Multipurpose Information Hiding Techniques in an Image

Rashmi[1], Sowmya[2], Nagaraja N S[3]
[1,2] *Assistant professor, Dept of ECE, Srinivas School of Engineering, Mukka*
[3] *Head of the Department, Dept of ECE, Srinivas School of Engineering ,Mukka*

Abstract- **Data hiding is a method of hiding secret messages into a cover-media such that an unintended observer will not be aware of the existence of the hidden messages. In this paper, 8-bit gray scale images are selected as the cove media. These images are called cover-images. Cover-images with the secret messages embedded in them are called stego images. For data hiding methods, the image quality refers to the quality of the stego-images. This project provides a hardware solution for information hiding in 8-bit gray scale image using Least Significant Image. Steganography technique followed by Image compression using Discrete Wavelet Transform. In this a data hiding method by LSB substitution process is proposed. The image quality of the stego-image can be greatly improved with low extra computational complexity.**

1. INTRODUCTION

In the digitized world extensive increase of use of extensive data communication the problem of security, authentication of the multimedia data also increases. The solution to this is digital watermarking. Digital watermarking is the process of the modification of original multimedia data to embed a data containing key information such as authentication or copyright codes. The embedded data must leave original data unchanged. Steganography is an art of hiding information in a way that apart from an intended recipient, suspects the existence of secret message. To hide a secret message within an object, Do it such a way that the presence of message is not visible.

Steganography is the advanced method for hiding secret information than any other methods used so far. The major advantage of steganography over other methods is that by this method, even the existence of hidden secret message will not be observed at all, where as in other methods, one may observe the hidden secret message.

Steganography is a system that hides information in an application cover carrier like image, text, audio, and video. Considerable amount of work has been carried out by different researchers on this subject. Least Significant Bit (LSB) insertion method was more suspicious and low robustness against attacks. The objectives of this study were to analyze various existing system and implement a dynamic substitution based Image Steganography (IS) with a secret key. Proposed method is more difficult to attack because of message bits are not inserted in to the fixed position. In our method, the message bits are embedded into deeper layer depending on the environment of the host image and a secret key resulting increased robustness. The robustness specially would be increased against those intentional attacks which try to reveal the hidden message. It is the study of techniques for hiding the existence of a secondary message in the presence of a primary message.

2. INFORMATION HIDING TECHNOLOGY

With the rapid development of computer technology, information security is facing increasingly tough challenges, the traditional theory of encrypting the secret file into cipher text made the illegal interceptor not be able to obtain confidential information from which to achieve the purpose of secrecy, but that is a fatal flaw because it clearly prompted which is the important information easily leading to the attacker's attention and the possibility of being cracked. Also, the attacker can decode the information in case of failure damage, resulting in legitimate recipient cannot receive information. Especially now that the rapid development of hardware technology and especially achieving maturation of force based on parallel computing power at the networks, the security of the traditional encryption algorithm met with a great shock. Multimedia technology and networks have been rapidly developing and the applications of digital media on the Internet has come

to be an explosive growth, more and more digital products are spreading by way of electronic communication on the Internet. The original digital information can be unlimitedly copied modified, edited, and spread with digital signal processing and network transmission technology, which have made it a more increasingly outstanding problem with intellectual property protection and information security. Therefore, knowledge of how to prevent illegal copying and dissemination of products is also the current need to address the new problems. Since these new problems cannot be solved with the traditional information security technology, information hiding technology is arising in this situation as a new information security technology. Information hiding is not only a new technology, but also the forefront of multimedia technology and network technology research, which appears a very broad prospect in application.

3. METHEDOLOGY

In this project here there are two methodologies are used to hide the data inside the image, using LSB & DWT.

Cover-Image: An image in which the secret information is going to be hidden. The term "cover" is used to describe the original, innocent message, data, audio, still, video etc. The cover image is sometimes called as the "host".

Stego-Image: The medium in which the information is hidden. The "stego" data is the data containing both the cover image and the "embedded" information. Logically, the processing of hiding the secret information in the cover image is known as embedding.

Stego key: This is the key used as a password to encrypt and decrypt the cover and stego respectively in order to extract the hidden message. Secret key is optional.

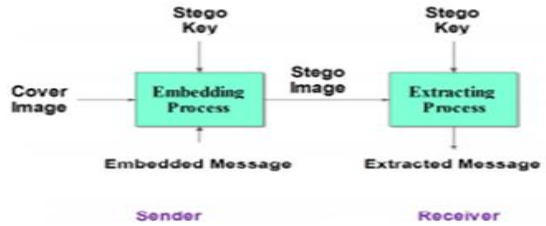

Figure 6. General block diagram of Steganography.

