Implementations of Steganography in Digital Image Watermarking System

Annisa'ur Rosi Lutfiana - 13512088
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
annisaurrosi@s.itb.ac.id

***Abstract* — Cryptography as a term referring to the impersonation technique for message confidentiality has been well known and widely used especially in the field of computer science. Steganography is a term that has not been widely known, yet is a method that has same effectiveness as cryptography in the case of confidentiality; the difference part is only in its way to represents the real message to the third party. This paper specially gives a brief explanation about the definition of steganography in general, its relation to digital watermarking system which is known as one of its most commonly used application, as well as examples of its usage and implementation in algorithm to physical program.**

***Index Terms* — Steganography, watermarking, Direct Cosine Transformation, Least Significant Bit**

I. INTRODUCTION

The use of cryptography system is sometimes sufficiently effective to keep the secrecy of a message, especially if supported with tricky code encryption systems which make it difficult to decrypt. However most of the time the first party as the message sender does not intend to let the third party to know that there is actually a 'hidden message' on the document being routed. The first party possibly does not want any suspicion spreads between the third parties that there is actually another message in the very inside of the file.

Another thing which is likely to happens in today's information era is the freely and widely-spread of the authors works through a variety of digital media. In case of the works are copyrightly protected, a new problem will come up as a consequence of the distribution of documents (especially via the web) which is almost uncontrollable and can hardly be traced. Mischievous usages of the documents becomes something inevitable.

In addition to these cases, there are other things that might be often occurred as a common academic issue. For example - if a group of students were given the task to process any identical digital files, then it will be a rough job for the examiner to identify the presence of fraud that as if there is duplication of documents to two different students. Clearly visible attached identity on the file may be easily removed. As a solution, it would be safer if each student has a specific signature that can only be detected by the examiners. A similar kind of solution can be used to override the prior problems by providing a mark which its presence can only be seen by the original owners of the files and some particular others.

In this case, further discussion is about to explain how a method called steganography protects the documents (mainly in the images file type) by attaching some types of encryption algorithms.

II. RELATED THEORIES

A. Definition of Steganography

Steganography is the art and science of encoding hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. It is a form of security through obscurity. The word *steganography* is of Greek origin and means "concealed writing." It combines the Greek words *steganos* (στεγανός), meaning "covered or protected," and *graphei* (γραφή) meaning "writing." The first recorded use of the term was in 1499 by Johannes Trithemius in his *Steganographia*, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages will appear to be (or be part of) something else: images, articles, shopping lists, or some other *cover text*. For example, the hidden message may be in invisible ink between the visible lines of a private letter.

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—will arouse interest, and may in themselves be incriminating in countries where encryption is illegal[1]. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

B. Basic Model of Steganography System

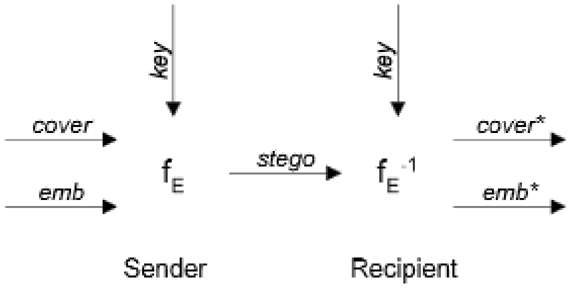


Fig. 2.1 Steganography scheme

f_E	: Steganographic function "embedding"
f_E^{-1}	: Steganographic function "extracting"
cover	: coverdata in which emb will be hidden
emb	: Message to be embedded
key	: Parameter of f
stego	: Coverdata with embedded message[2]

