EMITTER International Journal of Engineering Technology
ISSN: 2443-1168, Vol. 7, No. 2, December 2019, pp. 524~536
DOI : 10.24003/emitter.v7i2.405

Medical Image Encryption Using Modified Identity Based Encryption

Dian Neipa Purnamasari*, Amang Sudarsono, Prima Kristalina****

*Informatics Engineering Department, University of Trunojoyo Madura
**Electrical Engineering Department, Politeknik Elektronika Negeri Surabaya
E-mail: dneipa12@gmail.com, {amang,prima}@pens.ac.id

Received May 29, 2019; Revised June 14, 2019; Accepted August 30, 2019

Abstract

The development of technology and communication also affects the level of security needed for digital image transmission. It is known that digital images now have important meanings in both communication and video conference. In this paper, we propose a security method for medical encryption in the form of images. The proposed method is implemented in the modified Identity-Based Encryption scheme. The encryption algorithm used is Elliptic Curve Cryptography (ECC) to generate key pairs and the Advanced Encryption Standard (AES) to generate symmetric keys and encrypt process. This method has been tested based on computation time, histogram analysis and statistical analysis. The results of the test were obtained that the proposed method was resistant to statistical attacks despite having slower computing time. The proposed method has a higher entropy value and is able to make pixels in the ciper image evenly distributed than the comparison method.

Keywords: Image Encryption, Identity Based Encryption, ECC, AES.

1. INTRODUCTION

Image is one way to present information data. The purpose of presenting data in the form of images is so that readers can more easily understand the information to be conveyed. One of the information data that uses the form of images is medical data such as electrocardiogram, echocardiography, and others. The importance of healthcare data requires us to be able to protect and restrict user access. This is because nowadays it is the Internet era where everyone can access information data both legally and illegally.

In 1996, Schneider [1] stated that cryptography is both a science and an art that is used to maintain message security. Security is done using the encryption and decryption method. Encryption algorithms that can be used to maintain image security include Rijndael, Serpent, Twofish, MARS, RC6, MRC6, RSA (Rivest, Shamir, Adleman), and others [2]. The message used in the encryption method can be text, file, or image. In the research of L. D. Singh et al. [3], proposed a medical image security method using the improved ElGamal encryption technique. This method is designed to encrypt medical images by solving problems of data expansion and computational time. The results show that the proposed method has the characteristics of a strong cipher image and good computing speed.

In cryptography, several researchers have conducted research on security in images using symmetric algorithms such as DES (Data Encryption Standard) and AES (Advanced Encryption Standard) [4]–[7]. While others using asymmetric algorithms are [8]–[13]. The lack of each algorithm resulted in researchers starting to switch to hybrid schemes. In the research of T. Shahriyar et al. [14], the authors proposed image encryption using the advantages of Elliptic Curve Cryptography (ECC) and AES. The ECC algorithm is used as a random generator based on ECC parameters. While the AES algorithm is used to generate stream keys for image encryption. Acquired results that the proposed method meets the basics of cryptography. This research has divided the image into three basic colors such as red, green and blue. Each color is converted into data matrix masked by a primary key. Primary keys are obtained from a random number generator. The combination of each basic color will create a cipher image.

In this work, we propose image encryption using a modified IBE scheme. In this scheme, we use the ECC and AES algorithms to improve security levels. The ECC algorithm is used to generate key pairs of combinations between embedded identities and ECC parameters. The complexity of elliptic curve calculations can be used to avoid cipher analysis attacks and cover up AES deficiencies in key management. While the AES algorithm is used to generate key streams and for the encryption and decryption process. The computational speed of the AES algorithm is faster than the asymmetric algorithm making it possible to get results quickly. The information data used in this study is in the form of medical data, which are graphs and CT scans.

This paper is organized as follows: section II presents a review of previous research regarding the algorithms used in image encryption. Section III presents a review of the authors' contributions and originality in the study. Section IV describes the review for the IBE, AES, ECC scheme used in the research and application of the proposed method. Section V discusses the proposed performance of the algorithm. The conclusion is summarized in section VI.

2. RELATED WORKS

There are several researchers who discuss image encryption using different algorithms using both symmetric algorithms and asymmetric algorithms.

