Combination of 3des with dct algorithm in message security

S. Guntur[1], MKM Nasution[2] and RW Nasution[3]

[1,2]Master Program (S2) of Informatics Engineering, Faculty of Computer Science and Information Technology, University of Sumatera Utara, Medan, Indonesia.
[3]Department of Mathematics, Faculty of Mathematics and Natural Sciences, University of Sumatera Utara, Medan, Indonesia.

[1]suryaguntur91@gmail.com, [2] mahyuddin@usu.ac.id, [3]rahmatws@usu.ac.id

Abstract. In the digital era, communication through computer networks plays an important role. Through electronic communication, a person can make transactions or communication very quickly and practically. Sending data / messages from one place to another is much constrained by the issue of confidentiality. There are many ways you can hide data / messages that will be sent. First, using cryptographic techniques, namely by encoding data / messages using certain algorithms. Another technique is to insert a message that will be sent to other media, so that the message will be hidden and what will appear is other media used to insert messages.Here will be performed a Performance Analysis of the Combination of 3DES and DCT Algorithms in Securing Message Files into the Image.

1. INTRODUCTION

A very significant development in information technology, where internet bandwidth is getting bigger with cheaper access costs. The consequence is that risks in information security are increasing. Data security is the protection of data in a system against unauthorized authorization, modification, or destruction and protection of computer systems against unauthorized use or modification.

Sending data / messages from one place to another is much constrained by the issue of confidentiality. Especially if the data / message is a data / message that is very confidential, so that not just anyone can read. There are many ways you can hide data / messages that will be sent. First, using cryptographic techniques, namely by encoding data / messages using certain algorithms. Another technique is to insert a message that will be sent to other media, so that the message will be hidden and what will appear is other media used to insert messages.

The Data Encryption Standard (DES) is a cryptographic cipher block algorithm with a block size of 64 bits and a key size of 56 bits. [5]. DES was first published in the Federal Register on March 17, 1975. After much discussion, finally the DES algorithm was adopted as a standard algorithm used by NBS (National Bureau of Standards) on January 15, 1977. Since then, DES has been used in the world of information dissemination to protect data so that it cannot be read by others [6]. DES is divided into three groups where one group communicates with each other so that this technique is very effective in maintaining data security[7]. the time of encryption and decryption of text data uses the DES and 3DES algorithms that to get the plaintext without knowing the key requires 1,183x1043 years using a brute force attack. [8].

Discrete Cosine Transform (DCT) is a technique for converting a signal into a basic frequency component. DCT works by separating images to different parts of the frequency.

The insertion process is carried out on a high frequency part because human vision is not very sensitive with errors at high frequencies compared to those at low frequencies (Jianshenget al, 2018). Here we wants to do a Performance Analysis of Combination of 2D DES and DCT Algorithms on Securing Message Files into the Image.

2. STUDY OF LITERATURE

2.1 Cryptography

Cryptography makes data or messages become codes first by the sender. This process is known as encryption. Encryption is defined as the process of changing data or messages that are to be sent into a form that is barely recognized by third parties.

2.2 Steganography

Steganography is a technique to hide or disguise the existence of a secret message in a container media so that other people are not aware of the message in the media. Derived from the word steganos in Greek.Steganos means disguising or hiding and graphein or graptos is writing. Understanding steganography which is quite often used in learning with historical methodology is "writing hidden or veiled writings" (6).

2.3 Algorithm 3DES

Triple Data Encryption Standard (3DES) is an algorithm developed from DES (Data Encryption Standard) algorithm. Basically the algorithm used is the same, only in 3DES was developed by encrypting the implementation of the DES algorithm three times. 3DES has three 168-bit keys (three times the 56-bit key of DES). The 3DES algorithm is divided into three stages, each of which is an implementation of the DES algorithm. The first stage, the input plaintext is operated with the first external key (K1) and performs the encryption process using the DES algorithm. So as to produce the first pre ciphertext. The second stage, the first pre ciphertext produced in the first stage, then operated with the second external key (K2) and carried out the encryption process or decryption process (depending on the encryption method used) using the DES algorithm. So as to produce the second pre ciphertext. The last stage, the second pre ciphertext produced in the second stage, is operated with a third external key (K3) and performs the encryption process using the DES algorithm, resulting in a ciphertext (C). Triple Data Encryption Standard Algorithm can be seen as in Figure 1.