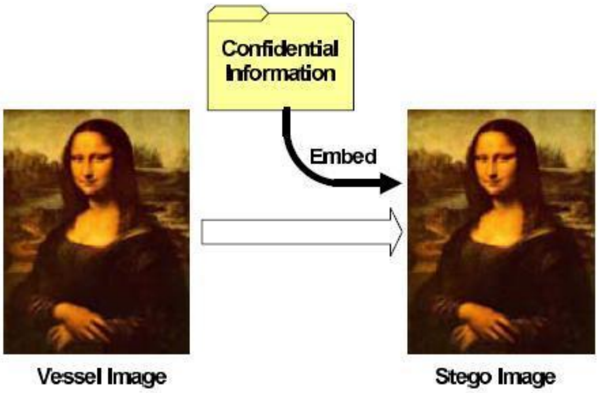


Fig. 2.2 Steganography process and result illustration

C. Comparison between Steganography and Criptography

Cryptography (or *cryptology*; from Greek κρυπτός, "hidden, secret"; and γράφειν, *graphein*, "writing", or -λογία, *-logia*, "study", respectively) is the practice and study of techniques for secure communication in the presence of third parties (called adversaries)[3]. More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries[4] and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation[5]. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Cryptography prior to the modern age was effectively synonymous with *encryption*, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

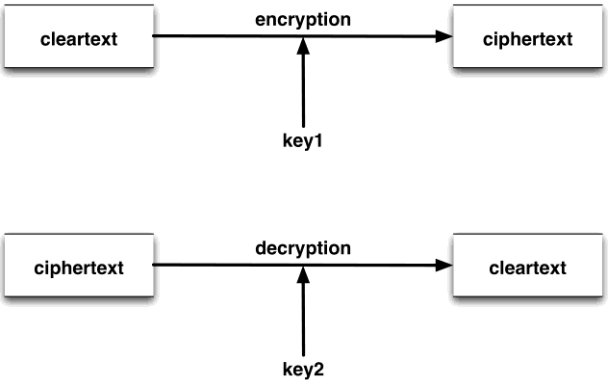


Fig. 2.3 Cryptography scheme

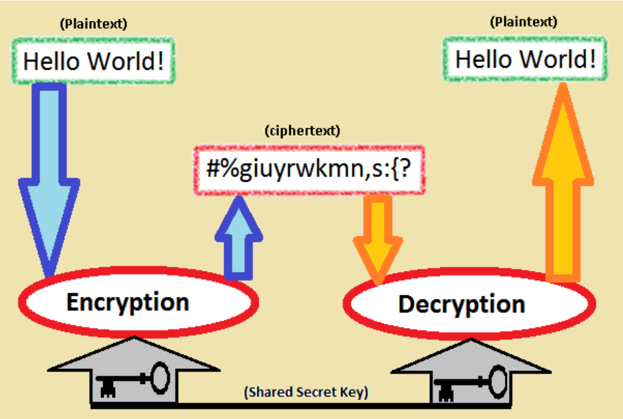


Fig. 2.4 Cryptography process and result illustration

Now comes to the comparison between these two methods. From the definition, it can be easily concluded that the difference between steganography and cryptography lies in the visual representation of the files after being sent from the first party. Encryption (can be in form of text chiper or embedded image) on steganography neatly pasted into an input file image the intermediaries might be unable to differentiate it with the original file. As in cryptography, encryption is included to change the file or text input so that its original form cannot be detected or returned unless using the appropriate key.

D. Methods of Watermarking Images Using Steganography

The method of steganography implementation varies from the simplest (less quality result image) to the most complicated which produce almost identical image result compared with the source. Now here only a couple methods will be discussed, which one of them is an example of quite simpler method while the other one has more complicated implementation yet produces better quality image. Here’s the brief definition and explanation of both methods, the implementation of its algorithms and how it works will be explained in Chapter III.

a. *LSB (Least Significant Bit) Image Hiding Method*

LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message into the image. The Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is changed to the bit of secret message. For 24 bit image, the colours of each component like RGB (red, green and blue) are changed. LSB is effective in using BMP images since the compression in BMP is lossless. But for hiding the secret message inside an image of BMP file using LSB algorithm it requires a large image which is used as a cover[6].

