Received: October 26, 2021. Revised: November 29, 2021. 57

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Image Encryption using Double Layer Chaos with Dynamic Iteration and Rotation Pattern

Fikri Budiman[1*] Pulung Nurtantio Andono[2] De Rosal Ignatius Moses Setiadi[2]

[1] *Faculty of Computer Science, Dian Nuswantoro University, Semarang, Indonesia*
[2]*Department of Informatics Engineering, Dian Nuswantoro University, Semarang, Indonesia*
* Corresponding author's Email: fikri.budiman@dsn.dinus.ac.id

Abstract: This research proposes an encryption method for images based on dual chaos systems and dual hash functions. SHA-256 and SHA-512 are hash functions chosen to process plain images and private keys. The purpose of using hash functions on plain and key images is to increase encryption resistance against differential attacks and perform local encryption in each image zone. The proposed method consists of two stages of encryption, the first involves dual hash functions and confusion with a chaotic system by performing encryption based on zoning and rotation of the image. The second stage is a diffuse process using a logistic map. The proposed method is proven to be strong against various attacks that have been tested with various measuring tools such as entropy, histogram analysis, chi-square, number of changing pixel rate (NPCR), unified averaged changed intensity (UACI), and the avalanche effect (AE). This method also proved to work better than the state-of-the-art method in this research, significantly based on entropy, UACI, and NPCR.

Keywords: Chaotic system, Logistic map, Zoning and rotate, Cryptosystem.

1. Introduction

Technology is growing and computer computing is getting faster, this has many positive benefits for humans in facilitating their work, for example in data transmission. However, this can also be a problem when used by irresponsible people and commit cybercrimes. Therefore, the security of data transmission needs to be strengthened [1]. Encryption is one way of securing data and is currently one of the interesting studies to study. Actually all digital data can be encrypted, but encryption research on image data has become the most conducted [2, 3]. Encryption in digital images has different characteristics when compared to text encryption. Several methods for text encryption, such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), 3-DES, and Rivest–Shamir–Adleman (RSA), have been proven to work well on text, but if applied to encryption of images or multimedia data, they are not suitable. Many researchers, such as in research [4–8], state that these methods make the encryption process less efficient, over-complex, and over-computing. Encryption on images is widely applied using the chaos method, which this method has many advantages in encrypting a digital image, some of which are ergodicity characters, sensitivity to more unpredictable initial values, low complexity, and strong correlation, and non-uniform distribution. [9–11], this is the reason for choosing the chaos system in this research.

There are many chaotic systems used in image encryption, such as Arnold [5, 7], logistic map [12–15], hyperchaotic [16, 17], and others. In many studies of encryption literature on digital images, the use of chaos systems is widely combined with various other encryption methods to improve message security. But if you look specifically, some research proposes a block-based encryption technique based on a chaos system as in the research [3, 18]. The block-based technique is done by dividing the image into smaller blocks, then encrypting each block. In research conducted by [3], Encryption of each block

is done dynamically with a different key and is also done with a dynamic pattern, so that each image block will indirectly have an independent key and increase security.

Another quiet method that is widely combined with the chaotic method is hashing. Hashing is a one-way encryption method that is widely used to encrypt passwords because the results of hashing encryption cannot be decrypted. The hashing method is implemented in image encryption, usually in the add key generation process. The key in question is generally a key that is processed from plaintext [10, 19–21] as well as the private key used for encryption [3], In addition, the hash method is also widely used to process keys generated from pseudo-random generators [17]. The purpose of the hash function here can serve to increase security from differential attacks because with the help of the hash function it can increase the diversity of keys when there is a minimal modification of the plaintext. Based on these hypotheses, this study develops an encryption method based on a chaotic algorithm combined with a hash function, then this research provides several modifications to the model for combining the chaos method with zoning and rotating techniques. This paper is composed of six parts, namely an introduction to this section, part two explaining related research, part three explaining the proposed model, part four presenting the results and analysis, part five presenting the discussion, and part six containing a conclusion.

2. Related research

Several studies have inspired this research in modifying the encryption model, one of which is research [7]. In this research, the encryption method is carried out by combining the chaotic method and the hybrid modulus substitution cipher, both of which are encryption with a chaotic system. The chaotic method is used to perform shuffle and hybrid modulus substitution cipher is used for the diffusion process.

Other research is [22], In this research, the contribution is in the l-shaped method of dynamic block. This method also uses a chaotic method combined with a hash function (SHA 512). SHA-512 is used to generate keys from plain images. In the early stages of encryption, each dynamic block is carried out with an L-shaped pattern to perform the scrambling process. The next step is the diffusion process with the l shape pattern and XOR function.

In research [3], the encryption technique is divided into stages, the first is confusion with the Arnold method locally in each sub-block then followed by a diffusion technique using a stream cipher. By using both stages of encryption, encryption is produced that is resistant to statistical and differential attacks.

Research [23] proposes a two-stage encryption technique, where the first is a horizontal and vertical permutation process. The permutation technique is similar to the confusion and scrambling technique, the goal is to randomize the position of the image pixels. The permutation process is carried out based on a random keystream generator. While the diffusion process is carried out based on a dynamic index generator. The diffusion process is carried out simultaneously based on certain iterations to produce an encrypted image.

From the several methods described, it can be concluded that the image encryption process must have at least two processes, namely confusion/permutation/scrambling and the diffusion stage. By combining these two processes will produce a strong encryption method. Tetapi proses enkripsi banyak dilakukan langsung pada whole image. Inspired by [3], This research also uses these two processes to propose an encryption model, to increase resistance to statistical attacks, a slight modification was carried out with a gradual encryption method based on local confusion with zoning and rotation techniques in the early stages, while at the other stage XOR operations were carried out with a logistic map. Furthermore, the hash function is performed on two of the key and on the image to increase the security of the differential, this method is further explained in section 3.

