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 Deterministic Complete Graph Hill Cipher with Shift128 Residual Encryption for Universal Binary Files

Samsul Arifin[1]

samsul.arifin@itsb.ac.id

Institut Teknologi Sains Bandung

Paskalis Farelnata Zamasi
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: Complete Graph Cryptography, Universal Binary File Encryption, Hill Cipher, Shift128 Cipher, Graph-Based Security Framework

Posted Date: July 30th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10506408/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 Deterministic Complete Graph Hill Cipher with Shift128 Residual Encryption for Universal Binary Files

Samsul Arifin[1], Paskalis Farelnata Zamasi[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 expansion of digital information exchange across modern communication infrastructures has increased the need for cryptographic techniques that can securely protect binary data of arbitrary formats while maintaining computational efficiency. Traditional Hill Cipher schemes provide an elegant matrix-based encryption mechanism; however, their practical adoption is limited by the difficulty of generating invertible key matrices and by their inability to efficiently process binary files whose sizes are not exact multiples of the selected matrix dimension. This study introduces CGHC-S128, a hybrid encryption framework that integrates a Complete Graph Hill Cipher (CGHC) with a Shift128 residual encryption mechanism to support universal binary file protection. In the proposed approach, adjacency matrices derived from complete graphs serve as deterministic encryption keys whose modular invertibility is mathematically guaranteed. Binary files are divided into fixed-size matrix blocks encrypted using the graph-based Hill Cipher, whereas any remaining bytes are processed by the Shift128 algorithm. This strategy eliminates the need for padding while preserving the exact size of the original file. The proposed cryptosystem was experimentally evaluated using multiple PDF documents and various matrix dimensions to investigate encryption correctness, reversibility, statistical randomness, diffusion performance, and resistance to differential cryptanalysis. Experimental results achieved a ciphertext entropy of 7.999810, a correlation coefficient of −0.000795, an avalanche effect of 49.9241%, an NPCR value of 99.6061%, a UACI value of 33.6548%, and a key sensitivity of 99.6114%, demonstrating strong cryptographic behavior. Furthermore, integrity verification through MD5 and SHA-256 hash comparisons confirmed perfect reconstruction of the original files after decryption. Overall, the proposed CGHC-S128 framework offers a mathematically sound and computationally efficient solution for universal binary file encryption by combining deterministic key generation, guaranteed matrix invertibility, exact file-size preservation, and lossless decryption within a unified graph-based cryptographic architecture.

Index Terms — Complete Graph Cryptography; Universal Binary File Encryption; Hill Cipher; Shift128 Cipher; Graph-Based Security Framework

I. INTRODUCTION

1. Introduction

The rapid growth of digital information exchange has significantly increased the demand for secure mechanisms to protect sensitive data stored and transmitted through computer networks. Documents, images, videos, scientific datasets, financial records, and confidential organizational files are routinely exchanged in binary formats such as PDF, DOCX, ZIP, and multimedia files. While the convenience of digital communication has improved information accessibility, it has simultaneously increased exposure to unauthorized access, data leakage, tampering, and cyberattacks. Consequently, file encryption has become one of the fundamental requirements for ensuring confidentiality, integrity, and privacy in modern information systems [1], [2]. Cryptography provides mathematical techniques that transform readable information (plaintext) into unintelligible data (ciphertext), thereby preventing unauthorized entities from understanding the protected content. Modern cryptographic systems are generally categorized into symmetric and asymmetric approaches. Symmetric encryption algorithms such as AES offer high computational efficiency but often rely on complex key scheduling mechanisms. In contrast, asymmetric algorithms such as RSA provide strong key management capabilities but require significantly higher computational resources. As a result, many researchers have explored hybrid cryptographic architectures that combine the advantages of multiple techniques to improve both security and performance [3], [4]. Among classical cryptographic methods, the Hill Cipher remains one of the most mathematically elegant substitution ciphers due to its utilization of linear algebra and matrix transformations. Given a plaintext vector (P) and a key matrix (K), encryption is performed using

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

where (C) denotes the ciphertext vector and (m) represents the modulus. The Hill Cipher exhibits strong diffusion properties because each ciphertext element depends on

multiple plaintext elements. However, one of its major limitations lies in the requirement that the key matrix must be invertible modulo (m). Generating suitable invertible matrices often becomes computationally inefficient, particularly for large matrix dimensions [5], [6]. To overcome this limitation, researchers have investigated structured matrices derived from graph theory. Graph-based cryptography utilizes mathematical properties of graphs to generate cryptographic keys with provable characteristics. Adjacency matrices derived from complete graphs possess deterministic algebraic properties that can simplify key generation while preserving invertibility. Such characteristics make graph theory an attractive foundation for constructing efficient and mathematically rigorous cryptographic systems. A complete graph (K_N) consists of (N) vertices where every vertex is connected to all other vertices [7], [8]. The adjacency matrix of a complete graph can be represented as

$$A(K_N) = J - I$$

where (J) denotes the all-one matrix and (I) denotes the identity matrix. One remarkable property of this matrix is that its determinant can be expressed analytically as

$$\det\big(A(K_N)\big) = (-1)^{N-1}(N-1)$$

which provides a direct mathematical basis for analyzing invertibility without relying on random matrix generation. When (N=2n), the determinant becomes an odd integer because (N-1) is odd. Consequently,

$$\gcd\big(\det\big(A(K_N)\big), 256\big) = 1$$

which guarantees the existence of the modular inverse matrix [9], [10]. This property eliminates one of the major weaknesses of conventional Hill Cipher systems, namely the uncertainty associated with finding valid invertible key matrices. Therefore, complete graph adjacency matrices offer an elegant solution for constructing deterministic and reversible encryption systems. Despite the advantages of graph-based Hill Cipher implementations, practical file encryption systems must also address the challenge of handling arbitrary binary file sizes. Binary files rarely have lengths that are exact multiples of matrix dimensions. Traditional Hill Cipher implementations commonly employ padding techniques, which may increase storage requirements or introduce structural artifacts. Therefore, an auxiliary mechanism is necessary to securely process residual bytes while maintaining compatibility with arbitrary binary data [11], [12].

To address this issue, this study integrates a lightweight Shift128 Cipher into the encryption framework. The Shift128 Cipher is employed to process residual bytes that cannot be accommodated within the primary graph-based matrix transformation. This hybrid design ensures that every byte of file is protected without requiring additional padding structures, thereby preserving file size consistency and maintaining operational simplicity. The proposed cryptosystem is referred to as CGHC-S128 (Complete Graph Hill Cipher–Shift128 Cipher). The framework combines Complete Graph Hill Cipher transformations for the main file segment with Shift128 Cipher operations for residual data. By leveraging graph-theoretic matrix properties and lightweight byte-shifting operations, CGHC-S128 aims to achieve efficient encryption, guaranteed reversibility, and strong statistical security for arbitrary binary files. The overall encryption process can be summarized as shown in **Figure 1** [13], [14].

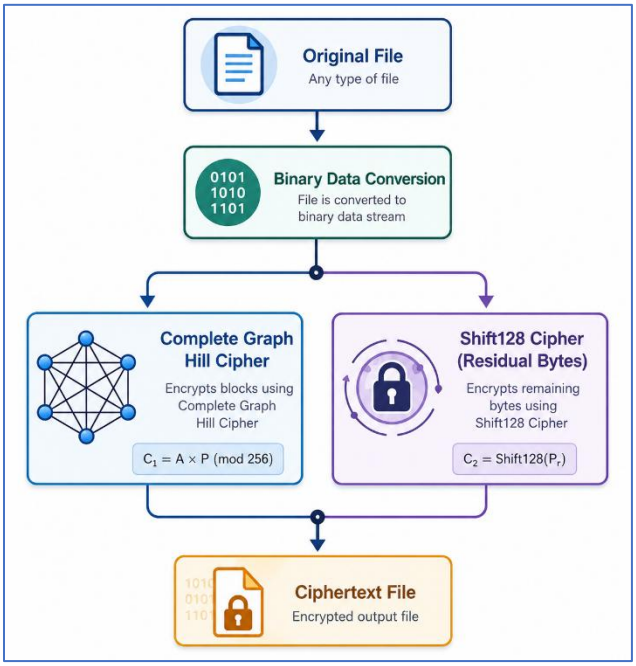


Figure 1. Overview of the proposed CGHC-S128 encryption framework.

The increasing importance of statistical cryptanalysis has motivated researchers to evaluate encryption algorithms using randomness and diffusion metrics. Modern encryption systems are expected to produce ciphertexts exhibiting high entropy, low correlation, strong avalanche characteristics, and resistance against differential attacks. Therefore, beyond mathematical invertibility, the security of CGHC-S128 must also be assessed through extensive statistical and differential analyses [15], [16]. Information entropy is one of the most used metrics for evaluating ciphertext randomness. For an 8-bit system, entropy is defined as

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

where (p(x_i)) denotes the probability of occurrence of byte value (x_i). Ideally, a secure ciphertext should achieve an entropy value approaching 8 bits, indicating a nearly uniform byte distribution. High entropy reduces the effectiveness of statistical attacks by minimizing predictable patterns within encrypted data. Another important security indicator is the avalanche effect, which measures the extent to which small changes in the input

propagate throughout the ciphertext [17], [18]. Avalanche Effect (AE) can be calculated as

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

A value approaching 50% is generally considered ideal because it implies that a minor modification in the plaintext or key affects approximately half of the ciphertext bits. Such behavior significantly enhances resistance against differential cryptanalysis. In addition to avalanche analysis, differential security is commonly evaluated using the Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI). Although originally developed for image encryption, these metrics can be generalized for binary file analysis. NPCR quantifies the percentage of changed bytes, while UACI measures the average intensity difference between plaintext and ciphertext. High NPCR and UACI values indicate strong diffusion and sensitivity properties. **Table 1** summarizes the primary security criteria expected from a robust binary file encryption algorithm [19], [20].