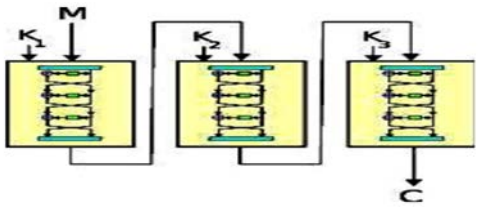

Figure 1. 3DES algorithm (Mitchell, C.J. 2016)

2.4 Discrete Cosinus Transform (DCT) Algorithm

Algorithms used in digital steganography are diverse but in general this technique uses redundant bits as a place to hide messages when data compression is done, and then use human sensory weaknesses that are not sensitive so that the message has no visible or audible differences. The DCT algorithm is one of the techniques used in image watermarks using a method by inserting data at low frequencies from pixels cover image. This technique can be used to insert data whose size is in accordance with needs. The size of the file that has been

inserted data is the same as the size of the file before the data is inserted plus the size of the data inserted into the file. In this technique, data is inserted at the end of the file with a special sign as the start identifier of the data and the final identifier of the data (Jiansheng, M., Li Sukang, L. & Tan Xiaomei, T. 2017).

DCT is a technique for converting a signal into a basic frequency component. The nature of DCT is to change significant image information concentrated only on several DCT coefficients where image blocks are transformed from the spatial domain to the spatial frequency domain called the DCT coefficient. The lower DCT coefficient frequency appears in the upper left of a DCT matrix and the higher frequency of the DCT coefficient is at the lower right of the DCT matrix. DCT works by separating images to different parts of the frequency. The insertion process is carried out at high frequencies because human vision is not very sensitive with errors that occur at high frequencies compared to those at low frequencies (8). The insertion steps with the DCT algorithm are as follows:

1. Calculation of the Transform Matrix
2. Calculation of the Transpose Matrix
3. Calculation of the DCT Coefficient Value

The DCT coefficient calculation process is:

1. Create a transform matrix, namely matrix A.
2. Create an original image matrix, namely the X matrix.
3. Multiplication of matrix A with X Namely the matrix A zero row zero row is multiplied by the X matrix to the zero column on the X matrix.
4. Add the A (transform matrix) to the X matrix (original image matrix) from the zero column matrix and to the zero row, to A line to N-1 and X column to N-1, where N is the number of image pixels. So that the multiplication of matrix A (transform matrix) to X (original image matrix) results in a Y value 'from row to N-1 to M-1.

2.5 Mean Squal Error (MSE)

Mean Squal Error (MSE) is the average error value between the original file and the insertion file. It can be systematically formulated:

$$\text{MSE}=\sqrt{\frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}[Ori(x,y)-(Emb(x,y))^2} \quad \ldots\ldots\ldots(2.4)$$

Information :
Ori (x, y): pixel value at position (x, y) on the original image;
Emb (x, y): pixel value at position (x, y) on a stego-object image;
M: Length of stego image (in pixels)
N: Stego image width (in pixels)

2.6 Peak Signal to Noise Ratio (PSNR)

PSNR is used to describe the degradation of an image due to the process of insertion, noising, encoding, compression or transmission errors. PSNR values are expressed in units of dB. The greater the value of the PSNR, the better the image quality of the stego imperceptibility will be.It can be systematically formulated:

$$\text{PSNR}= 10 \text{ Log }_{10} \frac{L^2}{MSE} \text{ (dB)}$$

... 1

The greater the PSNR value the better the quality of the steganographic image. According to Cole (2003), the PSNR value is said to be good if it is above the value of 20.

3. FINDINGS AND DISCUSSIONS

The analysis carried out by the author in this study is to combine the Triple Data Encryption Standard (3DES) algorithm with Discrete Cosine Transform (DCT) to secure message files into image files with the aim of increasing the security level of message files with cryptographic and steganographic techniques. The secured file is in the form of secret text encrypted with the 3DES algorithm and then inserted into a digital image file format BMP, JPG or PNG with 2D DCT algorithms.

To determine the level of security of the result of the insertion image (stego image) the value of Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) is calculated as well as the calculation of Data Recovery Rate (DRR) as a parameter of successful extraction of ciphertext from the stego image file where the value is smaller MSE, the file is safer because of the small difference between the pixel value of the cover image and the stego image.

