Advanced hill cipher algorithm for security image data with the involutory key matrix

Supiyanto¹ and S A Mandowen¹

¹Department of Mathematics and Science, Cenderawasih University, Jayapura, Indonesia
supi6976@gmail.com, kandera.awin@gmail.com (corresponding author)

Abstract. The security of important and confidential data is a top priority. Therefore, it is necessary to secure appropriate data to ensure confidentiality. Secrecy of data security can be done by randomizing the data in order to make the data is difficult to understand by anyone. One of the data security techniques that can be used is Advanced Hill Cipher cryptography. The purpose of this research was to create an application or software used to secure an image's data by applying the Advanced Hill Cipher algorithm. A classic cryptographic technique, which use a matrix as a key in the process of encrypting and decrypting data with the type of key used is the symmetric key type. The data used in this study was an image data, while the application development used the language of MATLAB Programming. The method used in this study was the Advanced Hill Cipher Cryptographic Algorithm. Basically the Advanced Hill Cipher Cryptography algorithm is much more like the Hill Cipher algorithm. However, on Advanced Hill Cipher, algorithms are developed using a key matrix that always has inverse; so that the disadvantages of the hill cipher algorithm are that the key matrix does not always have inverse resolved. In this research, the key matrix used is a 2x2 order involutory matrix with integer elements. The output of this study is an application that can be used to encrypting and decrypting grayscale and color image data with key matrix that always have inverse.

1. Introduction

Cryptography is an art or science that includes principles and methods to change plaintext into ciphertext and then transform the message back into its original form [1]. The purpose of cryptography is to maintain the confidentiality of information contained in the data so that the information cannot be known by unauthorized parties.

Digital image as one form of digital data is currently many used for storing photos, images, or works in digital format. When the data is confidential and its security is not guaranteed, it is feared that the data can fall to unwanted parties, which are then misused for negative things. One way to overcome this problem is to encode the image so that the image becomes scrambled form, and when falling into unwanted hands, these images cannot be used [2].

As with any text messages in keeping confidential messages, the image is also requires encryption techniques as much as possible simple but difficult to solve. The process of securing the messages in the form of images can be done by encrypting images into the image form again using certain algorithms. Therefore the development of cryptographic methods needs to expanded use not only limited to the encoding of text, but also images [3], audio and video [4].
In this study the advanced hill cipher method will be implemented to encode an image. This is possible considering that an image can be represented in a matrix containing integers. The image used in this research is limited to an image with 24 bit bmp format and the key matrix used is the Involutory matrix. The purpose of using the Involutory matrix is to overcome the disadvantages of using a random key matrix in the encryption process, which allows it to not be able to return the message as before, because the key matrix cannot be reversed and also to reduce computational complexity when the process finds inverse of the matrix at the time of decryption.

2. Research Methods

2.1. Hill Cipher

Based on the type of the key used, cryptography Hill Cipher included in the Symmetric Algorithms. this is because hill cipher only uses one key for the process of encryption and decryption of messages. For the encryption process, this algorithm takes sequential m plaintext and each character is given a numerical value such as a = 0, b = 1, ..., z = 25, [5, 11]. For m = 2, the equation system can be described as follows:

\[
\begin{align*}
C_1 &= (K_{11}P_1 + K_{12}P_2) \mod 26 \\
C_2 &= (K_{21}P_1 + K_{22}P_2) \mod 26
\end{align*}
\]  

This case can be expressed in terms of column vectors and matrices:

\[
\begin{pmatrix}
C_1 \\
C_2
\end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} \\
K_{21} & K_{22} \end{pmatrix} \begin{pmatrix} P_1 \\
P_2 \end{pmatrix} \mod 26
\]  

or simply we can write as \(C = KP\), where \(C\) and \(P\) are column vectors of length 2, representing the plaintext and ciphertext respectively, and \(K\) is a key matrix \(2 \times 2\). Therefore, when the decryption process requires the matrix inverse of the matrix \(K\). The inverse matrix \(K^{-1}\) is defined by the equation \(K.K^{-1} = K^{-1}.K = I\), where \(I\) is the identity matrix [6, 7]. In general process encryption and decryption we can write as follows:

For encryption:

\[
C = E_K(P) = PK
\]  

For decryption:

\[
P = D_K(C) = K^{-1}C = K^{-1}KP = P
\]  

2.2. Modular Arithmetic

The arithmetic operation presented here are addition, subtraction, unary operation, multiplication and division [8]. Based on this, the self-invertible matrix for Hill cipher algorithm is generated. The congruence modulo operator has the following properties:

- \(a \equiv b \mod p\) if \(n(a - b)\)
- \((a \mod p) = (b \mod p) \Rightarrow a \equiv b \mod p\)
- \(a \equiv b \mod p \Rightarrow b \equiv a \mod p\)
- \(a \equiv b \mod p\) and \(b \equiv c \mod p \Rightarrow a \equiv c \mod p\)

