Applied Mathematics and Computational Intelligence
Volume 13, No. 3, 2024 [13 – 25]

Self-Invertible Key on Cipher Polygraphic Polyfunction with Eigen Matrix based IMIE

Faridah Binti Yunos[1], Nur Aqilah Fakhira Binti Ayub[2*], Nurul Fatin Atiqa Binti Mohammad Rasyidi[3], Muhammad Asyraf Bin Asbullah[4]

[1,2,3]Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[4]Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[4]Centre of Foundation Studies for Agriculture Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.

* Corresponding author: faridahy@upm.edu.my; qikyrxxx@gmail.com

Received: 16 November 2023
Revised: 10 June 2024
Accepted: 15 July 2024

ABSTRACT

Hill Cipher's System and its modifications are still practiced mainly in sending a secret message involving images. One drawback that the recipient of the message is trying to overcome is to get the decryption key from the cipher text to plain text during the decryption process. Previous studies have proven that using self-invertible keys can reduce the complexity to obtain this key. This paper generates a self-invertible matrix based on Integer-Entry Matrix with all Integer Eigenvalues (IMIE). Subsequently, we executed it into Cipher Polygraphic Polyfunction Cryptosystem and observed the effect. We noticed that when the self-invertible key was employed during even-th transformations, the system became vulnerable to adversary attacks due to recurrence results. It is unnecessary to alter the original message through odd-th transformations, as this process only retrieves the original message.

Keywords: Hill Cipher, self-invertible, matrix, decryption, eigenmatrix

1 INTRODUCTION

Cryptography is the study of securing data by converting it into an unreadable form known as cipher text via an encryption process that can be classified into two categories, known as symmetric cipher and asymmetric cipher. It is a process for storing and transmitting data in a way only the designated receiver may access to achieve the information security goals of secrecy, integrity, authentication and nonrepudiation. Applied Mathematics, Computer Science, Physics, Electrical Engineering and Communication Science are all incorporated into modern cryptography. Nowadays, number theory, algebra and probability are the three branches of Mathematics most frequently employed in cryptography. Modern computing systems now place a high priority on information security. There is no doubt that most of the data and other sensitive information will be regularly fabricated, changed and formatted by system attackers if security precautions are not taken. Some current cryptographic algorithms that can protect information, data or communications include the Advanced Encryption Standard (AES), Data Encryption Standard (DES), Gosudarstvennyi

Standard (GOST), and Rivest–Shamir–Adleman (RSA) algorithms.

Cryptography encompasses two primary classifications: symmetric and asymmetric keys cryptography. Symmetric key further divides into classical and modern cryptography. In the realm of classical cryptography, we encounter transposition cipher and substitution cipher. On the other hand, modern cryptography comprises stream cipher and block cipher. Symmetric key cryptography employs a shared secret key for both plaintext encryption and ciphertext decryption. While the keys may be identical, a simple transformation process might be required to transition between them. Hill Cipher, a renowned symmetric key scheme, is a linear transformation acting on a message space consisting of m-dimensional vectors of integers [1]. A plaintext string, comprising characters from an alphabet of order m, is rewritten as a vector over Z_m using a natural correspondence [2].

According to [3], in the Hill Cipher method, the numerical representation of plaintext is often structured as a matrix P with d rows. Here, d is an arbitrary positive integer chosen for the purpose. To encrypt the plaintext, a key matrix K is selected, and the resulting ciphertext C is obtained through the following process:

$$C \equiv KP \pmod{N}$$

where N is a positive integer. To decrypt the ciphertext and convert the resulting matrix back into a string using the same alphabet, the decryption process is performed as follows:

$$P \equiv K^{-1}C \pmod{N}$$

where K^{-1} is the inverse of K in modulo N.

In the realm of Hill Cipher cryptography, employing involutory matrices as secret keys can significantly simplify the decryption process. An involutory matrix is a square matrix with the unique property that its inverse is equivalent to the matrix itself. This characteristic eliminates the requirement to find the inverse of the key matrix during decryption. The process of obtaining the inverse key matrix in invertible cases can be challenging, often involving elementary row operations and the concept of modular multiplicative inverse within modular arithmetic. By leveraging involutory matrices, we can streamline the Hill Cipher encryption and decryption procedures [4, 5]. [6] have unfolded some methods of generating any dimension of the self-invertible matrix to be used in Hill Cipher. These techniques were implemented in modified Hill Cipher system such as in [7–16].

[11] proposed a two-stage Hill Cipher, including selecting square blocks to manipulate a self-invertible matrix. The objective of this proposition was to regulate the amount of encryption of pixel changing rate. To achieve this, the researchers employed the Latin Square Image Cipher method to create a basic block of self-invertible matrix. They further compared the encryption information between two-stage and four-stage Hill Cipher techniques to improve the camera's intelligence and expand the scope of applicable fields. By doing so, they aimed to enhance the efficiency and versatility of their encryption approach in image processing applications.

