An Enhancement of One Time Pad Based on Monoalphabeth Caesar Cipher to Secure Grayscale Image

Christy Atika Sari*[1], **Lalang Erawan**[2]
Universitas Dian Nuswantoro, Jl. Imam Bonjol No. 207 Semarang, (024) 3517261
E-mail : atika.sari@dsn.dinus.ac.id[1], lalang.erawan@dsn.dinus.ac.id[2]*
**Corresponding author*

Eko Hari Rachmawanto[3], **De Rosal Ignatius Moses Setiadi**[4], **Tan Samuel Permana**[5]
Universitas Dian Nuswantoro, Jl. Imam Bonjol No. 207 Semarang, (024) 3517261
E-mail : eko.hari@dsn.dinus.ac.id[3], moses@dsn.dinus.ac.id[4], tansamuelpermana95@gmail.com[5]

Abstract – Image is an object that has been used by various people since long ago. Utilization of these images evolve in line with advances in technology. Image in this information technology era is not only in a physical form, there is also a form of so-called digital image. Many people use digital images for personal use, so prone to be manipulated by others. Cryptographic technique, such as Caesar Cipher and OTP is a security techniques that can be applied to the digital image to avoid manipulation or theft of data image. The result is, an image can be read only by the sender and the recipient's image alone. Combined the two algorithms have fast turnaround time, up to 0.017791 seconds for the image to the size of 512x341 and 0.032302 seconds for the image to the size of 768x512. In addition, the resulting image has a very low degree of similarity, with the highest PSNR value obtained is 6.8653 dB. It can be concluded that the combined algorithm and OTP Caesar Cipher algorithm is fast and difficult to solve.

Keywords – Security, Image, One Time Pad, Caesar Cipher

1. INTRODUCTION

Image or image is an object that has been used by the public for a long time. The image has been widely used in various fields of life, ranging from the arts, economics, to the field of education. However, not everyone is always associated with the image activity, because its use is limited to certain activities such as painting, reading a picture book, and shooting with a film camera so that the image is rarely used. The changing times that happened to enter the 21st century, the era of information technology has created a world [1]. From this virtual world, the use of digital images increasingly widespread and easy to use even by ordinary people though. Not a few people who take advantage of access into this virtual world to do business, social relationships with colleagues, seeking knowledge, and so forth. Of the various activities in the virtual world, one of which is often done is to send digital images.

Digital imagery that is sent in this virtual world can be confidential, so there is a need for security of this personal digital image message. Of course everyone does not want the secret image message to be accessible to anyone other than the recipient, so it takes a technique to secure the digital image [2]. Cryptography is a technique for randomizing a message so that it can only be read by the sender and receiver. Caesar Cipher and OTP are one of the many techniques that exist in cryptography. Both techniques can provide security to digital images, by way of encryption or randomization of digital image messages to be used.

Alan Blair in 2013 [3] presented method to secure information based on substitution cryptography method, namely Caesar Cipher that has been combinated using Vigenere Cipher. Sari, et al [4] has been secured all file extensions by utilizing cryptographic process, namely Vernam Cipher to prevent data theft. Setiadi, dkk [5] in his research on testing the OTP algorithm to encode a data, which can be applied to various fields due to its very strong security level and has been combinated using Discrete Cosine Transform (DCT) in steganography techniques. Thus, the main objective of this study is to use Caesar Cipher and OTP techniques as a way to secure an image data in digital form, so that it can not be used by others who have no authority to access the image data.

2. RESEARCH METHOD

2.1. Cryptography

First used by the Spartans of Greece [6], cryptography is a useful science to secure or hide an important message, derived from the Greek language that is cryptos and graphein which means hidden and written. Cryptography was originally only used for the military field to secure the secret messages used during the war, but the more changing times, the use of cryptography also began to change [7]. The current era of information technology, not only the use of cryptography for the military alone, but also education and economics.

Cryptography has 5 devices [6,7] namely Plain text, encryption, decryption, key, and ciphertext. Plain text is the original message, while the ciphertext is the result message of encryption or random message. Encryption itself is a process for randomizing the original message so that it can not be read by others. In order for the recipient to read the ciphertext, it needs decryption to return the ciphertext to plain text. Key itself is needed to perform the process of decryption and encryption. The process of cryptography itself can be seen in Figure 1.

