Received: August 15, 2022. Revised: August 30, 2022.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Medical Image Encryption Using Bit Plane Slicing, Dynamic Chaos, and Hash Function

De Rosal Ignatius Moses Setiadi[1]* **Rahmawati Zulfiningrum[1]**
Eko Hari Rachmawanto[1] **Pulung Nurtantio Andono[1]**

[1]*Faculty of Computer Science, Dian Nuswantoro University, Semarang, Indonesia*
* Corresponding author's Email: moses@dsn.dinus.ac.id

Abstract: Telemedicine is a communication in the medical field that requires privacy and confidentiality, so encryption is needed as a security method. The development of encryption methods must accompany technological developments. This research proposes a cryptography method developed and tested on medical images. This method consists of bit plane slicing, system chaos, and hash function. Bit plane slicing to break up the image bits so that they can be scrambled independently and dynamically with the chaos method. The hash function encrypts key 1, which is user input. The chaos method is run with dynamic parameters generated with a hash function to perform the confusion process on each bit plane. Then bit-plane join is performed, followed by the diffusion process using a logistic map with the second key for the parameter. The method is sensitive to slightly modified plain images or keys. Several measurement tools use to prove the method's performance. The result is a mean value are 7.999 for entropy information, 99.6027 for the number of pixels change rate (NPCR), 33.0925 for unified average changing intensity (UACI), 0.0021 for correlation coefficient, 231.8679 for chi-square and histogram, 50.0550 for avalanche effect, and perceptual analysis have proven the proposed method has satisfactory performance. The decryption is also done perfectly, as verified by the structural similarity index (SSIM)=1, peak signal-to-noise ratio (PSNR) is ∞, and bit error ratio (BER) is 0. Finally, this method can also work very fast in less than one second, so it can be implemented in real-time encryption.

Keywords: Medical cryptosystem, Dynamic chaotic map, Hybrid encryption, Bit plane slicing encryption, Adaptive hashing.

1. Introduction

Currently, the internet is one of the technologies that are the main needs of humans, and most modern work activities use the internet. Data transactions are activities that are almost always carried out through the use of the internet. Data security is needed when sending data, especially for personal and confidential data, such as military, diplomatic, national, and medical data [1, 2]. Medical data is used in telemedicine applications such as medical records, images, and even conversations. In particular, medical images are images that have different characteristics compared to natural images and graphic images. In general, medical images show a higher degree of homogeneity and correlation between neighboring pixels [3].

One method to secure various digital transactions is cryptography. Encryption and decryption procedures comprise digital cryptography. Encryption is done on the sender to convert plain text into cipher text. Cipher text has a different form and meaning than plain text, it even looks damaged. The decryption process is carried out on the receiving side to return the cipher text to plain text [4, 5]. The encryption and decryption processes must work perfectly so that the message can be read on the recipient's side without losing its meaning.

Many scholars have proposed various encryption methods. The aim is to increase security so that it is not easy for irresponsible parties to decrypt.

Encryption in digital images has different characteristics from the text. Some of them are high correlation between adjacent pixels, high redundancy, and large volume, so classical and standard encryption methods are not suitable for image encryption [3, 6, 7]. Especially in medical images, where this image has more homogeneous characteristics and a higher correlation [3]. The chaotic method is one of the solutions that is widely used in image encryption, and this is because of its characteristics which have a strong random level, unpredictable, integration complexity, ergodicity, and sensitivity to initial values [2, 3, 6-8].

The chaotic approach is frequently used in image encryption research, including [9-15]. This proves that the chaotic method is proven to have better effectiveness, but the chaotic method generally does not stand alone. Chaos method is often combined with other methods such as block cipher [16], splitting technique [12], substitution method[11], chaotic map combination [9, 10], bit plane technique [13, 14], etc. This combination of methods aims to produce a strong encryption method. As a result, the process of confusion and diffusion will be more optimal and get resistant to various statistical and differential attacks. The substitution method is the simplest, mostly using XOR or modulus operations with a certain key. While the block cipher method and splitting technique are the development of the substitution method. The combination of chaos algorithms is generally relatively stronger in the confusing process and more resistant to differential attacks. Bit-plane operations not only alter but also disperse pixels at the same time. As a result, no separate pixel action is required[14]. The bit-plane technique is a simple but powerful method for performing a substitution, confusion, and diffusion processes because each bit-plane can be processed independently.

The quality of encryption also depends on the quality of the key entered, a good key can increase the quality and strength of encryption from various attacks. To improve the quality of the key, a hashing method can be used as in research [3, 13, 14, 17, 18]. Another thing to consider is the encryption speed of a method, especially if a method is to be implemented in real-time applications [11, 19]

Therefore, this study proposes a method to encrypt medical images by combining several methods such as combination chaos operations, bit-plane and hashing to improve encryption quality. To clarify the flow of hypotheses and analyze the results of this study. The paper is presented in five parts, the first part is an introduction. Part two is an explanation of related work that inspires the proposed method. Part three is an explanation of the design of the proposed method. The fourth part is the presentation of the results and analysis, and the last part five is the conclusion.

2. Related work

Several previous studies have been proposed in the development of image encryption. Study [15] proposed combining two chaotic methods with a gradual encryption model. In the first stage, the complete image is descrambled using the logistic-sine map method. Then in the second stage the image is divided into small blocks with a size of 2×2 and then encrypted adaptively using a hyperchaotic map. This method has been tested with several measuring instruments such as keyspace and key sensitivity, entopy, correlation, and differential analysis. Although the results are quite good, the implementation of the method has only been tested on a limited dataset, especially standard images. In addition, the hash method has not been implemented in this research.

