A Modified High Capacity Image Steganography using Discrete Wavelet Transform

Moh Moh Zan, Nyein Aye
University of Technology (Yatanarpon Cyber City)

Abstract

Steganography is the most used technique for data hiding. We can implement it using any cover media like text, images and videos. This research presents a technique for image steganography based on DWT, where DWT is used to transform original image (cover image) from spatial domain to frequency domain. Two dimensional Discrete Wavelet Transform (2D-DWT) is performed on cover image of size M × N. The secret message is encrypted using Blowfish encryption algorithm. There are many cryptography techniques available. Among of them Blowfish is one of the most powerful techniques. This system will modify the LSB technique by putting the encryption step and new insertion algorithm. It improved the image quality and imperceptibility. Our method sustains the security attacks. Proposed system presents our new insertion technique which embeds the secret messages in frequency domain. It can measure the quality of container image with secret image after image hiding process PSNR values. Extensive testing is performed using different sizes of images and presented our results in payload and PSNR values.

Keywords: *Steganography, DWT, 2D-DWT, LSB and Blowfish encryption.*

1. Introduction

Data hiding can be done by cryptography, steganography and watermarking. We are here only considering steganography and cryptography. Steganography and Cryptography are two popular ways of sending vital information in a secret way. One hides the existence of the message and the other distorts the message itself. Steganography which literally means "covered writing" and is a branch of information hiding. The steganography is science of data hiding within another one, so that its presence is undetectable and suffers less security threats or attacks. It hides the content in cover media as not to provoke any doubt that there is some information or message hidden in the media [1]. In Steganography we have various techniques in different domains like spatial domain, frequency domain etc. to hide the message. There are many aspects to security and many applications. One essential aspect for secure communications is that of cryptography. In encryption the content is not hidden but not readable by the reader if the key is not known to him. But the encrypted content can be intercepted by anyone and chances always present that he will try to decode it or affect it by attempting to decode it for a purpose or just for the sake of curiosity. Whereas, steganography gives us more freedom to communicate and send secret information without leaving any evidence that opponent will intercept and try decoding your information. The idea of this paper is to apply both of them together with more security levels and to get a very highly secured system for data hiding. The combination of steganography and cryptography certainly provide much better secure communication For hiding data, different cover media can be used like, text, image, video etc. The content to be covertly sent is payload which is called stego text after application of any steganographic technique and media used is called stego image/text/video/protocol (depending on the choice of media). The opposite of it is steganalysis, which is out of the scope of this paper. The most popular cover object is image to perform steganography. In Steganography we have various techniques in different domains like spatial domain, frequency domain etc. to hide the message. It is very difficult to detect hidden message in frequency domain and for this domain we use various transformations like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and many others. In spatial domain messages are embedded in the intensity of image pixel like in LSB directly. Whereas in transform domain, image is first transformed using various transformation techniques and then message is encoded into the transformed image. There are many different image file formats exists, jpeg, bmp, png, etc,… But jpeg format proved to be the best among all [2].

2. Background Theory

2.1. Steganography

The word steganography comes from the Greek steganos , meaning covered or secret, and graphy , meaning writing or drawing. Therefore, steganography literally means covered writing.

Steganography simply takes one piece of information and hides it within another. Computer files (images, sounds recordings, even disks) contain unused or insignificant areas of data. Steganography takes advantage of these areas, replacing them with information (encrypted mail, for instance). The files can then be exchanged without anyone knowing what really lies inside of them. Rumor has it that terrorists used steganography to transmit messages to one another. The data to be concealed is compressed and hidden within another file. The first step is to find a file which will be used to hide the message (also called a carrier or a container). The next step is to embed the message one wants to hide within the carrier using a steganographic technique. Two different techniques commonly used for embedding are: Replace the least significant bit of each byte in the [carrier] with a single bit for the hidden message. Select certain bytes in which to embed the message using a random number generator; resampling the bytes to pixel mapping to preserve color scheme, in the case of an image...; hiding information in the coefficients of the discrete cosine, fractal or wavelet transform of an image; and applying mimic functions that adapt bit pattern to a given statistical distribution.