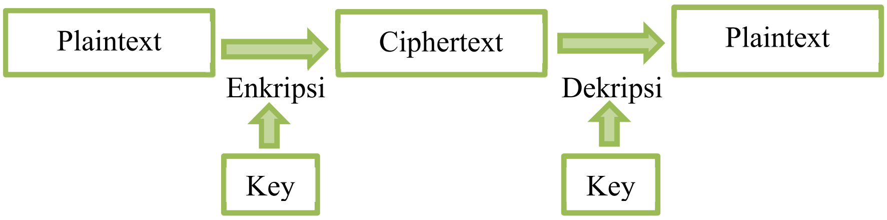


Figure 1. Commonly Cryptography Scheme

The main purpose of using cryptography is to maintain the confidentiality of a data [10]. The importance of data confidentiality is that the data can only be read by the creator and recipient of the message only [11], so that the data can not be accessed by others who do not have access rights. Cryptography consists of two parts: classical and modern cryptography [12]. Classical cryptography is divided into substitutions (Monoalphabetic and Poly Alphabetic) and transposition. As for modern cryptography, divided into symmetrical cryptography (Block Cipher and Stream Cipher) and asymmetric cryptography. Symmetric cryptography is cryptography with the same encryption and decryption keys, while asymmetric cryptography is cryptography with different encryption and decryption keys. More details can be seen in Figure 2.

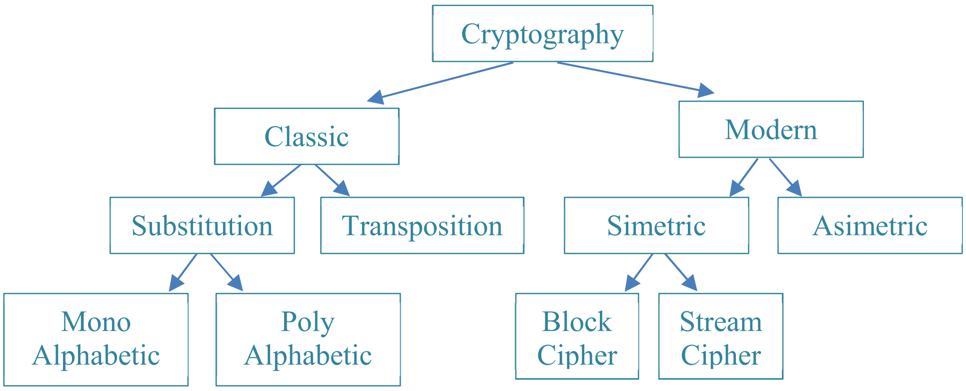


Figure 2. Cryptography Classification

Caesar Cipher is an algorithm in classical cryptography that uses substitution techniques in its encryption process [1]. Caesar Cipher itself is the first substitution algorithm found by Julius Caesar. Caesar Cipher works by replacing each character from plain text with the same key, so the formula is:

$$Ci = (Pi + k) \; mod \; 26 \qquad (1)$$

"*Pi*" is plain text to be encrypted, while '*k*' is the key. The process of encrypting plain text that amounts to 256 characters equals 26 characters, the difference lies only in the module. So we get the formula:

$$Ci = (Pi + k) \; mod \; 256 \qquad (2)$$

The decryption process uses the same key as the encryption process, in which the ciphertext is subtracted by the key, to obtain the formula:

$$Pi = (Ci - k) \; mod \; 26 \qquad (3)$$

Ciphertext with 256 characters has the same decryption process, the difference lies only in modulo, so get the formula:

$$Pi = (Ci - k) \; mod \; 256 \qquad (4)$$

2.2. One Time Pad (OTP)

OTP is a very powerful classical substitution algorithm. OTP is a substitution algorithm with a formula similar to Caesar Cipher that adds plain text with key, only the keys used are always different. The formula is:

$$Ci = (Pi + ki) \; mod \; 26 \qquad (5)$$

Plain text with 26 characters must be 26, and plain text with 256 characters must be modified with 256 as well, so the formula is:

$$Ci = (Pi + ki) \; mod \; 256 \qquad (6)$$

Decryption process is the same as encryption, only to be processed is ciphertext it by subtracting with key for encryption, so got formula:

$$Pi = (Ci - \ ki) \ mod \ 26 \tag{7}$$

Just like the 26 character ciphertext, for the process of decrypting ciphertext 256 different characters is just the number of module only, so the formula:

$$Pi = (Ci - ki) \ mod \ 256 \tag{8}$$

An algorithm can be said to be a OTP and unbreakable algorithm if it meets 3 main requirements [7]. First, the key to the encryption process of each character from the plain text is always different. Second, the key used must have the same character length as the plain text. And the last is the key to the encryption process is only used once.

2.3. Histogram

The color change of a digital image can be seen using a histogram, which will show the color difference from the initial image before the encryption process, and the image of the encryption process [13]. The importance of using this histogram is to analyze the level of color randomness.