Research [5] proposed a security method for images based on AES expansion keys. The encryption process is carried out using operations from a set of pixel images with 128-bit keys that always change each set of pixels. This method can generate keys independently. The results show that the proposed method can handle Brute Force attacks, statistical analysis, and key sensitivity tests.

Research [6] proposed a method for randomizing high-definition (HD) images using a modified AES algorithm. Authors improve AES performance by increasing security levels, reducing computing costs, and reducing hardware requirements. The results showed that the proposed method is more compatible with HD image encryption.

Research [7] proposed a method of improvement by combining clutter-based image encryption techniques with the improved DES algorithm. The work method of this method is that the system will do the encryption process twice by producing a pseudo-random sequence that can carry RGB values to disrupt the image, then do the second encryption with the DES algorithm that has been upgraded. The results showed that the proposed method can be used in actual image encryption.

Research [9] describes a review of cryptography and a comparison between RSA, DES and Blowfish algorithms applied to grayscale images. The author uses the prime number values chosen by the P and Q parameters to reduce the key compilation time. The results showed that the time taken from the RSA calculation made the process faster implemented and the data used was safer compared to the DES and Blowfish algorithms.

Research [11] proposes a security method to transmit images with maximum confidentiality and authenticity. Authors use ECC to safeguard information securely and confidentially and generate key pairs. In the decryption process, the secret key generated from the ECC method will be optimized using the genetic algorithm (GA). The results showed that the proposed method had an optimal PSNR value compared to other methods.

Research [12] proposed a security method in images by applying elliptic curve cryptography to encrypt, decrypt, and digital signatures. The purpose of this research is to obtain a security method that can provide authenticity and integrity of images received. The author groups pixel values and maps their values to elliptic curve coordinates. This is done to ignore the use of mapping tables that are used as references for encryption and decryption. The results showed that the proposed method could produce a password image with a low correlation.

Research [14] proposes a security method in images that can produce random number sequences based on elliptic curves and use the AES algorithm to obtain keys. Hybrid schemes are chosen to provide encryption techniques that can meet the basics of cryptography such as simplicity and truth. The results showed that the proposed method was effective for improving the security level.

3. ORIGINALITY

We propose a security method to secure medical data in the form of graphics or images. Medical data used are breath wave images, echocardiography, and liver CT scan. The encryption and decryption process of our proposed method is implemented using the modified IBE scheme so that the process is based on a user identity such as a medical identity number. The algorithm used is an elliptic curve algorithm to generate key pairs and AES to produce symmetric keys and to do the decryption-encryption process. This method will be compared with research [14] which uses the ECC and AES algorithms for image encryption.

4. SYSTEM DESIGN

In this section, we describe a brief review of cryptographic introductions specifically Identity-based Encryption (IBE), ECC algorithms, AES algorithms, and explain the security methods proposed in this paper.

4.1 Identity-based Encryption (IBE)

IBE is an encryption technique that uses identity to produce unique key pairs. The key pair can be generated independently by the sender and receiver, so this technique can reduce the occurrence of key exchanges on the communication lines. Another advantage is that the identity used can be any string such as name, email, telephone number, etc. In general, IBE is a scheme that has 4 stages, namely Setup, Encrypt, Extract and Decrypt [15]. To be clearer, Figure 1 shows the whole process of the IBE scheme.

In the proposed method, we modify the Setup and Extract stages to become the Key Generator stage. This is because the two stages work in the Public Key Generator (PKG) so that they can be combined to speed up computing time. When users want to communicate with each other the Key Generator will produce a secret key that can be used for encryption and decryption.

