Received: October 21, 2020. Revised: December 11, 2020.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Improved Color Image Encryption using Hybrid Modulus Substitution Cipher and Chaotic Method

Budi Harjo[1]* **De Rosal Ignatius Moses Setiadi[1]**

[1]*Department of Informatics Engineering, Dian Nuswantoro University, Semarang, Indonesia*
* Corresponding author's Email: budi.harjo@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 Vigenère and 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 images were 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 very 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]. Cryptography is a popular way to secure data. Cryptography is the study of data encryption to secure data. In this way, the encrypted data can change its form and meaning so that it cannot be read by unauthorized persons [4-6]. The encryption process is one of the main processes in cryptography, this process is carried out on the sender's side. The second main process, namely decryption, which is carried out on the receiving side, in this process is carried out so that it can restore to the original data form. These two processes are the main processes in cryptography[7].

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[8, 9], so did in this study used a digital image as an object for study. Image is one of the medias that has been widely used as a medium for cryptography implementation, where the scramble, stream, and substitution methods have been tested. The scramble method is also often called the permutation or diffusion method[10] where, algorithms that are widely in this method are Chaotic Map[5, 11-13]. Whereas the algorithms that are popular used in substitution methods are one-time pad (OTP), Vigenere, Hill cipher, etc[1, 14, 15]. Some modern cryptographic methods are also applied in image encryption such as DES and AES [16, 17]. However, the AES and DES methods are considered less suitable when applied to image data. This is due to several physical features of the image such as large data capacity, high redundancy, and a strong correlation between pixels [18, 19]. In a comparative study conducted by [20], the chaos method and OTP method have done comparisons with the same image data set where the result is that OTP has several advantages such as entropy analysis, sensitivity, histogram analysis so that it proved superior to statistical attacks. Besides, the OTP has a faster computation process. But the OTP method depends on the quality of the key, where the key used must be completely random and used only once, besides that the operation is also very simple, namely the XOR operation. Whereas many theories agree that the chaos method has several advantages including diffusion and confusion so that it is resistant to differential attacks [6, 18, 19, 21], however, if the chaotic method alone cannot produce a uniform histogram, it will be the same as the original because the chaotic method is a type of encryption that only randomizes the position of the pixels in the image. So that eventually many studies combine these types of encryption to increase security [11, 22-24].

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 Vigenère cipher algorithm that uses random keys in the encryption and decryption process. The Vernam algorithm is strong against attacks and difficult to decrypt. But the toughness of this algorithm depends on the key used. 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 [25]. One of the algorithms derived from the Vigenère cipher is the Beaufort cipher. Subtraction operations are carried out in the encryption and decryption process in Beaufort cipher, which distinguishes them from Vigenère ciphers [26]. The chaotic method is a type of cryptography that scrambles the pixel value of the image, which has a different way of working and has advantages than substitution cryptography as previously described. So this research proposes a hybrid substitution technique based on the modulus operation combined with the chaos method. In this way, a stronger security feature is obtained by taking the strengths of each method, namely diffusion, confusion, entropy analysis, histogram analysis, and sensitivity. Besides, the hybridization of two substitution methods that use two keys will increase security strength. In the next section, we will explain the literature review in section 2, the proposed methods in section 3, results and discussion in section 4, and conclusions in section 5.

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.

Vigenère cipher is one of the cryptographic algorithms that applies the substitution method and was very popular in its time. Vigenère cipher 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, 27]. 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 Eq. (1) and for decryption, it can be seen in Eq. (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 Vigenère cipher that uses a subtraction operation as its main process [26]. The Beaufort cipher has similarities with the Vigenère cipher having similar formulas. The similarity of the formulas for the two techniques is the use of the modulo function and the type of key used for encryption and decryption. The difference between these two algorithms is in the key role, wherein the encryption process Vigenère cipher is added to the key and plain text, while 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 the 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). 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, 28]. 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 Vigenère cipher and Beaufort cipher algorithm which has been modified using two random keys. Then proceed with encryption using ACM to get the final cipher. In more detail, the steps for the proposed method are described below:

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 using a pseudorandom integer generator. This matrix uses a random integer value range from 0 to 255, so that the 256 modulus operation is performed, then save this matrix as the first key ($rkey1$).
4. Create a second matrix with dimensions ($m \times n$) then fill using a pseudorandom integer generator. To generate random binary numbers, the modulus 2 operation is used then save this matrix as the second key ($rkey2$).
5. Perform hybrid encryption using Eq. (7)

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

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

The stages in the encryption process can be seen visually in Fig. 1.

