International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 2 Issue 5 ǁ May. 2014 ǁ PP.76-81

Implementation of Securing Confidential Data by Migrating Digital Watermarking and Steganography

Ganesh K,SharathYaji
Dept. of Computer Science and EngineeringSIT Mangalore, Karnataka
Asst.ProfessorDept. of Computer Science and EngineeringSIT Mangalore, Karnataka

Abstract - This paper introduces an algorithm of digitalwatermarking based on Discrete Wavelet Transform (DWT) and Steganography Based on Least Significant Bit(LSB). Steganography is a branch of information hiding. According to the characters of human vision, the information of digital watermarking which has been discrete wavelet transformed, is put into the high frequency band of the image which has been wavelet transformed. Then distills the digital watermarking with the help of the original image and the watermarking image. The steganography is the process of concealing one medium of information within another. There are lots of techniques available to achieve steganography like least significant bit insertion method and transform domain technique. This project implements the new method selecting a cover image and applying the watermarking for the copyright protection and embedding the secrete file into the watermarked image providing password with encryption method and sending to other system through the network.

Key words *-LSB, DWT, Steganography, Watermarking*

I. INTRODUCTION

In this modern era, computers and the internet are major Communication media. They connect different parts of the world and have made the world one global virtual world. As a result, people can easily exchange information without distance being a hindrance. However, the safety and security of long-distance communication is an important consideration. The need to solve this problem has led to the development of steganography and watermarking techniques.

Digital watermarking is a new technology of information hiding and it has effective effect for Copyright Protection. Digital watermarking technology is to use the digital embedding method to hide the watermarking information into the digital products of image, visible and video. Seen form the field of signal process, the watermarking signal being embeded into carrier is as a feeble signal to add into a strong background. As long as the intensity of watermarking is lower than the contrast restriction of human visible system (HVS) or the apperceiverestriction of human audio system(HAS), the watermarking signal won't be felt by HVS or HAS[2].

Steganography is a strong security tool that provides a high level of security. But this is particularly when it is combined with encryption. In image steganography image is one of the most popular cover objects. Schemes like LSB insertion and JPEG steganography makes the steganalysis very simple for the opponent. Steganography is about hiding the message so that intermediate persons cannot see the message. Steganography refers to information or a file that has been concealed inside a digital Picture, Video or Audio file. The increasing need of better methods of image steganography has motivated this new concept [1].

II. LEAST SIGNIFICANT BIT SUBSTITUTION

This is the most popular technique when dealing with images. The simplicity of this method is at the cost of compression which is inherently lossy. The traditional LSB technique takes into account every possible bit. 3 bits are safeguarded in every pixel since there is a option to use red, green or blue. The method works by choosing last bit to store the information [3]. The simplest of the LSB steganography techniques is LSB replacement. LSB replacement steganography flips the last bit of each of the data values to reflect the message that needs to be hidden. Consider an 8-bit grayscale bitmap image where each pixel is stored as a byte representing a grayscale value [4]. Suppose the first eight pixels of the original image have the following grayscale values:

11010010
01001010
10010111
10001100
00010101

01010111
00100110
01000011

To hide the letter C whose binary value is 10000011, we would replace the LSBs of these pixels to have the following new grayscale values:

11010011
01001010
10010110
10001100
00010100
01010110
00100111
01000011.

Note that, on average, only half the LSBs need to change. The difference between the cover (i.e. original) image and the stego image will be hardly noticeable to the human eye.

LSB steganography, as described above, replaces the LSBs of data values to match bits of the message. The difference being that the choice of whether to add or subtract one from the cover image pixel is random. This will have the same effect as LSB replacement in terms of not being able to perceive the existence of the hidden message . This Steganographic technique is called LSB matching. Both LSB replacement and LSB matching leave the LSB unchanged if the message bit matches the LSB. When the message bit does not match the LSB, LSB replacement replaces the LSB with the message bit; LSB matching randomly increments or decrements the data value by one. LSB matching is also known as 1 embedding.

