Journal of Applied Intelligent System (e-ISSN : 2502-9401 | p-ISSN : 2503-0493)
Vol. 2 No. 1, April 2017, pp. 1 – 11

# Secure Image Steganography Algorithm Based on DCT with OTP Encryption

**De Rosal Ignatius Moses Setiadi [1], Eko Hari Rachmawanto[2],**
*[1,2]Faculty of Computer Science, Dian Nuswantoro University, Semarang*
*E-mail: *[1]moses@dsn.dinus.ac.id, [2]eko.hari@dsn.dinus.ac.id*
**Corresponding author*

**Christy Atika Sari[3]**
*[3]Faculty of Computer Science, Dian Nuswantoro University, Semarang*
*E-mail: [3]christy.atika.sari@dsn.dinus.ac.id*

**Abstract -** Rapid development of Internet makes transactions message even easier and faster. The main problem in the transactions message is security, especially if the message is private and secret. To secure these messages is usually done with steganography or cryptography. Steganography is a way to hide messages into other digital content such as images, video or audio so it does not seem nondescript from the outside. While cryptography is a technique to encrypt messages so that messages can not be read directly. In this paper have proposed combination of steganography using discrete cosine transform (DCT) and cryptography using the one-time pad or vernam cipher implemented on a digital image. The measurement method used to determine the quality of stego image is the peak signal to noise ratio (PSNR) and normalized cross Correlation (NCC) to measure the quality of the extraction of the decrypted message. Of steganography and encryption methods proposed obtained satisfactory results with PSNR and NCC high and resistant to JPEG compression and median filter.

**Keywords**—Image Steganography, Discrete Cosine Transform (DCT), One Time Pad, Vernam Chiper, Image Cryptography

## 1. INTRODUCTION

Internet technology is currently growing rapidly. Internet is becoming one of the basic needs in real life. The increasing number of internet users and the increasing speed of access makes it easy for everyone to get and provide information. Internet network that is used by a lot of people make the internet unsafe. Therefore, confidentiality and information security becomes very important and necessary, especially for private and sensitive messages. Steganography, cryptography and watermarking is the solution to overcome these things so that research in this area becomes an interesting thing [1].
Steganography is a technique for hiding data or sensitive personal information and confidential into a digital content transmitted, such that the digital content still looks normal from the outside. Digital content that can be used as a place to embed a message can be text, images, video, and audio, as well as the message that will be embedded. In this paper discussed steganography and cryptography in the digital image. Scheme steganography in digital image can be done in two domains, namely the spatial domain and frequency domain [2]. In the spatial domain the message is inserted directly into the pixels of the cover image, usually using the method of least significant bit (LSB). While in the frequency domain using the many

transformations such as discrete cosine transform (DCT), discrete wavelet transform (DWT), and singular decomposition value (SVD) [3]. Currently the implementation of a steganography technique is not enough to provide security transaction message delivery. In order to deal challenges of digital content security threats at this time a lot of research that combines steganography and cryptography technique. Cryptography is a way to encode information into different forms that can not be read before it's decoded. To increase security before it is inserted, the secret message needs to be encrypted first. In previous research [4], [5], [6] has combined steganography and cryptography technique. All three use DCT to insert a secret message. The difference in encryption techniques performed on the message before it is inserted, Arnold's Transform to scramble message in [4], Blowfish Algorithm in [5], and RSA in [6].

One Time Pad is one of the algorithms are quite popular and are often used in cryptography techniques. OTP is a symmetric algorithm which uses the same key for encryption and decryption. Encryption and decryption process in this technique uses XOR operations to generate the cipher file [7]. Bruce Schneier [8] said that the OTP is "the perfect encryption scheme" on the condition that if the key is truly random and never reused. In this research applied to steganography by using DCT to insert a secret message on a grayscale image combined with the one-time pad algorithm (OTP) to encrypt secret messages. To measure the quality of image steganography evaluated with PSNR and MSE whereas for measurement robustness of the extracted message image were evaluated by NCC.

