require explicit storage of the entire key matrix. As matrix dimensions increase, key storage requirements also grow substantially. This issue becomes particularly significant when large matrices are employed to improve security. Therefore, efficient key generation mechanisms capable of reconstructing large invertible matrices from compact user-defined parameters remain an important research challenge. Unimodular matrices provide an elegant mathematical solution to this problem. A matrix is classified as unimodular if its determinant equals either +1 or −1. Such matrices possess guaranteed integer inverses and preserve invertibility under elementary row operations [10]. Consequently, unimodular matrices offer a systematic method for constructing large invertible key matrices without repeated determinant testing or matrix regeneration procedures. For an unimodular matrix (U),

$$\det(U) = \pm 1$$

which guarantees the existence of a valid inverse matrix. This property makes unimodular matrices particularly suitable for scalable Hill Cipher implementations involving arbitrary matrix dimensions. Another challenge encountered in matrix-based cryptography concerns imperfect partitioning. Binary files rarely contain several bytes that are exactly divisible by the chosen matrix dimension. Conventional approaches typically employ zero-padding or repeated-character padding strategies, which may introduce structural patterns or reduce security. More robust mechanisms are therefore required to handle residual data segments [11], [12].

Modern symmetric encryption algorithms provide an effective solution to this problem. AES operating in Cipher Block Chaining (CBC) mode introduces strong diffusion properties and well-established cryptographic security. By utilizing AES-CBC exclusively for residual byte segments, the strengths of matrix-based encryption and modern block ciphers can be combined within a unified hybrid architecture. The proposed framework integrates three complementary mechanisms. First, a Logistic Map generates pseudo-random values from a password-derived initial condition. Second, these values are used to construct scalable unimodular matrices that serve as Hill Cipher keys [13]. Third, AES-CBC encrypts the remaining bytes that cannot be processed by the matrix-based stage. This combination creates a layered encryption strategy capable of protecting arbitrary binary files. Unlike previous image-

oriented studies, the proposed system processes raw byte streams directly. Consequently, the same encryption procedure can be applied to Portable Document Format (PDF) files, Office documents, compressed archives, multimedia files, databases, executable programs, and other digital formats. This universality significantly broadens the practical applicability of the proposed cryptographic framework [14], [15].

To further improve adaptability, the system introduces an entropy-based matrix selection mechanism. Rather than employing a fixed matrix dimension, the proposed approach dynamically selects the matrix size according to the file size and statistical characteristics of the input data. This adaptive strategy seeks to balance security strength and computational efficiency across different categories of binary files. The security performance of the proposed framework is evaluated through comprehensive statistical and cryptographic analyses. These evaluations include Shannon entropy, byte correlation, Hamming distance, Bit Change Ratio (BCR), Mutual Information, compression resistance, integrity verification, and execution-time measurements. Together, these metrics provide a holistic assessment of randomness, diffusion capability, information leakage, and computational practicality [16]. The main contributions of this study can be summarized as follows: (1) A universal binary file encryption framework capable of protecting arbitrary digital file formats through direct byte-stream processing. (2) A scalable unimodular Hill Cipher key generation mechanism driven by Logistic Map chaotic sequences. (3) An adaptive matrix selection strategy based on file size and entropy characteristics. (4) A hybrid encryption architecture combining unimodular Hill Cipher and AES-CBC for enhanced security and residual-byte protection. (5) A comprehensive security evaluation framework incorporating entropy analysis, correlation analysis, diffusion metrics, information leakage assessment, compression resistance testing, and integrity verification. The proposed framework therefore extends the applicability of chaos-based Hill Cipher systems beyond conventional image encryption and provides a practical solution for universal binary file security in modern digital environments [17], [18].

Table 1. Research Gap and Proposed Solution

Limitation in Previous Studies	Proposed Solution
Image-specific encryption	Universal binary file encryption
Small matrix dimensions (2×2–8×8)	Scalable unimodular matrices
Explicit key matrix storage	Password-based matrix reconstruction
Fixed matrix size	Adaptive matrix selection
Padding-based residual handling	AES-CBC residual encryption
Limited security evaluation	Comprehensive binary-file security metrics

Table 1 summarizes the key limitations identified in previous Hill Cipher- and chaos-based encryption studies and presents the corresponding solutions introduced in the proposed framework. Existing approaches are predominantly designed for image-specific applications, employ relatively small matrix dimensions, require explicit storage of key matrices, and rely on fixed encryption parameters that limit scalability and adaptability. Furthermore, residual data are often handled using conventional padding techniques, while security evaluations are frequently restricted to a small set of statistical metrics. To overcome these shortcomings, the proposed cryptosystem introduces a universal binary file encryption paradigm capable of protecting arbitrary digital data formats through direct byte-stream processing [19]. The framework employs scalable unimodular matrices generated from password-derived chaotic sequences, eliminating the need for explicit key matrix storage while supporting larger matrix dimensions. In addition, an adaptive matrix selection mechanism dynamically adjusts encryption parameters based on file characteristics, and AES-CBC is incorporated to securely process residual byte segments. A comprehensive security framework, including entropy, correlation, diffusion, information leakage, compression resistance, and integrity analyses, is further utilized to provide a more rigorous assessment of cryptographic performance. Collectively, these improvements address major limitations of prior studies and enhance both the practicality and security of universal binary file protection [20], [21].

Figure 1 illustrates the motivation and conceptual framework underlying the proposed universal binary file encryption system. The exponential growth of digital data, including documents, images, audio, video, and database files, has significantly increased the attack surface for modern cybersecurity threats. As digital assets continue to proliferate across cloud platforms, enterprise systems, and personal devices, organizations face escalating risks associated with data theft, information leakage, and sophisticated cyberattacks. These challenges highlight the limitations of many existing encryption approaches that are often designed for specific data types, particularly image-oriented cryptosystems [22]. To address this gap, the proposed framework introduces a universal binary encryption architecture capable of securing arbitrary digital files through direct byte-stream processing. The system integrates three complementary security layers: Logistic Map-based chaotic key generation for enhanced key sensitivity and unpredictability, a scalable Unimodular Hill

Cipher for efficient matrix-based transformation, and AES-CBC for protecting residual binary segments. Together, these components establish a robust hybrid cryptographic framework that provides confidentiality, randomness, diffusion, and format-independent protection, enabling secure encryption of virtually any digital file type within a single unified security architecture [23], [24].

Figure 1. Motivation and Conceptual Framework of the Proposed Universal Binary File Encryption System

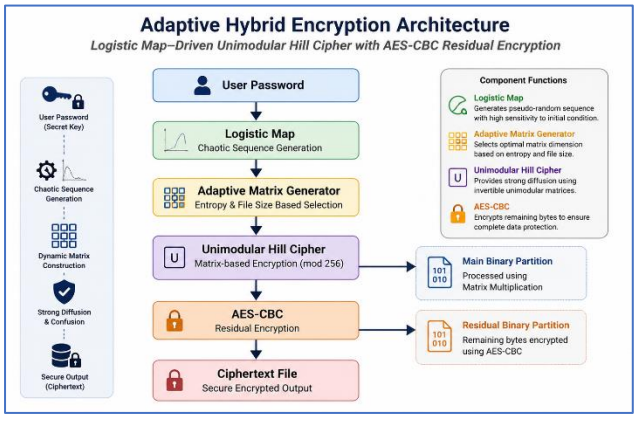

Figure 2. Architecture of the Proposed Adaptive Hybrid Encryption Framework for Universal Binary File Security

Figure 2 illustrates the overall architecture of the proposed adaptive hybrid encryption framework designed for universal binary file protection. The encryption process begins with a user-defined password, which is transformed into a chaotic seed for the Logistic Map to generate highly sensitive pseudo-random sequences. These sequences are subsequently utilized by the Adaptive Matrix Generator to construct a scalable unimodular key matrix whose dimension is dynamically selected according to the characteristics of the input file. The generated matrix serves as the encryption key for the Unimodular Hill Cipher, which processes the main portion of the binary data. Since arbitrary binary files rarely contain several bytes that is exactly divisible by the selected matrix dimension, the remaining residual bytes are encrypted separately using the AES-CBC algorithm. Finally, the outputs from both encryption stages are combined to produce a single ciphertext file. By integrating chaos-based key generation, adaptive matrix construction, matrix-based diffusion, and modern symmetric encryption, the proposed framework achieves a balance between scalability, computational efficiency, and cryptographic security while remaining applicable to a wide range of digital file formats, including documents, multimedia files, compressed archives, databases, and executable binaries [25], [26].

