Image Steganography based on DWT using Huffman Encoding with Arithmetic Coding

Kshitija Pol
Computer Science and Engineering Department, Dronacharya College of Engineering,Gurgaon

***Abstract*—Internet offers great convenience in transmitting large amounts of data in different parts of the world. As every computer user knows that there are numerous security threats for digitized objects hence methods like steganography are getting more importance day by day. Though steganography is a very old method of hiding information behind some object, but still this is very effective for secure data transfer and data exchange.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 apply 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 Arithmetic 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.**

***Keywords*—Steganography, DWT, Huffman Encoding, Arithmetic Coding**

I. INTRODUCTION

Steganography comes from the combination of the Greek words Stegano means sealed and Graphy referring to writing which means secret writing. A stego-system (steganographic system) in image steganography refers to a system capable of hiding a secret message within an image, such that no third-parties are aware that the message exists. The image that is output from this process is known as a stegogramme, and great care is taken to ensure that this looks as innocent as possible so that the secret message has the best chance of reaching its intended recipient. However, the stego-system not only refers to encoding the message, it also refers to the system that makes it possible to read the message when it reaches its recipient[1]. Steganography is an important area of research in recent years involving a number of applications [2] 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 file e.g. text, image, audio and video file [3] in such way that **no one** else except stores the secret information in any media 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[4].Cryptography scrambles the data to be secured while information hiding embeds the information into files which do not reveal the presence of information Steganography means is not to alter the structure of the secret message, but hides it inside a cover-object (carrier object). After hiding process cover object and stego-object (carrying hidden information object) are similar. So, steganography (hiding information) and cryptography (protecting information) are totally different from one another Aim of both steganography and cryptography is same but achieved by different ways.

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 [5]. 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 [6]. 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 [7]. 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.
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 Quantized data of secret image/message before embedding and each bit of Huffman code of secret image/message is embedded inside the 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.

In comparison to other transforms, wavelet transforms gives best results for image transformation. In its basic operations, it decomposes the input signal into set of .functions which are called waveletsFor 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.

Arithmetic Coding

When a string is converted to arithmetic encoding, frequently used characters will be stored with fewer bits and not-so-frequently occurring characters will be stored with more bits, resulting in fewer bits used in total. Arithmetic coding encodes the entire message into a single number, a fraction n where ($0.0 \leq n < 1.0$).

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 Arithmetic 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.

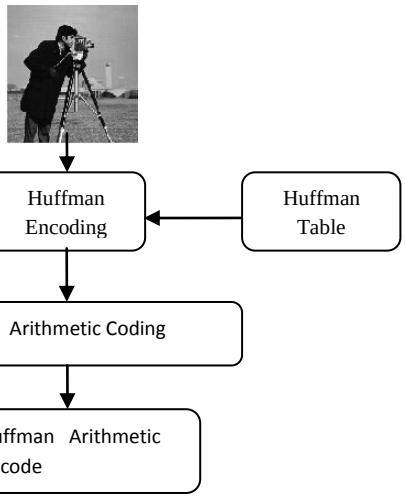

Figure 1 - Encoding Secrete Image

Embedding Secrete image into Cover Image using DWT image is shown in Fig.2.

