ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Image Steganography Method Using Integer Wavelet Transform

[1]M.Vijay , [2]V.VigneshKumar

[1]Dept.of ECE, AAA College of Engineering &Tech, Tamilnadu, India.

[2]Dept.of ECE, AAA College of Engineering &Tech, Tamilnadu, India.

ABSTRACT— Digital Steganography explains the art and science of writing hidden messages in such a way that, apart from the sender and intended recipient, no one suspects the existence of the message, a form of security through the state of being unknown. The main two famous schemes used for image steganography are spatial domain embedding and transform domain embedding. The main aim of Wavelet Transform is used to transform original image (cover image) from spatial domain to frequency domain. But here in our proposed work, Integer Wavelet Transform is performed on a gray level cover image and in turn embeds the message bitstream into the LSB's of the integer wavelet coefficients of a the image . The main purpose of the proposed work is to focus on improving embedding capacity and bring down the distortion occurring to the stego image. The refinement of the algorithm plays an important role for accomplishing higher embedding capacity and low distortion rate. The experimental results prove that the assessment metric such as PSNR is improved in a high manner. The experimental results show that the algorithm has a high capacity and a good invisibility.

KEYWORDS - Image Steganography, Frequency Domain, IWT, Information Hiding.

I. INTRODUCTION

Ever since the origin of internet, the information technology and communication fields have their major factor as the security of information [1]. Cryptography provides a technique for securing the communication secret and keeps it as such. Steganography includes many algorithms not only to keep the secret message but also to have the existence of the message secret. Steganography refers to hiding the information for a secure communication [2]. The major use of steganography over cryptography is that messages don't attract have much attention to attackers and even receivers. Image steganography implies hiding information utterly in images. Two other technologies that are closely related to steganography are watermarking and fingerprinting. All digital file formats are appropriate for steganography but the apt one for it is the file with high degree of redundancy.

Some novel techniques for Image Steganography based on Block-DCT and Huffman Encoding [14] and a method Using Matrix and LSB Embedding based on Huffman Encoding [15] are proposed but its robustness is not high.

In a blind image steganographic system, a message is embedded in a digital image by the stegosystem encoder which uses a key. The resulting stego-image is transmitted over a channel to the receiver where it is processed by the stegosystem decoder using the same key. In general, if the channel is monitored by someone who is allowed to modify the information flow between the two parties, he is called an active warden; but if he can only observe it, he is called a passive warden. Another technique depends on the introduction of high-frequency, low-amplitude noise and the use of direct sequence spread spectrum coding. This method combines techniques from spread spectrum communication, error-control coding, and image processing. The fundamental concept is that the data is embedded in the noise, which is added to the original image. Because the noise is low power and the decoding process is not perfect, a low-bit error-correcting code is incorporated.

But here in our proposed work, Integer Wavelet Transform (IWT) [16] is performed on a gray level cover image and in turn embeds the message bitstream into the LSB's of the integer wavelet coefficients of a the image . The main purpose of the proposed work is to focus on improving embedding capacity and bring down the distortion occurring to the stego image. The experimental discussions shows that the proposed algorithm has a high capacity, good invisibility and low distortion rate.

This paper is organized as follows. In section II, we analyze the methods used for steganography. In section III, the Wavelet transform method is discussed. In Section IV proposed algorithm is discussed. Section V affords the simulation results. The conclusion is made at section VI.

II.METHOD ANALYSIS

Steganography defines the usage of spatial [3, 4, 5] and frequency schemes [6, 7, 8]. The least significant bit (LSB) approach uses many approaches like modified side match scheme but these results proved to be fatal. It is not robust against attacks and improving the embedding capacity.

By using Vector Quantization compression method, the gray-level secret image is compressed before embedding. After while the compressed gray-level secret image is encrypted and then embedded into the DWT coefficients of the cover image. It provides a recovery scheme to repair the secret image if the stego-image is destroyed, but the PSNR does not reach the expectations. The DWT based A popular approach which is based on DWT scheme [9] with the help of a mapping table, the secret message is embed in the high frequency coefficients. Compare to all other previous methods, this method not only provides good visual quality but also increases embedding capacity. Based on the same embedding capacity of [9], our proposed method improves both image quality and security.

