SPECTA Journal of Technology
E-ISSN : 2622-9099
P-ISSN : 2549-2713
Homepage jurnal: https://journal.itk.ac.id/index.php/sjt

Implementation of Elliptic Curve Cryptography Method in Digital Image Security in the Medical Image

Yanuar Bhakti Wira Tama[1*], Syamsul Mujahidin[2]

[1]Departement of Mathematics, Institut Teknologi Kalimantan, Balikpapan, Indonesia.
[2]Departement of Informatics, Institut Teknologi Kalimantan, Balikpapan, Indonesia.

*Corresponding email: *yanuar.bhakti@lecturer.itk.ac.id*

Received: 08/December/2024 Revised: 21/December/2024
Accepted: 29/December/2024 Published: 31/December/2024

To cite this article:
Tama, Y. B. W & Mujahidin, S. (2024). Implementation of Elliptic Curve Crytography Method in Digital Image Security in the Medical Image. *SPECTA Journal of Technology*, *8*(3), 233-241. **https://10.35718/specta.v8i3.1253**

Abstract

Digital security become increasingly important particularly in medical field as impact of patient privacy and the protection of patient data. This attempt for this research will be made to use elliptic curve cryptography to hide messages in the form of digital images using multiplication matrix modified hill chipper and count entropy and time encryption and decryption. The encryption process, which utilizes matrix multiplication, ensures that the images achieve near-ideal entropy values, close to 8, indicating a high degree of randomness and security. The result is entropy for encrypted image near 8 it means that randomness of image is quite random. Meanwhile for computational time encrypted and decrypted image for one block is around 400000 nano second for encrypt image and 1500000000 nano second for decrypt image.

Keywords: digital image, elliptic curve, entropy, medical image

1. Introduction

Digital security can be defined as a set of actions used to protect important data and information from threats or attacks that can damage, steal, or disrupt the continuity of a computer system or network. The purpose of digital security is to maintain the confidentiality, integrity, and availability of data and systems used. Digital security has become increasingly important in today's priority list. This is due to the increasing personal and professional activities conducted online, such as interacting on social media and communicating via email with colleagues. Digital security must be a top priority for financial institutions and other organizations to protect their data and systems from damaging and harmful attacks. One of the issues occurring in Indonesia related to digital security is data breaches that happen in governmental and private institutions. One type of leaked data is image data such as photos of ID cards, driving licenses, or photos that should be private.

In addition to the digital images mentioned earlier, digital image security in the medical field is also required. Forms of digital images in the medical field include MRI imaging, X-ray imaging, and CT-Scans, all of which use digital image technology to produce pictures of body organs and tissues for the purpose of diagnosis and patient monitoring. Digital images in the medical field need to be kept confidential because they concern patient privacy and the protection of patient data. An example of a digital image in the medical field can be seen in Figure 1.

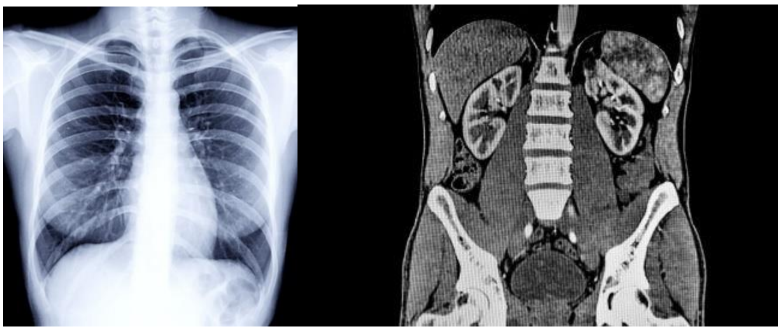


Figure 1: Example of Digital Medic Image

There are many methods can be used for digital image security. The main idea of this research based on combine hill chipper and elliptic curve cryptography (Dawahdeh et al., 2018) and cryptography in healthcare application (Mohan et al., 2016). One of the key concepts is utilizing elliptic curve cryptography, which is commonly employed for encrypting and decrypting text messages on the internet (Kumari & Kapoor, 2020), also there are encryption and decryption using matrix multiplication such that using double hill cipher with self-invertible key and random permutation of pixels locations (Lakhera et al., 2016), modification hill chipper using the logical XOR and shift operations (Paragas et al., 2019), combine hill chipper and RSA (Santoso, 2021), and modified hill chipper highly predictable and suffers from lack of sufficiently strong and complex intermediate operations along with Hill cipher (Vishwa Nageshwar & Ravi Shankar, 2021). Because in this research using image encryption to hiding information for digital image security, there are some research already done that using various ways such that Image Encryption by Novel Cryptosystem Using Matrix Transformation (Acharya et al., 2008), Image Encryption scheme with permutation (Jolfaei et al., 2016), image encryption using some various elliptic curve cryptography such that verification and digital signature (Singh & Singh, 2015), and image encryption using matrix semi-tensor product for multiplication (Zou et al., 2021).

