HAAR WAVELET DOMAIN ANALYSIS OF IMAGE STEGANOGRAPHY

Vikas pratap singh, Prof. Shrikant lade
Dept. Of Information and technology Dept. of Information and technology
RKDF 1ST , Bhopal, India RKDF 1ST ,Bhopal,India

***Abstract*—- The Internet and multimedia techniques, digital data such as texts, images, videos, and audios now have been widely used in our daily life. The security of the computer networks is insufficient, and the transmitted data could be intercepted or grabbed by an illegal user. Therefore, how to ensure the digital data to be securely transmitted via the Internet is an important issue. In this research paper we propose a new frequency domain method for image steganography. The merit is to increase image quality by hiding the messages in HL, LH, and HH sub-bands while keeping LL sub-band invariant. The advantage of this is that the original cover image does not have to be present on the receiver side. Therefore, the risk of disclosure of secret communication is lower and easily finds the patterns of artificial changes by comparing the original and stego object and provides the higher security then other because after embedded the secret data the cover image is encrypted using 32 bit key. we find the proposed algorithm support high capacity rate reach up to ¾ bits per pixel and that is form above 75% from the size of the input image cover file at SNR above 57 dB for the output signal. The proposed algorithm was implemented by using Matlab (2009a) programming. The proposed algorithm was tested using five cover image files: Airplane, Lena, Baboon, Papper and Girl. Each image has resolution of 8 bits per pixel and diamention is 256*256 pixel and text file is used in tests as secret messages. The quality of output signal in each test was computed using SNR and Time Complexity.**

***Index Terms*— Steganography, Haar-DWT transform.** *(key words)*

I. Introduction

Information hiding is the process of hiding the details of an object or function.

In addition, information hiding effectively decouples the calling code from the internal workings of the object or function being called, which makes it possible to change the hidden portions without having to also change the calling code. Encapsulation is a common technique programmers use to implement information hiding. The rising possibilities of modem communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the Internet increases. Therefore, the confidentiality and data integrity are required to protect against unauthorized access. This has resulted in an explosive growth of the field of information hiding. Information hiding techniques are receiving much attention today. The main motivation for this is largely due to fear of encryption services getting illegal, and copyright owners who want to track confidential and intellectual property copyright against unauthorized access and use in digital materials such as music, film, book and software through the use of digital watermarks. Advance security is not maintained by the password protection but it is gained by hiding the existence of the data which can only be done by Steganography. Steganography is “data hiding”technique, In the modern day sense of the word usually refers to information or a file that has been concealed inside a digital Picture Video or Audio file. This is derived from the lizard “Stegosaurs” covered or secret and graphy meaning writing or drawing. Therefore steganography literally means covered writing. It simply takes one piece of information and hides it within another. It is not intended to replace cryptography but supplement it. Hiding a message with Steganography methods reduces the chance of a message being detected. This hidden information can be plain text, cipher text, or even images. Steganography is mainly oriented around the undetectable transmission of one form of information within another. The steganography algorithms were primarily developed for digital images and video sequence, interest and research in audio steganography started if an attacker knows the embedding method. Steganography works by replacing bits of useless or unused data in regular computer. Any steganography technique has to satisfy two basic requirements. The first requirement is perceptual transparency, i.e. cover object (object not containing any additional data) and stego object (object containing secret message) must be perceptually unclear. The second constraint is high data rate of the embedded data. images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist specific. For these different image file formats, different steganographic algorithms exist. To hide information, straight message insertion may encode every bit of information in the image or selectively embed the message in “noisy” areas that draw less attention those areas where there is a great deal of natural color variation. The message may also be scattered randomly throughout the image. A number of ways exist to hide information in digital media. Common approaches include as vast channels for communication such as the Internet are becoming popular, the security of digital media becomes a greater concern. The hiding of a message will reduce the probability of detecting this message. This method hides a gray image in one another. The cover is divided into blocks of equal sizes. Each block size equals the size of the embedding image Compare each pixel in embedding image with all the corresponding pixels in the blocks of the cover image (assume there are C blocks).i.e. pixel (i,j) in the embedding image is compared with the pixel (i,j) in all C blocks of cover image. Select the best pixel to be embedding in. Best pixel is the pixel that gives minimum difference between it and the pixel to embed. For Example, if pixel (i,j) to embed has a value 250, and corresponding pixels values are: 248, 230, 249, 252, 255, 260, 270, and 262 (assume cover is divided into 8 blocks). Then the pixel with value 249 will be selected to embed 250. Wavelet based steganography is a new idea in the application of wavelets. However, the standard technique of storing in the least significant bits (LSB) of a pixel still applies. The only difference is that the information is stored in the wavelet coefficients of an image, instead of changing bits of the actual pixels. The idea is that storing in the least important coefficients of each 4 x 4 Haar transformed block will not perceptually degrade the image. While this thought process is inherent in most steganographic techniques, the difference here is that by storing information in the wavelet coefficients, the change in the intensities in images will be imperceptible.