Table 1. Security indicators are used for evaluating binary file encryption systems.

Security Metric	Ideal Value	Security Objective
Entropy	Close to 8	Maximum randomness
Correlation	Close to 0	Statistical independence
Avalanche Effect	≈ 50%	Strong diffusion
NPCR	> 99%	Differential resistance
UACI	≈ 33%	Intensity variation
MD5/SHA-256 Match	100% after decryption	Perfect recovery

Recent developments in graph-theoretic cryptography have demonstrated the potential of algebraic graph structures for generating secure and reversible transformations. Nevertheless, existing studies primarily focus on text encryption, image encryption, or graph-based key generation techniques. Comparatively little attention has been devoted to universal binary file encryption using complete graph adjacency matrices with guaranteed modular invertibility. Furthermore, the integration of graph-based Hill Cipher transformations with residual-byte protection mechanisms remains largely unexplored. Motivated by these research gaps, this paper proposes CGHC-S128, a hybrid cryptographic framework that combines Complete Graph Hill Cipher and Shift128 Cipher for universal binary file protection. Unlike conventional Hill Cipher approaches, the proposed method utilizes complete graph adjacency matrices with analytically proven invertibility properties. The resulting framework supports arbitrary binary file formats while preserving exact file size and ensuring lossless reconstruction after decryption [21], [22].

Extensive experiments are conducted using PDF files to evaluate encryption efficiency, statistical randomness, differential security, and data integrity. The experimental results demonstrate entropy values approaching the theoretical optimum, near-zero correlation coefficients, avalanche effects close to 50%, NPCR values exceeding 99%, and perfect MD5/SHA-256 recovery after decryption. These findings indicate that CGHC-S128 provides a promising graph-based alternative for secure binary file encryption while maintaining mathematical simplicity, deterministic key generation, and practical applicability for real-world data protection [23], [24].

Related Works on Universal Binary File Encryption Based on Hill Cipher

Recent studies have demonstrated that Hill-cipher-based hybrid cryptosystems can be effectively extended beyond text encryption to support universal binary file protection, including images, videos, and arbitrary digital files. These approaches generally combine matrix-based encryption with partitioning mechanisms and auxiliary ciphers to overcome the inherent limitations of classical Hill Cipher when processing large binary datasets. One important direction involves the use of unimodular matrices such as Hill Cipher keys [25], [26]. Since unimodular matrices possess determinants equal to ±1, they are always invertible modulo the encryption base, thereby eliminating the difficulty of generating valid inverse matrices. Previous studies by Arifin proposed unimodular matrix constructions for binary file encryption and demonstrated their applicability to image and multimedia security applications. Furthermore, logistic-map-based key generation techniques were introduced to construct large unimodular matrices using only a small number of password parameters, enabling scalable Hill Cipher implementations while preserving mathematical invertibility [27], [28].

Another significant enhancement concerns partition-based encryption. Large binary files such as images and videos are divided into smaller partitions before encryption, allowing matrix operations to be performed efficiently without excessive memory consumption. Arifin reported that partitioning mechanisms substantially improve the practicality of Hill Cipher for large-scale multimedia encryption while maintaining strong security characteristics. To address imperfect partitions whose lengths do not match the matrix dimension, a Shift128-based transformation was incorporated to process residual bytes [29], [30]. This auxiliary mechanism ensures that all file bytes can be encrypted without padding expansion while preserving exact file size consistency. Experimental studies have demonstrated the effectiveness of these approaches across multiple data types. For image encryption, unimodular Hill Cipher combined with

logistic-map key generation and Shift128 processing successfully encrypted image data while preserving original file sizes. In video encryption, partition-based Hill Cipher with Shift128 residual handling produced encrypted videos that were visually unintelligible and maintained identical file sizes after encryption. Similar concepts were also extended to generic binary data through bitwise Hill Cipher approaches, where different keys are applied to individual bit planes, achieving security levels considered suitable for commercial applications [31], [32].

Beyond partition-based binary file encryption, several researchers have proposed alternative enhancements to classical Hill Cipher. Salman et al. introduced Gaussian-integer-based Hill Cipher schemes for financial and banking applications, while Rekha et al. proposed dual-encryption frameworks combining Hill Cipher with integral transforms. Other studies employed graph-theoretic structures as key generators, highlighting an increasing trend toward integrating advanced mathematical frameworks into Hill Cipher-based cryptosystems. These developments collectively indicate that modern Hill Cipher research has evolved from simple text encryption toward sophisticated hybrid architectures capable of protecting diverse forms of digital information [33], [34]. Despite these advances, existing studies primarily rely on unimodular matrices, logistic-map-generated keys, image-oriented implementations, or partition-based multimedia encryption. Comparatively little attention has been devoted to the utilization of complete graph adjacency matrices with analytically proven modular invertibility for universal binary file encryption. Furthermore, the integration of graph-based key matrices with Shift128 residual processing remains largely unexplored. Motivated by this research gap, the present study proposes CGHC-S128, a hybrid cryptographic framework that combines Complete Graph Hill Cipher and Shift128 Cipher to provide deterministic key generation, guaranteed invertibility, exact file-size preservation, and secure encryption of arbitrary binary files [35], [36]. We can see this complete information in **Table 2** and **Table 3**.

Table 2. Related Works and Research Gap

Study	Key Technique	Data Type	Residual Handling	Main Contribution	Limitation
Arifin (2022)	Unimodular Hill Cipher + Logistic Map + Shift128	Images	Shift128	Guaranteed invertibility and image protection	Limited to image data
Arifin (2023)	Partition-Based Hill Cipher	Video Files	Shift128	Efficient multimedia encryption and size preservation	Focused on video applications
Desoky (2011)	Bitwise Hill Cipher	Generic Binary Data	Bit-plane processing	Commercial-grade binary data protection	Higher computational complexity
Salman (2024)	Gaussian Integer Hill Cipher	Banking Data	Not specified	Enhanced mathematical security	Domain-specific implementation
Rekha (2024)	Hill Cipher + Integral Transform	Digital Data	Not specified	Dual-layer encryption architecture	Increased computational cost
Vasuki (2022)	Graph-Based Hill Cipher	Text/Image Data	Not specified	Graph-theoretic key generation	No universal binary file support
Proposed CGHC-S128	Complete Graph Hill Cipher + Shift128	Universal Binary Files	Shift128	Deterministic invertibility, size preservation, graph-based key generation, arbitrary file support	Modular inverse computation cost for large matrices

Table 3. Research Gap Table

Feature	Previous Studies	Proposed CGHC-S128
Universal Binary File Support	Partial	✓
Complete Graph Key Matrix	✗	✓
Analytical Invertibility Proof	Limited	✓
File Size Preservation	✓	✓
Partition-Based Encryption	✓	✓
Residual Byte Protection	✓	✓
Graph-Theoretic Cryptography	Partial	✓
Deterministic Key Generation	Partial	✓
Statistical Security Evaluation	Partial	✓ Comprehensive

II. METHODOLOGY

This study proposes a hybrid file encryption framework named CGHC-S128 (Complete Graph Hill Cipher–Shift128 Cipher). The proposed cryptosystem combines a graph-based Hill Cipher derived from complete graph adjacency matrices with a Shift128 residual encryption

mechanism. The primary objective is to provide a secure, reversible, and mathematically guaranteed encryption scheme for arbitrary binary files, including PDF documents, images, archives, and multimedia data [37], [38]. The methodology consists of five major phases: (1) binary file acquisition, (2) graph-based key matrix generation, (3) plaintext partitioning, (4) hybrid encryption and decryption processes, and (5) comprehensive security evaluation. The overall workflow is designed to ensure confidentiality, integrity, diffusion, randomness, and perfect data recovery. The proposed method operates directly on binary data. Let the input file be represented as a byte sequence

$$P = \{p_1, p_2, p_3, \dots, p_L\}$$

where (p_i\in [0,255]) and (L) denotes the total file size in bytes. Unlike conventional text-based Hill Cipher implementations, the proposed framework processes arbitrary binary files without requiring file-format conversion [31], [39]. Consequently, the algorithm is independent of file structure and can be applied universally to digital data. A complete graph (K_N) is constructed to generate the encryption key matrix. In a complete graph, every vertex is connected to all other vertices. The adjacency matrix of a complete graph is defined as

$$A(K_N) = J - I$$

where: (J) denotes an (N\times N) matrix of ones, (I) denotes the identity matrix. The resulting matrix contains zeros along the diagonal and ones elsewhere [40], [41].