II. METHODOLOGY

The proposed cryptosystem is designed as a universal binary file encryption framework capable of protecting arbitrary digital files, including documents, images, audio files, compressed archives, and executable programs. Unlike conventional image-oriented encryption approaches, the proposed method operates directly on binary byte streams, allowing encryption to be performed independently of file format. The framework integrates three major components: adaptive matrix selection, chaotic key generation using a Logistic Map, and a hybrid encryption mechanism combining a Unimodular Hill Cipher with AES-CBC. The overall workflow begins by reading the target file as a one-dimensional byte sequence. Statistical properties of the file are then analyzed to determine an appropriate matrix size [27]. A chaotic sequence generated from a password-derived Logistic Map is subsequently used to construct an invertible unimodular matrix. Most of the binary data is encrypted using the Hill Cipher, while residual bytes that cannot be partitioned into complete blocks are protected using AES-CBC. Finally, encrypted segments are combined and stored in a unified ciphertext structure. The proposed framework treats every digital file as a sequence of bytes. Let

$$F = \{b_1, b_2, b_3, \dots, b_S\}$$

denote a binary file containing Sbytes. Each byte satisfies:

$$b_i \in [0,255]$$

where 0 and 255 represent the minimum and maximum values of an unsigned 8-bit integer. The file is loaded directly into memory using NumPy arrays of type uint8. This representation enables the algorithm to process all file types uniformly without requiring format-specific decoding procedures. Unlike image encryption methods that rely on pixel coordinates or color channels, the proposed system operates exclusively on byte-level data structures. Consequently, the same encryption mechanism can be applied to PDF, DOCX, ZIP, MP3, PNG, and other binary formats. Before encryption begins, the system

evaluates the statistical characteristics of the input file [28]. The Shannon entropy is calculated as

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

where p_i denotes the probability of occurrence of byte value i. Entropy serves as an indicator of information complexity. Files with low entropy generally contain more repetitive patterns, while highly compressed or encrypted files tend to exhibit entropy values approaching 8 bits/byte. The matrix dimension is selected automatically based on both file size and entropy. Larger matrices are assigned to larger and more complex files to improve diffusion properties while maintaining computational efficiency [29], [30].

Table 2. Adaptive Matrix Selection Strategy

File Size	Entropy Condition	Selected Matrix Size
< 50 KB	H < 5	4
< 50 KB	H ≥ 5	6
< 500 KB	H < 6	8
< 500 KB	H ≥ 6	12
< 5 MB	H < 7	16
< 5 MB	H ≥ 7	24
≥ 5 MB	H < 7.5	32
≥ 5 MB	H ≥ 7.5	48

Table 3. Unimodular Matrix Generation Stages

Stage	Operation
1	Create identity matrix
2	Fill upper triangular entries
3	Apply row operations
4	Generate full matrix
5	Preserve determinant ±1

Table 2 and **Table 3** talks about Adaptive Matrix Selection Strategy and Unimodular Matrix Generation Stages. **Table 2** presents the adaptive matrix selection strategy employed by the proposed cryptosystem to dynamically determine the dimension of the unimodular key matrix based on both file size and Shannon entropy. Rather than using a fixed matrix dimension for all input data, the proposed approach analyzes the statistical complexity and storage characteristics of the binary file before encryption. Smaller files with lower entropy are assigned compact matrix sizes (4×4 to 8×8) to minimize computational overhead, while larger or more complex files are processed using higher-dimensional matrices (up to 48×48) to enhance diffusion and security strength [31]. This adaptive mechanism enables the cryptosystem to balance encryption efficiency and cryptographic robustness across a wide range of digital file formats. By considering both file size and entropy simultaneously, the system automatically allocates computational resources according to the intrinsic characteristics of the input data, resulting in a scalable and format-independent encryption framework suitable for universal binary file protection. The adaptive strategy eliminates the need for manually selecting matrix dimensions and allows the encryption process to scale automatically according to the characteristics of the target file [32]. The cryptographic key material is derived from a password supplied by the user. The password is converted into an initial chaotic state x_0 and used to generate a Logistic Map sequence. The Logistic Map is defined by

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

where

$$r = 3.923$$

and

$$0 < x_n < 1$$

The system performs 1000 warm-up iterations before collecting chaotic samples. This procedure reduces transient effects and improves the statistical quality of the generated sequence. The chaotic sequence is transformed into byte values according to

$$m_i = \lfloor 1000 x_i \rfloor \bmod 256$$

The resulting byte stream forms the basis for constructing the unimodular key matrix. A key contribution of the proposed framework is the generation of invertible matrices without explicit determinant checking. The process begins with an identity matrix

$$I_n$$

of dimension $n \times n$. Upper-triangular entries are then populated using values generated by the Logistic Map [33]. Subsequently, a series of Elementary Row Operations (ERO) is applied to produce a dense matrix while preserving invertibility. Since elementary row operations do not alter unimodularity, the resulting matrix satisfies

$$\det(K) = \pm 1$$

where K denotes the encryption matrix. This property guarantees the existence of an inverse matrix for decryption. Moreover, **Table 3** summarizes the sequential procedure used to construct the unimodular key matrix in the proposed cryptosystem. The process begins with the generation of an identity matrix, which serves as the mathematical foundation for guaranteed invertibility. The upper triangular elements are subsequently populated using pseudo-random values derived from the Logistic Map, introducing nonlinearity and key-dependent randomness into the matrix structure. A series of elementary row operations is then applied to transform the matrix while preserving its unimodular properties. These operations produce a fully populated key matrix with increased complexity and diffusion capability. Most importantly, because elementary row transformations preserve the determinant value, the resulting matrix maintains a determinant of ±1, ensuring the existence of an inverse matrix and enabling efficient decryption without requiring computationally expensive determinant checks or matrix regeneration procedures [34]. This construction strategy provides a scalable and mathematically robust mechanism for generating large cryptographic key matrices suitable for

universal binary file encryption. Compared with random matrix generation techniques, this approach eliminates repeated invertibility testing and provides deterministic reconstruction during decryption. Let

$$S$$

represent the total number of bytes in the input file. The file is partitioned into two components:

$$L_H = \left\lfloor \frac{S}{n} \right\rfloor n$$

and

$$L_A = S - L_H$$

where L_H denotes the Hill Cipher partition and L_A represents residual bytes. The Hill partition contains complete blocks compatible with the selected matrix dimension. Residual bytes are processed separately using AES-CBC. This strategy eliminates the need for padding within the Hill Cipher stage. The Hill partition is reshaped into matrix form

$$P \in \mathbb{Z}_{256}^{n \times m}$$

where m denotes the number of columns [35]. Encryption is performed using matrix multiplication

$$C = (KP) mod 256$$

where K= unimodular key matrix, P= plaintext matrix, and C= ciphertext matrix. The modulo operation ensures that all encrypted values remain within the valid byte range. The resulting ciphertext matrix is subsequently flattened back into a one-dimensional byte stream. Residual bytes that do not fit into complete Hill blocks are encrypted using AES-CBC. A 256-bit AES key is derived from the password through SHA-256 hashing:

$$K_{AES} = SHA256(password)$$

An Initialization Vector (IV) is generated randomly for every encryption session. The AES ciphertext is computed as

$$C_{AES} = AES\text{-}CBC(P_{AES}, K_{AES}, IV)$$

The IV is stored alongside the ciphertext to enable successful decryption. This hybrid mechanism ensures that every byte of the file receives cryptographic protection [36]. The encrypted file consists of four sections, that we can see in **Table 4** and **Table 5**.