Cipher Polygraphic Polyfunction presented in [13] is a modification of the Hill Cipher technique in modern cryptography. It was built on the system using three symbols or letters and more than one transformation of the original message. The modular arithmetic of a key matrix plays an important role in the encryption and decryption processes. A crucial aspect of the encryption process is to get

the inverse matrix for self-invertible matrices. [12] found some solutions for $L^3_{2\times2} \equiv A_{2\times2} \pmod N$, where the self invertible marix can be generated by $L_{2\times2}$ via Type 1 method [6]. To enhance the security of Cipher Tetragraphic Trifunction (CTetraTri), some patterns of $L_{2\times2}$ as generator key should be avoided before implementing CTetraTri since they are easily attacked by a third party. Meanwhile, [13] also faced the same effects on Cipher Hexagraphic Polyfunction (CHexaPoly) when they implemented a self-invertible encryption key for each transformation. This key is generated by $L_{3\times3}$ using Type 2 method [6] where $L^2_{3\text{x}3} \equiv A_{3\times3} \pmod N$.

Furthermore, [14] gave some solution of $L^2_{2\times2} \equiv A_{2\times2} \pmod N$ and generated suitable self-invertible matrices from $L_{2\times2}$ through Type 2 method [6]. This reduced the complexity of finding the decryption key in CTriPoly.

Although the Hill Cipher algorithm is one of the symmetric methods that provide a simple structure and quick computations, it has a low level of security since the transmitter and receiver must use and exchange the same private key through insecure channels. Thus, [15] proposed the combination of Elliptical Curve Cryptography over a binary field and Hill Cipher as a new grayscale image encryption method. The self-invertible matrix implemented using the Type 1 method [6] in this research expedites the decryption process for grayscale images with a resolution of 128×128. This is achieved by removing the need to calculate the inverse of the key matrix, resulting in a robust key that thwarts attackers and offers enhanced security, as the key need not be shared with others.

[16] introduced a novel image encryption method incorporating a three-dimensional conservative system characterized by hyperbolic functions. The dynamical properties of the proposed system are analysed through Lyapunov exponents and bifurcation diagrams. A 4×4 self-invertible matrix-based Type 1 [6] is designed using a modified Diffie-Hellman key exchange protocol to generate the key matrix K. The image encryption approach consists of three primary stages. In the first stage, the proposed three-dimensional system utilizes the original image to generate three sequences, two of which are employed for confusion and diffusion processes. The second stage involves pixel position alteration to introduce confusion. Lastly, in the third stage, the 4×4 sub-blocks of the confused image are encrypted by multiplying them with K. Simulation results demonstrate that the proposed image encryption scheme exhibits a high level of security and resistance against statistical analysis, noise, and various attacks.

The highlights of the above study focus on using self-invertible keys to reduce the complexity to obtain inverse keys and improve the security system in Hill Cipher and its extension. In this paper, we re-used the Type 3 method proposed by [6] to generate these keys. An issue that arises pertains to the identification of specific characteristics inherent to diagonal matrices that render them non-singular and meet the prerequisites for self-invertible matrices ($A_{4\times4}$) prior to utilizing matrix A as the encryption key within the Cipher Polygraphic Polyfunction.

The organization of this paper is as follows. Section 1 describes the implementation of the self-invertible matrix in Hill cipher and its variant with some advantages. In Section 2, the preliminaries of this study are presented. Meanwhile, Section 3 compares the number of invertible and self-invertible matrices in modulo a prime number. This was followed by a discussion on generating a self-invertible matrix based on Integer-Entry Matrix with All Integer Eigenvalues (IMIE). The effect of using this new self-invertible as an encryption key in Cipher Polygraphic Polyfunction is

discussed in Section 4. The concluding section contains a summary of the paper.

2 PRELIMINARIES

The following are some notations to be considered in this paper:

Plaintext is the ordinary message delivered to the receiver [17]. P refers to the corresponding number in the plaintext, such as $A = 0$, $B = 1$, $C = 2$,..., $Z = 25$. The plaintext would be arranged in matrix form $P_{i\times j}$. For example, the corresponding number sequence of plaintext $O\ P\ T\ I\ M\ I\ Z\ A\ T\ I\ O\ N$ is 14 15 19 08 12 08 25 00 19 08 14 13, which are arranged by matrix 4 by 3 given by $P_{4\times 3} = \begin{bmatrix} 14 & 15 & 19 \\ 08 & 12 & 08 \\ 25 & 00 & 19 \\ 08 & 14 & 13 \end{bmatrix}$

Ciphertext is the encrypted message sent to the recipient [18]. $C^{(t)}_{i\times j}$ is an equivalent numbers sequence with ciphertext based on i^{th} row and j^{th} column matrix at t - transformation for $t = 1, 2, 3, \ldots$. Let $C^{(1)}_{i\times j} = C_{i\times j}$ [12, 13]. For example, the corresponding number of ciphertext $P\ Q\ R\ S\ T\ U$ produced by the third transformation is 15 16 17 18 19 20 arranged by a matrix having 2 rows and 3 columns given by $C^{(3)}_{2\times 3} = \begin{bmatrix} 15 & 16 & 17 \\ 18 & 19 & 20 \end{bmatrix}$.

