National Conference on Information, Communication, VLSI and Embedded systems (ICVE 2K16)
(16 - 17 March 2016)
International Journal of Engineering Research & Science (IJOER)
ISSN: [2395-6992] [Vol-2, Issue-3 March- 2016]

A New Secure Image Steganography Using Lsb And Spiht Based Compression Method

M.J.Thenmozhi[1], Dr.T.Menakadevi[2]

[1]PG Scholar, Department of ECE, Adiyamaan college of Engineering ,Hosur, Tamilnadu, India
[2]Professor, Department of ECE, Adiyamaan college of Engineering, Hosur, Tamilnadu, India

Abstract— *Steganography is nothing but the covered writing or secret writing. It is the science of secret communication. steganography is used to hide the survival of the message from unauthorized party. Images are the basic forms of transmitting information in the visual format. With the help of Image encryption methods any particular set of images can be transmitted without worrying about security. In this paper a very simple and real time algorithm which is used for the encryption of the images. In the proposed paper the message image is compressed by using the SPIHT method of lossless compression and then it is encoded in to the other image. Image contains a combination of RGB layers. If we consider a pixel as an 8 bit value than each pixel has the value in the range of 0 to 255. This algorithm compress the secret message image by SPIHT and convert in to a binary sequence, divides the binary sequence in to a blocks, change the order of block using a key-based randomly generated permutation, concatenates the permuted blocks can be changed in to a permuted binary sequence, and then utilizes the Least-Significant-Bit (LSB) approach to embed the permuted binary sequence into image. After the completion of the pixel value changing all the images is placed in a sequential manner. In the decoding side the message image is decoded and decompressed so that we can get the message image.*

Keywords— Steganography, SPHIT, LSB, Wavelet transform, Data hiding.

I. INTRODUCTION

With the growth of computer network, security of data has become a main concern and thus data hiding technique has concerned people around the world. Steganography techniques are used to deal with digital copyrights management, protect information, and conceal secrets. Data hiding techniques provide an motivating challenge for digital forensic investigators. Data is the backbone of today's communication. To ensure that data is secured and does not go to unplanned destination, the concept of data hiding came up to protect a part of information. Digital data can be delivered over computer networks with little errors and often without interference. The Internet provides a communication method to distribute information to the masses. Therefore, the privacy and data reliability are required to protect against unauthorized access and use. Steganography relies on hiding message in unsuspected multimedia data and is generally used in secret communication between recognized parties. The technique replaces unused or insignificant bits of the digital media with the secret data. The concept is to embed the hidden object into a considerably larger object so that the change is undetectable by the human eye. All digital file formats can be used for steganography, but the formats those are with a high scale of redundancy are more suitable. The redundant bits of an object are those bits that can be distorted without the alteration being detected easily. The most popular cover objects used for steganography are digital images. Digital images often have a huge amount of redundant data, and this is what steganography uses to hide the message. However, after checking one million images, no hidden messages were found, so the practical use of steganography still seems to be limited. To conceal a message inside an image without changing its perceptible properties, the cover source can be altered in "noisy" areas with many color variations, so less concentration will be drawn to the modifications. The most common methods to make these alterations involve the usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image. These techniques can be used with unreliable degrees of success on different types of image files.

The proposed method should provide better security while transferring the data or messages from one end to the other end. The main objective of the paper is to hide the message or a secret data into an image which acts as a carrier file having secret data and to transmit to the intention securely without any modification. If any distortions occur in the image or on its resolution while inserting the secret message into the image, there may be a chance for an unauthorized person to modify the data. So, the data encryption into an image and decryption and steganography plays an important role in this paper.

II. OVERVIEW OF STEGANOGRAPHY

2.1 Types of Steganography

2.1.1 Text steganography

It consists of hiding the information inside the text files. In this method, the secret data is hidden behind every nth letter of every words of text message. Numbers of methods are available for hiding data in text file. These methods are i) Format Based Method; ii) Random and Statistical Method; iii) Linguistics Method.

2.1.2 Image steganography

Hiding the data by attractive the cover object as image is referred as image steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are extensively used cover source because there are number of bits presents in digital representation of an image.

2.1.3 Audio steganography

It involves hiding data in audio files. This method hides the data in WAV, AU and MP3 sound files. There are different methods of audio steganography. These methods are i) Low Bit Encoding ii) Phase Coding iii) Spread Spectrum.