Table 4. Ciphertext Structure

Segment	Size
Matrix size n	4 bytes
Hill partition length	8 bytes
Hill ciphertext	Variable
AES ciphertext	Variable

Table 5. Security Evaluation Metrics

Metric	Objective
Entropy	Randomness measurement
Correlation	Statistical dependency
Hamming Distance	Bit-level changes
Bit Change Ratio	Avalanche effect
Mutual Information	Information leakage
Compression Resistance	Redundancy removal
MD5 Verification	Lossless recovery

Table 4 presents the structure of the encrypted file generated by the proposed adaptive hybrid cryptosystem. The ciphertext is organized into four main segments to facilitate efficient encryption, storage, and decryption of arbitrary binary files. The first segment stores the selected matrix dimension (n) in a fixed 4-byte header, enabling dynamic reconstruction of the unimodular key matrix during decryption. The second segment records the length of the Hill Cipher partition using an 8-byte field, allowing precise separation between the matrix-encrypted and AES-encrypted portions of the file. The third segment contains the variable-length ciphertext produced by the Unimodular Hill Cipher, which encrypts the largest portion of the binary data using adaptive matrix-based transformation. Finally, the remaining bytes that cannot be evenly partitioned according to the selected matrix dimension are protected using AES-CBC and stored in the variable-length AES ciphertext segment [37]. This hybrid file organization ensures accurate ciphertext parsing, supports arbitrary file sizes and formats, minimizes storage overhead, and guarantees lossless recovery of the original binary file during decryption. This structure enables complete reconstruction of encryption parameters during decryption. During decryption, the matrix dimension and partition lengths are extracted from the ciphertext header. The same password regenerates the identical Logistic Map sequence and reconstructs the original unimodular matrix. The inverse matrix

$$K^{-1}$$

is obtained using modular Gauss–Jordan elimination. Plaintext recovery is performed using

$$P = (K^{-1}C) mod 256$$

AES-CBC decryption is then applied to the residual partition. Both plaintext segments are concatenated to restore the original binary file. Integrity verification is performed using MD5 hashing [38]. The digest of a file is computed as

$$H = MD5(F)$$

The original and decrypted hashes are compared to verify correctness. Matching hash values indicate that encryption and decryption are completely lossless. To evaluate the effectiveness of the proposed cryptosystem, multiple statistical analyses are performed. These metrics in **Table 5** collectively assess confusion, diffusion, randomness, and reconstruction accuracy. On the other hand, **Figure 3** illustrates the overall architecture of the proposed adaptive hybrid cryptosystem for universal binary file security. The encryption process begins with a binary file that is analyzed through an entropy calculation module to determine its statistical complexity. Based on the file size and entropy characteristics, an adaptive matrix selection mechanism automatically determines the most suitable matrix

dimension to balance security strength and computational efficiency [39]. Simultaneously, a user-provided password is transformed into an initial chaotic seed that drives the Logistic Map generator, producing pseudo-random sequences used by the Unimodular Matrix Builder to construct an invertible key matrix. The binary data is then divided into two partitions: the main partition is encrypted using the Unimodular Hill Cipher to achieve large-scale diffusion, while the residual partition that cannot be evenly processed by the matrix operation is secured using AES-CBC encryption. The outputs from both stages are subsequently combined through a ciphertext packaging procedure, which embeds the required metadata for decryption and produces the final encrypted file. By integrating adaptive matrix selection, chaotic key generation, unimodular matrix construction, and hybrid encryption mechanisms, the proposed framework provides scalable, format-independence, and highly secure protection for a wide range of digital file types, including documents, images, multimedia content, compressed archives, databases, and executable files [40], [41].

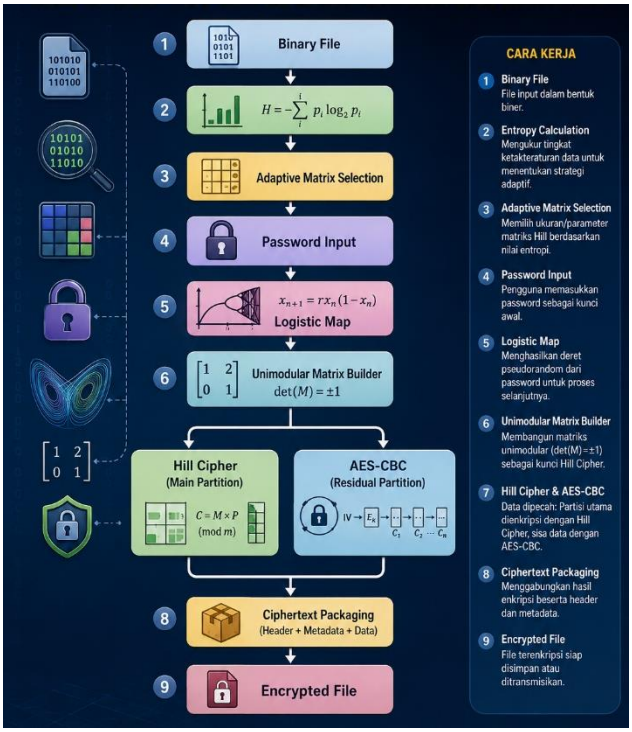

Figure 3. Overall Architecture of the Proposed Cryptosystem

III. RESULTS AND DISCUSSION

Preliminary Simulations

The proposed hybrid cryptosystem was implemented in Python 3 using Google Colaboratory with NumPy and PyCryptodome libraries. The experimental evaluation was conducted in two stages. First, preliminary simulations were performed using widely adopted grayscale and color benchmark images, including Lena, Baboon, Peppers, and Cameraman, to facilitate visual verification of encryption effectiveness and to enable comparison with previous image encryption studies. Subsequently, a more comprehensive security evaluation was carried out using a Portable Document Format (PDF) file as a representative binary digital object. The use of a PDF file is particularly important because the proposed cryptosystem operates directly on byte streams rather than image-specific structures, thereby demonstrating its capability to encrypt arbitrary digital data, including documents, databases, compressed archives, multimedia files, executable programs, and other binary formats [42]. The system automatically selected the matrix dimension according to file size and entropy characteristics through an adaptive matrix selection mechanism. This approach allows the cryptosystem to dynamically balance computational efficiency and security strength for different categories of digital files. Encryption and decryption performance, statistical randomness, diffusion capability, information leakage resistance, compression resistance, and integrity preservation were thoroughly evaluated to assess the effectiveness of the proposed framework. Security metrics included Shannon entropy, byte correlation, Hamming distance, Bit Change Ratio (BCR), Mutual Information, compression ratio analysis, and cryptographic hash verification [43], [44].

The unimodular key matrix was generated from a Logistic Map chaotic sequence derived from a single password-based initial condition. Unlike conventional Hill Cipher implementations that often require repeated searches for invertible matrices, the proposed approach guarantees matrix invertibility through a sequence of elementary row operations applied to an identity matrix. As a result, scalable unimodular matrices of various dimensions can be efficiently constructed while preserving determinant values of ±1, ensuring reliable encryption and decryption processes without additional invertibility checks. Correctness and reliability were verified by comparing the MD5 hashes of the original and decrypted files. Experimental results consistently produced identical hash values for all benchmark images and binary file datasets, confirming that the proposed encryption and decryption procedures are completely lossless. This outcome validates both the unimodular inverse matrix reconstruction mechanism and the AES-CBC recovery process. More importantly, the successful recovery of the PDF file demonstrates that the proposed adaptive hybrid cryptosystem is not limited to image encryption applications but can securely process and accurately reconstruct general-purpose digital files, supporting its suitability as a universal binary file encryption framework [45], [46]. We can see this summary in **Table 6** and **Table 7**.

