ISSN 2007-9737

Improved Color Image Encryption using Modified Modulus Substitution Cipher, Dual Random Key and Chaos Method

De Rosal Ignatius Moses Setiadi, Abu Salam, Eko Hari Rachmawanto, Christy Atika Sari

Dian Nuswantoro University,
Department of Informatics Engineering, Semarang,
Indonesia

{moses, abu.salam, eko.hari, atika.sari}@dsn.dinus.ac.id

Abstract. This study proposes the hybrid substitution cryptography method followed by chaotic methods to improve the security of digital image transactions on the internet. The substitution method used is a hybrid of the modification of the Vigenèreand Beaufort cipher algorithm. To do a hybrid, two random keys are used. The first random key is a matrix with 8-bits integer values, while the second random key is a matrix that contains binary values. The modulus operation is used in the main process of substitution methods. In this study, 24-bits true-color image was used as a dataset for the testing experiment. Measurement of encryption quality is measured by Entropy, MSE, PSNR, SSIM, UACI, and NPCR, whereas tic toc functions for measuring the computational time needed. To ensure the decryption process runs perfectly, measuring instruments such as SSIM, MSE, and PSNR are used to compare the decrypted image with the original image, the tic toc function is also used to measure computing performance. Based on the results of testing the quality of image encryption proved to have excellent results where the entropy value is close to 8, the ideal NPCR and UACI values, as well as excellent visual values based on MSE, PSNR and SSIM measurements. The image can also be decrypted perfectly with relatively fast computing time in the encryption and decryption process.

Keywords. Image encryption, substitution cipher, modulus operation, random key, hybrid cryptography.

1 Introduction

The reality of modern technology has changed the landscape of digital multimedia and created unexpected problems related to the security of sending and sharing data in the cyber world.

The number of theft cases in the cyber world makes the security of data a matter that needs special attention [1–3]. One way to secure data is by cryptography. Cryptography is the science of data encoding to secure the data. In this way, the encoded data will change in form and meaning so that it cannot be read directly [4, 5]. The encoding process is called the encryption process, while the process to restore data is encoded into the original data decryption process. Both of these processes are the main processes in cryptography [6].

Various digital files can be used as objects to be coded with cryptographic methods in previous studies. Digital images are one of the most favorite objects used in cryptographic research today [7, 8], so did in this study used a digital image as an object for study. Many cryptographic methods have been applied to images such as scramble, stream and substitution methods. The scramble method is also often called the permutation or diffusion method[9] where, algorithms that are popular in this method are Chaotic Map [5, 10]. While the algorithms that are widely used in substitution methods are one-time pad (OTP), Vigenere, Hill cipher, etc. [1, 11, 12]. Some modern cryptographic methods are also applied in image encryption such as DES and AES [13, 14].

But in research [15, 16] it is said that the AES and DES methods are not suitable if implemented on the image due to some physical features of the image such as bulky data capacity, high redundancy and strong correlation between pixels. In a comparative study conducted by [17], it was stated that the scrambling method has advantages in diffusion and confusion properties, but this

method is quite slow to compute especially if it has a large number of iterations. The lack of a scrambling method also produces the same image histogram as the original image. Whereas OTP has advantages in the results of image encryption based on several measurements such as entropy analysis, the unified average change in intensity (UACI), the Number of Pixel Change Rate (NPCR), Peak Signal to Noise Ratio (PSNR), and Structural Similarity Index (SSIM) and has faster computing processes.

OTP is a substitution cryptography algorithm also known as Vernam cipher. This algorithm uses XOR or modulo operations as its main operation [1]. Vernam algorithm is the development of the Vigenèrecipher algorithm that uses random keys in the process of encryption and decryption. The Vernam algorithm is strong against attacks and difficult to decrypt. But the toughness of this algorithm depends on the key used. In order to obtain encryption, the strong key must be completely random, only used once, and only known by the sender and receiver. Because the algorithm that has a simple, fast and powerful operation makes this algorithm much developed [18]. One of the algorithms derived from Vigenèrecipher is Beaufort cipher. Subtraction operations are carried out in the encryption and decryption process in Beaufort cipher, which distinguishes them from Vigenèreciphers [19]. To improve security, this study proposes a cryptographic method by modifying the modulus-based substitution cipher to hybridize the Vigenèreand Beaufort algorithm with two random keys followed by the chaos method.

2 Literature Review

Cryptography is a science that has been carried out to secure secret messages from ancient times until now. The substitution method is a cryptographic method that encrypts by changing the meaning and content of the message based on the key value. In the substitution method, the key will have an important role in the strength of the encoding, the better the key the stronger the results of encryption.