This attempt for this research will be made to use elliptic curve cryptography to hide messages in the form of digital images using multiplication matrix modified hill chipper as sub matrix multiplication. This research is conducted as a foundation for the implementation of digital image security using elliptic curve cryptography. It is expected that this basic program can be developed towards digital images with more common colour scale such as RGB.

2. Study Literature

2.1. Hill Chipper and Matrix Multiplication

The Hill cipher is one of the polyalphabetic cryptosystems introduced by Lester Hill in 1929, which can be categorized as a block cipher (Forouzan, 2020). Hill cipher use matrix multiplication to encrypt and decrypt matrix with some matrix key K**.** The matrix multiplication operation that used in this research as follows: if matrix $B = [b_{i,j}]_{n\times n}$ is some key matrix and $A = [a_{i,j}]_{p\times q}$ is image matrix then n must divide p and q evenly. For the key matrix K of size $n \times n$, it will be used in the encryption of grayscale images with matrix size $p \times q$ where p and q are each divisible by n. The encryption matrix can then be formed as follows:

$$B_{n\times n} \odot A_{p\times q} := \begin{bmatrix} \begin{bmatrix} b_{1,1} & \cdots & b_{1,n} \\ \vdots & \vdots & \vdots \\ b_{n,1} & \cdots & b_{n,n} \end{bmatrix} \cdot \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \vdots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{bmatrix} & \cdots & \begin{bmatrix} b_{1,1} & \cdots & b_{1,n} \\ \vdots & \vdots & \vdots \\ b_{n,1} & \cdots & b_{n,n} \end{bmatrix} \cdot \begin{bmatrix} a_{1,q-n+1} & \cdots & a_{1,q} \\ \vdots & \vdots & \vdots \\ a_{n,q-n+1} & \cdots & a_{n,q} \end{bmatrix} \\ \vdots & \vdots & \vdots \\ \begin{bmatrix} b_{1,1} & \cdots & b_{1,n} \\ \vdots & \vdots & \vdots \\ b_{n,1} & \cdots & b_{n,n} \end{bmatrix} \cdot \begin{bmatrix} a_{p-n+1,1} & \cdots & a_{p-n+1,n} \\ \vdots & \vdots & \vdots \\ a_{p,1} & \cdots & a_{p,n} \end{bmatrix} & \cdots & \begin{bmatrix} b_{1,1} & \cdots & b_{1,n} \\ \vdots & \vdots & \vdots \\ b_{n,1} & \cdots & b_{n,n} \end{bmatrix} \cdot \begin{bmatrix} a_{p-n+1,q-n+1} & \cdots & a_{p-n+1,q} \\ \vdots & \vdots & \vdots \\ a_{p,q-n+1} & \cdots & a_{p,q} \end{bmatrix} \end{bmatrix} \quad (1)$$

As an example, consider matrix A of size 2×2 and matrix B of size 4×4. The product of their submatrix will be as follows:

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \odot \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 5 & 6 \end{bmatrix} & \begin{bmatrix} 1 & 2 \\ 5 & 6 \end{bmatrix} \cdot \begin{bmatrix} 3 & 4 \\ 7 & 8 \end{bmatrix} \\ \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 9 & 10 \\ 13 & 14 \end{bmatrix} & \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 11 & 12 \\ 15 & 16 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 7 & 10 & 15 & 22 \\ 23 & 34 & 31 & 46 \\ 39 & 58 & 47 & 70 \\ 55 & 82 & 63 & 94 \end{bmatrix}$$

Note that for the identity matrix I_n if it is operated with matrix A of size $p\times q$ then $I_n \odot A = A$ holds. Thus, if matrix D and E can be obtained such that $DE = I_n$, it means that matrix D and E are inverses of each other. From this, the encryption process of a matrix A with matrix key E can be described as follows:

$$encrpyt_K(A) = K \odot A \quad (2)$$

If the result of the encryption is matrix B, with matrix key $L = K^{-1}$, then the decryption of image process will be as follows:

$$decrypt_L(B) = L \odot B \quad (3)$$

For decryption, it can also be checked that $decrypt_L(B) = L \odot K \odot A = I_n \odot A = A,$ Thus, decryption will return the original matrix after encryption. Since the scope of this article only uses digital images in grayscale form, there needs to be a constraint in the calculations. In grayscale coloring, since the color of each block can be represented as a number between 0 and 255, the operations performed are modulo 256. Therefore, encryption and decryption in the equations (2) and (3) are also performed using modulo 256 operations.

