Jurnal Ilmu Komputer dan Informasi (Journal of a Science and Information). 12/1 (2019), 41-49
DOI: http://dx:doi:org/10:21609/jiki:v12i1:646

GOOD PERFORMANCE IMAGES ENCRYPTION USING SELECTIVE BIT T-DES ON INVERTED LSB STEGANOGRAPHY

Christy Atika Sari, Eko Hari Rachmawanto, and Edi Jaya Kusuma

Department of Informatics Engineering, Faculty of Computer Science, Dian Nuswantoro University, Jl. Imam Bonjol 207, Semarang, 50131, Indonesia

E-mail: christy.atika.sari@dsn.dinus.ac.id

Abstract

Transmitting image through the internet needs to be secured because of risk to be stolen. Security techniques that can be used for securing data especially image are cryptography and steganography. Combine these techniques can provide double protection in image security. In this research, we proposed the used of T-DES encryption with a selective bit to improve the time performance because time aspect is one of the important aspects of data transmission process. Four MSB of the secret image will be selected, then it will be encrypted using T-DES. After that, this encrypted results will be combined with other 4 LSB. This encryption scheme result will be embedded into a cover image using inverted LSB because inverted LSB can produce high imperceptible value. From 6 testing images which encrypted using proposed scheme present that proposed encryption scheme is twice faster than classic triple DES and slightly faster than double DES. While the embedding scheme can produce PSNR value above 40 dB with the range between 51 dB to 61 dB as well as SSIM which close to 1. This result denoted that proposed scheme generated good quality of stego images.

Keywords: *Cryptography, T-DES, Steganography, LSB, images*

Abstrak

Mengirimkan gambar melalui internet perlu diamankan karena risiko dicuri. Teknik keamanan yang dapat digunakan untuk mengamankan data terutama gambar adalah kriptografi dan steganografi. Menggabungkan teknik-teknik ini dapat memberikan perlindungan ganda dalam keamanan gambar. Dalam penelitian ini, kami mengusulkan penggunaan enkripsi T-DES dengan bit selektif untuk meningkatkan kinerja waktu karena aspek waktu adalah salah satu aspek penting dari proses transmisi data. Empat MSB dari gambar rahasia akan dipilih, kemudian akan dienkripsi menggunakan T-DES. Setelah itu, hasil terenkripsi ini akan digabungkan dengan 4 LSB lainnya. Hasil skema enkripsi ini akan ditanamkan ke dalam gambar cover menggunakan LSB terbalik karena LSB terbalik dapat menghasilkan nilai tak terlihat yang tinggi. Dari 6 pengujian gambar yang dienkripsi menggunakan skema yang diusulkan, skema enkripsi yang diusulkan dua kali lebih cepat daripada DES tripel klasik dan sedikit lebih cepat daripada DES ganda. Sedangkan skema embedding dapat menghasilkan nilai PSNR di atas 40 dB dengan kisaran antara 51 dB hingga 61 dB serta SSIM yang mendekati 1. Hasil ini menunjukkan bahwa skema yang diajukan menghasilkan kualitas gambar stego yang baik.

Kata Kunci: *Kriptografi, T-DES, Steganografi, LSB, citra*

1. Introduction

Data is a representation of an entity in the world. Through the internet, people can access and transfer the data each other. Some types of data can be easily accessed by the public, but there are also private data where only a few people have special privileges. Due to limited access, some people attempt to steal important data. Furthermore, sending private data through the internet has a risk to be stolen. Therefore Security techniques need to be implemented to prevent these data security issues.

