Securing Digital Color Image based on Hybrid Substitution Cipher

Moch. Sjamsul Hidajat*[1], **Ichwan Setiarso**[2]
STMIK Kadiri Kediri Jawa Timur Indonesia
*E-mail : gus.sjamsul@gmail.com**[1]*, ichwan10stmik@gmail.com*[2]
**Corresponding author*

Abstract - This study proposes securing digital color images with hybrid substitution cryptographic methods combined with the Vigenere and Beaufort methods. The hybrid process is carried out using the help of two randomly generated keys. The first key is a matrix with an 8-bits value and the second key is a matrix with a binary value. The binary key is used to determine the Vigenere or Beaufort process, while the 8-bit key is used for modulus operations based on the Vigenere or Beaufort algorithm. At the test stage used a standard image that has an RGB color channel as a dataset. The quality of the cryptographic method is measured by several measuring instruments such as MSE, PSNR, and SSIM to determine the quality of encryption visually and the perfection of decryption, besides that it is used Entropy, NPCR and UACI to determine the probability of encryption resistance and quality against differential attacks. The TIC TOC function is also used to measure the computing speed of the encryption and decryption process. Measurement results using all measuring instruments indicate that the proposed method has very satisfying results and has fast computing.

Keywords – Cryptography**,** Substitution Cipher, Modulus Function, Encryption, Decryption, Image Transmission

1. INTRODUCTION

Nowadays the digital multimedia landscape has changed due to the increasingly modern technology and many positive things but also an unexpected problem related to the security of sending multimedia data in cyberspace. Not a few cases of theft, the theft that occurs in the cyber world, so it needs special attention to data security. Cryptography is one solution that can be used to secure multimedia data[1]–[3]. Cryptography is a study that is used to secure data by encoding the data. The process of coding data will change the form that can be random or become another form that has a different meaning from the original data so that the data cannot be read directly[1], [4], [5]. The encryption process and the decryption process are the two main processes in cryptography, where encryption is used to encode data while decryption is used to return the encoded data to its original form[6].

In cryptographic research, there are many digital files that have been used as objects, where digital image files are one of the favorite objects that have been studied in various cryptographic researches today[7]–[11]. This research also focuses on digital image cryptography. In various image cryptographic research previously, chaos methods have been proposed to do scramble on images, this method is also often called permutation or diffusion method. Another method that is very favorite is the substitution method[12]. The popular algorithm in this chaotic method is Chaotic Map[13]. While the algorithms that are widely used in the substitution method are RC4, Vernam, Vigenere, Beaufort, Caesar, etc[3], [14]–[20]. In research on comparative studies of several cryptographic algorithms conducted by Setiadi et al

[19], It is stated that the chaos method is superior to blueness and diffusion, but has a slower computation due to a number of iterations performed. The number of iterations plays an important role in the speed of computation, so if iterations are set up quite a lot then the performance will slow down. Another disadvantage of the chaotic method is that the image histogram does not change because the pixel value does not change only the position of the scrambled pixels. In contrast to the chaotic method, RC4 and OTP have advantages in the process of image encryption based on several measuring tools such as entropy analysis, Number of Pixel Change Rate (NPCR), unified average change in intensity (UACI), visually Structural Similarity Index (SSIM) and Peak values Signal to Noise Ratio (PSNR) refers to more random visuals. Whereas the fastest computing speed is in the OTP method.

OTP is a substitution cryptographic algorithm that is also popularly known as Vernam cipher. The XOR operator or modulo operation is the main operation in the encryption and decryption process [1]. Vernam cipher is an improvement of the Vigenere cipher algorithm, where random keys are used as the main component in encryption and decryption. Vernam's algorithm is very powerful against attacks so it is difficult to decrypt without knowing the key used. The quality of this algorithm depends on the key chosen. To get strong encryption results, the selected key must be ensured to be truly random, used only once, and guaranteed secrets. The algorithm also has simple, fast and powerful operations so that it can be continuously developed and combined to increase resistance to attacks[20]. Beaufort cipher offers a Vigenere-derived algorithm built on a subtraction operation. Both the encryption and decryption processes use subtraction operations as the main operation based on modulus operations[21]. Based on these theories, this research uses a hybrid cipher substitution method which is inspired by Vigenere and Beaufort algorithms by utilizing two random keys