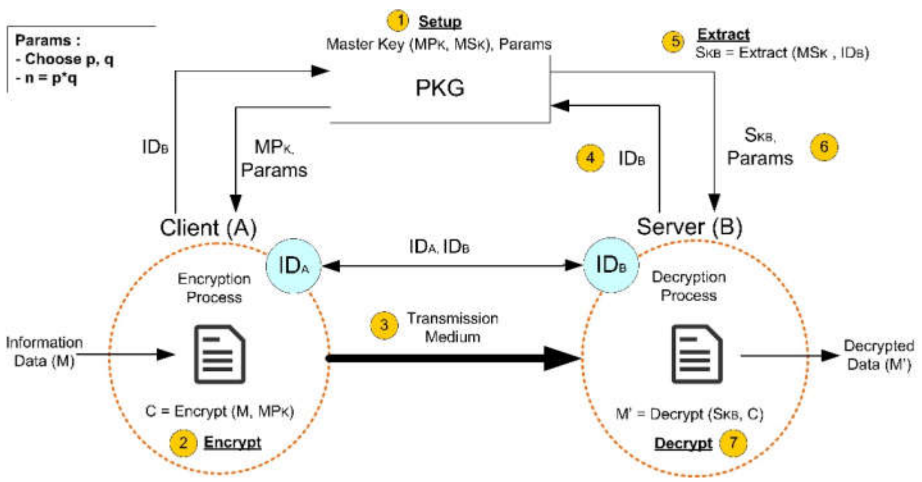

Figure 1. Identity-based Encryption Scheme [15]

4.2 Elliptic Curve Cryptography (ECC)

ECC is one of the asymmetric key cryptography used for the implementation of public key cryptography. The strength of this algorithm is in the calculation of the elliptic curve which does not have subexponential time to solve the mathematical problem of the elliptic curve logarithm so that the resulting key pair has a high level of security even with a shorter key length. The elliptic curve equation is shown in the following equation,

$$y^2 = x^3 + ax + b \tag{1}$$

Where values a and b are integers.

There are two types of elliptic curves used in cryptographic applications, namely the elliptic curve modulo prime which is defined by GF_p and binary curves built on GF_{2^m}. The set of parameters used in the GF_p field is (p, a, b, G, n, h), while in the GF_{2^m} field are (m, f (x), a, b, G, n, h).

4.3 Advanced Encryption Standard (AES)

AES is one of the encryption techniques that include symmetric key cryptography where the key used for the encryption and decryption process is the same. This algorithm converts information data into 128 bits of cipher blocks according to the size of the key used. The type of AES is divided into three, namely:

1. AES-128
2. AES-192
3. AES-256

The numbers behind the word AES indicate the key length used. Each AES has a different round number such as AES-128 using 10 round, AES-192 using 12 round, and AES-256 using 14 round.

4.4 Proposed Security Method

The security method proposed is an image encryption method on medical data using a hybrid algorithm, a combination of modified IBE schemes, ECC and AES algorithms. This method is used to increase security levels and avoid key exchanges. Safety data used are breath wave images, echocardiography and CT Scan of the Liver. The system design used in this paper is shown in Figure 2.

In this paper, we only use 3 stages in the IBE scheme, namely key generator, encrypt and decrypt. Reducing the number of stages in the IBE scheme is done in order to shorten the request and response times at the Setup and Extract stages of secret key requests. The key generator stage is used to generate key pairs and secret keys needed in the encryption and decryption process. Each user has a public and unique identity such as name, medical identity number, and others. Secret keys can be generated from input ECC key pairs containing user identities. To connect the ECC and AES algorithms, we need a protocol key agreement shown in Algorithms 1 line 4a and 4b. This protocol uses the ECDH algorithm so that the key pairs produced by ECC can be converted into symmetric keys that AES requires for the encryption and decryption process. Before conducting the communication, each user must specify the ECC parameters used for communication to be performed. ECDH algorithm is a key agreement protocol that allows users to have elliptic curve key pairs and make share secrets as in research [16] which uses the ECDH algorithm to generate AES keys.

