Image Steganography based on DWT using Huffman LWZ Encoding

Kshitija Pol

***Abstract* — In this modern era, internet offers great convenience in transmitting large amounts of data in different parts of the world. However, the safety and security of long distance communication remains an issue. In order to solve this problem has led to the development of Steganography schemes. Steganography is the science that communicates secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. DWT is used to transform original image (cover image) from spatial domain to frequency domain. First two dimensional Discrete Wavelet Transform (2-D DWT) is performed on a gray level cover image of size M × N and Huffman encoding is performed on the secret messages/image b. The resulted secrete image is encoded by using LWZ encoding techniques. Then each bit of resulted secrete code of secret message/image is embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Image quality is to be improved by preserving the wavelet coefficients in the low frequency sub band.**

***Index Terms* — Steganography, DWT, Huffman Encoding, LZW**

I. INTRODUCTION

The basic need of every growing area in today's world is communication. Everyone wants to keep the inside information of work to be secret and safe. We use many insecure pathways in our daily life for transferring and sharing information using internet or telephonically, but at a certain level it's not safe. The advent of the internet age has led to the increase of prominent network security issues. Information encryption has long been a method used for information security. With the rapid development of parallel computing capacities of computer hardware, this method alone could not be trusted to ensure security by increasing the key sizes, thus bringing in the information hiding techniques into the scenario.

Steganography comes from the combination of the Greek words Stegano means sealed and Graphy referring to writing which means secret writing. Steganography is a very old art of embedding personal information into other data by using some rules and techniques. Steganography is an important area of research in recent years involving a number of applications [3]Security of the secret information has been a challenge when the large amount of data is exchanged on the internet. A secure transfer of information can be very much achieved by Steganography. Steganography is information security tool which stores the secret information in any media file e.g. text, image, audio and video file [2] in such way that no one else except the sender of the information and the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data satisfactory security is maintained.

Cryptography is closely related to Steganography. Cryptography is also an information security tool which provides encryption techniques to hide the secret information. Aim of both steganography and cryptography is same but achieved by different ways. Good imperceptibility (difficult to detect hidden information) and sufficient data capacity (efficiency of hidden information) are two properties which should be possessed by all the steganography techniques. Cryptography scrambles the data to be secured while information hiding embeds the information into files which do not reveal the presence of information. A combination of Cryptography and Steganography results in very strong cryptosystems

There are other two technologies that are closely related to steganography are watermarking and fingerprinting [1]. These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than steganography. In watermarking all of the instances of an object are "marked" in the same way. Watermarking is used to implement copyright protection On the other hand, in fingerprinting unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the intellectual property owner to identify customers who break their licensing agreement by supplying the property to third parties [1]. Steganography techniques are being widely used these days to increase the security of information.

Image steganography can be classified as (1) spatial domain based techniques; (2) transform domain based techniques [4]. In this method secret data is embedded directly into the least significant bit (LSB) plane of the cover image. This method is also called LSB substitution. The spatial domain based steganography technique use either the LSB or Bit Plane Complexity Segmentation (BPCS) algorithm [5]. This method is also called transform domain based steganography. In this method before embedding the secret data into the cover image, it is needed to be transformed into frequency domain coefficients. It is done by using DCT or DWT [6]. Different sub-bands of frequency domain coefficients give significant information about where the vital and non-vital pixels of image resides. It is very complex method and takes more time than spatial domain techniques.

Manuscript received March 12, 2014.
Kshitija Pol, Associate Professor, Computer Science & Engineering Department, Dronacharya College of Engineering, Gurgaon, India, 9899363191

LSB (least significant bits) technique was mostly used, while MSB (most significant bits) technique was very less used. There were also several other techniques used such as SSHDT, RSTEG, DCT, DWT, LWT etc. Combined techniques of steganography and cryptography are also used.

Steganography has played a very beneficial role in various applications. It increased the level of information security with a wide use of its techniques. Steganography is alleged by intelligence service. Steganography methods can be used to distribute the payload through multiple carrier files in diverse locations to make detection more difficult.

II. RELATED WORKS

Image steganography based on Huffman Encoding. Two 8 bit gray level image of size M X N and P X Q are used as cover image and secret image respectively. Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of the Huffman encoded bit stream and Huffman Table are also embedded inside the cover image, so that the Stego-Image becomes standalone information to the receiver. The experimental result shows that the algorithm has a high capacity and a good invisibility. Moreover Peak Signal to Noise Ratio (PSNR) of stego image with cover image shows better result in comparison with other existing steganography approaches.