2. LITERATURE REVIEW

Cryptography is the science of encoding data that has been used from the past until now with the aim of securing secret messages. The classic cryptographic method that is popular until now is the method of substitution, the way to change the meaning and content of messages based on the key. In the method of substitution, the quality of the key will largely determine the quality of the encryption results, the better the quality of the key, the stronger the encryption results.

One of the substitution methods that was very popular in its time was Vigenere cipher. In the early days of the encryption and decryption process utilizing the tabula recta table. This method continues to be developed, then by Gilbert Vernam, modifications are made using random keys so that the encryption results become stronger. The modification of the Vigenere cipher by Gilbert Vernam is now known as the Vernam cipher[1], [3]. The encryption formula in Vernam cipher is presented in Eq. (1) and Eq. (2) presents the decryption formula.

$$B = (A + k) \ mod \ 256 \qquad (1)$$

$$A = (B - k) \ mod \ 256 \qquad (2)$$

where:

B is cipher image, A is plain image, k is key.

For the note, the value of k has a range of 0-255. This value is obtained because the image pixel value is 8-bits so to get this value a modulo operation with the number 256 is performed. The popularity of the Vigenere cipher made this method developed and modified, one of the results of the modification of the Vigenere cipher was the Beaufort cipher. This method is similar to Vigenere cipher but uses a combination of subtraction and modulus techniques as the main operation, both in the encryption and decryption process [21]. In the encryption process, the subtraction is done on the key with plaintext while in the decryption process the subtraction is done on the key with the ciphertext. For more details, see formula (3) for Beaufort's encryption process and formula (4) for Beaufort's decryption.

$$B = (k - A) \; mod \; 256 \qquad (3)$$

$$A = (k - B) \; mod \; 256 \qquad (4)$$

3. PROPOSED METHOD

The section describes the proposed method using hybrid Vigenere and Beaufort cipher. The method will be divided into two main processes, the encryption process, and the decryption process. The stages in the encryption process are presented in Fig. 1

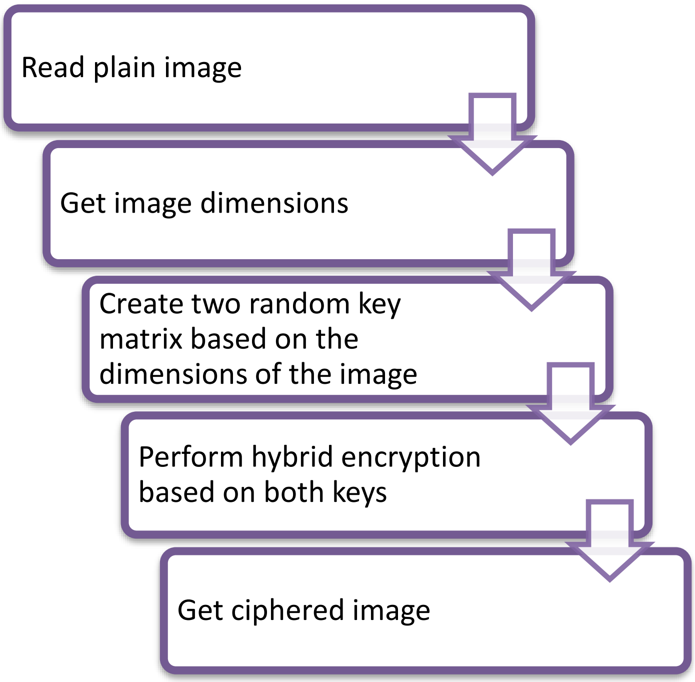

Read plain image
Get image dimensions
Create two random key matrix based on the dimensions of the image
Perform hybrid encryption based on both keys
Get ciphered image