2.4. MSE and PSNR

MSE (Mean Square Error) can be used to see the error value between the original image and the inserted image [14], while the PSNR (Peak Signal to Noise Ratio) [15] can see the quality or resemblance of the original image and the image the message has inserted . The formula for finding MSE is:

$$MSE = \frac{1}{N\,M} \sum \begin{matrix} M-1 \\ m=0 \end{matrix} \sum \begin{matrix} N-1 \\ n=0 \end{matrix} (m,n)^2 \tag{9}$$

Where (m, n) is the error value of the original image and the colored image, whereas N and M are the number of row and column pixels of the image. Having obtained the value of MSE PSNR can be searched it:

$$PSNR = 10 \log \frac{S^2}{MSE} \tag{10}$$

S represents 255 for 8-bit images. Images that have a good resemblance will have a PSNR value above 40 dB (deciBel), and a low MSE value. While images that have a poor resemblance will have a PSNR value below 40 dB and a large MSE value.

3. RESEARCH METHOD

From Figure 3, we can explain the research model as follows:

1. Prepare digital image messages to be processed.
2. Input the original image, then encrypt with Caesar Cipher with the key that has been prepared.

3. Once you get the cipher file Caesar, encrypt again with OTP with the key that has been prepared and will get cipher file OTP.
4. The next process is decryption, before the decryption process begins, inputkan cipher file to be described.
5. After that decrypt with OTP and the key used is the same key as when the encryption process and will get cipher file Caesar.
6. Cipher file Caesar that has been obtained, decrypted with Caesar Cipher with the same key as well as during the encryption process.
7. It will get the original digital image message or plain file.

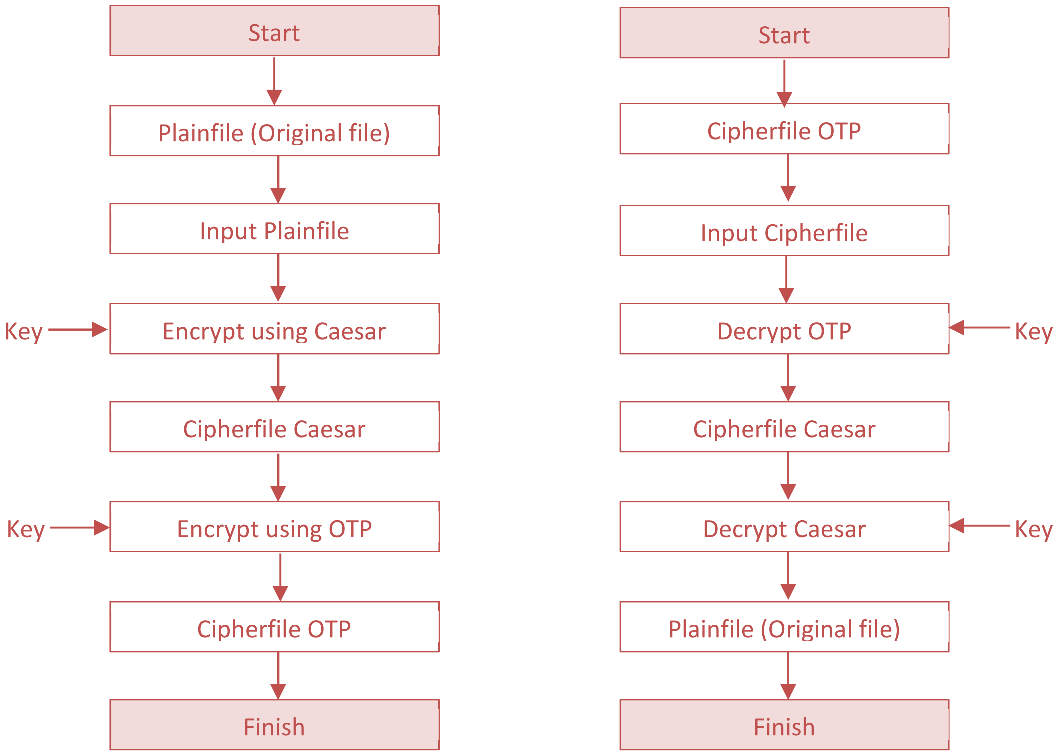
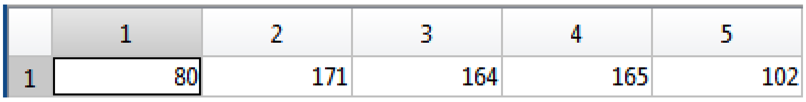


Figure 3. Proposed Method

4. RESULT AND DISCUSSION

The algorithm to be used for the first encryption process is a Caesar Cipher with a key of 111. The sample to be used for calculation is grayscale image with the name water.png (Figure 4) and has a 512x341 size. The color to be tested is taken from the 1st row of the 1st column to the 1st row of the 5th column (Figure 5). The formula to be used is *Ci = Pi + k mod 256*.