## 2. RESEARCH METHOD

### 2.1 Discrete Cosine Transform (DCT)

DCT in digital image processing is usually done by dividing the images into small pieces or sub-block with standard size 8x8 pixels [9]. The results of transformation of 8x8 pixel sub-blocks will generate 64 coefficients which consist of a DC coefficient and 63 AC coefficients. Eq. 1-3 is the equation of DCT where input images, A, DCT coefficients for image output, B. In these equations, x, the input image having I x J pixels, C (i, j) is the intensity of the pixel in rows m and columns n of the image, and T (p, q) is the DCT coefficient in row u and column v of the DCT matrix.

$$T_{pq} = \alpha_p \alpha_q \sum_{i=0}^{I-1} \sum_{j=0}^{J-1} C \cos\frac{\pi(2i+1)p}{2I} \cos\frac{\pi(2j+1)q}{2J}, \quad \begin{matrix} 0 \le p \le I-1 \\ 0 \le q \le J-1 \end{matrix} \tag{1}$$

where

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{I}}, p = 0 \\ \sqrt{\frac{2}{I}}, 1 \le p \le I-1 \end{cases} \tag{2}$$

and

$$\alpha_q = \begin{cases} \frac{1}{\sqrt{J}}, q = 0 \\ \sqrt{\frac{2}{J}}, 1 \le q \le J-1 \end{cases} \tag{3}$$

To reconstruct the image after DCT operation according to Eq. 4-6:

$$C_{ij} = \sum_{i=0}^{I-1}\sum_{j=0}^{J-1} \alpha_p \alpha_q T_{pq} \cos\frac{\pi(2i+1)p}{2I} \cos\frac{\pi(2j+1)q}{2J}, \quad 0 \le p \le I-1 \quad 0 \le q \le J-1 \tag{4}$$

where

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{I}}, p = 0 \\ \sqrt{\frac{2}{I}}, 1 \le p \le I-1 \end{cases} \tag{5}$$

and

$$\alpha_q = \begin{cases} \frac{1}{\sqrt{J}}, q = 0 \\ \sqrt{\frac{2}{J}}, 1 \le q \le J-1 \end{cases} \tag{6}$$

DCT has several reasons to be used in image watermarking according to [10], that is:

1. The features of the human visual system (HVS) can be embedded into image watermarking in the domain transformation is more effective.
2. The energy of the copyright signal is embedded in the domain transformation will spread to all the pixels in the spatial domain. It is advantageous to not visible (invisible).
3. Can be implemented in the domain of international image compression and compression video standards, such as JPEG, MPEG, H. 261, and H.263 DCT-based.

## 2.2 One Time Pad (OTP)

One Time Pad or often called the Vernam cipher is one of the algorithms are quite popular and are often used in cryptography techniques. OTP is a symmetric algorithm which uses the same key for encryption and decryption. OTP excellence is to have an algorithm that is simple but very difficult to solve because it has the same length as the key messages to be encrypted and has a truly random key [7]. OTP can be a perfect encryption and can not be solved if the keyword used to be truly random and used only once during the process of encryption and decryption.

Of all the cryptography methods that have been designed, OTP is a method that has proven completely safe mathematically [11], cause every person who wants to solve it should try every possible key when performing the decryption and impossible to guess the original plain text. Following are the OTP formula:

$$Ci = (Mi + k)\ mod\ X \tag{7}$$

where :

Ci = Cipher image,
Mi = Message image,
k = random key.
X = Max value of image intensity

Besides using the above formula, operator XOR can also be used with the following formula is used when the image message is a binary image as follows:

$$Ci = Mi \oplus k \tag{8}$$

The decryption process is calculated by subtracting the cipher image with the key:

$$Mi = (Ci - k)\ mod\ X \qquad (9)$$

## 2.3 Proposed Method

The proposed watermarking algorithm is based on DCT and OTP. DCT For detailed method is shown in figure 1 and 2 and discussed below as follows:

### 2.3.1 Embedding Algorithm

Visualization of embedding message in DCT-OTP transformation is shown in Fig. 1.