Let \(Z_p = [0,1,\ldots,p - 1]\) the set of residues modulo \(p\). If modular arithmetic is performed within this set \(Z_p\), the following equations present the arithmetic operations:

- Addition
  \((a + b) \mod p = [(a \mod p) + (b \mod p)] \mod p\)
- Negation:
\[-a \mod p = p - (a \mod p)\]

- **Subtraction**
  \[(a - b) \mod p = [(a \mod p) - (b \mod p)] \mod p\]

- **Multiplication**
  \[(a \times b) \mod p = [(a \mod p) \times (b \mod p)] \mod p\]

- **Division**
  \[(a / b) \mod p = c \text{ when } a = (b \times c) \mod p\]

### 2.3. Involutory Matrix

An involutory matrix is a matrix that is its own inverse. That is, multiplication by matrix \(A\) is an involution if and only if \(A^2 = I\). Involutory matrices are all square roots of the identity matrix. This is simply a consequence of the fact that any nonsingular matrix multiplied by its inverse is the identity [9].

With take an example of Involutory matrix.

\[
A = \begin{bmatrix} 4 & -1 \\ 15 & -4 \end{bmatrix}
\]

Calculate

\[
A^2 = \begin{bmatrix} 4 & -1 \\ 15 & -4 \end{bmatrix} \times \begin{bmatrix} 4 & -1 \\ 15 & -4 \end{bmatrix} = \begin{bmatrix} 16 - 15 & -4 + 4 \\ 60 - 60 & -15 + 16 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}
\]

Therefore, we can see that \(A^2 = I\) which means \(A\) is **Involutory matrix**.

### 2.4. Image Encryption using Advanced Hill

Advanced Hill Cipher is a cipher technique which is an extension of Hill Cipher. Advanced Hill Cipher belong to the classical algorithm which is an encryption algorithm that existed before today's digital age. We tried to adopt a Hill cipher algorithm to encrypt grayscale and color images. For the grayscale image, the modulus will be 256 while for the color image, first decompose the color image into the component (R-G-B). Second, encrypt each component (R-G-B) separately by an algorithm. Finally, combine the encrypted components together to get an encrypted color image [10].

### 3. Advanced Hill Cipher Algorithm

The advanced hill cipher algorithm is described as follows:

#### 3.1. Image Encryption Algorithm

The following are steps on how to encrypt images using the advanced hill cipher algorithm:

- Determine involutory matrix of \(m \times m\) which will be a key matrix approved by the sender and recipient.
- Take the input image to be encrypted.
- If the input image is a color image, then transform it first into a grayscale image, as the scheme in Figure 1 [12].
Figure 1. Encryption Process Scheme of color image

- Take the color component value (in pixel) from the image then change its size to a row vector with a size \([1 \ldots m \times m]\).
- Share pixel values or images in blocks which if expressed in matrix form, the row size is as much as \(m\).
- Encrypt using the hill cipher key for each matrix of each color component using the following equation;

\[
\begin{pmatrix}
\varepsilon_1 \\
\varepsilon_2
\end{pmatrix} =
\begin{pmatrix}
K_{11} & K_{12} \\
K_{21} & K_{22}
\end{pmatrix}
\begin{pmatrix}
P_1 \\
P_2
\end{pmatrix}
\]

\(\mathbf{C} = \begin{pmatrix}
\varepsilon_1 \\
\varepsilon_2
\end{pmatrix}, \quad \mathbf{K} = \begin{pmatrix}
K_{11} & K_{12} \\
K_{21} & K_{22}
\end{pmatrix}, \quad \mathbf{P} = \begin{pmatrix}
P_1 \\
P_2
\end{pmatrix}\)

where \(\mathbf{P}\) = Plaintext; \(\mathbf{C}\) = Ciphertext, dan \(\mathbf{K}\) = The Key Matrix

- Change the size of the encrypted matrix to the original image.
- The encrypted matrix is returned as an intent value using color transformation to produce a new image that has been encoded.

3.2. Image Decryption Process

The following are steps on how to decrypt images using the advanced hill cipher algorithm

- Take the image to be decrypted.
- Use the key matrix agreed upon before to determine the inverse matrix that will be used to decrypt the image using the hill cipher method.
- Color transformation so that the RGB color component of the encoded image is separated as in the encryption process, as the scheme in Figure 2 [12].

Figure 2. Decryption Process Scheme of color image

- The decryption process uses the advanced hill cipher method, the process is the same as the step in the encryption process for each color matrix. The deciphering process is carried out using the following equation;

\[
D = D_k(C) = K^{-1}C = K^{-1}K_p
\]
The decrypted vector is returned as the color intensity value using color transformation. The decryption results will produce the same image as the original image if the application runs properly and correctly.