III. WAVELET DOMAIN APPROACH

A) Integer Wavelet Transform (IWT)

By using WT, the significant parts of the spatial domain image exist in the approximation band that consists of low frequency bands and the edge and texture details usually exist in high frequency sub bands. Normally the human eyes are not sensitive to the small changes in the edges and textures of an image but very sensitive to the small variations in the smooth parts. This helps the secret image to be embedded at high frequency sub-bands without being perceived by the eye. The discrete wavelet transform allows independent processing of the resulting components without significant perceptible interaction between them; hence it is expected to make the process of imperceptible embedding more effective. The wavelet transform along with integer mapping helps to improve the effectiveness of Wavelet transform.

The main example of wavelet transforms that map integers to integers is the S-transform[16]. The equation is given by,

$$T(n)=\frac{y(2n)+y(2n+1)}{2}. \qquad (1)$$

$$D(n)= y(2n) - y(2n+1)) \qquad (2)$$

IV. PROPOSED METHOD

The implementation of wavelet transforms that map integers to integers in the area of image steganography allowed the embedded message to be recovered without loss.

Then the proposed algorithm holds the bit stream in the least significant bits of the transform coefficients. It does not affect the integrality of the embedded coefficients. To implement this algorithm in a better way, a preprocessing step is applied which helps to adjust the saturated pixel components in a way to prove that they do not exceed their maximum value due to modifying their corresponding coefficients. In case of color images, an adjustment of cover image is done using,

$$D'(x,x,z) = \begin{cases} D(x,y,z)-(2^N-1); & D(x,y,z)=255 \\ D(x,y,z) & \text{Otherwise} \end{cases} \qquad (3)$$

The embedding and extracting module algorithm is given below

A) Embedding Algorithm

a) Convert the secret message into a bit stream sequence.
b) Applying Integer Wavelet Transform (IWT) the on the cover image. In case of color image wavelet transform is performed on each color plane separately.
c) The embedding process stores (N) message bits in the least significant bits
d) (LSB) of the IWT coefficients of the cover image.
e) After embedding, the stego image is produced by applying the Inverse of the Integer Wavelet Transform (IIWT) on the modified coefficients.
f) To arrange the coefficients in an order, the pseudorandom permutation Scheme is applied.

B) Extracting Algorithm

a) Apply IWT on each color plane of the stego image.
b) Apply permutation scheme for extracting the bit sequence
c) Selecting the embedded coefficients, until extracting the embedded message bits from the N LSB's of the integer coefficients.
d) The extracted bits are further converted into its original message.