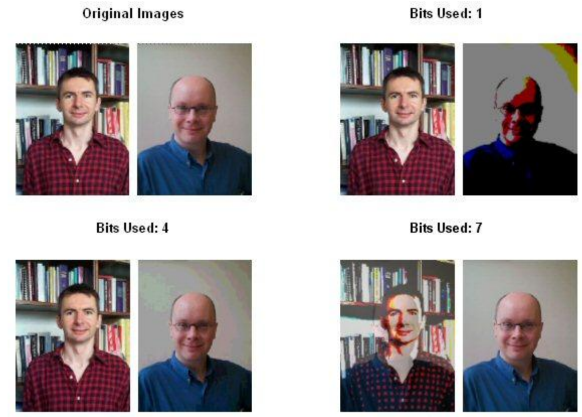


Fig. 2.5 The comparison of difference usage of bit

The left photo supposed to be the host and the right one is the photo as 'secret message'. This method works well when both the host and secret images are given equal priority. When one has significantly more room than another, quality is sacrificed. The only job is to adjust how the least significant bits are filled in the host image. However this technique makes it very easy to find and remove the hidden data[7].

b. *Direct Cosine Transformation (DCT) Method*

Image transforms are very important in digital processing they allow to accomplish less with more. For example the LSB may be used to effectively process images with simple algorithms or the Discrete Cosine Transform may be used to significantly decrease space occupied by images without noticeable quality loss[8].

The DCT transforms a signal or image from the spatial domain to the frequency domain. It separates the image into parts (or spectral sub-bands) of differing importance (with respect to the image visual quality). It can separate the Image into High, Middle and Low Frequency components[9]. Hiding via a DCT is useful as someone who just looks at the pixel values of the image would be unaware that anything is amiss. Also the hidden data can be distributed more evenly over the whole image in such a way as to make it more robust.

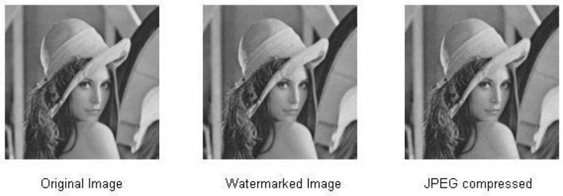


Fig. 2.6 Images generated by DCT method

III. Implementation

A. *LSB (Least Significant Bit) Image Hiding Method*

LSB is the lowest bit in a series of numbers in binary. e.g. in the binary number: 10110001, the least significant bit is far right 1. The LSB based Steganography is one of the steganographic methods, used to embed the secret data in to the least significant bits of the pixel values in a cover image. e.g. 240 can be hidden in the first eight bytes of three pixels in a 24 bit image.

PIXELS: (00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

240 : 011110000

RESULT: (00100110 11101001 11001001)
(00100111 11001001 11101000)
(11001000 00100110 11101000)

Here number 240 is embedded into first eight bytes of the grid and only 6 bits are changed[10].

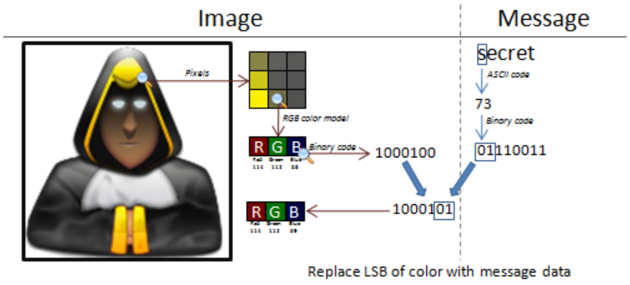


Fig. 3.1 LSB method illustration

Algorithm to embed text message

Step 1 : Read the cover image and text message which is to be hidden in the cover image.

Step2 : convert the color image into grey image.

Step 3 : Convert text message in binary.

Step 4 : Calculate LSB of each pixels of cover image.

Step 5 : Replace LSB of cover image with each bit of secret message one by one.

Step 6 : Write stego image.

Algorithm to retrieve text message

Step 1 : Read the stego image.

Step 2 : Calculate LSB of each pixels of stego image.

Step 3 : Retrieve bits and convert each 8 bit into character[11].