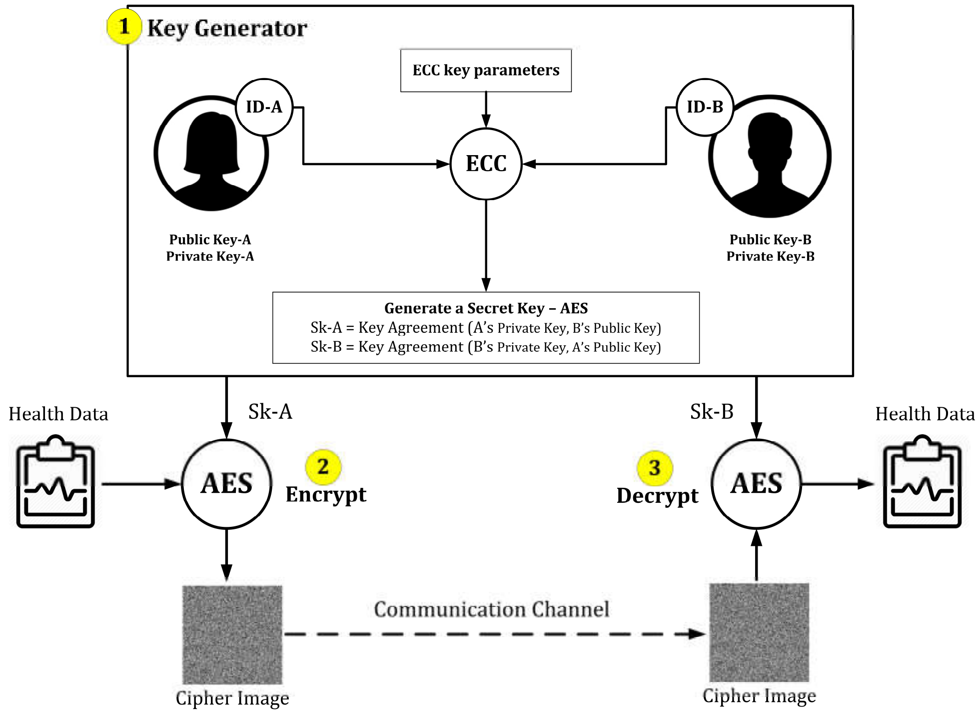

Figure 2. Proposed Method Design

In the encrypt stage, a secret key from the sender is needed to encrypt medical data. The algorithm used for the encryption process is AES-256 which uses a 256-bit cipher key and must pass 14 rounds. We used AES-256 because the symmetric algorithm recommended by NIST [17] for 2016-2030 is AES-256 to avoid Brute force attacks. Previously, medical data will be converted into a byte array and grouped into 128-bit data blocks. In the AES algorithm, each round consists of four stages, namely AddRoundKey, SubBytes, ShiftRows, and MixColumns. The results of this stage are cipher images containing medical data.

Before going through the decrypt stage, the recipient will get an image cipher through the communication channel. Then the recipient will send his identity and the sender's identity to the key generator to get his secret key. This secret key is used for the decryption process in the cipher image and is converted into an original message, namely medical data.

Algorithm 1 `Key Generator`

1. Input: User identity `IDu`, recipient's identity `IDr`, and Elliptic Curve `P`.
2. Calculate :
   a. `MDu`, `MDr` = message digest from the user's identity (`IDu`) and the recipient's identity (`IDr`) using the SHA-256 algorithm.
   b. `SRu`, `SRr` = secure random number for user and recipient.
   c. `SRu = SRu.setSeed(MDu)` %Used to set the seed of `SRu` using `MDu`
   d. `SRr = SRr.setSeed(MDr)` %Used to set the seed of `SRr` using `MDr`
3. Obtain the key pairs from ECC :
   a. `PubKey_u = (P, SRu)` % User's public key
   b. `PubKey_r = (P, SRr)` % Recipient's public key
   c. `PrivKey_u = (SRu)` % User's private key
   d. `PrivKey_r = (SRr)` % Recipient's private key
4. Generate a secret key using Key Agreement protocol:
   a. `Sku = (PrivKey_u, PubKey_r)` % User's secret key
   b. `Skr = (PrivKey_r, PubKey_u)` % Recipient's secret key

5. EXPERIMENT AND ANALYSIS

The proposed security method has been implemented for communication with two users. This method applies the modified IBE scheme. The algorithm used is ECC as a secret key generator and AES as an encryption algorithm. The purpose of this study is to analyze the performance of the proposed security method. Some parameters tested are computation time, entropy analysis, and statistical analysis.