Vigenèrecipher is one of the cryptographic algorithms that applies the substitution method and was very popular in its time. Vigenèrecipher uses tabula recta tables for the encryption and decryption process, then was developed by Gilbert Vernam by modifying the use of keys, where the key used is random, then also known as Vernam cipher [1, 20]. Because the quality of this method is very dependent on the key, the use of random keys has better performance and is harder to solve. The Vernam cipher formula for the encryption process can be seen in formula (1) and for decryption, it can be seen in formula (2):

$$Cc = (Pc + k)\ mod\ 256, \tag{1}$$

$$Pc = (Cc - k)\ mod\ 256, \tag{2}$$

where:

Cc = cipher image,

Pc = plain image,

k = key, range value between 0 until 255, 256 have been selected as a constant modulo because of the pixel value between 0 until 255.

Beaufort cipher is a modification of the Vigenèrecipher that uses a subtraction operation as its main process [19]. The formula used in Beaufort cipher has similarities with Vigenèrecipher. The similarity between the two techniques is the use of the modulo function and the type of key used. The difference between these two algorithms is the key role, in the Vigenèrecipher, in the encryption process, the key is used as a plain text enhancer, whereas in the decryption process, the key is used as a subtraction of the ciphertext. Whereas in Beaufort cipher, the key used for the reduction operation is the encryption and decryption process. For more details, the Beaufort cipher encryption formula can be seen in Eq. (3) and decryption formula in Eq. (4):

$$Cc = (k - Pc)\ mod\ 256, \tag{3}$$

$$Pc = (k - Cc)\ mod\ 256. \tag{4}$$

Another cryptographic method that is popularly used today in image encryption is the scrambling method, one of the popular algorithms of this method is the Arnold Chaotic Map (ACM).

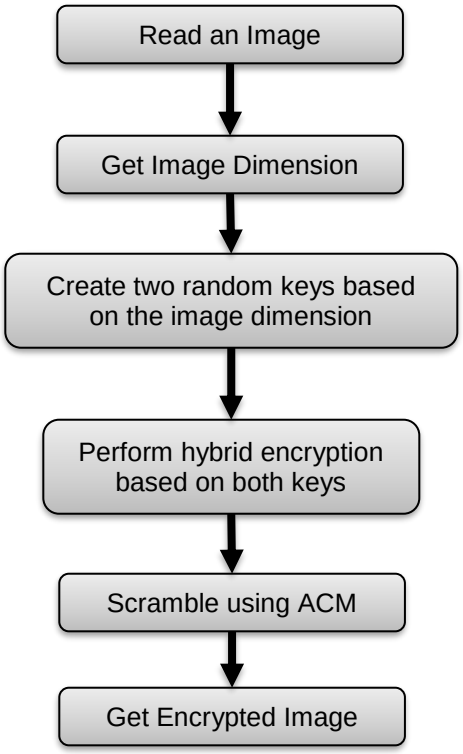


Fig. 1. Encryption Process

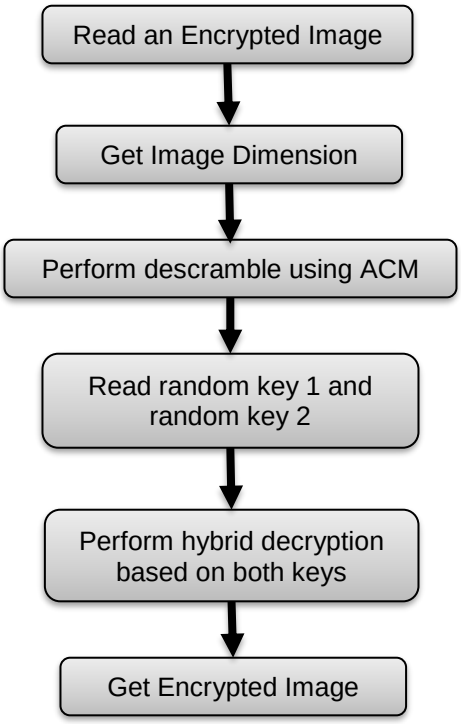


Fig. 2. Decryption Process

This method is widely proposed for cryptography in images, because of its superiority against differential attacks. ACM can provide an efficient combination of the properties of confusion and diffusion. The scramble method differs from the substitution method, the encrypted image scramble method does not change the pixel value, only the randomness of the pixel is performed by a certain formula [21, 22].

This method has a sensitivity to the initial state and has ergodicity property so that it is strong against certain security conditions [5]. To encrypt images with ACM you can use Eq. (5), while the decryption process can use Eq. (6):

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & k \\ l & kl+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \ mod\ W\ , \qquad (5)$$

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & k \\ l & kl+1 \end{bmatrix}^{-1} \begin{bmatrix} x' \\ y' \end{bmatrix} \ mod\ W\ , \qquad (6)$$

where x and y are the pixel coordinates, x' and y' are the new pixel coordinates, k and l are positive integer numbers, W is the length or width of the image, where the length and width of the image must be the same.

For the record, Eq. (5) and Eq. (6) done in one iteration or one Arnold period. Iteration can be done several times as needed.

3 Proposed Method

The cryptographic method consists of two main stages, i.e encryption, and decryption. The proposed method uses a hybrid method of the Vigenèrecipher and Beaufort cipher algorithm which has been modified using two random keys. Then proceed with encryption using ACM to get the final cipher.