Cryptography is the science used to protect data from people who don't have permission. Currently, there are several cryptography techniques that often used in data security such as DES, AES, RSA, OTP, MD5, etc [1]–[3]. DES or Data Encryption Standard was becoming the standard of encryption in 1976 before being replaced by AES [4]. However, DES recently still be used in ATM machine and mobile phone operator sim card [1]. DES has the 64 bit of key and effectively used only 56 bit. Therefore, Some researcher proposed modified DES, for instance, DES, DESX, Double DES, Triple DES, etc. Triple-DES or T-DES is one of DES modification where perform DES encryption in 3 times with 3 different keys [5]. This modification can solve the issue of key length on DES and also can resist the brute-force attack. Using 3 different keys means the length key that used is 192 bits. But based on [ ], the effective key that used in T-DES only 168 bit. Due to use of DES encryption 3 times, its means T-DES has high complexity [6]. T-DES is slow compared to the other block cipher techniques [7]. Especially when encrypting a file that has many blocks such like image file that consisted of 8 bit in each image pixel. To reduce the processing time of encryption and decryption some research proposed selective image encryption, for instance, Li et al [8] proposed selective image encryption using Chaotic maps and DNA coding. Selective image means only encrypted half of image pixel bit-plane (four most significant bit of image pixel). This selective image encryption scheme can improve the encryption speed. Other research [9], proposed selective medical image encryption using JPEG compression algorithm. This scheme can reduce the processing time of encryption and decryption, where only 9% until 43% image information that encrypted. Merging T-DES with selective image encryption can enhance the processing time and it can resist brute-force attack.

Integrated cryptography and steganography to increase the information security have been done by several studies [1], [5], [10]. Steganography is the science used to hide message into cover media (audio, images, video, etc) [11]. File media that often used in steganography is images [12]. There is some method in image steganography such as LSB, PVD, DWT, DCT, etc. LSB or Least Significant Bit has advantages in execution time and it can produce good quality of stego-file. This is because the process of LSB is directly inserted the messages into each image pixel [13]. Kusuma et al [1], proposed LSB which inserted into edges areas of the image to increased the imperceptibility value. Actually, LSB has a drawback because of its simple process so that the attacker can easily extract the message directly [14]. Hence LSB needs to be modified to deceive the attacker while they tried to extract the messages without reducing its imperceptibility value. One modification that can confuse attacker and also provide the good imperceptible value of stego-file is inverted LSB. Akhtar et al [15] proposed inverted LSB scheme which used 3 LSB of the original cover image as a pattern to calculate the probability of changed bit and also to determine which pattern will be inverted. Bhardwaj et al [16] also combined inverted LSB scheme with bit complement to improve the security of secret messages. Therefore, this research will combine the selection bit T-DES with Inverted LSB to improve the performance as well as the imperceptible value and also provide double protection in images exchanged.

2. Research Method

2.1 Literature Review

2.1.1 Triple DES (T-DES)

Triple DES or T-DES is a modification of DES which operates DES encryption three times. T-DES required three 64-bit difference keys to encrypt 64-bit block messages means that it used 192-bit keys (3×64=192) to perform one block encryption. Because in DES encryption the effective key that used only 56-bit then the effective key that used in T-DES is 168-bit (3×56=168). Meanwhile, based on [4], the security level of T-DES that applied three different keys is 112-bit. The Encryption process of T-DES which used three different keys are shown below:

$$Cipher = Enc(\,Dec(\,Enc(\,P, K1\,), K2\,), K3\,) \qquad (1)$$

$$Plain\,Text = Dec(\,Enc(\,Dec(C, K3\,), K2\,), K1\,) \qquad (2)$$

where,
P = Plaintext,
C = Ciphertext,
K1 = First key,
K2 = Second key,
K3 = Thirth key,
Enc = Encryption using DES,
Dec = Decryption using DES.

To encrypt the message or plaintext as shown in Equation 1, firstly the message will be encrypted using K1 then the result will be decrypted using K2 and finally encrypted again with K3. While to decrypt the ciphertext in Equation 2, the ciphertext will be decrypted using K3 then encrypted using K2 and finally decrypted using K1. Each encryption and decryption process using DES algorithm and each key that used is independent key.