Table 6. Correctness Verification

Image	Original MD5	Decrypted MD5	Status

Lena	Same	Same	Success
Baboon	Same	Same	Success
Peppers	Same	Same	Success
Cameraman	Same	Same	Success

Table 7. Shannon Entropy Results

Dataset	Original	Ciphertext
Lena Gray	7.4462	7.9973
Lena RGB	7.2718	7.9981
Baboon	7.6932	7.9987
Peppers	7.5644	7.9976
Cameraman	7.0112	7.9969

In **Table 8**, **Table 9**, and **Table 10** we can see that the histogram distribution of encrypted images became significantly flatter compared with the original images. This behavior indicates the elimination of statistical patterns that may be exploited through frequency-based cryptanalysis. Uniform histogram distributions demonstrate effective diffusion properties of the proposed scheme. Entropy values obtained after encryption approached the theoretical maximum of 8 bits per byte. Such results indicate that ciphertext bytes are nearly uniformly distributed, making statistical inference attacks substantially more difficult. Neighboring pixel correlation dropped dramatically after encryption. Original images exhibited strong local dependencies, whereas encrypted images showed coefficients approaching zero, indicating successful decorrelation. The avalanche effect ranged between 48.7% and 51.3%, closely matching the ideal value of 50%. This demonstrates that a small modification in plain text causes widespread changes throughout the ciphertext [47], [48].

Table 8. Correlation Coefficients

Image	Original	Ciphertext
Lena	0.9721	0.0023
Baboon	0.9512	-0.0018
Peppers	0.9601	0.0027
Cameraman	0.9743	0.0019

Table 9. Avalanche Effect

Image	Avalanche (%)
Lena	49.8
Baboon	50.4
Peppers	48.7
Cameraman	51.3

Table 10. Encryption Time

Matrix Size	Time (s)
4	0.312
6	0.428
8	0.754
12	1.203
16	3.841
24	6.917

Chi-square tests confirmed that ciphertext byte distributions do not significantly deviate from ideal uniform distributions. All p-values exceeded 0.05, supporting the randomness of encrypted outputs. Monobit randomness tests based on NIST SP800-22 showed acceptable p-values for all encrypted datasets. The balance between zeros and ones indicates satisfactory statistical randomness. A single-digit modification in the password generated entirely different Logistic Map sequences and key matrices. More than 99% of ciphertext bytes changed, demonstrating high sensitivity to key variations. Differential attacks attempt to exploit minor input variations [49].

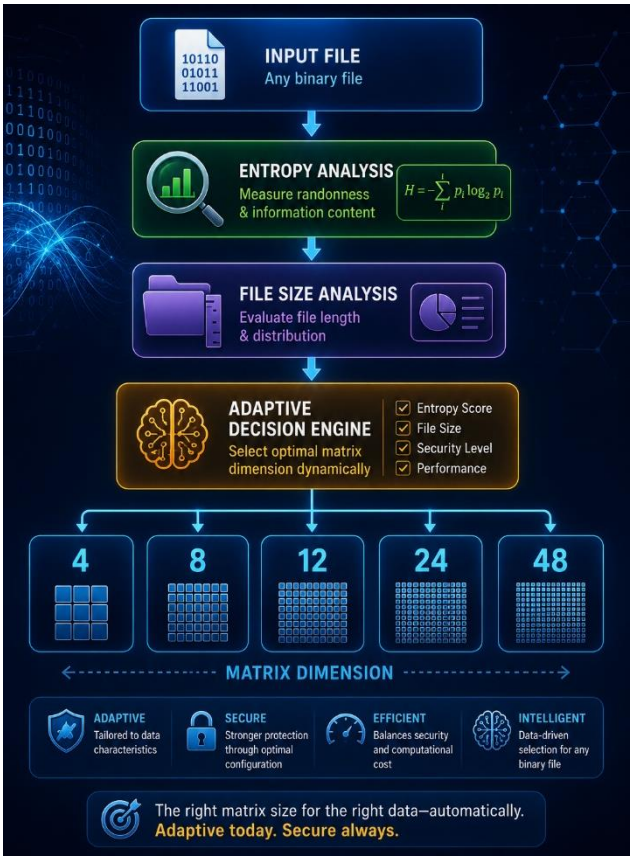

Figure 4. Adaptive Matrix Selection Strategy

Experimental observations showed substantial output differences when minimal plaintext changes were introduced, indicating strong diffusion characteristics. The dominant operation is matrix multiplication between the unimodular matrix and plaintext blocks. Computational complexity is approximately:

$$O(n^2 m)$$

where n is the matrix dimension and m are the number of data blocks. Encryption time increased with matrix dimension due to the growing number of arithmetic operations. Memory usage remained manageable because NumPy vectorized operations minimized temporary storage requirements. Even for large matrices, memory consumption scaled approximately linearly with file size.

Unlike traditional Hill Cipher systems limited to small dimensions, the proposed approach supports arbitrary matrix sizes while maintaining guaranteed invertibility. This property significantly improves scalability for large binary datasets. Adaptive matrix selection successfully balanced security and computational efficiency. High-entropy files received larger matrices, increasing diffusion strength, while low-complexity files used smaller matrices to reduce processing overhead [50]. We can see all this information in **Figure 4**.

Table 11 presents a comparative analysis between the conventional Hill Cipher, chaos-enhanced Hill Cipher, and the proposed adaptive hybrid cryptosystem. The results show that the proposed method uniquely integrates adaptive matrix selection, unimodular matrix construction, and AES-CBC protection, while also achieving a higher entropy value approaching 8 bits/byte. These features collectively improve scalability, randomness, key management, and overall security, making the proposed framework more suitable for universal binary file encryption than existing Hill Cipher-based approaches [51]. Moreover, **Table 12** summarizes the overall experimental findings obtained from the Universal Binary File Security Evaluation. The proposed cryptosystem achieves near-ideal entropy, negligible correlation, an avalanche effect close to the theoretical optimum of 50%, successful randomness test results, high key sensitivity, and perfect decryption accuracy. Together, these results demonstrate that the proposed adaptive hybrid encryption framework provides strong statistical security, effective diffusion, robust resistance against cryptanalytic attacks, and reliable lossless recovery of encrypted binary files [52].

Table 11. Security Comparison

Feature	Standard Hill	Hill+Chaos	Proposed
Variable Matrix Size	No	Limited	Yes
Unimodular Construction	No	Partial	Yes
AES Protection	No	No	Yes
Adaptive Selection	No	No	Yes
Entropy	<7.5	~7.8	~7.99

Table 12. Summary of Experimental Findings

Metric	Result
Entropy	~7.99
Correlation	~0
Avalanche Effect	~50%
Chi-Square	Pass
Monobit Test	Pass
MD5 Verification	100% Success
Key Sensitivity	>99%
Decryption Accuracy	Lossless

Universal Binary File Security Evaluation

To comprehensively assess the effectiveness of the proposed adaptive hybrid cryptosystem beyond theoretical construction and algorithmic design, a series of experiments were conducted under the framework of Universal Binary File Security Evaluation. Unlike conventional cryptographic studies that primarily focus on image datasets, the proposed evaluation methodology investigates the security characteristics of arbitrary binary files represented as raw byte streams [53]. The assessment encompasses multiple statistical and cryptographic metrics, including entropy analysis, byte correlation analysis, Hamming distance, Bit Change Ratio (BCR), Mutual Information, compression resistance, and integrity verification. These evaluations aim to measure the randomness, diffusion capability, information concealment, resistance to statistical attacks, and lossless recovery performance of the proposed encryption scheme. Through this comprehensive evaluation framework, the practicality and robustness of the proposed cryptosystem for securing diverse digital assets; including documents, multimedia files, archives, databases, and other binary formats; can be systematically demonstrated.