For 2-D images, applying DWT (Discrete Wavelet Transform) separates the image into a lower resolution approximation image or band (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH). With the DWT, the significant part(smooth parts) of the spatial domain image exist in the approximation band that consists of low frequency wavelet coefficients and the edge and texture details usually exist in high frequency sub bands, such as HH, HL, and LH. DWT based approach scheme using a mapping table, the secret message is embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Among all other methods mentioned earlier, this method provides better quality of image, increases embedding capacity and is also robust against attack.

LWZ is the foremost technique for general purpose data compression due to its simplicity and versatility. Typically, you can expect LZW to compress text, executable code, and similar data files to about one-half their original size. LZW also performs well when presented with extremely redundant data files, such as tabulated numbers, computer.

III. PROPOSED METHOD

As we know that to use image steganography we require two images. They are Cover Image & Secrete Image. In a proposed method apply Huffman code using Huffman table on Secrete Image. Apply LWZ encoding on resulted Secrete Image. Now apply DWT on Cover image. Embed SEI on resulted cover image. Process of encoding Secrete Image is shown in Fig.1. Embedding Secrete image into Cover Image using DWT image is shown in Fig.2. Extracting the secrete image from Cover Image is shown in Fig.3. Decodes LWZ Code, then Huffman code using Huffman Table to Extract original Secrete image is shown in Fig. 4.