Figure 4. Water.png



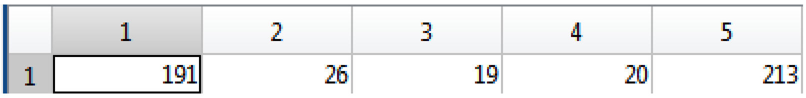
	1	2	3	4	5
1	80	171	164	165	102

Figure 5. Plain text from water.png

Based on the plain text of Figure 4, the following calculations can be calculated:

$C_{(1,1)}$ = (80+111) mod 256 = 91 mod 256 = 191
$C_{(1,2)}$ = (171+111) mod 256 = 282 mod 256 = 26
$C_{(1,3)}$ = (164+111) mod 256 = 275 mod 256 = 19
$C_{(1,4)}$ = (165+111) mod 256 = 276 mod 256 = 20
$C_{(1,5)}$ = (102+111) mod 256 = 213 mod 256 = 213

Then we will get the image Caesar Cipher encryption results. Ciphertext and Image Caesar Cipher encryption can be seen in Figure 6 and Figure 7.



	1	2	3	4	5
1	191	26	19	20	213

Figure 6. An Encrypted Caesar Cipher

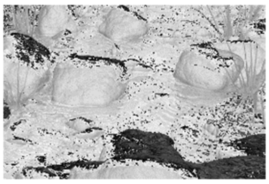
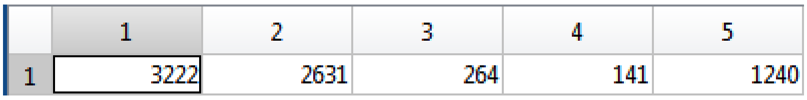


Figure 7. Image encryption results using Caesar Cipher

After the Caesar Cipher process is done, the next encryption process is OTP. The Caesar Cipher encryption image is again encrypted with OTP with the OTP key (Figure 8) that has been prepared. The OTP encryption formula is *Ci = Pi + ki mod 256.*



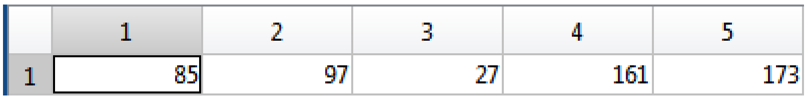
	1	2	3	4	5
1	3222	2631	264	141	1240

Figure 8. OTP Key

With the key above, we get the OTP text cipher:

$C_{(1,1)}$ = (191+3222) mod 256 = 3413 mod 256 = 85
$C_{(1,2)}$ = (26+2631) mod 256 = 2657 mod 256 = 97
$C_{(1,3)}$ = (19+264) mod 256 = 283 mod 256 = 27
$C_{(1,4)}$ = (20+141) mod 256 = 161 mod 256 = 161
$C_{(1,5)}$ = (213+1240) mod 256 = 1453 mod 256 = 173

OTP text will be obtained, can be seen in Figure 9. The resulting image, shown in Figure 10.



	1	2	3	4	5
1	85	97	27	161	173

Figure 9. Encrypted File using OTP

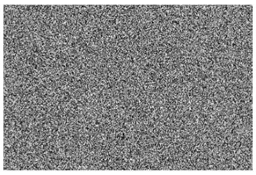
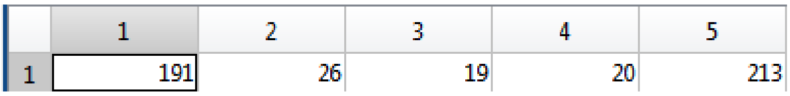


Figure 10. Image encryption results using OTP

Decryption is required to enable the recipient to read the contents of the received digital image message. Because the last encryption process is OTP, then the first decryption process is OTP. OTP is symmetric cryptography so the key used is the same as during encryption. The formula *Pi = Ci - ki mod 256*. The process of calculation:

$P_{(1,1)}$ = (85-3222) mod 256 = (-3137) mod 256 = 191
$P_{(1,2)}$ = (97-2631) mod 256 = (-2534) mod 256 = 26
$P_{(1,3)}$ = (27-264) mod 256 = (-237) mod 256 = 19
$P_{(1,4)}$ = (161-141) mod 256 = (20) mod 256 = 20
$P_{(1,5)}$ = (173-1240) mod 256 = (-1067) mod 256 = 213

After the decryption process is done, it will get back ciphertext Caesar his and the image of Caesar Cipher encryption (before encrypted with OTP) can be seen in Figure 11 and Figure 12.