As for the stages of image decryption, see Fig. 2 below. Based on Fig. 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 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.
5. Read the first random key ($rkey1$) and the second random key ($rkey2$).
6. Perform decryption using Eq. (8), based on both random keys.

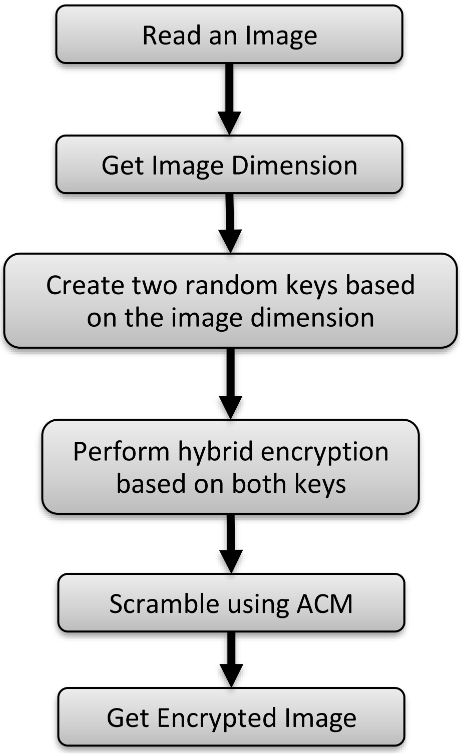

Read an Image
Get Image Dimension
Create two random keys based on the image dimension
Perform hybrid encryption based on both keys
Scramble using ACM
Get Encrypted Image

Figure. 1 Proposed encrypted method

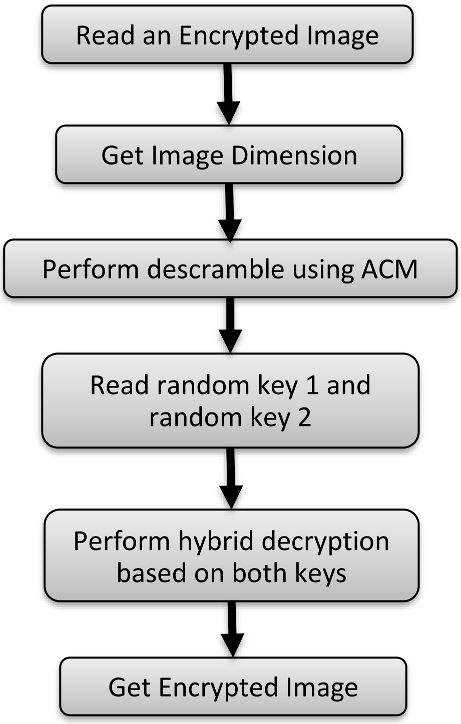

Read an Encrypted Image
Get Image Dimension
Perform descramble using ACM
Read random key 1 and random key 2
Perform hybrid decryption based on both keys
Get Encrypted Image

Figure. 2 Decryption process

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

7. 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 [29]. Fig. 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. Fig. 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. As a note, for encryption with ACM, we use 10 iterations. While the constant 1 in formula (5) and formula (6) can be replaced with other constants in the form of integers, however in this research test, a constant 1 was used. The results were then tested for encryption quality using several measuring devices such as entropy,

