Current Trends in Technology and Science
ISSN : 2279-0535
8thSASTech 2014 Symposium on Advances in Science & Technology-Commission-IV Mashhad, Iran

New Method of DWT-based Image Steganography by using Fuzzy Logic

Saeede Goodini
Student, Islamic Azad University, Science And Research Branch,
Sirjan, Iran, Email ID : my_red_ir@ yahoo.com

Mahdi Jafari Shahbazzadeh
Assistant Professor, Organization : Assistant Professor of University,
Email ID : m_j_shahbazi@yahoo.com

***Abstract* — In this paper, a new image steganography method is presented by using a Fuzzy Logic algorithm, which involves two inputs and one output in the field of the wavelet transform, thereof the message bits of an image become hidden in wavelet transform coefficients from the image edges via Fuzzy Logic. Also, it is confirmed that this method is a non-blind method in the wavelet transform frequency domain to assess SNR, MSE, and Similarity Criteria with highly acceptable transparency, defiance, and data rate as its implementation is easy. If the recovery time length is less important, this algorithm can be combined with the encryption algorithms and enhance the system security.**

***Keyword* — Cryptography, Fuzzy Logic, Steganography, Wavelet Transform (DWT).**

1. INTRODUCTION

The present era is called the information and communication era. Generally, the biggest characteristic of this era is the widespread faster information exchange of the communication means of and consequently the communication equipments could be misused for unauthorized access to the others' information. In essence, one of the information characteristics (digital) is that data duplication and copy is very easy, so that it possibly could annihilate the book, movie and music, and software industry. Therefore, this is one of the most important problems in this industry's development. In fact, unlimited number of illegal texts and audio or video data proliferation needs the study approaches to embed copyright information and serial numbers on data.

In order to solve this problem, two scientific disciplines are developed: cryptography and steganography.

Philosophy of steganography is that the message becomes hidden in a way that no one could observe its presence, while the cryptography aims to change the message in a way that is incomprehensible for others and it does not matter if someone notices.

Steganography techniques are used to hide the message by the other symbols intangibility. By these techniques, the data are kept away from unauthorized recipients. Information is hidden without any damage to the signs. Message carriers can have image, video, audio, text or else. The principle of encryption is the use of the spaces of the information carriers which does not damage the carrier's identity. With a little care we can realize that the highest possible to hiding is image hiding because there is much bandwidth for image transfer and therefore gives us more space for hiding.

The basic steganography features include keeping the host transparency and the defiance of the system against attacks at the amount of the hidden information in the system.

Steganography depends on the application as divided into different categories, i.e. watermarking and steganography, while two general methods are implemented on the time domain and transform domain.

Spatial domain contains algorithms for the message bits that are inserted into the host bits accurately. For example, the image is used as the host in LSB technique as one of the simplest techniques, in which the message bits are inserted into the least valuable bits in each pixel. Spatial domain methods, despite having many advantages, i.e. implementation simplicity, high implementation rate, acceptable resolution, and there are some disadvantages too. The main defect of these methods is their low defiance against image processing, i.e. cutting, noise, image format change, or image rotation. In regard of the mentioned issue, it is necessary to find approaches to increase the image defiance by means of hidden information. The best solution to this problem is hiding the information within the higher image frequency layers instead of the spatial domains. Therefore, the encryption methods in the transform domain are created and developed. The generally used transforms in this domain are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT).

In this paper, the video message is hidden into the wavelet edge coefficients of the host image. Many steganography algorithms are used to analyze sound or image files and find the ideal areas to find the information. If the image coefficients on level and certain area would have the least slight change, as these areas are strip or noised. Wavelet transform is a high-quality tool to identify the favourable areas, because this transform breaks image recursion to obtain an appropriate model.

In this transform model, the level and certain areas are modelled at high volumes, while they contain noise and the detail parts are analyzed in multiple times. The natural solution is using steganography (hidden information)

coefficients that model very small and slightly areas. This boundary changes corners of an image or crossing points of a sound file that it is difficult for humans to detect these changes.

The recent researches on the human eye vision indicate that the human retina divides images into the multiple frequency channels as each channel has a particular bandwidth that is approximately one octave and the signals for each of these channels are processed in the brain separately. In the wavelet transform, an image is divided into the frequency bands with logarithmic scale, which are approximately equal. As a result, the changes in the wavelet transform domain are less detectable to the human eye.