II. History Of Work

To keep secret messages over the Internet secure, data encryption and information hiding are two possible solutions [1][2]. The confidentiality and data integrity are required to protect against unauthorized access. This has resulted in an explosive growth of the field of data hiding [3]. Data hiding also reduces system complexity for increased robustness by limiting interdependencies between software components. Data hiding is also known as data encapsulation or information hiding [4]. The key to successful data hiding is the finding of holes that are not suitable for exploitation by compression algorithms. A further challenge is to fill these holes with data in a way that remains invariant to a large class of host signal transformations [5]. In recent years, enormous research efforts have been invested in the development of digital image steganographic techniques[6]. The major goal of steganography is to enhance communication security by inserting secret message into the digital image, modifying the nonessential pixels of the image [7]. A simple and well known approach is directly hiding secret data into the least-significant bit (LSB) of each pixel in an image [8]. The sender embeds a secret message into digital media (e.g. im-age) where only receiver can extract this message [9]. Watermarking has become the key method for protecting digital elements such as image, audio and video [10]. In the early days, the writing of hidden messages was done on paper only, but in the digital age, people are using steganography and watermarks to hide messages in all kinds of computer files, like recordings or images [11]. This hidden information can be plain text, cipher text, or even images [12]. The hiding of information within word sequences, the actual dictionary items can be used to encode one or more bits of information per word using a codebook of mappings between lexical items and bit sequences, or words themselves can encode the hidden information [13].

III. Proposed Work

In this research paper a new frequency domain method for image steganography. The merit is to increase image quality by hiding the messages in HL, LH, and HH sub-bands while keeping LL sub-band invariant. the simplest DWT is applied to obtain 4 sub-bands. Here determine how many bits should be embedded in a DWT coefficient according to the magnitude of that coefficient and the requirement of the user. After the secret messages are embedded, the slightly modified DWT coefficients are transformed back to spatial domain. The resulted stego-image is hence ready for quality evaluation. To extract secret messages from the stego-image, we just perform the algorithm in the opposite direction.

In this research method starts by inputting the secret message which is to be embedded into cover image. The secret message can be any text file or image or any audio wave file .and then selecting the cover image in which message is to be embedded. This cover message must be sufficient large to embed the entire message. Suppose X is the original 8-bit gray-level cover-image of MC × NC pixels. It is denoted as:

$$X=\{x_{ij}\mid 1\le i\le M_C, 1\le j\le N_C, x_{ij}\in\{0,1,\_,255\}\}\_\_\_\_ \quad (1)$$

After selection of input secret message and cover image next, we find out the size of the image as well as size of the text file. Check whether the size of the image is greater or less than the text file. If the size of the image is less than the size of the selected text file then print the error message, otherwise it is possible to embed the text file into selected Cover image.

Before hiding the secret message into cover image it must be converted into the encrypted form so that it can’t be interpretable by intruder .To do so first, we convert the secret data or message into its binary form . let P is the n-bit secret message represented as:

$$P=\{p_i\mid 1\le i\le n, p_i\in\{0,1\}\}\_\_\_\_\_\_\_\_ \quad (2)$$

random number to generate the private key of length same as the length of message because the size of encrypt message is equal to the original message, then apply X-OR operator to generate the cipher message of length n bits.

$S = P \oplus K$ Where

$$K=\{k_i\mid 1\le i\le n, k_i\in\{0,1\}\}\_\_\_\_\_\_\_\_ \quad (3)$$

and

$$S=\{s_i\mid 1\le i\le n, c_i\in\{0,1\} \text{ and } s_i=p_i\oplus k_i\}\_\_\_\_\_\_ \quad (4)$$

Apply DWT on X to obtain the frequency domain matrix H. The 4 sub-bands obtained are denoted as HLL, c (All 4 sub-bands have the same size of MC/2 × NC/2).Secret message embedding stage is based on one of the selected detailed coefficient of each image.In the message recovery algorithm, first we select the stego image Y from which data is to be extracted. Let the 8-bit gray-level stego-image of MC × NC pixels is represented as:

$$Y=\{y_{ij}\mid 1\le i\le M_C, 1\le j\le N_C, y_{ij}\in\{0,1,\_,255\}\}\_\_\_\_ \quad (5)$$

IV. CIRCUIT SIMULATION RESULT

The capacity of the method remains the same and it is represented by 1/4 of cover image size for 1-level decomposition of the cover image. The payload is 0.25 bit/pixel in case of using the maximum capacity and it also varies depending on numbers of detail coefficient are used during the embedding phase. The proposed algorithm employs 1-Level L decomposition of the image hence the total capacity (in bits) is represented by 1/4 of image size number of DWT detail coefficient, which are altered.