4. Results and Discussion
To test the Hill Cipher Advanced Algorithm with an involutory matrix as its key matrix is a cryptographic technique, the following encryption-decryption process will be tested from the Hill Cipher Algorithm above.

Security testing for encryption keys is done on several grayscale images and color images of various sizes with the type .JPG or .BMP. Histogram analysis is done to find out the difference between plain and cipher image. In order to accommodate the proposed concept, then when generating an advanced Hill Cipher key, the Involutory matrix is used with a 2 x 2 order with a positive integer element number.

4.1. Encryption Results
The test is carried out in 4 different types of images, the format and size using the same key, while the results can be seen visually in the following Figure 3.

Figure 3 indicates that the original image cannot be seen after the encryption process. Image encoding results show significant color randomness and color intensity changes, this indicates that the encryption process works well. The following are examples of a histogram of a color image. The results of the histogram analysis in Figure 4 and Figure 5 show visually that there is a significant difference between the image histogram before and after encryption. In the encrypted histogram it looks flat for each color intensity, this shows that the encryption algorithm used cannot provide any instructions for statistical attacks by cryptanalysts because there is no prominent intensity as seen in the original image histogram.
Color Image Histogram before encrypted.  

Color Image Histogram after encrypted.

4.a 4.b

4.c 4.d

4.e 4.f

Figure 4. Color image histogram before and after encryption from image 3.a

The following figures are example of a histograms of grayscale image.

5.a 5.b

Figure 5. Histogram of grayscale image before and after encrypted [image (3.b)]

4.2. Decryption Results

To find out the decryption algorithm used in this research runs well, the encrypted image will be decrypted again. The decryption process is expected to return the encrypted image to the original image. Based on the key type, Hill Cipher is included in symmetrical cryptography, so in the
decryption process of the encrypted image as in Figure 6. The key used in the decryption process is the same key in the encryption process.

![Decryption Result Image](image)

**Figure 6.** Results of the decryption process

Figure 6 shows that the image that has been encrypted can be returned like the original image. The decrypted image shows image distortion. However, this result shows that the decryption process works well.

5. **Conclusion**

Based on the discussion above:

- An involutory matrix with round elements can be used as a key matrix in Advanced Hill Cipher cryptography
- The image encoding process with Hill Cipher shows significant color randomness, this indicates that the encryption process works well.
- Decryption process with Advanced Hill Cipher technique from the encrypted image can be returned as the first image or original image even though the decrypted image has a distortion. Yet, the decryption process still works well.

**References**

[1] Bibhudendra A, Girija S R, Sarat K P, Saroj K P 2007 Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm *International Journal of Security* Vol 1 Issue 1 2007 pp. 14-21.

[2] Marta K 2017 Implementasi Algoritma Affine Cipher Pada Citra Menggunakan Binomial Newton Sebagai Matriks Kunci *Pelita Informatika Budi Darma* Vol XVI, Nomor: 1 Januari ISSN : 2301-9425

[3] Siang J J 2002 Implementasi Sand Hill untuk Penyandian Citra *Jurnal Informatika* vol 3 No.1

[4] Soplanitand Susani 2005 Digital Audio Encryption Using New Chaotic Substitution ImageEncryption (NCSIE) *Prosiding SNTI* 2005 ISSN: 1829-9156 vol 2 Nomor 1.

[5] Menezes A J, P C Van Oorschotand S A Van Stone 1996 *Handbook of Applied Cryptography* CRC press.
[6] Imai H, Hanaoka G, Shikata J, Otsuka A, and Nascimento A C 2002 Cryptography with Information Theoretic Security Information Theory Workshop 2002 Proceedings of the IEEE, 20-25 Oct 2002

[7] Overbey J, Traves W, and Wojdylo J 2005 On the keyspace of the Hill cipher Cryptologia, vol 29 No. 1:59-72.

[8] Bruce S 1996 Applied Cryptography 2nd edition, John Wiley & Sons

[9] Higham and Nichols 2008 Involutory Matrices Functions of Matrices : Theory and Computation Philadelphia PA: Society for Industrial and Applied Mathematics (SIAM), pp. 165–166

[10] Li S, and Zheng X 2002. On the Security of an Image Encryption Method.

[11] Stallings W 2005 Cryptography and Network Security 4th edition, Prentice Hall.

[12] Supiyanto 2015 Implementasi Hill Cipher Pada Citra Menggunakan Koefisien Binomial Sebagai Matriks Kunci, Seminar Nasional Informatika 2015 (Semnasif 2015) ISSN: 1979-2328 UPN ”Veteran” Yogyakarta, 14 November 2015