Encryption refers to the process of implementing transformations on plaintext, to generate an altered version called ciphertext. This process is carried out following a specific encryption algorithm and making use of a chosen key. The resultant ciphertext maintains confidentiality and security, primarily when transmitted or stored in insecure environments. Encryption key $A_{i\times i}$ is arranged based on matrix i^{th} row and i^{th} column while $A^{-1}_{i\times i}$ is the inverse matrix for $A_{i\times i}$ such that $|A_{i\times i}| \neq 0$ [12, 13]. In contrast, decryption is the procedure that enables the conversion of ciphertext back into its original form, known as plaintext. This process necessitates the use of a decryption algorithm and the corresponding key. Unlike encryption, which may employ a public key to encrypt plaintext into ciphertext, decryption requires a secret key to perform the reverse operation, transforming the ciphertext into the original plaintext.

The cryptosystem that we will focus on in this research is constructed based on Cipher Polygraphic Polyfunction as follows:

Theorem 1. [13] Let Cipher Polygraphic Polyfunction Transformation be defined as:

$C^{(t)}_{i\times j} \equiv A^{t}_{i\times i} P_{i\times j} \pmod N$

where $t \in \mathbb{Z}^+$ and $A_{i\times i}$ act as an encryption key. Assume that the determinant for $A_{i\times i}$ is not zero and $\gcd(|A_{i\times i}|, N) = 1$. Then, $P_{i\times j}$ have a unique solution and the decryption algorithm is given as follows:

$P_{i\times j} \equiv (A^{-1}_{i\times i})^{t} C^{(t)}_{i\times j} \pmod N$

where the decryption key $A^{-1}_{i\times i}$ is the inverse matrix of $A_{i\times i}$.

Remark:

1. For the decryption process, the determinant of $A_{i\times i}$ must be non-zero to assure that A has an inverse. There is a possibility that $A_{i\times i}$ is self-invertible. This ensures the plaintext is unique with condition $\gcd(|A_{i\times i}|, N) = 1$.

2. If $i = 3$, $i = 4$, $i = 5$, and $i = 6$, then the above system is denoted as Cipher Trigraphic Polyfunction (CTriPoly), Cipher Tetragraphic Polyfunction (CTetraPoly), Cipher Pentagraphic Polyfunction (CPentaPoly) and Cipher Hexagraphic Polyfunction (CHexaPoly), respectively. If $A_{i\times i} \equiv A_{i\times i}^{-1} \pmod N$, then $A_{i\times i}$ is considered self-invertible matrix, where $A_{i\times i}^{-1}$ represents an inverse of $A_{i\times i} \pmod N$ [12], [13].

3. N is not necessarily a prime number.

4. An $i\times i$ matrix A is diagonalizable if there is an invertible $i\times i$ matrix B such that $D = B^{-1}AB$ is a diagonal matrix. The matrix B is said to be diagonalized A.

3 GENERATION OF SELF-INVERTIBLE MATRIX

The following theorems can compare the total number of invertible and self-invertible matrix.

Theorem 2. [2], [19] The number of $d \times d$ invertible matrices over $\mathbb{Z}_N$ for a prime N is

$$|GL(d, \mathbb{Z}_N)| = \prod_{i=0}^{d-1}(N^d - N^i).$$

Theorem 3. [2] For a $d \times d$ integer matrix X, the number of solutions of $X^2 \equiv I \pmod{N^{a+1}}$ for an odd prime is given by

$$T(d, N^{\alpha+1}) = \sum_{t=0}^{d}\left(\frac{g_d}{g_t g_{d-t}} N^{2t(d-t)a}\right)$$

where $\alpha \geq 0$ and g_t is given by

$$g_t = N^{t^2}\prod_{i=1}^{t}(1-N^{-i}) = \prod_{i=1}^{t-1}(N^t - N^i),$$

for $0 < t \leq d$ and $g_0 = 1$.

Example 1. We obtained the number of 4×4 invertible matrices for $\mathbb{Z}_{13}$ by using $|GL(4, \mathbb{Z}_{13})| = \prod_{i=0}^{3}(13^4 - 13^i) = 610296923230525440$. Meanwhile, the number of self-invertible matrices can be found by $T(4, 13) = \sum_{t=0}^{4}\left(\frac{g_4}{g_t g_{4-t}}\right) = 898990432$ with $g_t = 13^{t^2}\prod_{i=1}^{t}(1 - 13^{-i})$.