	1	2	3	4	5
1	191	26	19	20	213

Figure 11. Ciphertext Result using OTP

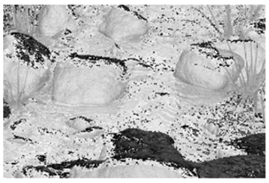
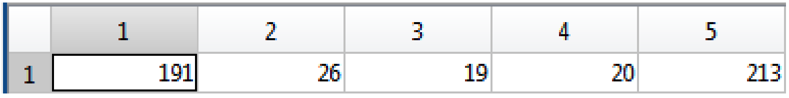


Figure 12. Image Result using OTP

The final decryption process will be done with Caesar Cipher. Just like OTP, the key used is the same as encryption, which is 111. The formula is *Pi = Ci - k mod 256*. Here is the process of completion:

$P_{(1,1)}$ = (191-111) mod 256 = 85 mod 256 = 80
$P_{(1,2)}$ = (26-111) mod 256 = (-85) mod 256 = 171
$P_{(1,3)}$ = (19-111) mod 256 = (-92) mod 256 = 164
$P_{(1,4)}$ = (20-111) mod 256 = (-91) mod 256 = 105
$P_{(1,5)}$ = (213-111) mod 256 = 102 mod 256 = 102

After going through the final decryption process, it will get the original plain text which if the process of decryption has been correct, then plain text the image of the decryption and the original image must be the same, can be seen in Figure 13. The final result obtained is the image of the decryption or original image, shown in Figure 14.



	1	2	3	4	5
1	191	26	19	20	213

Figure 13. Ciphertext result using Caesar Cipher Plaintext

Figure 14. Image Result using OTP

Software used in this research is Matlab R2015b. The object to be studied is taken from petitcolas.net [9], totaling 10 digital images, divided into 2 pixel sizes, 512x341 and 768x512, each measuring 5 digital images. The image used is grayscale image with PNG file format. The key used for encryption and decryption of Caesar Cipher is worth 111, while for OTP ranges from 0-5000.

Table 1. Time Execution for Encryption and Decryption Process

No	Name of Image	Time Execution (second)			
		Encryption		Decryption	
		512x341	768x512	512x341	768x512
1	newyork.png	0,017168	0,032667	0,014426	0,031412
2	st1x20.png	0,018150	0,032045	0,014494	0,029451
3	terraux.png	0,016580	0,031903	0,014478	0,029598
4	water.png	0,018393	0,032991	0,015342	0,030667
5	z1x25.png	0,018663	0,031904	0,014979	0,030485
Average		0,017791	0,032302	0,014744	0,030323

Table 1 shows the comparison of processing times of each process, both encryption and decryption processes. It is seen that the image pixel size influences the speed of the encryption process as well as the decryption.

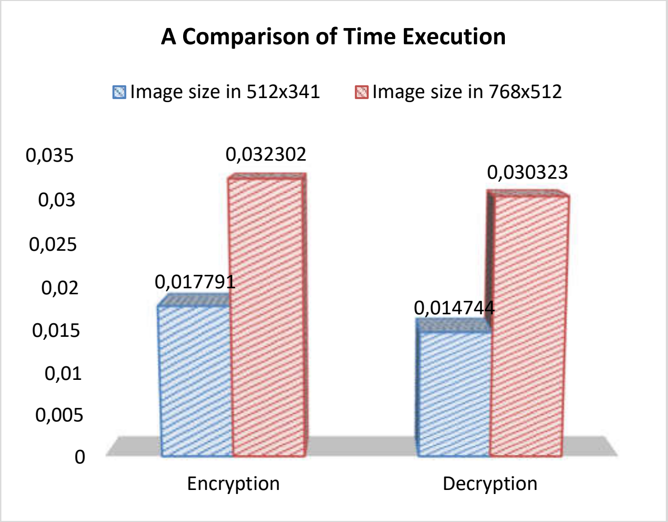


Figure 15. Graphic of Time Execution between Encrytion and Decryption

Based on the graph in Figure 15, it appears that the decryption process is faster than the image encryption process. Imagery with 768x512 pixel size takes time for encryption and decryption process that is longer than image with 512x341 pixel size. This indicates that the image size affects the speed of the encryption and decryption process.