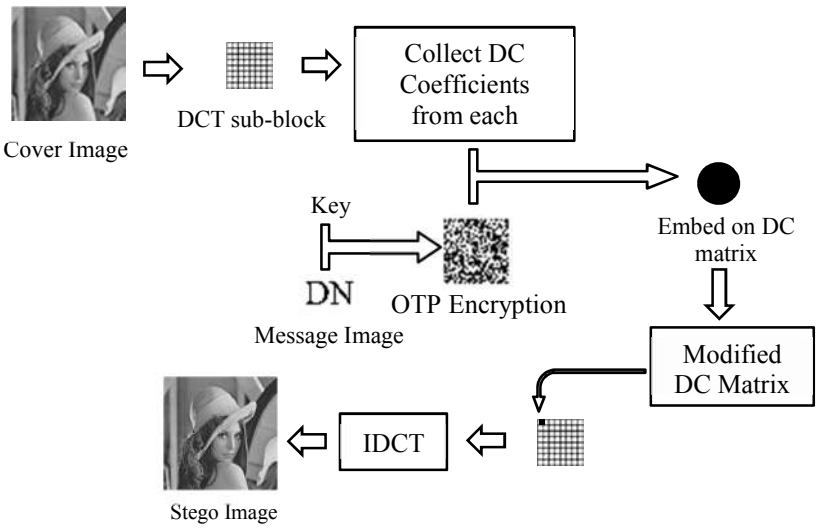



*Figure 1. Visualization of embedding message*

Embedding message algorithm is illustrated in Fig. 1 followed by a detailed explanation as follows:

1. Cover image divided into 16x16 subblock to apply DCT transformation.
2. Collect DC Coefficient from each subblock to make DC matrix
3. At the same time generate key and read message image, then apply OTP encryption
4. Embed encryption message in DC matrix, then embedding is done as follows:

$$DCM_m = DCM + (\alpha * E_m) \qquad (10)$$

where:

$DCM_m$ = DC matrix after embedding message
DCM = DC matrix of cover image
α = the intensity factor of embedded
$E_m$ = Encryption message

5. Replace the modified DC coefficients in the corresponding subblocks, then perform inverse DCT will produce Stego Image.

### 2.3.2 Extracting Algorithm

Below is a visualization of this process.

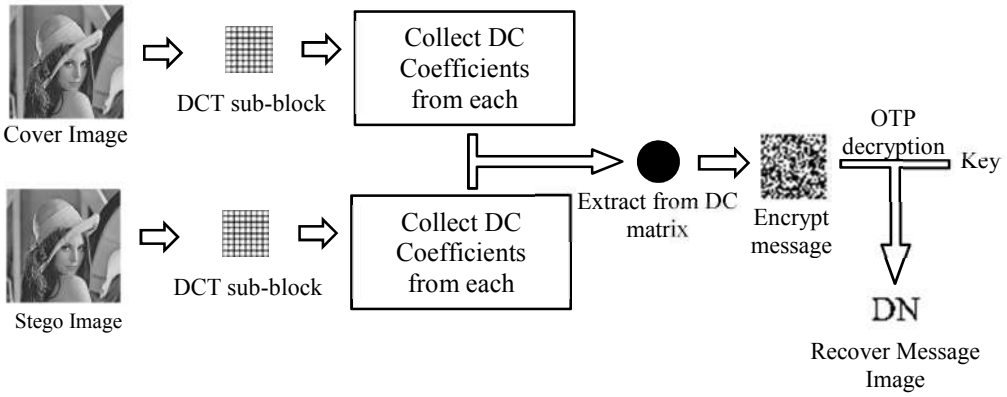



*Figure 2. Visualization of extracting copyright*

Extracting algorithm is illustrated in Fig. 2 followed by a detailed explanation as follows:

1. Stego and cover image divided into 16x16 subblock to apply DCT transformation
2. Collect DC coefficients from each subblock to make DC matrix cover image and DC matrix stage image.
3. Extract message in DC matrix, then extracting is done as follows:

$$E_m=DCM_s-(\alpha*DCM_c) \quad (11)$$

where:

$E_m$ = extracting encrypted message
$DCM_s$ = DC matrix of stego image
$\alpha$ = the intensity factor of embedded
$DCM_c$ = DC matrix of cover image

4. Perform OTP description then produce recover message image

## 3. RESULTS AND DISCUSSION

In this paper be used 10 grayscale images with a size of 512 * 512, and the image of the message with the size of 32 * 32. Below are the images used in this paper:


Babbon.bmp


Barbara.bmp


Cameraman.bmp


Car.bmp


F16.bmp


Lena.bmp


Peppers.bmp


Ship.bmp


Soccer.bmp


Women.bmp

*Figure 3. Cover Image*

DN

*Figure 4. Message Image*

Then all the cover image inserted with the message image with the methods that have been proposed. To measure results use Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR). MSE is a simple measurement parameter, function to find the quadratic loss. The error is the difference in the number of estimator with the amount to be estimated. Differences occur due to randomness or because the estimator does not take into account information that can produce more accurate estimates [12]. The smaller the MSE value of an image the better the quality. MSE is given by Eq. 11.

$$MSE = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \sum_{k=0}^{2} \|g(i,j,k) - f(i,j,k)\|^2 \qquad (11)$$

where:

M, N = numbers of columns and rows in pixel
g(i,j,k) = input image
f(i,j,k) = output image

PSNR are used as a measure of a quality of the reconstructed image. It is most commonly used as a measure of the quality of reconstruction of image watermarking to indicate imperceptibility. Imperceptibility means that the perceived quality of the host image should not be distorted by the watermark [13]. A higher PSNR would indicate that the reconstruction is of higher quality. PSNR is given by Eq. 12.

$$PSNR_{dB} = 10 \log 10 \left( \frac{255^2}{\sqrt{MSE}} \right) \quad (12)$$

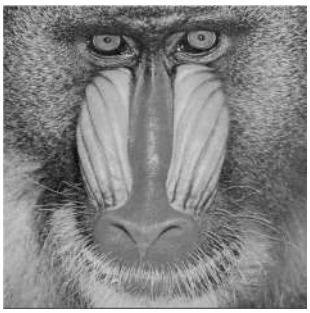
As for measurement robustness of the extracted message image is evaluated using normalized cross correlation (NCC) metric values [14]. NCC is given by Eq. 13.

$$NCC = \frac{M_{ij} \times R_{ij}}{M_{ij} \times M_{ij}} \quad (13)$$

where:

$M_{ij}$ = message image
$R_{ij}$ = recover message image

Below is shown ego image and results in analysis table insertion and extraction message image.


Babbon.bmp


Barbara.bmp


Cameraman.bmp


Car.bmp

F16.bmp


Lena.bmp


Peppers.bmp


Ship.bmp


Soccer.bmp


Women.bmp

*Figure 5. Stego Image*

*Table 1. Result Analysis embedding and embedding message on various Image*

| Cover Image | PSNR | MSE | NCC |
|---|---|---|---|
| Babbon.bmp | 51.1242 | 0.5020 | 1 |
| Barbara.bmp | 51.1326 | 0.5010 | 1 |
| Cameraman.bmp | 51.0915 | 0.5057 | 1 |
| Car.bmp | 51.3053 | 0.4814 | 1 |
| F16.bmp | 51.1242 | 0.5020 | 1 |
| Lena.bmp | 50.9099 | 0.5273 | 1 |
| Peppers.bmp | 51.0488 | 0.5107 | 1 |
| Ship.bmp | 51.0157 | 0.5146 | 1 |
| Soccer.bmp | 51.1411 | 0.5000 | 1 |
| Women.bmp | 51.3319 | 0.4785 | 1 |
| **Average** | **51.1225** | **0.50232** | **1** |

To test the robustness, stage image is compressed by the method of Joint Photographic Experts Group (JPEG), because many applications on the internet which compress the image when transmitted to accelerate the transaction process. JPEG is a world standard for digital image compression. JPEG compression consists of two main compression algorithm, namely lossy compression and lossless compression [9], [14]. JPEG compression standard use DCT transformation with 8x8 sub-blocks, which consist the encoder and decoder. The encoder is a process for compressing image while the decoder is a process to restore the image to the size of its raw form. Below is an overview of standards encoder and decoder based on DCT in JPEG compression.