Since the self-invertible can be manipulated to reduce computation time for the decryption process, in this section, we want to find a way to generate such a matrix before implementing it in a Cipher

Polygraphic Polyfunction cryptosystem. We begin with choosing such a matrix which is IMIE defined as follows:

Definition 1. [20] A matrix A is an IMIE if it is an integer-entry matrix with (all) integer eigenvalues. In other words, the polynomial of A factors completely over $\mathbb{Z}$.

[20] introduced a simple method to construct such a matrix from a predetermined set of eigenvectors. Concisely, to construct $A = BDB^{-1}$ which is IMIE, where D is a diagonal matrix whose diagonal entries are the eigenvalues of A while the column of matrix B that is an invertible matrix form as the basis of eigenvectors for A. According to the following theorem, matrix B (with a specific determinant) and its inverse can be found from the outer product of two vectors.

Theorem 4. [20] Given two i-vectors $\overrightarrow{u}$, $\overrightarrow{v} \in \mathbb{Z}^i$ with $\overrightarrow{u} \cdot \overrightarrow{v} = \beta$, $B = I + \overrightarrow{u}\overrightarrow{v}^T$ has determinant $B = 1 + \beta$. In addition, if $\beta \neq -1$, then $B^{-1} = I - \frac{1}{1+\beta}\overrightarrow{u}\overrightarrow{v}^T$, where $\overrightarrow{u}\overrightarrow{v}^T$ is the $i \times i$ outer product of matrix and $\overrightarrow{v}^T$ is the transpose of the vector $\overrightarrow{v}$.

Based on Theorem 4, it has produces two corollaries which are:

Corollary 1. [20] Given two i-vectors $\overrightarrow{u}$, $\overrightarrow{v} \in \mathbb{Z}^i$ with $\overrightarrow{u} \cdot \overrightarrow{v} = -2$, the matrix $B^{-1} = B = I + \overrightarrow{u}\overrightarrow{v}^T$ is integral and involuntary, where $B = B^{-1}$.

Corollary 2. [21] Given two i-vectors $\overrightarrow{u}$, $\overrightarrow{v} \in \mathbb{Z}^i$ which are orthogonal, the matrix $B = I + \overrightarrow{u}\overrightarrow{v}^T$ has $\det(B) = 1$ and its inverse $B^{-1} = I - \overrightarrow{u}\overrightarrow{v}^T$.

However, in this paper, we only focus on Corollary 2 to produce an eigenmatrix A, which is IMIE when $\delta = \det(B) = 1$. This follows from the idea obtained from the following theorem:

Theorem 5. [20] Let B be an $i \times i$ integer matrix with determinant δ not equal to 0. Let D be a diagonal matrix whose diagonal entries are all integers that are mutually congruent modulo δ. Then, $A = BDB^{-1}$ is an integer matrix.

Concisely, let $B \in GL_i(\mathbb{Z})$ and $D = (\lambda_1, ..., \lambda_i)$ with eigenvalues $\lambda_j \in \mathbb{Z}$. If $\lambda_1 \equiv \lambda_2 \equiv \lambda_3 \equiv ... \equiv \lambda_i \mod \delta$, then BDB^{-1} is a diagonalizable IMIE. This implies that $\lambda_j = \pm 1$ because $\delta = 1$. Now, we proceed with the following algorithm to generate a matrix, A. Steps 1 until 3 will guide us to find matrix B and its inverse using Corollary 2. Meanwhile, the last step is to find the eigenmatrix, A, by applying Theorem 5. Hence, such matrix is self-invertible since $A^{-1} = (BDB^{-1})^{-1} = A$ (refer Type 3 in Appendix).

Algorithm 1.

1. Choose vectors $\overrightarrow{u}$ and $\overrightarrow{v}$ that are orthogonal where the inner product of $\overrightarrow{u}$ and $\overrightarrow{v}$ are equal to 0.
2. Compute matrix B by $B = I + \overrightarrow{u}\overrightarrow{v}^T$.
3. Compute its inverse by $B^{-1} = I - \overrightarrow{u}\overrightarrow{v}^T$.
4. Generate self -invertible matrix (A) using $A \equiv BDB^{-1} (\mod N)$.

Example 2. Let $\overrightarrow{\mathrm{u}} \equiv \begin{bmatrix} 9 \\ 3 \\ 1 \\ 3 \end{bmatrix}$ and $\overrightarrow{\mathrm{v}} \equiv \begin{bmatrix} 2 \\ 4 \\ 7 \\ 5 \end{bmatrix}$ be two vectors in modulo 26.

The self-invertible matrix A can be found through the following steps:

Step 1
The inner product of $\overrightarrow{\mathrm{u}}$ and $\overrightarrow{\mathrm{v}}$ is 0. Therefore, they are orthogonal.