In the case of still grayscale images of type bitmap, every pixel is represented using 8 bits, with 11111111 (=255) representing white and 00000000 (=0) representing black. Thus, there are 256 different grayscale shades between black and white which are used in grayscale bitmap images [10]. In LSB steganography, the LSBs of the cover image is to be changed. As the message bit to be substituted in the LSB position of the cover image is either 0 or 1, one can state without any loss of generality that the LSB's of about 50 percent pixel changes.

III. DISCRETE WAVELET TRANSFORM

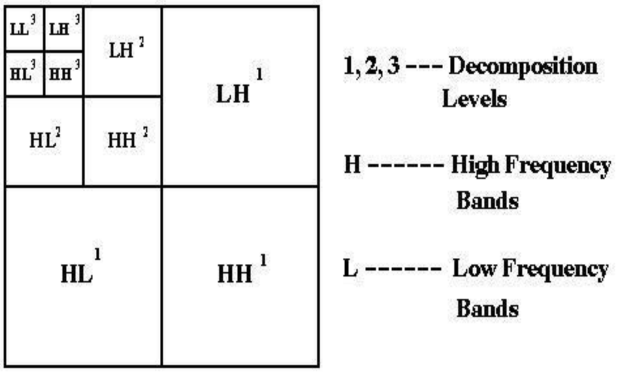

LL3
LH3
HL3
HH3
LH2
HL2
HH2
LH1
HL1
HH1
1, 2, 3 --- Decomposition Levels
H ------ High Frequency Bands
L ------ Low Frequency Bands

Fig.1 Sketch Map of Image DWT Decomposed

Wavelet transform is time domains localized analysis methods with the windows size fixed and form convertible [12]. There is quite good time differentiated rate in high frequency part of signals DWT transformed. Alsothere is quite good frequency differentiated rate in its low frequency part. It can distill the information from signal effectively.

The basic idea of discrete wavelet transform (DWT) in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency district. Then transform the coefficient of sub-image. After the original image has been DWT transformed, it is decomposed into 4 frequency districts which is one low-frequency district(LL) and three high-frequency districts(LH,HL,HH). If the information of low-frequency district is DWT transformed, the sub-level frequency district information will be obtained [5]. A two-dimensional image after three-times DWT decomposed can be shown as Fig.1. Where, L represents low-pass filter, H represents high-pass filter. An original image can be decomposed of frequency districts of HL1, LH1, HH1. The low-frequency district information also can be decomposed into sub-level frequency district information of LL2, HL2, LH2 and HH2. By doing this the original image can be decomposed for n level wavelet transformation [8].

The information of low frequency district is a image close to the original image. Most signal information of original image is in this frequency district. The frequency districts of LH, HL and HH respectively represents the level detail, the upright detail and the diagonal detail of the original image.

According to the character of HVS, human eyes is sensitive to the change of smooth district of image, but not sensitive to the tiny change of edge, profile and streak. Therefore, its hard to conscious that putting the watermarking signal into the big amplitude coefficient of high-frequency band of the image DWT transformed [9]. Then it can carry more watermarking signal and has good concealing effect.

IV. PROPOSED METHOD IMPLEMENTATION

A. Sender Module

The sender module takes the cover image and adds the watermarking to the cover image for authentication purpose. Then sender is selecting a secret data to be hidden inside the watermarked image as the input. It performs the encryption of secret data using a password chosen by sender. By embedding bits in the LSB of noisy pixels it hides this encrypted secret data.