3. Proposed method

In this section, a symmetric encryption method is proposed which involves several methods with modifications in several parts. The proposed method consists of two main processes, namely encryption, and decryption. These two processes involve two chaotic methods, hash functions combined with zoning and rotation techniques. In detail the encryption process is explained as follows:

1. Read the plain image, use it as input for two processes, namely: the SHA-1 hash function and the zoning function. As a limitation, the plain image used has a size of 512×512 pixels.
2. SHA-256 hash function of plain image (P) will generate $keyB$ as the key to performing the rotation. Also, perform the SHA-256 hash function for the complement value of the image (P'). The results of the two SHA functions are combined and produce a 64-character $keyB$ key. For an illustration see Eq. (1) create $keyB$.

$$keyB = JOINT\big(SHA256(P), SHA256(P')\big) \quad (1)$$

3. Divide the image into small zones with a size of 64×64. So, the image is divided into 64 zones.
4. Change each $keyB$ character to ASCII number form, resulting in 64 ASCII numbers for 64 zones. Then perform the modulus 4 function on each character to determine the rotation angle of each zone.
5. Rotate the zone based on the remaining ASCII quotient ($keyB$). For the remaining 0 no rotation is performed, the remaining 1 is rotated 90°, the remaining 2 is rotated 180°, the remaining 3 is rotated 270, see Fig. 1 for sample results. Save $keyB$ for the decryption process.
6. On the other hand, read $keyA$ then encrypt the SHA512 hash, then convert the encryption result to an ASCII number
7. Perform the modulus operation for each ASCII number to get the chaotic encryption key for each image zone. Use Eq. (2) to get the p value, Eq. (3) to get the value of q, Eq. (4) for the number of iterations (r), and Eq. (5) to perform a chaotic operation. So that the chaotic operation is carried out dynamically on each image zone based on $keyA$.

$$p = mod(ASCII[i], 256) \quad (2)$$

$$q = 256 - mod(ASCII[i], 256) \quad (3)$$

$$r = mod(ASCII[i], 32) \quad (4)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod\ M \quad (5)$$

8. Where the image must have a size of $M \times M$, x and y are the pixel coordinates of the original image, x' and y' are the pixel coordinates of the image after scrambled, the chaotic operation is carried out with the number of iterations r, i is the index of each ASCII number. The results of this stage will produce the first stage of encryption.

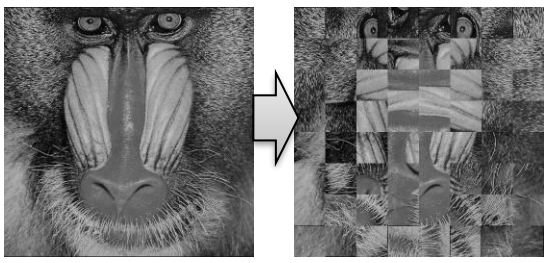

Figure. 1 Sample result after rotate zoning image

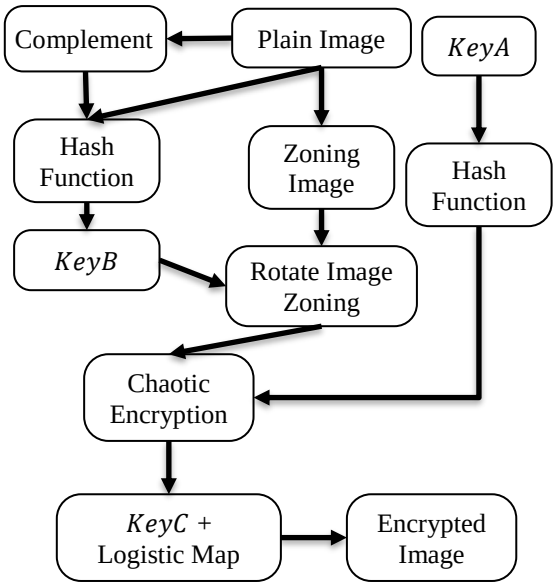

Figure. 2 Encryption Model

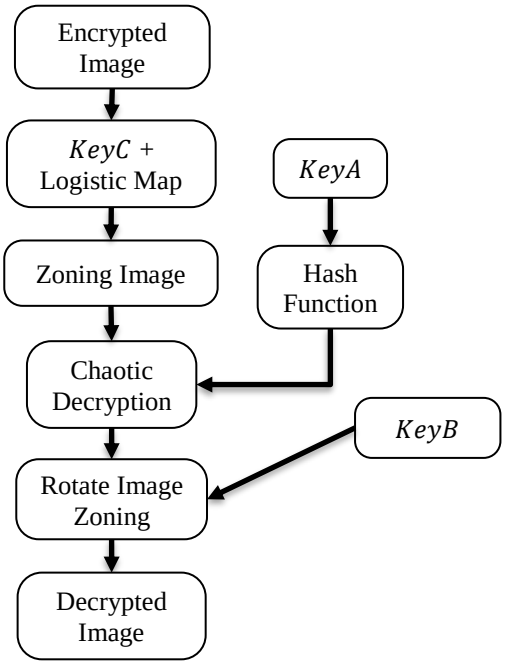

Figure. 3 Decryption model

9. Create L with a logistic map with Eq. (6).

$$L_{n+1} = round(keyC\ L_n(1 - L_n) \times 255) \quad (6)$$

Where L_0 is the initial value, $0 < L_0 < 1$, $keyC$ is the bifurcation parameter $0 < keyC < 4$, selected $keyC$ =3.99, while n=262144 is the logistic length.