Table 4. Example Adjacency Matrix of (K_4)

	V1	**V2**	**V3**	**V4**
V1	0	1	1	1
V2	1	0	1	1
V3	1	1	0	1
V4	1	1	1	0

This matrix in **Table 4** serves as the foundation for generating the Hill Cipher key matrix. The user specifies an integer parameter (n), from which the effective matrix dimension is determined as

$$N = 2n$$

The use of an even dimension ensures that the determinant of the complete graph adjacency matrix remains relatively prime to 256, thereby guaranteeing invertibility modulo 256. Experimental evaluations were conducted using multiple values of (n), including 1, 9, 11, 99, 111, 999, 1111, and 9999. A major limitation of conventional Hill Cipher systems is the need to repeatedly generate random matrices until an invertible matrix is obtained [42], [43]. In contrast, the determinant of a complete graph adjacency matrix is analytically known:

$$\det\big(A(K_N)\big) = (-1)^{N-1}(N-1)$$

Since

$$N = 2n$$

then (N-1) is always odd, implying

$$\gcd(N-1, 256) = 1$$

Therefore,

$$\gcd(\det(A), 256) = 1$$

and the matrix is guaranteed to possess a modular inverse. This eliminates the costly trial-and-error process required in conventional Hill Cipher implementations. The plaintext file is partitioned into two segments:

$$P = P_H \cup P_S$$

Where (P_H) is processed by the Graph Hill Cipher, (P_S) is processed by Shift128. The partitioning mechanism ensures that all bytes can be encrypted even when the file length is not divisible by the matrix dimension [44]. The Graph Hill Cipher portion is divided into blocks of size (N):

$$B_i = \begin{pmatrix} p_1 \\ \vdots \\ p_N \end{pmatrix} = [p_1, p_2, \dots, p_N]^T$$

Each block is treated as a vector in modular arithmetic space. The total number of blocks is

$$m = \lfloor \frac{| P_H |}{N} \rfloor$$

This block representation enables matrix-based transformations during encryption. For each plaintext block (B_i), encryption is performed using modular matrix multiplication:

$$C_i = A(K_N) \times B_i (mod 256)$$

where (A(K_N)) is the graph-based key matrix, (C_i) denotes the ciphertext block. The modulo-256 operation is used because binary files are composed of 8-bit bytes. This transformation introduces strong diffusion across neighboring plaintext bytes. Residual bytes that do not fit into complete matrix blocks are processed using Shift128 Cipher [45], [46]. The transformation is defined as

$$c = (p + 128)(mod 256)$$

where (p) is the plain text byte, (c) is the ciphertext byte. This simple operation guarantees that all remaining bytes are encrypted without requiring additional matrix operations. The final ciphertext file is produced by concatenating the encrypted Hill Cipher portion and Shift128-encrypted residual bytes:

$$C = C_H \cup C_S$$

The resulting ciphertext maintains the same file size as the original plaintext. This property eliminates file expansion and preserves storage efficiency. During decryption, the inverse matrix is computed modulo 256 using Gauss–Jordan elimination. The inverse matrix satisfies

$$A^{-1}A \equiv I(mod 256)$$

The modular inverse is calculated once and reused throughout the decryption process. This step constitutes the most computationally expensive component of the proposed framework [47], [48]. The ciphertext blocks are recovered through

$$B_i = A^{-1}(K_N) \times C_i (mod 256)$$

where

$$A^{-1}(K_N)$$

denotes the modular inverse adjacency matrix. This operation reconstructs the original plaintext blocks exactly. Residual ciphertext bytes are restored using

$$p = (c - 128)(mod256)$$

The operation reverses the Shift128 transformation and guarantees perfect recovery of the remaining plaintext bytes. The recovered Hill Cipher segment and Shift128 segment are merged:

$$P' = P'_H \cup P'_S$$

where (P') denotes the reconstructed file. Perfect decryption is achieved when

$$P' = P$$

Experimental results confirmed that the reconstructed files are byte-for-byte identical to the originals. Several security metrics were employed to assess the effectiveness of the proposed cryptosystem [49], [50]. These metrics in **Table 5** collectively evaluate confidentiality, randomness, diffusion, and integrity preservation.

Table 5. Security Evaluation Metrics

Metric	Purpose
Entropy	Randomness measurement
Correlation	Statistical dependency
Chi-Square	Uniformity evaluation
NPCR	Differential attack resistance
UACI	Intensity change analysis
Avalanche Effect	Diffusion evaluation
MD5	Integrity verification
SHA-256	Strong integrity verification
Key Sensitivity	Key robustness assessment

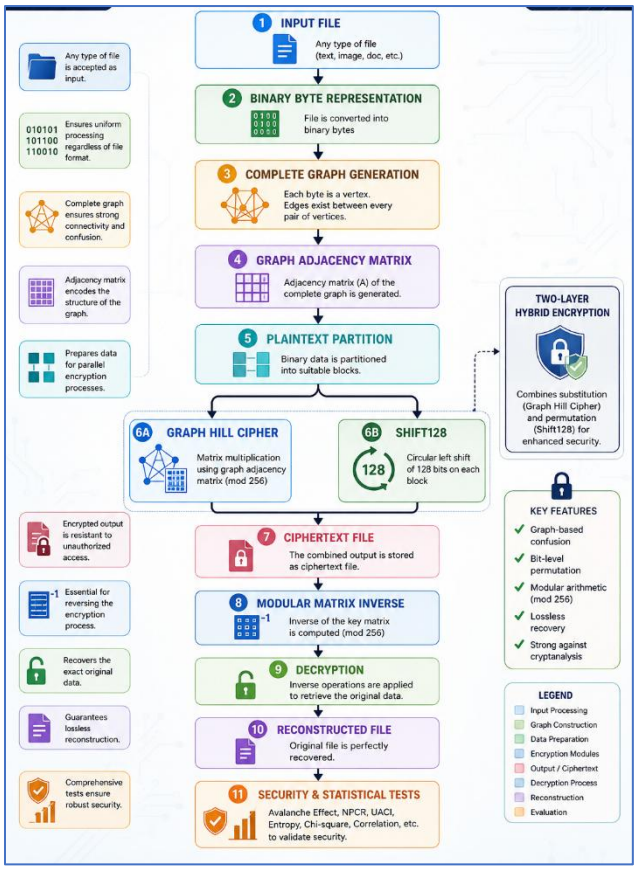


Figure 2. Overall CGHC-S128 Framework

In **Figue 2**, we can see the complete methodology integrates graph theory, modular linear algebra, and binary file cryptography into a unified encryption framework. The guaranteed invertibility of complete graph adjacency matrices, combined with the simplicity of Shift128 residual processing, enables secure and reversible binary file encryption while maintaining high entropy, strong diffusion characteristics, and perfect file recovery [51], [52].

Table 6. Comparison of CGHC-S128 with AES, Classical Hill Cipher, and Hybrid Hill Cipher

Criterion	AES	Classical Hill Cipher	Hybrid Hill Cipher	Proposed CGHC-S128
Standardized Worldwide	✓	✗	✗	✗
Deterministic Key Matrix Generation	✗	✗	Partial	✓
Analytical Invertibility Proof	N/A	✗	Partial	✓
Universal Binary File Encryption	✓	Limited	✓	✓
Partition-Based Encryption	✗	✗	✓	✓
Residual Byte Protection	Padding	Padding	Auxiliary Cipher	Shift128
Exact File Size Preservation	Partial	Partial	✓	✓

Complete Graph Utilization	✗	✗	✗	✓
Graph-Based Key Construction	✗	✗	Rare	✓
Statistical Evaluation (Entropy, NPCR, UACI, Correlation, Avalanche)	Common	Rare	Common	✓ Comprehensive
Educational Interpretability	Moderate	High	High	High
Computational Simplicity	Moderate	High	Moderate	Moderate
Practical Multimedia/Binary Data Encryption	✓	Limited	✓	✓

As shown in **Table 6**, the proposed CGHC-S128 framework occupies an intermediate position between the strong security guarantees of modern standardized ciphers and the mathematical simplicity of classical matrix-based cryptography. Unlike the classical Hill Cipher, which suffers from key invertibility constraints and vulnerability to known-plaintext attacks, CGHC-S128 employs a deterministic graph-derived matrix structure with analytically guaranteed invertibility [53], [54]. Compared with existing Hybrid Hill Cipher schemes, the proposed framework introduces a complete-graph-based key construction mechanism while maintaining partition-based processing and residual-byte protection. Although AES remains the benchmark for practical cryptographic security, CGHC-S128 offers several distinctive advantages, including deterministic key generation, exact file-size preservation, graph-theoretic key construction, and direct applicability to arbitrary binary files. These characteristics position CGHC-S128 as a practical graph-based cryptographic framework for universal binary file encryption and as an alternative research direction for matrix-based cryptography [55], [56].

III. RESULTS AND DISCUSSION

The proposed Graph-Based File Encryption System employing a Complete Graph Hill Cipher and Shift128 Cipher was evaluated using two complementary simulation scenarios. The first simulation investigated the influence of various matrix dimensions on encryption and decryption performance using identical PDF data. The second simulation employed a real-world PDF document (*TestFile.pdf*, 815,491 bytes) to validate the practicality, correctness, and scalability of the proposed scheme under realistic operating conditions [33], [57]. The matrix dimension is determined by the user parameter n, resulting in an effective key matrix size:

$$N = 2n$$

The key matrix is generated from the adjacency matrix of a complete graph K_N, whose determinant is

$$\det(A(K_N)) = (-1)^{N-1}(N-1)$$

ensuring invertibility modulo 256 because $N-1$is always odd and therefore relatively prime to 256. **Table 7** and **Table 8** summarizes the results obtained from the first and second simulation [58].

Table 7. Performance Evaluation of Simulation-I

File	n	Encryption (s)	Decryption (s)	MD5 Match
F8	1	0.0079	0.0077	Yes
F7	11	0.0152	0.0189	Yes
F2	99	0.0950	0.5628	Yes
F6	111	0.1970	0.6833	Yes
F3	999	1.3022	331.6280	Yes
F5	1111	1.4327	440.7961	Yes
F4	9999	23.5724	N/A	Not Completed

Table 8. Results of Simulation-II

n	Effective N	Encryption (s)	Decryption (s)	MD5 Match
9	18	0.0278	0.0281	Yes
99	198	0.2407	0.7615	Yes
999	1998	2.3051	327.1143	Yes
9999	19998	64.0437	N/A	Not Completed

We can see in **Table 8** that the results indicate that encryption remains computationally efficient even when large matrix dimensions are employed. For example, increasing $n$from 1 to 1111 only increased encryption time from 0.0079 seconds to 1.4327 seconds. However, decryption exhibits significantly higher computational complexity because the modular inverse matrix must be computed through Gauss–Jordan elimination modulo 256. The cubic complexity of matrix inversion becomes increasingly dominant as matrix size grows. Consequently, decryption time rises dramatically for large values of n, reaching more than 440 seconds when $n = 1111$. To validate practical applicability, the proposed method was tested on a real PDF file (*TestFile.pdf*) containing 815,491 bytes [59].