B. Direct Cosine Transformation (DCT) Method

DCT is a general orthogonal transform for digital image processing and signal processing with advantages such as high compression ratio, small bit error rate, good information integration ability and good synthetic effect of calculation complexity[12]. One dimensional DCT can be described with the help of (1) and (2):

$$F(0) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} f(x) \qquad (1)$$

$$F(u) = \sqrt{\frac{2}{N}} \sum_{x=0}^{N-1} f(x)\, Cos\, \frac{2(x+1)u\pi}{2N} \qquad (2)$$

Where F (u) is cosine transform coefficient, u is general frequency variable, u=1, 2, 3…., N-1; if f(x) is M sequence of time domain, x= 1, 2, 3… N-1, one dimensional inverse discrete cosine transform is defined as (3):

$$f(x) = \sqrt{\frac{1}{N}} F(u) + \sqrt{\frac{2}{N}} \sum_{x=0}^{N-1} f(x)\, Cos\, \frac{2(x+1)u\pi}{2N} \qquad (3)$$

Two dimensional DCT can be defined analogously as (4):

$$f(x,y) = C(u)C(v) \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} F(u,v)\, Cos\left[\frac{(2x+1)u\pi}{2N}\right] Cos\left[\frac{(2y+1)v\pi}{2N}\right] \qquad (4)$$

The inverse of two dimensional DCT can be defined as (5):

$$F(u,v) = \frac{2}{N} C(u)C(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y)\, Cos\left[\frac{(2x+1)u\pi}{2N}\right] Cos\left[\frac{(2y+1)y\pi}{2N}\right] \qquad (5)$$

For x, y =0, 1, 2… N −1. N is horizontal and vertical pixel number of pixel block, generally N=8. If N is more than 8, efficiency is increased a little but complexity is increased many times[13].

DCT allows an image to be broken up into different frequency bands namely the high, middle and low frequency bands thus making it easier to choose the band in which the watermark is to be inserted. The literature survey reveals that mostly the middle frequency bands are chosen because embedding the watermark in a middle frequency band does not scatter the watermark information to most visual important parts of the image i.e. the low frequencies and also it do not overexpose them to removal through compression and noise attacks where high frequency components are targeted.

Numerous watermarking techniques based on DCT are proposed. Although some of the watermarking techniques embed the watermark in the DC component, most techniques utilize the comparison of middle band DCT coefficients to embed a single bit of watermark information into a DCT block. The middle-band frequencies (FM) of an 8*8 DCT block can be shown below in figure 3.2. DCT block consists of three frequency bands-Low frequency band (FL), High frequency band (FH), mid frequency band (FM). We have chosen FM for embedding the watermark.

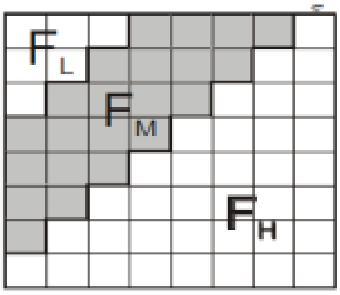


Fig 3.2 DCT regions

Two locations Mi (u1, v1) and Mi (u2, v2) from the frequency band FM are chosen as the region for comparison. The choice in selection of the two locations is dependent on the JPEG quantization table given below in table 2.1. The two locations with similar quantization values are chosen for embedding one watermark bit of information.

Table 2.1 Quantization values

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

The DCT block will encode a “0” if Mi (u1, v1) < Mi (u2, v2), otherwise it will encode a “1”. The coefficients are then swapped if the relative size of each coefficient does not agree with the bit that is to be encoded. The number of watermark bits that can be embedded is directly dependent on the number of pairs of locations in quantization table with similar values. The robustness of the watermark can be improved by introducing a watermark strength or gain constant k, such that Mi (u1, v1) - Mi (u2, v2) > k. Coefficients that do not meet this criteria are modified though the use of random noise as to then satisfy the relation. Increasing k thus reduces the chance of detection errors at the expense of additional image degradation[14].