The tests were performed with a gray standard testing image Lena and other cover image with the same size 256x256 pixels (containing 64 kB). The secret message what represented by (containing 2048B).JSteg and F5 methods do not embed a fixed number of secret bits within a given cover image. JMQT method uses the 2-LSBs of each predefined middle frequency coefficient as redundant bits for data hiding. Since it embeds secret data in 26 quantized DCT coefficients of each block, then each block of 8x8 pixels can hide 2bits*26=52 secret bits. Therefore, a cover image of 256x256 pixels can hold: 52 x (256x256) / (8x8) =53248 secret bits.

On the other hand, 16*16 quantization method can embed 242 secret bits in each block of 16x16 pixels using the same technique of JMQT and 16x16 quantization table . Therefore, the capacity of a cover image of 256x256 pixels is 242 x (256x256) / (16x16) = 61952 secret bits.

TABLE I: The Capacity(bits) of Our proposed Steganography Method and other method considered

Method / Image	**Lena**	**Peppers**	**Baboon**	**Girl**	**Airplane**
JSteg	10421	10854	19006	8593	11752
F5	5637	16112	24124	13572	17360
JMQT	53248	53248	53248	53248	53248
16x16 Quantization Method	61952	61952	61952	61952	61952
Base paper method	49152	49152	49152	49152	49152
Our proposed Method	49152	49152	49152	49152	49152

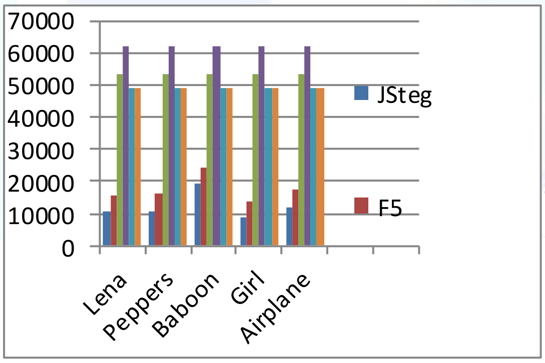


Figure 1: The Capacity(bits) compairison of Our proposed Steganography Method with other existing method

Figure 1 shows the PSNR values (quality) of obtained stego images (Table 4.2). The quality of our method's stego images is good and acceptable compared to the stego images' quality of other three steganography methods.

TABLE II: The PSNR(dB) of Our proposed Steganography Method and other method considered

Method / Image	**Lena**	**Peppers**	**Baboon**	**Girl**	**Airplane**
JSteg	**37.17**	**37.58**	**35.57**	**38.79**	**36.46**
F5	**37.45**	**38.33**	**38.33**	**38.81**	**37.06**
JMQT	**41.25**	**42.75**	**50.09**	**42.97**	**41.02**
16x16 Quantization Method	**40.82**	**42.38**	**36.46**	**42.76**	**40.86**
Our proposed Method	**57.44**	**57.46**	**57.23**	**58.37**	**57.29**

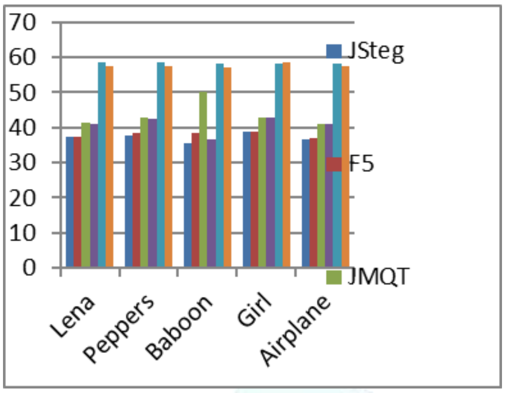
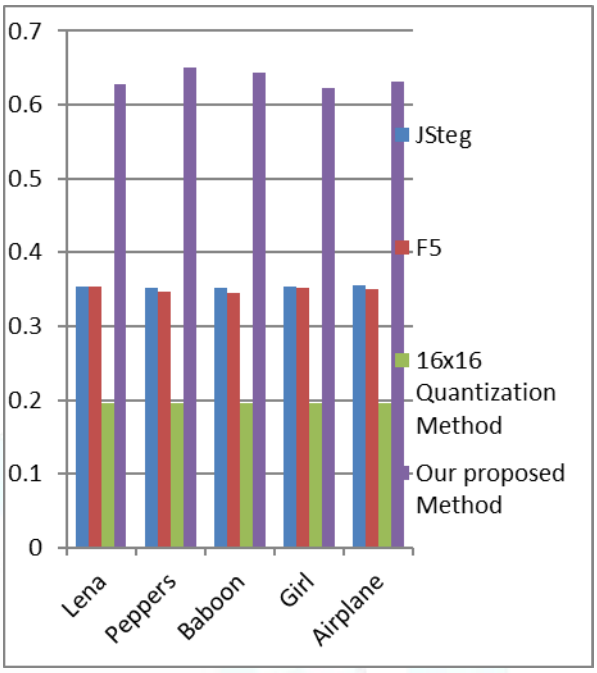