2.1.2 Inverted LSB

Inverted LSB steganography is a modification of classic LSB which can provide better security than LSB as well as improved imperceptibility of stego-file. Akhtar et al [15] proposed the inverted LSB scheme where it can misguide the steganalysis attack and complicated the message reconstruction process because several bits have been inverted. To perform inverted LSB The process of inverted LSB is the message bit will be inserted into LSB of each pixel using classic LSB. Here for example: message bits 1 0 0 1 1 0 1 0 1 will be hidden into nine image pixels:

01100100	00110011	10101011
10010011	10010010	10000110
11001110	11000101	11111001

After insertion using classic LSB:

01100101	00110010	10101010
10010011	10010011	10000110
11001111	11000100	11111001

After that, used 2nd and 3rd LSB bitplane to determine the pattern and also considered LSB of the original cover image to add more difference pattern [15]. below is the pattern that showed in red font.

01100101	00110010	10101010
10010011	10010011	10000110
11001111	11000100	11111001

Then, calculate the appearance of the changed bit after insertion process in each LSB of each pattern. If the probability of the changed bit is above 50% then it will be inverted.

TABLE 1
THE PROBABILITY OF EACH PATTERN BASED ON APPEARANCE OF THE CHANGED BIT

Pattern	Total appearance	The changed bit	LSB	Appearance	Changed Bit	The probability of Changed Bit (%)	Invert?
00	1	0	0	0	0	0	No
			1	1	0	0	No
01	4	3	0	1	1	100	Yes
			1	3	2	66,6	Yes
10	2	2	0	1	1	100	Yes
			1	1	1	100	Yes
11	2	1	0	2	1	50	Yes
			1	0	0	0	No

After calculating the probability of the changed bit, then invert LSB based on the probability result on Table 1.

01100100	00110011	10101011
10010010	10010010	10000111
11001110	11000101	11111001

The total changed pixel in inverted LSB only 2 pixels compared to classic LSB that has 5 changed pixel. This means that invert LSB can provide good quality stego-file especially increased imperceptibility value [16].

2.1.3 Sample Images

To perform this study, we used 3 color images with 64×64 image size and 3 grayscale images with 128×128 image size as secret images. Then for cover images, we used 2 color images and 2 grayscale images with 512×512 image size. All images in BMP format and taken from this source [17].

Figure 1. Secret Images Database: (a) house.bmp, (b) F16.bmp, (c) lena.bmp, (d) indian.bmp, (e) aerial.bmp, (f) tank.bmp

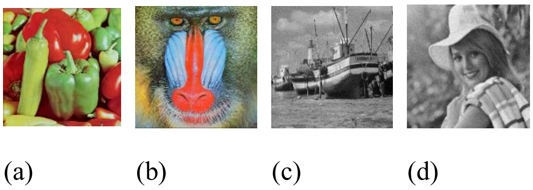


Figure 2. Cover Image Database: (a) peppers.bmp, (b) baboon.bmp, (c) boat.bmp, (d) elaine.bmp

2.2 Proposed Method

According to the processing time issue of T-DES, the author proposed a selective bit T-DES to secure image file. Selective bit or selective encryption is encryption process that only encrypts four MSB of each pixel bitplane of the image. This scheme can reduce processing time in the encryption process and decryption process. In addition, to strengthen the security, we combine this proposed encryption scheme with inverted LSB steganography. This combination can provide double protection as well as a good performance, especially in processing time. Inverted LSB steganography also produced good quality of stego-file. Our proposed method consists of two scheme which is embedding scheme where the secret image is encrypted and inserted into cover images and extracting scheme where we retrieved the cipher image from stego-file and perform decryption process to get the secret image.