The stages in the encryption process can be seen in Figure 1. Based on figure 1 can be explained in more detail with the steps in the encryption process as follows:

ISSN 2007-9737

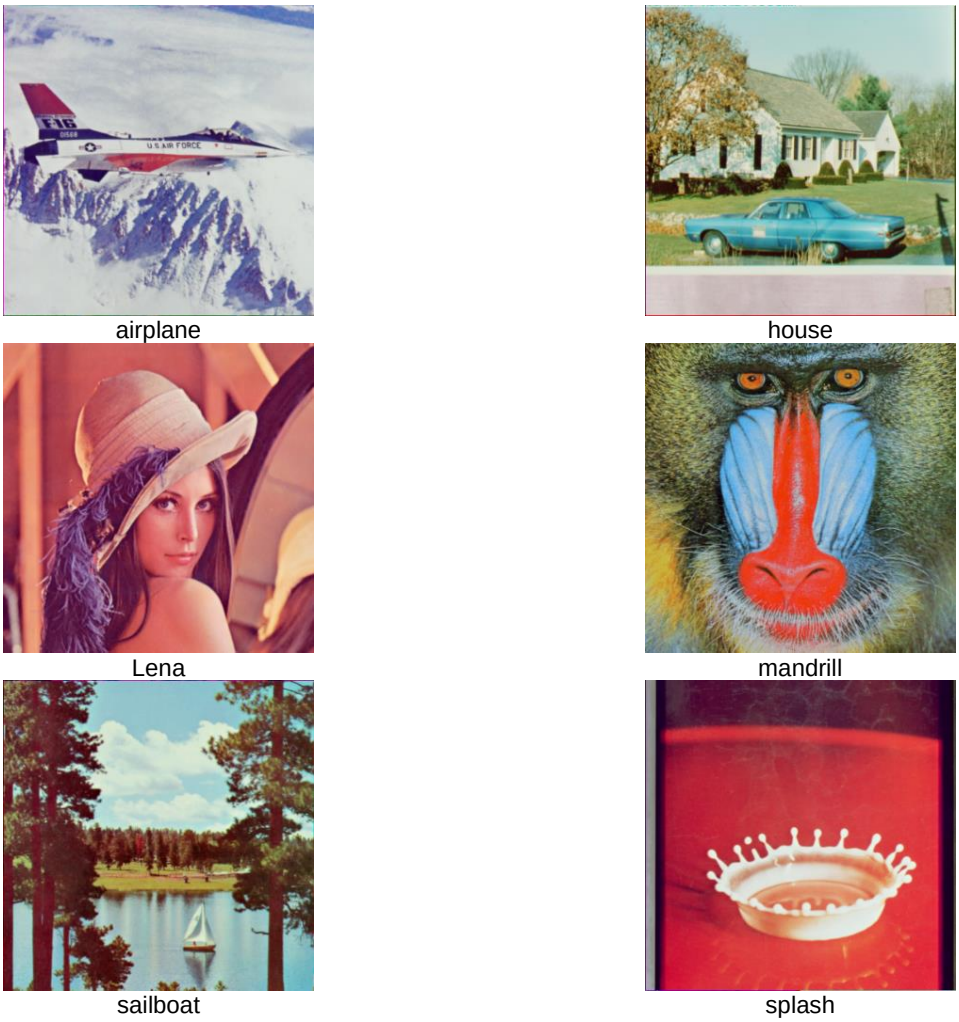


Fig. 3. Image Dataset used in this research

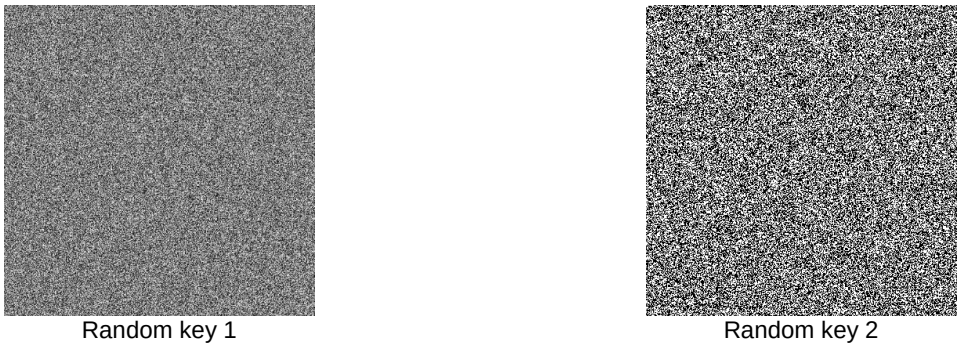


Fig. 4. Sample random key used in this research

1 Read the image as input, then save the image in a variable I.
2 Get the dimensions of the I image and save it into variable $m, n, o,$ where m is the width, n is height, and o is the image layer (RGB).
3 Create a matrix with dimensions ($m \times n$) then fill with random numbers in the range of 0 to 255 using a random generator, save this matrix as the first key ($rkey1$).
4 Create a second matrix with dimensions ($m \times n$) then fill with random binary numbers using a random generator, then save this matrix as the second key ($rkey2$).
5 Perform hybrid encryption using formula (7):

$$E_{mno} = \begin{cases} mod\big((rkey1_{mn} - I_{mno}), 256\big), rkey2 = 1 \\ mod\big((I_{mno} + rkey1_{mn}), 256\big), rkey2 = 0 \end{cases}. \quad (7)$$