Research [14] also proposed combining two chaotic map methods. In this method, SHA-256 is also used to improve the quality of the key. The first time the image is divided into eight-bit planes. Furthermore, image encryption is carried out in stages using the Piece-wise Linear Chaotic Map (PWLCM) method gradually on each bit-plane, and then the horizontal and vertical gradual merging process is carried out. In the second stage, the scrambling process is carried out with a 2D logistic adjusted sine map [20]. This method is evaluated with several measuring instruments such as keyspace and sensitivity, entropy, NPCR and UACI, and correlation on standard images.

Research [9] proposed an encryption method for DICOM images. The proposed method is quite interesting by using four logistic map processes. Logistic map 1 and logistic map 2 are in charge of permuting the image as a whole, while logistic map 3 and logistic map 4 are for randomization with XOR operations on pixels in odd and even positions, respectively. This method has been tested with several standard measuring instruments and performs well.

Study [11] performed a combination of chaos method, dynamic box substitution method (S-Box), and AES. In this method, two keys are used. The first key is used to control AES-based chaotic sequences, and the second key is to perform S-Box operations dynamically. The XOR operation is performed at each encryption stage. This method was tested on various medical images such as MRI, CT Scan, and

X-ray. This research also tested several chaotic methods such as Arnold, Henon, Barker, etc. This method can use various types of chaotic maps and can pass various security tests. This shows that the chaos method can improve the performance of image encryption.

The chaotic approach with the random split picture methodology was also proposed in research [12]. A scrambling procedure is performed on random blocks in the early stages of encryption. The scrambling process is carried out for the confusing process and follows a zigzag pattern. Furthermore, a logistic map at the diffusion stage is carried out encryption. This method was tested on various medical images with both grayscale and color types and had good results on various security tests.

Based on some of the literature that has been described, it appears that the use of the chaos method can improve the quality of the encryption results. One of the stages in the chaos method is generally the scrambling process. If the scrambling process is carried out per bit plane dynamically, it will be able to increase the pixel scattering process. The bit-plane method is relatively simple so it can reduce the need for encryption and decryption time. In addition, the hash method can improve the quality of the key, which means that the quality of the key can enhance the quality of encryption. Based on these theories, this research proposes a bit-plane-based multilevel chaos adaptive method combined with a hash function to be tested on medical images. Statistical measuring tools to determine the resistance of statistical and differential attacks, in addition to computational speed were also tested in this study

3. Proposed method

This section details the phases of the proposed method. The procedure is divided into two steps: encryption and decryption. Section 3.1 describes the encryption process in depth, whereas Section 3.2 describes decryption.

3.1 Encryption scheme

At the encryption stage, two inputs are needed: the key that comes from user input and the image to be encrypted. In more detail, the steps are as follows:

1. Open an image with dimensions $N \times N$ and read the pixel values.
2. Split the pixels in each image channel into eight-bit planes. In this process, eight binary matrices per channel will be generated. As an illustration, Fig. 1 is given a sample matrix of image pixels with a size of 2×2.

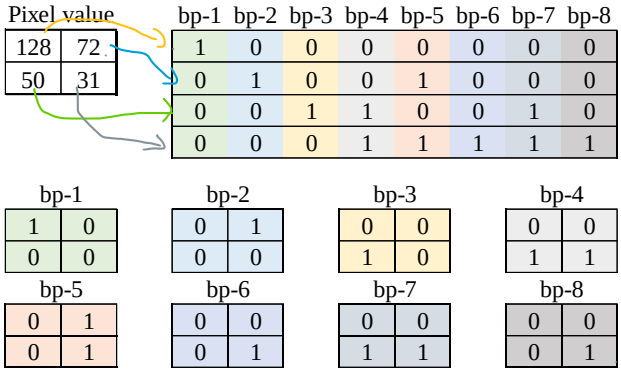

Figure. 1 Pixel value conversion to bit-plane matrix

3. Read the key input from the user ($k1$) and then perform a hash operation with SHA-512 so that all input keys are 64 characters long.
4. Split 64 characters into eight characters each, then convert them to ASCII numbers as dynamic parameters of Arnold scrambling on each bit plane matrix. The scrambling process is done with some shrimp paste. The Arnold transform formula on Eq. (1), then the parameters a, b, and iteration can be calculated by Eqs. (2) to (4).

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} mod\ N \quad (1)$$

$$a = 1 + \left(\sum_{i=(p*8)-7}^{p*8} H_i\right) mod\ x \quad (2)$$

$$b = 1 + \left(\sum_{i=(p*8)-7}^{p*8} H_i\right) mod\ y \quad (3)$$

$$it = 5 + \left(\sum_{i=(p*8)-7}^{p*8} H_i\right) mod\ z \quad (4)$$

Where a, b are positive integers, it is the number of iterations. H is the hash key, i is the index hash key, $p \in (1 \ldots 8)$, x, y, z are set parameters.