B. Hiding Module

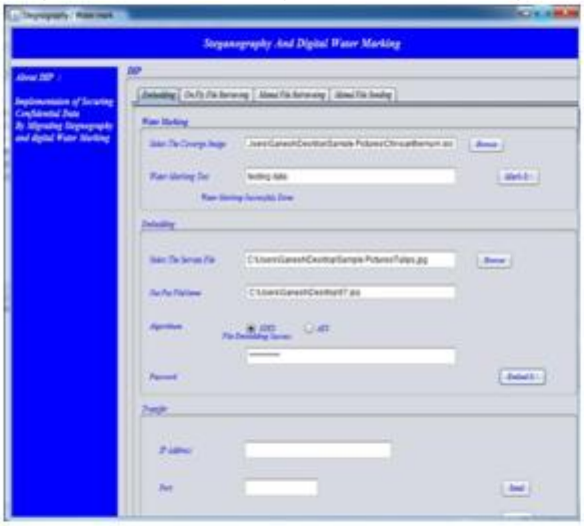
Hiding message is the most crucial module of steganography. It involves covering the message into the cover text. Each pixel typically has three numbers, one each for red, green, and blue intensities. These values often range from 0-255. In order to hide the message, data is first converted into byte format. It is then stored in a byte array. The message is encrypted. Then it is embedded each bit into the LSB position of each pixel[3].

C. Encryption

Encryption includes a message or a file encrypting. Encryption involves converting the message to be hidden into a cipher text. Encryption can be done by passing a secret key. Secret key can be used for encryption of the message to be hidden. It provides security by converting it into a cipher text [3]. This makes it difficult for hackers to decrypt. Greater security is added if the message is password protected. Then while retrieving message, the retriever has to enter the correct password for viewing the message.

AES [6] is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. Triple DES (3DES) uses a key bundle which comprises three DES keys, K_1, K_2 and K_3, each of 56 bits (excluding parity bits) [7].

In this paper using both AES and 3DES. This paper is implemented in java. Here can use any one algorithm to encrypt and same algorithm to use for decrypt the data. Below fig.2 shows the design of the project.



Steganography And Digital Water Marking

About DIP :

Implementation of Securing Confidential Data By Migrating Steganography and digital Water Marking

Water Marking

Water Marking Text: testing data

Embedding

Algorithm: ● 3DES ○ AES

Password: ********

Transfer

IP address:

Port:

Fig.2 Design of the project

D. Receiver Module

The receiver module takes the cover image with the hidden data as the input. The encrypted secret data is then retrieved by applying suitable algorithm. The secret data is obtained by using AES and 3DES decryption algorithm.

E. Retrieve

It involves retrieving the embedded data from the Image. After retrieval the message has to be converted into original message or file. The read data will be in the bytes format. It is essential that the message is in the suitable output file format.

F. Decryption

Decryption involves converting the cipher text into decrypted format. Decryption involves use of a secret key. Itenhances security by converting the cipher text, into the original data message or file. The robustness of the system can be increased further if the data is password protected. Then while retrieving message, the retriever has to enter the correct password and correct decryption algorithm for viewing the data.

V. EXPERIMENTAL RESULTS

A. Watermarking

Select the original image or cover image for watermarking and embedding the secrete file. The Fig.3 shows Desert image as selected as a cover image. The Text entered for watermark is, “Sample testing watermarking”, result of the watermarking shows in fig.4 and there is no distortion in the image.