In these two dimensional wavelet transforms, the image with X, Y dimensions is divided into four regions: LL, LH, HL, HH, where LL is a region with X/2 and Y/2 dimensions. Afterwards, LL is divided into four regions with X/4 and Y/4 dimensions: LL1, LH1, HL1, and HH1. Then LL1 is divided into four regions and this process continues until the desired outcome. The wavelet transform in (n) decomposition level of this process occurs n times. Finally LLn region will result X/2n and Y/2n dimensions. Therefore, at the wavelet transform domain (DWT), the image is transformed like a pyramid structure as shown in Fig. 1.

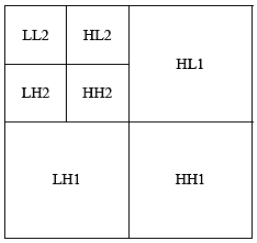

Fig. 1. Image pyramid structure on wavelet transforms

2. Proposed Algorithm

In this paper, a method is proposed to hide data in images that in during it, the message data are hidden in coefficients of wavelet transform of host image using fuzzy logic. The proposed algorithm is as follows:

2.1. Encryption process

The steganography includes the following stages

1) Each pixel of the message image is divided to four couplet parts.
2) The wavelet transform of the host image is taken.
3) The fuzzy algorithm consists of two inputs as the first input has 8 member functions [0 7] and the second input has 4 member functions [0 3] and one output that has 8 member functions [0 7] as shown in Fig. 2.
4) Output matrix is determined based on selecting the wavelet transform coefficients of the host image as the first input and the spread bits of the message image as the second input.
5) The inverse wavelet transform is taken from the final result and thus the host image with the message image is obtained.

The steganography process is shown in Fig. 3.

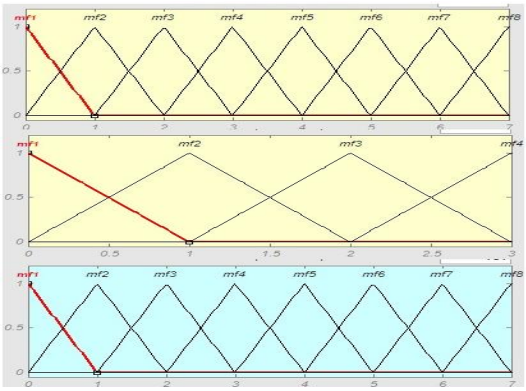

Fig. 2. Inputs and output member function on steganography algorithm

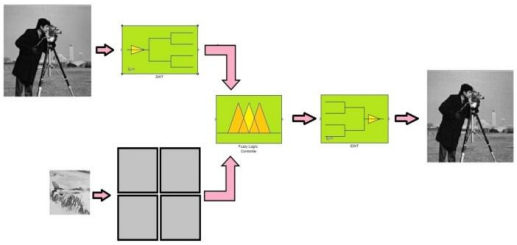

Fig. 3. Steganography process of message image

2.2. Detection Process

The following data objects are needed to detect the message:

1. The main image, 2. The message carrier image

The message detection phases are as following:

1) A fuzzy algorithm consists of two inputs that the first input has 27 member functions [0 255] and the second input has 56 member functions [0_255] and one output that has 4 member functions [0 3] is defined in Fig. 4.
2) The wavelet transform of the main image is taken.
3) The wavelet transform is taken from the message carrying image.
4) The output is obtained based on the wavelet transform coefficients selection of the host image as the first input and the wavelet transform coefficients of the message carrying image as the second input..
5) The integration of the four binary bit parts of the output matrix restores one byte of the message.

Detection processes are shown in Fig. 5.