6 Perform ACM using Eq. (5) on the E matrix to produce an encrypted image.

As for the stages of image decryption, see Figure 2 below. Based on figure 2, it 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 E.
2. Get the dimensions of the E image and save it to $m, n, o,$ where m is the width, n is height, and o is the image layer (RGB).
3. Descramble the matrix E with Eq. (6) for each layer.
4. Read the first random key ($rkey1$) and the second random key ($rkey2$).
5. Perform decryption using Eq. (8), based on both random keys.:

$$D_{mno} = \begin{cases} mod\big((rkey1_{mn} - E_{mno}), 256\big), rkey2 = 1 \\ mod\big((E_{mno} - rkey1_{mn}), 256\big), rkey2 = 0 \end{cases}. \quad (8)$$

6. Get the decrypted image (D).

4 Results and Discussion

A standard image dataset in the RGB (24-bit) channel format is used at this stage. This image is a standard testing image for digital image processing which can be downloaded on the SIPI image database page [23]. Figure 3 presents some sample images used for the images used in this study. After the image is downloaded, the image is used directly as a dataset to be tested on the proposed encryption method. All images do not undergo preprocessing, so the pixel values, dimensions, and image extensions are the same as the original version. This is done so that it is easy to compare with subsequent research. All images used have dimensions of 512 × 512.

The first step before starting the encryption process is to create two random keys. Create two random keys according to the dimensions of the image to be encrypted, for more details see steps 3 and 4 of the method proposed in section 3. Figure 4 is an example of a random key generated by a random generator and tested in this research.

The first random key is a grayscale image (8-bits) and the second random key is a binary image. Next, use the two random keys for the encryption process using formula (7). The encryption results were then randomized again using ACM with the formula (5) so that the encrypted image is generated. The results were then tested for encryption quality using several measuring devices such as entropy, MSE, PSNR, SSIM, UACI, and NPCR. Entropy (H) is a feature that is used to measure the randomness of probability (p) encrypted images that can be decrypted [24]. Entropy can be calculated by the formula (9):

$$H_i = -\sum_0^{2^8-1} p_i \, log_2(p_i), \quad (9)$$

MSE, PSNR, and SSIM are used to measure the quality of image encryption based on errors, noise, and structural changes in the image. Formulas (10, 11, 12), each of which is used to calculate MSE, PSNR, and SSIM. UACI and NPCR are used to measure the encryption strength of differential attacks [24, 25]. Where the formula used to calculate UACI and NPCR is shown in formulas (13, 14):

$$MSE = \sum_{m=0}^{255} \sum_{n=0}^{255} \sum_{o=0}^{255} \|E(m,n,o) - I(m,n,o)\|, \quad (10)$$

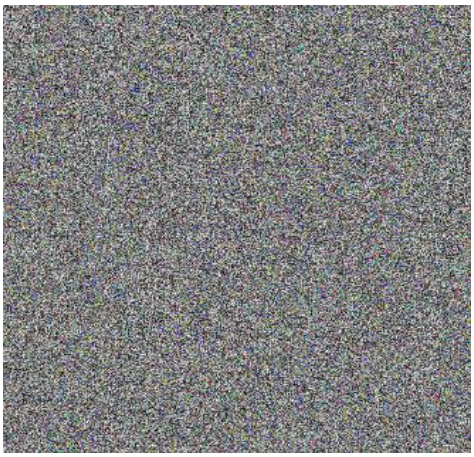
$$PSNR = 10 \, log_{10}\left(\frac{255^2}{\sqrt{MSE}}\right), \quad (11)$$

Table 1. Image Encryption Measurement (Entropy, MSE, PSNR, SSIM, Time)

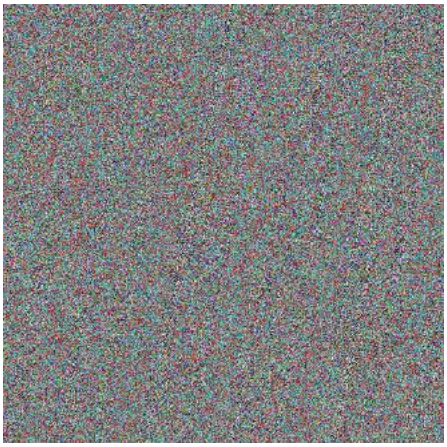
Image Name	Entropy (Red)	Entropy (Green)	Entropy (Blue)	MSE	PSNR	SSIM	Time (seconds)
Airplane	7.9993	7.9992	7.9992	10363.3117	7.9758	0.0005	2.196500
House	7.9992	7.9992	7.9993	11200.3896	7.6385	0.0006	2.020584
Lena	7.9994	7.9993	7.9993	11215.9747	7.6324	0.0007	2.289976
Mandrill	7.9994	7.9993	7.9992	10106.1305	8.0850	0.0004	2.261854
Sailboat	7.9993	7.9994	7.9993	11222.3829	7.6300	0.0009	2.194902
Splash	7.9993	7.9993	7.9993	11231.1979	7.6265	0.0004	2.325276