2.2.1 Embedding Scheme

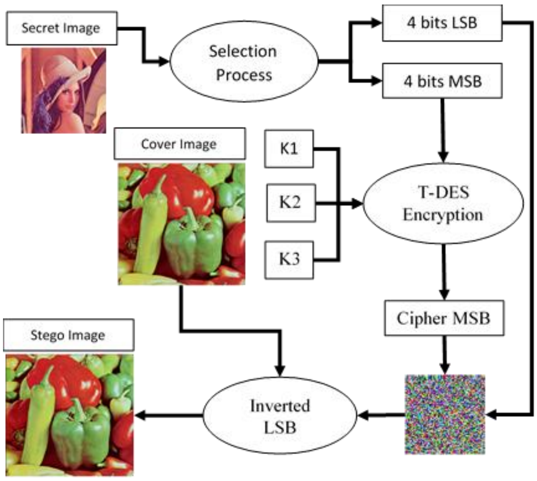


Figure 3. Proposed Embedding Scheme using Selective Bit T-DES and Inverted LSB

Proposed embedding scheme in Figure 3 can be derived into two parts which are encryption and insertion process. At encryption process, firstly choose a secret image and also cover image, then select 4 bit of MSB of each secret image pixel. After that, input three independent keys which will be used by T-DES to encrypt this selection result. Then combine the encryption result with another 4 bit left. This result will be inserted into a cover image using classic LSB. After that calculate the probability of the changed bit in each pattern to determine which pattern will be inverted. Finally, invert the bit in each pattern depend on the probability result and save the result as stego image file.

2.2.2 Extracting Scheme

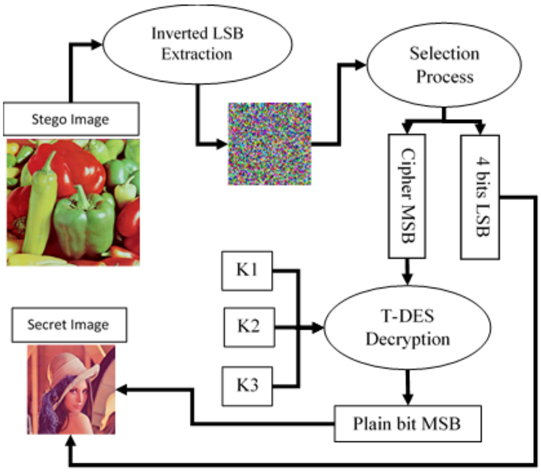


Figure 4. Proposed Extracting Scheme using Selective Bit T-DES and Inverted LSB

The process of proposed extracting scheme in Figure 4 is firstly we input the stego image and three independent key that will used in T-DES decryption. From stego image we will retrieve the cipher bit. Then reconstruct the cipher bit into cipher image so that we can select 4 bit of MSB of each pixel. After that, decrypt the selection result using T-DES with three different keys. Finally, combine the decryption result with other 4 bit left so that it can be original secret image.

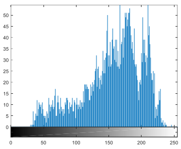
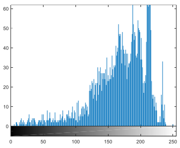
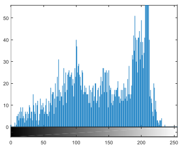
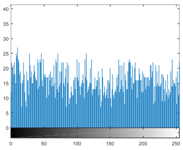
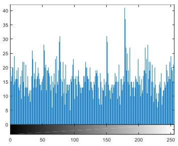
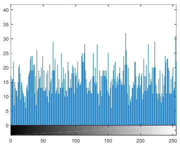
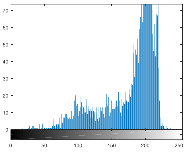
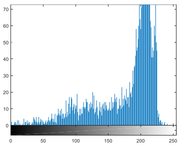
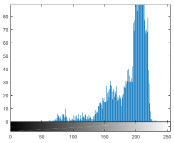
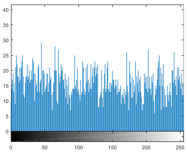
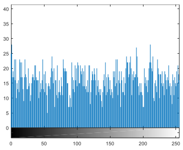
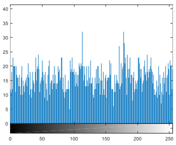
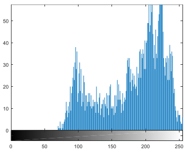
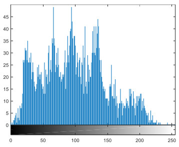
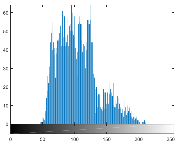
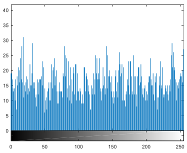
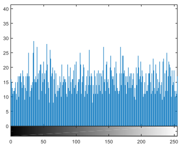
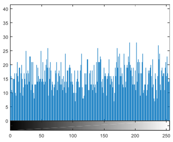
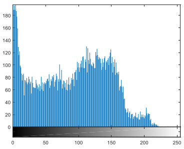
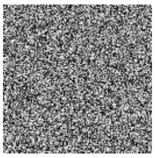
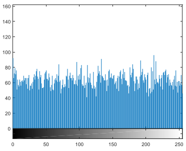
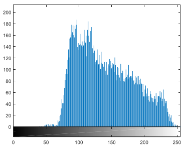
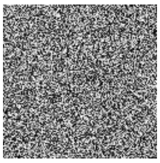
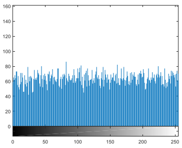
3. Result and Testing