Fig. 1. Encryption Process

Based on figure 1 can be explained in more detail with the steps in the encryption process as follows:

1. Read the plain image to be encrypted, then in a variable A.
2. Get the dimensions of the A image and save it to the variable d, e, f, where d is the width, e is height, and f is the image channel (RGB).
3. Create a first random key matrix with ranges 0 – 255 with dimensions $d \; * \; e$ using a random generator, then save it to the $k1$ variable
4. Create a second matrix containing random numbers with ranges 0-1 with dimensions $d \; * \; e$ using a random generator, then save it to the $k2$ variable.

5. Perform encrypt using formula (5)

$$C_{def} = \begin{cases} mod\left(\left(k1_{de} - A_{def}\right), 256\right), k2 = 1 \\ mod\left(\left(A_{def} + k1_{de}\right), 256\right), k2 = 0 \end{cases} \tag{5}$$

6. Get a ciphered image(C).

As for the stages of image decryption, see Fig.2 below.

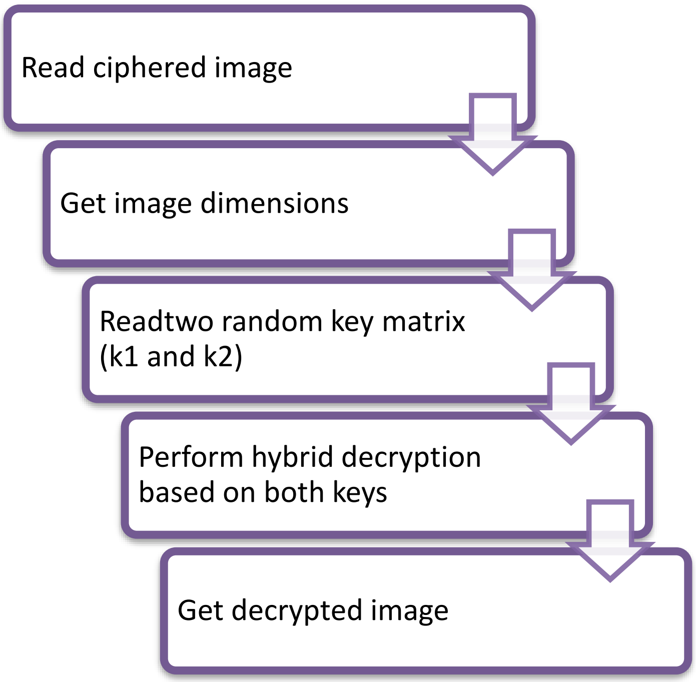

Read ciphered image
Get image dimensions
Readtwo random key matrix (k1 and k2)
Perform hybrid decryption based on both keys
Get decrypted image

Fig. 2. Decryption Process

Based on figure 2 can be explained in more detail with the steps in the decryption process as follows:

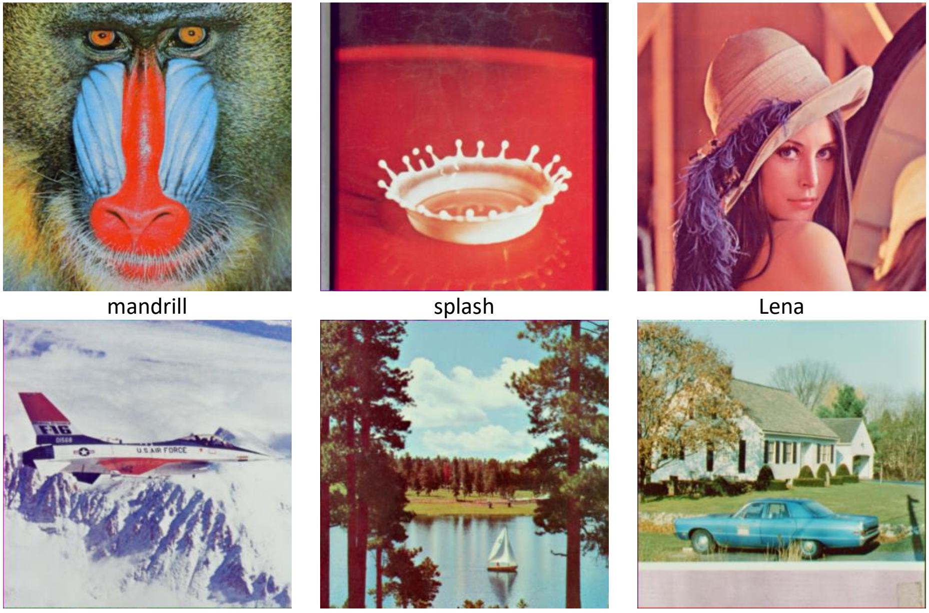
1. Read the encrypted image, save the image in variable C.
2. Get the dimensions of the C image and save it to d,e,f, where d is the width, e is height, and f is the image layer (RGB).
3. Read the first random key (k1) and the second random key (k2).
4. Perform decryption using formula (6):