Table 2. Image Encryption Measurement (NPCR and UACI)

Image Name	NPCR			UACI		
	Red	Green	Blue	Red	Green	Blue
Airplane	99.6174	99.6178	99.6258	31.9945	33.1712	32.7779
House	99.5952	99.6155	99.6025	30.2055	31.3364	31.2868
Lena	99.5956	99.6223	99.6227	32.9805	30.5929	27.6362
Mandrill	99.6311	99.6318	99.6150	29.9489	28.7772	31.8353
Sailboat	99.6140	99.6204	99.5899	27.9453	34.3163	34.3236
Splash	99.6177	99.6021	99.6288	34.2339	35.6784	31.9677



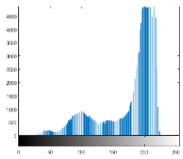
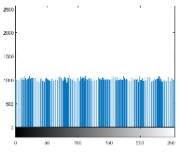
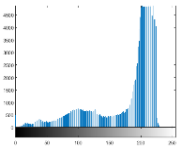
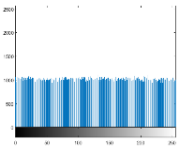
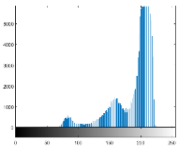
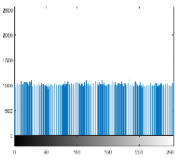
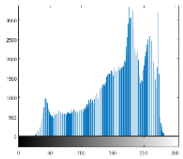
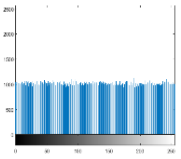
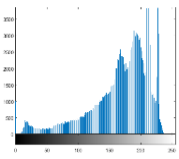
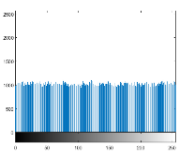
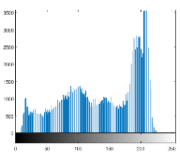
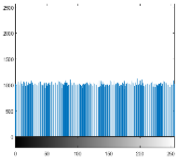
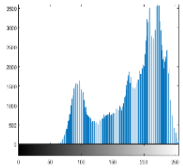
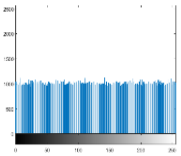
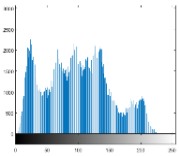
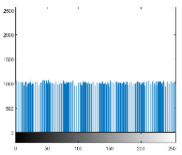
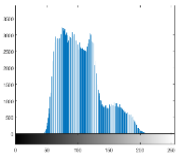
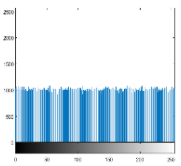
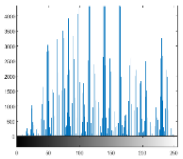
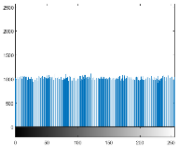
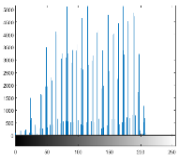
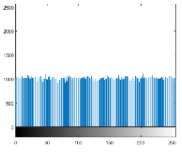
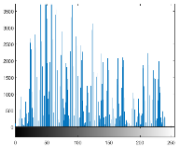
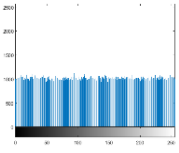
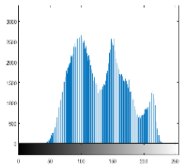
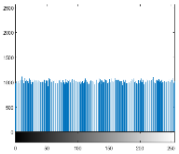
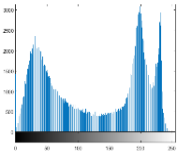
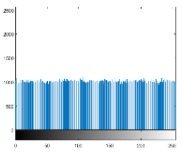
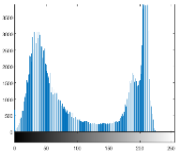
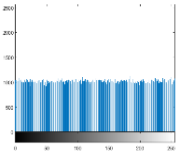
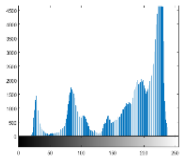
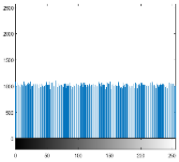
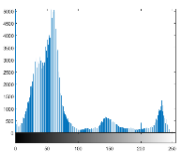
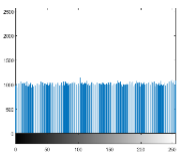
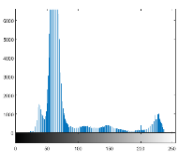
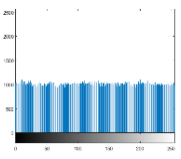
Encrypted Lena image