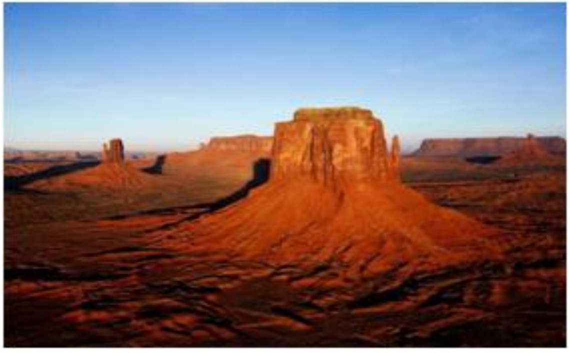


Fig.3 cover image

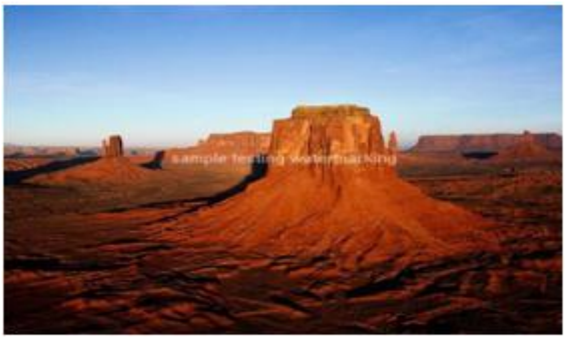


Fig.4 Watermarked image

B. Steganography

Selecting the secrete file or data file for embedding into the watermarked image. The secrete file should be video, image, text file. Figure 4 shows the watermarked image. Fig.5 shows the stego image means secrete file is embedded into the watermarked image and there is no visible difference between the fig.4 and fig.5 images.

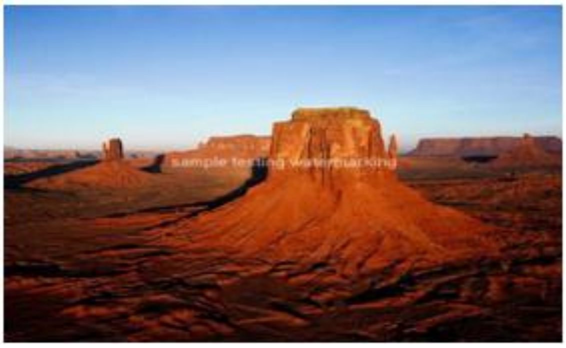
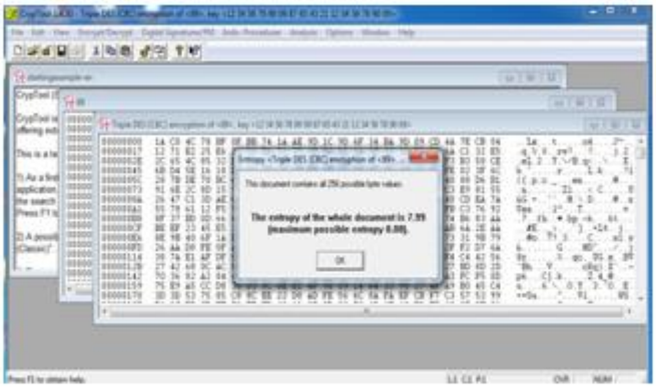


Fig.5 Stego image

C. Encryption methods comparisons

The Triple Des (3DES) encryption algorithm is having a more efficiency than the AES encryption algorithm by using the ,“ True CrypT tool ”, as shown in the below fig.6.



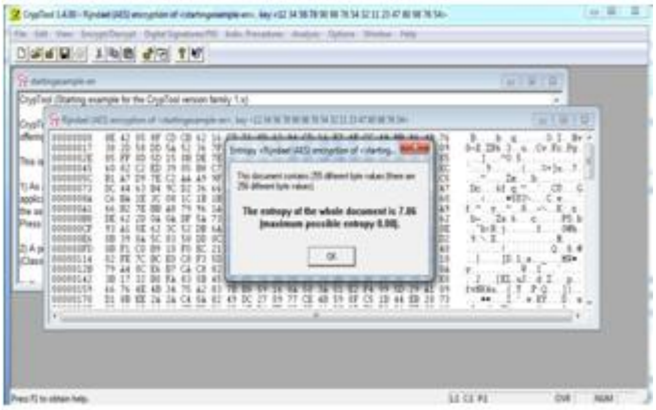
This document contains all 256 possible byte values.

The entropy of the whole document is 7.99 (maximum possible entropy 8.00).