3.1Image Embedding Process

3.1.1 Least Significant Bit Insertion (LSB)

Characters in the ASCII code can be represented using 8 bits. The value of discrete coefficients can be manipulated slightly without being noticed by visual inspection after the image is reconstructed using the manipulated lifting coefficients. This research project is based on the premise that the bits of ASCII 6 characters can be included in lifting coefficients without resulting in a visible appearance. The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels.

3.1.2Process of Adding a Message:

The process of adding a message to the pixels of an image is a multi-step process. In brief, an ASCII character stream is split into two-bit pairs, a lifting scheme is applied to an image, the two-bit pairs is inserted into the image in either the trends or details in the lifting domain, and then the inverse lifting process is applied to reconstruct the image. The channels of the image pixels are split into separate arrays upon initialization. There is one array for each color channel. Then it calculates the entropy and retrieves the text that has been entered by user.

3.1.3Encoding the Message in the Image:

The program then splits the ASCII character stream into 4 two-bit pairs per character. The two-bit pairs are created because the 2 LSBs of a pixel will be replaced with these two-bit pairs. Since all the characters in the English alphabet are within the lower 127 ASCII characters, only 4 two-bit pairs are needed to represent each character. These two-bit pairs are stored in an array for later manipulation. The lifting scheme is then applied to the image down to the level specified by the user. Since the image is split into three color channels, the discrete scheme must be applied three times, once for each color channel. The program automatically adjusts the encoding according to the discrete decomposition level.

Once the transformations are complete, the two bit pairs of the ASCII characters are then hidden in the pixels of the processed image. The text offset value of the color channel specified by the user determines which bits are used to hide each subsequent two-bit pair of the ASCII character. Hiding the two-bit pair in the image is accomplished by overwriting the two

selected bits of a pixel with the value of the two-bit pair. This is done by performing a bitwise AND operation with 0 and the two bits of the pixel, which effectively sets the two bits to 0. Then the two-bit pair to be hidden in this pixel is then combined with the pixel by a bitwise OR operator, effectively setting these pixel bits to the message bits.

3.1.4 Decoding a Message from the Image:

Decoding a message that is inserted into an image requires fewer steps than to encode. The process flow starts out the same way as encoding with the user selecting the parameters that were used to encode the message. At this point the program splits the image into its color channels and applies the inverse discrete scheme to each channel to the level specified by the user. When the discrete transformation is completed, the program retrieves the message out of the pixels of the cover image.

3.2 Data Hiding Using LSB.

Data hiding using LSB it is best way to implement steganography. It embeds the data into the cover so that it cannot be detected by a observer. The technique works by replacing some of the information in a given pixel with information from the data in the image. While it is possible to embed data into an image on any bit-plane in a LSB embedding, we lose some information from the cover image. [it is not visible]. Both lossy & lossless image can be used.

Data hiding using LSB it is best way to implement steganography. It embeds the data into the cover so that it cannot be detected by a observer. The technique works by replacing some of the information in a given pixel with information from the data in the image. While it is possible to embed data into an image on any bit-plane in a LSB embedding, we lose some information from the cover image. [it is not visible]. Both lossy & lossless image can be used.

The LSB is the lowest significant bit in the byte value of the image pixel. The LSB based image steganography embeds the secret in the least significant bits of pixel values of the cover image (CVR). To illustrate LSB technique, we provide the following example. Suppose the CVR has the following two pixel values:

(0000 1010 0011 0010 0111 0100)
(1111 0101 1100 0011 1100 0111)

Also, assume that the secret bits are: 101101.

After embedding the secret bits, the result pixel values are:

(0000 1011 0011 0010 0111 0101)
(1111 0101 1100 0010 1100 0111)

The underlined bits indicate that the bits were changed from their original value. Only three bits in the cover image were modified. On average about half of the bits in the cover image will be modified when embedding the secret image. The above LSB method limits the size of the secret data to eighth of the size of the CVR.