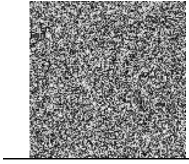
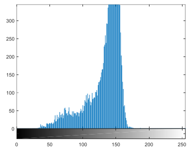
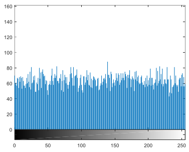
To examine the performance of our proposed method we used entropy, histogram analysis, and processing times to look the quality of encryption scheme result. While to find out the performance and the quality of stego-file we will used MSE, PSNR, and SSIM.

3.1 Histogram Analysis

Histogram analysis can be used to find out the quality of encrypted images againts statistical attack. Below is the comparison between histogram of original testing image and histogram of encrypted images.

TABLE 2
COMPARISON OF EACH HISTOGRAM OF TESTING IMAGES WITH ENCRYPTION RESULT

Images	Red	Green	Blue
			
			
			
			
			
			
		Grayscale	
			
			
			
			

From histogram comparison in Table 2 can be concluded that our proposed encryption scheme can secure the original from histogram analysis attack because histogram of the encryption result is significant difference from histogram of original image. Moreover histogram of encrypted images does not give any clue because of its equally distributed which means it can resisted image from statistical attack [18].

3.2 Entropy Analysis

Entropy calculation is parameter to determine the randomness level of the images. The randomness level of image depends on the variation of gray level of each pixel of image. To calculate entropy value can be used this formula [19]:

$$H(m) = \sum_{i=0}^{2^{n-1}} p(m_i) log_2 \frac{1}{p(m_i)} \qquad (3)$$

From Equation 3, P(mi) is the probability of the appearance of gray value in each image pixel. Below is the result of entropy calculation in each testing images.

TABLE 3
COMPARISON OF ENTROPY VALUE BETWEEN PROPOSED METHOD AND PREVIOUS METHOD

Image Name	DES	Double-DES	Triple-DES	Proposed Method
House.bmp	7.9861	7.9844	7.9837	7.9770
F16.bmp	7.9847	7.9852	7.9858	7.9795
Lena.bmp	7.9822	7.9852	7.9863	7.9789
Indian.bmp	7.9890	7.9887	7.9890	7.9840
Aerial.bmp	7.9883	7.9873	7.9877	7.9891
Tank.bmp	7.9887	7.9892	7.9894	7.9886
Average	7.986500	7.986667	7.986983	7.982850

From Table 3 can be seen that our proposed method generated entropy value that has small difference compared to other techniques. But based on Table 4 and Table 5, our method has processing time two times faster than Triple-DES and slightly better than Double-DES.

3.3 Processing Times

To find out the processing time, we tried to performing time testing at same hardware and using same keys in encryption and decryption process. This examination can describe the possibility of actual processing times.