$$B_{def} = \begin{cases} mod\left(\left(k1_{de} - C_{def}\right), 256\right), k2 = 1 \\ mod\left(\left(C_{def} - k1_{de}\right), 256\right), k2 = 0 \end{cases} \tag{6}$$

5. Get the decrypted image (B).

4. RESULTS AND DISCUSSION

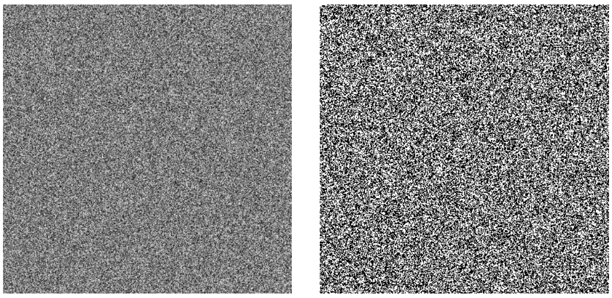
In this section, we use the 24-bit true-color image in the RGB color channel. The images used are a standard test image that can be downloaded at the SIPI image database website address[22]. Figure 3 shows the image used in this study. After all images have been downloaded, these images are used directly as a dataset to be tested and measured in the proposed method. All images taken from the website are not pre-processed, so the pixel values in the image do not change and in accordance with the original image, this is intended so that later this method will be easily compared.



mandrill splash Lena

airplane sailboat house

Fig. 3. Image Dataset used on this research



key 1 key 2

Fig. 4. Sample random key used in this research

All images have a dimension of 512 * 512, according to the dimensions of the original image. Before the encryption process is carried out, it takes the step of making two random keys as in the third step and the fourth step of the proposed method. Figure 4 is an example of a random key generated in this study. The first random key is a gray scale image and the second random key is a binary image. By using both random keys, the encryption process is carried out by formula (1). Encrypted images are then tested for encryption quality using several gauges such as entropy, MSE, PSNR, SSIM, UACI, and NPCR. Entropy (En) is a randomness feature that is used to measure the likelihood of (p) decrypted images[7]. Entropy can be calculated by the formula (7). MSE, PSNR, and SSIM are used to measure the quality of image encryption based on errors, noise, and structural changes in the image. Formulas (8), (9), and (10), each of which is used to calculate MSE, PSNR, and SSIM. UACI and NPCR are used to measure the encryption strength of differential attacks [19, 20]. Where the formula used to calculate UACI and NPCR is shown in formulas (11) and (12).