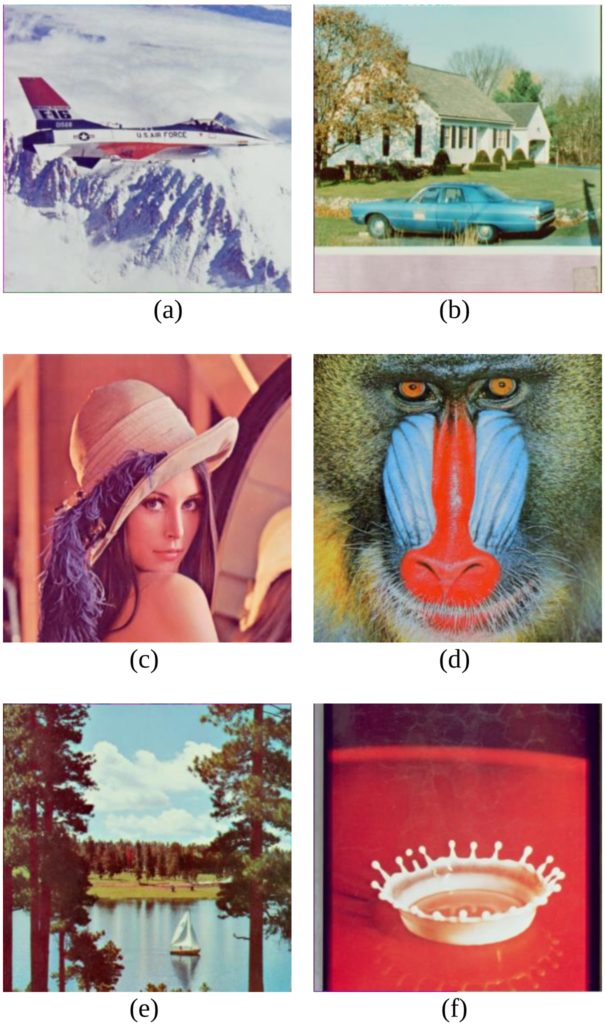

(a) (b)
(c) (d)
(e) (f)

Figure. 3 Image dataset used in this research: (a) airplane, (b) house, (c) Lena, (d) mandrill, (e) sailboat, and (f) splash

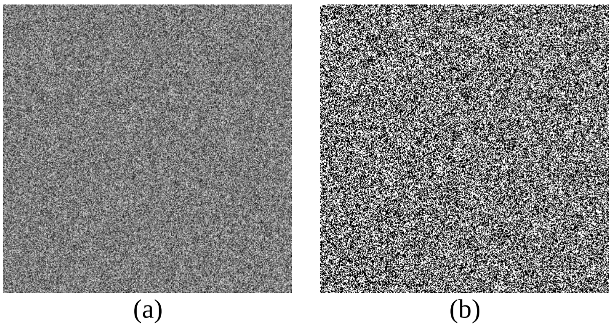

(a) (b)

Figure. 4 Sample random key used in this research: (a) random key 1and (b) random key 2

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[30]. 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), and (12), each of which is used to calculate MSE, PSNR, and SSIM. UACI and NPCR are used to measure the encryption strength of sensitivity and differential attacks[19,30-31]. Where the formula used to calculate UACI and NPCR is shown in formulas (13) and (14).

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

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

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

$$NPCR = \frac{1}{m \times n \times o}\sum_{m=0}^{255}\sum_{n=0}^{255}\sum_{o=0}^{255} C(mno) \times 100\%,$$
$$C(mno) = \begin{cases} 0, I(mno) = E(mno) \\ 1, I(mno) \neq E(mno) \end{cases} \quad (13)$$

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

Where E is an encrypted image, I is the original image, m is the image width, n is the image 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; $c_1 = (k_1L)^2$; $c_2 = (k_2L)^2$; L is a dynamic range of the image$(0 - 255)$ with the default value $k_1 = 0.01$ and $k_2 = 0.03$ [32].