5. Use the parameters from step 4 to perform dynamic scrambling using Eq. (1) on each bit-plane.
6. Joint all the bit-planes to become whole image pixels again ($c1$).
7. Generate the second key (key 2) with a logistic map. The logistic map parameters are dynamic based on the standard deviation (σ) of the ASCII value of the hash key. Get the logistic map parameter ($k2$) with Eq. (5). Save it to perform the extraction process.

$$k2 = 3.5 + \left((\sigma_H - \lfloor \sigma_H \rfloor) \times 0.4999\right) \quad (5)$$

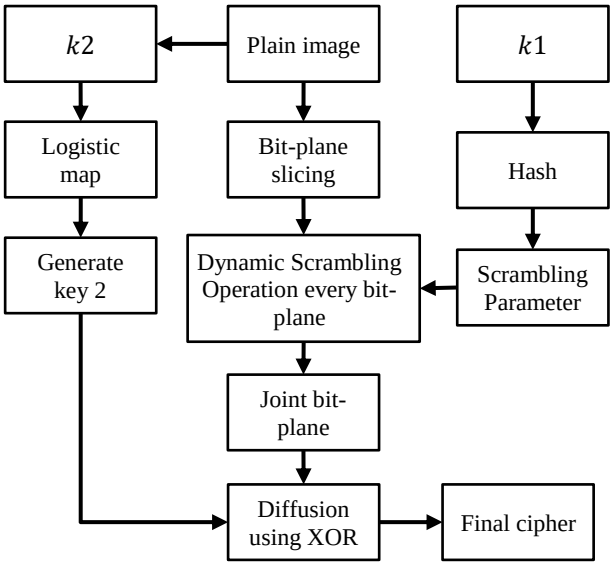

Figure. 2 Encryption scheme

8. Do the diffusion between key 2 and $c1$ with XOR operation to get the final cipher.

To see more clearly the proposed encryption scheme, see Fig.2.

3.2 Decryption scheme

The proposed method is a symmetric cryptography variant, meaning that the decryption process must utilize the same key as the encryption process. Three inputs are utilized in the decryption stage: second keys and a cipher image. The following are the detailed procedures for decryption:

1. Use $k2$ that has been stored in the encryption stage, as a logistic map parameter to generate key 2.
2. Read the cipher image, then perform XOR operation with key 2
3. Perform the bit-plane slicing operation to obtain eight binary matrices.
4. On the other hand, read $k1$ which is the user's input password.
5. Perform hash operations on $k1$ to get scrambling parameters a, b, and it.
6. Perform dynamic descrambling operations on each bit-plane with the generated parameters using Eq. (6).

$$\begin{bmatrix} i \\ j \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}^{-1} \begin{bmatrix} i' \\ j' \end{bmatrix} mod\ N \qquad (6)$$

7. Perform joint-bit plane operation to get the decrypted image

As an illustration of the proposed method, see Fig. 3.

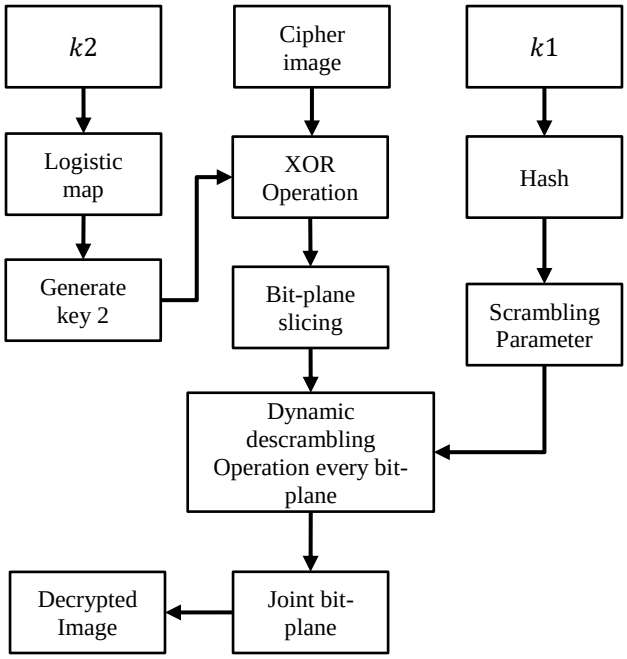

Figure. 3 Decryption scheme

4. Results and analysis

At this stage, the proposed method is tested with two types of medical images: CT and MRI. The image used has two kinds of bit-depth, 8 and 24, with dimensions 512×512 and 256×256, see Fig. 4. These