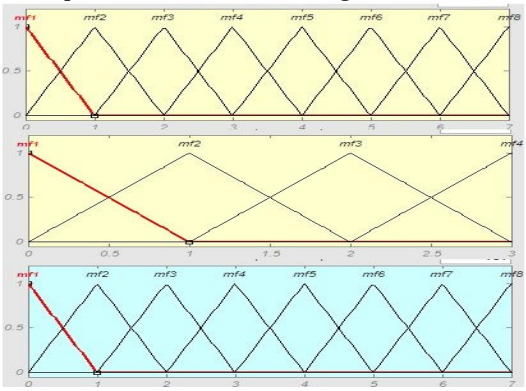

Fig. 4. Inputs and output member functions of detection algorithm

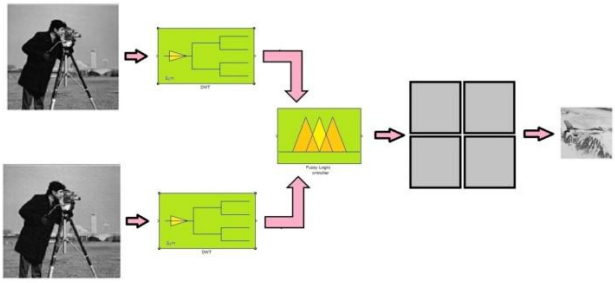

Fig. 5. Restoration phases of message image

3. TEST RESULTS

The study uses the photographer's image (512*512 bits) as the host image and the image (256*256 bits) as the message image by this method.

Fig. 6 shows the main image, the message image, the message carrying image, and the restored message carrying image by using this method.

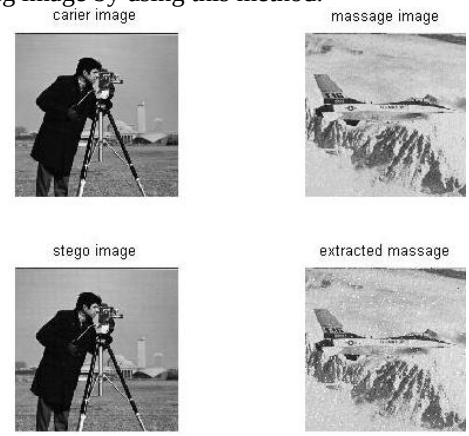

Fig. 6. Main image, message image, message carrying image (steganography image) and restored message carrying image

The histogram of the main image and the message carrying image are shown in Fig. 7.

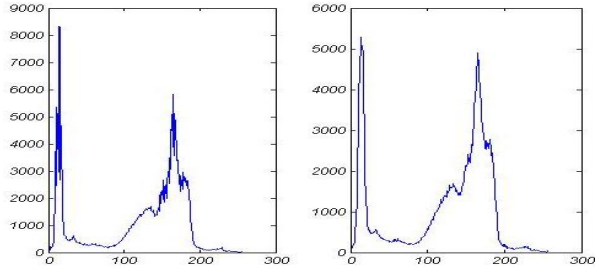

Fig. 7. Histogram of main image and steganography image

2.2. Evaluation

The following evaluation criteria are used to evaluate the proposed method.

Signal-To-Noise Ratio (SNR):

SNR is used to measure the image quality and it represents the transparency level of the steganography system. SNR is obtained among two 8 bits per pixel images based on dB with the following equation:

$$SNR = 10 \times 10 \log_{10} \frac{\sum_{m,n} x^2(m,n)}{\sum_{m,n} (y(m,n) - x(m,n))^2} \quad (1)$$

Where $x(m,n)$ represents the values of the main image pixels and $y(m,n)$ represents the values of the message carrying image. If SNR is more or equal to 40, the difference of the main and the restored images are almost undistinguishable by the human eye.

Similarity coefficient:

The similarity between the main and restored images is defined in following equation:

$$K = \frac{\sum_m \sum_n s(m,n)\hat{s}(m,n)}{\sum_m \sum_n s^2(m,n)} \quad (2)$$

Where $s(m,n)$ represents the values of main message image and $\hat{s}(m,n)$ represents the values of the restored message image.

Mean square differences (MSE) of brightness:

MSE of brightness is used to the measure image quality and it represents the transparency level of the steganography system. MSE of brightness between the two 8 bits per pixel images is obtained based on dB with the following equation,

$$MSE = \frac{\sum_{m,n} (x(m,n) - y(m,n))^2}{N_1 \times N_2} \quad (3)$$

Whereas $x(m,n)$ represents the values of the main image pixels and $y(m,n)$ represents the values of the message carrying image and N1 and N2 are the dimensions of the images.

The evaluation results of this method are based on the triple characteristics of system as following:

Transparency: In this method, the transparency of the message carrying image is measured by the criteria of MSE and SNR and based on test results of the images, as SNR is equal to 34.12 and MSE is equal to 0.00038, while these values indicate very fine transparency in this system.