10. Reshape the first stage of encryption into an array and then perform the XOR operation with L.
11. Get the encrypted image by reshaping the encrypted array.

To see in more detail all the encryption steps, see Fig. 2. At the decryption stage, it is explained in detail as follows:

1. Use the encrypted image as the first input, then reshape the encrypted image into an array.
2. Perform the 8th step in the encryption process, to create an array logistic map.
3. Perform XOR operation on L and array encrypted image. Then reshape the results of the XOR operation into an image with a size of $M \times M$.
4. Do zoning image.
5. Enter $KeyA$, then perform the SHA512 hash operation. Then convert to ASCII numbers. To get the values of p, q and r use Eq. (2), Eq. (3), and Eq. (4).
6. Perform chaotic decryption on each image zone based on the values of p, q and r using Eq. (7).

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}^{-1} \begin{bmatrix} x' \\ y' \end{bmatrix} mod\ M \qquad (7)$$

7. Enter $KeyB$ to derotate each decrypted image zone so that a complete decrypted image is obtained.

For more clearly the method of decryption can be seen in Fig. 3. For the note, the above process is carried out for grayscale images. In RGB images, the same process is carried out on each color channel.

4. Results and analysis

At this stage the proposed encryption model is tested on a public dataset that has been applied to previous research, the aim is to find out how much contribution is generated. The image dataset used is presented in Fig. 4. The image dataset used consists of 13 images, all of which have dimensions of 512×512 pixels, where 10 images are standard images with two types of models, namely grayscale and RGB, while the other three images are batik images. Batik is one of the original cultural heritage of Indonesia. This batik image is used in this study because in this research it is one of the research branches created by the author in developing Batik research, which has previously been published in research [24, 25]. The goal is to develop the security of storing batik images. Furthermore, the encryption model is implemented on each image so that the resulting encrypted image is presented in Fig. 5.

Visually the results presented in Fig. 5 have a broken display and have no correlation with the original image, this means that the resulting encryption is good. However, the visual display does not have a definite value so that more measurable measurements are needed. Therefore, several measures are used, the first is information entropy.

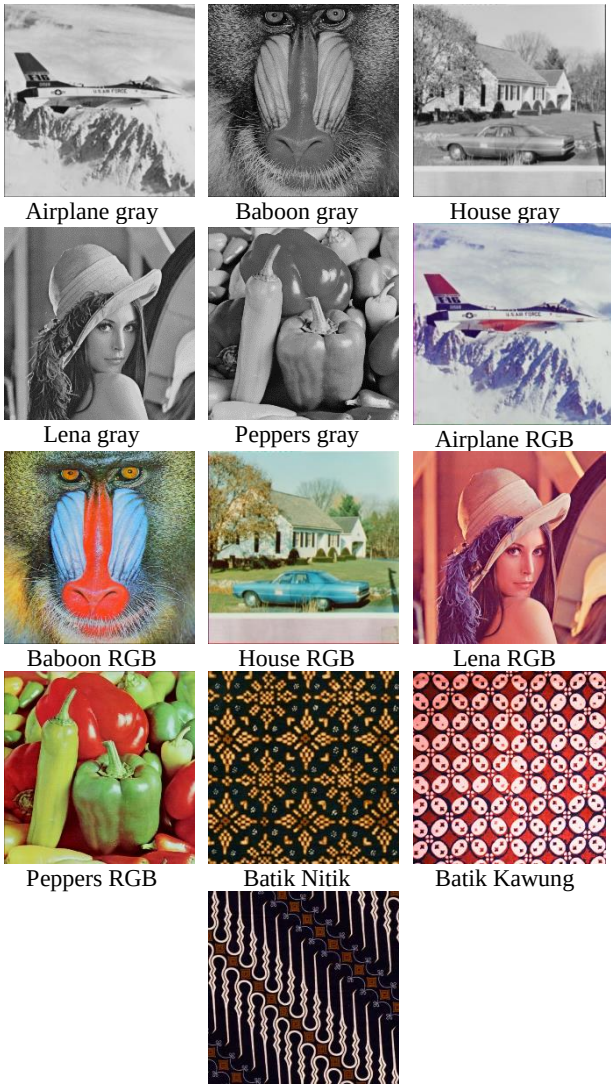

Figure. 4 Image dataset

Information entropy is a measuring tool used to calculate the randomness value of an image. The encrypted image should have a greater entropy value than the original image. The maximum value of entropy is 8, and if the entropy of the encrypted image has a value that is getting closer to 8, it means that the encryption results based on entropy are very good.[26]. The entropy value can be calculated by Eq. (8), while the calculation results are presented in Table 1.