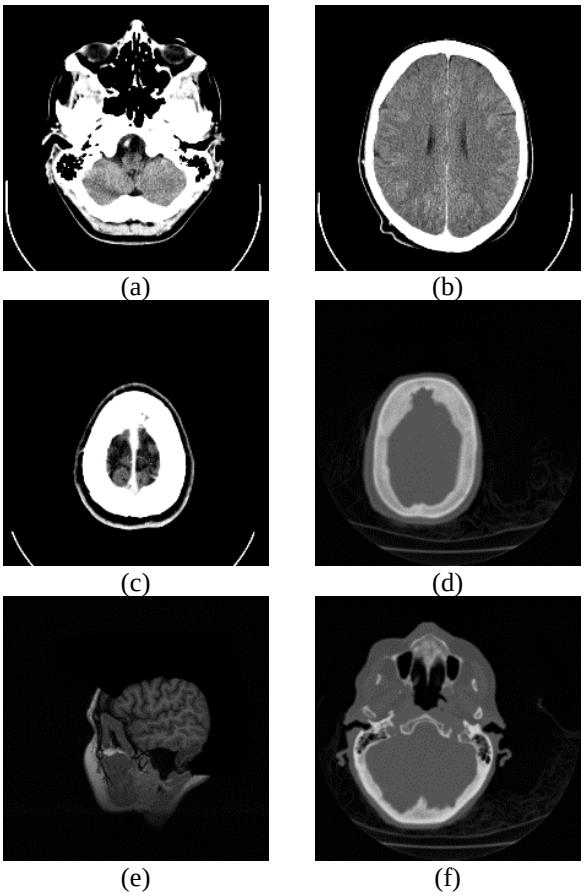

Figure. 4 Sample image dataset

Table 1. Summary results of various statistical and differential attack

Image	Entropy	χ^2	NPCR	UACI	AE	Correlation Coeficient		
						D	V	H
a	7.9994	253.7645	99.5917	32.9739	49.98	-0.0129	0.0102	0.0085
b	7.9991	237.2798	99.6085	33.3159	50.12	0.0182	-0.0079	0.0218
c	7.9993	228.3521	99.5849	33.2653	50.05	-0.0183	0.0092	0.0138
d	7.9994	221.3572	99.6177	32.8749	50.04	-0.0073	-0.0175	0.0067
e	7.9981	231.4682	99.6158	33.2413	49.93	0.0029	0.0053	-0.0102
f	7.9988	218.9856	99.5975	32.8839	50.21	0.0136	0.0055	-0.0037
Mean	7.9990	231.8679	99.6027	33.0925	50.0550	-0.0006	0.0008	0.0062

Table 2. Summary results of lossless and perceptual analysis

Image	Encryption		Decryption		
	PSNR	SSIM	PSNR	SSIM	BER
a	5.2187	0.0048	∞	1	0
b	5.4328	0.0037	∞	1	0
c	5.3291	0.0049	∞	1	0
d	5.4192	0.0032	∞	1	0
e	5.2192	0.004	∞	1	0
f	5.7821	0.0038	∞	1	0
Mean	5.4002	0.0041	∞	1.0000	0.0000

images can be downloaded from [21] and [22]. The dataset used in this study is similar to studies [12] and [3]. Both of these studies proposed a method for encrypting medical images and proved to have a fairly good performance, so we compared it with our proposed method.Since the proposed encryption and decryption scheme is only used on 8-bits images, then on 24-bits images (such as Fig. 4 (a-c)) the encryption scheme is performed three times on each channel. Even though using the same scheme, the encryption results will be different because encryption is not only affected by $k1$ but also influenced by $k2$, so the encryption method can still work reliably. To prove it, several tests were carried out in this research, and are presented in sections 4.1 to 4.7. In summary, all measurement results at this testing stage are presented in Table 1 and 2.

4.1 Information entropy (IE) analysis

Analyzing IE is one of the most significant things to know about the strength of encryption against statistical assaults. The IE value of an image can indicate its amount of unpredictability. Eq. (7) can be used to compute the entropy value, which has a maximum value of eight. Based on the entropy values from the data in Table 1, it appears that the suggested technique gives an outstanding value close to 8. Although not in all images, the value given is superior to one of the prior techniques. This demonstrates how the effect of separate scrambling on each plane may increase entropy.

Table 3. Entropy results and comparison

Image	Method[12]	Method[3]	Proposed
a	7.9993	**7.9994**	**7.9994**
b	**7.9994**	7.9993	7.9991
d	7.9974	7.9993	**7.9994**
e	7.9972	**7.9993**	7.9981
f	7.9977	**7.9993**	7.9988

$$IE = -\sum_{z=1}^{n} p_z log_2(p_z) \quad (7)$$

Where z is the index, n is the number of pixels, p is the probability distribution. The results of the entropy measurement are presented in Table 3.

4.2 Chi-square (χ^2) and histogram analysis

Besides EI, an essential statistical measurement tool in cryptography is the histogram. Histogram analysis can offer an overview of image encryption's resistance to statistical attacks. A proper histogram bins distribution pattern in the encrypted image must seem uniform. The histogram of the encryption results shown in Fig. 5 shows a considerable change, with homogenous histogram bins becoming equally distributed following the encryption procedure. However, this analysis may only appear visually, so it is necessary to add χ^2 analysis to provide numerical values. The analysis of χ^2 can be calculated by Eq. (8).