3.4 Data hiding using DWT

Data hiding using DWT Wavelet transform decomposes a signal into a set of basis functions. These basis functions are called wavelets DWT transforms a discrete time signal to a discrete wavelet representation. In this process image pixel values are divided into even & odd sample, as shown in following

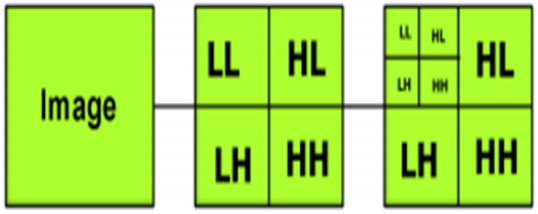

Figure 6.2 Decomposition of Image using DWT

Discrete Wavelet Transform based steganography approach was proposed by Ahmed A. Abdelwahab et al. In this approach, the cover image is decomposed into four sub-images such as approximation coefficients (CA), horizontal detail coefficients (CH), vertical detail coefficients (CV) and diagonal detail coefficients (CD). Similarly, the secret image is decomposed into four sub-images. These sub-images are divided into non-overlapping blocks. The blocks of approximation coefficients of cover image are subtracted from approximation coefficient of secret image. The differences of these coefficients are called error blocks. The replacement of an error block is being done with the best matched CH block. Besides using CH block, we have done experimentation using CV and CD blocks also to see the effect on PSNR of the stegano image using the algorithm as proposed by

Ahmed A. Abdelwahab et al. The experimental work includes six different attacks.

3.5 Algorithm

The algorithm to hide the data inside the image using DWT along with LSB technique is given below:

1. Select the secrete data [or Message].
2. Convert the secrete data from decimal to binary.
3. Read a cover image.
4. Resize the cover image by 256 x 256.
5. Convert the cover image from RBG to gray.
6. Read the Gray level image [Cover image].
7. Create the header file.
8. Break the byte of secrete data to be hidden into bits.
9. Take first 8 bytes of original data from cover Image.
10. Replace the least significant bit by one bit of the data to be hidden.
11. Display new pixel valued image [Stego Image] on VB [Using LSB].
12. Display new pixel valued image [Stego Image] on VB [Using DWT].
13. Display extracted data using Hyper Terminal Window.
14. Display the value of MSE & PSNR using Hyper Terminal window.

4. RESULTS

4.1 Results of steganography

In this project LSB and DWT steganography methodologies are used. After embedding the secret message inside an image, the results of both the methodologies are shown below.

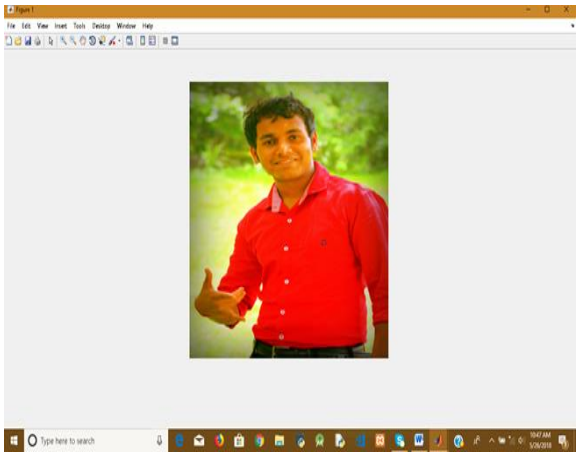

Figure 7.1 Result of LSB Steganography

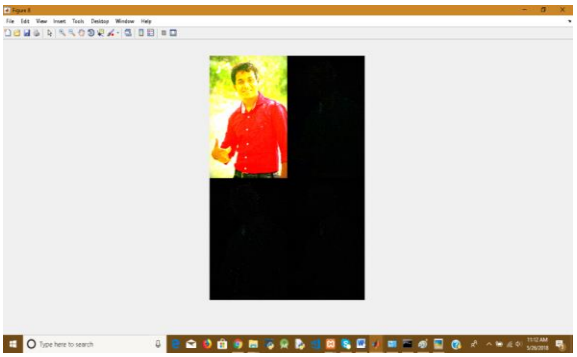

Figure 7.2 Result of DWT Steganography

4.2 Analysis of LSB and DWT Steganography

During the analysis of DWT steganography and LSB steganography, the algorithm for LSB method is simple than the DWT method. In LSB method the clarity and the quality of the image will be more compare to DWT method, because in LSB method the process is to replace only the LSB value of pixel by secret information. The time delay taken by the LSB algorithm is less than the DWT algorithm.