$$H_i = -\sum_{0}^{2^8-1} p_i \, log_2(p_i) \qquad (8)$$

Where H_i is entropy, p_i and $log_2 p_i$ refer to the

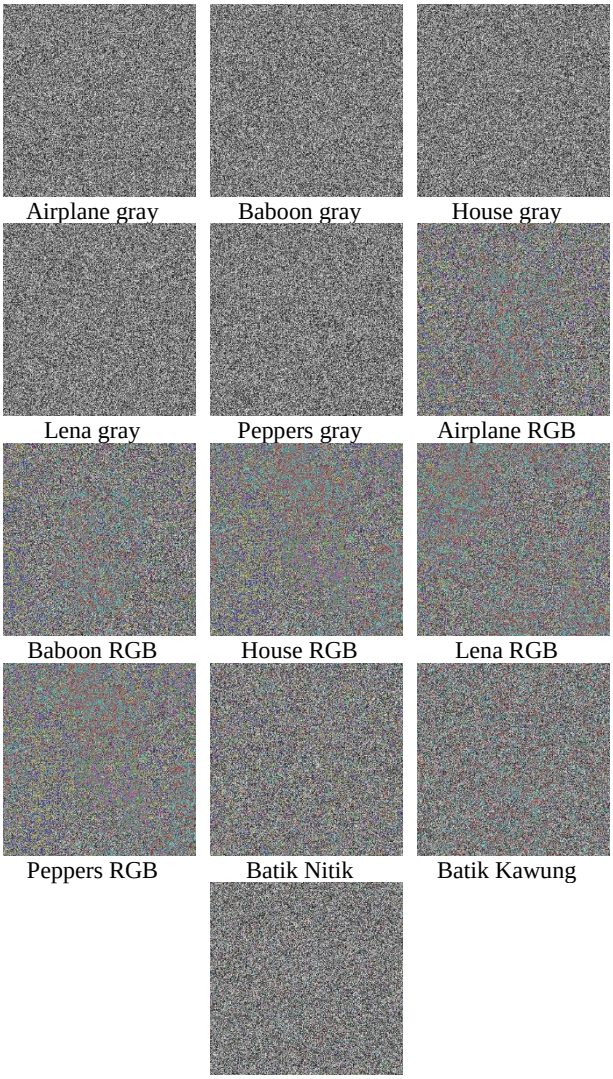

Figure. 5 Encrypted image results

Table 1. Entropy results

Image	Entropy	
	Before Encryption	After Encryption
Airplane gray	6.7025	7.9997
Baboon gray	7.3771	7.9996
House gray	7.2334	7.9995
Lena gray	6.8677	7.9998
Peppers gray	7.5937	7.9997
Airplane RGB	6.6639	7.9997
Baboon RGB	7.7624	7.9996
House RGB	7.4858	7.9997
Lena RGB	7.7502	7.9998
Peppers RGB	7.6698	7.9998
Batik Kawung	7.4148	7.9997
Batik Nitik	7.0165	7.9996
Batik Parang	6.6716	7.9997
Average	7.2469	7.9997

Table 2. Entropy comparison in lena color image

Approach	Entropy
Research [27]	7.9993
Research [28]	7.9993
Research [29]	7.6635
Research [3]	7.9997
Proposed	7.9998

Table 3. Entropy comparison in lena gray image

Method in	Entropy
Research [30]	7.9972
Research [5]	7.9976
Research [31]	7.9993
Research [3]	7.9993
Proposed	7.9998

probability of the occurrence of the symbol i and base 2 logarithms, respectively

Based on the results presented in Table 1, it appears that there is a significant increase in the entropy results. The entropy value is very close to 8, this means that the entropy-based image encryption security is proven to be good. In addition, this study also carried out several comparisons with other related methods, the comparison of entropy is presented in Table 2.

The second test was performed using NPCR and UACI values. Both of these measuring tools serve to measure encryption resistance against differential attacks. Both of these measuring instruments can be used by using two encrypted images (E1 and E2) which are generated by replacing the 1-bit plain image. NPCR stands for the number of pixels change rate which can be calculated by Eq. (9), while UACI stands for Unified Average Changing Intensity which can be calculated by Eq. (10) [32]. The ideal value of NPCR is 99.6093 and UACI is 33.4635 [33]. The results of the NPCR and UACI measurements are presented in Table 4.

$$NPCR = \left(\frac{1}{M \times N} \sum_{x=0}^{M} \sum_{y=0}^{N} D(x,y) \right) \qquad (9)$$
$$D(x,y) = \begin{cases} 0, E_1(x,y) = E_2(x,y) \\ 1, otherwise \end{cases}$$

$$UACI = \left(\frac{1}{M \times N} \sum_{x=0}^{M} \sum_{y=0}^{N} \frac{| E_1(x,y) - E_2(x,y)|}{(2^8) - 1} \right) \qquad (10)$$

For the record, the NPCR and UACI values

Table 4. UACI and NPCR results

Image	UACI	NPCR
Airplane gray	33.5114	99.5682
Baboon gray	33.4192	99.6168
House gray	33.4331	99.5897
Lena gray	33.4517	99.5904
Peppers gray	33.5251	99.6487
Airplane RGB	33.3909	99.6234
Baboon RGB	33.4287	99.5979
House RGB	33.4321	99.6368
Lena RGB	33.5098	99.6016
Peppers RGB	33.4097	99.5897
Batik Kawung	33.4354	99.5946
Batik Nitik	33.4134	99.6319
Batik Parang	33.4314	99.6213
Average	33.4455	99.6085

Table 5. UACI and NPCR comparison in lena color image

Approach	UACI	NPCR
Research [27]	33.2800	99.6000
Research [28]	33.4707	99.6098
Research [29]	33.4254	99.6082
Research [3]	33.2349	99.6009
Proposed	33.5098	99.6016

Table 6. UACI and NPCR comparison in lena gray image

Approach	UACI	NPCR
Research [34]	33.2161	99.4602
Research [5]	28.6600	99.6400
Research [31]	33.4197	99.6213
Research [3]	33.4192	99.6212
Proposed	33.4517	99.5904

presented on the RGB image are the average values of the R, G, and B layers in each image, while the plaintext modification of the image is located at location 256,256.