$$En = -\sum_{0}^{255} p \, log_2(p) \qquad (7)$$

$$MSE = \sum_{m=0}^{255}\sum_{n=0}^{255}\sum_{o=0}^{255} \| A(d,e,f) - C(d,e,f) \| \tag{8}$$

$$PSNR = 10\ log_{10}\left(\frac{(2^8) - 1}{\sqrt{MSE}}\right) \tag{9}$$

$$SSIM\ = \frac{(2\mu_C\mu_A + b_1)(2\sigma_{CI} + b_2)}{(\mu_C^2 + \mu_A^2 + b_1)(\sigma_C^2 + \sigma_A^2 + b_2)} \tag{10}$$

$$NPCR = \frac{1}{def}\sum_{m=0}^{255}\sum_{n=0}^{255}\sum_{o=0}^{255} G(def) * 100\%,$$
$$G(mno) = \begin{cases} 0, A(def) = C(def) \\ 1, A(def) \neq C(def) \end{cases} \tag{11}$$

$$UACI\ = \frac{1}{def}\sum_{m=0}^{255}\sum_{n=0}^{255}\sum_{o=0}^{255} \frac{|I(def) - C(def)|}{255} * 100\% \tag{12}$$

Where C is an encrypted image, A is the original image, d is the image width, e is the image height, and f is the number of layers, σ_{CA} is the image covariance A against C; σ_A^2 is a variant of image A; σ_C^2 is a variant of image C; $b_1 = (k_1L)^2$; $b_2 = (k_2L)^2$; L is a dynamic range of the image$(0 - 255)$ with the default value $k_1 = 0.01$ and $k_2 = 0.03$.

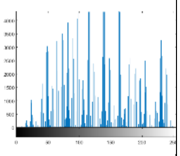
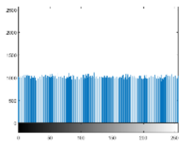
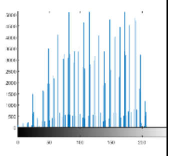
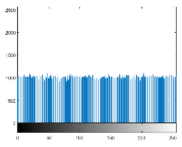
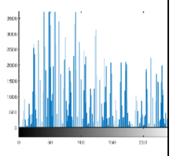
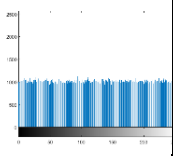
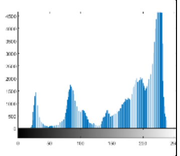
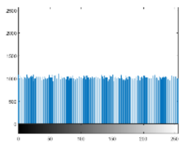
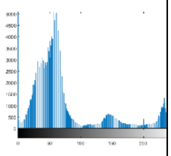
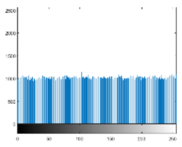
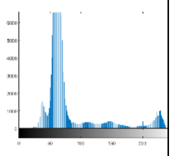
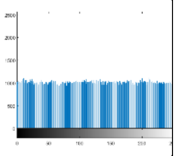
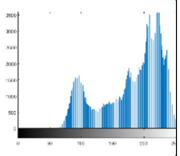
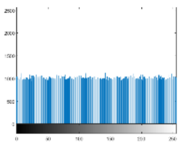
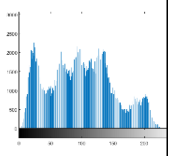
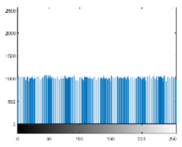
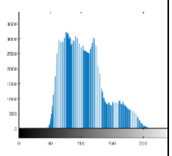
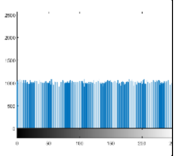
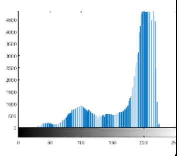
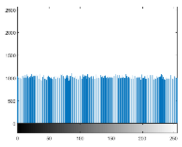
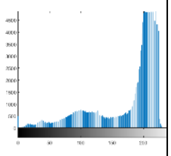
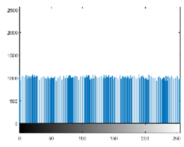
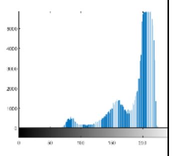
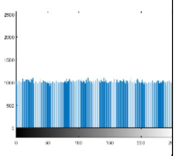
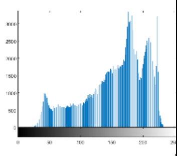
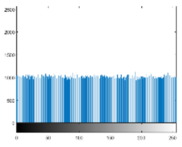
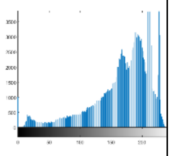
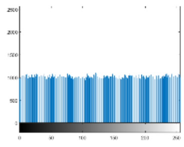
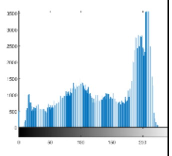
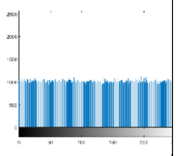
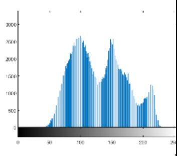
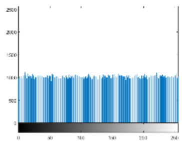
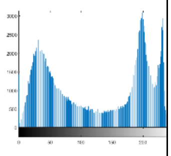
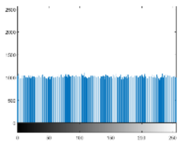
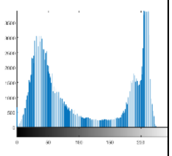
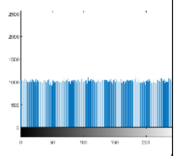
Table 1. Image Encryption Measurement