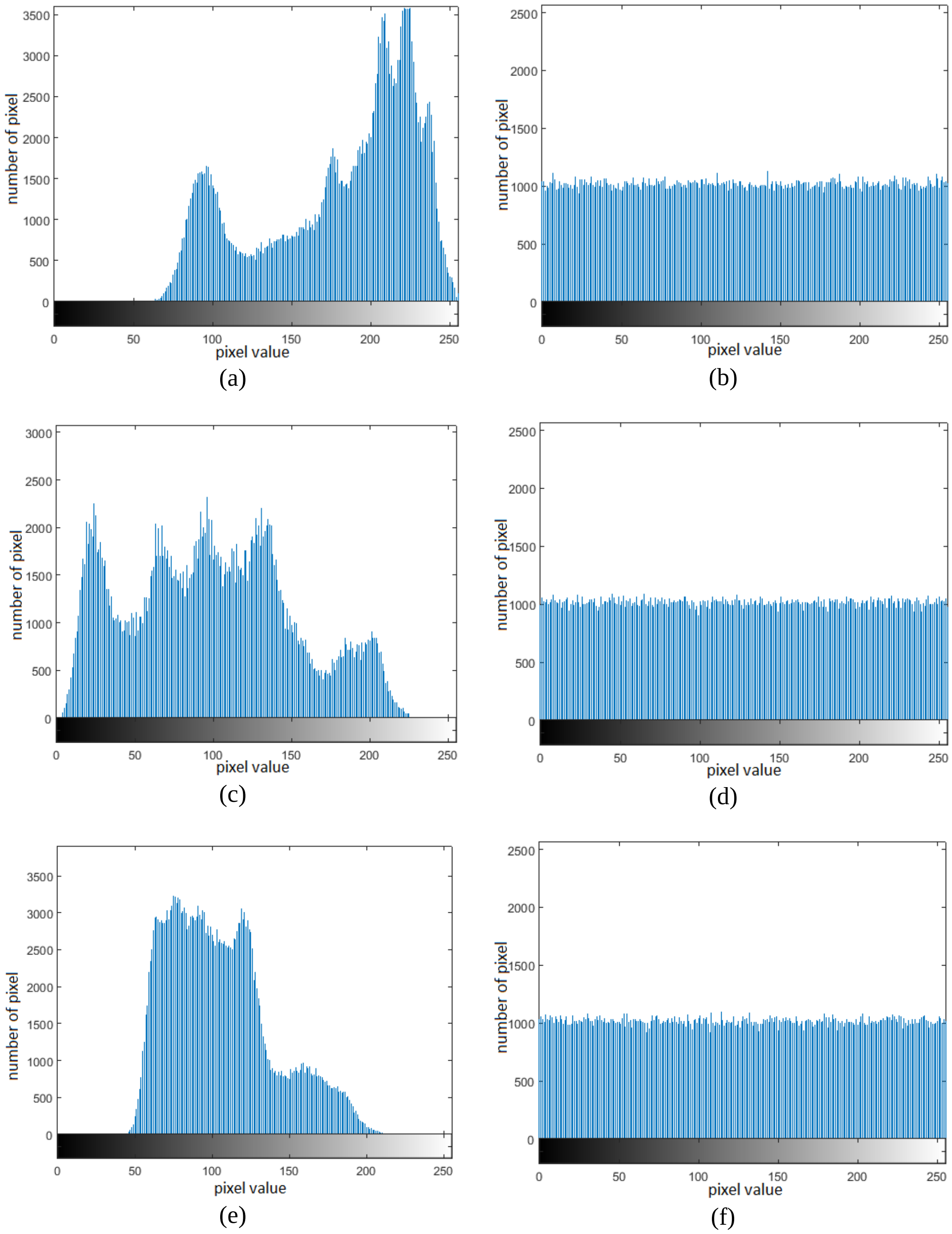
The measurement of encryption quality is shown in Table 1 and Table 2. In Table 1 there are several measurement results such as Entropy, MSE, PSNR, and SSIM, then in Table 2, there are NPCR and UACI. The entropy value produced from the whole image is very good because the entropy produced is close to 8 (maximum value)[20]. 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 [33]. 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

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



(a) (b) (c) (d) (e) (f)

Figure. 5 Histogram results: (a) original red channel, (b) encrypted red channel, (c) original green channel, (d) encrypted green channel, (e) original blue channel, and (f) encrypted blue channel

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 [30, 31]. The better the encryption quality, the histogram will show a more uniform intensity of the histogram value across all pixels. The distribution of pixel values will also be more even across all values in the range 0 to 255. Fig. 5 provides a histogram comparison of the original image and the encrypted 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

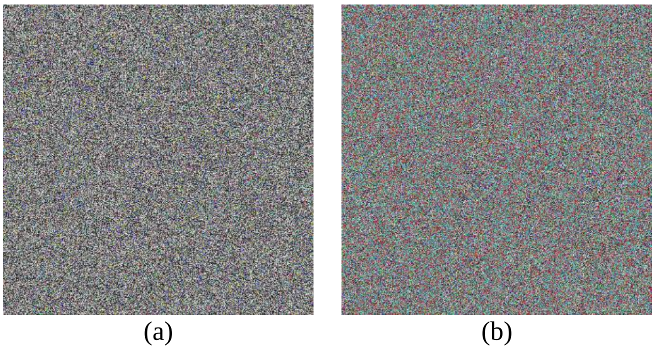


Figure. 6 Sample image encryption results: (a) encrypted Lena image and (b) encrypted baboon image

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 3.