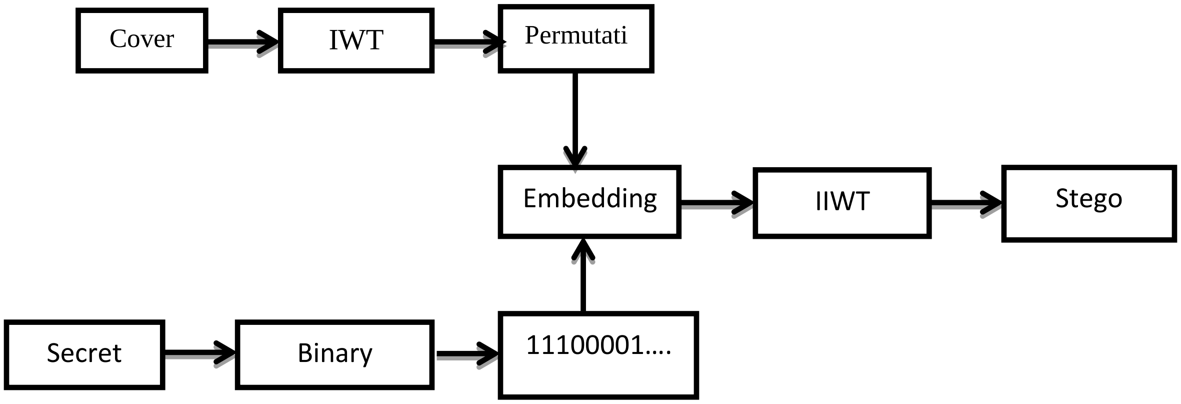

Figure 1: Insertion of secret image into a Cover image

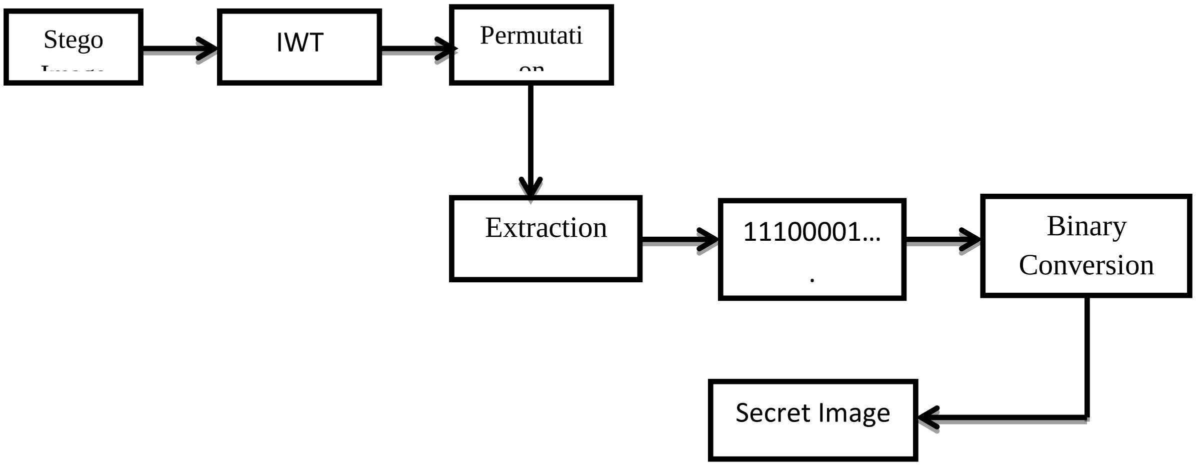

Figure 2: Extraction of secret image from the Cover image

V. Simulation Results

In this section, some experiments are carried out to prove the efficiency of the proposed method. The proposed method has been simulated using the MATLAB 7.5 program on Windows 7 platform. A set of 8- bit gray scale images of size 512 × 512 are used as the cover-image to form the stego-image. Peak Signal to Noise Ratio measures the transparency of the stego image. When the obtained PSNR values are greater than 40 db then the stego-image have a best quality.

The Figure 3 shows the original cover (carrier) image and Figure 4 show the original secret message. By using the PSNR value the invisibility of the stego-images is evaluated. The proposed method is compared with various standard techniques like DWT, DCT, Matrix Rotation, LSB technique. PSNR values are calculated and the comparisons of other methods are shown in the table I.

TABLE I : PSNR COMPARISION OF IMAGE STEGANOGRAPHY TECHNIQUES

METHODS	PSNR(dB)	PSNR(dB)	PSNR(dB)
	Lena(512 X512)	Barbara(512X512)	Boat (512X512)
DWT[10]	46.08	46.73	47.82
DCT[14]	47.12	46.91	46.83
MATRIX Rotation[15]	52.9	52.85	52.86
LSB Technique[3]	53.43	53.75	52.76
Proposed Method	**54.92**	**54.21**	**54.1**