Step 2
Compute the outer product as follows:

$$\overrightarrow{\mathrm{u}}\,\overrightarrow{\mathrm{v}}^T \equiv \begin{bmatrix} 9 \\ 3 \\ 1 \\ 3 \end{bmatrix} \begin{bmatrix} 2 & 4 & 7 & 5 \end{bmatrix} \equiv \begin{bmatrix} 9(2) & 9(4) & 9(7) & 9(5) \\ 3(2) & 3(4) & 3(7) & 3(5) \\ 1(2) & 1(4) & 1(7) & 1(5) \\ 3(2) & 3(4) & 3(7) & 3(5) \end{bmatrix} \equiv \begin{bmatrix} 18 & 10 & 11 & 19 \\ 6 & 12 & 21 & 15 \\ 2 & 4 & 7 & 5 \\ 6 & 12 & 21 & 15 \end{bmatrix} \pmod{26}.$$

Next, we compute $B = I + \overrightarrow{\mathrm{u}}\,\overrightarrow{\mathrm{v}}^T$, which yields:

$$B \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 18 & 10 & 11 & 19 \\ 6 & 12 & 21 & 15 \\ 2 & 4 & 7 & 5 \\ 6 & 12 & 21 & 15 \end{bmatrix} \equiv \begin{bmatrix} 19 & 10 & 11 & 19 \\ 6 & 13 & 21 & 15 \\ 2 & 4 & 8 & 5 \\ 6 & 12 & 21 & 16 \end{bmatrix} \pmod{26}$$

where $|B| = 1$.

Step 3
Find $B^{-1} = I_n - \overrightarrow{\mathrm{u}}\,\overrightarrow{\mathrm{v}}^T$ as follows:

$$B^{-1} \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} 18 & 10 & 11 & 19 \\ 6 & 12 & 21 & 15 \\ 2 & 4 & 7 & 5 \\ 6 & 12 & 21 & 15 \end{bmatrix} \equiv \begin{bmatrix} 9 & 16 & 15 & 7 \\ 20 & 15 & 5 & 11 \\ 24 & 22 & 20 & 21 \\ 20 & 14 & 5 & 12 \end{bmatrix} \pmod{26}.$$

Step 4

Since we have obtained that $|B| = 1$, then $\lambda = \pm 1$ yields $D \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 25 & 0 & 0 \\ 0 & 0 & 25 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \pmod{26}$.

Evaluate an eigenmatrix which is self-invertible as follows:

$$A \equiv BDB^{-1} \equiv \begin{bmatrix} 15 & 0 & 4 & 0 \\ 2 & 3 & 20 & 22 \\ 22 & 0 & 11 & 0 \\ 2 & 2 & 20 & 23 \end{bmatrix} \pmod{26}.$$

4 THE EFFECT OF SELF-INVERTIBLE MATRIX ON CIPHER POLYGRAPHIC POLYFUNCTION

In this section, the implementation of a self-invertible matrix of $A_{i\times i}$ will be discussed which has been generated in Section 3 on Cipher Polygraphic Polyfunction system (refer to Theorem 1). This system considers a self-invertible $A_{i\times i} \pmod N$ as a decryption key. The following example is to show the process of encryption and decryption.

Example 3. Consider "ACCOUNTABILITIES" as plaintext and rewrite its corresponding numbers as $P_{4\times4} \equiv \begin{bmatrix} 0 & 2 & 2 & 14 \\ 20 & 13 & 19 & 0 \\ 1 & 8 & 11 & 8 \\ 19 & 8 & 4 & 18 \end{bmatrix} \pmod{26}$. We choose the self-invertible matrix generated in Example 2 as the secret key. Since $(|A_{4\times4}|, 26) = 1$, then $P_{4\times4}$ has a unique solution. The encryption process of $P_{4\times4}$ to $C^{(3)}_{4\times4}$ is shown as follows:
The first transformation encryption of $P_{4\times4}$ to $C^{(1)}_{4\times4}$ is given by

$$C^{(1)}_{4\times4} \equiv A_{4\times4}P_{4\times4} \equiv \begin{bmatrix} 15 & 0 & 4 & 0 \\ 2 & 3 & 20 & 22 \\ 22 & 0 & 11 & 0 \\ 2 & 2 & 20 & 23 \end{bmatrix} \begin{bmatrix} 0 & 2 & 2 & 14 \\ 20 & 13 & 19 & 0 \\ 1 & 8 & 11 & 8 \\ 19 & 8 & 4 & 18 \end{bmatrix} \equiv \begin{bmatrix} 4 & 10 & 22 & 8 \\ 4 & 15 & 5 & 12 \\ 11 & 2 & 9 & 6 \\ 3 & 10 & 16 & 4 \end{bmatrix} \pmod{26}.$$