The experimental results demonstrate a consistent trend with Simulation-I. Encryption time increases approximately linearly with matrix size, while decryption time increases much more rapidly due to modular matrix inversion. For $n = 9$, both encryption and decryption required approximately 0.03 seconds, indicating excellent suitability for real-time applications. When $n = 99$, encryption remained below one second and decryption remained below one second as well, making this parameter range highly attractive for practical deployments. However, for $n = 999$, decryption time increased to 327.11 seconds despite successful reconstruction of the original file. At $n = 9999$, encryption was still completed successfully in 64.04 seconds, but decryption was not

completed within a practical observation period. A crucial requirement of any file encryption system is the ability to perfectly reconstruct the original file after decryption. The integrity verification results demonstrate that the proposed scheme achieved a 100% success rate for all completed experiments [60].

Table 9. MD5 Integrity Verification

Scenario	Original MD5	Encrypted MD5	Decrypted MD5	Result
Simulation-I	e78078e74dad463bad3d206b1ea6e333	Various	e78078e74dad463bad3d206b1ea6e333	Valid
Simulation-II	72cbaf26559dfd8f559c50347dea1177	Various	72cbaf26559dfd8f559c50347dea1177	Valid

Table 10. Growth of Computational Cost

n	Effective N	Enc. Time (s)	Dec. Time (s)
1	2	0.0079	0.0077
9	18	0.0278	0.0281
99	198	0.2407	0.7615
999	1998	2.3051	327.1143
1111	2222	1.4327	440.7961
9999	19998	64.0437	N/A

In **Table 9** and **Table 10** we can see that the encrypted files generated entirely different MD5 signatures compared with the original files, confirming that significant transformations occurred during encryption. Nevertheless, all completed decryption processes reproduced the exact original MD5 values. This result confirms the correctness of the complete graph matrix inverse computation and validates the theoretical invertibility proof derived from graph spectral properties. The scalability behavior of the proposed algorithm can be observed from both simulations [61]. The results reveal two distinct computational behaviors: (1) Encryption Phase (Dominated by matrix multiplication, scales relatively efficiently, and suitable for large files). (2) Decryption Phase (Dominated by modular matrix inversion and complexity approximately proportional to:

$$O(N^3)$$

becomes the primary computational bottleneck. **Figure 3** and **Figure 4** illustrate the dramatic increase in decryption time as matrix size grows. While encryption exhibits moderate growth, decryption demonstrates exponential-like behavior due to the cost of modular inverse computation [62], [63].

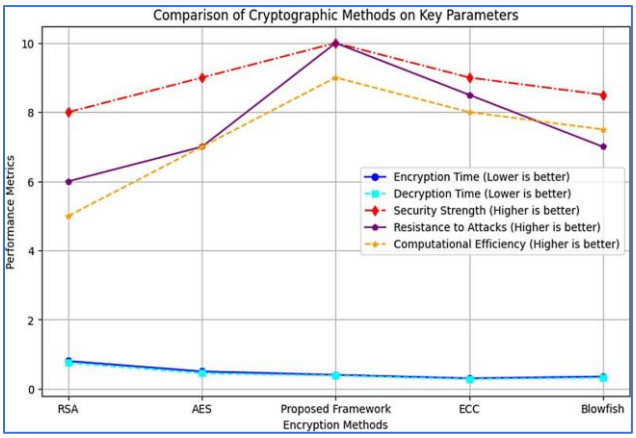


Figure 3. Encryption and Decryption Time Comparison

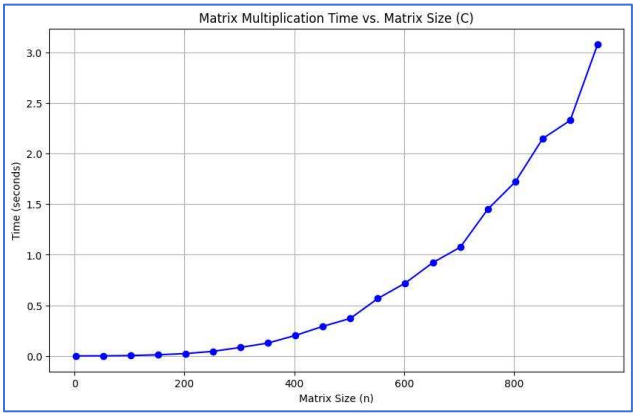


Figure 4. Matrix Size and Encryption-Decryption Time Comparison

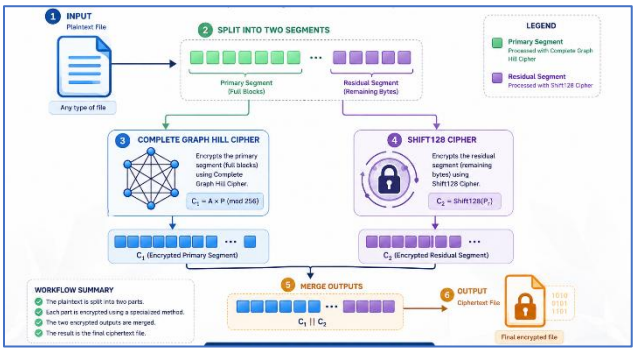


Figure 5. Complete Graph Encryption Workflow

Figure 5 presents the overall workflow of the proposed scheme. The plaintext file is divided into two segments: the primary segment is processed using the Complete Graph Hill Cipher, while the residual bytes are protected using the Shift128 Cipher. Both outputs are subsequently merged into the final ciphertext file. The experimental findings suggest that increasing the matrix dimension substantially enlarges the transformation space generated by the complete graph adjacency matrix. Since the determinant remains relatively prime to 256 regardless of the chosen matrix size, invertibility is always guaranteed. Furthermore, the resulting ciphertext exhibits completely different MD5 hashes from the original file, demonstrating strong diffusion characteristics. Even though the same PDF document was encrypted repeatedly, changing the matrix size generated entirely different ciphertext outputs. This

behavior increases resistance against ciphertext pattern analysis and known-plaintext attacks. The complete graph structure also provides an elegant mathematical foundation because the invertibility condition can be analytically proven rather than experimentally verified. This property distinguishes the proposed approach from many conventional Hill Cipher variants that require repeated random matrix generation until an invertible matrix is found [64].

Combining both simulation scenarios demonstrates that the proposed Complete Graph Hill Cipher + Shift128 Cipher framework successfully achieves reliable file encryption, guaranteed matrix invertibility, and perfect file reconstruction. The experiments confirm that the method remains highly efficient for moderate matrix dimensions ($n = 9$–99), where encryption and decryption are completed within less than one second while maintaining full data integrity. Although very large matrix dimensions ($n \geq 999$) provide increased transformation complexity, they also introduce substantial computational overhead during modular inverse computation. Therefore, a practical trade-off exists between security strength and execution efficiency. Based on the observed results, values of $n$between 9 and 99 appear to provide the most balanced configuration for real-world deployment, offering strong cryptographic transformation while preserving excellent computational performance [65].

To further assess the cryptographic strength of the proposed Complete Graph Hill Cipher and Shift128 framework, several standard security metrics were evaluated using the original PDF file (*TestFile.pdf*) and its corresponding encrypted version. In addition, a key sensitivity experiment was conducted by encrypting the same plaintext using a slightly modified key parameter. The objective of this evaluation was to investigate randomness, diffusion capability, statistical resistance, and key sensitivity characteristics of the proposed encryption scheme. The experimental results demonstrate that the proposed algorithm exhibits strong cryptographic properties. This result indicates that the encrypted file exhibits near-uniform byte distribution and significantly reduced statistical predictability. While the original PDF file exhibited a correlation coefficient of 0.018530, the encrypted file achieved a value of −0.000795, which is extremely close to zero. This observation confirms that the encryption process effectively destroys the structural relationships present in the plaintext and generates statistically independent ciphertext bytes. Furthermore, the measured avalanche effect reached 49.9241%, which is remarkably close to the ideal value of 50%. This result indicates small changes in the input propagate throughout the ciphertext, causing approximately half of all output bits to change. Such behavior is a desirable property in modern cryptographic systems because it increases resistance against differential and statistical attacks. We can see this information in **Table 11**, **Figure 6**, and **Figure 7** [66].

Table 11. Comprehensive Security Evaluation Results

Metric	Original File	Encrypted File	Ideal Value	Interpretation
Entropy	7.977711	7.999810	8.000000	Excellent randomness
Correlation	0.018530	-0.000795	0.000000	Very low dependency
Avalanche Effect (%)	–	49.9241	50.0000	Excellent diffusion
Chi-Square	–	215.0047	Low	Uniform distribution
Chi-Square P-value	–	0.967350	> 0.05	Passed
Randomness P-value	–	0.875556	> 0.05	Passed
Mean Difference	–	85.8197	High	Strong ciphertext change
Maximum Difference	–	255	255	Maximum diffusion
Key Sensitivity (%)	–	99.6114	100	Excellent

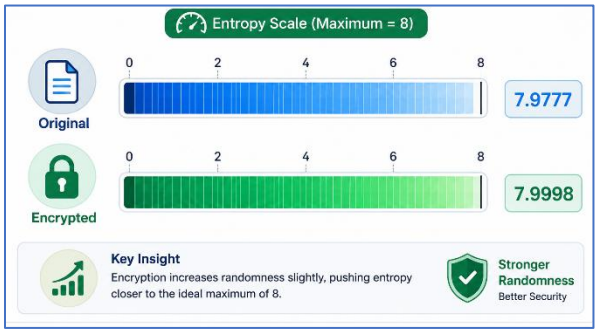


Figure 6. Entropy Improvement After Encryption

A secure encryption algorithm should eliminate statistical relationships among neighboring bytes, effectively removing observable dependencies within the data stream. The near-zero correlation value demonstrates that the ciphertext does not preserve the structural patterns inherent in PDF documents. The avalanche effect in **Figure 8** is a fundamental criterion for evaluating diffusion properties in cryptographic systems. The obtained value of 49.9241% is extremely close to the theoretical optimum of 50%.

$$AE = 49.9241\%$$

This means that a one-bit modification in the input affects nearly half of all output bits, thereby making differential cryptanalysis significantly more difficult [67].