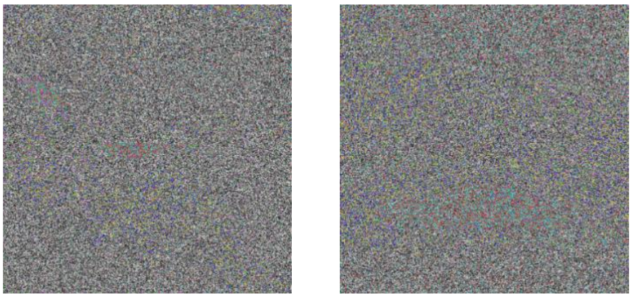
Image Name	Entropy	MSE	PSNR	SSIM	UACI	NPCR	Encrypting Time (seconds)
Airplane	7.9995	10226.3910	8.1813	0.0010	33.59%	99.61%	1.596500
House	7.9996	9051.9137	8.5685	0.0011	31.93%	99.78%	1.570584
Lena	7.9996	8742.4205	8.9163	0.0009	31.47%	98.98%	1.539926
Mandrill	7.9995	8785.4035	8.8932	0.0007	31.23%	99.69%	1.601654
Sailboat	7.9996	9986.3101	8.2935	0.0012	33.21%	99.71%	1.534602

The results of the encrypted image measurements are presented in table 1. Based on the observations of table 1, it can be seen that the entropy value produced has a nearly perfect value, which is close to 8.[19]. From these results, it was concluded that based on the entropy value of the encrypted image, it would be very difficult to do the decryption process without knowing the key used. Visually the encryption results also show very significant changes, so there is no correlation or meaning associated with the original image at all[23]. The results of MSE and PSNR measurements also emphasize the excellent quality of encryption due to the spread of errors and the amount of noise in the encrypted image. Likewise, the SSIM value is very close to zero, this means that the structure of the encrypted image really has no resemblance to the original image. In addition, the UACI and NPCR values also produce very good values, so it can be concluded that the encryption results will be resistant to various types of attacks. The computational performance of the algorithm is also measured in this research. The measuring instrument used is the tic toc function on the Matlab R2015a, which uses an AMD A12 7th Gen processor and 4GB of memory. The result, it only takes about 1.5 seconds to do the encryption process. This performance is relatively very fast and relevant if it will be implemented in a real time application.

Another test conducted in this research is histogram analysis. Histogram analysis is used to measure the strength of image encryption against statistical attacks [7], [24]. Table 2 presents the histogram of the original and encrypted images. The encrypted image histogram of all images has the same typical characteristics. On the histogram, it appears that the intensity of each pixel has a relatively uniform value. This indicates that the encryption quality is very good because the more uniform the intensity of the histogram indicates the better encryption quality[1], [19].