Another category of DCT based watermarking techniques add a pseudo number sequence in the mid frequency band of the image to be watermarked. A strength factor k used which gives robustness to the watermark. The value of k should be intelligently decided otherwise imperceptibility of the watermarked image with the original unwatermarked is reduced. For the mid frequency band of given DCT block x, y the embedding process can be shown using the equation (6) shown below:

$$I_{W_{x,y}}(u,y) = \begin{cases} I_{x,y}(u,\bar{v}) + K * W_{x,y}(u,v), & u,v \in F_M \\ I_{x,y}(u,v), & u,v \in F_M \end{cases} \quad (6)$$

Algorithm to embed text message

Step 1 : Read cover image.

Step 2 : Read secret message and convert it in binary.

Step 3 : The cover image is broken into 8×8 block of pixels.

Step 4 : Working from left to right, top to bottom subtract 128 in each block of pixels.

Step 5 : DCT is applied to each block.

Step 6 : Each block is compressed through quantization table.

Step 7 : Calculate LSB of each DC coefficient and replace with each bit of secret message.

Step 8 : Write stego image.

Algorithm to retrieve text message

Step 1 : Read stego image.

Step 2 : Stego image is broken into 8×8 block of pixels.

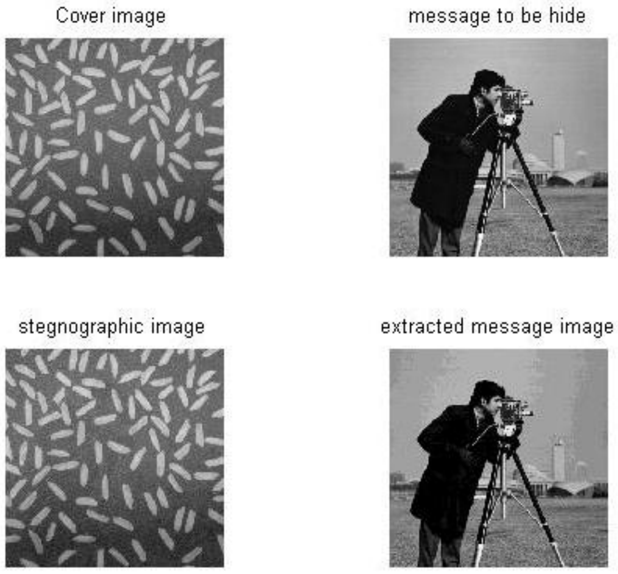
Step 3 : Working from left to right, top to bottom subtract 128 in each block of pixels.

Step 4 : DCT is applied to each block.

Step 5 : Each block is compressed through quantization table.

Step 6 : Calculate LSB of each DC coefficient[11].

IV. RESULTS



4.1 Images generated by LSB method

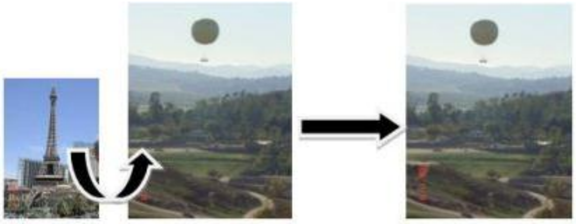


Fig.4.2 Images generated by DCT method

By a single glance of comparison it appears that the changes in the processed image by LSB are more visible than by DCT. In LSB the stegno (generated picture) and the extracted message image tend to experience a change from the original looks. To override this problem, the sender should be more concerned about the allocation of bits for both of pictures so that the changes can be less visible.

As for the DCT method, the resulting image is arguably very precise compared with the original image. The image message camouflaged almost flawlessly in the stegno. This indicates that the algorithm used in this method is very effective for steganographic system.

The analysis of LSB based and DCT based steganography has been done on basis of parameters like PSNR, MSE, processing time, security. PSNR computes the peak signal to noise ratio, in decibels, between two images. This ratio is used as a quality measurement between two images. If PSNR ratio is high then images are best of quality.