2.1.4 Video Steganography

It is the technique of hiding any kind of files or data into digital video format. In this case video (combination of pictures) is used as carrier for hiding the data. Generally discrete cosine transform (DCT) alter the values (e.g., 8.667 to 9) which is used to hide the data in each of the images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats used by video steganography.

2.1.5 Network or Protocol Steganography

It involves hiding the information by taking the network protocol such as TCP, UDP, ICMP, IP etc, as cover object. In the OSI layer network model there exist secret channels where steganography can be used.

III. RESEARCH METHODOLOGY

3.1 LSB Algorithm

LSB (Least Significant Bit) replacement is the process of adjusting the LSB pixels of the carrier image. It is a simple approach for embedding message into the image. The Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8^{th} bit of each byte of the image is distorted to the bit of secret message. For JPEG, the direct substitution of steganographic techniques is not possible since it will use lossy compression. So it uses LSB substitution for embedding the data into images.

3.2 SPIHT Algorithm

The SPIHT algorithm is a more efficient implementation of EZW (Embedded Zero Wavelet) algorithm which was presented by Shapiro. After applying wavelet transform to an image, the SPIHT algorithm partitions the decomposed wavelet into significant and insignificant partitions based on the following function.

$$Sn(T) = \begin{cases} 1, max \\ 0, otherwise \end{cases} (i,j) \in T\{ |C_{i,j}| \} \geq 2^n$$

Here Sn(T) is the significance of a set of coordinates T, and ci,j is the coefficient value at coordinate (i, j). There are two passes in the algorithm- the sorting pass and the refinement as pass.

Peak signal-to-noise ratio, often abbreviated **PSNR**, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very extensive dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression). The signal in this

case is the original data, and the noise is the error introduced by compression. When comparing compression codecs, PSNR is an *approximation* to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. One has to be extremely careful with the range of validity of this metric; it is only conclusively valid when it is used to compare results from the same codec (or codec type) and same content.

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=1}^{N} \sum_{j=1}^{M} [I(i,j) - I'(i,j)]^2$$

$$\text{PSNR} = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

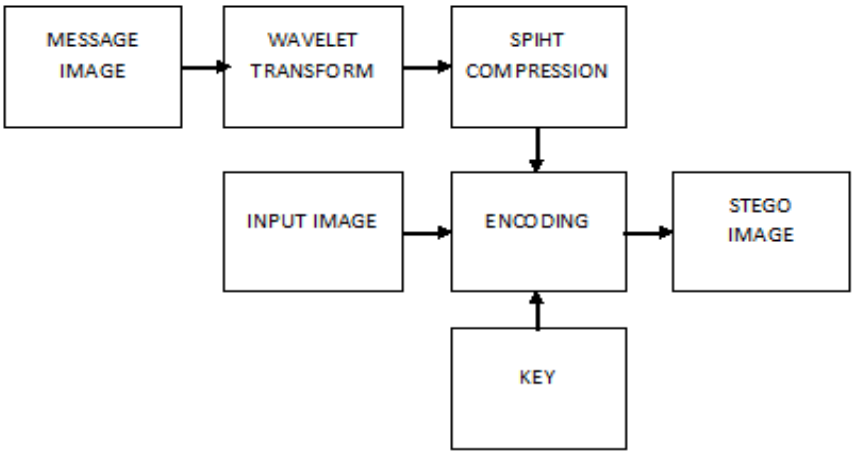
IV. PROPOSED METHOD

The main objective of the proposed system is to hide information image into a cover image of same size as that of the secret image. The paper generally focuses on gaining an efficient embedding capacity. In different steganographic techniques, it is to be noted that the cover images appear in larger sizes. Most often the cover images seems to have twice or four times the size of input secret images. For a high delivery the cover image should be effectively larger to contain the total information. So, proposed method leads to seal the secret data into a cover image of same size however big the secret data is. The proposed technique first compress the message image by using the SPIHT algorithm and then the compressed data is then embed into the cover image using the LSB technique. The compressions is made by the wavelet transform and then compress using the SPIHT coding.

In the repossess side, first the data is decoded using the LSB method and then it is decompressed using the SPIHT algorithm, and then inverse wavelet transform is applied so that we can get the original secret image.