The second transformation encryption of $C^{(1)}_{4\times4}$ to $C^{(2)}_{4\times4}$ is

$$C^{(2)}_{4\times4} \equiv A_{4\times4}C^{(1)}_{4\times4} \equiv \begin{bmatrix} 15 & 0 & 4 & 0 \\ 2 & 3 & 20 & 22 \\ 22 & 0 & 11 & 0 \\ 2 & 2 & 20 & 23 \end{bmatrix} \begin{bmatrix} 4 & 10 & 22 & 8 \\ 4 & 15 & 5 & 12 \\ 11 & 2 & 9 & 6 \\ 3 & 10 & 16 & 4 \end{bmatrix} \equiv \begin{bmatrix} 0 & 2 & 2 & 14 \\ 20 & 13 & 19 & 0 \\ 1 & 8 & 11 & 8 \\ 19 & 8 & 4 & 18 \end{bmatrix} \pmod{26}.$$

The third transformation encryption of $C^{(2)}_{4\times4}$ to $C^{(3)}_{4\times4}$ is

$$C^{(3)}_{4\times4} \equiv A_{4\times4}C^{(2)}_{4\times4} \equiv \begin{bmatrix} 15 & 0 & 4 & 0 \\ 2 & 3 & 20 & 22 \\ 22 & 0 & 11 & 0 \\ 2 & 2 & 20 & 23 \end{bmatrix} \begin{bmatrix} 0 & 2 & 2 & 14 \\ 20 & 13 & 19 & 0 \\ 1 & 8 & 11 & 8 \\ 19 & 8 & 4 & 18 \end{bmatrix} \equiv \begin{bmatrix} 4 & 10 & 22 & 8 \\ 4 & 15 & 5 & 12 \\ 11 & 2 & 9 & 6 \\ 3 & 10 & 16 & 4 \end{bmatrix} \pmod{26}.$$

Hence, the secret message we acquired through this encryption process is "EKWIEPFMLCJG DKQE".

For the decryption process, we focus on obtaining back the original plaintext that is "ACCOUNTABILITIES". First and foremost, we need the inverse of secret key $A_{4\times4}$, which is $A^{-1}_{4\times4}$, to undergo the process of decryption. The decryption key will remain the same as the encryption key due to the secret key is self-invertible.
The first transformation decryption of $C^{(3)}_{4\times4}$ to $C^{(2)}_{4\times4}$ is given by

$$C^{(2)}_{4\times4} \equiv A_{4\times4}C^{(3)}_{4\times4} \equiv \begin{bmatrix} 15 & 0 & 4 & 0 \\ 2 & 3 & 20 & 22 \\ 22 & 0 & 11 & 0 \\ 2 & 2 & 20 & 23 \end{bmatrix} \begin{bmatrix} 4 & 10 & 22 & 8 \\ 4 & 15 & 5 & 12 \\ 11 & 2 & 9 & 6 \\ 3 & 10 & 16 & 4 \end{bmatrix} \equiv \begin{bmatrix} 0 & 2 & 2 & 14 \\ 20 & 13 & 19 & 0 \\ 1 & 8 & 11 & 8 \\ 19 & 8 & 4 & 18 \end{bmatrix} \pmod{26}.$$

The second transformation decryption of $C_{4\times4}^{(2)}$ to $C_{4\times4}^{(1)}$ is given by

$$C_{4\times4}^{(1)} \equiv A_{4\times4}C_{4\times4}^{(2)} \equiv \begin{bmatrix} 15 & 0 & 4 & 0 \\ 2 & 3 & 20 & 22 \\ 22 & 0 & 11 & 0 \\ 2 & 2 & 20 & 23 \end{bmatrix} \begin{bmatrix} 0 & 2 & 2 & 14 \\ 20 & 13 & 19 & 0 \\ 1 & 8 & 11 & 8 \\ 19 & 8 & 4 & 18 \end{bmatrix} \equiv \begin{bmatrix} 4 & 10 & 22 & 8 \\ 4 & 15 & 5 & 12 \\ 11 & 2 & 9 & 6 \\ 3 & 10 & 16 & 4 \end{bmatrix} \pmod{26}.$$

The third transformation decryption of $C_{4\times4}^{(1)}$ to $P_{4\times4}$ is

$$P_{4\times4} \equiv A_{4\times4}C_{4\times4}^{(1)} \equiv \begin{bmatrix} 15 & 0 & 4 & 0 \\ 2 & 3 & 20 & 22 \\ 22 & 0 & 11 & 0 \\ 2 & 2 & 20 & 23 \end{bmatrix} \begin{bmatrix} 4 & 10 & 22 & 8 \\ 4 & 15 & 5 & 12 \\ 11 & 2 & 9 & 6 \\ 3 & 10 & 16 & 4 \end{bmatrix} \equiv \begin{bmatrix} 0 & 2 & 2 & 14 \\ 20 & 13 & 19 & 0 \\ 1 & 8 & 11 & 8 \\ 19 & 8 & 4 & 18 \end{bmatrix} \pmod{26}.$$

Finally, we obtained the original plaintext after the decryption process.