3.1 Combination of 3DES and DCT Algorithms

In this study we propose a combination of 3DES and DCT algorithms for message security into image files. The proposed algorithm scheme can be seen in figure 2

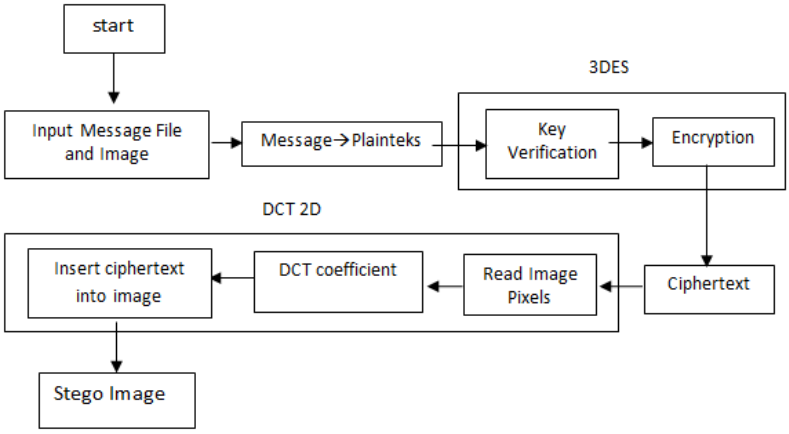

Figure 2. Encryption Process

The encoding process above is done by inserting a bmp format image file then the plaintext will be encrypted using the 3DES algorithm to getciphertext after verifying the external key entered by the user to get 16 internal keys. Read the pixel value of the image frame to get the DCT coefficient and then insert a ciphertext into the image file to produce a stego image that contains a secret message.

3.2 Result of Decryption Process

The combination of 3DES and DCT algorithms is implemented with VB.Net. To determine the level of image security from the insertion (stego image), the Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) values are calculated as well as the Data Recovery Rate (DRR) calculation as a parameter of the success of ciphertext extraction from

the stego image file where the smaller value MSE, the safer the file is because of the small difference between the pixel value of the original image file (cover image) and the image resulting from the insertion (stego image).

Insertion text messages are in txt format with a number of characters or letters that vary from 100 to 500 characters. The image from the insertion process (stego image) is calculated the MSE and PSNR values to assess the quality of the insertion algorithm and the text message that is inserted into the image file, the value of Data Recovery Rate (DRR) is calculated.

Table 1. Average MSE and PSNR Insertion Results

Cover Image	Size (MB)	Average MSE Value	Average PSNR Value
PIC1	2.8	0.4926	52.846
PIC2	5.49	0.455	59.616
PIC3	1.37	0.5114	52.916
PIC4	1.37	0.4708	53.226
PIC5	0.7050	0.4478	53.574