2.2. Wavelet Transform

Wavelet transform gives the best result for image transformation [3]. It decomposes signal into a set of basic functions. There are two flavors of wavelet transform, one is discrete and other is continuous. For our proposed system, we focus on discrete wavelet transform. In DWT we have 1-D, 2-D… n-D levels. 2D-DWT is used in our research work. It uses the scaling and wavelet functions of 1D-DWT. Figure 1 illustrate the 2D-DWT level. We can increase levels at the cost of complexity. It is two times decomposition of original signal via sub-division.

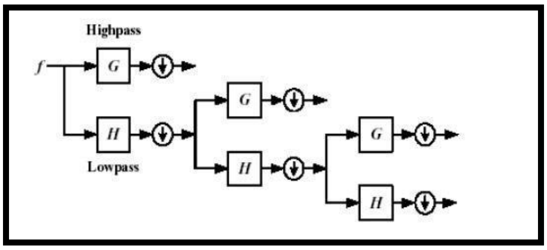

Figure 1. 2D-DWT for image

2.3. Blowfish (Encryption Algorithm)

It was designed by a cryptologist named Bruce Schneier and made it accessible for public. It is a 64-bit block cipher and variable key length. It has two parts. A first deal with the key expansion and second part performs the encryption of information. It increases contrast value in image by reducing the redundant information. In [4], it is presented that blowfish performs outclass compared to other encryption algorithms like AES, DES. We have selected blowfish to fulfill need of encrypted information.

4. Related Work

Amitava Nag, Sushanta Biswas, Debasree Sarkar & Partha Pratim Sarkar in [6] presented a novel technique using DWT transform for the cover image transformation and then Huffman is used on secret message before embedding. It uses only high frequency coefficients for embedding message bits and neglected low ones to get better image quality. Another image steganographic method using wavelet and Microsoft Utility for RC4 encryption [5] proposed which proves to be more secure. M. F. Tolba, M. A. Ghonemy, I. A. Taha, and A. S. Khalifa in 2004 [7] utilizes wavelet transforms that map integers to integers and proposed an algorithm that embeds the message bit stream into the LSB's of the integer wavelet coefficients of a true-color image. Proposed system can give the high invisibility even with large message size. The paper [8] propose hybrid steganography (HDLS) which is an integration of both spatial and transform domains. The cover image as well as the payload is divided into two cells each. The RGB components of cover image cell I are separated and then transformed individually from spatial to transform domain using DCT/DWT/FFT and embedded in a special manner, the components of cell II retained in spatial domain itself. [9] propose a new steganography technique which embeds the secret messages in frequency domain. According to different user's demands on the embedding capacity and image quality, the proposed algorithm is divided into two modes and 5 cases. They are fixed mode and varying mode. In the fixed mode, two cases are considered and in the varying mode, three cases are considered. Secret message are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Coefficients in the low frequency sub-band are preserved unaltered to improve the image quality. The system [10] devised a new algorithm to hide the text in any colored image of any size using wavelet transform. It improves the image quality and imperceptibility. This method sustains the security attacks. Extensive testing is performed using different sizes of images and presented our results in payload and PSNR values. Before embedding the text in colored image, the text is encrypted in blowfish encryption algorithm for more secure.

5. Proposed Steganography Method

Although steganography is applicable to all data objects that contain redundancy, in this paper, JPEG images are considered only. People often transmit digital pictures over email and other Internet communication, and JPEG is one of the most common formats for images. Moreover, steganographic systems for the JPEG format seem more interesting because the systems operate in a transform space and are not affected by visual attacks. (Visual attacks mean that steganographic messages can be seen on the low bit planes of an image because they overwrite visual structures; this usually happens in BMP images). Figure 2 shows a general representation of the proposed steganography method.

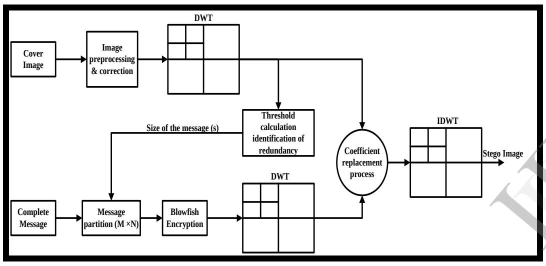

Figure 2. General representation for proposed steganography method

6. Proposed Insertion Technique

The extraction process is also reverse of insertion process as well. Firstly, extract the LSB from each HH, LH and HL. After that, it needs to transform back into octal number and then to hexadecimal format. The output hexadecimal format of cipher text can be decrypted by Blowfish decryption algorithm process. The contribution of proposed system is a new insertion method for hiding data in cover image and is more secure than inserting LSB of the image directly into steganographic system.