$$\chi^2 = \sum_{z=1}^{256} \frac{(r_z - f)^2}{f} \quad (8)$$

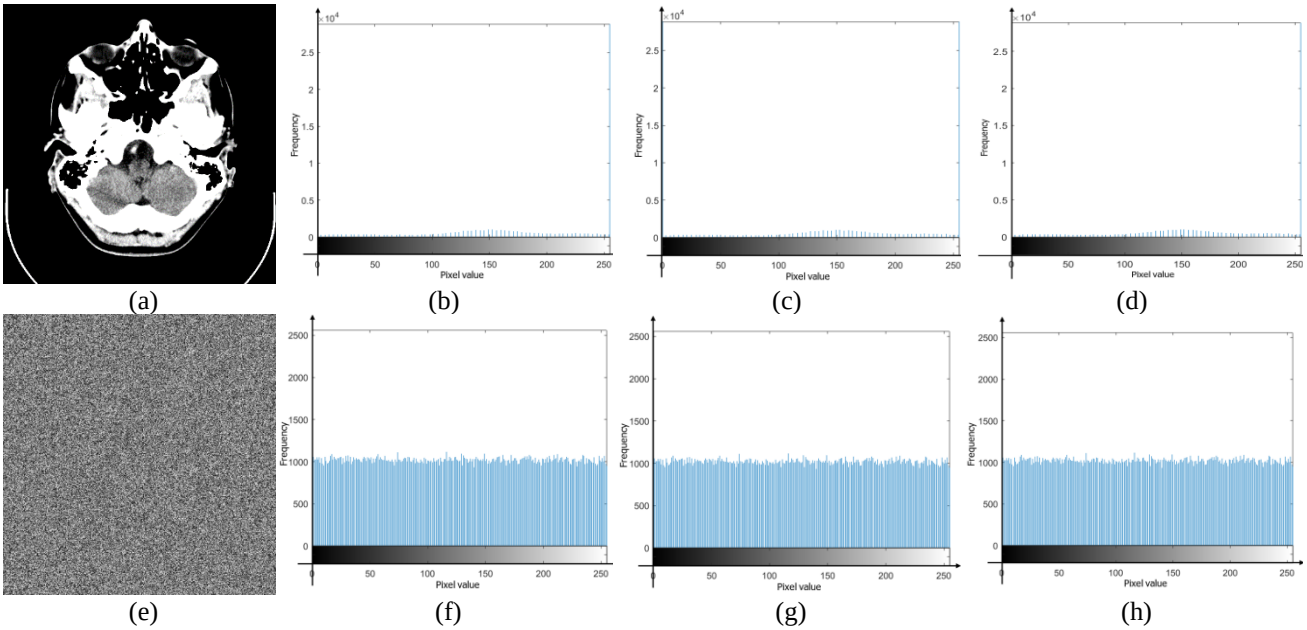

Figure. 5 Sample encryption results and histogram: (a) plain image, (b-d) the red, green, and blue histogram of the plain image, respectively, (e) encrypted image, and (f-h) the red, green, and blue histogram of the encrypted image, respectively

Table 4. χ^2results and comparison

Image	Method[12]	Method[3]	Proposed
a	262.9102	**250.5562**	253.7645
b	242.0332	243.6589	**237.2798**
d	232.2969	**215.2689**	221.3572
e	270.7578	249.5689	**231.4682**
f	**212.4219**	215.3695	218.9856

Where f is the frequency in each gray value $\left(f = \frac{r}{256}\right)$, r_z is the gray recurrence value of z. If 0.05 is chosen as the significant level and 255 as the degree of freedom, so the χ^2value must be less than 293.2478. Thus then the histogram is demonstrated to be uniform. Table 4 displays the results of the χ^2 measurement.

Based on the data presented in Table 2, it appears that the proposed method is superior, especially in two images (b and d). All χ^2 values also pass and prove that the image histogram is uniform.

4.3 NPCR and UACI measurements

The NPCR and UACI are statistical measurement tools to determine the robustness of differential attacks. The tool calculates the correlation between two encrypted images slightly modified by the plain image. Modifications are generally performed one bit on the plain image at random. The optimal NPCR value is 99.6094, while the UACI is 33.4635[23]. NPCR and UACI values that are near to optimal should be considered excellent. The UACI and NPCR can be calculated by Eqs. (9) and (10), respectively.

Table 5. UACI results and comarison

Image	Method[12]	Method[3]	Proposed
a	-	**33.4495**	32.9739
b	33.4406	**33.4489**	33.3159
d	33.4813	**33.4709**	32.8749
e	33.4535	**33.4585**	33.2413
f	33.4903	**33.4715**	32.8839

Table 6. NPCR results and comparison

Image	Method[12]	Method[3]	Proposed
a	-	99.5894	**99.5917**
b	99.6623	99.5995	**99.6085**
d	99.6216	99.6189	**99.6177**
e	99.6002	99.5963	**99.6158**
f	99.6231	**99.6118**	99.5975

$$UACI = \left[\frac{1}{N\times N}\sum_{i=1}^{N}\sum_{j=1}^{N}\frac{E_1(i,j)-E_2(i,j)}{255}\right]\times 100 \quad (9)$$

$$NPCR = \left[\frac{1}{N\times N}\sum_{i=1}^{N}\sum_{i=1}^{N}D(i,j)\right]\times 100,$$
$$D(i,j)\begin{cases}0, E_1(i,j) = E_2(i,j)\\ 1, E_1(i,j) \neq E_2(i,j)\end{cases} \quad (10)$$

Where E_1 is the first encrypted image, E_2 is the second encrypted image, D is different, i, j are pixel coordinates. The calculation results of the UACI value calculation are presented in Table 5, while the NPCR is presented in Table 6.

The proposed method seems to have an advantage in the NPCR value because almost all of the values are superior except for image f. Unfortunately, the UACI value of the proposed method does not appear to be better than the previous method. In fact, it tends

to be the least. However, this value is still relatively close to the ideal value, so based on this statistical tool, this method is resistant to differential attacks.