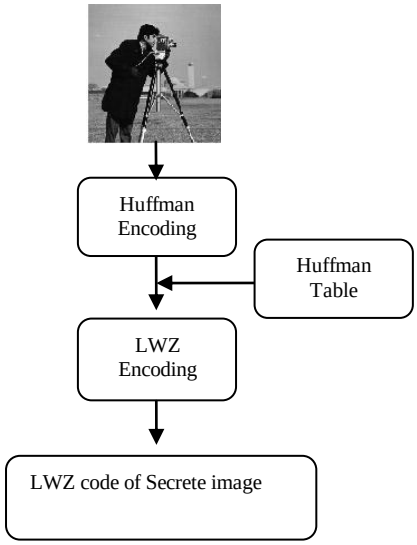

Figure 1 - Encoding Secrete Image

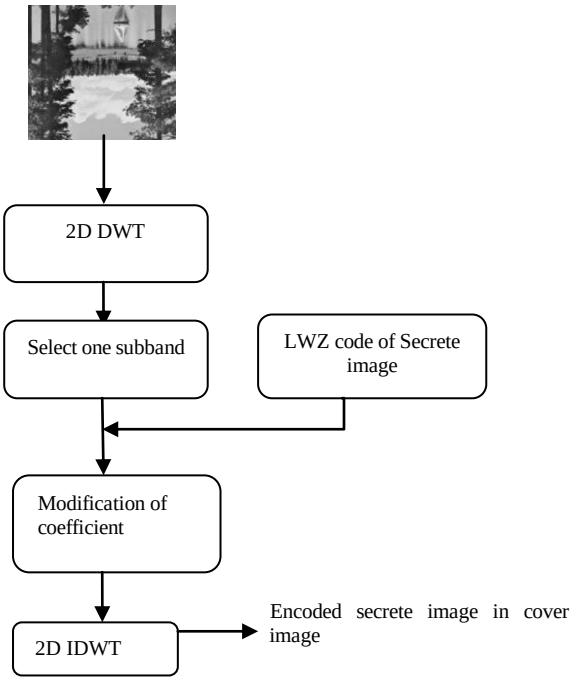

Figure2 - Encoding Secrete Image Insertion of Huffman LWZ code into Cover Image

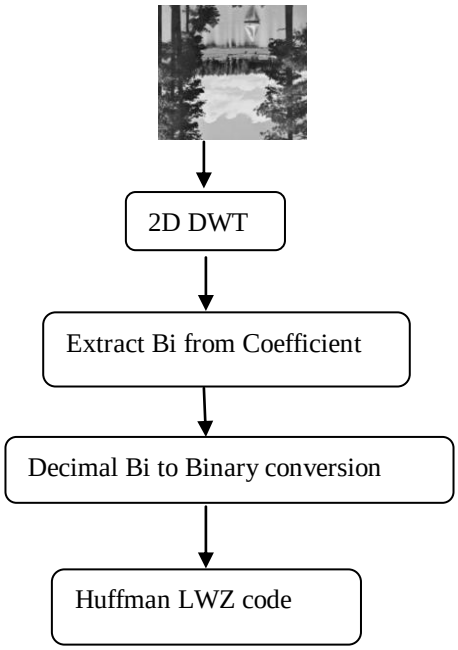

Figure 3 - Removal of Huffman LWZ code from cover image

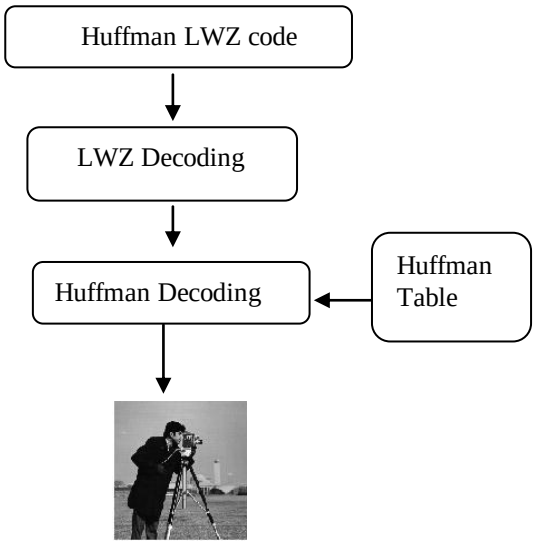

Figure 4 - Huffman LWZ Decoding of Secrete Image

A. *Generations of Huffman code*

Secrete image is to be embedded in Cover image. We choose Huffman code because it is lossless. Another region to use Huffman encoding is that no one reveals what is the meaning of Huffman encoding without Huffman Table. For an image Huffman coding assigns a binary code to each intensity value of the image and a 2-D M2 × N2 image is converted to a 1-D bits stream with length LH < M2 × N2. Huffman code H is now decomposed into 4-bits blocks and thus form a decimal value ranging from 0 to 15.Binary sequence is now changed to Decimal no. (D) Where

D= {Bi|1<=t<=16*M*N/4, Bi= {0,1,2..15}

B. *Embedding of Secrete image*

Decompose cover image using DWT. We choose DWT because it provides better quality of image, increases embedding capacity and is also robust against attack. Select one sub-band for embedding the secret message. Apply inverse DWT on DWT Transformed image.

C. *Extraction of the Secret Message / Image*

The stego-image is received in spatial domain. DWT is applied on the stego-image to transform the stego-image from spatial domain to frequency domain. Extract bit stream to decode LWZ code. The size of the encoded bit stream and the encoded bit stream of secret message/image are extracted along with the Huffman Encoding using Huffman table.

IV. RESULT

Result was verified using MatLab 7 on Windows 7 Home Edition. Image data to be considered for Cover image is as shown in Fig.5. Fig.6 shows cover image.

Figure 5 - Secrete Image

Figure 6 - Cover image

IV. CONCLUSION

When stego image is transmitted it may be corrupted due to noise. Image steganography method generally does not provide privacy of image data. In this paper, the major importance is given on the privacy of image information. The embedding process is hidden under the transformation (DWT and IDWT) of cover image. On the other hand to obtain privacy we have used Huffman encoding and LWZ. This method gives good result in term of PSNR. It is found that PSNR (db) is 55.11. In future, this model should be extended to apply in to medical image and medical report transaction process

REFERENCES

[1] Raja, K.B., Chowdary, C.R., Venugopal, K.R. , Patnaik, L.M. "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images" Intelligent Sensing and Information Processing, 2005. ICISIP 2005, PAGE 170-176,14-17 Dec 2012.

[2] Das R.,Tuithung T., "A Novel Steganography method for image based on Huffman Coding" NCETACE , Page14-18 30-31 March 2012.

[3] Masud Moshtaghi, TimothyC.Havens, JamesC.Bezdek, LaurencePark, hristopherLeckie, Sutharshan Rajasegarar, JamesM.Keller, Marimuthu Palaniswami", "Clustering ellipses for anomaly detection". Pattern Recognition 44,page 55–69,July 2010.

[4] Jing-Ming Guo, Thanh-Nam Le, "Secret Communication Using JPEG Double Compression", Signal Processing Letters, IEEE, Vol. 17, Issue No. 10, Pages No. 879 – 882, Oct., 2010.

[5] P. Nithyanandam, T. Ravichandran, N. M.Santron, E. Priyadarshini, "A Spatial Domain Image Steganography Technique Based on Matrix Embedding and Huffman Encoding", International Journal of Computer Science and Security (IJCSS), Vol. 5, Issue No. 5, 2011.

[6] Amitha G.,Meethu Vrkey " Biometric Steganographic Technique Using DWT and Encryption" International Journal of Advanced Research in Computer Science and Software Engineering, pages 566-572, March 2013.

Kshitija Pol, Associate Professor, Computer Science & Engineering Department, Dronacharya College of Engineering, Gurgaon, India, +91-9899363191.