Our third test measures the avalanche effect (AE). AE is also a measuring tool to determine the resilience of differentials such as NPCR and UACI, the difference is that AE tends to use small modifications (usually 1-bit) in the password, then compared to two encrypted images (E1 and E2). In this method, modifications are made to $keyA$ (see Fig. 2. AE can be calculated with Eq. (11), where the ideal AE value is 50%. In this study, the AE value was calculated in three trials, where modifications of the 1-bit password were performed at the front, middle, and end. AE test results are presented in Table 7.

Table 7. Avalanche effect results

Image	Bit Password Modification in (%)		
	Initial	Middle	Last
Airplane gray	50.0109	50.0034	50.0311
Baboon gray	50.0192	50.0426	50.0415
House gray	50.0139	50.1075	50.0438
Lena gray	50.0172	50.0213	50.0091
Peppers gray	50.0560	50.0228	50.0239
Airplane RGB	50.0312	49.9950	50.0118
Baboon RGB	49.9892	50.0002	50.0104
House RGB	50.0514	50.0241	50.0023
Lena RGB	50.0018	50.0103	50.0114
Peppers RGB	49.9985	50.0391	49.9986
Batik Kawung	50.0053	49.9981	50.0218
Batik Nitik	50.0108	50.0396	50.0275
Batik Parang	50.0518	50.0057	49.9892
Average	50.0198	50.0238	50.0171
Average all	50.0202		

Table 8. Avalanche effect comparison in lena image

Approach	Image Type	Avalanche Effect (%)
Research [35]	Color	50.0123
Research [3]	Color	49.9822
Proposed	Color	50.0159
Research [5]	Gray	49.9767
Research [3]	Gray	50.0366
Proposed	Gray	50.0078

$$AE = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N} D_{x,y}}{M \times N} \times 100\%, \quad D_{x,y}\begin{cases} E_1(x,y) \neq E_2(x,y), 1 \\ E_1(x,y) = E_2(x,y), 0 \end{cases} \tag{11}$$

The fourth test is carried out histogram analysis and chi-square test, the aim is to determine the encryption resistance of statistical attacks [6]. Visually, the histogram that looks uniform and has a significant difference from the original image histogram indicates that the quality of the proposed encryption is very good. Histogram results from image encryption are presented in Fig. 6. Even though the chi-square (χ^2) measurement used to validate this quality. The value of chi-square can be calculated by Eq. (12), and the results of the calculations are presented in Table 9.

$$\chi^2 = \sum_{x=1}^{i} \frac{(f_x - g_x)^2}{g_x} \tag{12}$$

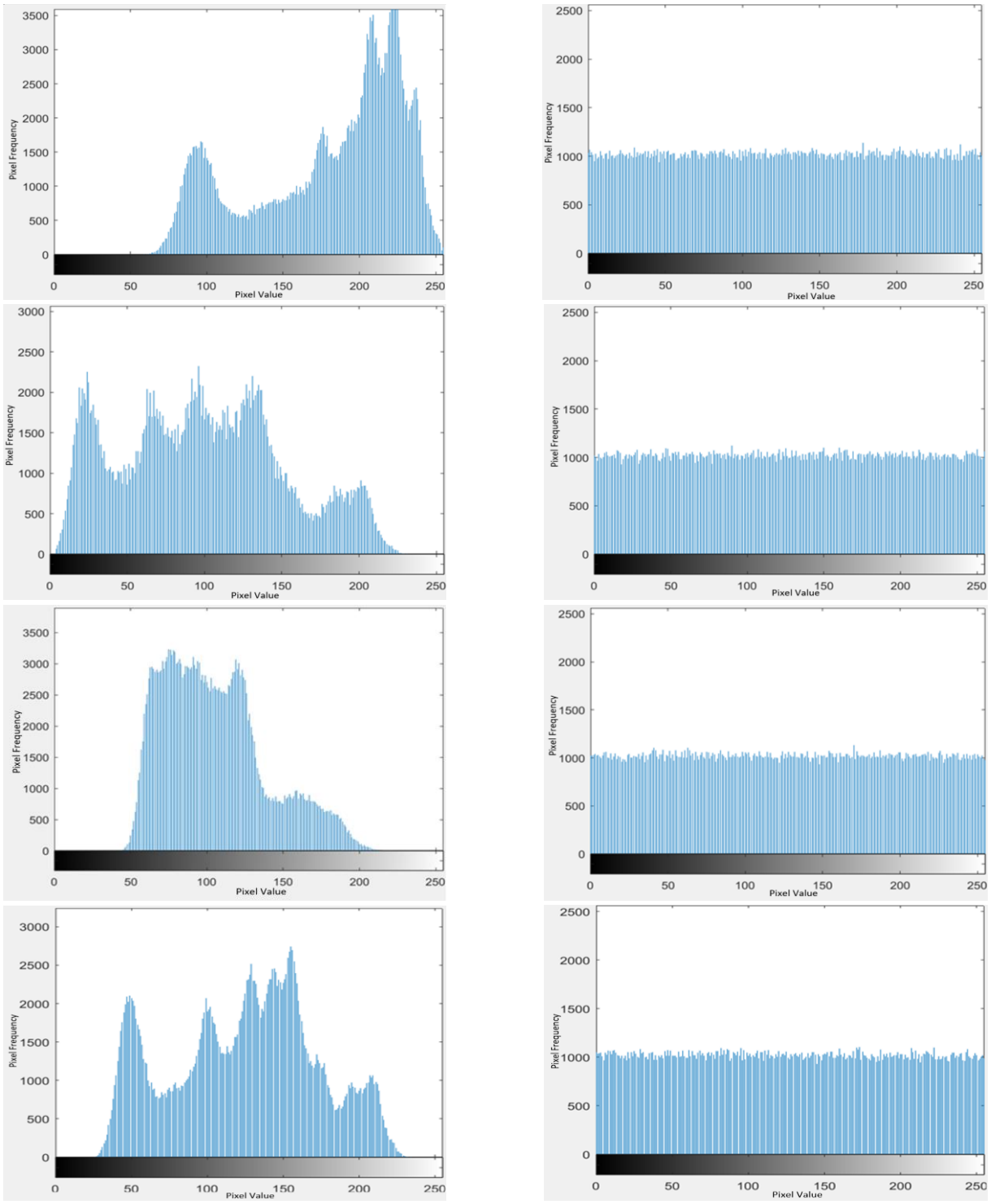

Figure. 6 Sample histogram of Lena image, the first column is the original histogram, the second column is an encrypted histogram, the first row is red channel, the second row is green channel, the third row is the blue channel, the fourth row is the gray channel