The results shown in Table 3 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

Table 3. Image decryption measurement and results

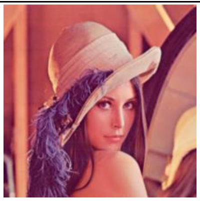
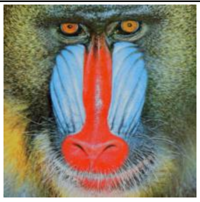
Image Name	MSE	PSNR	SSIM	Decrypting Time (seconds)	Results
Airplane	0	inf	0	2.420104	
House	0	inf	0	2.424534	
Lena	0	inf	0	2.536312	
Mandrill	0	inf	0	2.512338	
Sailboat	0	inf	0	2.511917	
Splash	0	inf	0	2.521384	

Table 4. Comparison with the previous method based on NPCR, UACI, and entropy on Lena image

Measurement Tools		**Ref** [22]	**Ref** [23]	**Ref** [24]	**Proposed**
NPCR	Red	99.6475	94.6836	99.6585	**99.5956**
	Green	99.6231	95.6836	99.6570	**99.6223**
	Blue	**99.5941**	98.6810	99.6570	99.6227
UACI	Red	33.5328	**33.4647**	33.5101	32.9805
	Green	33.2752	**34.5048**	33.5173	30.5929
	Blue	33.4394	35.4999	**33.4767**	27.6362
Entropy	Red	7.9808	-	7.9969 (average RGB)	**7.9994**
	Green	7.9811	-		**7.9993**
	Blue	7.9814	-		**7.9993**

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[22-24], where the comparison is done with the same image dataset, namely Lena's image, the comparison is presented in Table 4.

It should be noted that the three methods that are compared with the proposed method presented in Table 4 have several similarities, namely the three methods use a combination of the chaos method and the substitution model. Comparisons were also carried out on the same dataset, namely the Lena 24-bits color image. Although the substitution model used in the proposed method looks simpler, with the hybrid Vigenere and Beaufort cipher models it can produce the highest entropy value, which is close to 8. Likewise, the NPCR value also dominates, namely the red and green color channels are superior because it is closer to the ideal value, which is 99.6093. However, the proposed method has not yielded the best UACI value, which is ideally close to 33.4635. But with two more dominant gauge appears that the method is proved to have the best performance.

5. Conclusions

This study proposes a hybrid encryption substitution method for Vigenère and Beaufort algorithms combined with scramble encryption with the ACM method. 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 4, it can be seen that the contribution generated from this method, namely the NPCR and Entropy values of the proposed method are superior. The entropy value is very dominant with the highest value is 7.9994 while the best NPCR value is 99.5956. In addition, the computation of the proposed method is relatively fast, which is about 2 seconds with relatively standard computer specifications. However, the UACI value still needs to be improved in further research.

Conflicts of Interest

The authors 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.

Authors Contribution

Budi Harjo contributed to concept design, methodology, implementation, testing, and writing of the initial draft. De Rosal Ignatius Moses Setiadi contributed to the review, editing, supervision, and validation of the results.

References

[1] A. Setyono, D. R. I. M. Setiadi, and Muljono, "Dual encryption techniques for secure image transmission", *J. Telecommun. Electron. Comput. Eng.*, Vol. 10, No. 3–2, pp. 41–46, 2018.

[2] H. Diab, "An Efficient Chaotic Image Cryptosystem Based on Simultaneous Permutation and Diffusion Operations", *IEEE Access*, Vol. 6, pp. 42227–42244, 2018.