Encrypted baboon image

Fig. 5. Sample Image Encryption Results

Table 3. Image encryption histogram

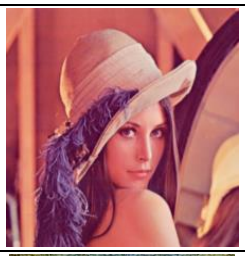
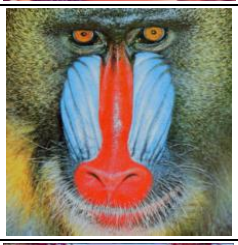
Image Name	Histogram R		Histogram G		Histogram B	
	Original	Encrypted	Original	Encrypted	Original	Encrypted
Airplane						
House						
Lena						
Mandrill						
Sailboat						
Splash						

$$SSIM = \frac{(2\mu_E\mu_I+c_1)(2\sigma_{EI}+c_2)}{(\mu_E^2+\mu_I^2+c_1)(\sigma_E^2+\sigma_I^2+c_2)}, \quad (12)$$

$$NPCR = \frac{1}{m*n*o}\sum_{m=0}^{255}\sum_{n=0}^{255}\sum_{o=0}^{255} C(mno)*100\%, \quad (13)$$

ISSN 2007-9737

Table 4. Image decryption measurement and results

Image name	MSE	PSNR	SSIM	Decrypting time (seconds)	Results
Airplane	0	inf	0	2.420104	
House	0	inf	0	2.424534	
Lena	0	inf	0	2.536312	
Mandrill	0	inf	0	2.512338	
Sailboat	0	inf	0	2.511917	
Splash	0	inf	0	2.521384	

$$C(mno) = \begin{cases} 0, I(mno) = E(mno) \\ 1, I(mno) \neq E(mno) \end{cases}$$

$$UACI = \frac{1}{m \times n \times o} \sum_{m=0}^{255} \sum_{n=0}^{255} \sum_{o=0}^{255} \frac{|I(mno) - E(mno)|}{255} \times 100\%, \quad (14)$$

where E is an encrypted image, I is the original image, m is the image width, n is the imag
e height, and o is the number of layers, σ_{EI} is the image covariance I against E; σ_I^2 is a variant of image I; σ_E^2 is a variant of image E; $c_1 = (k_1 L)^2$; $c_2 = (k_2 L)^2$; L is a dynamic range of the image$(0 - 255)$ with the default value $k_1 = 0.01$ and $k_2 = 0.03$.

The measurement of encryption quality is shown in table 1 and table 2. In table 1 there are several measurement results such as Entropy, MSE, PSNR, and SSIM, then in table 2, there are NPCR and UACI. The entropy value produced from the whole image is very good because the entropy produced is close to 8 (maximum value) [17]. Based on the entropy value, it can be concluded that the encrypted image will be very difficult to decrypt without knowing the key used. Visually encrypted images also show very significant changes when compared to the original image, there is no correlation or meaning related [26].

This is evidenced by a large MSE value and a very small PSNR value, the square of the error is very high so that it directly impacts the amount of noise that distorts the image. The image structure also changed significantly, which is indicated by an SSIM value close to 0. Besides the combination of hybrid substitution and scrambling methods with ACM produces ideal UACI and NPCR values, so it can be concluded that the encryption results are also strong against differential attack attacks.

Other tests are also carried out, i.e. the computational time needed. The tic toc function on Matlab R2015a is used as a measurement tool, based on the measurement results it takes about 2 seconds for encryption and decryption of each image tested in this research. As a note in this research used hardware with specifications: AMD A12 7th processor and 4GB RAM. Of course, this performance is relatively very fast and relevant if later implemented in a real application. The last test conducted was a histogram analysis. This test has an important role in knowing how much the encryption strength of images against statistical attacks [24, 25]. Table 3 presents a comparison of the histogram of the original image and the encrypted image if the histogram is observed from the encryption results all images have a similar form. It seems that the value of each pixel has almost the same intensity or uniformity.

Because the better the quality of encryption, the histogram will show a more uniform intensity of values across all pixels. The distribution of pixel values will also be more evenly distributed across all values in the range of 0 to 255, [1, 17].

Table 5. Comparison with the previous method based on NPCR, UACI, and Entropy

Measurement Tools		Ref [27]	Ref [28]	Ref [29]	Proposed
NPCR	Red	99.6475	**99.6836**	94.6836	99.5956
	Green	99.6231	**99.6836**	95.6836	99.6223
	Blue	99.5941	**99.6810**	98.6810	99.6227
UACI	Red	33.5328	33.4647	33.4647	**32.9805**
	Green	33.2752	33.5048	34.5048	**30.5929**
	Blue	33.4394	33.4999	35.4999	**27.6362**
Entropy	Red	7.9808	7.9992	-	**7.9994**
	Green	7.9811	7.9992	-	**7.9993**
	Blue	7.9814	7.9991	-	**7.9993**

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 correlate with the original image.