Where i is gray-level, g_x is the pixel frequency of each gray value to the theoretical histogram, f_x is the pixel frequency of each gray value concerning the actual histogram, χ^2 represents the degree of deviation between the tested histogram and the ideal histogram. When the significant level is 0.05, then $\chi^2_{0.05}(255) = 293.24783$, so when the value of χ^2 encrypted image $< \chi^2_{0.05}$ can be concluded the histogram is approximately uniform.

Based on the results presented in Table 9, it appears that 10 of the 13 images have the ideal chi-

Table 9. Chi-square results

Image	χ^2
Airplane gray	**315.7288**
Baboon gray	286.3879
House gray	277.9237
Lena gray	289.7390
Peppers gray	**310.3829**
Airplane RGB	257.1270
Baboon RGB	286.8623
House RGB	**298.8913**
Lena RGB	291.2394
Peppers RGB	283.3699
Batik Kawung	290.3876
Batik Nitik	271.2368
Batik Parang	283.9238
Average	287.9385
Pass Rate	10/13

Table 10. Decryption measurements

Image	BER	PSNR	SSIM
Airplane gray	0	∞	1
Baboon gray	0	∞	1
House gray	0	∞	1
Lena gray	0	∞	1
Peppers gray	0	∞	1
Airplane RGB	0	∞	1
Baboon RGB	0	∞	1
House RGB	0	∞	1
Lena RGB	0	∞	1
Peppers RGB	0	∞	1
Batik Kawung	0	∞	1
Batik Nitik	0	∞	1
Batik Parang	0	∞	1
Pass Rate	13/13		

square value, while the other 3 have not yet obtained the ideal chi-square value. However, the value of the three images has a chi-square value which is not too far from the ideal, so it can be concluded that this method has satisfactory results based on the chi-square.

The last test is the image decryption process, the aim is to determine the performance of the decryption process. The encrypted image must be completely decrypted so as not to change the meaning of the image. Therefore, to find out the decrypted image needs to be measured by bit error ratio (BER), peak signal to noise ratio (PSNR), and structural similarity index (SSIM). These three measuring instruments are widely used in various image security methods, such as cryptography and steganography [5, 36].

$$BER = \frac{\sum_{z=1}^{O} d_z}{M \times N \times 8}, \quad d_z \begin{cases} D_z \neq P_z, 1 \\ D_z = P_z, 0 \end{cases} \tag{13}$$

BER serves to find out if there are errors that occur in the image bits, how to change the described image (D) and plain image (P) into binary form and reshape it into a 1-D array and then compare each bit at the same z index, which is calculated with Eq. (13). The BER value must be 0 to get perfect decryption. While the PSNR is to find out how much noise occurs in the image encryption and decryption process, the value indicates that there is no noise in the described image. While SSIM is to check the image structure, if the value is 1 then the described image structure is the same as the plain image. These three measuring tools compare the plain image and the described image, where PSNR can be calculated by Eq. (14) and SSIM is calculated by Eq. (15).

$$PSNR = 10 \log_{10} \left(\frac{255}{\frac{1}{M\ x\ N} \sum_{x}^{M} \sum_{y}^{N} [P(x,\mathrm{y}) - D(x,\mathrm{y})]^2} \right) \tag{14}$$

$$SSIM\ (P, C) = \frac{(2\mu_P \mu_D + v_1)(2\sigma_{PD} + v_2)}{(\mu_P^2 + \mu_D^2 + v_1)(\sigma_P^2 + \sigma_D^2 + v_2)} \tag{15}$$

Where μ_P is mean of the P; μ_D is mean of the D; σ_{PD} is the covariance P against D; σ_P^2 is a variant of P; σ_D^2 is a variant of D; $v_1 = (l_1 D)^2$ and $v_2 = (l_2 D)^2$; D is a dynamic range $(2^{bits} - 1)$ with the default value $l_1 = 0.01$ dan $l_2 = 0.03$

5. Discussion

In section 4 it can be seen that there are several comparisons of the methods presented. Comparison of color images and gray images. The comparison is done on the same dataset, namely the image of Lena. The previous encryption methods generally used a combination of diffusion and confusion methods. It can be seen that the proposed method is not entirely dominant, but after analyzing the results, it appears that the resulting method has very satisfactory values from various measurements. Based on statistical testing using the entropy value, all encrypted images have a value that is very close to the maximum value. The average value of entropy is very good, which is 7.9997. Meanwhile, for Lena's image with both

grayscale and color types, the results look better than the previous methods, see Table 2 and Table 3, this means that the proposed method has a dominant contribution based on the entropy measurement tool. Other statistical measuring tools used are histogram and chi-square analysis. Visually based on the histogram, there was a significant histogram change besides the histogram pattern looked uniform in the bit distribution from 0 to 255. Based on the chi-square value, three images still did not pass, but the average chi-square value of the 13 images showed that the histogram is relatively uniform.