Data rate: In this method, the data rate is equal to one quarter of the message carrying image, since the wavelet transform of two bits information is encrypted in each coefficient.

Defiance: This method has high resistance in contrast of the histogram analysis. Also this method has less divergence and vulnerability in the spatial domain methods compared to the image processing techniques. In

order to measure this topic the salt and pepper noise was added to the message carrying image as it is observed that the similarity value of the main image and restored image degraded from 0.9916 to 0.9597, respectively.
The noise effect on the message carrying image and the restored image is shown in Fig. 8.

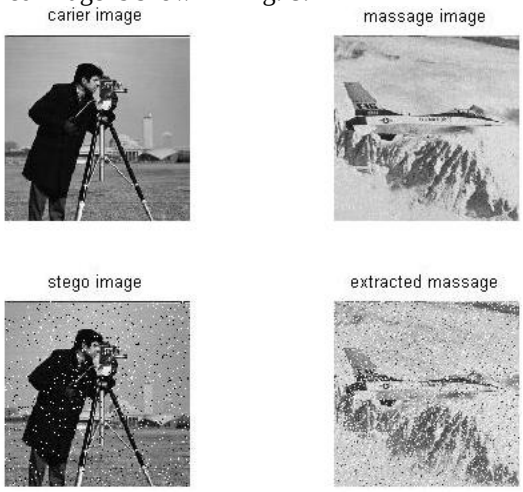

Fig. 8. Noise effect on message carrying image and restored message image

4. RESULTS

The results of implementing this method are as following:

Advantages:

- This method has high hidden data rate, so that several LSB bits can be applied, although the image similarity reduces by the increased number of bits.
- In this method, the similarity of the main image and the message carrying image is high.
- In this method, the similarity of the main image and the restored image is proper.

In this paper, the non-blind watermarking method is presented in the frequency domain of the wavelet transform. The results of the implementation indicate that this method has high and acceptable data rate and high transparency and defiance, meanwhile its implementation is easy as well. If the recovery time is less important, this algorithm can be combined with the encryption algorithms to enhance the system security.

REFERENCES

[1] Sarreshtedari- S. and Ghaemmaghami- S., "Hih Capacity Image Steganography in Wavelet Domain", IEEE, 2010.
[2] C.Gonzales, "Digital Image Processing Using Matlab", Pearson Prentice Hall, 2004.
[3] Wayner- Peter, "Disappearing Cryptography: Information On Hiding: Steganography And Watermarking", Second Edition, 2002.
[4] Mertinz- Alfered, Moradi- Mohammad Hassan, "Wavelet Signal Analysis, Filterbank, Time-Frequency Transformations and Their Applications", First Edition, 2002.
[5] Shin- Hi Tae, "Steganography And Steg-analysis", Multimedia Security Systems, Spring, 2006.
[6] Soheily, Mohammadreza, "Steganography of Recurring Patterns Using Wavelet Transform", The 3rd conf. on Information and Knowledge Technology, Ferdowsi University, Mashhad, Iran, 2007.
[7] Amiri Taze Kand- Hosein, "Provide a New Method for Watermarking in Images Using Wavelet Transform Coefficients of Border of Image", The 2nd Int. Conf. on Communications and Information Technology, Islamic Azad University, Malayer, Iran, 2011.
[8] Sabetiyan, Mohammad, "Evaluation of Methods of Hiding Information in Audio and Implementations of Several Methods", Imam Hosein University, Tehran, Iran, 2004.
[9] Chen*- Po-Yueh and Lin- Hung-Ju, "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering, p: 275-290, 2006.
[10] D.Dickman- Shawn, "An Overview Of Steganography", James Madison University Infosec Techreport, Department of Computer Science, July 2007.
[11] G.Bors- Adrian, "3-D Digital Watermarking", University Of York Computer science Department, 2007.
[12] Yang- Bo and Deng- Beixing, "Steganography In Gray Images Using Wavelet", Department of Electronic Engineering, Tsinghua University, Beijing, China, 2005.
[13] Cachin- Christian, February 17, "Digital Steganography", IBM Res, 2005.

AUTHOR'S PROFILE

Saeede Goodini
I am studying in master of communication engineering at Islamic Azad University, Science And Research Branch, Sirjan. I am at the first place in university.