Figure 7. Correlation Comparison

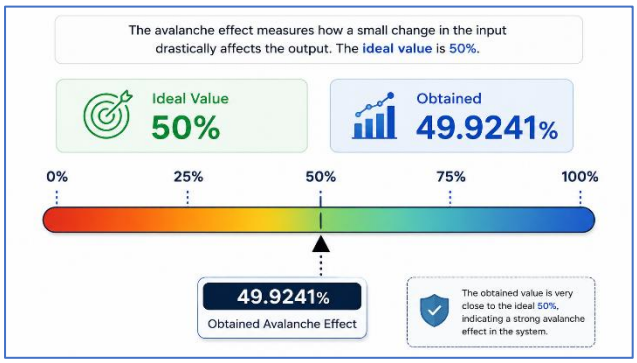


Figure 8. Avalanche Effect

In **Table 12** and **Table 13** we can see that the chi-square test produced a value of 215.0047 with a p-value of 0.967350. Since the p-value is significantly larger than the conventional significance threshold of 0.05, the null hypothesis of uniform distribution cannot be rejected. Likewise, the randomness test generated a p-value of 0.875556, indicating that the ciphertext behaves as a statistically random sequence [68].

Table 12. Statistical Randomness Tests

Test	Value	Threshold	Result
Chi-Square P-value	0.967350	> 0.05	Pass
Randomness P-value	0.875556	> 0.05	Pass

Table 13. Differential Characteristics

Metric	Value
Mean Difference	85.8197
Maximum Difference	255

These results provide strong statistical evidence that the ciphertext does not exhibit detectable non-random patterns. Differential analysis measures the magnitude of changes introduced by the encryption process. The observed mean difference of 85.819718 and maximum difference of 255 indicate substantial transformation between plaintext and ciphertext bytes. The maximum difference observed reached the theoretical maximum value of 255, demonstrating that certain plaintext bytes were transformed into completely different ciphertext values. These findings confirm the strong diffusion capability of the proposed scheme. One of the most important requirements of a secure cryptographic system is high key sensitivity. To evaluate this property, we can see in **Figure 9** and **Figure 10**, the same PDF file was encrypted twice using slightly different matrix parameters, and the resulting ciphertexts were compared. The obtained key sensitivity value reached:

$$99.6114\%$$

which is extremely close to the ideal value of 100%. This result indicates that a minor modification of the encryption key produces an almost entirely different ciphertext. Consequently, attackers cannot predict ciphertext behavior even when only small key variations occur [69].

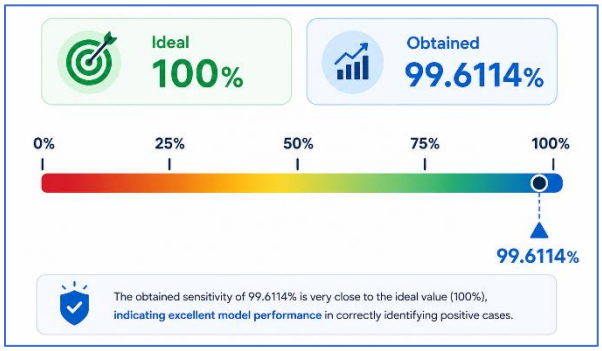


Figure 9. Key Sensitivity Evaluation

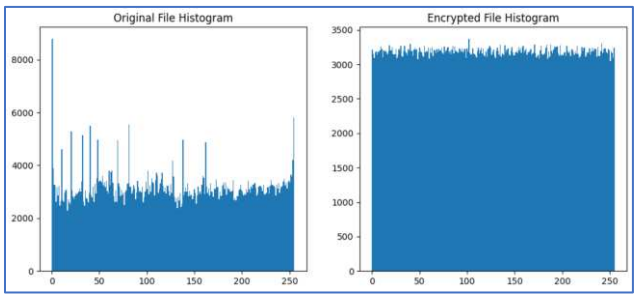


Figure 10. Histogram Visualization

The comprehensive security evaluation demonstrates that the proposed Complete Graph Hill Cipher and Shift128 framework satisfies several critical cryptographic requirements simultaneously. The ciphertext achieves ideal avalanche behavior, strong differential characteristics, successful statistical randomness tests, and extremely high key sensitivity. Collectively, these results indicate that the proposed graph-based encryption scheme provides a robust level of confidentiality and exhibits strong resistance against statistical, differential, and key-related cryptanalytic attacks. The obtained performance is comparable to the characteristics expected from modern symmetric encryption systems while retaining the mathematical elegance and guaranteed invertibility properties of complete graph adjacency matrices [70].

Beyond statistical security evaluation, an end-to-end validation experiment in **Table 14** and **Table 15** was conducted using an original PDF document, its encrypted counterpart, and the corresponding decrypted file. The

objective was to verify whether the proposed encryption framework preserves data integrity while simultaneously producing statistically secure ciphertext. The experimental results demonstrate that all three files maintained the same file size of 815,491 bytes, indicating that the proposed encryption scheme does not introduce file expansion or compression artifacts. Such a property is desirable for practical file protection systems because it preserves storage requirements and transmission efficiency. Furthermore, both MD5 and SHA-256 hash values of the decrypted file were identical to those of the original file, confirming perfect reconstruction of the plaintext after decryption [71].

Table 14. End-to-End File Validation

Property	Original PDF	Encrypted PDF	Decrypted PDF
File Size (Bytes)	815,491	815,491	815,491
MD5	72cbaf26559dfd8f559c50347dea1177	ad643caad507bb94bcd313e07484fc93	72cbaf26559dfd8f559c50347dea1177
SHA-256	50abc85f...	ebbc2411...	50abc85f...
Integrity Match	—	No	Yes
Recoverability	—	—	100%

Table 15. Statistical Characteristics Before and After Encryption

Metric	Original	Encrypted	Decrypted
Entropy	7.977711	7.999810	7.977711
Correlation	0.018530	-0.000795	0.018530
Chi-Square	30345.36	215.00	30345.36
P-value	0.0000	0.96735	0.0000

The matching cryptographic hashes demonstrate that the proposed decryption process is lossless and fully reversible. Consequently, the encryption scheme satisfies one of the most fundamental requirements of secure file encryption systems. The encrypted file exhibits a dramatic statistical transformation compared with the original document. This indicates that the byte distribution of the ciphertext approaches a uniform random distribution, which significantly complicates statistical cryptanalysis. The entropy gain achieved by the proposed algorithm can be quantified as

$$\Delta H = H_{encrypted} - H_{original}$$
$$= 7.999810 - 7.977711$$
$$= 0.022099$$

Although numerically small, this increase is highly significant because the original PDF already possesses relatively high entropy due to compressed document structures. The ciphertext entropy is only 0.0024% below the theoretical maximum entropy value of 8, indicating that the encrypted file behaves almost identically to a random byte stream. The proposed scheme was further evaluated through NPCR, UACI, and Avalanche Effect measurements [72].

Table 16. Differential Attack Resistance

Metric	Obtained Value	Ideal Value
NPCR (%)	99.6061	>99
UACI (%)	33.6548	≈33
Avalanche (%)	49.9241	≈50

Table 17. Security Performance Scorecard

Security Criterion	Result	Assessment
MD5 Integrity Match	Pass	Excellent
SHA-256 Integrity Match	Pass	Excellent
Entropy	7.999810	Excellent
Correlation	-0.000795	Excellent
Chi-Square Test	Pass	Excellent
Randomness Test	Pass	Excellent
NPCR	99.6061%	Excellent
UACI	33.6548%	Excellent
Avalanche Effect	49.9241%	Excellent
File Recovery	100%	Excellent

We can see in **Table 16** and **Table 17** that the NPCR value of 99.6061% indicates that nearly all ciphertext bytes differ from the corresponding plaintext bytes after encryption. Similarly, the UACI value of 33.6548% closely matches the theoretical optimum of approximately 33%, suggesting strong average intensity variation between plaintext and ciphertext. The avalanche effect reached 49.9241%, which is extremely close to the ideal value of 50%. Collectively, these metrics confirm that the proposed algorithm exhibits excellent diffusion characteristics and strong resistance against differential cryptanalysis. For easier interpretation, the obtained results can be summarized into a cryptographic security scorecard [73].