4.4 Correlation coefficient (CC) analysis

Basically, a plain image has a high CC pixel value (close to 1), because adjacent pixel values generally have a small difference. A decent encryption scheme should be able to reverse the CC value of this pixel [15]. CC analysis can be calculated by Eq. (11).

$$CC_{ij} = \frac{cov(ij)}{\sqrt{D_i}\sqrt{D_j}} \quad (11)$$

$$cov(ij) = \frac{1}{n}\sum_{z=1}^{n}[i_z - E(i)]\,[y_z - E(y)] \quad (12)$$

$$D(i) = \frac{1}{n}\sum_{z=1}^{n}[i_z - E(i)]^2 \quad (13)$$

$$D(j) = \frac{1}{n}\sum_{z=1}^{n}[j_z - E(j)]^2 \quad (14)$$

Where i and j are values of two adjacent pixel, $E(i)$ and $E(j)$, n is the total pixels. The horizontal, diagonal, and vertical directions are used to compute CC for each image, and each employs 2000-pixel pairs. It can be seen that in Table 7, the CC value presented by the proposed method has a good value and is close to this, at some points, this method is also superior.

4.5 Avalanche effect (AE) analysis

AE is a measuring tool that is quite similar to NPCR and UACI, which is also used to measure resistance to differential attacks. The difference is, that the AE modification is done on the plain image.

Table 7. Correlation coefficient results and comparison

Image	Dir	Method[12]	Method[3]	Proposed
a	H	-	-0.0113	**0.0085**
	D	-	**-0.0027**	-0.0129
	V	-	**0.0063**	0.0102
b	H	0.0182	**-0.0013**	0.0218
	D	0.0165	**0.0052**	0.0182
	V	-0.0108	0.0089	**-0.0079**
d	H	**0.0059**	-0.0078	0.0067
	D	0.008	-0.0094	**-0.0073**
	V	-0.0237	**0.0046**	-0.0175
e	H	-0.0044	**0.0039**	-0.0102
	D	0.0081	-0.0038	**0.0029**
	V	0.0046	**0.0028**	0.0053
f	H	0.0298	0.0051	**-0.0037**
	D	**0.0012**	-0.0023	0.0136
	V	0.0063	-0.0084	**0.0055**

Table 8. AE results and comparison

Image	Method[3]	Proposed
a	50.08	**49.98**
b	**50.02**	50.12
d	50.05	**50.04**
e	**50.04**	49.93
f	**50.01**	50.21

So the first encrypted image comes from the original plain image, and the second comes from the plain image with a modified bit. AE is generally used as a measurement tool for text encryption but in some research on image encryption. The ideal AE value is close to 50%[24]. In order to calculate the AE value, the encrypted image needs to be transformed to binary (bE) with Eq. (15).

$$AE = \frac{\sum_{z=1}^{n} bE1_z \underline{\vee} bE2_z}{n} \times 100 \quad (15)$$

The AE values in Table 8 prove that the proposed method performs satisfactorily. All AE values are close to 50%, and images a and d are superior to the related method.

4.6 Lossless and perceptual analysis

PSNR and SSIM are evaluation tools that are commonly used in image processing research to assess image output quality in terms of visual appearance. The ideal PSNR value is ∞, while the SSIM is 1[25]. In image encryption, the value must be on the contrary. PSNR and SSIM must be close to zero, thus meaning that the changes in the shape of the image are visually different. PSNR and SSIM are different measuring tools, PSNR measures based on error while SSIM is based on image structure.

$$PSNR = 20\log 10\left(\frac{I_{max}}{\sqrt{MSE}}\right) \quad (16)$$

$$MSE = \frac{1}{N\times N}\sum_{i=1}^{W}\sum_{j=1}^{H}\left(P_{ij} - E_{ij}\right)^2 \quad (17)$$

$$SSIM = \frac{(2\mu_P\mu_E + C_1)(2\sigma_{PE} + C_2)}{(\mu_P^2 + \mu_E^2 + C_1)(\sigma_P^2 + \sigma_E^2 + C_2)} \quad (18)$$

$$C_1 = (sc_1 D)^2 \quad (19)$$

$$C_2 = (sc_2 D)^2 \quad (20)$$

$$BER = \frac{\sum_{z=1}^{n} bP_z \underline{\vee} bE_z}{n} \times 100 \quad (21)$$

PSNR and SSIM can also be utilized to determine a method's lossless level. Image encryption must be possible to decrypt correctly. Hence the PSNR value

Table 9. PSNR results and comparison after encryption

Image	Method[12]	Method[3]	Proposed
a	**5.1192**	5.2584	5.2187
b	5.8811	**5.1268**	5.4328
c	-	-	**5.3291**
d	5.6824	5.4895	**5.4192**
e	5.2935	5.2568	**5.2192**
f	6.0865	**5.3689**	5.7821

Table 10. SSIM results and comparison after encryption

Image	Method[3]	Proposed
a	0.0054	**0.0048**
b	**0.0023**	0.0037
d	0.0051	**0.0032**
e	0.0042	**0.0040**
f	**0.0036**	0.0038

in the decryption process must be ∞ and the SSIM must be 1. By comparing the plain and encrypted pictures, the PSNR and SSIM encryption process can be computed. While the decryption process is calculated by comparing the decrypted and plain images. The measuring instrument that is often used in the decryption process is BER. The calculation method is quite similar to PSNR and SSIM, but the difference is, that in BER, the value is calculated based on bit error, so the image needs to be converted into binary form. The perfect BER value for the decryption process is 0. PSNR, SSIM, and BER can be calculated using Eq, respectively. (16), Eq. (18), and Eq. (21). The calculation results of PSNR and SSIM, values are presented in Table 9 and 10. Based on the results in Table 9 and 10, this method tends to be superior in terms of perceptual analysis. The PSNR and SSIM figures reported here are also superior to the prior technique. This method's decryption procedure can also perform properly because all of the PSNR value is ∞ , SSIM is 1, and BER is 0.