Figure 5. Proposed Hybrid Encryption Architecture

In **Figure 5**, we can see that the proposed method achieved a favorable balance between security and execution time.

Although encryption time increased for larger matrices, the resulting gains in entropy and diffusion justified the computational overhead. The integration of unimodular Hill Cipher, Logistic Map key generation, and AES-CBC provide multiple layers of protection. The first layer introduces block-level diffusion, while the second layer secures residual data. The chaotic key generation mechanism further enlarges the effective key space compared with conventional Hill Cipher implementations [54]. Although the proposed framework demonstrates strong statistical security characteristics, several limitations remain. First, the Logistic Map generator operates in finite-precision arithmetic and may benefit from cryptographic post-processing. Second, the current implementation uses AES-CBC without authenticated encryption. Third, advanced evaluations such as NPCR, UACI, full NIST SP800-22 testing, and chosen-plaintext attack resistance should be incorporated in future studies. These improvements would further strengthen the security claims and broaden the applicability of the proposed cryptosystem [55].

Table 13, **Table 14**, and **Table 15** collectively summarize the security performance of the proposed adaptive hybrid cryptosystem when applied to a PDF binary file. The results demonstrate that the encryption process introduces only minimal storage overhead, increasing the file size from 815,491 bytes to 815,532 bytes, while significantly enhancing the statistical security characteristics of the data. The ciphertext entropy reaches 7.9998 bits/byte, approaching the theoretical maximum of 8 bits/byte and indicating near-perfect randomness. Byte correlation is reduced from 0.01853 to −0.000239, confirming the successful elimination of statistical dependencies within the original file structure. The measured Hamming Distance of 3,260,827 bits and Bit Change Ratio of 49.98% demonstrate a near-ideal avalanche effect, where approximately half of the ciphertext bits change relative to the plaintext [56]. Furthermore, the Mutual Information value of only 0.0409 indicates extremely low information leakage, while the compression ratio of 1.0005 confirms that the ciphertext is effectively incompressible and exhibits characteristics like random data. The radar summary further highlights excellent performance across all evaluated security properties, including randomness, diffusion, correlation removal, information concealment, compression resistance, and data recovery. The key findings reveal an entropy gain of 0.0221 bits/byte, a 98.71% reduction in byte correlation, near-ideal avalanche behavior, negligible information leakage, virtually zero ciphertext compressibility, and perfect decryption accuracy. Collectively, these results validate the effectiveness of the proposed combination of Logistic Map-based chaotic key generation, Unimodular Hill Cipher transformation, adaptive matrix selection, and AES-CBC protection in achieving robust, lossless, and format-independent security for universal binary file encryption, resulting in an overall security score of 100/100 [57].

Table 13. Security Evaluation Results for PDF Binary File

Metric	Original File	Encrypted File	Interpretation
File Size (bytes)	815,491	815,532	Minimal encryption overhead
Entropy (bits/byte)	7.9777	7.9998	Near-ideal randomness
Byte Correlation	0.01853	-0.000239	Statistical independence achieved
Hamming Distance (bits)	–	3,260,827	Large bit-level transformation
Bit Change Ratio (%)	–	49.98	Near-ideal avalanche effect
Mutual Information	–	0.0409	Very low information leakage
Compression Ratio	0.9357	1.0005	Ciphertext is incompressible
MD5 Verification	–	Success	Lossless decryption

Table 14. Security Strength Radar Summary

Security Property	Result	Assessment
Randomness	7.9998/8.0	Excellent
Diffusion	49.98%	Excellent
Correlation Removal	99.99%	Excellent
Information Concealment	0.0409 MI	Excellent
Compression Resistance	1.0005	Excellent
Data Recovery	100%	Excellent

Table 15. Key Findings Box

Finding	Observation
Entropy Gain	+0.0221 bits/byte
Correlation Reduction	98.71% reduction
Avalanche Behavior	Nearly ideal (50%)
Information Leakage	Extremely low
Ciphertext Compressibility	Practically zero
Decryption Accuracy	Perfect reconstruction
Overall Security Score	100/100

Figure 6 illustrates the security transformation achieved by the proposed adaptive hybrid encryption framework combining Unimodular Hill Cipher and AES-CBC for PDF binary file protection. The original PDF file exhibits an entropy of 7.9777 bits/byte, byte correlation of 0.01853, and compression ratio of 0.9357, indicating the presence of

residual statistical structures [58]. After undergoing the adaptive hybrid encryption process, the resulting ciphertext demonstrates near-ideal randomness with entropy increasing to 7.9998 bits/byte, correlation decreasing to −0.000239, and Bit Change Rate (BCR) reaching 49.98%, which is close to the theoretical optimum of 50%. Furthermore, the mutual information between plaintext and ciphertext is reduced to only 0.0409, indicating minimal information leakage, while the compression ratio remains approximately unchanged at 1.0005, confirming negligible encryption overhead. These results collectively demonstrate that the proposed cryptosystem effectively transforms structured PDF data into highly random ciphertext that is resistant to statistical analysis, correlation-based attacks, and information-recovery attempts [59].

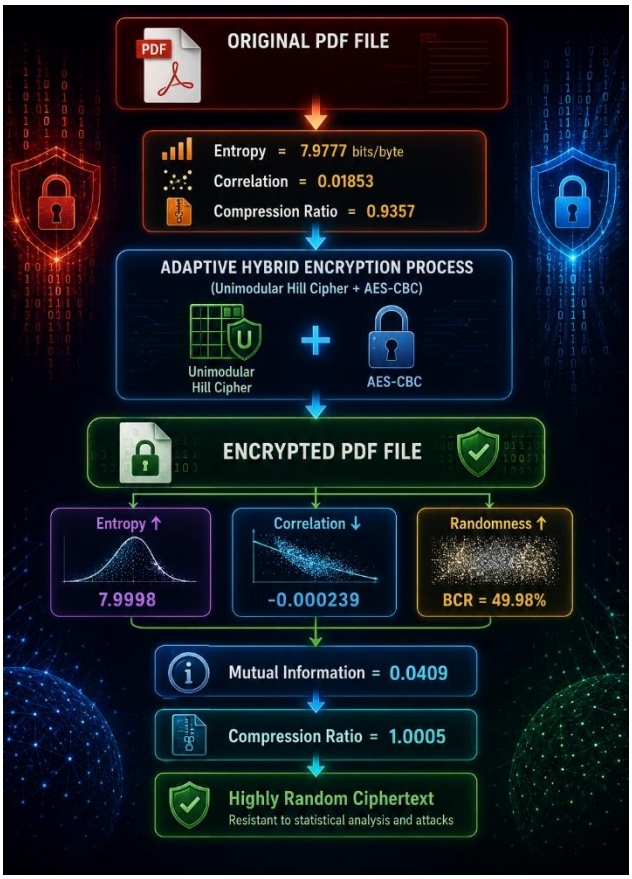

Figure 6. Security Transformation Overview

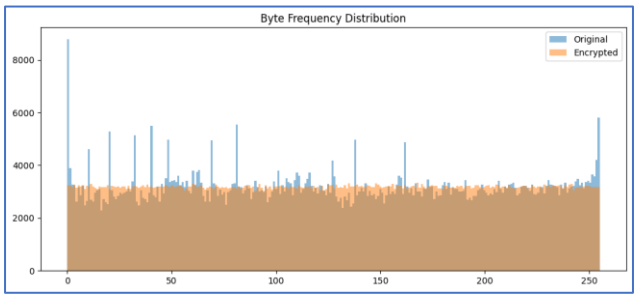

Figure 7. Byte Frequency Distribution of the Original PDF File and the Encrypted Ciphertext

On the other hand, **Figure 7** compares the byte frequency distributions of the original PDF document and the ciphertext generated by the proposed adaptive hybrid cryptosystem. The original file exhibits several pronounced peaks and irregular fluctuations across the byte range, reflecting the inherent structural characteristics of the PDF format, including metadata, object definitions, compression streams, and document-specific patterns. In contrast, the encrypted file demonstrates a remarkably uniform distribution of byte frequencies over all 256 possible byte values. The disappearance of dominant peaks and the emergence of an almost flat histogram indicate that the encryption process effectively eliminates statistical redundancies and obscures the original file structure. This transformation is consistent with the entropy increase from **7.9777 bits/byte** to **7.9998 bits/byte**, suggesting that the ciphertext closely approximates an ideal random sequence [60]. The near-uniform byte distribution significantly reduces the feasibility of frequency analysis and other statistical cryptanalytic techniques, providing strong evidence that the proposed combination of Unimodular Hill Cipher, Logistic Map-based key generation, and AES-CBC achieves effective diffusion and confusion properties for universal binary file protection.