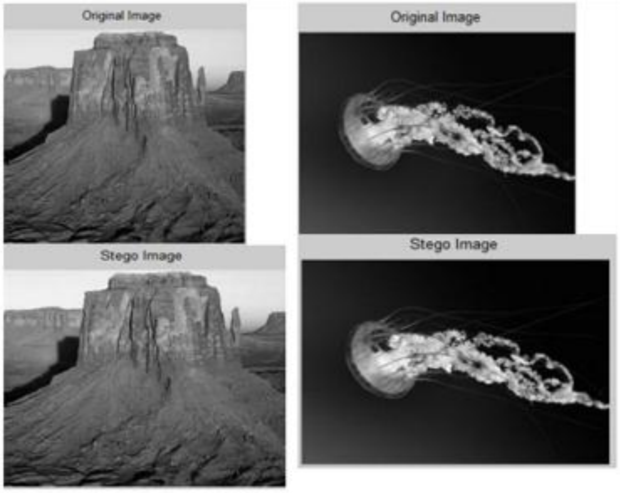


Fig.4.3 LSB images for analysis table

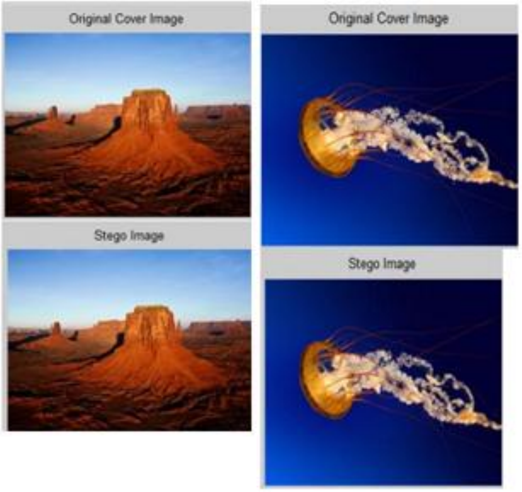
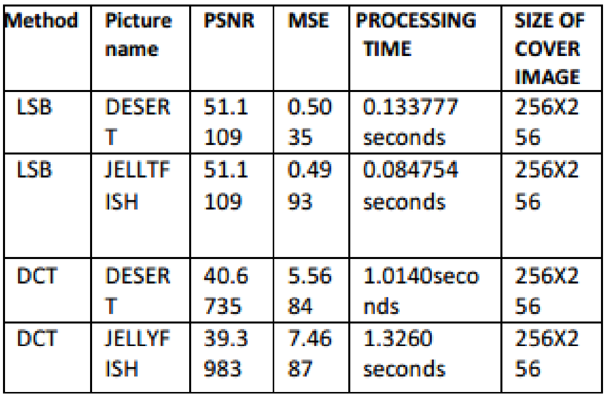


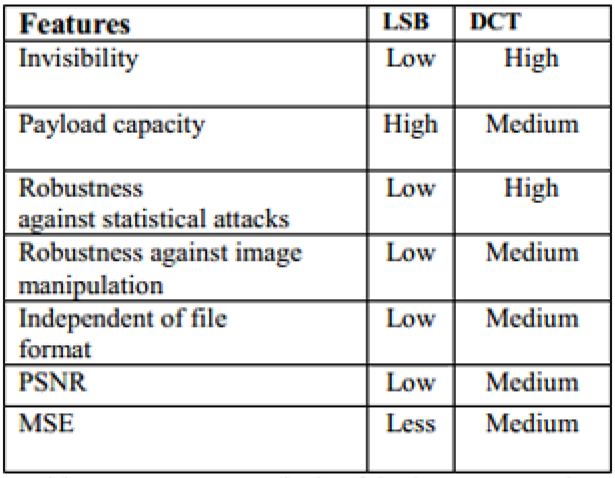
Fig.4.4 DCT images for analysis table

Table 4.1 Image quality analysis



Method	Picture name	PSNR	MSE	PROCESSING TIME	SIZE OF COVER IMAGE
LSB	DESERT	51.1109	0.5035	0.133777 seconds	256X256
LSB	JELLTFISH	51.1109	0.4993	0.084754 seconds	256X256
DCT	DESERT	40.6735	5.5684	1.0140seconds	256X256
DCT	JELLYFISH	39.3983	7.4687	1.3260 seconds	256X256

Table 4.2 Qualitative parameter analysis



Features	LSB	DCT
Invisibility	Low	High
Payload capacity	High	Medium
Robustness against statistical attacks	Low	High
Robustness against image manipulation	Low	Medium
Independent of file format	Low	Medium
PSNR	Low	Medium
MSE	Less	Medium

V. Conclusion

The use of watermarks on image file type can secretly provide an identity in order to trace the distribution of digital images, especially on the web. In addition it also enables to minimize the acts of copyright abuse by using a watermark on every works. Steganography method is highly recommended to give the code on the host file barely without visible traces so it does not spoil the view. Cryptography or manually giving identity with conventional watermark image or text can be less advisable for the sake of security and visibility.