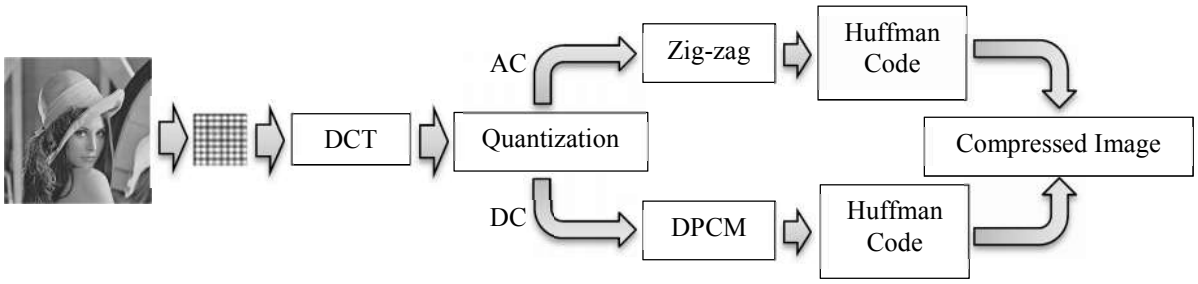



*Figure 6. Encoder process on JPEG standard*

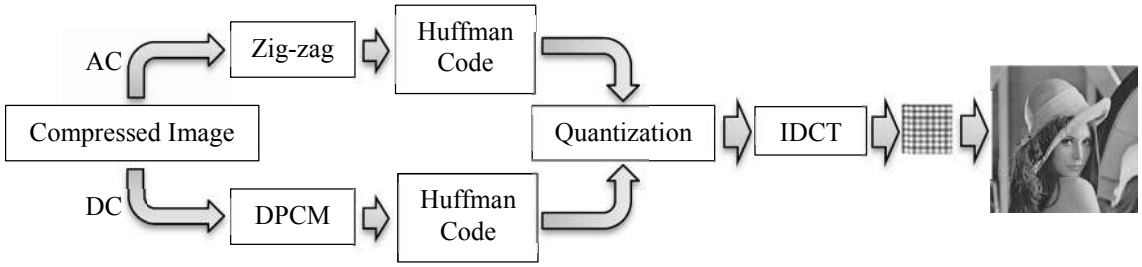



Figure 7. Decoder process on JPEG standard

The table below shows the analysis of the extracted message after stage image is compressed with JPEG method with compression quality 50% and 75%.

*Table 2. Result Analysis extracting message after JPEG Compression*

| Cover Image | NCC | |
|---|---|---|
| | Quality 50 % | Quality 75% |
| Babbon.bmp | 0.8984 | 1 |
| Barbara.bmp | 0.8972 | 0.9977 |
| Cameraman.bmp | 0.9068 | 0.9981 |
| Car.bmp | 0.8898 | 1 |
| F16.bmp | 0.8832 | 1 |
| Lena.bmp | 0.8762 | 0.9989 |
| Peppers.bmp | 0.9177 | 1 |
| Ship.bmp | 0.8276 | 0.9645 |
| Soccer.bmp | 0.8731 | 0.9921 |
| Women.bmp | 0.8689 | 0.9843 |
| **Average** | **0.8839** | **0.9936** |

Besides JPEG compression attack, stage image was also tested with a median filter. Each pixel output shows the median value of 3x3 neighborhood pixel corresponding to the input image. The table below shows the analysis of the extracted message after stage image is filtered.