Table 2. Image Encryption Histogram

Image Name	Histogram R		Histogram G		Histogram B	
	Original	Encrypted	Original	Encrypted	Original	Encrypted
Mandrill						
Splash						
Lena						
Airplane						
House						
Sailboat						



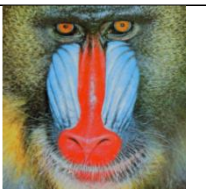
encrypted airplane image encrypted house image

Fig. 5. Sample Image Encryption Results

Figure 5 shows a sample of the results of the encryption process that has been applied to the original image. Visually, the image encryption process is very random and does not have a correlation with the original image.

The next step is to test image decryption. At this stage, the perfect decryption result must be produced, ie the decryption image must be exactly the same as the original image. Measuring instruments used in the decryption stage are, MSE, PSNR and SSIM measured. In addition, computational performance is also measured using a decryption algorithm with the tic toc function in Matlab. The entire measurement results of the decryption process are shown in table 3.

Table 3. Image Decryption Measurement and Results

Image Name	**MSE**	**PSNR**	**SSIM**	**Decrypting Time (seconds)**	**Results**
Mandrill	0	inf	0	1.595638	
Splash	0	inf	0	1.591684	
Lena	0	inf	0	1.531572	
Airplane	0	inf	0	1.510804	
House	0	inf	0	1.427434	
Sailboat	0	inf	0	1.536717	

Based on the results presented in table 3, it can be concluded that the decryption process can be carried out properly without errors. This is proven by the value of MSE = 0, which means that there is no error in the image reconstruction process. PSNR value = inf, this means no noise enters the decrypted image. The SSIM value is also equal to 0, this indicates that there is a similarity in the structure of the encrypted image with the original image. The time needed for the decryption process is also almost the same as the extraction process, which is about 1.5 seconds.

5. CONCLUSION

This study proposes a hybrid substitution method using modulus operations for digital image encryption. The hybrid method is done by utilizing two random keys which also function to increase security. This method has been tested with various tests such as entropy analysis to measure image randomness, histogram analysis to measure statistical attack strength, differential attack testing using UACI and NPCR, and measurement of error, noise and structural changes in images using MSE, PSNR, and SSIM. All measurement instruments show that the proposed encryption method is of very good quality. Likewise, the decryption process can be carried out properly without errors. This method also has a calculation that is relatively simple and fast, but strong against various attacks.

.

REFERENCES

[1] A. Setyono, D. R. I. M. Setiadi, and Muljono, “Dual encryption techniques for secure image transmission,” *J. Telecommun. Electron. Comput. Eng.*, 2018.

[2] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, “DNA Chaos Blend to Secure Medical Privacy,” *IEEE Trans. Nanobioscience*, vol. 16, no. 8, pp. 850–858, Dec. 2017.

[3] F. Mushtaq Sher Ali and F. Hassan Sarhan, “Enhancing Security of Vigenere Cipher by Stream Cipher,” *Int. J. Comput. Appl.*, vol. 100, no. 1, pp. 975–8887, 2014.

[4] C. Irawan, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, and M. Doheir, “Hybrid Encryption using Confused and Stream Cipher to Improved Medical Images Security,” *J. Phys. Conf. Ser.*, vol. 1201, no. 1, p. 012022, May 2019.

[5] R. Ahuja, B. E. Student, M. Ramrakhyani, B. Manchundiya, and S. Shroff, “Dual Layer Secured Password Manager using Blowfish and LSB,” *Int. J. Comput. Appl.*, vol. 143, no. 3, pp. 975–8887, 2016.

[6] V. M. Putrie, C. A. Sari, D. R. I. M. Setiadi, and E. H. Rachmawanto, “Super Encryption using Transposition-Hill Cipher for Digital Color Image,” in *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 2018, pp. 152–157.

[7] X. Q. Fu, B. C. Liu, Y. Y. Xie, W. Li, and Y. Liu, “Image encryption-then-transmission using DNA encryption algorithm and the double chaos,” *IEEE Photonics J.*, vol. 10, no. 3, Jun. 2018.