In the encryption algorithm provided as an example, the outcome of the second transformation closely resembles the plaintext. On the other hand, the result obtained from the third transformation is identical to the first transformation. Generally, for $n \in \mathbb{Z}^+$, we obtain

$$C_{i\times j}^{2n} \equiv A_{i\times i}^{2n}P_{i\times j} \equiv (A_{i\times i}^{2})^{n}P_{i\times j} \equiv I^{n}P_{i\times j} \equiv P_{i\times j} \,(\text{mod } N) \tag{1}$$

whereas

$$C_{i\times j}^{2n+1} \equiv A_{i\times i}^{2n+1}P_{i\times j} \equiv A_{i\times i}(A_{i\times i}^{2})^{n}P_{i\times j} \equiv A_{i\times i}I^{n}P_{i\times j} \equiv A_{i\times i}P_{i\times j} \equiv C_{i\times j}^{(1)} \,(\text{mod } N). \tag{2}$$

Consequently, the outcome of odd-th and even-th transformations will generate the secret message and plaintext, respectively. In simpler terms, when the encryption key is self-invertible, the sender of the original message should transmit the message only up to the second transformation. With the specific property of the product of two column vectors u and v from the beginning of Algorithm 1, the third parties can analyze the ciphertext even though they do not know the decryption keys. To acquire the precise plaintext values, one must test a combination of u and v for a total of N^N times. Despite this, achieving such speed can be accomplished through the use of an appropriate algorithm and a high-performance computer.

5 CONCLUSION

In conclusion, we are able to find the self-invertible matrix based on IMIE using Algorithm 1. It was also successfully implemented into the Cipher Polygraphic Polyfunction cryptosystem. Upon observing the use of a self-invertible key during the even-th transformation, we found that the system became vulnerable to attacks by adversaries, leading to a recurrence outcome. Unfortunately, it is unnecessary to encrypt the original message through odd-th transformations, as this process will only get back the original one. Since the self-invertible key is suitable for use as it reduces the complexity for finding the encryption key, our study can further expand using different self-invertible keys for each transformation.

REFERENCES

[1] L. S. Hill, "Cryptography in an algebraic alphabet," *The American Mathematical Monthly*, vol. 36, no. 6, pp. 306–312, 1929. [Online]. Available: https://doi.org/10.1080/00029890.1929.11986963

[2] J. Overbey, W. Traves, and J. Wojdylo, "On the keyspace of the hill cipher," *Cryptologia*, vol. 29, no. 1, pp. 59–72, 2005.

[3] C. Christensen, "Cryptography of the vigenère cipher," in *Proceedings of Computer Sciences Corporation*, 2006, pp. 1–18.

[4] R. Bronson and G. B. Costa, *Linear algebra: An introduction*. Academic Press, 2007.

[5] R. A. Mollin, *An introduction to cryptography*. Chapman and Hall/CRC, 2006.

[6] B. Acharya, G. Rath, S. Patra, and S. K. Panigrahy, "Novel methods of generating self-invertible matrix for hill cipher algorithm," *International Journal of Security*, vol. 1, no. 1, pp. 14–21, 2007.

[7] S. K. Panigrahy, B. Acharya, and D. Jena, "Image encryption using self-invertible key matrix of hill cipher algorithm," in *Proceedings of the 1st International Conference on Advances in Computing*, February 2008.

[8] B. Acharya, S. K. Patra, and G. Panda, "Involutory, permuted and reiterative key matrix generation methods for hill cipher system," *International Journal of Recent Trends in Engineering*, vol. 1, no. 4, p. 106, 2009.

[9] B. Acharya, M. D. Sharma, S. Tiwari, and V. K. Minz, "Privacy protection of biometric traits using modified hill cipher with involutory key and robust cryptosystem," *Procedia Computer Science*, vol. 2, pp. 242–247, 2010. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050910003613

[10] S. Dey, "Sd-aei: An advanced encryption technique for images," in *2012 Second International Conference on Digital Information Processing and Communications (ICDIPC)*. IEEE, 2012, pp. 68–73.

[11] S. Naveenkumar, H. Panduranga *et al.*, "Partial image encryption for smart camera," in *Proceedings of the 2013 IEEE International Conference on Recent Trends in Information Technology (ICRTIT)*, 2013, pp. 126–132.

[12] F. Yunos, S. Ling, and M. R. Md Said, "Effect of self invertible matrix on cipher tetragraphic trifunction," in *Proceeding of the 25th National Symposium On Mathematical Science (SKSM25)*, June 2018.

[13] P. C. Sally Lin and F. Yunos, "Effect of self-invertible matrix on cipher hexagraphic polyfunction," *Cryptography*, vol. 3, no. 2, 2019. [Online]. Available: https://www.mdpi.com/2410-387X/3/2/15

[14] F. Yunos, A. Z. Kamalulzaman, M. S. Jamaludin, and W. Basri, "Solution of $l^2 = a$ matrix to generate involutory matrices for cipher trigraphic polyfunction," *Applied Mathematics and Computational Intelligence*, vol. 12, no. 1, pp. 1–17, 2023.