Table 2. The Changes of Image File

No	Nama Citra	Size File Citra (KB)			
		Citra Asli		Enkripsi	
		512x341	768x512	512x341	768x512
1	newyork.png	112	245	171	385
2	st1x20.png	95	193	171	385
3	terraux.png	98,3	209	171	385
4	water.png	129	272	171	385
5	z1x25.png	105	239	171	385
Average		107,9	231,6	171	385

Based on the results of the research in Table 2, shows the change in image file size after the encryption process. All encrypted images of the same pixel size have the same size.

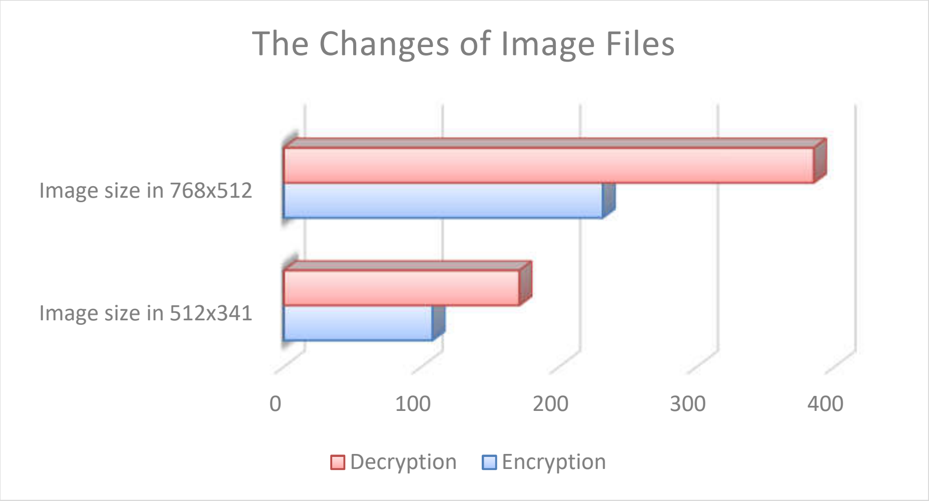
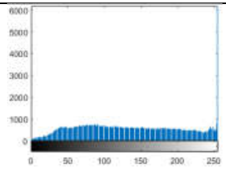
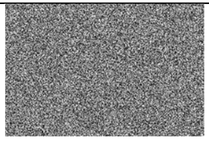
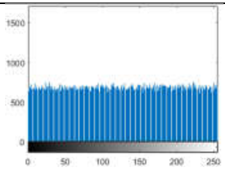
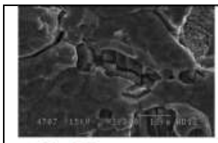
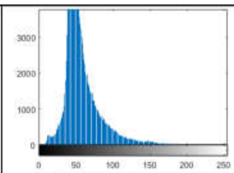
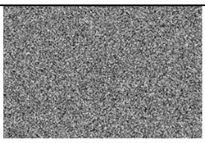
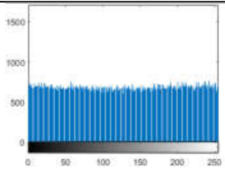
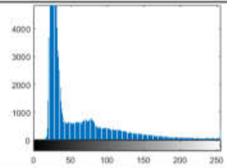
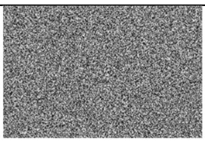
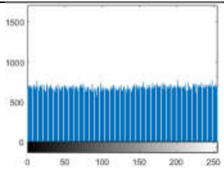
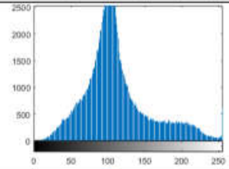
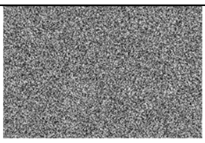
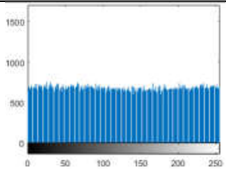
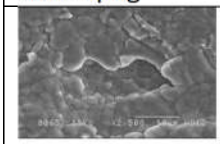
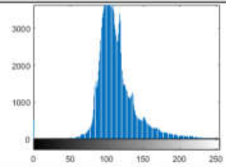
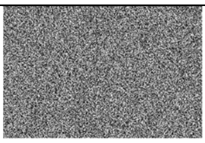
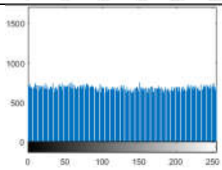


Figure 1 The Changes of Image Files

Figure 16 shows the graph of image file size of encryption process result. Image file size changes size large enough. Good for images with 512x341 or 768x512 pixel size, both have image file size changes.