*Table 3. Result Analysis extracting message after median filter*

| Cover Image | NCC |
|---|---|
| Babbon.bmp | 0.6060 |
| Barbara.bmp | 0.8356 |
| Cameraman.bmp | 0.9212 |
| Car.bmp | 0.7811 |
| F16.bmp | 0.8629 |
| Lena.bmp | 0.9004 |

| | |
|---|---|
| Peppers.bmp | 0.9301 |
| Ship.bmp | 0.5772 |
| Soccer.bmp | 0.9149 |
| Women.bmp | 0.8295 |
| **Average** | **0.8159** |

## 4. CONCLUSION

In this paper, we propose a combination of steganography with DCT and OTP encryption. This system encrypts a secret message before embedding in digital imagery. Based on the evaluation of the proposed algorithm produces an image that is identical to the cover image, this is evidenced by the value of PSNR and MSE are relatively excellent, as well as a perfect extraction. In addition, this algorithm is also quite robust to JPEG compression and mid filter

## 5. FUTURE WORK

For future work, this method can be combined with PN Sequence. It can also be combined with other transformation methods such as discrete wavelet transform (DWT), discrete Fourier transform (DFT), haar wavelet transforms (HWT), or others transformation. Another encryption method such as RSA, DES or AES can also be applied to this method

## *REFERENCES*

[1] O. Cetin dan A. T. Ozocerite, "A new steganography algorithm based on color histograms for data embedding into raw video streams," *Computers & Security,* vol. XXVIII, no. 7, p. 670–682, 2009.

[2] T.-H. Lan-dan A. H. Tewfik, "A Novel High-Capacity Data-Embedding System," *IEEE Transactions on Image Processing,* vol. XV, no. 8, pp. 2431-2440, 2006.

[3] P. Patel dan Y. Patel, "Secure and authentic DCT image steganography through DWT –SVD based Digital watermarking with RSA encryption," dream *Fifth International Conference on Communication Systems and Network Technologies*, Gwalior, 2015.

[4] B. G. Banik dan S. K. Bandyopadhyay, "Implementation of Image Steganography Algorithm using Scrambled Image and Quantization Coefficient Modification in DCT," dream *International Conference on Research in Computational Intelligence and Communication Networks.*, 2015.

[5] M. Gunjal dan J. J., "Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm," *International Journal of Computer Trends and Technology,* vol. XI, no. 4, pp. 144-150, 2014.

[6] S. T, "A Secure DCT Image Steganography based on Public-Key Cryptography," *International Journal of Computer Trends and Technology (IJCTT),* vol. IV, no. 7, pp. 2039-2043, 2013.

[7] O. Cornea, M. E. Borda, V. Paczki dan R. Malutan, "DNA Vernam Cipher," dream *International Conference on E-Health and Bioengineering*, Iaşi, 2011.

[8] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons Inc, 1996.

[9] A. Bovik, The Essential Guide to Image Processing, Texas: Elsevier Inc., 2009.

[10] J. Huang, Y. Q. Shi dan Y. Shi, "Embedding Image Watermarks in DC Components," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 10, no. 6, pp. 974 - 979, September 2000.

[11] R. Shukla, H. O. Prakash, R. Bhushan, S. Venkataraman dan G. Varadan, "Sampurna Suraksha:

Unconditionally Secure And Authenticated One Time Pad Cryptosystem," dream *International Conference on Machine Intelligence Research and Advancement*, Katra, 2013.

[12] E. Lehmann dan G. Casella, Theory of Point Estimation, 2nd penyunt., G. Casella, S. Fienberg dan I. Olkin, Penyunt., New York: Springer Verlag, 1998.

[13] A. Al-Haj, "Combined DWT-DCT Digital Image Watermarking," *Journal of Computer Science,* vol. 3, pp. 740-746, September 2007.

[14] P. Singh, S. Shivani dan S. Agarwal, "A Chaotic Map Based DCT-SVD Watermarking Scheme For Rightful Ownership Verification," dream *Students Conference on Engineering and Systems (SCES)*, Allahabad, 2014.

[15] G. K. Wallace, "The JPEG still picture compression standard," *IEEE Consumer Electronics Society,* vol. 38, no. 1, pp. 18-34, February 1992.