OK

Fig.6 3DES encryption efficiency

The above fig.6 shows the efficiency of 3DES algorithm. This algorithm is giving a more efficient than AES, out of 8.00% 3DES is getting 7.99% efficiency.



This document contains 255 different byte values (there are 256 different byte values).

The entropy of the whole document is 7.86 (maximum possible entropy 8.00).

OK

Fig.7 AES encryption efficiency

The above fig.7 shows the efficiency of AES algorithm. This algorithm is giving a less efficient than 3DES, out of 8.00% AES is getting 7.86% efficiency.

VI. CONCLUSION

This paper introduces a discrete wavelet transform (DWT) for the digital watermark algorithm based on visible watermarking. Watermarking system not only can keep the image quality well, but also can be robust against many common image processing operations of filer and sharp enhancing. This paper also introduces a least significant bit(LSB) algorithm for embedding the secrete file into the watermarked image. Providing the encryption and decryption methods like 3DES and AES for securing the secrete data by the hackers.

REFERENCES

[1] Vijay Kumar Sharma, “A Steganography Algorithm For Hiding Image In Image By Improved LSBSubstitution By Minimize Detection ” ,Journal of Theoretical andApplied Information Technology 15th February 2012.Vol. 36 No.1.

[2] Y. Zhang, “Blind Watermark Algorithm Based on HVS and RBF Neural Network in DWT Domain”, WSEAS Transactions on Computers, Vol. 8, No. 1, 2009, pp. 174- 183.

[3] Usha B A, Dr. N K Srinath, Dr. N K Cauvery, “Data Embedding Technique In Image Steganography Using Neural Network”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 5, May 2013.

[4] Anwar H. Ibrahim, Waleed M. Ibrahim, “Text Hidden in Picture Using Steganography: Algorithms and Implications for Phase Embedding and Extraction Time” , (IJITCS) (ISSN No : 2091-1610) Volume 7 : No : 3 : Issue on January / February, 2013.

[5] Mei Jiansheng, Li Sukang and Tan Xiaomei, “A Digital Watermarking Algorithm Based On DCT and DWT”, International Symposium on Web Information Systems and Applications (WISA09) Nanchang, P. R. China, May 22-24, 2009, pp. 104-107.

[6] Fei Shao, Nanjing, Zinan Chang, Yi Zhang, “AES Encryption Algorithm Based on the High Performance Computing of GPU” , Second International Conference on Communication Software and Networks, 2010.

[7] Thomas J. Watson Research Center, P. O. Box 218, Yorktown Heights, New York 10598, USA, “Data Encryption Standard its strength against attacks” ,IBM journal of research and development ,May 1994.

[8] Y. Zhang, “Blind Watermark Algorithm Based on HVS and RBF Neural Network in DWT Domain” , WSEAS Transactions on Computers, Vol. 8, No. 1, 2009.

[9] A. Salama, R. Atta, R. Rizk and F. Wanes, “ A Robust Digital Image Watermarking Technique Based on Wave-let Transform ” , IEEE International Conference on System Engineering and Technology, Shah Alam, June 2011.

[10] Mandal, J.K. and Sengupta, M., Steganographic Technique Based on Minimum Deviation of Fidelity (STMDF), Proceedings of Second International Conference on Emerging Applications of Information Technology, IEEE Conference Publications,2011.

[11] GuorongXuan, Yun Q. Shi, Chengyun Yang1, YizhanZheng, DekunZou and Peiqi Chai, Lossless Data Hiding Using Integer Wavelet Transform and Threshold Embedding Technique, in 2005.

[12] MadhumitaSengupta and J. K. Mandal, “Self Authentication of color image through Wavelet Transformation Technique (SAWT)” , Proceedings of ICCS 2010, November 19, 2010 November 20, 2010.

[13] Arvind Kumar and Km. Pooja, “ Steganography A Data Hiding Technique” , International Journal of Computer Applications ISSN 0975 8887, Volume No.7, November2010.