2.2. *Elliptic Curve Cryptography*

Elliptic curve cryptography over the field $\mathbb{Z}_p$ with parameters a,b, and some prime number p not equal to 2 or 3 that satisfy $4a^3 + 27b^2 \neq 0 \ mod\ p$ (Stinson & Paterson, 2018) is defined by equation (3).

$$y^2 = x^3 + ax + b \ mod\ p \quad (4)$$

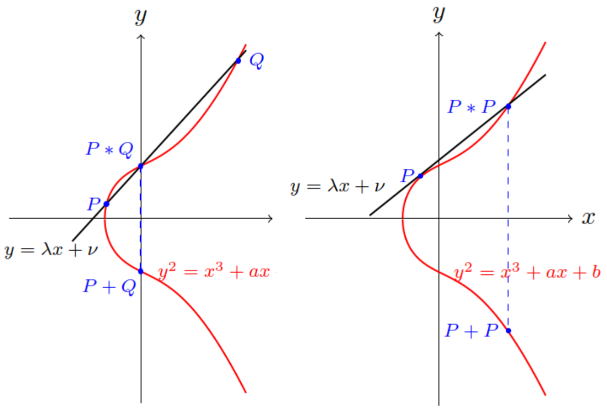


Figure 1: Point Addition (Left) and Doubling Operation (Right)

For additional point $P(x_1, y_1)$ and $Q(x_2, y_2)$ with $x_2 \neq x_1$ can be obtained $(P+Q)(x_3, y_3)$ with satisfy equation (5)-(7)

$$\mathcal{L} = (y_2 - y_1)(x_2 - x_1)^{-1} \; mod \; p \tag{5}$$
$$x_3 = \mathcal{L}^2 - x_1 - x_2 \; mod \; p \tag{6}$$
$$y_3 = \mathcal{L}(x_1 - x_3) - y_1 \; mod \; p \tag{7}$$

For doubling point $P(x_1, y_1)$ which is $2P(x_4, y_4)$ can be obtained with equation (8)-(10)

$$\mathcal{L} = (3x_1^2 + a)(2y_1)^{-1} \; mod \; p \tag{8}$$
$$x_3 = \mathcal{L}^2 - x_1 - x_1 \; mod \; p \tag{9}$$
$$y_3 = \mathcal{L}(x_1 - x_3) - y_1 \; mod \; p \tag{10}$$

Meanwhile, for scalar multiplication can be defined with equation (11) as below

$$nP = \underbrace{P + P + \cdots + P}_{n \; times} \tag{11}$$

For $n = 0$, defined $0P = O$. The operations from equations (5)-(11) will form a group with the identity point being the point O. Some publications regarding application elliptic curve cryptography can be found in (Abdelfatah, 2020; Alkhatib, 2020; Di Matteo et al., 2021; Muchtadi-Alamsyah et al., 2020; Tama & Fahmi, 2023)

2.3. Information Entropy

Information entropy is used to express randomness and can measure the distribution of gray values in the image (Su et al., 2017). The more uniform the distribution of pixel gray values, the greater the information entropy is. Information Entropy can be evaluated by calculating it first $\boldsymbol{p(x)}$ or proportion between number of pixels with value $\boldsymbol{x}$ and total number of pixels for every $\boldsymbol{x}$ with grayscale value from 0 to 255. Information Entropy equation defined in Equation 12

$$E = -\sum_{x=1}^{256} p(x) \times \log_2 p(x) \tag{12}$$

The ideal information entropy when every pixel has the same probability $p(x)$, for gray image with will get ideal information entropy when probability is uniform or $p(x) = \frac{1}{256}$. Then ideal information entropy would be 8. If the information entropy tends to near ideal information entropy it means that the distribution is random.

3. Methods

The method of this research to be used follows the following steps:

1. Determine Parameters:
   Begin by determining the parameters a, b, and p from the elliptic curve in Equation 4, and ensuring that the number of points obtained is 256.
2. Map Points to Grayscale:
   Once 256 points are obtained, map them to a scale of 0 to 255 based on grayscale colouring. The rule for mapping is from 0 to 255, with the points that satisfy Equation 4 ordered first by their smaller x-coordinate and then by their y-coordinate. Pixel with color tends to 0 for darker pixel, meanwhile pixel with color tends to 255 for lighter pixel as seen in Figure 2.