[15] F. Yunos and M. N. A. Buhari, "Gabungan kriptografi lengkuk eliptik dan saifer hill dalam perutusan imej berskala samar," *Jurnal Asas Ilmu Matematik*, vol. 1, no. 4, pp. 68–81, 2022.

[16] A. Neamah and A. Shukur, "A novel conservative chaotic system involved in hyperbolic functions and its application to design an efficient colour image encryption scheme," *Symmetry*, vol. 15, no. 1511, pp. 1–22, 2023.

[17] O. G. Abood and S. K. Guirguis, "A survey on cryptography algorithms," *International Journal of Scientific and Research Publications*, vol. 8, no. 7, pp. 495–516, 2018.

[18] D. R. Clark, "Crypto corner," https://crypto.interactive-maths.com/glossary.html/, 2019.

[19] W. R.S., "The centro-invertible matrix: A new type of matrix arising in pseudo-random number generation," *Journal of Linear Algebra and its Applications*, vol. 434, no. 1, pp. 144–151, 2011.

[20] C. Towse and E. Campbell, "Constructing integer matrices with integer eigenvalues," *Applied Probability Trust*, pp. 1–8, 2016.

[21] J. Ortega, "Generation of test matrices by similarity transformations," *Communications of the ACM*, vol. 7, no. 6, pp. 377–378, 1964.

[22] Q. Kong, T. Siauw, and A. Bayen, *Python Programming and Numerical Methods: A Guide for Engineers and Scientists*. Academic Press, 2020.

APPENDIX

In this section, we recall three methods for generating a self-invertible matrix A that was presented in [6] as follows:

Let $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1i} \\ a_{21} & a_{22} & \cdots & a_{2i} \\ \vdots & \vdots & \vdots & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ii} \end{bmatrix}$ be an $i \times i$ matrix partitioned to $A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$. For i an even, A_{11}, A_{12}, A_{21} and A_{22} are matrices with order $\frac{i}{2} \times \frac{i}{2}$. This can be simplified to the solution $A = \begin{bmatrix} A_{11} & k(I - A_{11}) \\ \frac{1}{k}(I - A_{11}) & -A_{11} \end{bmatrix}$ where $k \in \mathbb{Z}$ and $(k,\, N) = 1$. We name this kind of method as Type 1.

They also proposed another method for generating A for any i, but considered A_{11} as $[a_{11}]$ is a 1×1 matrix, $A_{12} = \begin{bmatrix} a_{12} & a_{13} & \cdots & a_{1i} \end{bmatrix}$ is a $1 \times (i-1)$ matrix, $A_{21} = \begin{bmatrix} a_{21} \\ a_{31} \\ \cdots \\ a_{i1} \end{bmatrix}$ is a $(i-1) \times 1$ matrix, $A_{22} = \begin{bmatrix} a_{22} & a_{23} & \cdots & a_{2i} \\ a_{32} & a_{33} & \cdots & a_{3i} \\ \cdots & \cdots & \cdots & \cdots \\ a_{i2} & a_{i3} & \cdots & a_{ii} \end{bmatrix}$ is a $(i-1) \times (i-1)$ matrix.

Since A is self-invertible, it satisfies $A^2 = I$. Therefore

$$A_{12}A_{21} = 1 - A_{11}^2 = 1 - a_{11}^2, \tag{3}$$

and

$$A_{12}(a_{11}I + A_{22}) = 0. \tag{4}$$

Also, $a_{11} = -$(one of the eigenvalues of A_{22} other than 1). Since $A_{21}A_{12}$ is a singular matrix having the rank 1 and

$$A_{21}A_{12} = I - A_{22}^2, \tag{5}$$

then A_{22} must have eigenvalues ± 1. It can also be proved that the consistent solution obtained for matrix A_{21} and A_{12} by solving (5) term by term will also satisfy (3). General steps for generating A are given as follows:

Algorithm 2.

1. *Select A_{22}, a non-singular $(i-1)\times(i-1)$ matrix which has $(i-2)$ number of eigenvalue of either $+1$ or -1 or both. The method for calculating an eigenvalue from $|\lambda I - A_{22}| = 0$ can be referred to in [22].*

2. *Determine the other eigenvalue λ of A_{22}.*

3. Set $a_{11} = -\lambda$.

4. Obtain the consistent solution of all elements of A_{21} *and* A_{12} *by using (5).*

5. Formulate the matrix A.

We name this technique as Type 2.

The third method, namely Type 3, is represented as follows:

Let A and B be invertible matrices such that $A = BDB^{-1}$, in which D is a diagonal matrix where the diagonal elements consist of eigenvalues. If $D = \begin{bmatrix} \lambda_1 & 0 & 0 & 0 & . & . & 0 \\ 0 & \lambda_2 & 0 & 0 & . & . & 0 \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & . & . & \lambda_i \end{bmatrix}$ with eigenvalues $\lambda_i = \pm 1$ then $D = D^{-1}$, subsequently A is self-invertible.