5.1 Implementation of System

Tests performed on the proposed method are simulations using two OS hosts that are connected to a LAN network. The sender will send medical data in the form of a graph or image that has been encrypted using the proposed method, while the recipient will decrypt the ciphertext in order to obtain original medical data. The devices used in this study are shown in Table 1.

Table 1. Hardware Specifications

CPU	Intel Pentium CPU 2020M 2.40 GHz
Software	VirtualBox v5.2.8, Java 1.8.0_171
VM O/S	Debian GNU/Linux 7 (wheezy)
RAM VM O/S	1 GB

5.2 Experimental Result and Analysis

This subsection explains the results of the testing of the proposed security method. We propose a security method that implements a modified IBE scheme and uses the ECC and AES algorithms. The data used is in the form of graphics or images that represent patient medical data. We compared the proposed method with a comparison method that would be tested based on computational time, entropy analysis, and statistical analysis.

1. Time Measurement

This test is implemented in the communication between the sender and the recipient with the payment of the time required by the system. It is estimated that the two computational times recorded are the calculation of time in the key generator and the total computational time during the encryption-decryption process.

In the key generator stage, the user can generate his key pair and other key pairs using the person's identity. This makes it easy for users to avoid key exchanges on the communication channel. Making key pairs that do not belong to them are used as supporting parameters in creating secret keys. We tested the key generator stage by recording the computing time the system needed to produce 1 to 10 secret keys and compare the results with other methods.

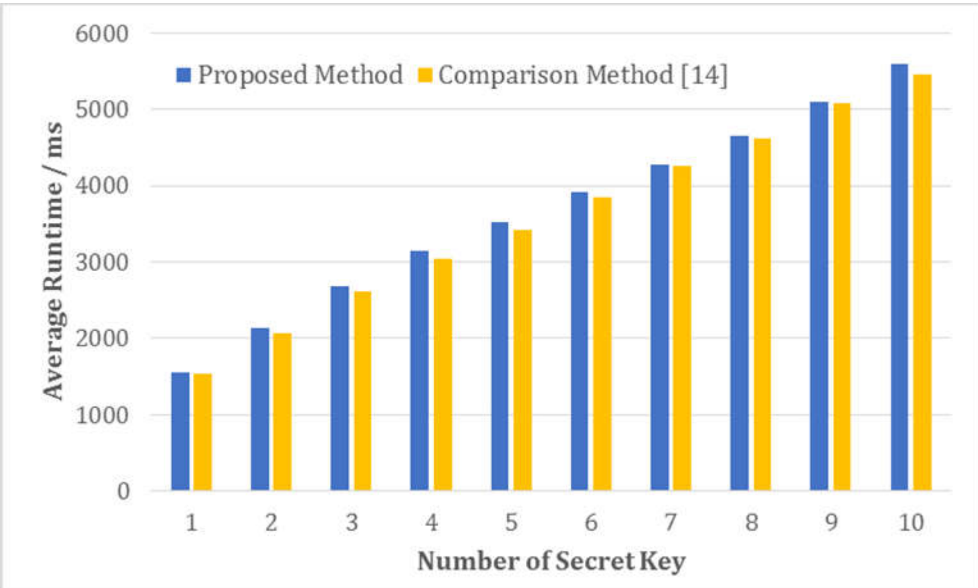

Figure 3. Computational Time Comparison of The Proposed Method and Comparison Method [14]

The results of computation time comparison between the proposed method and comparison method [14] shown in Figure 3, it was found that the proposed method has a slower computation time. This is because when the ECC key pair is formed there are additional parameters, namely the user's identity. The total time needed for the system to produce 1 to 10 secret keys is 36585 ms for the proposed method and 35978 ms for the comparison method. So that the error percentage of the total computational time obtained by the proposed method in the key generator stage is 1.69%.

Table 2. Total Computing Time of the Encrypt-Decrypt Stage

Elliptic Curve	AES	Proposed Method (ms)	[14] (ms)
P-256	AES-256	477,33	453,00
P-384	AES-256	509,00	508,67
P-521	AES-256	515,00	511,00

At the encrypt and decrypt stage, the user performs the encryption and decryption process using the AES-256 algorithm. There are several standards that describe the domain parameters of an elliptic curve, including NIST. NIST has recommended five curves over F (p) including P-192, P-224, P-256, P-384, P-521 (where xxx is the size of P in bits) [19]. In this test, the parameters changed are elliptic curves that are used, among others, P-256, P-384, and P-521. This can affect computing time in generating key pairs using ECC. Based on Table 2, it was found that the proposed method was slower for all elliptic curve variants for the encrypt and decrypt stages. The computing time is almost the same as the comparison method, namely when the system uses the elliptic curve P-384 with an error percentage of 0.07%.