Submitted December 2024, Revised December 2024, Accepted December 2024, Published December 2024

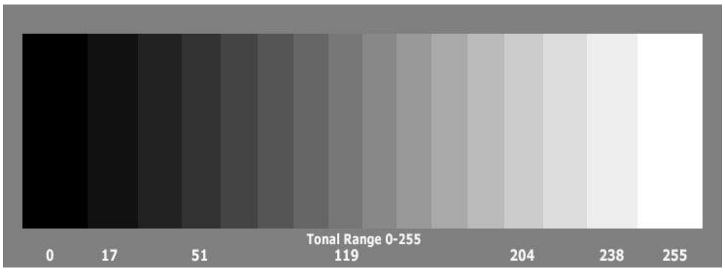


Figure 2: Scaling Grayscale Image

3. Represent Image Pixels:
   After mapping, represent each pixel in an image of size $m \times n$ as a coordinate on the elliptic curve.
4. Select Square Matrix:
   Choose a square matrix of size $p \times p$ such that p divides both m and n.
5. Matrix Multiplication for Encryption:
   Perform matrix multiplication as described in Equation 1 to encrypt and decrypt the image, using modulo 256 to ensure that the result entries are between 0 and 255.
6. Calculate Pixel Probabilities:
   After encryption, calculate the probability of each pixel value.
7. Compute Information Entropy:
   Calculate the information entropy and compare it to the ideal information entropy.
8. Measure Encryption/Decryption Time:
   Measure the time taken for image encryption and decryption.

For this research will be used three digital medical images with various dimension limited with even number to make it easier to select submatrices. Also, for choosing parameter $a, b,$ and p in Equation 1, choose only one combination.

4. Result and discussion

The data for this research using three sample data from Large Dataset of Labeled Optical Coherence Tomography (OCT) and Chest X-Ray Images (Kermany et al., 2018). For the computational purpose, all the computation using python in Google Collaboratory on personal computer with ~16GB RAM and 12th Gen Intel® Core™ i5-1240P (16 CPUs) Processor and Windows 11 is used in this research. First, to ensure that it is obtained 256 points based on the Equation 1, choose elliptic curve that define in Equation 13

$$y^2 = x^3 + 9x + 3 \; mod \; 239 \tag{13}$$

The point obtained from Equation 13 then mapping to number from 0 to 255 according to order of x-coordinate then y-coordinate. The sample point mapping to number can be seen in Table 1.

Table 1: Point Mapping to Number 0 to 255

Number	Point	Number	Point	Number	Point	Number	Point	Number	Point
0	O	6	(6,150)	12	(9,151)	⋮	⋮	250	(235,57)
1	(0,106)	7	(7,109)	13	(12,40)	⋮	⋮	251	(235,182)
2	(0,133)	8	(7,130)	14	(12,199)	⋮	⋮	252	(237,107)
3	(2,56)	9	(8,78)	15	(13,40)	⋮	⋮	253	(237,132)
4	(2,183)	10	(8,161)	16	(13,199)	⋮	⋮	254	(238,94)
5	(6,89)	11	(9,88)	17	(14,31)	⋮	⋮	255	(238,145)

After all numbers in pixel has been mapping to point in elliptic curve, prepare digital medical image that will be used in this research as seen in Figure 3.

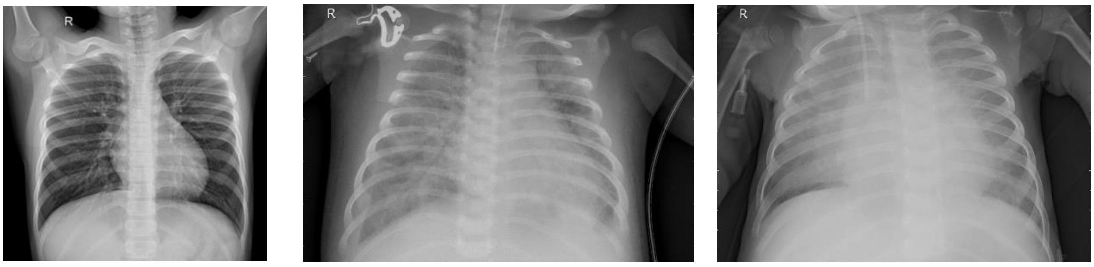


Figure 3: Example of Digital Image

Let's start with Figure 3 (Left), that medical image has $\mathbf{316 \times 328}$ dimensions with matrix of image can be seen below

$$\boldsymbol{A}=\begin{bmatrix} \mathbf{91} & \mathbf{96} & \cdots & \mathbf{171} & \mathbf{152}\\ \mathbf{92} & \mathbf{95} & \cdots & \mathbf{150} & \mathbf{101}\\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0}\\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0}\end{bmatrix}$$