TABLE 4
COMPARISON OF EXECUTION TIMES IN ENCRYPTION PROCESS

Image Name	DES	Double-DES	Triple-DES	Proposed Method
House.bmp	3.074231	6.312150	10.166062	5.500971
F16.bmp	3.334083	6.066865	9.092830	4.493580
Lena.bmp	2.977649	6.260398	9.119326	4.557636
Indian.bmp	3.747562	8.170396	12.852723	7.377887
Aerial.bmp	3.947431	8.257686	12.942323	7.827122
Tank.bmp	3.786630	8.044823	14.449349	6.206587
Average	3.477931	7.185386	11.437102	5.993964

Based on encryption time in Table 4, our proposed method can encrypt our testing images two times faster than Triple-DES. For Decryption time is showed below:

Furthermore, decryption time of our proposed method in Table 5 is faster than Triple-DES and Double-DES. These result denoted that our proposed method has better performance compared to other modified DES algorithm.

TABLE 5
COMPARISON OF EXECUTION TIMES IN DECRYPTION PROCESS

Image Name	DES	Double-DES	Triple-DES	Proposed Method
House.bmp	3.812003	7.289178	10.472164	6.410017
F16.bmp	3.195879	6.730322	9.411340	4.683629
Lena.bmp	3.606332	6.502543	9.417266	4.747543
Indian.bmp	5.660305	9.059090	12.475996	6.339933
Aerial.bmp	4.962577	10.242170	12.106214	6.126059
Tank.bmp	4.004803	8.283152	13.550990	7.457710
Average	4.206983	8.017743	11.238995	5.960815

Steganography Analysis (MSE, PSNR, and SSIM) To evaluate the quality of stego images we used MSE, PSNR, and SSM calculation. MSE (Mean Square Error) value can be calculated using formula [20]:

$$MSE = \frac{1}{M \times N} \sum_{x=1}^{x} \sum_{y=1}^{y} \sum_{z=1}^{z} \| C_i(x,y,z) - S_i(x,y,z) \|^2 \qquad (4)$$

Equation 4 shown that MSE value can be obtained by comparing cover image (Ci) with stego image (Si) where M and N is the size of both images. While to calculate PSNR or Peak Signal to Noise Ratio value we can use formula [21]:

$$PSNR = 10\ log_{10} \frac{Max^2}{MSE} \qquad (5)$$

Minimum acceptable value of PSNR is 35 dB [22]. Based on Equation 5, PSNR value can be obtained by divided square value of the max value or dynamic range of an image with MSE. Then for the SSIM or Structure Similarity will be used to determine the similarity between stego image and original cover image. Below is a formula for SSIM calculation [23]:

$$SSIM(A,B) = \frac{(2\mu_A\mu_B + c_1)(2\sigma_{AB} + c_2)}{(\mu_A^2 + \mu_B^2 + c_1)(\sigma_A^2 + \sigma_B^2 + c_2)} \qquad (6)$$

where,
μ_A and μ_B = mean of A Image and B Image
σ_{AB} = covariance of A Image towards B Image
σ_A^2 = variance of A Image
σ_B^2 = variance of B Image
$c_1 = (k_1L)^2$; $c_2 = (k_2L)^2$
L is a dynamic range of the image (2bit – 1) with a default value of k_1= 0.01 and k_2= 0.03

From Equation 6 above, it can be seen that to obtain the SSIM value we need to determine mean, covariance and variance of both images. The range of SSIM value is between -1 to 1 [24]. High SSIM value means that both images are similar or identical.