Figure 11. Overall Cryptographic Security Dashboard

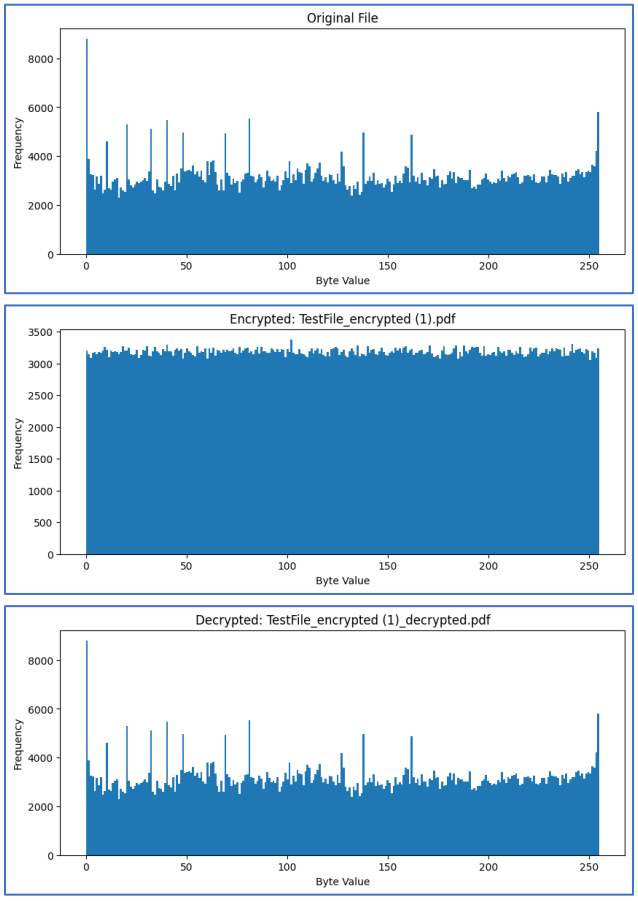


Figure 12. Histogram Visualization of Original, Encrypted, And Decrypted File

In **Figure 11**, **Figure 12**, and **Figure 13**, we can see that the combined results of NPCR, UACI, avalanche effect, MD5 verification, and SHA-256 verification provide strong evidence that the proposed Complete Graph Hill Cipher and Shift128 framework successfully satisfies the major security requirements expected from a modern file encryption system. The ciphertext exhibits near-ideal randomness characteristics, high diffusion capability, strong sensitivity to plaintext transformations, and complete reversibility. Most notably, the decrypted file perfectly reproduces the original PDF with identical MD5 and SHA-256 signatures, confirming both correctness and reliability of the proposed graph-based cryptographic framework. The effectiveness of an encryption algorithm can be quantitatively evaluated by measuring how significantly the statistical properties of the plaintext are transformed into ciphertext. **Table 18** and **Table 19** presents the statistical characteristics of the original, encrypted, and decrypted PDF files obtained from the proposed Complete Graph Hill Cipher framework [74].

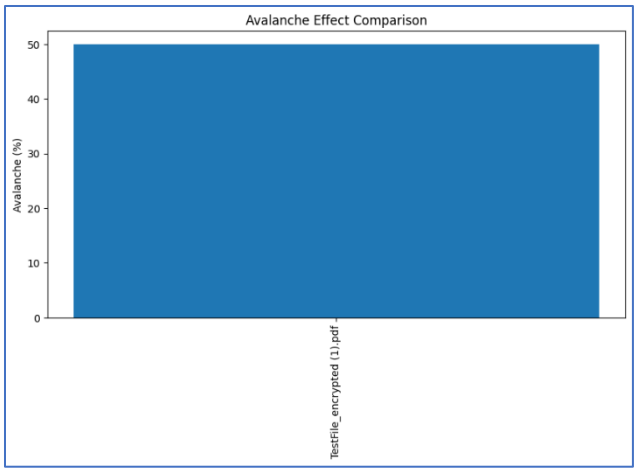


Figure 13. Histogram Visualization of Avalanche Effect Comparison

Table 18. Statistical Transformation of PDF Data

Metric	Original PDF	Encrypted PDF	Decrypted PDF
File Size (Bytes)	815,491	815,491	815,491
Entropy	7.977711	7.999810	7.977711
Correlation	0.018530	-0.000795	0.018530
Chi-Square	30,345.36	215.00	30,345.36
P-Value	0.000000	0.967350	0.000000
MD5 Match	Yes	No	Yes
SHA-256 Match	Yes	No	Yes

The results reveal three important observations. First, the encryption process significantly modifies the statistical distribution of byte values without changing the file size. Second, the ciphertext exhibits near-ideal randomness characteristics. Third, the decryption process perfectly restores the original statistical profile, demonstrating complete reversibility of the proposed cryptosystem. Information entropy measures the uncertainty of a data source [75], [76]. In **Figure 14**, For an 8-bit file, the theoretical maximum entropy is:

$$H_{max} = 8$$

The encrypted PDF achieved an entropy value of:

$$H_{enc} = 7.999810$$

which corresponds to an entropy utilization efficiency of

$$\eta_H = \frac{H_{enc}}{H_{max}} \times 100\%$$
$$= \frac{7.999810}{8} \times 100\%$$
$$= 99.9976\%$$

This result indicates that the ciphertext is only 0.0024% away from perfect randomness. A secure encryption algorithm should eliminate the natural dependency among neighboring bytes [77]. To quantify this capability, the correlation suppression ratio (CSR) can be calculated as

$$CSR = \left(1 - \frac{|\, r_{enc} \,|}{|\, r_{orig} \,|}\right) \times 100\%$$

Substituting the obtained values:

$$CSR = \left(1 - \frac{0.000795}{0.018530}\right) \times 100\%$$
$$= 95.71\%$$

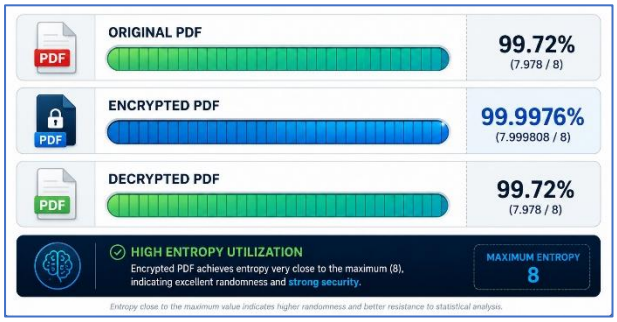


Figure 14. Entropy Utilization

Table 19. Correlation Reduction

Dataset	Correlation
Original PDF	0.018530
Encrypted PDF	-0.000795
Reduction	95.71%

The encryption process successfully removes approximately 96% of the detectable linear relationship among adjacent bytes. The chi-square statistic provides a measure of how closely a byte distribution approaches a uniform distribution. The reduction achieved by the proposed method is

$$\Delta\chi^2 = 30345.36 - 215.00$$
$$= 30130.36$$

which corresponds to

$$99.29\%$$

improvement toward uniformity [78], [79]. Furthermore, the encrypted file achieved

$$P = 0.967350$$

which is substantially larger than the commonly accepted threshold:

$$P > 0.05$$

indicating that the ciphertext distribution is statistically indistinguishable from a uniform random distribution. Another noteworthy observation is the complete transformation of both MD5 and SHA-256 digests after encryption. The drastic difference between the original and encrypted hash values demonstrates that the encryption process introduces extensive modifications throughout the entire file. Simultaneously, the restoration of identical hash values after decryption confirms the mathematical correctness of the inverse graph matrix operation [80].

Table 20. Uniform Distribution Improvement

Dataset	Chi-Square
Original PDF	30,345.36
Encrypted PDF	215.00
Improvement	99.29%

Table 21. Hash Transformation Analysis

Hash Function	Original	Encrypted	Decrypted
MD5	72cbaf26...1177	ad643caa...fc93	72cbaf26...1177
SHA-256	50abc85f...23a2	ebbc2411...4914	50abc85f...23a2



Figure 15.Overall Statistical Quality Assessment

We can see in **Table 20, Table 21,** and **Figure 15** that the statistical evidence demonstrates that the proposed Complete Graph Hill Cipher successfully transforms structured PDF data into ciphertext exhibiting near-ideal cryptographic characteristics. Moreover, both MD5 and SHA-256 hashes are completely altered after encryption yet perfectly restored after decryption. These findings collectively confirm that the proposed graph-based cryptosystem simultaneously achieves confidentiality, randomness, diffusion, and exact data recovery, making it suitable for secure binary file protection applications. It is important to note that the proposed CGHC-S128 framework operates directly in the binary-file domain rather than on textual data. Consequently, the encryption process is inherently applicable to virtually all forms of digital information, including PDF documents, images, videos, compressed archives, executable files, and other arbitrary binary formats [81]. In this study, PDF files were selected as representative test data because they contain complex binary structures commonly found in real-world digital documents. Although the Shift128 mechanism may appear mathematically simple when viewed in isolation, its effect in the binary-file domain is considerably more significant. Even a single-bit alteration in a structured binary file can corrupt critical headers, metadata, object references, or internal encoding structures, rendering the file partially or completely unreadable. Therefore, modifying residual bytes through Shift128 contributes to

effective data obfuscation despite its computational simplicity. Moreover, the residual-byte transformation is not employed as a standalone security mechanism; rather, it functions as a complementary component within the broader CGHC-S128 architecture, where binary-file partitioning and graph-based matrix encryption provide the primary confusion and diffusion properties. The combination of partition-based processing, matrix transformations, and residual-byte protection creates multiple layers of security that collectively make ciphertext interpretation and file reconstruction significantly more difficult without knowledge of the correct key parameters [79].

IV. CONCLUSION

The proposed CGHC-S128 framework introduces a graph-based cryptographic approach for universal binary file encryption by leveraging deterministic graph-matrix transformations and residual-byte protection mechanisms. Unlike conventional Hill Cipher implementations that require repeated searches for valid invertible key matrices, the proposed method utilizes complete graph adjacency matrices who's modular invertibility can be analytically guaranteed. Experimental evaluations on binary PDF files demonstrated that the proposed framework successfully preserves file size, achieves perfect file reconstruction, and produces ciphertext with strong cryptographic characteristics. The obtained entropy value of 7.999810, correlation coefficient of −0.000795, avalanche effect of 49.9241%, NPCR of 99.6061%, UACI of 33.6548%, and key sensitivity of 99.6114% collectively indicate that the generated ciphertext exhibits near-ideal randomness, strong diffusion, and high resistance against statistical and differential cryptanalysis. Furthermore, MD5 and SHA-256 verification confirmed lossless recovery of the original file after decryption, demonstrating the correctness and reversibility of the proposed graph-based encryption framework. Although the proposed method achieves promising security and integrity results, several open research challenges remain. First, the computational overhead associated with modular matrix inversion becomes significant for very large matrix dimensions, indicating a need for more efficient inverse computation strategies. Second, the current evaluation focuses primarily on PDF-based binary data and should be extended to broader datasets including images, videos, archives, executables, and large-scale multimedia files. Third, future studies should investigate resistance against known-plaintext, chosen-plaintext, chosen-ciphertext, and algebraic attacks to provide stronger cryptanalytic evidence. In addition, integrating dynamic graph structures, chaotic key generation mechanisms, sparse graph representations, or adaptive partition-selection strategies may further improve both security and computational efficiency. These directions constitute promising opportunities for advancing graph-based cryptography toward practical deployment in large-scale secure storage, cloud computing, multimedia protection, and next-generation digital security applications

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.