The next step is testing the image decryption process. At this stage, it can be done without any errors so that the decrypted image has a value that is the same as the original image.

To measure the results of decryption, MSE, PSNR, and SSIM are measured. Besides, computational performance is also measured using the decryption algorithm with the tic toc function in Matlab. The results of measuring the decryption process are shown in table 4.

The results shown in table 4 show that the decryption process can be done well without any errors. This is evidenced by the value of MSE = 0, which means that there is no single error in the reconstruction of the decrypted image. PSNR value = inf, this means there is no noise entering the image. The SSIM value is also equal to 0, this shows that the similarity of the image structure is encrypted with the original image. The time needed for the decryption process is also almost the same as the extraction process, which is about 2 seconds

After measuring the quality of encryption, and the performance of the proposed method. Furthermore, a comparison of the results was carried out with some research on image encryption that had been published previously. Comparison is done based on several measuring devices such as entropy, NPCR, and UACI. Some research that is used as a comparison is [27 - 29], where the comparison is done with the same image dataset, namely Lena's image, the comparison is presented in Table 55 Conclusion.

This study proposes a combination of the substitution and scramble encryption method by hybridizing the Vigenère and Beaufort algorithm combined with ACM encryption. Hybrid is done by using modulus operations and two random keys. The encryption results from the hybrid substitution method are then encrypted again using ACM to get multiple layers of protection. The aim is to improve image security.

To measure the quality of encryption, several tests are carried out, such as entropy analysis to measure the randomness of images and decrypted probabilities, histogram analysis to measure the strength of encryption from statistical attacks, UACI and NPCR to measure unawareness of differential attacks. Besides that, the level of error, noise and structural changes in the image were also measured using MSE, PSNR, and SSIM to determine the level of image randomness visually. All measurement instruments show that the proposed encryption method is of very good quality. Likewise, the decryption process can work well without errors which can change the meaning of the original image.

When compared with some of the previous methods presented in Table 5 it appears that the UACI and Entropy values of the proposed method are superior, even though the NPCR value is still not more effective and can be used as something that should be improved in further research. This method also has relatively simple and fast but powerful computing against various attacks, so it is very relevant if it will be implemented in various applications.

References

1. **Setyono, A., De Rosal-Ignatius, M.S., Muljono, M., (2018).** Dual encryption techniques for secure image transmission. Journal of Telecommunication, Electronic and Computer Engineering, Vol. 10, No. 3-2.
2. **Diab. H. (2018).** An efficient chaotic image cryptosystem based on simultaneous permutation and diffusion operations. IEEE Access, Vol. 6, pp. 42227–42244. DOI: 10.1109/ACCESS.2018.2858839.
3. **Setiadi, D.R.I.M. (2019).** Improved payload capacity in LSB Image Steganography uses dilated hybrid edge detection. Journal of King Saud University - Computer and Information Sciences. DOI: 10.1016/j.jksuci.2019.12.007.
4. **Ravichandran, D., Praveenkumar, P., Rayappan, J.B.B., Amirtharajan, R. (2017).** DNA Chaos blend to secure medical privacy. IEEE Trans. Nanobioscience, Vol. 16, No. 8, pp. 850–858. DOI: 10.1109/TNB.2017. 2780881.
5. **Irawan, C., De Rosal-Ignatius, M.S., Rachmawanto, E.H., Sari, C.A., Doheir, M.**

(2019). Hybrid encryption using confused and stream cipher to improved medical images security. J. Phys. Conf. Ser., Vol. 1201, No. 1, pp. 012022.