4.7 Computational speed

According to the information provided in sections 4.1 to 4.6, it indicates that the suggested technique outperforms the method [12], but is quite balanced with the method [3]. The proposed method is superior in calculating NPCR values and perceptual analysis but less superior in UACI calculations, while other measuring tools are almost equivalent. One of the advantages of the proposed method is a more straightforward design to reduce computation time. The bit-plane slicing method has the most important influence on maximizing the dynamic chaos method. So in this section a comparison is made with method [3], by replicating the method and conducting at least ten experiments on each image.

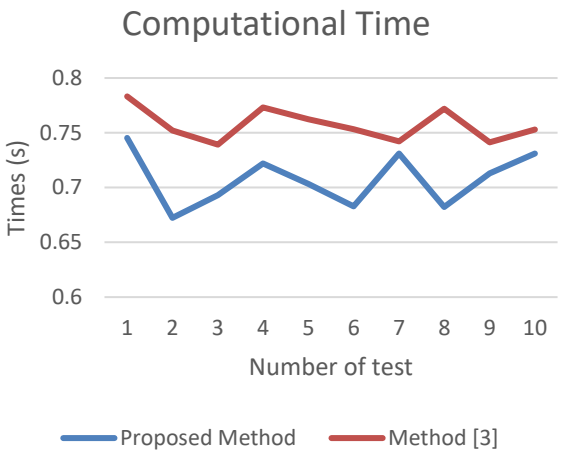

Figure. 6 Computational time method consumption

The experiment was carried out with the Matlab R2016A application, with the tic toc function with an intel Evo i7 processor, 16 GB memory size and Intel Iris G7 GPU. Meanwhile, the dataset is resized to 256×256 and converted to grayscale. It can be seen that the results presented in Fig. 6 have advantages in terms of computational speed.

5. Conclusions

Medical image is one of the important medical data. The different characteristics of medical images require strong encryption methods against various attacks. This study proposes a medical image encryption method using the bit plane slicing method combined with hash and chaos map operations to perform chaos scrambling on each image plane dynamically and independently. The aim is to increase the effect of confusion and diffusion on the image and optimize computational speed. In the confusion process, the chaos method uses a logistic map with parameters that depend on the standard deviation of the plain image. This is useful for increasing the effect of resistance to differential attacks. The proposed method is proven to have high security. This is represented by the excellent values of entropy, histogram, and χ^2 values and differential evidenced by the NPCR, UACI, and AE. This method can also produce good correlation coefficients and perceptual analysis and perfectly perform decryption. The proposed method is also faster than the previous method in the computational speed case. Future research is proposed to optimize the security and computing side again.

Conflicts of Interest

We would like to certify that no known conflicts of interest are linked with this publication. This

research has received no major funds, which may have impacted its conclusion. We also affirm that the paper was reviewed and approved by all mentioned authors and that no additional individuals who met the requirements for authorship but are not listed have done so.

Author Contributions

Methodology, DRIMS; Conceptualization, DRIMS; Software, EHR; Formal analysis, EHR, and RZ; Investigation, EHR; Resources, PNA; Data curation, DRIMS; Validation, EHR, and RZ; Writing—original draft preparation, DRIMS; Writing—review and editing, PNA and EHR; Visualization, DRIMS; Supervision, DRIMS; Project administration, RZ.

Abbreviation: DRIMS: De Rosal Ignatius Moses Setiadi; RZ: Rahmawati Zulfiningrum; Eko Hari Rachmawanto; PNA: Pulung Nurtantio Andono

Acknowledgments

The authors are grateful for the support for research funding in 2022 provided by the Ministry of Research and Technology / National Research and Innovation Agency with number 072/E5/PG.02.00.PT/2022, 016/LL6/PL/AK.04/2022, 056/F9/UDN.09/VI/2022.

References

[1] A. H. Mohammed, A. K. Shibeeb, and M. H. Ahmed, "Image Cryptosystem for IoT Devices Using 2-D Zaslavsky Chaotic Map", *Int. J. Intell. Eng. Syst.*, Vol. 15, No. 2, pp. 543-553, 2022, doi: 10.22266/ijies2022.0430.48.

[2] M. A. Alzain, "Efficient Segment-based Image Ciphering using Discretized Chaotic Standard Map with ECB, OFB and CBC", *Int. J. Adv. Comput. Sci. Appl.*, Vol. 13, No. 5, pp. 421-428, 2022, doi: 10.14569/ijacsa.2022.0130550.

[3] D. R. I. M. Setiadi, E. H. Rachmawanto, and R. Zulfiningrum, "Medical image cryptosystem using dynamic josephus sequence and chaotic-hash scrambling", *J. King Saud Univ. - Comput. Inf. Sci.*, 2022, doi: 10.1016/j.jksuci.2022.04.002.

[4] R. R. Suman, B. Mondal, and T. Mandal, "A secure encryption scheme using a Composite Logistic Sine Map (CLSM) and SHA-256", *Multimed. Tools Appl.*, pp. 27089-27110, 2022, doi: 10.1007/s11042-021-11460-4.