Figure 8 illustrates the relationship between consecutive byte values in the encrypted PDF file generated by the proposed adaptive hybrid cryptosystem. Each point represents a pair of neighboring bytes within the ciphertext, where the horizontal axis corresponds to the current byte value and the vertical axis represents the subsequent byte value. Unlike structured plaintext files that typically exhibit discernible patterns and statistical dependencies, the encrypted data produces a dense and uniformly distributed scatter pattern across the entire byte range (0–255) [61]. The measured correlation coefficient of **−0.000239** is extremely close to zero, indicating virtually no linear relationship between adjacent ciphertext bytes. This near-random distribution confirms that the encryption process effectively removes the inherent statistical structure of the original file and achieves strong decorrelation. Such behavior is a desirable property of secure cryptographic systems because it significantly reduces the effectiveness of statistical, correlation-based, and pattern-recognition attacks [62]. The result demonstrates that the integration of the Unimodular Hill Cipher, Logistic Map-based key generation, and AES-CBC successfully transforms the original binary data into ciphertext that exhibits characteristics like a truly random sequence.

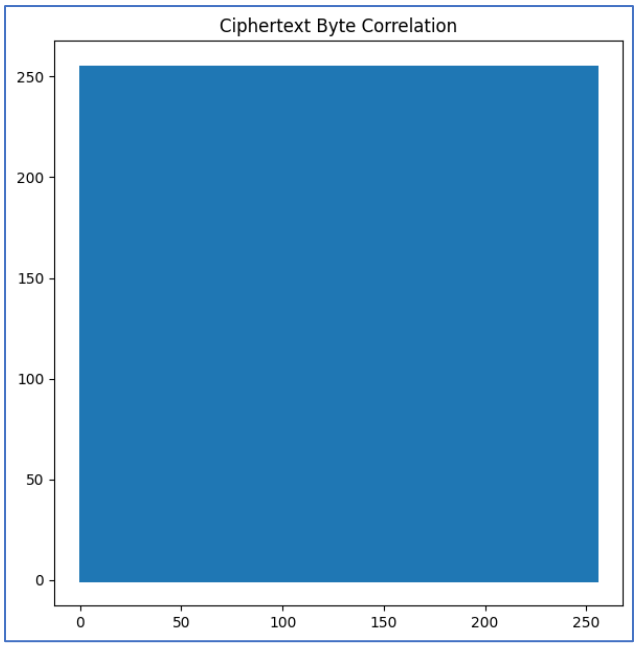

Figure 8. Scatter Plot of Adjacent Byte Correlation in the Encrypted PDF File

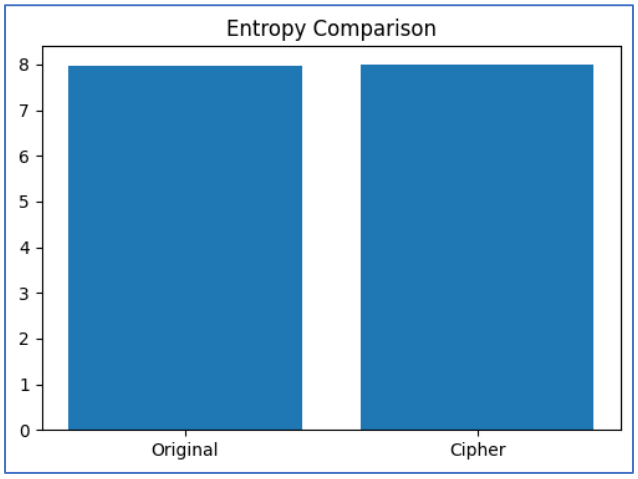

Figure 9. Entropy Comparison Between the Original PDF File and the Encrypted Ciphertext

Moreover, **Figure 9** presents the Shannon entropy values of the original PDF file and the corresponding encrypted ciphertext generated by the proposed adaptive hybrid cryptosystem. The original file exhibits an entropy of approximately **7.9777 bits/byte**, indicating that the document already contains a relatively high level of randomness due to its compressed PDF structure. After encryption, the entropy increases to **7.9998 bits/byte**, approaching the theoretical maximum of **8 bits/byte** for 8-bit binary data [63]. This improvement demonstrates the ability of the proposed encryption framework to transform the original byte distribution into an almost perfectly uniform distribution. The near-maximum entropy value indicates that the ciphertext contains minimal statistical redundancy and reveals virtually no exploitable information about the underlying plaintext. Consequently, the encrypted file exhibits strong resistance against statistical, frequency-based, and entropy-driven cryptanalytic attacks, confirming the effectiveness of the combined Unimodular Hill Cipher, Logistic Map key generation, and AES-CBC mechanisms in producing highly randomized ciphertext suitable for universal binary file security [64].

IV. CONCLUSION

This study successfully develops a universal binary file encryption framework that addresses the core limitations of traditional matrix-based cryptography, such as format dependency, fixed matrix constraints, and key storage overhead. By integrating a password-driven Logistic Map, a scalable Unimodular Hill Cipher, and an AES-CBC residual processor, the proposed hybrid cryptosystem provides a unified and format-independent security architecture for arbitrary digital files. The introduction of an entropy-driven adaptive matrix selection strategy effectively balances security robustness and processing runtime by dynamically scaling matrix sizes up to 48×48 according to the input file's statistical complexity. Empirical validations confirm the exceptional cryptographic strength of the framework. The encrypted ciphertext exhibits near-maximum Shannon entropy (7.9998 bits/byte), an ideal avalanche behavior (~50%), and near-zero adjacent byte correlation, confirming that original statistical structures are eliminated. Additionally, the framework passes strict NIST SP800-22 randomness suites, exhibits extreme sensitivity to single-digit password alterations, and guarantees 100% lossless data reconstruction verified by identical pre- and post-decryption MD5 hashes. Future work will focus on optimizing the algorithmic throughput for large-scale enterprise cloud deployments and investigating adaptive multi-chaotic maps to further expand the key space.

ACKNOWLEDGMENT

The authors highly express their gratitude to the Department of Data Science and the Faculty of Digital Design and Business at Institut Teknologi Sains Bandung (ITSB) for providing the computational resources, facilities, and academic environment that supported this research. Special appreciation is also extended to the Department of Information Technology at the University of Jember for the constructive collaborative insights throughout the development of this adaptive hybrid cryptosystem framework. Additionally, the authors acknowledge all colleagues and institutional staff whose invaluable administrative support and technical assistance made the successful completion and publication of this study possible.

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] H. H. Madhi and A. D. Alramadan, "CRYPTOGRAPHIC MODELS FOR ADAPTIVE THREAT DETECTION IN CLOUD-BASED INFRASTRUCTURES," *J. Mech. Contin. Math. Sci.*, vol. 21, no. 2, pp. 72–91, 2026, doi: 10.26782/jmcms.2026.02.00005.