Based on the results of the above tests, it was found that the proposed security method had a relatively slower time than the comparison method. This is because in the proposed method there is an additional algorithm, namely the existence of a user identity process that is embedded in a key pair. The computational error percentage of the proposed method is <2% for the key generator stage and <0.1% for the total computational time at the decrypt encrypt stage.

2. Entropy Analysis

Entropy uses the concept of probability in determining the entropy of a random variable. In this test, we use entropy to measure the randomness of the cipher image produced by the proposed method and the comparison method. The high entropy value is obtained from the random pixel value distribution in the cipher image and Equation 2 is used for the entropy value.

$$H(\sigma) = \sum_{i=0}^{M\times N} P(\sigma_i) log_2 \frac{1}{p}(\sigma_i)\ bits \tag{2}$$

Where $P(\sigma_i)$ is the probability that occurs in pixels σ_i and the log used is base 2 so that the entropy value is expressed in bits.

Table 3. The Entropy of Cipher Images

Image	Size	Proposed Method	[14]
Breathwave	256 x 256	7.9984	7.9977
Echocardiography	512 x 512	7.9994	7.9993
CT Scan of Liver	512 x 512	7.9997	7.9995

Table 3 shows the results of calculating the entropy value in the cipher image. This value is influenced by the size of the key, the original image and the encryption method used. In several previous works (e.g., [14], [18]) the average value for entropy is between 7.90 and 7.99. Based on the test results it was found that the proposed method had a higher entropy value than the comparison method. This states that the cipher image produced by the proposed method has near-ideal randomness.

3. Statistical Analysis

Statistical analysis that has been done on the proposed method is histogram cipher image analysis and analysis of the correlation of adjacent pixels. The purpose of this test is to find out whether the proposed method is resistant to statistical attacks. An image histogram is a diagram that describes the frequency distribution of pixel intensity values in an image. The pixel intensity value is expressed by the horizontal axis, while the vertical axis is the frequency or number of pixels. A good encryption method can make pixels distributed uniformly.