Based on analysis methods above which have been implemented on stego-image can be obtained the result as shown below:

TABLE 6
THE TESTING RESULT OF STEGO IMAGE USING MSE, PSNR, AND SSIM

Cover Image	Secret Image	MSE	PSNR	SSIM
Peppers	House	0.062096	60.200192	0.999878
	F16	0.061855	60.217033	0.999880
	Lena	0.061929	60.211858	0.999884
	Indian	0.081951	58.995254	0.999839
	Aerial	0.082695	58.956011	0.999836
	Tank	0.082832	58.948804	0.999836
Baboon	House	0.062071	60.201882	0.999975
	F16	0.062079	60.201349	0.999975
	Lena	0.062036	60.204374	0.999975
	Indian	0.081951	58.995254	0.999958
	Aerial	0.082966	58.941810	0.999957
	Tank	0.082879	58.946338	0.999957
Boat	House	0.186077	55.433874	0.999663
	F16	0.185478	55.447875	0.999660
	Lena	0.186123	55.432806	0.999654
	Indian	0.245853	54.224041	0.999615
	Aerial	0.248508	54.177392	0.999608
	Tank	0.248997	54.168867	0.999612
Elaine	House	0.186069	55.434052	0.999686
	F16	0.185478	55.447875	0.999660
	Lena	0.186123	55.432806	0.999654

Indian	0.245853	54.224041	0.999593
Aerial	0.248737	54.173394	0.999589
Tank	0.248859	54.171263	0.999591

From Table 6, it can be observed that our proposed method can produce good quality of stego images. This can be proved by the range of PSNR result is between 54 dB to 61 dB. High PSNR value represented that our stego result has good imperceptibility value, where it cannot be distinguished by Human Visual System (HVS) [25]. Moreover, SSIM value of our proposed method almost reaches 1 which represented that our stego file did not significantly change even after the secret image has been inserted.

4. Conclusion

This research presented T-DES encryption was modified using selective encryption and combined with inverted LSB steganography has been implemented in images security. Encryption scheme was tested using 6 testing images and given the results that our proposed method is two times faster than original Triple-DES and generated average Entropy value equal to 7.982850. Furthermore, the encryption scheme result will be embedded using inverted LSB. At this process, stego image can produce the PSNR range between 54 dB to 61 dB. PSNR above 40 dB indicated that proposed method generated good quality of stego file. Moreover, based on SSIM result proved that stego images are almost similar to the original cover images because of the range of SSIM results between 0.99958 to 0.99998. Because the value of SSIM is close to 1 means the stego images have a high level of resemblance to the original cover images. Based on the result analysis can be concluded that our proposed method has better performance compared to other modified DES techniques and can produce good quality of stego image which cannot be distinguished by human eyes (HSV).

Future work, proposed encryptions scheme will be combined with another encryption method such as a chaotic map which can improve the randomness of the encrypted result. While for embedding process can improve with inserted the message bits into the edge area [1] [20] of the cover image to increase imperceptible value.

References

[1] E. J. Kusuma, O. R. Indriani, C. A. Sari, D. R. I. M. Setiadi, and E. H. Rachmawanto, “An Imperceptible LSB Image Hiding on Edge Region Using DES Encryption,” in International Conference on Innovative and Creative Information Technology (ICITech), 2017, pp. 1–5.

[2] R. D. Ardy, O. R. Indriani, C. A. Sari, D. R. Ignatius, and M. Setiadi, “Digital Image Signature using Triple Protection Cryptosystem (RSA, Vigenere, and MD5),” in International Conference on Smart Cities, Automation & Intelligent Computing Systems, 2017, pp. 1–6.

[3] W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, “A Good Performance OTP Encryption Image based on DCT-DWT Steganography,” TELKOMNIKA, vol. 15, no. 4, pp. 1987–1995, 2017.

[4] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, “A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish,” Procedia Comput. Sci., vol. 78, no. December 2015, pp. 617–624, 2016.

[5] G. Ardiansyah, C. A. Sari, D. Setiadi, and E. H. Rachmawanto, “Hybrid Method using 3-DES , DWT and LSB for Secure Image Steganography Algorithm,” in 2017 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 2017, pp. 248–253.

[6] M. Boussif, N. Aloui, and A. Cherif, “New watermarking/encryption method for medical images full protection in m-Health,” Int. J. Electr. Comput. Eng., vol. 7, no. 6, pp. 3385–3394, 2017.