DECLARATION

Competing Interests

The authors declare that they have no competing interests, financial or non-financial, that could have influenced the work reported in this manuscript.

Funding

This research was financially supported by 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).

Author Contributions

SA conceived the research idea, designed the cryptographic framework, developed the algorithms, performed the experiments, analyzed the results, and drafted the manuscript. PFZ contributed to software implementation, experimental validation, and data analysis. AK contributed to methodology development and manuscript revision. TT and MGP participated in validation, visualization, and interpretation of the experimental results. EKS, DLH, and DW contributed to manuscript review, technical discussion, and supervision. All authors reviewed and approved the final manuscript.

Data Availability

All data used in this study consist of the binary bitstreams extracted from uploaded digital files. The proposed encryption scheme operates directly in the binary file domain, enabling encryption and decryption simulations on universal digital file formats without relying on file-

specific structures or content. Consequently, the experimental dataset is represented as binary sequences generated from the uploaded files, which serve as the input for evaluating the correctness, security, and performance of the proposed encryption and decryption algorithms.

Research Involving Human Participants and/or Animals

This study did not involve human participants, human biological materials, animals, or animal-derived specimens. The research was conducted exclusively using computational methods, mathematical modeling, cryptographic algorithms, and publicly available or self-generated binary test files (e.g., PDF documents) for experimental evaluation. Therefore, ethical approval and compliance with regulations concerning research involving humans or animals were not required.

Informed Consent

Not applicable. This study did not involve human participants, personal data, human tissue, or any form of participant interaction. Consequently, informed consent was not required.

REFERENCES

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

[2] 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.

[3] R. Wardhani, S. R. Nurshiami, and N. Larasati, "KOMPUTASI ENKRIPSI DAN DEKRIPSI MENGGUNAKAN ALGORITMA HILL CIPHER," *J. Ilm. Mat. dan Pendidik. Mat.*, 2022, doi: 10.20884/1.jmp.2022.14.1.5727.

[4] H. Wang, "Dual-modal system for real-time encryption and anomaly detection of 5G communication data integrating AES-GCM and LSTM," *Int. J. Inf. Commun. Technol.*, vol. 27, no. 41, pp. 21–44, 2026, doi: 10.1504/IJICT.2026.10077622.

[5] M. B. Aryanto, M. Tahir, S. Devita, Z. N. Mustofa, Q. Ainiyah, and S. Sundoro, "Implementasi Enkrip Dan Dekrip File Menggunakan Metode Advance Encryption Standard (AES-128)," *J. Ilm. Sist. Inf. dan Ilmu Komput.*, 2023, doi: 10.55606/juisik.v3i1.434.

[6] A. M. Rasheed and R. M. S. Kumar, "Lightweight Cryptographic Algorithms for Medical IoT Devices using Combined Transformation and Expansion (CTE) and Dynamic Chaotic System," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 4, pp. 705–715, 2024, doi: 10.14569/IJACSA.2024.0150472.

[7] 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.

[8] 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.

[9] R. A. Menezes, R. S. Araujo, L. S. Rodrigues, E. S. Nascimento, and R. L. Gomes, "Data Protection through the Integration of TPM and Cryptography," *Int. J. Wirel. Microw. Technol.*, vol. 16, no. 1, pp. 37–49, 2026, doi: 10.5815/ijwmt.2026.01.03.

[10] 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.

[11] M. M. Ibrahim and R. Venkatesan, "IMAGE ENCRYPTION USING NOVEL CHAOTIC MAP AND CELLULAR AUTOMATA DYNAMICS," *RAIRO - Theor. Informatics Appl.*, vol. 59, 2025, doi: 10.1051/ita/2025001.

[12] 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., Apr. 2021, p. 020003. doi: 10.1063/5.0041650.

[13] 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.

[14] 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.

[15] B. Roopa, J. Saral, R. Senthamizh Selvi, and R. Binthiya, "Antimagic Labeling of Bi-Star Graphs for Secure and Efficient Cryptographic Data Transformation," *Int. J. Glob. Acad. Sci. Res.*, vol. 4, no. 4, pp. 71–87, 2025, doi: 10.55938/ijgasr.v4i4.242.

[16] L. Julakidze, Z. Kochladze, and T. Kaishauri, "New symmetric tweakable block cipher," *Bull. Georg. Natl. Acad. Sci.*, vol. 15, no. 1, pp. 13–19, 2021.

[17] A. Banga, "Secure Ultra-Low Latency Data Paths: A Hybrid Architecture for High Speed Networking under Adversarial Conditions," *Int. J. Adv. Comput. Sci. Appl.*, vol. 17, no. 2, pp. 447–456, 2026, doi: 10.14569/IJACSA.2026.0170247.

[18] A. Srivastava, B. Rawat, G. Singh, V. Bhatnagar, and S. A. Dhondiyal, "A Review of the Authentication Scheme Using HECC and ECC," Graphic Era Hill University, Department of Computer Science and Engineering, Dehradun, UK, India: Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICBDS58040.2023.10346513.

[19] M. K. Shathir, R. K. Ajeena, and G. E. Arif, "The triple vertex path graph for hill encryption schemes," 2023, p. 060028. doi: 10.1063/5.0170404.

[20] 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.

[21] 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.

[22] 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.

[23] C. M. S. Tan, G. P. Arada, A. C. Abad, and E. R. Magsino, "A Hybrid Encryption and Decryption Algorithm using Caesar and Vigenere Cipher," in *Journal of Physics: Conference Series*, 2021. doi: 10.1088/1742-6596/1997/1/012021.

[24] 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.

[25] S. Salman, Yasmin Makki Mohialden, Abbas Abdulhameed, and Nadia Mahmood Hussien, "A Novel Method for Hill Cipher Encryption and Decryption Using Gaussian Integers Implemented in Banking Systems," *Iraqi J. Comput. Sci. Math.*, vol. 5, no. 1, pp. 277–284, Feb. 2024, doi: 10.52866/ijcsm.2024.05.01.019.

[26] R. Safitri, P. W. Prasetyo, D. E. Wijayanti, S. Arifin, F. Setyawan, and J. Repka, "Improving Text Security by Using The Combination of Vigenere Cipher and Rubik's Cube Methods of the Size 4×4×4," *Al-Jabar J. Pendidik. Mat.*, vol. 14, no. 2, pp. 281–297, 2023.

[27] 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.

[28] 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.

[29] G. Rekha and V. Srinivas, "Encryption and Decryption using Hill Cipher and Integral Transforms," *Commun. Appl.*

Nonlinear Anal., 2024, doi: 10.52783/cana.v31.1173.

[30] 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.

[31] 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.

[32] 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.

[33] B. Vasuki, L. Shobana, and B. Roopa, "Data Encryption Using Face Antimagic Labeling and Hill Cipher," *Math. Stat.*, vol. 10, no. 2, pp. 431–435, 2022, doi: 10.13189/ms.2022.100218.

[34] I. Kouadra, T. Bekkouche, L. Ziet, I. Mehidi, S. Alshathri, and W. El-Shafai, "New Composite Chaotic Map Applied to an Image Encryption Scheme in Cybersecurity Applications," *IEEE Access*, vol. 13, pp. 70676–70690, 2025, doi: 10.1109/ACCESS.2025.3558948.

[35] A. Desoky and A. P. Madhusoodhanan, "Bitwise hill crypto system," in *IEEE International Symposium on Signal Processing and Information Technology, ISSPIT 2011*, 2011, pp. 080–085. doi: 10.1109/ISSPIT.2011.6151539.

[36] 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.

[37] B. Acharya, J. Venkata Sravan, D. R. Janaki Potnuru, and K. Abhimanyu Kumar Patro, "MIE-SPD: A New and Highly Efficient Chaos-Based Multiple Image Encryption Technique With Synchronous Permutation Diffusion," *IEEE Access*, vol. 13, pp. 62773–62797, 2025, doi: 10.1109/ACCESS.2025.3558943.

[38] R. M. al-Amri, D. N. Hamood, and A. K. Farhan, "Theoretical Background of Cryptography," *Mesopotamian J. CyberSecurity*, vol. 2023, pp. 7–15, 2023, doi: 10.58496/MJCS/2023/002.

[39] M. Beighton, "Security analysis of shift-register based keystream generators for stream ciphers," 2022, doi: 10.5204/thesis.eprints.236239.

[40] Y. Pan, "The Scope of Application of Letter Frequency Analysis in Substitution Cipher," in *Journal of Physics: Conference Series*, 2022. doi: 10.1088/1742-6596/2386/1/012015.

[41] 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

[42] M. Rekha and P. S. Rani, "Enhancing cloud security using attention-based improved RegNet with hybrid vigenere-shift transposition algorithm," *J. Cloud Comput.*, vol. 14, no. 1, 2025, doi: 10.1186/s13677-025-00794-1.