6. **Rathidevi, M., Yaminipriya, R., Sudha, S.V. (2017).** Trends of cryptography stepping from ancient to moder. IEEE International Conference on Innovations in Green Energy and Healthcare Technologies, pp. 1–9. DOI: 10.1109/IGEHT.2017.8094107.
7. **Bao, L., Yi, S., Zhou, Y. (2017).** Combination of sharing matrix and image encryption for lossless (k,n)-secret image sharing. IEEE Trans. Image Process., Vol. 26, No. 12, pp. 5618–5631. DOI: 10.1109/TIP.2017.2738561.
8. **Jolfaei, A., Wu, X.W., Muthukkumarasamy, V. (2016).** On the security of permutation-only image encryption schemes. IEEE Trans. Inf. Forensics Secur., Vol. 11, No. 2, pp. 235–246. DOI: 10.1109/TIFS.2015.2489178.
9. **Li, C., Lin, D., Lu, J. (2017).** Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. IEEE Multimed., Vol. 24, No. 3, pp. 64–71. DOI: 10.1109/MMUL.2017.3051512.
10. **Wang, X., Zhu, X., Zhang, Y. (2018).** An image encryption algorithm based on josephus traversing and mixed chaotic map. IEEE Access, Vol. 6, pp. 23733–23746. DOI: 10.1109/ACCESS.2018.2805847.
11. **Venkata-Vidya-Deepthi, D., Homer-Benny, B., Sreenu, K., Id, E. (2019).** Various ciphers in classical cryptography. Journal Phys. Conf. Ser., Vol. 1228, No. 1.
12. **Kumar, M., Mishra, R., Pandey, R.K., Singh P. (2010).** Comparing classical encryption with modern techniques. Journal Phys. Sci. Eng. Technol., Vol. 1, No. 1, pp. 49–54.
13. **Zhang, Q., Qunding, A. (2016).** Digital image encryption based on advanced encryption standard (AES) algorithm. Proceedings - 5th International Conference on Instrumentation and Measurement, Computer, Communication, and Control, pp. 1218–1221. DOI: 10.1109/ IMCCC.2015.261.
14. **Pathak, S., Kamble, R., Chaursia, D. (2014).** An efficient data encryption standard image encryption technique with RGB random uncertainty. Proceedings of the International Conference on Reliability, Optimization and Information Technology, pp. 413–421. DOI: 10.1109/ICROIT.2014.6798366.
15. **Wang, X., Zhang, H. (2015).** A color image encryption with heterogeneous bit-permutation and correlated chaos. Opt. Commun., Vol. 342, pp. 51–60. DOI: 10.1016/j.optcom.2014. 12.043.
16. **Ghadirli, H.M., Nodehi, A., Enayatifar, R. (2019).** An overview of encryption algorithms in color images. Signal Processing, Vol. 164, pp. 163–185. DOI: 10.1016/j.sigpro.2019.06.010.
17. **Setiadi, D.R.I.M.. Rachmawanto, E.H., Sari, C.A., Susanto, A., Doheir, M. (2018).** A comparative study of image cryptographic method. International Conference on Information Technology Computer, and Electrical Engineering (ICITACEE), pp. 336–341. DOI: 10.1109/ICITACEE.2018.8576907.
18. **Rekhate, V., Tale, A., Sambhus, N., Joshi, A. (2017).** Secure and efficient message passing in distributed systems using one-time pad. International Conference on Computing. Analytics and Security Trends, pp. 393–397. DOI: 10.1109/CAST.2016.7915001.
19. **Alallayah, K., Amin, M., Abd El-Wahed, W. Alhamami, A. (2010).** 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.
20. **Mushtaq Sher-Ali, F., Hassan-Sarhan, F. (2014).** Enhancing security of vigenèrecipher by stream cipher. Int. J. Comput. Appl., Vol. 100, No. 1, pp. 975–8887.
21. **Chen, L., Zhao, D., Ge, F. (2013).** Image encryption based on singular value decomposition and Arnold transform in fractional domain. Opt. Commun., Vol. 291, pp. 98–103. DOI: 10.1016/j.optcom.2012.10.080.
22. **Alawida, M., Samsudin, A., Sen-Teh, J., Alkhawaldeh, R.S. (2019).** A new hybrid digital chaotic system with applications in image encryption. Signal Processing, Vol. 160, pp. 45–58. DOI: 10.1016/j.sigpro.2019.02.016.
23. **Ming Hsieh Department of Electrical Engineering USC Viterbi School of Engineering (2019).** SIPI Image Database. http://sipi.usc.edu/database/.

24. **Fu, X.Q., Liu, B.C., Xie, Y.Y., Li, W., Liu, Y. (2018).** Image encryption-then-transmission using DNA encryption algorithm and the double chaos. IEEE Photonics J., Vol. 10, No. 3, pp. 1–15. DOI: 10.1109/JPHOT.2018.2827165.
25. **Abd El-Latif, A.A., Abd-El-Atty, B., Talha, M. (2017).** Robust encryption of quantum medical images. IEEE Access, Vol. 6, pp. 1073–1081. DOI: 10.1109/ACCESS.2017.2777869.
26. **Mokhtar, M.A., Gobran, S.N., El-Badawy E. S.A.M. (2015).** Colored image encryption algorithm using DNA code and Chaos theory. Proceedings - 5th International Conference on Computer and Communication Engineering: Emerging Technologies via Comp-Unication Convergence, pp. 12–15. DOI: 10.1109/ICCCE.2014.17.
27. **Liu, H., Kadir, A., Gong, P. (2015).** A fast color image encryption scheme using one-time S-Boxes based on complex chaotic system and random noise. Opt. Commun., Vol. 338, pp. 340–347. DOI: 10.1016/j.optcom.2014.10.021.
28. **Mohammad-Seyedzadeh, S., Mirzakuchaki, S. (2012).** A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. Signal Processing, Vol. 92, No. 5, pp. 1202–1215. DOI: 10.1016/j.sigpro.2011.11.004.
29. **Hussain, I., Shah, T., Gondal, M.A. (2012).** Image encryption algorithm based on PGL(2,GF(2 8)) S-boxes and TD-ERCS chaotic sequence. Nonlinear Dyn., Vol. 70, No. 1, pp. 181–187. DOI: 10.1007/s11071-012-0440-0.

Article received on 04/12/2018; accepted on 05/07/2021.
Corresponding author is De Rosal Ignatius Moses Setiadi.