[7] S. Mankotia and M. Sood, “A Critical Analysis of Some Symmetric Key Block Cipher Algorithms,” Int. J. Comput. Sci. Inf. Technol., vol. 6, no. 1, pp. 495–499, 2015.

[8] L. Li, Y. Yao, and X. Chang, “Plaintext-Dependent Selective Image Encryption Scheme Based on Chaotic Maps and DNA Coding,” in 2017 International Conference on Dependable Systems and Their Applications (DSA), 2017, pp. 57–65.

[9] M. K. Abdmouleh, A. Khalfallah, and M. S. Bouhlel, “A Novel Selective Encryption Scheme for Medical Images Transmission based-on JPEG Compression Algorithm,” Procedia Comput. Sci., vol. 112, pp. 369–376, 2017.

[10] M. N. M. Najih, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, and S. Astuti, “An improved secure image hiding technique using PN-sequence based on DCT-OTP,” in 2017 1st International Conference on

Informatics and Computational Sciences (ICICoS), 2017, pp. 47–52.

[11] G. Prasetyadi, R. Refianti, and A. B. Mutiara, “File Encryption and Hiding Application Based on AES and Append Insertion Steganography,” TELKOMNIKA (Telecommunication Comput. Electron. Control., vol. 16, no. 1, p. 361, Feb. 2018.

[12] V. A. Kumar, C. Dharmaraj, and C. S. Rao, “A Hybrid Digital Watermarking Approach Using Wavelets and,” Int. J. Electr. Comput. Eng., vol. 7, no. 5, pp. 2483–2495, 2017.

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

[14] S. Sarkar, “Comparison of various Edge Detection Techniques for maximum data hiding using LSB Algorithm,” Int. J. Comput. Sci. Inf. Technol., vol. 5, no. 3, pp. 4722–4727, 2014.

[15] N. Akhtar, S. Khan, and P. Johri, “An Improved Inverted LSB Image Steganography,” Int. Conf. Issues Challenges Intellegent Comput. Tech., pp. 749–755, 2014.

[16] R. Bhardwaj and V. Sharma, “Image Steganography Based on Complemented Message and Inverted Bit LSB Substitution,” Procedia Comput. Sci., vol. 93, no. September, pp. 832–838, 2016.

[17] “SIPI Image Database.” .

[18] E. Setyaningsih, C. Iswahyudi, and N. Widyastuti, “Image Encryption on Mobile Phone using Super Encryption Algorithm,” Telkomnika, vol. 10, no. 4, pp. 837–845, 2012.

[19] A. Kulsoom, D. Xiao, Aqeel-ur-Rehman, and S. A. Abbas, “An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules,” Multimed. Tools Appl., vol. 75, no. 1, pp. 1–23, 2016.

[20] C. Irawan, D. R. I. M. Setiadi, C. A. Sari, and E. H. Rachmawanto, “Hiding and Securing Message on Edge Areas of Image using LSB Steganography and OTP Encryption,” in International Conference on Informatics and Computational Sciences (ICICoS), 2017.

[21] A. Setyono, D. R. I. M. Setiadi, and M. Muljono, “StegoCrypt Method using Wavelet Transform and One-Time Pad for Secret Image Delivery,” 2017 4th Int. Conf. Inf. Technol. Comput. Electr. Eng., 2017.

[22] H. Al-Dmour and A. Al-Ani, “A steganography embedding method based on edge identification and XOR coding,” Expert Syst. Appl., vol. 46, pp. 293–306, 2016.

[23] K. Seshadrinathan et al., “Image Quality Assessment,” in The Essential Guide to Image Processing, Elsevier, 2009, pp. 553–595.

[24] N. A. Abbas, “Image encryption based on Independent Component Analysis and Arnold ’ s Cat Map,” Egypt. Informatics J., vol. 17, no. 1, pp. 139–146, 2016.

[25] J. Bai, C.-C. Chang, T.-S. Nguyen, C. Zhu, and Y. Liu, “A high payload steganographic algorithm based on edge detection,” Displays, vol. 46, pp. 42–51, 2017.