Hexadecimal ➡ Octal
8754269774 101162707060

Initial Array

F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

Start Encoding ⬇

2																
2	2															
2	2	2														
2	2	2	1													
2	2	2	1	0	4											
2	2	2	1	0	4	0	1									
2	2	2	1	0	4	0	1	0	7							
2	2	2	1	0	4	0	1	0	7	6						
2	2	2	1	0	4	0	1	0	7	6	2					
2	2	2	1	0	4	0	1	0	7	6	2	2				
2	2	2	1	0	4	0	1	0	7	6	2	2	6			
2	2	2	1	0	4	0	1	0	7	6	2	2	6	2		

Encoded Number – **222104010762262**

Encoded bit string – **010,010,010,001,000,100, 000,001,000,111,110,010,010,110,010**

For "**010**" – $\mathbf{0_{HH}\ 1_{LH}\ 0_{HL}}$

Figure 3. Proposed insertion method

6.1. New Insertion Method Flow

First, from the output octal number string "101162707060", it needs to search in left side of string properties for any same number. If not found in left side array then also needs to search in Initial Array also and when found out the same number properties then insert the position of it into encoded bit string array. For '1' at position '0' will enter to its array properties of '2'. For '0' at position '1' will enter to '2'. For '1' at position '2' will enter to '2'. For the next '1' at position '3' will enter to '1'. There, if the position string value is greater than '7' set that value to '0' and subtract value '7' from array position property until it becomes less than '8'. So, for '6' at position '4' will go to into process of Position=4+7=11, 11-7=4, thus set '0' and '4' to its array properties. And the rest processes will go as described above.

6.2. Extraction Process

Extraction process will go as follow;

(a) Extract the LSB from each HH, LH, HL.
(b) Transform LSB into octal number.
(c) Convert octal number into hexadecimal format.
(d) Decrypted with Blowfish algorithm.
(e) Find original message.

7. Conclusion

In this paper we presented an improved image steganography technique for any colored image of any size using wavelet transform and blowfish encryption algorithm with the newly developed insertion method is presented. This new method gives better invisibility and security of communication. Our method provides double security by involving blowfish, which satisfies the need of imperceptibility. Future work may be carried out to increase the payload and maintain the higher PSNR values.

8. References

[1] N. Provos, P. Honeyman, “Hide and seek: “An introduction to steganography”, IEEE Security Privacy Magazine (2003), Volume: 1, Issue: 3, Publisher: IEEE Security & Privacy, Pages: 32-44

[2] Johnson, N.F. & Jajodia, S., “Exploring Steganography: Seeing the Unseen”, Computer Journal, February 1998

[3] Almohammad, A.;Ghinea, G.; “Stego image quality and the reliability of PSNR”, 2nd International Conference on Image Processing Theory Tools Applications(IPTA),2010,Pages:215-220

[4] Aamer Nadeem et al, “A Performance Comparison of Data Encryption Algorithms”,IEEE 2005

[5] Wavelet Transform and Denoising: http://scholar.lib.vt.edu/theses/available/etd-12062002-152858/unrestricted/Chapter4.pdf

[6] Amitava Nag, Sushanta Biswas, Debasree Sarker & Partha Pratim Sarkar, “A Novel Technique for Image Steganography Based on DWT and Huffman Encoding”, International Journal of Computer Science and Security, IJCSS, Volume (4): Issue (6)

[7] M. F. Tolba, M. A. Ghonemy, I. A. Taha, and A. S. Khalifa, “Using Integer Wavelet Transforms in Colored Image-Steganography”, IJICIS Vol. 4 No. 2, July 2004

[8] K B Shiva Kumar, K B Raja, Sabyasachi Pattnaik, “Hybrid Domain in LSB Steganography”, IJCA Vol. 19 No.7, April 2011

[9] Po-Yueh Chen* and Hung-Ju Lin, “A DWT Based Approach for Image Steganography”, International Journal of Applied Science and Engineering 2006. 4, 3: 275-290

[10] Saddaf Rubba M. Younus, “Improved Image Steganography Technique for Colored Images using Wavelet Transform”, International Journal of Computer Applications, IJCA, Volume 39 No 14, 2012