Figure 2: The PSNR(dB) comparison of Our proposed Steganography Method with other existing method

In our method, we kept a considerable number of coefficients to represent each block, hence stego images of our method have good quality. Even though we have slightly modified the middle frequency coefficients, it gives better results than discarding such coefficients. However, we embedded the secret bits by modifying low coefficients; therefore the stego images of our method have good quality.The running time of our method is almost double of that in the JSteg and JMQT methods. The steganographic capacity and stego image imperceptibility represent the two main requirements of image steganography methods (Zhang and Wang, 2005). As a result, our steganography method provides larger steganographic capacity and acceptable stego image quality which makes it superior to the other steganography methods tested.

TABLE III: The Execution time (sec) of Our proposed Steganography Method and other method considered

Method / Image	**Lena**	**Peppers**	**Baboon**	**Girl**	**Airplane**
JSteg	0.3531	0.3515	0.3528	0.3542	0.3546
F5	0.3533	0.3466	0.3447	0.3516	0.3504
16x16 Quantization Method	0.1954	0.1957	0.1951	0.1955	0.1955
Our proposed Method	0.6284	0.6501	0.6432	0.6308	0.6308



V. CONCLUSIONS

The research aim to increase the steganographic capacity and improve the quality of stego images The proposed scheme was tested for different hiding capacity and the results showed that it has excellent output quality. From the tests we find the proposed algorithm support high capacity rate reach up to ¾ bits per pixel and that is form above 75% from the size of the input image cover file at SNR above 57 dB for the output signal. The algorithm was implemented by using Matlab (2009a) programming. The proposed algorithm was tested using five cover image files: Airplane, Lena,Baboon,Papper and Girl. Each image has resolution of 8 bits per pixel and diamention is 256*256 pixel and text file is used in tests as secret messages. The quality of output signal in each test was computed using SNR and Time Complexity.

REFERENCES

[1]. T. S. Chen, C. C. Chang, and M. S. Hwang, “A virtual image cryptosystem based upon vector quantization,” IEEE Transactions on Image Processing, 1998, Vol. 7, No. 10, pp. 1485-1488.

[2]. R. Z. Wang, C. F. Lin, and J. C. Lin, “Image hiding by optimal LSB substitution and genetic algorithm,” Pattern Recognition, 2001, Vol. 34, No. 3, pp. 671-683.

[3]. Zaidoon Kh., AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi,” Overview: Main Fundamentals for Steganography “, journal of computing, volume 2, issue 3, March 2010.

[4]. http://www.techopedia.com/definition/14738/data-hiding.

[5]. W. Bender,D. Gruhl, N. Morimoto,” Techniques for data hiding”, IBM SYSTEMS JOURNAL, VOL 35, NOS 3&4, 1996.

[6]. Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, Digital image steganography: Survey and analysis of current methods Signal Processing 90 (2010) 727–752.

[7]. W. Bender, D. Gruhl, N. Morimoto, A. Lu, Techniques for data hiding, IBM Syst. J. 35 (3&4) (1996) 313–336

[8]. Bruice Schneier, Applied Cryptography Protocols, Algorithm and Source Code in C. Second edition. Wiley India edition 2007

[9]. Nedeljko Cvejic, “Algorithms For Audio Watermarking And Steganography”, Department of Electrical and Information Engineering, Information Processing Laboratory, University of Oulu 2004.

[10]. Rajkumar Yadav,” Study of Information Hiding Techniques and their Counterattacks”, International Journal of Computer Science & Communication Networks, p.p. 142-164 Vol 1(2), Oct-Nov 2011.

[11]. Petitcolas, F.A.P., Anderson, R., Kuhn, M.G.,"Information Hiding - A Survey", July 1999.

[12]. Prof. Samir Kumar Bandyopadhyay, Tuhin Utsab Paul , Avishek Raychoudhury, ” A Robust Audio Steganographic Technique based on Phase Shifting and Psycho – acoustic Persistence of Human Hearing Ability”, International Journal of Computing and Corporate Research .

[13]. Bender, W., Gruhl, D., Morimoto, N. & Lu, A., “Techniques for data hiding”, IBM Systems Journal, Vol 35, 1996