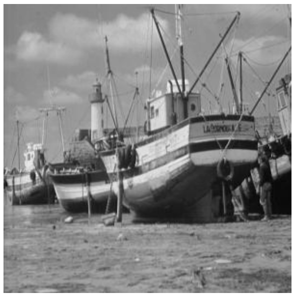

Figure 3: Cover Image

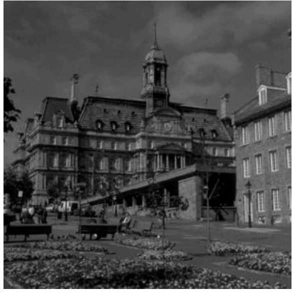

Figure 4: Secret Image

VI. CONCLUSION

Normally, image steganography method does not provide much attention on the basic demand of secrecy and privacy. But in our proposed work the main importance is given to the secrecy as well as the privacy of information. The embedding process is hidden under the transformation of cover image. These operations provide sufficient secrecy. On the other hand to obtain privacy, IWT is used. The embedding capacity of the cover image is increased, at the same time the PSNR also controlled. The proposed technique is robust against any geometrical distortion such as rotation, translation, scaling, cropping etc., induced on the stego image. After comparisons it is found that, PSNR is higher than other methods.

REFERENCES

[1] N. F. Johnson and S. Katzenbeisser, ―*A survey of steganographic techniques"*. Information Hiding, Artech House, pp. 43-78, 2000.

[2] Moerland, T. ―*Steganography and Steganalysis*". Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf.

[3] Chan, C.K. and Cheng. L.M. ―*Hiding data in image by simple LSB substitution*". Pattern Recognition, 37: 469 – 474, 2003.

[4] Chang, C.C and Tseng, H.W. ―*A Steganographic method for digital images using side match*" Pattern Recognition Letters, 25: 1431 – 1437, 2004.

[5] H. Arafat Ali. ―*Qualitative Spatial Image Data Hiding for Secure Data Transmission*". GVIP Journal, 7(1):35-43, 2007

[6] Chen, T.S., Chang C.C., and Hwang, M.S. ―*A virtual image cryptosystem based upon vector quantization*". IEEE transactions on Image Processing, 7,(10): 1485 – 1488, 1998.

[7] Chung, K.L., Shen, C.H. and Chang, L.C. ―*A novel SVD-and VQ-based image hiding scheme. Pattern Recognition Letters*" 22: 1051 – 1058, 2001.

[8] Iwata, M., Miyake, K., and Shiozaki, A. ―Digital Steganography Utilizing Features of JPEG Images, IEICE Transfusion Fundamentals". E87-A (4):929 – 936, 2004**.**

[9] Chen, P.Y. and Wu, W.E. ―*A Modified Side Match Scheme for Image Steganography*". International Journal of Applied Science and Engineering, 7(1): 53 – 60, 2009.

[10] Prabakaran. G and Bhavani.R ―*A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform*" international publish, 2012.

[11]M. Yang, M.Trifas, N. Bourbakis, and C. Cushing, "*A Robust Information Hiding Methodology in Wavelet Domain", Proceedings of 12th International Conference on Signal and Image Processing*", Honolulu, Hawaii, August 2007.

[12]Gonzalez, R.C. and Woods, R.E., Digital Image Processing using MATLAB, Pearson Education, India,2006.

[13]Jayaraman, S., Esakkirajan, S. and Veerakumar, T. Digital Image Processing, Tata McGraw Hill Education Private Limited, India, 2009

[14]Amitava Nag, S. Biswas, D. Sarkar, P.P. Sarkar. ―A Novel Technique for Image Steganography Based on Block-DCT and Huffman Encoding" , International Journal of Computer Science and Information Technology, Volume 2, Number 3, pp. 103-112,June 2010.

[15]P. Nithyanandam , T. Ravichandran, E. Priyadharshini and N.M. Santron.―A Image Steganography Technique on Spatial Domain Using Matrix and LSB Embedding based on Huffman Encoding", Journal of Future Engineering and Technology, vol 6, no.3, Feb 2011.

[16] A.R. Calderbank, Ingrid Daubechies, Wim Sweldens, Boon-lock Yeo, *Lossless image compression using integer to integer wavelet transforms*, in the international conference on image procrssing, Piscataway, NJ: IEEE Press, 1997, vol. I, pp 596-599.