[8] E. Setyaningsih, C. Iswahyudi, and N. Widyastuti, “Image Encryption on Mobile Phone using Super Encryption Algorithm,” *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 10, no. 4, pp. 815–824, 2012.

[9] N. Yu *et al.*, “Double images encryption in optical image subtraction/addition 4F system,” *Optik (Stuttg).*, vol. 178, pp. 135–141, Feb. 2019.

[10] H. Diab, “An Efficient Chaotic Image Cryptosystem Based on Simultaneous Permutation and Diffusion Operations,” *IEEE Access*, vol. 6, pp. 42227–42244, Jul. 2018.

[11] Z. Hua, Y. Zhou, and H. Huang, “Cosine-transform-based chaotic system for image encryption,” *Inf. Sci. (Ny).*, vol. 480, pp. 403–419, Apr. 2019.

[12] C. Li, D. Lin, and J. Lu, “Cryptanalyzing an Image-Scrambling Encryption Algorithm of Pixel Bits,” *IEEE Multimed.*, vol. 24, no. 3, pp. 64–71, 2017.

[13] X. Wang, X. Zhu, and Y. Zhang, “An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map,” *IEEE Access*, vol. 6, pp. 23733–23746, Feb. 2018.

[14] B. B. Mohammed, “Automatic Key Generation of Caesar Cipher,” *Int. J. Eng. Trends*

Technol., vol. 6, no. 6, 2013.

[15] D. Venkata Vidya Deepthi, B. Homer Benny, K. Sreenu, and E. Id, "Various Ciphers in Classical Cryptography," *J. Phys. Conf. Ser.*, vol. 1228, no. 1, 2019.

[16] M. Rathidevi, R. Yaminipriya, and S. V. Sudha, "Trends of cryptography stepping from ancient to modern," in *IEEE International Conference on Innovations in Green Energy and Healthcare Technologies - 2017, IGEHT 2017*, 2017.

[17] P. Jindal and B. Singh, "RC4 Encryption-A Literature Survey," *Procedia Comput. Sci.*, vol. 46, pp. 697–705, 2015.

[18] A. Bhowmick, N. Sinha, R. V. Arjunan, and B. Kishore, "Permutation-Substitution architecture based image encryption algorithm using middle square and RC4 PRNG," in *2017 International Conference on Inventive Systems and Control (ICISC)*, 2017, pp. 1–6.

[19] D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, A. Susanto, and M. Doheir, "A Comparative Study of Image Cryptographic Method," in *2018 5th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, 2018, pp. 336–341.

[20] V. Rekhate, A. Tale, N. Sambhus, and A. Joshi, "Secure and efficient message passing in distributed systems using One-Time Pad," in *International Conference on Computing, Analytics and Security Trends, CAST 2016*, 2017, pp. 393–397.

[21] K. Alallayah, M. Amin, W. Abd El-Wahed, and A. Alhamami, "Attack and Construction of Simulator for Some of Cipher Systems Using Neuro-Identifier," *Int. Arab J. Inf. Technol.*, vol. 7, no. 4, pp. 365–372, 2010.

[22] Ming Hsieh Department of Electrical Engineering USC Viterbi School of Engineering, "SIPI Image Database." [Online]. Available: http://sipi.usc.edu/database/. [Accessed: 27-Mar-2019].

[23] M. A. Mokhtar, S. N. Gobran, and E. S. A. M. El-Badawy, "Colored image encryption algorithm using DNA code and Chaos theory," in *Proceedings - 5th International Conference on Computer and Communication Engineering: Emerging Technologies via Comp-Unication Convergence, ICCCE 2014*, 2015, pp. 12–15.

[24] A. A. Abd El-Latif, B. Abd-El-Atty, and M. Talha, "Robust Encryption of Quantum Medical Images," *IEEE Access*, vol. 6, pp. 1073–1081, Nov. 2017.