Change entry of matrix A to point elliptic curve based on Table 1, the result can be seen below

$$\boldsymbol{A}=\begin{bmatrix} \mathbf{(80,32)} & \mathbf{(87,137)} & \cdots & \mathbf{(160,79)} & \mathbf{(141,211)}\\ \mathbf{(80,207)} & \mathbf{(87,102)} & \cdots & \mathbf{(140,161)} & \mathbf{(91,78)}\\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \boldsymbol{O} & \boldsymbol{O} & \cdots & \boldsymbol{O} & \boldsymbol{O}\\ \boldsymbol{O} & \boldsymbol{O} & \cdots & \boldsymbol{O} & \boldsymbol{O}\end{bmatrix}$$

Because matrix A has dimension $\mathbf{316 \times 328}$ then choose matrix B with size $\mathbf{2 \times 2}$ because $\mathbf{2}$ divide 316 and 328. Choose $\boldsymbol{B}=\begin{bmatrix}\mathbf{1} & \mathbf{3}\\ \mathbf{0} & \mathbf{7}\end{bmatrix}$ and doing multiplication to image encryption based on Equation 2 in modulo 256. There are some results of image encryption using scalar multiplication based on Equation (11) and addition or doubling multiplication based on Equation (5)-(10).

- $\begin{bmatrix}\mathbf{1} & \mathbf{3}\\ \mathbf{0} & \mathbf{7}\end{bmatrix}\cdot\begin{bmatrix}\mathbf{(80,32)} & \mathbf{(87,137)}\\ \mathbf{(80,207)} & \mathbf{(87,102)}\end{bmatrix}=\begin{bmatrix}\mathbf{(80,32)+3\cdot(80,207)} & \mathbf{(87,137)+3\cdot(87,102)}\\ \mathbf{7\cdot(80,207)} & \mathbf{7\cdot(87,102)}\end{bmatrix}=\begin{bmatrix}\mathbf{(109,91)} & \mathbf{(77,168)}\\ \mathbf{(153,158)} & \mathbf{(108,139)}\end{bmatrix}=\begin{bmatrix}\mathbf{119} & \mathbf{86}\\ \mathbf{164} & \mathbf{118}\end{bmatrix}$
- $\begin{bmatrix}\mathbf{1} & \mathbf{3}\\ \mathbf{0} & \mathbf{7}\end{bmatrix}\cdot\begin{bmatrix}\mathbf{(160,79)} & \mathbf{(141,211)}\\ \mathbf{(140,161)} & \mathbf{(91,78)}\end{bmatrix}=$ $\begin{bmatrix}\mathbf{(160,79)+3(140,161)} & \mathbf{(141,211)+3(91,78)}\\ \mathbf{7\cdot(140,161)} & \mathbf{7\cdot(91,78)}\end{bmatrix}=\begin{bmatrix}\mathbf{(157,153)} & \mathbf{(49,160)}\\ \mathbf{(96,158)} & \mathbf{(115,205)}\end{bmatrix}=\begin{bmatrix}\mathbf{170} & \mathbf{50}\\ \mathbf{106} & \mathbf{122}\end{bmatrix}$
- $\begin{bmatrix}\mathbf{1} & \mathbf{3}\\ \mathbf{0} & \mathbf{7}\end{bmatrix}\cdot\begin{bmatrix}\boldsymbol{O} & \boldsymbol{O}\\ \boldsymbol{O} & \boldsymbol{O}\end{bmatrix}=\begin{bmatrix}\boldsymbol{O+3O} & \boldsymbol{O+3O}\\ \boldsymbol{7\cdot O} & \boldsymbol{7\cdot O}\end{bmatrix}=\begin{bmatrix}\boldsymbol{O} & \boldsymbol{O}\\ \boldsymbol{O} & \boldsymbol{O}\end{bmatrix}=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$

For decrypt image using $\boldsymbol{B}^{-1}=\begin{bmatrix}\mathbf{1} & \mathbf{219}\\ \mathbf{0} & \mathbf{183}\end{bmatrix}$ because satisfy

$$\boldsymbol{B}\cdot\boldsymbol{B}^{-1}=\begin{bmatrix}\mathbf{1} & \mathbf{3}\\ \mathbf{0} & \mathbf{7}\end{bmatrix}\cdot\begin{bmatrix}\mathbf{1} & \mathbf{219}\\ \mathbf{0} & \mathbf{183}\end{bmatrix}\boldsymbol{mod}\ \mathbf{256}=\begin{bmatrix}\mathbf{1+0}\ \boldsymbol{mod}\ \mathbf{256} & \mathbf{219+3\cdot 183}\ \boldsymbol{mod}\ \mathbf{256}\\ \mathbf{0}\ \boldsymbol{mod}\ \mathbf{256} & \mathbf{7\cdot 183}\ \boldsymbol{mod}\ \mathbf{256}\end{bmatrix}=\begin{bmatrix}\mathbf{1} & \mathbf{0}\\ \mathbf{0} & \mathbf{1}\end{bmatrix}$$

There are some results of image encryption using scalar multiplication based on Equation (11) and addition or doubling multiplication based on Equation (5)-(10).

