Information hiding in images using Discrete Cosine Transform

G Emmanuel, G G Hungil, J Maiga and A J Santoso*
Universitas Atma Jaya Yogyakarta, Yogyakarta, Indonesia

*albjoko@staff.uajy.ac.id

Abstract. In this era of development and increasing use of the Internet, user facing security problem during information sharing in which unauthorized receivers can gain access to the information transmitted. Data hiding during the transmission of information via the internet is one of the techniques used to keep the secrecy of the information to the unauthorized/unintended persons. Steganography is a way of hiding secrets information by inserting it into an audio, video, image or text file without raising any suspicious to unintended persons. This paper presents the study which hides text messages into the image file by using Discrete Cosine Transform (DCT) steganography method. The method of this work by transforming the cover image and text message from spatial domain to frequency domain and use redundant bit of cover image to hide text message in such a way that unintended person will continue to see it as a normal image. The method continues to keep the quality of the cover image which transfers the information to reduce suspicion. Steganography is mostly used in military, law enforcement agency, corporate spies and in the medical area for hiding sensitive information.

1. Introduction
High speed penetration of the internet in the world has led to the increased sharing of information using smartphone and computer [1]. However, the problem is, everything being shared in the website channel such as social media, an online business can be accessed by unauthorized receivers. The solution is to hide data/information during transmission. Steganography is an art or science of hiding secret data/information without drawing attention to an unintended recipient [2]. The method can hide data in audio, video, image, or text in degree that the cover file which carries the data remains normal as if it does not carry any secret information. Steganography is mostly used in military, law enforcement agencies, corporate spies, a terrorist organizations, whistleblowers, drug dealers, and even in medical imaging in all cases the main aim is to hide sensitive information [3–5].

The idea and practice of information hiding (steganography) have long been there since ancient Greece and Persia. One example was when the Roman general used to embed the tattooed message on the shaved head of a slave when the hair grows the tattooed messenger was sent to deliver the secret message [6]. The problem with this approach is if the secret is known it’s easy to access the secret message by shaving all slaves who pass. The current computerized approach involves using a redundant bit of the cover file being replaced with a secret message in a way that the cover file will look normal. With this new approach reduces suspicious feeling that there is a secret message in the stego media. Even if the secret is known that there is a secret message in the cover media it’s difficult and time-consuming process trying to decode and access the secret message [7]. Cryptography and Steganography
are two related terms with a different meaning. Cryptography is a method of hiding the information by making the information unreadable with the main setback that it raises suspicions to an unauthorized receiver [8]. Steganography aims to resolve the setback by reducing/ removing suspicions that there is a secret message in the communication. This paper presents a steganography method of hiding text message in the image by transforming the cover image and text message from spatial representation to frequency representation using a Discrete Cosine Transform (DCT). This approach hides the data in unnecessary bits of the carrier cover image in frequencies representation.

This paper is divided into five parts, first is an introduction in which problem and solution is discussed, then related work in which works related to this work will be explained in a second part. After that, the detailed explanation and implementation of the proposed steganography method will be discussed in the methodology part. Then the fourth will be the results and the final part will be the conclusion of this study.

2. Related work

Steganography method of hiding information in the image can be conducted using two approaches, using image spatial domain representation or frequency domain representation. One of the method which uses spatial domain is Least Significant Bit (LSB) [9,10], this approach hides information in the image by which intended message is hidden in the last unnecessary bit of the image but as the amount of hidden information increase the quality of carrier image decreases which can rise suspicions. Another method is Grey Level Modification Method (GLM) [10], in this approach the mathematical formula is used to modify grey level value of image into odd or even grey pixel and use it to represent binary data [11]. The pixel value differencing (PVD) Method [12] is also among of the spatial domain methods where it uses the difference value between two successive pixels in a block for calculating where the secret bits should be fixed [13].