Based on the differential attack test using UACI, NPCR, and AE measurements. It can be seen that this method is very superior because the average value of UACI and NPCR produced is very close to the ideal value (UACI = 33.4635, NPCR = 99.6093), even when compared to the previous method in both grayscale and color images, especially in the Lena image. The proposed method looks superior, see Table 5 and Table 6. Meanwhile, the AE value is also very good because the average AE value is close to the ideal value (50%).

At the decryption stage, the proposed method is proven to be able to carry out a perfect decryption process. This is evidenced by all images capable of producing a BER = 0, which indicates that there is no error in the bit value of the image, PSNR =∞ which means that there is no noise at all and, SSIM = 1 which means that there is no change in the image structure of the entire image after going through the encryption and decryption process.

These results prove that the proposed method produces a relatively better performance than the previous method. This is caused by gradual encryption and is performed in each local area of the image. In the initial encryption, each image area is encrypted with the same method but with a dynamic key based on the plain image hashing function, in the next stage, an XOR operation is carried out based on the logistic map and $keyC$ of this section which increases the strength of statistical attacks. In addition, the hashing function on the key also increases the strength of the differential attack as evidenced by the UACI and NPCR values.

6. Conclusions

This study proposes an encryption model that combines two chaos methods with two hash functions. The first chaos method is carried out with zoning and rotation techniques based on key hash functions and plain text to create local encryption for each image zone. Furthermore, the overall encryption is carried out on the image with a logistic map. This encryption model uses the confusion process with the chaotic system in each image zone in the first step and the diffusion process in the second chaotic system is carried out thoroughly. Gradual encryption techniques have been shown to have a positive effect, so that this method can produce encrypted images that are resistant to statistical and differential attacks as evidenced by the measurement results of the average entropy = 7.9997, NPCR = 99.6085, UACI = 33.4455, avalanche effect = 50.0202, relatively very uniform histogram, and chi-square analysis which has a pass rate of 10/13. In addition, all decryption processes can run perfectly as evidenced by measurements of BER=0, PSNR=∞, and SSIM=1. In the future, this method can certainly be developed to be even stronger, for example by using more key combinations, as well as more complex combinations of chaotic systems. However, it is also necessary to measure the efficiency of the method against computational costs.

Conflicts of interest

We wish to confirm that there are no known conflicts of interest associated with this publication and there has been no significant financial support for this work that could have influenced its outcome. We confirm also that the manuscript has been read and approved by all named authors and that there are no other persons who satisfied the criteria for authorship but are not listed.

References

[1] A. Setyono and D. R. I. M. Setiadi, “An Image Watermarking Method Using Discrete Tchebichef Transform and Singular Value Decomposition Based on Chaos Embedding”, *International Journal of Intelligent Engineering and Systems*, Vol. 13, No. 2, pp. 140–150, 2020, doi: 10.22266/ijies2020.0430.14.

[2] X. Zhang, L. Wang, G. Cui, and Y. Niu, “Entropy-Based Block Scrambling Image Encryption Using DES Structure and Chaotic Systems”, *Int. J. Opt.*, 2019, doi: 10.1155/2019/3594534.

[3] F. Budiman and D. R. I. M. Setiadi, “A Combination of Block-Based Chaos with Dynamic Iteration Pattern and Stream Cipher for Color Image Encryption”, *International Journal of Intelligent Engineering and Systems*, Vol. 13, No. 6, pp. 132–141, 2020, doi: 10.22266/ijies2020.1231.12.

[4] S. Kandar, D. Chaudhuri, A. Bhattacharjee, and B. C. Dhara, “Image encryption using sequence generated by cyclic group”, *J. Inf. Secur. Appl.*,

Vol. 44, pp. 117–129, 2019, doi: 10.1016/J.JISA.2018.12.003.

[5] A. Susanto, D. R. I. M. Setiadi, E. H. Rachmawanto, I. U. W. Mulyono, C. A. Sari, M. K. Sarker, and M. R. Sazal, "Triple layer image security using bit-shift, chaos, and stream encryption", *Bull. Electr. Eng. Informatics*, Vol. 9, No. 3, pp. 980–987, 2020, doi: 10.11591/eei.v9i3.2001.

[6] S. Koppu and M. Viswanatham, "2D Chaotic Map Based on 2D Adaptive Grey Wolf Algorithm for Ultra Sound Medical Image Security", *International Journal of Intelligent Engineering and Systems*, Vol. 10, No. 1, 2017, doi: 10.22266/ijies2017.0228.12.

[7] B. Harjo and D. R. I. M. Setiadi, "Improved Color Image Encryption using Hybrid Modulus Substitution Cipher and Chaotic Method", *International Journal of Intelligent Engineering and Systems*, Vol. 14, No. 2, pp. 157–165, 2021, doi: 10.22266/ijies2021.0430.14.

[8] A. P. Kari, A. H. Navin, A. M. Bidgoli, and M. Mirnia, "A novel multi-image cryptosystem based on weighted plain images and using combined chaotic maps", *Multimed. Syst.*, Vol. 27, No. 5, pp. 907–925, 2021, doi: 10.1007/s00530-021-00772-y.

[9] R. Lan, J. He, S. Wang, T. Gu, and X. Luo, "Integrated chaotic systems for image encryption", *Signal Processing*, Vol. 147, pp. 133–145, 2018, doi: 10.1016/J.SIGPRO.2018.01.026.

[10] C. Chen, K. Sun, and S. He, "An improved image encryption algorithm with finite computing precision", *Signal Processing*, Vol. 168, p. 107340, 2020, doi: 10.1016/j.sigpro.2019.107340.