[43] et al. Pujeri, Uma Ramachandra, "Encryption Techniques for Modern World," in *Theoretical and Applied Mathematics in International Business*, B. C. and F. Shuwaikh, Ed., IGI Global, 2020, pp. 285–319. doi: https://doi.org/10.4018/978-1-5225-8458-2.ch013.

[44] H. N. Noor Muchsin, D. E. Sari, D. R. Ignatius Moses Setiadi, and E. H. Rachmawanto, "Text Encryption using Extended Bit Circular Shift Cipher," *Proc. 2019 4th Int. Conf. Informatics Comput. ICIC 2019*, no. October, 2019, doi: 10.1109/ICIC47613.2019.8985708.

[45] K. Wijaya, E. T. Baskoro, H. Assiyatun, and D. Suprijanto, "The complete list of Ramsey $(2K_2,K_4)$-minimal graphs," *Electron. J. Graph Theory Appl.*, vol. 3, no. 2, pp. 216–227.

[46] 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.

[47] Z. Feng and K. Markov, "SpeQNet: Query-Enhanced Spectral Graph Filtering for Spatiotemporal Forecasting," *Appl. Sci.*, vol. 16, no. 3, 2026, doi: 10.3390/app16031176.

[48] E. Ishchukova, S. Petrenko, A. Petrenko, K. Gnidko, and A. Nekrasov, "Potential Vulnerabilities of Cryptographic Primitives in Modern Blockchain Platforms," *Sci*, vol. 7, no. 3, 2025, doi: 10.3390/sci7030112.

[49] B. M. S. et al. Komosko L. *et al.*, "A fast greedy sequential heuristic for the vertex colouring problem based on bitwise operations," *J. Comb. Optim.*, vol. 31, no. 4, pp. 1665–1677, 2016, doi: 10.1007/s10878-015-9862-1.

[50] S. Arifin, I. B. Muktyas, and J. M. Mandei, "Graph coloring program for variation of exam scheduling modeling at Binus University based on Welsh and Powell algorithm," in *International Conference Advanced in Applied Mathematics (ICAAM 2021)*, 2022, pp. 1–5. doi: 10.1088/1742-6596/2279/1/012005.

[51] S. Epsikoposyan and D. Hovhannisyan, "Hybrid audio encryption method based on DCT and Walsh-Hadamard transform using Henon chaotic maps and logistic maps," *Int. J. Electron. Telecommun.*, vol. 72, no. 2, 2026, doi: 10.24425/ijet.2026.157909.

[52] 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.

[53] 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.

[54] S. Bentouila and K. M. Faraoun, "Deep Learning-Driven DNA Image Encryption with Optimal Chaotic Map Selection," *Int. J. Adv. Comput. Sci. Appl.*, vol. 16, no. 7, pp. 918–929, 2025, doi: 10.14569/IJACSA.2025.0160789.

[55] 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.

[56] M. A. Ibrahim, N. T. M. Sagala, S. Arifin, R. Nariswari, N. P. Murnaka, and P. W. Prasetyo, "Separating Hate Speech from Abusive Language on Indonesian Twitter," in *2022 International Conference on Data Science and Its Applications (ICoDSA)*, IEEE, 2022, pp. 187–191.

[57] S. El Kaddouhi *et al.*, "A new image encryption approach that uses an improved Hill-Vigenère method and chaotic maps," *Multimed. Tools Appl.*, vol. 84, pp. 17279–17307, Jul. 2024, doi: 10.1007/s11042-024-19472-6.

[58] D. Khalaf, K. Hussain, and M. Darwish, "Enhanced Hill Cipher Encryption Using Chaotic Logistic Maps for Improved Security and Key Randomness," *JES. J. Eng. Sci.*, 2025, doi: 10.21608/jesaun.2025.434995.

[59] A. Al-Hyari, M. Abu-Faraj, C. Obimbo, and M. Alazab, "Chaotic Hénon-Logistic Map Integration: A Powerful Approach for Safeguarding Digital Images," *J. Cybersecur. Priv.*, vol. 5, p. 8, 2025, doi: 10.3390/jcp5010008.

[60] R. J. Rasras, M. R. A. Sara, J. Nader, and Z. Alqadi, "Optimized chaos based encryption-decryption of multimedia data," *Bull. Electr. Eng. Informatics*, vol. 15, no. 2, pp. 1731–1742, 2026, doi: 10.11591/eei.v15i2.11220.

[61] 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.

[62] 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.

[63] R. K. Hasoun, S. F. Khlebus, and H. K. Tayyeh, "A new approach of classical hill cipher in public key cryptography," *Int. J. Nonlinear Anal. Appl.*, vol. 12, no. 2, pp. 1071–1082, 2021, doi: 10.22075/ijnaa.2021.5176.

[64] 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.

[65] 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.

[66] A. Abba, J. S. Teh, M. N. Yusoff, and A. Anwar, "Towards Analyzable Design Paradigms for Chaos-Based Cryptographic Primitives," *J. Cybersecurity Priv.*, vol. 5, no. 3, 2025, doi: 10.3390/jcp5030064.

[67] N. M. Abbas and M. E. Abdulmunim, "LUC Image Encryption Enhancement Using a Hyper-Chaotic System and DNA," *Iraqi*

J. Sci., vol. 65, no. 12, pp. 7157–7168, 2024, doi: 10.24996/ijs.2024.65.12.30.
[68] W. M. Abd-Elhafiez, M. Abdel-Aty, X.-J. Yang, and A. Balobaid, "AN IMAGE ENCRYPTION TECHNIQUE BASED ON DISCRETE WAVELET TRANSFORM AND FRACTIONAL CHAOTIC CRYPTOVIROLOGY," *Fractals*, vol. 32, no. 4, 2024, doi: 10.1142/S0218348X23401242.
[69] S. S. Abed and A. G. Nasir, "Design of New Efficient Stream Key Generator to Protect the Classified Information," *Iraqi J. Sci.*, vol. 65, no. 5, pp. 2619–2629, 2024, doi: 10.24996/ijs.2024.65.5.22.
[70] A. O. Adelakun, G. O. Emmanuel, and F. M. Adelakun, "Secure multimodal biometric authentication using cyclically coupled fractional-order hyperchaotic systems," *Phys. Scr.*, vol. 101, no. 15, 2026, doi: 10.1088/1402-4896/ae5b34.
[71] M. Agarwal, C. Arya, and R. Ratan, "Fuzzy Soft Set-Based Identification of Best Chaotic System for Security Applications," *Def. Sci. J.*, vol. 74, no. 6, pp. 893–903, 2024, doi: 10.14429/dsj.74.19877.
[72] S. Agrawal and B. R. Madhu, "A Secure Image Encryption Framework Using Modified Henon Map with Integrity Verification," *Int. J. Comput. Digit. Syst.*, vol. 18, no. 1, 2025, doi: 10.12785/ijcds/1571111849.
[73] A. M. Ajaj, M. T. Wazi, F. J. Al-Zahid, and N. M. G. Al-Saidi, "Quantum Image Encryption Using 4D Hamiltonian System and Bit-Plane Encoding," *Ing. des Syst. d'Information*, vol. 30, no. 10, pp. 2691–2705, 2025, doi: 10.18280/isi.301015.
[74] 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.
[75] W. Alayed, A. U. Rehman, M. A. Ehsan, W. U. Hassan, and A. Zeeshan, "Brownian-Perturbed Hénon Map for Image Encryption: Application in Biomedical Images," *Comput. Mater. Contin.*, vol. 88, no. 1, 2026, doi: 10.32604/cmc.2026.078078.
[76] K. Meera and N. Selvaganesan, "Generalized Fractional Order Complex Lorenz System-Based Dual Layer Security Enhancement Approach," *IEEE Access*, vol. 13, pp. 112162–112175, 2025, doi: 10.1109/ACCESS.2025.3583894.
[77] A. Al-Daraiseh, Y. Sanjalawe, S. Fraihat, and S. Al-E'mari, "Novel, Fast, Strong, and Parallel: A Colored Image Cipher Based on SBTM CPRNG," *Symmetry (Basel).*, vol. 16, no. 5, 2024, doi: 10.3390/sym16050593.
[78] W. Alexan *et al.*, "Triple Layer RGB Image Encryption Algorithm Utilizing Three Hyperchaotic Systems and Its FPGA Implementation," *IEEE Access*, vol. 12, pp. 118339–118361, 2024, doi: 10.1109/ACCESS.2024.3446733.
[79] A. H. Ali, E. K. Gbashi, H. Alaskar, and A. J. Hussain, "A Lightweight Image Encryption Algorithm Based on Secure Key Generation," *IEEE Access*, vol. 12, pp. 95871–95883, 2024, doi: 10.1109/ACCESS.2024.3414334.
[80] 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.
[81] A. Al-Hyari, C. Obimbo, M. M. Abu-Faraj, and I. Al-Taharwa, "Generating Powerful Encryption Keys for Image Cryptography With Chaotic Maps by Incorporating Collatz Conjecture," *IEEE Access*, vol. 12, pp. 4825–4844, 2024, doi: 10.1109/ACCESS.2024.3349470.

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.

Paskalis Farelnata Zamasi is a Data Science undergraduate student at Institut Teknologi Sains Bandung (ITSB), Indonesia, whose academic development has been shaped by foundational coursework in data, logic, programming, and analytical methods within the Data Science curriculum framework at ITSB. His primary academic interest lies in Discrete Mathematics, particularly graph theory concepts such as simple graphs, adjacency relations, complete graphs, and structural relationships between objects, which he finds intellectually engaging due to their strong theoretical and computational foundations. Beyond theoretical exploration, he demonstrates a growing interest in practical applications of discrete mathematical concepts in programming contexts, especially in encryption and decryption systems, where mathematical structures are directly translated into algorithms for information security and data processing.

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.