Submitted December 2024, Revised December 2024, Accepted December 2024, Published December 2024

- $\begin{bmatrix}1 & 219\\0 & 183\end{bmatrix}\cdot\begin{bmatrix}(109,91) & (77,168)\\(153,158) & (108,139)\end{bmatrix}=$
  $\begin{bmatrix}(109,91)+219\cdot(153,158) & (77,168)+219\cdot(108,139)\\183\cdot(153,158) & 183\cdot(108,139)\end{bmatrix}=\begin{bmatrix}(80,32) & (87,137)\\(80,207) & (87,102)\end{bmatrix}$
- $\begin{bmatrix}1 & 219\\0 & 183\end{bmatrix}\cdot\begin{bmatrix}(157,153) & (49,160)\\(96,158) & (115,205)\end{bmatrix}=$
  $\begin{bmatrix}(157,153)+219(96,158) & (49,160)+219(115,205)\\183\cdot(96,158) & 183\cdot(115,205)\end{bmatrix}=\begin{bmatrix}(160,79) & (141,211)\\(140,161) & (91,78)\end{bmatrix}$
- $\begin{bmatrix}1 & 219\\0 & 183\end{bmatrix}\cdot\begin{bmatrix}O & O\\O & O\end{bmatrix}=\begin{bmatrix}O+219O & O+219O\\183\cdot O & 183\cdot O\end{bmatrix}=\begin{bmatrix}O & O\\O & O\end{bmatrix}$

Result matrix for the last multiplication is $\begin{bmatrix}91 & 96\\92 & 95\end{bmatrix}$, $\begin{bmatrix}171 & 152\\150 & 101\end{bmatrix}$, and $\begin{bmatrix}O & O\\O & O\end{bmatrix}$ respectively. Then, result of image encryption and decryption compared to original image can be seen in Figure 4.

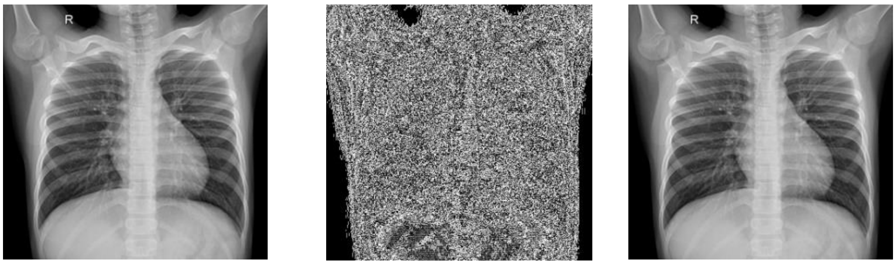


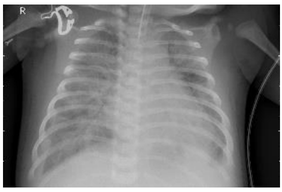
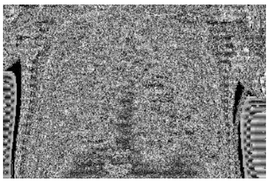
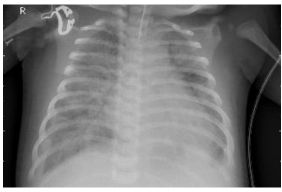
Figure 4: Original image (left) vs Encrypt Image (center) vs Decrypt Image (right)

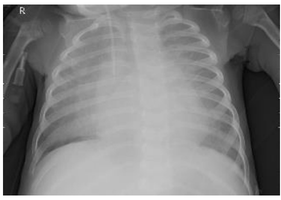
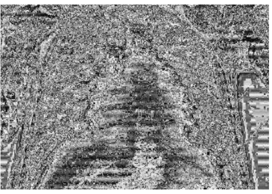
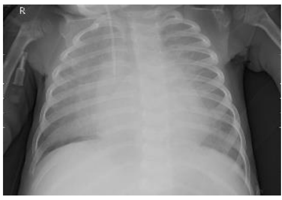
Based on Figure 4, there are no differences between original and decrypt image, so it can be said that this system can return encrypted image to original image. Meanwhile, the similarities between original and encrypt image located on the outside x-ray image where all blanks. After that compute the ideal information entropy. After find the distribution every value of pixel information entropy for encrypted image in Figure 4 can be found approximately 1.2715, it means that information entropy for this encrypted image is far from ideal this may be due to what was previously stated, namely that there are several block matrixes is blank also it means that the encrypted image not too random.