Furthermore, Pixel Mapping Method (PMM) [14] is also a method or an approach in which the pixel to insert the secret information is selected based on mathematical function and pixel intensity value of seed pixel and its 8 neighbors pixel [15,16]. Also, there is the method proposed by Ahmed T et al. where information among the dimensional house of the gray scale image, where the separation of the elements into equal of the total vary of 1’s among the four bits on the left aspect of the pixels [17]. Pixel Mapping Method (PPM) [13] is the one which takes the pixels of cover image where the confidential data is going to be hidden for Embedding pixels selected based on some mathematical function which depends on the pixel concentration value of the seed pixel and its 8 neighbors are selected in counter clockwise direction [14,15]. Also, there is the method proposed by Ahmed T et al. where information among the dimensional house of the gray scale image, where the separation of the elements into equal of the total vary of 1’s among the four bits on the left aspect of the pixels [16].

On the frequency domain (transformation domain steganography) the authentication of the image is transformed into a coefficient form of the combined image [15]. Among used techniques includes Fast Fourier Transform (FFT) [18,19], Wavelet Transform (WT) [20,21] and Gabor Transform (GT) [20]. The most used steganography approaches in the image follow the steps shown in Fig.1.
This paper uses a Discrete Cosine Transform (DCT) to hide text message in the image. The method hide information in the transformed coefficient of the frequency domain of the image. The proposed method hide information in the image without much altering of the image which does not raise

3. Methods
Discrete Cosine Transform (DCT) use frequency domain of the image to hide the information. In this study, we are going to shows how to hide text message in the image using DCT. The way it operates first cover image pixel is grouped into 8 x 8-pixel blocks, then the pixel blocks are transformed into 64 DCT coefficients. The pixel blocks can be divided into high, middle and low-frequency bands based on cover image visual quality. The DCT coefficients of the cover image and text message are calculated by the formula below adopted from the study by Johnson et al. [5].

\[ C(u, v) = a(v) \sum_{u=0}^{N-1} a(u) \sum_{x=0}^{N-1} x_i \cos \left( \frac{(2i+1)ux}{2N} \right) \times \cos \left( \frac{(2i+1)ux}{2N} \right) \]  

(1)

From the formula u,v start from 0,1,2, ..., N – 1 and C(u,v) presents the matrix of DCT coefficient in a row u and column v. Then the 64 DCT coefficients are quantized by using the following formula below.

\[ C^Q(u, v) = \frac{C(u,v)}{Q(u,v)} \]  

(2)

Where Q(u,v) represent 64 elements of the quantization table.

After getting the quantized DCT coefficients, its least significant bits can be used as redundant bits to hide the text message and get the stego image. This approach works well with the JPEG image format. Change made in the middle frequencies band is difficult to be noted by human eyes, its better the hidden message to be inserted there.

The method of encoding the Text message can be summarized in Figure 2.
To extract the message involve taking the stego image and divide into 8 by 8-pixel block then transform into 64 DCT coefficient of each pixel block and quantized them after that extract the text message in the middle of the frequency band. Fig.3 shows how it occurs.

![Diagram of decoding process using DCT]

**Figure 3.** Process of decoding using DCT.

4. **Results and discussion**

To implement the Discrete Cosine Transform (DCT) method, the study uses MATLAB image processing toolkit on window operating system with Intel Core i5 CPU @ 2.30 GHz and 4 GB of RAM. The Figure 4 of cover image and stego image with difference image size is shown below. Based on results it shows that the data size of stego images increases as the amount of hidden information increase.

![Lena image with 9.18 kb and 'Hello World' as stego image]

**Figure 4.** Lena image before and after steganography.

The Fig. 4. Show the results of steganography on lena image by inserted the message ‘Hello World’ in it. The size of stego image increase from 9.18 kb to 17.4 kb.