[11] Y. Luo, X. Ouyang, J. Liu, and L. Cao, "An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems", *IEEE Access*, Vol. 7, pp. 38507–38522, 2019, doi: 10.1109/ACCESS.2019.2906052.

[12] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps", *Opt. Lasers Eng.*, Vol. 78, pp. 17–25, 2016, doi: 10.1016/J.OPTLASENG.2015.09.007.

[13] M. Kanafchian and B. F. Vajargah, "A Novel Image Encryption Scheme Based on Clifford Attractor and Noisy Logistic Map for Secure Transferring Images in Navy", *Int. J. E-Navigation Marit. Econ.*, Vol. 6, pp. 53–63, 2017, doi: 10.1016/J.ENAVI.2017.05.007.

[14] C. Fu, G. Y. Zhang, M. Zhu, Z. Chen, and W. M. Lei, "A New Chaos-Based Color Image Encryption Scheme with an Efficient Substitution Keystream Generation Strategy", *Secur. Commun. Networks*, Vol. 2018, 2018, doi: 10.1155/2018/2708532.

[15] M. Ge and R. Ye, "A novel image encryption scheme based on 3D bit matrix and chaotic map with Markov properties", *Egypt. Informatics J.*, Vol. 20, No. 1, pp. 45–54, 2019, doi: 10.1016/J.EIJ.2018.10.001.

[16] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map", *Signal Processing*, Vol. 143, pp. 122–133, 2018, doi: 10.1016/J.SIGPRO.2017.08.020.

[17] M. Naim, A. A. Pacha, and C. Serief, "A novel satellite image encryption algorithm based on hyperchaotic systems and Josephus problem", *Adv. Sp. Res.*, Vol. 67, No. 7, pp. 2077–2103, 2021, doi: 10.1016/J.ASR.2021.01.018.

[18] 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.

[19] 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.

[20] D. Wei and M. Jiang, "A fast image encryption algorithm based on parallel compressive sensing and DNA sequence", *Optik (Stuttg).*, Vol. 238, p. 166748, 2021, doi: 10.1016/J.IJLEO.2021.166748.

[21] J. I. M. Bezerra, V. V. D. A. Camargo, and A. Molter, "A new efficient permutation-diffusion encryption algorithm based on a chaotic map", *Chaos, Solitons & Fractals*, Vol. 151, p. 111235, 2021, doi: 10.1016/J.CHAOS.2021.111235.

[22] X. Wang and Y. Chen, "A New Chaotic Image Encryption Algorithm Based on L-Shaped Method of Dynamic Block", *Sens. Imaging*, Vol. 22, No. 1, 2021, doi: 10.1007/s11220-021-00357-z.

[23] H. Diab, "An Efficient Chaotic Image Cryptosystem Based on Simultaneous Permutation and Diffusion Operations", *IEEE Access*, Vol. 6, pp. 42227–42244, 2018, doi: 10.1109/ACCESS.2018.2858839.

[24] F. Budiman, A. Suhendra, D. Agushinta, and A. Tarigan, "Determination of SVM-RBF kernel space parameter to optimize accuracy value of Indonesian Batik images classification", *J. Comput. Sci.*, Vol. 13, No. 11, pp. 590–599, 2017, doi: 10.3844/jcssp.2017.590.599.

[25] F. Budiman, "SVM-RBF parameters testing optimization using cross validation and grid search to improve multiclass classification", *Sci. Vis.*, Vol. 11, No. 1, pp. 80–90, 2019, doi: 10.26583/sv.11.1.07.

[26] X. Wang and H. Sun, "A chaotic image encryption algorithm based on improved Joseph traversal and cyclic shift function", *Opt. Laser Technol.*, Vol. 122, p. 105854, 2020, doi: 10.1016/j.optlastec.2019.105854.

[27] X. L. Chai, Z. H. Gan, Y. Lu, M. H. Zhang, and Y. R. Chen, "A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system - IOPscience", *Chinese Phys. B*, Vol. 25, 2016.

[28] 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.

[29] A. U. Rehman, X. Liao, R. Ashraf, S. Ullah, and H. Wang, "A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2", *Optik (Stuttg).*, Vol. 159, pp. 348–367, 2018, doi: 10.1016/j.ijleo.2018.01.064.

[30] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation", *Opt. Lasers Eng.*, Vol. 90, pp. 238–246, 2017, doi: 10.1016/j.optlaseng.2016.10.020.

[31] A. Babaei, H. Motameni, and R. Enayatifar, "A new permutation-diffusion-based image encryption technique using cellular automata and DNA sequence", *Optik (Stuttg).*, Vol. 203, p. 164000, 2020, doi: 10.1016/j.ijleo.2019.164000.

[32] 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.

[33] Y. Jain, R. Bansal, G. Sharma, B. Kumar, and S. Gupta, "Image Encryption Schemes: A Complete Survey", *Int. J. Signal Process.*, Vol. 9, No. 7, pp. 157–192, 2016, doi: 10.14257/ijsip.2016.9.7.15.

[34] A. Bakhshandeh and Z. Eslami, "An authenticated image encryption scheme based on chaotic maps and memory cellular automata", *Opt. Lasers Eng.*, Vol. 51, No. 6, pp. 665–673, 2013, doi: 10.1016/j.optlaseng.2013.01.001.

[35] S. M. Seyedzadeh and S. Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map", *Signal Processing*, Vol. 92, No. 5, pp. 1202–1215, 2012, doi: 10.1016/j.sigpro.2011.11.004.

[36] 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.