Moving on to computing time, time to encrypt image from original need 11567583011 nano second, for decrypting need 367249876675 nano second. It can be noted that the encryption time is faster than the decryption time, this can happen because entry of matrix is small number rather than its inverse, so there will be more scalar multiplication for decrypt rather than encrypt. Because the original matrix has dimension 316 · 328 then there will be 25912 submatrix operation, or the average of encrypt time would be approximately 446417 nano second and for decrypt would be approximately 14172965 nano second.

Result for the other two medical image in Figure 3 can be seen in Table 2

Table 2: Other Result for Different Image

No	Original Image	Size	Encrypt Image	Entropy	Decrypt Image	Computation Time
1		760 × 1152		7.8745		Encrypt: 96676256623 Decrypt: 3457232112689

2		816 × 1186		8.4631		Encrypt: 107987257447 Decrypt: 3678061961823

Based on Table 2, there are no differences between original and decrypt image, further strengthens the opinion that this system can return encrypted image to original image. The information entropy much higher than result from Figure 2. Compare each entropy to ideal information entropy. Because the information entropy for both images is near 8, it can be said that the distribution of encrypted images in both figures is random.

For computational time, time to encrypt first image from original need 96676256623 nano second, for decrypting need 3457232112689 nano second. As the same as before that the encryption time is faster than the decryption time. Because the original first image has dimension 760×1152 then there will be 218880 submatrix operation, or the average of encrypt time would be approximately 441686 nano second and for decrypt would be approximately 15795102 nano second. For the second image has dimension 816×1186 there will be 241944 submatrix operation. Average of encrypt time would be approximately 446331 nano second, meanwhile for decrypt time approximately 15202120 nano second.

Based on the three images that have been encrypted, it can be observed that the entropy values of the three images are quite close to 8, indicating that their distribution can be considered random. However, there is one image with a relatively low entropy value due to the presence of black blocks. It can also be seen that the results are random for the images without black blocks. Meanwhile, the average computation time for encryption and decryption is consistent, around 400000 nanoseconds for encryption and around 15000000 nanoseconds for decryption.

5. Conclusion

In conclusion, this research demonstrates the application of elliptic curve cryptography combined with a modified Hill cipher to enhance digital image security, particularly for medical images. By encrypting grayscale medical images and analyzing their entropy and computational performance, the study shows that the encrypted images exhibit randomness close to the ideal entropy value of 8, indicating effective encryption or it can be interpreted that encrypted images is quite random. Furthermore, the encryption process is computationally efficient, with faster encryption times compared to decryption with average computation time for one block encryption and decryption is consistent, around 400000 nanoseconds for encryption and around 15000000 nanoseconds for decryption. The findings suggest that elliptic curve cryptography provides a robust and efficient method for securing sensitive digital medical images. Based on image results, there are no differences between original image and decryption image it means that cryptosystem can hide or encrypt image and return it back to original image.

Acknowledgments
Thank you to Direktorat Riset, Teknologi, dan Pengabdian Kepada Masyarakat, Direktorat Jenderal Pendidikan Tinggi, Riset, dan Teknologi, Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia for providing research funding in 2024, enabling this research to be carried out successfully.

References

Abdelfatah, R. I. (2020). Secure Image Transmission Using Chaotic-Enhanced Elliptic Curve Cryptography. *IEEE Access, 8*, 3875–3890. https://doi.org/10.1109/ACCESS.2019.2958336

Acharya, B., Patra, S. K., & Panda, G. (2008). Image Encryption by Novel Cryptosystem Using Matrix Transformation. *2008 First International Conference on Emerging Trends in Engineering and Technology*, 77–81. https://doi.org/10.1109/ICETET.2008.110

Alkhatib, M. (2020). High-Speed and Secure Elliptic Curve Cryptosystem for Multimedia Applications ECC Elliptic Curve Cryptosystem RLA Right to Lift Algorithm SPA Simple Power Attack STA Simple Time Attack SM Sequential Multiplication SA Sequential Addition PM Parallel Multiplier TSM Time-consumption for one sequential multiplication TM Time-consumption for one multiplication operation TKP Time-consumption for scaler multiplication GF Galious Field NAF Non-Adjacent-Form. *IJACSA) International Journal of Advanced Computer Science and Applications*, *11*(9).