5. **Conclusion**

This study uses Discrete Cosine Transform (DCT) to hide text message in the image. This is good steganography approach as it keep the quality of cover image which carrier the text message to look normal and reduce suspicious to the unintended recipients. Based on the result above it show that as the amount of the information stored in the cover image increase the quality of cover image decrease as it can erase suspicious. In future work the study will look ways of increasing the amount of information which can be carried in the cover image.

**References**

[1] Malaysian Communication and Multimedia Commission 2018 Internet Users Survey 2018: Statistical Brief Number Twenty-Three *Internet users Surv.* pp 1–39

[2] Islam M M and Kamal A H M 2014 Facilitating and securing offline e-medicine service through image steganography *Healthc. Technol. Lett.* 1(2) pp 74–79

[3] Waziri V O and Ochoche A 2012 Steganography and Its Applications in Information Dessimilation on the Web Using Images as SecurityEmbedddment: A Wavelet Approach *01*(02) pp 194–202
[4] Channalli S and Jadhav A 2009 Steganography An Art of Hiding Data Int. J. Comput. Sci. Eng. 1(3) pp 137–141
[5] Johnson N F and Jajodia S 1998 Exploring steganography: Seeing the unseen Computer (Long, Beach, Calif) 31(2) pp 26–34
[6] Chan C K and Cheng L M 2004 Hiding data in images by simple LSB substitution Pattern Recognit 37(3) pp 469–474
[7] Ning J, Singh I, Madhyastha H V, Krishnamurthy S V, Cao G, and Mohapatra P 2014 Secret message sharing using online social media 2014 IEEE Conf. Commun. Netw. Secur. CNS pp 319–327
[8] Potdar V M and Chang E 2005 Grey level modification slegenography for secret communication pp 223–228
[9] Wang C M, Wu N I, Tsai C S, and Hwang M S 2008 A high quality steganographic method with pixel-value differencing and modulus function J. Syst. Softw. 81(1) pp 150–158
[10] Tseng H W and Leng H S 2013 A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number J. Appl. Math. 2013 pp 1–8
[11] Tse-Hua Lan, Mansour M F, and Tewfik A H 2002 Robust high capacity data embedding pp 581–584
[12] Mandal S and Bhattacharyya S 2016 Secret data sharing in cloud environment using steganography and encryption using GA Proc. 2015 Int. Conf. Green Comput. Internet Things, ICGCIO T 2015 pp 1469–1474
[13] Banerjee I, Bhattacharyya S, and Sanyal G 2014 Hiding & Analyzing Data in Image Using Extended PMM Procedia Technol. 10 pp 157–166
[14] Medeni M B O and Souidi E M 2011 A novel steganographic method for gray-level images with four-pixel differencing and LSB substitution Int. Conf. Multimed. Comput. Syst. -Proceedings pp 1–4
[15] Rafferty C 2005 Steganography & Steganalysis of Images Natl. Univ. Ireland, Galw.
[16] Wimp J, McPeak R, and McPeak S 2006 The Fast Fourier Transform Workshop Am. Math. Mon. 105(3) p 289
[17] Lil X, Zhao H, Chen Z, and Hu J 2018 A Comparison between Fast Fourier Transform and Matrix Pencil Method for Spectral Integration Calculation 2018 IEEE Int. Conf. Comput. Electromagn. ICCEM 2018(4) pp 5–7
[18] Dautov C P and Ozerdem M S 2018 Wavelet transform and signal denoising using Wavelet method 26th IEEE Signal Process. Commun. Appl. Conf. SIU 2018 pp 1–4
[19] Qian S and Chen D 1993 Discrete Gabor Transform IEEE Trans. Signal Process 41(7) pp 2429–2438
[20] Thepade S D, Dewan J H, Erandole S S, and Jadhav S R 2015 Extended performance comparison of self mutated hybrid wavelet transforms in image compression with hybrid wavelet transforms & orthogonal transforms Glob. Conf. Commun. Technol. GCCT 2015, no. Gcct pp 317–322