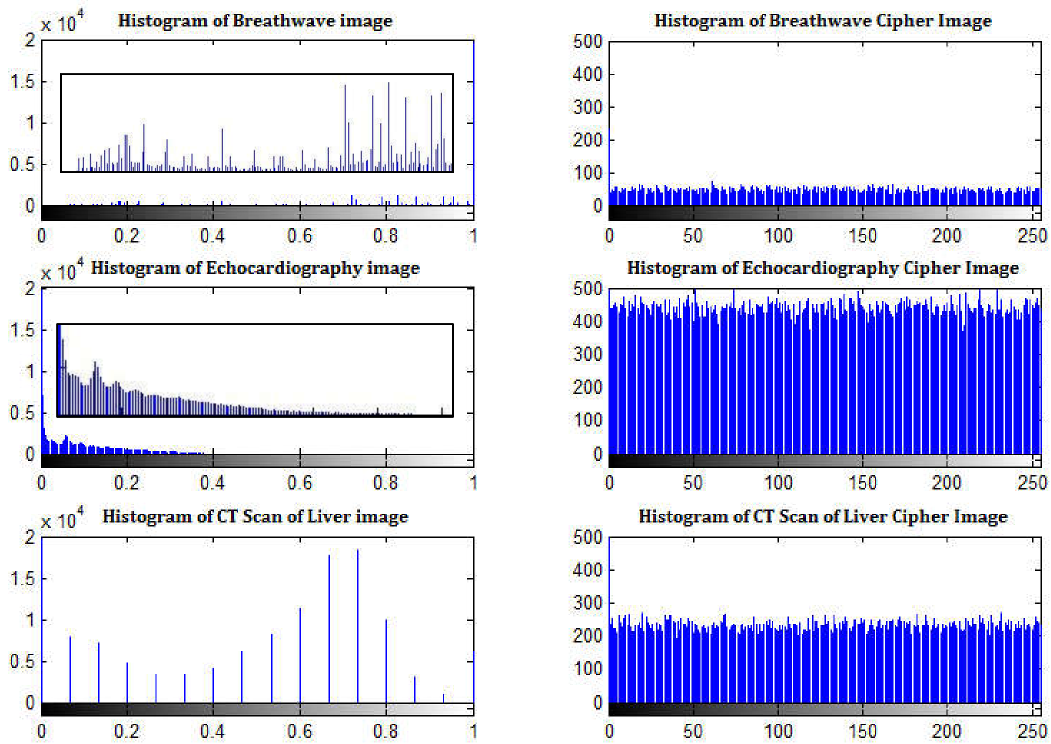

Figure 4. Histogram of Plain and Cipher Image

Figure 4 shows a histogram of the original image and cipher image. It can be observed in the cipher image that the distribution of the number of pixels in all variants of medical images is uniform.

Correlation of pixels with adjacent pixels in an image is expressed in three directions namely horizontal, vertical and diagonal. Cipher images are declared good if they have the smallest correlation with adjacent pixels. To calculate the correlation value of pixels with adjacent pixels, use Equation 3.

$$\gamma_{uv} = \frac{\sum_{i=1}^{N}(u_i - mean(u))(v_i - mean(v))}{(\sum_{i=1}^{N}(u_i - mean(u)^2))^{1/2} \times (\sum_{i=1}^{N}(v_i - mean(v)^2))^{1/2}} \quad (3)$$

In the analysis of the correlation of adjacent pixels, the proposed method will be compared with the comparison method [14] by calculating the pixel correlation in three variants of medical data expressed in three directions. The test results are shown in Table 4.

Table 4. Correlation between Plain and Cipher Image

Medical Data	**Directions**	**Correlation of Plain Image**	**Encryption Methods**	
			Proposed Method	**[14]**
Breath wave	Horizontal	0,9194	0,0306	0,0485
	Vertical	0,9850	0,0179	0,0213
	Diagonal	0,8537	0,0063	0,0096
Echocardiography	Horizontal	0,9594	-0,0001	0,0001
	Vertical	0,9687	-0,0080	-0,0014
	Diagonal	0,9500	-0,0006	-0,0025
CT Scan of Liver	Horizontal	0,9583	0,0123	0,0131
	Vertical	0,9649	-0,0040	-0,0010
	Diagonal	0,9517	0,0017	0,0035

The results of adjacent pixel correlation calculations are stated in Table 4, it was found that the proposed method has a lower correlation value for all data variants and directions. The smaller the correlation value, the cipher image can be declared good. The negative value in Table 4 is a correlation sign that allows one negative picture and must be reversed to get a correlation near +1.

Based on the results of statistical analysis tests it is stated that the proposed method is resistant to statistical attacks. This is evidenced by the results of a histogram analysis which states that the proposed method is able to make pixels in a uniformly distributed cipher image, and the results of adjacent pixel correlation analysis suggest that the proposed method is superior to the comparison method.

6. CONCLUSION

In this paper, a security method for encryption of medical data has been proposed. This method is implemented in the modified IBE scheme into three stages, namely Key Generator, Encrypt, and Decrypt. The encryption algorithms used are ECC and AES. We use the user identity and ECC parameters to create unique key pairs. Security analysis of the proposed method shows that the proposed method is resistant to statistical attacks even though it has a slower computing time. The proposed method has a higher entropy value and is able to make pixels in the ciper image evenly distributed than the comparison method. The optimal encryption algorithm that can be used for encryption is the elliptic curve P-384 with 384 ECC bits and 256 AES key bits.

Acknowledgements
The author would like to thank Anwar, a Postgraduate student at Politeknik Elektronika Negeri Surabaya (PENS) in 2018, for his assistance in obtaining medical data so that it can improve the quality of this paper.