Dawahdeh, Z. E., Yaakob, S. N., & Razif bin Othman, R. (2018). A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher. *Journal of King Saud University - Computer and Information Sciences*, *30*(3), 349–355. https://doi.org/10.1016/j.jksuci.2017.06.004

Di Matteo, S., Baldanzi, L., Crocetti, L., Nannipieri, P., Fanucci, L., & Saponara, S. (2021). Secure elliptic curve crypto-processor for real-time iot applications. *Energies*, *14*(15). https://doi.org/10.3390/en14154676

Forouzan, B. A. (2020). *INTRODUCTION TO CRYPTOGRAPHY AND NETWORK SECURITY* (1st ed.). McGraw-Hill.

Jolfaei, A., Wu, X.-W., & Muthukkumarasamy, V. (2016). On the Security of Permutation-Only Image Encryption Schemes. *IEEE Transactions on Information Forensics and Security*, *11*(2), 235–246. https://doi.org/10.1109/TIFS.2015.2489178

Kermany, D. S., Goldbaum, M., Cai, W., Valentim, C. C. S., Liang, H., Baxter, S. L., McKeown, A., Yang, G., Wu, X., Yan, F., Dong, J., Prasadha, M. K., Pei, J., Ting, M. Y. L., Zhu, J., Li, C., Hewett, S., Dong, J., Ziyar, I., … Zhang, K. (2018). Identifying Medical Diagnoses and Treatable Diseases by Image-Based Deep Learning. *Cell*, *172*(5), 1122-1131.e9. https://doi.org/10.1016/j.cell.2018.02.010

Kumari, A., & Kapoor, V. (2020). Competing secure text encryption in intranet using elliptic curve cryptography. *Journal of Discrete Mathematical Sciences and Cryptography*, *23*(2), 631–641. https://doi.org/10.1080/09720529.2020.1729509

Lakhera, M., Rauthan, M. M. S., & Agarwal, A. (2016). Securing biometric template using double hill cipher with self-invertible key and random permutation of pixels locations. *2016 2nd International Conference on Next Generation Computing Technologies (NGCT)*, 814–817. https://doi.org/10.1109/NGCT.2016.7877522

Mohan, M., Kavithadevi, M. K., & Jeevan Prakash, V. (2016). Improved Classical Cipher for Healthcare Applications. *Procedia Computer Science*, *93*, 742–750. https://doi.org/10.1016/j.procs.2016.07.285

Muchtadi-Alamsyah, I., Bhakti, Y., & Tama, W. (2020). Implementation of Elliptic Curve25519 in Cryptography. In *Theorizing STEM Education in the 21st Century* (p. 189). www.intechopen.com

Paragas, J. R., Sison, A. M., & Medina, R. P. (2019). Hill Cipher Modification: A Simplified Approach. *2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*, 821–825. https://doi.org/10.1109/ICCSN.2019.8905360

Santoso, Y. S. (2021). Message Security Using a Combination of Hill Cipher and RSA Algorithms. *Jurnal Matematika Dan Ilmu Pengetahuan Alam LLDikti Wilayah 1 (JUMPA)*, *1*(1), 20–28. https://doi.org/10.54076/jumpa.v1i1.38

Singh, L. D., & Singh, K. M. (2015). Image Encryption using Elliptic Curve Cryptography. *Procedia Computer Science*, *54*, 472–481. https://doi.org/10.1016/j.procs.2015.06.054

Stinson, D. R., & Paterson, M. B. (2018). *Cryptography*. Chapman and Hall/CRC. https://doi.org/10.1201/9781315282497

Su, X., Li, W., & Hu, H. (2017). Cryptanalysis of a chaos-based image encryption scheme combining DNA coding and entropy. *Multimedia Tools and Applications*, *76*(12), 14021–14033. https://doi.org/10.1007/s11042-016-3800-9

Tama, Y. B. W., & Fahmi, M. F. (2023). Sistem Kriptografi Klasik Dengan Memanfaatkan Orde Dari Grup Titik Pada Kurva Eliptik Bentuk Montgomery. *Euler : Jurnal Ilmiah Matematika, Sains Dan Teknologi*, *11*(2), 361–371. https://doi.org/10.37905/euler.v11i2.23009

Vishwa Nageshwar, K., & Ravi Shankar, N. (2021). *Cryptanalysis of Modification in Hill Cipher for Cryptographic Application* (pp. 659–666). https://doi.org/10.1007/978-981-15-5243-4_62

Zou, C., Wang, X., & Li, H. (2021). Image encryption algorithm with matrix semi-tensor product. *Nonlinear Dynamics*, *105*(1), 859–876. https://doi.org/10.1007/s11071-021-06542-9