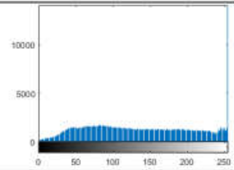
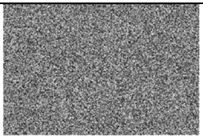
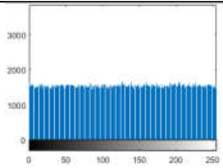
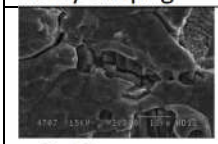
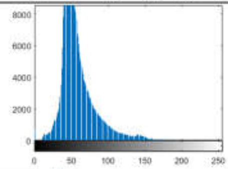
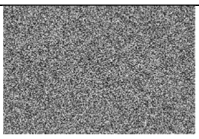
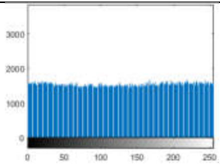
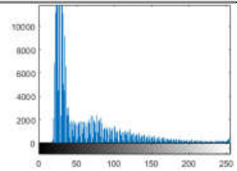
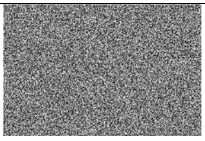
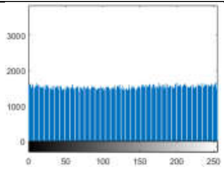
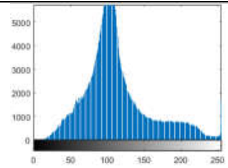
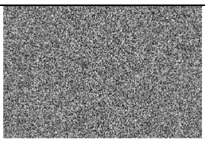
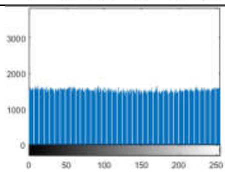
Table 3. Histogram of Image with size in 512x341

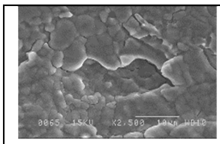
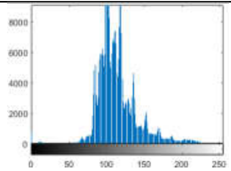
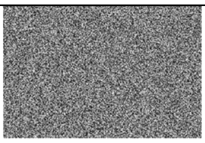
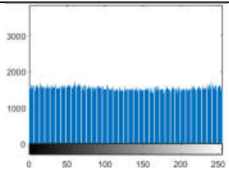
Original Image	Histogram Of Original Image	Encrypted Image	Histogram Of Encrypted Image
 newyork.png			

 st1x20.png			
 terraux.png			
 water.png			
 z1x25.png			

Based on Table 3, it can be seen that the image encryption size 512x341 has a good level of randomness, because the distribution of color in each pixel evenly, so it will be difficult to look for certain instructions to solve it.

Table 4. Histogram of Image with size in 756x512

Citra Asli	Histogram Citra Asli	Citra hasil enkripsi	Histogram Citra Hasil Enkripsi
 newyork.png			
 st1x20.png			
 terraux.png			
 water.png			

 z1x25.png			

Similar to Table 3, Table 4 also shows a good level of image randomness for the size of 756x512, because the distribution of colors per pixel is evenly distributed. The attackers will not find clues to solve the image of the encryption.

Table 5. MSE Value between Encrypted dan Decrypted Image Nilai MSE

No	Nama Citra	MSE			
		Enkripsi		Dekripsi	
		512x341	768x512	512x341	768x512
1	newyork.png	12400,997	12471,867	0	0
2	st1x20.png	11082,654	11024,017	0	0
3	terraux.png	13383,047	13315,805	0	0
4	water.png	7699,798	7709,707	0	0
5	z1x25.png	6378,897	6377,582	0	0

Based on Table 5, the encrypted image has a high degree of randomness, because the error value obtained from the MSE calculation is high enough. As for the process of decryption, resulting in a value of 0, which means there is absolutely no error between the image of the decryption with the original image indicating that the two pieces of the image is the same image or identical.

Table 6. PSNR Value between Encrypted dan Decrypted Image

No	Nama Citra	PSNR (dB)			
		Enkripsi		Dekripsi	
		512x341	768x512	512x341	768x512
1	newyork.png	7,1962	7,1715	Infinite	Infinite
2	st1x20.png	7,6844	7,7074	Infinite	Infinite
3	terraux.png	6,8653	6,8871	Infinite	Infinite
4	water.png	9,2660	9,2604	Infinite	Infinite
5	z1x25.png	10,0833	10,0842	Infinite	Infinite

Table 6 shows that the encrypted image has a very small degree of similarity, since the PSNR value is below 40 dB. In addition, the process of decryption successfully restore the image to its original shape because it has infinite value.