REFERENCES
[1] Bruce Schneier, **Applied Cryptography: Protocols, Algorithms, and Source Code in C**. New York: John Wiley & Sons, 1996.
[2] C. A. Rohmatika, **Aplikasi Keamanan Gambar dengan Kriptografi Menggunakan Algoritma AES (Advanced Encryption Standard)**, Politeknik Negeri Sriwijaya, 2017.
[3] L. D. Singh and K. M. Singh, **Medical image encryption based on improved ElGamal encryption technique**, *Opt. - Int. J. Light Electron Opt.*, 2017.
[4] S. H. Kamali, M. Hedayati, R. Shakerian, and Mohsen Rahmani, **A New Modified Version of Advanced Encryption Standard Based Algorithm**, in *International Conference on Electronics and Information Engineering (ICEIE 2010)*, 2010, vol. 1, pp. 141–145.
[5] B. Subramanyan, V. M. Chhabria, and T. G. S. Babu, **Image Encryption Based On AES Key Expansion**, in *Second International Conference on Emerging Applications of Information Technology Image*, 2011, pp. 217–220.
[6] S. M. Wadi and N. Zainal, **High Definition Image Encryption Algorithm Based on AES Modification**, *Wirel. Pers Commun.*, vol. 79, pp. 811–829, 2014.
[7] Z. Yun-peng, L. Wei, C. Shui-ping, Z. Zheng-jun, N. Xuan, and D. Wei-di, **Digital Image Encryption Algorithm Based on Chaos and Improved DES**, in *2009 IEEE International Conference on Systems, Man, and Cybernetics*, 2009, no. October, pp. 474–479.
[8] Z. Zhao and X. Zhang, **ECC-Based Image Encryption Using Code Computing**, in *Proceedings of the ICCEAE2012*, 2013, pp. 859–865.
[9] A. E. Taki, E. Deen, and S. N. Gobran, **Digital Image Encryption Based on RSA Algorithm Digital Image Encryption Based on RSA Algorithm**, *IOSR J. Electron. Commun. Eng.*, vol. 9, no. 1, pp. 69–73, 2016.
[10] L. Li, A. A. A. El-latif, and X. Niu, **Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images**, *Signal Processing*, vol. 92, pp. 1069–1078, 2012.

[11] K. Shankar and P. Eswaran, **An Efficient Image Encryption Technique Based on Optimized Key Generation in ECC Using Genetic Algorithm**, *Artif. Intell. Evol. Comput. Eng. Syst.*, pp. 705–714, 2016.
[12] L. D. Singh and K. M. Singh, **Image Encryption using Elliptic Curve Cryptography**, *Procedia Comput. Sci.*, vol. 54, pp. 472–481, 2015.
[13] G. Zhao, X. Yang, B. Zhou, and W. Wei, **Rsa-Based Digital Image Encryption Algorithm In Wireless Sensor Networks**, in *2nd International Conference on Signal Processing Systems*, 2010, pp. 640–643.
[14] T. Shahriyar, M. H. Fathi, and Y. A. Sekhavat, **An Image Encryption Scheme Based on Elliptic Curve Pseudo Random and Advanced Encryption System**, *Signal Processing*, vol. 141, pp. 217–227, 2017.
[15] D. N. Purnamasari, A. Sudarsono, and P. Kristalina, **Secure Data Sharing Scheme using Identity-based Encryption for e-Health Record**, in *2018 International Electronics Symposium on Engineering Technology and Applications (IES-ETA)*, 2019, pp. 60–65.
[16] Rafi'i, Muhammad, and Jazi Eko Istiyanto, **Implementasi Algoritma ECDH dan AES untuk Pengamanan Pesan SMS pada Telepon Seluler**. BIMIPA, vol. 24(1), pp. 39-50, 2016.
[17] **NIST Recommendations** – Cryptographic Key Length Recommendation, available from (https://www.keylength.com/en/4/).
[18] S. Sathyanarayana, M. A. Kumar, K. H. Bhat, **Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points**, International Journal of Network Security, vol. 12(3), pp. 137–150, 2011.
[19] Gemalto, **Benefits of Elliptic Curve Cryptography**, March 2012, available from (www.securitydocumentworld.com › gov_wp_ecc1).