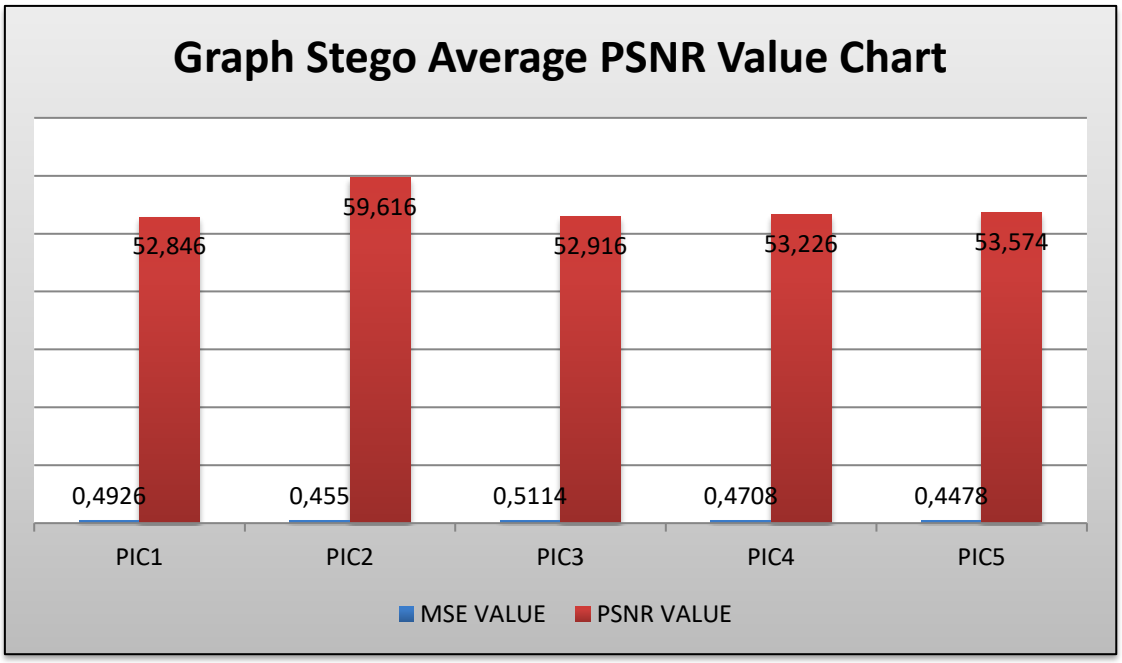

Figure 3. Graph Stego Average MSE and PSNR Value Chart

Figure 3 above shows the average taken in the MSE and PSNR calculation process in the assessment of the quality of the insertion algorithm and the text messages inserted into the image file.

4. CONCLUSION

The conclusion that can be drawn from this study is obtained by the results of the insertion of the smallest MSE value with a cover image of PIC5 measuring 0.7050 MB in the amount of 0.4478 and PSNR of 53.574. The largest MSE value with a PIC3 cover image measuring 1.37 MB is 0.5114 and PSNR is 52.916.

Based on the results of the extraction test, the extraction results are obtained with a data recovery rate of 100%, which means that all data inserted into the stego image can be

retrieved. From the decryption results, the ciphertext file can be decrypted back into plaintext.

5. REFERENCES

[1] Aliwa, M. B., Tarek E., T, Fahmy& Nasr, M. E. N. 2016. *Robust Digital Watermarking Based Falling-off-Boundary in Corners Board-MSB-6 Gray Scale Images*.International Journal of Computer Science and Network Security, VOL.9 No.8, August 2016. Faculty of Computers & Information Sciences-Ain Shams University, Egypt.

[2] Chin-Chen Chang, Tung-Shou Chen, Lou-Zo Chung. 2002. *A Steganographic Method Based upon JPEG and Quantization Table Modification*. Information Sciences 141 (2002) 123-138.

[3] Cuddy, Aileen, Walden, Elisabeth, Zalewski, Sarah, 2001, *The Discrete Cosine Transform.*

[4] Marvel, Lisa M., Charles G. Boncelet, dan Charles T. Retter. 1999. *Spread Spectrum Image Steganography*. IEEE Transaction on Image Processing.

[5] Gonzalez, R.C., Woods, R.E. 2008. *Digital Image Processi*ng.3rd Edition. Pearson Education, Inc : Upper Saddle River, New Jersey.

[6] Halim, S. A. & Sani, M. F. A. 2015. *Embedding Using Spread Spectrum Image Steganography with GF(2m)*. Proceedings of the 6th IMT-GT Conference on Mathematics, Statistics and its Applications (ICMSA2015) Universiti Tunku Abdul Rahman, Kuala Lumpur, Malaysia.

[7] Jiansheng, M., Li Sukang, L. & Tan Xiaomei, T. 2017. *A Digital Watermarking Algorithm Based On DCT and DWT*. Proceedings of the 2017 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, May 22-24, 2017.

[8] KrikorLala, Sami Baba, Thawar Arif, *Image Encryption Using DCT and Stream Cipher*, European Journal of Scientific Research, ISSN 1450-216X Vol.32 No.1 (2009), pp.47-57

[9] Megalingam, R. K., Nair, M. M, Srikumar, R., Balasubramanian, V. K. &Sarma, VSV. 2015. *A Comparative Study on Performance of Novel, Robust Spatial Domain Digital Image Watermarking with DCT Based Watermarking*. International Journal of Computer Theory and Engineering, Vol. 2, No. 4, August, 2015.

[10] Mitchell, C.J. 2016. *On the Security of 2-key Triple DES*. *IEEE Transactions on Information Theory*. Volume: 62, Issue: 11, September 2016 : 6260-6267.