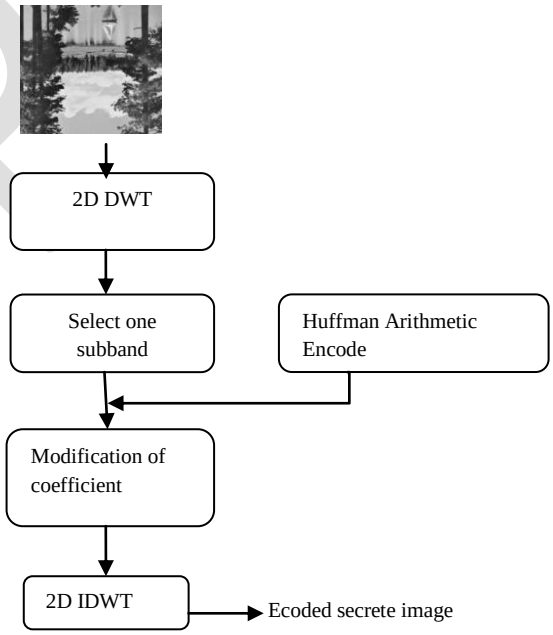

Figure 2.Encoding Secrete Image Insertion of Huffman Encode into Cover Image

Extracting the secrete image from Cover Image is shown in Fig.3. Decodes Arithmetic Code, then Huffman code using Huffman Table to Extract original Secrete image is shown in Fig. 4.

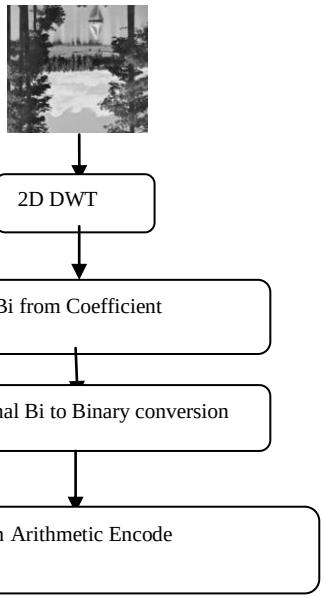

Figure 3 - Removal of Huffman LWZ code from cover image

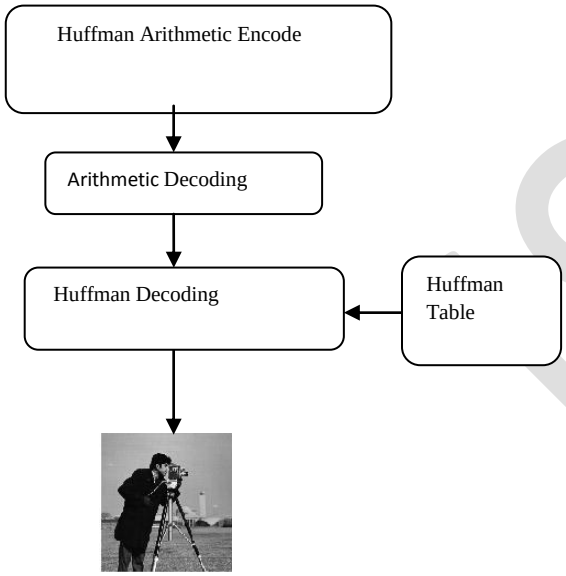

Figure 4 – Arithmetic Decoding & Huffman Decoding of Secrete Image

A. Generations of Huffman code with Arithmetic Coding

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 3-bits blocks and thus form a decimal value ranging from 0 to 7.Binary sequence is now changed to Decimal no. (D) Where

D= {Bi|1<=t<=8*M*N/4, Bi= {0,1,2..7}

Convert each decimal number as decimal number / 8.

We choose DWT because. Initially interval is set to between [0, 1). The encoder divides the current interval into sub-intervals, each representing a fraction of the current interval proportional to the probability of that symbol in the current context. Whichever interval corresponds to the actual symbol that is next to be encoded becomes the interval used in the next step.

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 Arithmetic 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

V. 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 Arithmetic coding. This method gives good result in term of PSNR. This method gives good result in term of PSNR. It is found that PSNR (db) is 60.10. It gives more capacity for larger image

sizes. It enhances security and also preserves the image quality

REFERENCES

[1] Saeed Ahmed Sohag, Dr. Md. Kabirul Islam, Md. Baharul Islam " Novel Approach for Image Steganography Using Dynamic Substitution and Secret Key" American Journal of Engineering Research (AJER) Volume-02, Issue-09, pp-118-126,2013

[2] 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

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

[4] Mehdi Hussain and Mureed Hussain "A Survey of Image Steganography Techniques" International Journal of Advanced Science and Technology Page-113-124, Vol. 54, May, 2013

[5] 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.

[6] 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.

[7] 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.