[5] M. Kaur, S. Singh, and M. Kaur, "Computational Image Encryption Techniques: A Comprehensive Review", *Math. Probl. Eng.*, Vol. 2021, No. i, 2021, doi: 10.1155/2021/5012496.

[6] F. Budiman, P. N. Andono, and D. R. I. M. Setiadi, "Image Encryption using Double Layer Chaos with Dynamic Iteration and Rotation Pattern", *Int. J. Intell. Eng. Syst.*, Vol. 15, No. 2, pp. 57-67, 2022, doi: 10.22266/ijies2022.0430.06.

[7] S. R. M. Halagowda and S. K. Lakshminarayana, "Image Encryption Method based on Hybrid Fractal-Chaos Algorithm", *Int. J. Intell. Eng. Syst.*, Vol. 10, No. 6, 2017, doi: 10.22266/ijies2017.1231.24.

[8] X. Meng, J. Li, X. Di, Y. Sheng, and D. Jiang, "An Encryption Algorithm for Region of Interest in Medical DICOM Based on One-Dimensional e λ -cos-cot Map", *Entropy*, Vol. 24, No. 7, pp. 1-28, 2022.

[9] S. Mortajez, M. Tahmasbi, J. Zarei, and A. Jamshidnezhad, "A novel chaotic encryption scheme based on efficient secret keys and confusion technique for confidential of DICOM images", *Informatics Med. Unlocked*, Vol. 20, p. 100396, 2020, doi: 10.1016/j.imu.2020.100396.

[10] A. A. Arab, M. J. B. Rostami, and B. Ghavami, "An image encryption algorithm using the combination of chaotic maps", *Optik (Stuttg).*, Vol. 261, No. April, p. 169122, 2022, doi: 10.1016/j.ijleo.2022.169122.

[11] S. Ibrahim, "Framework for Efficient Medical Image Encryption Using Dynamic S-Boxes and Chaotic Maps", *IEEE Access*, Vol. 8, pp. 160433-160449, 2020, doi: 10.1109/ACCESS.2020.3020746.

[12] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A new image encryption algorithm for grey and color medical images", *IEEE Access*, Vol. 9, pp. 37855-37865, 2021, doi: 10.1109/ACCESS.2021.3063237.

[13] Z. H. Gan, X. L. Chai, D. J. Han, and Y. R. Chen, "A chaotic image encryption algorithm based on 3-D bit-plane permutation", *Neural Comput. Appl.*, Vol. 31, No. 11, pp. 7111-7130, 2019, doi: 10.1007/s00521-018-3541-y.

[14] D. Sravanthi, K. A. K. Patro, B. Acharya, and S. Majumder, "A secure chaotic image encryption based on bit-plane operation", in *Advances in Intelligent Systems and Computing*, Vol. 758, pp. 717-726, 2018.

[15] X. Chen and C. J. Hu, "Adaptive medical image encryption algorithm based on multiple chaotic mapping", *Saudi J. Biol. Sci.*, Vol. 24, No. 8, pp. 1821-1827, 2017, doi: 10.1016/j.sjbs.2017.11.023.

[16] M. A. I. Pekereng and A. D. Wowor, "Square

transposition: an approach to the transposition process in block cipher", *Bull. Electr. Eng. Informatics*, Vol. 10, No. 6, pp. 3385-3392, 2021, doi: 10.11591/eei.v10i6.3129.

[17] X. Wang, X. Zhu, X. Wu, and Y. Zhang, "Image encryption algorithm based on multiple mixed hash functions and cyclic shift", *Opt. Lasers Eng.*, Vol. 107, pp. 370-379, 2018, doi: 10.1016/J.OPTLASENG.2017.06.015.

[18] M. Demirtaş, "A new RGB color image encryption scheme based on cross-channel pixel and bit scrambling using chaos", *Optik (Stuttg).*, Vol. 265, No. June, pp. 0-2, 2022, doi: 10.1016/j.ijleo.2022.169430.

[19] Z. Li, C. Peng, W. Tan, and L. Li, "An Effective Chaos-Based Image Encryption Scheme Using Imitating Jigsaw Method", *Complexity*, Vol. 2021, 2021, doi: 10.1155/2021/8824915.

[20] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map", *Inf. Sci. (Ny).*, Vol. 339, pp. 237-253, 2016, doi: 10.1016/j.ins.2016.01.017.

[21] Wikipedia Commons, "Category:Computed tomography images of Mikael Häggström's brain - Wikimedia Commons.", https://commons.wikimedia.org/wiki/Category:Computed_tomography_images_of_Mikael_Häggström%27s_brain (accessed Aug. 12, 2022).

[22] M. Levoy, "The Stanford Volume data archive.", https://graphics.stanford.edu/data/Voldata/ (accessed Aug. 12, 2022).

[23] H. Zhao, S. Xie, J. Zhang, and T. Wu, "A dynamic block image encryption using variable-length secret key and modified Henon map", *Optik (Stuttg).*, Vol. 230, p. 166307, 2021, doi: 10.1016/j.ijleo.2021.166307.

[24] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption", *Signal Processing*, Vol. 160, pp. 45-58, 2019, doi: 10.1016/J.SIGPRO.2019.02.016.

[25] D. R. I. M. Setiadi, "PSNR vs SSIM: imperceptibility quality assessment for image steganography", *Multimed. Tools Appl.*, Vol. 80, No. 6, pp. 8423-8444, 2021, doi: 10.1007/s11042-020-10035-z.