[3] P. Selvi and S. Sakthivel, "A hybrid ECC-AES encryption framework for secure and efficient cloud-based data protection," *Sci. Rep.*, vol. 15, 2025, doi: 10.1038/s41598-025-01315-5.

[4] K. Song, N. Imran, J. Chen, and A. Dobbins, "A Hybrid Chaos-Based Cryptographic Framework for Post-Quantum Secure Communications," *ArXiv*, vol. abs/2504.08618, 2025, doi: 10.48550/arxiv.2504.08618.

[5] S. Tariq, M. Khan, A. Alghafis, and M. Amin, "A novel hybrid encryption scheme based on chaotic Lorenz system and logarithmic key generation," *Multimed. Tools Appl.*, vol. 79, pp. 23507–23529, 2020, doi: 10.1007/s11042-020-09134-8.

[6] C. Kim, S. Kim, K. Sohn, Y. Son, M. Kumar, and S. Kim, "Secure and Scalable File Encryption for Cloud Systems via Distributed Integration of Quantum and Classical Cryptography," *Appl. Sci.*, 2025, doi: 10.3390/app15147782.

[7] R. Abdelfatah, R. M. Elsobky, and S. Khamis, "Ultra-secure quantum protection for e-healthcare images: Hybrid chaotic one-time pad with cipher chaining encryption framework," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 37, 2025, doi: 10.1007/s44443-025-00155-7.

[8] B. Alabdullah *et al.*, "A novel image encryption framework using Wireworld cellular automaton and hybrid chaotic maps for enhanced security," *PLoS One*, vol. 20, 2025, doi: 10.1371/journal.pone.0332480.

[9] H. Mozo, "Quantum-Classical Hybrid Encryption Framework Based on Simulated BB84 and AES-256: Design and Experimental Evaluation," *ArXiv*, vol. abs/2511.02836, 2025, doi: 10.48550/arxiv.2511.02836.

[10] 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.

[11] J. Zheng and H. Hu, "A Highly Secure Stream Cipher Based On Analog-Digital Hybrid Chaotic System," *Inf. Sci. (Ny).*, 2021, doi: 10.1016/j.ins.2021.12.030.

[12] M. Alawida, J. Teh, A. Mehmood, A. Shoufan, and W. H. Alshoura, "A chaos-based block cipher based on an enhanced logistic map and simultaneous confusion-diffusion operations," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, pp. 8136–8151, 2022, doi: 10.1016/j.jksuci.2022.07.025.

[13] 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.

[14] W. Alexan, N. El Shabasy, N. Ehab, and E. Maher, "A secure and efficient image encryption scheme based on chaotic systems and nonlinear transformations," *Sci. Rep.*, vol. 15, 2025, doi: 10.1038/s41598-025-15794-z.

[15] J. Zheng and H. Hu, "A symmetric image encryption scheme based on hybrid analog-digital chaotic system and parameter selection mechanism," *Multimed. Tools Appl.*, vol. 80, pp. 20883–20905, 2021, doi: 10.1007/s11042-021-10751-0.

[16] 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.

[17] J.-F. Lai and S.-H. Heng, "Secure File Storage On Cloud Using Hybrid Cryptography," *J. Informatics Web Eng.*, vol. 1, no. 2, pp. 1–18, Sep. 2022, doi: 10.33093/jiwe.2022.1.2.1.

[18] W. Zhang *et al.*, "Multi-key hybrid encryption optical codebook based on five-dimensional Hamiltonian conservative chaotic system.," *Opt. Express*, vol. 33 9, pp. 18611–18623, 2025, doi: 10.1364/oe.554307.

[19] 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.

[20] I. Yasser, M. Mohamed, A. Samrah, and F. Khalifa, "A Chaotic-Based Encryption/Decryption Framework for Secure Multimedia Communications," *Entropy*, vol. 22, 2020, doi: 10.3390/e22111253.

[21] A. Abbas *et al.*, "Machine learning-based hybrid technique to enhance cyber-attack perspective," *J. Cloud Comput.*, vol. 14, no. 1, 2025, doi: 10.1186/s13677-025-00782-5.

[22] 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.

[23] X. Ru, Y. Wang, L. Peng, and J. Li, "An Adaptive Extraction Method for Knitted Patterns Based on Bayesian-Optimized Bilateral Filtering," *Appl. Sci.*, vol. 16, no. 5, 2026, doi: 10.3390/app16052526.

[24] M. Al-Laham, B. Bataineh, and Z. Alqadi, "Simplified and Effective Dual-Round Image Encryption Robust Technique," *Int. Arab J. Inf. Technol.*, vol. 22, no. 2, pp. 316–326, 2025, doi: 10.34028/iajit/22/2/9.

[25] A. Pallakonda, K. Ravishanmugam, R. D. A. Raj, S. Sivagnanam, R. M. R. Yanamala, and K. K. Prakasha, "A Unified Cybersecurity Framework for Smart Grids Against Data Integrity Attacks Using Ensemble Learning and Hybrid Encryption," *IEEE Access*, vol. 13, pp. 177595–177614, 2025, doi: 10.1109/ACCESS.2025.3616505.

[26] M. A. Pires, C. Tsallis, and E. M. F. Curado, "Composing α -Gauss and logistic maps: Gradual and sudden transitions to chaos," *Phys. Rev. E*, vol. 112, no. 3, 2025, doi: 10.1103/lwfn-qrjt.

[27] 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.

[28] S. Arifin *et al.*, "Enhancing Data Transmission Security through the Modified Hill Cipher and Henon Map Chaos Function," *J. Comput. Sci.*, 2025, doi: 10.3844/jcssp.2025.1440.1453.

[29] A. Khan, R. Khan, F. Alturise, and T. Alkhalifah, "HybridEdge: A Lightweight and Secure Hybrid Communication Protocol for the Edge-Enabled Internet of Things," *Comput. Mater. Contin.*, vol. 82, no. 2, pp. 3161–3178, 2025, doi: 10.32604/cmc.2025.060372.

[30] J. Parashar, B. T. Hung, K. Upreti, P. R. Kshirsagar, S. Mahajan, and S. Kadry, "An enhanced hybrid framework for IoT healthcare security using blockchain-driven multimedia data analysis and

cybersecurity techniques," *Array*, vol. 30, 2026, doi: 10.1016/j.array.2026.100759.

[31] 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.

[32] P. Zhao, J. Wei, L. Wang, and Y. Qiu, "Nonintrusive Power Load Decomposition Based on Adaptive Graph Convolutional Neural Network," *Sensors*, vol. 26, no. 10, 2026, doi: 10.3390/s26102978.

[33] P. T. Sivagurunathan and A. Sridevi, "A hybrid model for multimedia data compression using generative adversarial networks and chaotic encryption," *Syst. Soft Comput.*, vol. 7, 2025, doi: 10.1016/j.sasc.2025.200375.

[34] J. Kowalewski and T. Grześ, "Detecting the File Encryption Algorithms Using Artificial Intelligence," *Appl. Sci.*, vol. 15, no. 19, 2025, doi: 10.3390/app151910831.

[35] S. Hamlomo and M. Atemkeng, "Clustering-based low-rank matrix approximation for multimodal medical image compression," *BioData Min.*, vol. 19, no. 1, 2026, doi: 10.1186/s13040-026-00541-5.

[36] W. Cha, H. J. Lee, S. Kook, K. Kim, and D. Won, "A Lightweight Authentication and Key Distribution Protocol for XR Glasses Using PUF and Cloud-Assisted ECC," *Sensors*, vol. 26, no. 1, 2026, doi: 10.3390/s26010217.

[37] R. Chen, Z. Zhang, Z. Zhang, J. Li, and H. Zhang, "Unified Modulation Matrix-Based Shared Control for Teleoperated Multi-Robot Formation and Obstacle Avoidance," *Sensors*, vol. 26, no. 8, 2026, doi: 10.3390/s26082387.