When the author only needs simple algorithms and programs as its implementation, LSB method can be the solution. Then if the quality of the image as the main priority, the DCT method is recommended. Lastly, it is not such impossible thing that that other methods work better than the two examples of implementations which have been discussed.

VI. Acknowledgment

Annisa’ur Rosi Lutfiana, as the author of this paper, want to express her grateful thanks to God for His blessing during the making of this paper, her deepest gratitude to Dra. Harlili, M.Sc and Dr. Ir. Rinaldi Munir, M.T. as the lecturers of IF2120 – Matematika Diskrit.

Special thanks to my family back home and all my friends in HMIF for all the supports and guidances.

Also thanks for all of the authors which I got a lot of this study references from, may God bless your knowledge with endless abundances.

References

[1] Pahati, OJ (2001-11-29). *Confounding Carnivore: How to Protect Your Online Privacy*. AlterNet. Archived from the original on 2007-07-16. Retrieved 2008-09-02.

[2] B. Pfitzmann, *Information Hiding Terminology*. In R. Anderson, Information Hiding: First International Workshop, Proceedings (Lecture notes in computer science; Vol. 1147), Berlin: Springer, 1996.

[3] Rivest, Ronald L. "Cryptology". In J. Van Leeuwen.*Handbook of Theoretical Computer Science* **1**. Elsevier, 1990.

[4] Bellare, Mihir; Rogaway, Phillip (2005-09-21). "Introduction". *Introduction to Modern Cryptography*. p. 10.

[5] Menezes, PC van Oorschot, and SA Vanstone, *Handbook of Applied Cryptography*. ISBN 0-8493-8523-7.

[6] Bloom, J. A. et al,. *Digital Watermarking and Steganography*. 2nd ed. MorganKaufmann, 2008.

[7] M. D. Swanson, B. Zhu and A. H. Tewfik, *Robust Data Hiding for Images*, IEEE Digital Signal Processing Workshop, pp. 37-40, Department of Electrical Engineering, University of Minnesota, http://www.assuredigit.com/tech_doc/more/Swanson_dsp96_robust_datahiding.pdf, September 1996.

[8] Sumbera Dr. Taylor, J., M SOE Final Project ,*Wavelet Transform using Haar Wavelets*. 2001.

[9] Rafferty,C., M sc Comms Sys Theory. *Steganography & Steganalysis of Images*. 2005.

[10] Ankur M. Mehta, Steven Lanzisera, and Kristofer S. J. Pister, *Steganography 802.15.4 Wireless Communication*. 2005.

[11] Anil K Jain, *Fundamentals of Digital Image Processing*. University of California-Davis, Prentice Hall, 1988.

[12] Zhu, Gengming and Nong Sang, *Watermarking Algorithm Research and Implementation Based on DCT Block*, World Academy of Science, Engineering and Technology 45. 2008.

[13] Khayam, Syed Ali. *The Discrete Cosine Transform (DCT): Theory and Application*, ECE 802 – 602: Information Theory and Coding. 2003.

[14] Hsu, C.-T., Wu, J.-L, *Multiresolution Watermarking for Digital images*, in IEEE Transactions on Circuits and Systems - II: Analog and Digital Signal Processing, vol. 45,no. 8, pp. 1097-1101. 1998.

STATEMENT

I hereby stated that this paper is copyrighted to myself, neither a copy from other’s paper nor a translation of similar paper.

Bandung, 13 Desember 2013

Annisa’ur Rosi Lutfiana – 13512088