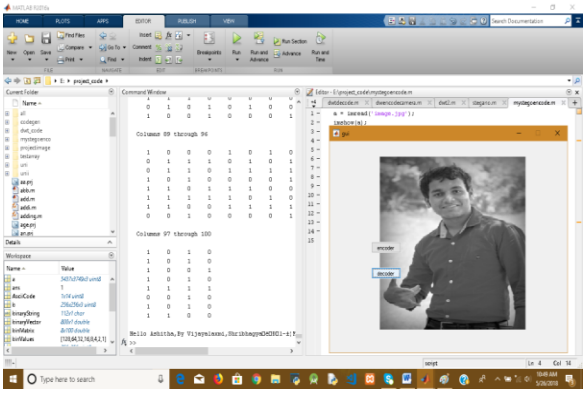

Figure 7.3 Encoder Decoder panel of GUI

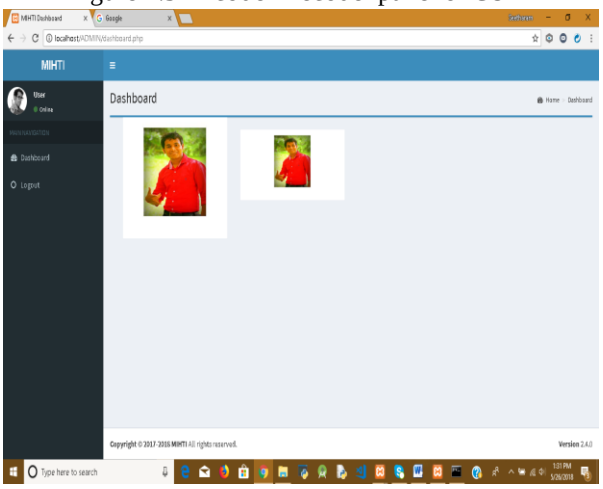

Figure 7.4 Dash Board

5. ADVANTAGES

1. Saving memory

Embedding the information in the corresponding image saves memory required for storing the complete information.

2. Avoid detachment

Embedding the information in an image is lead to avoid detachment risk and misplacing of the records.

3. Confidentiality and security

Through this technique, confidentiality and security of data can be resolved by using advanced encryption techniques along with the imperceptibility and dependency on key.

4. Controlling integrity

This can be very well resolve the integrity issues through fragile watermark as well as can evaluate the extent to which image is tampered and also the modified regions.

5. Authentication and captioning

This can be combined with cryptography techniques to resolve authentication issues. Some small captions as watermarks provides extra beneficial information.

6. CONCLUSION

This project provides a hardware solution for information hiding in 8-bit gray scale image using Least Significant Image. Steganography technique followed by Image compression using Discrete Wavelet Transform. “You never know if a message is hidden”, this is the dilemma that empowers steganography. As more emphasis is placed on the areas of copyright protection & privacy protection. We believe that steganography will continue to grow in importance as a protection mechanism. Steganography can be used along with cryptography to make an highly secure data high way.

In this a data hiding method by LSB substitution process is proposed. The image quality of the stego-image can be greatly improved with low extra computational complexity. Experimental result shows the effectiveness of the proposed method. In the proposed algorithm, the number of steps are very less. Thus, the computational complexity is reduced, so it is easy to be implementing in both grayscale and color image. Benefited from the effective optimization, a good balance between the security and the image quality is achieved.

During the analysis of DWT steganography and LSB steganography, the algorithm for LSB method is simple than the DWT method. In LSB method the clarity and the quality of the image will be more compare to DWT method, because in LSB method the process is to replace only the LSB value of pixel by secret information.The time delay taken by the LSB algorithm is less than the DWT algorithm.

REFFERENCE

[1] Ravi Kumar, Kavita Choudhary, Nishant Dubey, “An Introduction of Image Steganographic Techniques and Comparison”, International Journal of Electronics and Computer Science Engineering.

[2] Prashanti .G, Sandhya Rani.K, Deepthi.S “ LSB and MSB Based Steganography for Embedding Modified DES Encrypted Text”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 8, August 2013, pp.788-799.

[3] Namita Tiwari, Dr.Madhu Shandilya, ”Evaluation of Various LSB based Methods of Image Steganography on GIF File Format”, International Journal of Computer Applications, Vol. 6– No.2, September 2010 , pp .1-4.

[4] Mr. Rohit Garg, “Comparison Of Lsb & Msb Based Steganography In Gray-Scale Images Vol.1, Issue 8, Oct 2012”, International Journal of Engineering Research and Technology (IJERT).

[5] MamtaJuneja, Parvinder S.Sandhu, and Ekta Walia,”Application of LSB Based Steganographic Technique for 8-bit Color Images”, World Academy of Science, Engineering and Technology, 2009.

[6] Shailender Gupta, Ankur Goyal, Bharat Bhushan, ”Information Hiding Using Least Significant Bit, Steganography and Cryptography”, I.J. Modern Education and Computer Science 2012, Vol .6 pp. 27- 34

[7] M.Sivaram B.DurgaDevi J. Anne Steffi, “Steganography of two lsb bits”, International Journal of Communications and Engineering, Vol.1– No.1, Issue: 01, March 2012.