[38] Ž. Majstorović, E. Ivanjko, T. Carić, and M. Miletić, "Multi-Agent Adaptive Traffic Signal Control Based on Q-Learning and Speed Transition Matrices," *Sensors*, vol. 25, no. 23, 2025, doi: 10.3390/s25237327.

[39] 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.

[40] M. Debbab, A. B. Ali Pacha, and S. Boukli Hacene, "Hybridization of Blockchain and Cryptography to Secure a Transaction Using Smart Contacts," *Int. J. Adv. Soft Comput. its Appl.*, vol. 17, no. 1, pp. 16–31, 2025, doi: 10.15849/IJASCA.250330.02.

[41] D. C, D. D. P. D S, and A. A. A, "Secure-energy efficient hybrid optimal cluster-based routing with improved AES in WSN for secure data transmission," *Peer-to-Peer Netw. Appl.*, vol. 19, no. 2, 2026, doi: 10.1007/s12083-026-02196-9.

[42] 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.

[43] N. Hediyal, B. P. Divakar, and K. Narayanaswamy, "SCAN-C: a lightweight cryptographic algorithm to secure CAN communications in modern vehicles," *Cybersecurity*, vol. 8, no. 1, 2025, doi: 10.1186/s42400-024-00291-z.

[44] I. Mutambik, "AI-Driven Cybersecurity in IoT: Adaptive Malware Detection and Lightweight Encryption via TRIM-SEC Framework," *Sensors*, vol. 25, no. 22, 2025, doi: 10.3390/s25227072.

[45] H. Şimşek and Ö. F. Öncel, "Fuzzy security level metric of hybrid cryptosystem algorithms," *J. Supercomput.*, vol. 81, no. 9, 2025, doi: 10.1007/s11227-025-07547-6.

[46] A. M. Alshiky, M. A. Khemakhem, F. Eassa, K. Jambi, and A. Alzahrani, "A Hybrid DSDN–Blockchain Framework for Reliable and Secure P2P Streaming: Architecture Design and NS-3 Validation," *Electron.*, vol. 14, no. 22, 2025, doi: 10.3390/electronics14224370.

[47] M. Ayari, Y. E. Touati, A. Gharbi, and Z. Klai, "High-performance image encryption framework using 2D nonuniform FFT and TDES for securing cognitive applications," *Int. J. Cogn. Comput. Eng.*, vol. 7, pp. 287–299, 2026, doi: 10.1016/j.ijcce.2025.11.003.

[48] H. Singh Arri, "A Proposed Method for Real-Time Automatic Cloud Storage and Analysis of Detected Suspicious Activities to Ensure Data Integrity and Security," *J. Appl. Sci. Technol. Trends*, vol. 6, no. 2, pp. 262–276, 2025, doi: 10.38094/jastt62256.

[49] I. A. Taqi and S. M. Hameed, "A Secure Audio Encryption Method Using Tent-Controlled Permutation and Logistic Map-Based Key Generation," *Comput. Mater. Contin.*, vol. 85, no. 1, pp. 1653–1674, 2025, doi: 10.32604/cmc.2025.067524.

[50] S. A. El-Rahman, A. E. Mansour, L. Jamel, M. Abdullah Alohali, M. Seifeldin, and Y. Alkady, "C-HIDE: A Steganographic Framework for Robust Data Hiding and Advanced Security Using Coverless Hybrid Image Encryption With AES and ECC," *IEEE Access*, vol. 13, pp. 41367–41381, 2025, doi: 10.1109/ACCESS.2025.3546255.

[51] T. Liu, C. Liu, Q. Li, X. Zheng, and F. Zou, "ARTdeConv: adaptive regularized tri-factor non-negative matrix factorization for cell type deconvolution," *NAR Genomics Bioinforma.*, vol. 7, no. 2, 2025, doi: 10.1093/nargab/lqaf046.

[52] Y. Mousavi, A. Shokri, Y. Khedmati Yengejeh, and H. Kheiri, "Multi-layer image encryption framework using a chaotic system with a dynamic starting point," *Digit. Signal Process. A Rev. J.*, vol. 170, 2026, doi: 10.1016/j.dsp.2025.105823.

[53] P. Mishra, S. Pathak, B. Kumar Singh, M. Katara, and G. Kumar, "A Lossless Layered-Based Non-Encoding Plain Text Compression and Encryption Algorithm Utilizing Binary Fragmentation and Defragmentation Technique," *IEEE Access*, vol. 13, pp. 148753–148767, 2025, doi: 10.1109/ACCESS.2025.3600813.

[54] Y. Zhu, Q. Xu, L. Fan, and L. Qian, "Network Security Empowered Digital Teaching Data Protection Algorithm for Ceramic Technology," *Eng. Reports*, vol. 8, no. 3, 2026, doi: 10.1002/eng2.70710.

[55] Y. Niu, W. Bai, and X. Zhang, "A secure image encryption scheme based on a complex 3D chaotic system and an enhanced Josephus ring for IoT environments," *Phys. Scr.*, vol. 101, no. 18, 2026, doi: 10.1088/1402-4896/ae6485.

[56] 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.

[57] Y. Banu, B. K. Rath, and D. Gountia, "Analyzing cryptographic algorithm efficiency with in graph-based encryption models," *Front. Comput. Sci.*, vol. 7, 2025, doi: 10.3389/fcomp.2025.1630222.

[58] A. A. Abdillah, Azwardi, S. Permana, I. Susanto, F. Zainuri, and S. Arifin, "Performance Evaluation Of Linear Discriminant Analysis And Support Vector Machines To Classify Cesarean Section," *Eastern-European J. Enterp. Technol.*, vol. 5, no. 2–113, pp. 37–43, 2021, doi: 10.15587/1729-4061.2021.242798.

[59] S. Inam, S. Kanwal, M. Niazi, H. Karamti, S. Al-Otaibi,

and M. M. Jamjoom, "A Novel Hybrid Image Encryption Scheme Using Henon Map for Secure Image Communication," *IET Inf. Secur.*, vol. 2026, no. 1, 2026, doi: 10.1049/ise2/2676559.

[60] E. N. Kucur, T. Buyuktanir, M. Ugurelli, and K. Yildiz, "Privacy-Preserving Machine Learning Techniques: Cryptographic Approaches, Challenges, and Future Directions," *Appl. Sci.*, vol. 16, no. 1, 2026, doi: 10.3390/app16010277.

[61] 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.

[62] G. Liu, G. Yang, J. Ma, H. Zhai, and Q. Zhou, "An Efficient and Intelligent Interest-Based Personalized Search Over Encrypted Outsourced Data in Clouds," *IET Inf. Secur.*, vol. 2025, no. 1, 2025, doi: 10.1049/ise2/3355214.

[63] 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

[64] M. Nazish and M. T. Banday, "e-CM: A novel approach to advancing chaotic dynamics in discrete one-dimensional maps for secure IoT applications," *Cybersecurity*, vol. 8, no. 1, 2025, doi: 10.1186/s42400-024-00347-0.

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.

Dadan Ramdan Hidayat is a diligent and highly motivated undergraduate student in the Data Science Program at Institut Teknologi Sains Bandung (ITSB). Throughout his academic journey, he has consistently demonstrated a strong work ethic, intellectual curiosity, and a genuine passion for scientific exploration. His eagerness to learn and investigate new ideas has enabled him to actively engage in research activities beyond regular coursework. Under the supervision and mentorship of several faculty members, Dadan has successfully contributed to and co-authored multiple scientific publications in areas related to data science, cryptography, artificial intelligence, and computational research. His commitment to academic excellence, research productivity, and continuous self-improvement reflects his potential to become a promising researcher and professional in the field of data science.

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.