4. CONCLUSION

Based on the results of tests that have been done, it has been proved that the highest MSE value is 6377,582 with 768x512 image size, while the value of MSE decrypted on all images is 0. This indicates that the decryption process goes well. Another test by calculating PSNR, it is known that the encryption process produces a small PSNR value which means the image has been through the encoding process correctly. This is different from the watermarking technique that results in high PSNR values. In cryptography, the low value of PSNR actually indicates that the process has been running well. In the decryption process, the image size of 512x341 and 768x512 has resulted in infinite value.

The conclusion is that the combined algorithm of Caesar Cipher and OTP is very strong and difficult to solve. In addition, this algorithm has a very fast processing time, up to 0.017791 seconds. But the disadvantage is the encryption process causes the image file size to be larger than the original size before it is encrypted.

The suggestions for further research are that they can be implemented with GUI and with colors other than grayscale. In addition, the cryptographic object can be applied to other file types such as text, audio and video.

REFERENCES

[1] J. Thakur and N. Kumar, “DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis,” *Int. J. Emerg. Technol. Adv. Eng.*, vol. 1, no. 2, pp. 6–12, 2011.

[2] M. G. V. Kumar and U. S. Ragupathy, “A Survey on current key issues and status in cryptography,” in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2016, pp. 205–210.

[3] A. Blair, “Learning the Caesar and Vigenere Cipher by hierarchical evolutionary re-combination,” in *2013 IEEE Congress on Evolutionary Computation*, 2013, pp. 605–612.

[4] C. A. Sari, E. H. Rachmawanto, D. W. Utomo, and R. R. Sani, “Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan Kriptografi Vernam Cipher dan Bit Shiffting,” *J. Appl. Intell. Syst.*, vol. 1, no. 3, pp. 179–190, 2016.

[5] D. R. I. M. Setiadi, E. H. Rachmawanto, and C. Sari, “Secure Image Steganography Algorithm Based on DCT with OTP Encryption,” *J. Appl. Intell. Syst.*, vol. 2, no. 1, pp. 1–11, 2017.

[6] A. Al-haj and H. Abdel-nabi, “Digital Image Security Based on Data Hiding and Cryptography,” in *International Conference on Information Management Copyright*, 2017, pp. 437–440.

[7] L. Erawan, C. A. Sari, and E. H. Rachmawanto, “Lalang_Erawan_Implementasi_Kriptografi_Simetris_OTP,” in *Seminar Nasional Multidisiplin Ilmu Universitas Budi Luhur Jakarta*, 2017.

[8] C. A. Sari and E. H. Rachmawanto, “Gabungan Algoritma Vernam Chiper Dan End of File,” *Techno.COM*, vol. 13, no. 3, pp. 150–157, 2014.

[9] E. H. Rachmawanto and C. A. Sari, “Keamanan File Menggunakan Teknik Kriptografi Shift Cipher,” *Techno.COM*, vol. 14, no. 4, pp. 329–335, 2015.

[10] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, “Digital Image Steganography : Survey and Analysis of Current Methods,” *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.

[11] C. Sari, E. Rachmawanto, Y. Astuti, and L. Umaroh, “Optimasi penyandian file menggunakan kriptografi shift cipher,” in *Seminar Multi Disiplin Ilmu Unisbank (SENDI_U) ke-2 Semarang*, 2016.

[12] Y. P. Astuti, E. H. Rachmawanto, and C. A. Sari, “Optimasi Enkripsi Password Menggunakan Algoritma Blowfish,” *Techno.COM*, vol. 15, no. 1, pp. 15–21, 2016.

[13] X. Li, W. Zhang, B. Ou, and B. Yang, “A brief review on reversible data hiding: Current techniques and future prospects,” in *2IEEE China Summit & International Conference on Signal and Information Processing (ChinaSIP)*, 2014, pp. 426–430.

[14] R. Jain and J. B. Sharma, “Symmetric color image encryption algorithm using fractional

DRPM and chaotic baker map," in *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 2016, pp. 1835–1840.

[15] A. Goswami and S. Khandelwal, "Hybrid DCT-DWT Digital Image Steganography," *Int. J. Adv. Res. Comput. Commun. Eng. Vol.*, vol. 5, no. 6, pp. 228–233, 20 99o16.