[3] D. R. I. M. Setiadi, "Improved payload capacity in LSB image steganography uses dilated hybrid edge detection", *J. King Saud Univ. - Comput. Inf. Sci.*, 2019.

[4] 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, 2017.

[5] 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, 2019.

[6] 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.

[7] M. Rathidevi, R. Yaminipriya, and S. V. Sudha, "Trends of cryptography stepping from ancient to modern", In: *Proc. IEEE International Conf. on Innovations in Green Energy and Healthcare Technologies*, 2017.

[8] L. Bao, S. Yi, and Y. Zhou, "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, 2017.

[9] A. Jolfaei, X. W. Wu, and V. Muthukkumarasamy, "On the Security of Permutation-Only Image Encryption Schemes", *IEEE Trans. Inf. Forensics Secur.*, Vol. 11, No. 2, pp. 235–246, 2016.

[10] 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.

[11] 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, 2018.

[12] 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.

[13]S. R. M. Halagowda and S. K. Lakshminarayana, "Image Encryption Method based on Hybrid Fractal-Chaos Algorithm", *International Journal of Intelligent Engineering and Systems*, Vol. 10, No. 6, 2017.

[14] 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.

[15] M. Kumar, R. Mishra, R. K. Pandey, and P. Singh, "Comparing Classical Encryption With Modern Techniques", *J. Phys. Sci. Eng. Technol.*, Vol. 1, No. 1, pp. 49–54, 2010.

[16] Q. Zhang and A. Qunding, "Digital image encryption based on Advanced Encryption Standard(AES) algorithm", In: *Proc. of International Conf. on Instrumentation and Measurement, Computer, Communication, and Control*, 2016, pp. 1218–1221.

[17] S. Pathak, R. Kamble, and D. Chaursia, "An efficient data encryption standard image encryption technique with RGB random uncertainty", In: *Proc. of International Conf. on Reliability, Optimization and Information Technology*, pp. 413–421, 2014.

[18] X. Wang and H. L. Zhang, "A color image encryption with heterogeneous bit-permutation and correlated chaos", *Opt. Commun.*, Vol. 342, pp. 51–60, 2015.

[19] H. M. Ghadirli, A. Nodehi, and R. Enayatifar, "An overview of encryption algorithms in color images", *Signal Processing*, Vol. 164, pp. 163–185, 2019.

[20] D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, A. Susanto, and M. Doheir, "A Comparative Study of Image Cryptographic Method", In: *Proc.of International Conf. on Information Technology, Computer, and Electrical Engineering*, pp. 336–341.

[21] M. Alawida, A. Samsudin, J. Sen Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption", *Signal Processing*, Vol. 160, pp. 45–58. 2019.

[22] H. Liu, A. Kadir, and P. Gong, "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, 2015.

[23] I. Hussain, T. Shah, and M. A. Gondal, "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, 2012.

[24] U. S. Choi, S. J. Cho, J. G. Kim, S. W. Kang, H. D. Kim, and S. T. Kim, "Color image encryption based on PC-MLCA and 3-D chaotic cat map", in *Proc. International Conference on Computer and Communication Systems*, pp. 272–277, 2019.

[25] V. Rekhate, A. Tale, N. Sambhus, and A. Joshi, "Secure and efficient message passing in distributed systems using One-Time Pad", In: *Proc. of International Conf. on Computing, Analytics and Security Trends*, 2017, pp. 393–397.

[26] 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.

[27] 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.

[28] L. Chen, D. Zhao, and F. Ge, "Image encryption based on singular value decomposition and Arnold transform in fractional domain", *Opt. Commun.*, Vol. 291, pp. 98–103, 2013.

[29] 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].

[30] 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, 2018.

[31] 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, 2017.

[32] D. R. I. M. Setiadi, "PSNR vs SSIM: imperceptibility quality assessment for image steganography", *Multimed. Tools Appl.*, pp. 1–22, 2020.

[33] M. A. Mokhtar, S. N. Gobran, and E. S. A. M. El-Badawy, "Colored image encryption algorithm using DNA code and Chaos theory", In: *Proc. of International Conf. on Computer and Communication Engineering: Emerging Technologies via Comp-Unication Convergence*, pp. 12–15, 2015.