4.1 Block Diagram of Encoding and Decoding

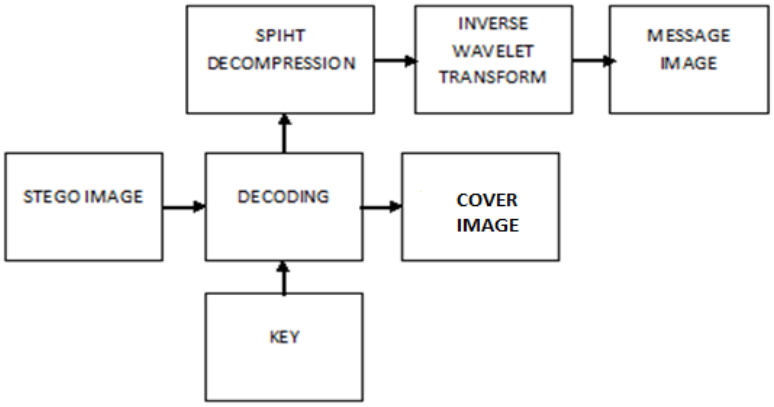
4.1.1 Encoding



SPIHT codes the individual bits of the image wavelet transform coefficients following a bit-plane sequence. Thus, it is capable of improving the image perfectly (every single bit of it) by coding all bits of the transform. However, the wavelet transform yields perfect reconstruction only if its numbers are stored as infinite-precision numbers. In practice it is frequently possible to recover the image perfectly using rounding after recovery, but this is not the most efficient approach.

National Conference on Information, Communication, VLSI and Embedded systems (ICVE 2K16)
(16 - 17 March 2016)
International Journal of Engineering Research & Science (IJOER)
ISSN: [2395-6992] [Vol-2, Issue-3 March- 2016]

4.1.2 Decoding



V. EXPERIMENTAL RESULT

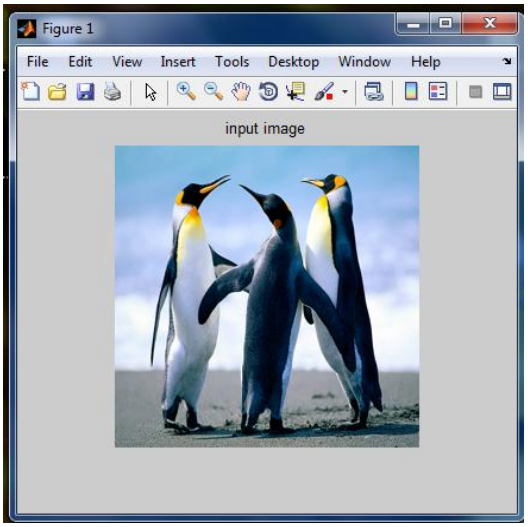


FIG:1. INPUT IMAGE

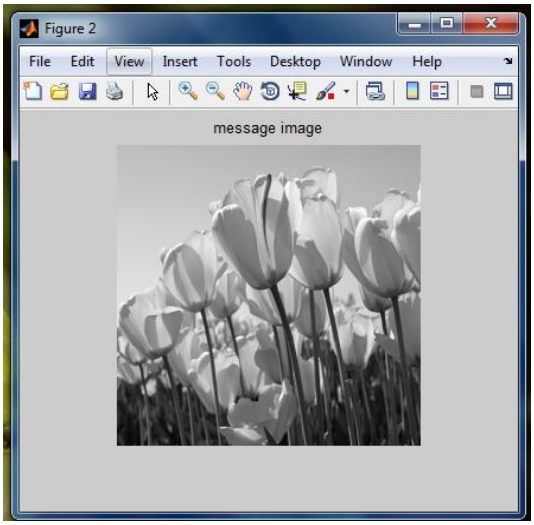


FIG:2. MESSAGE IMAGE

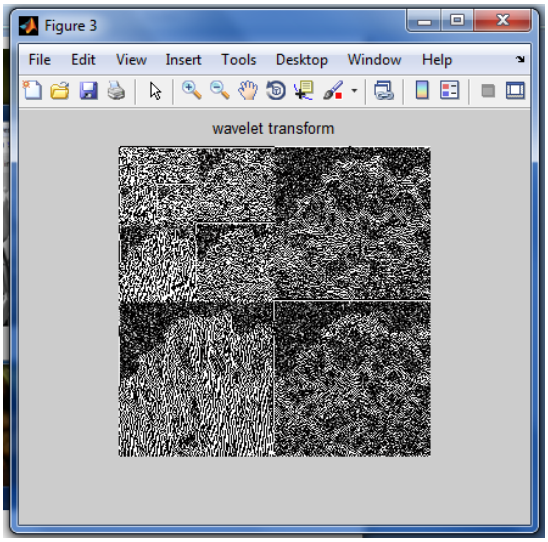


FIG:3. WAVELET TRANSFORM

FIG:4. ENCODED IMAGE

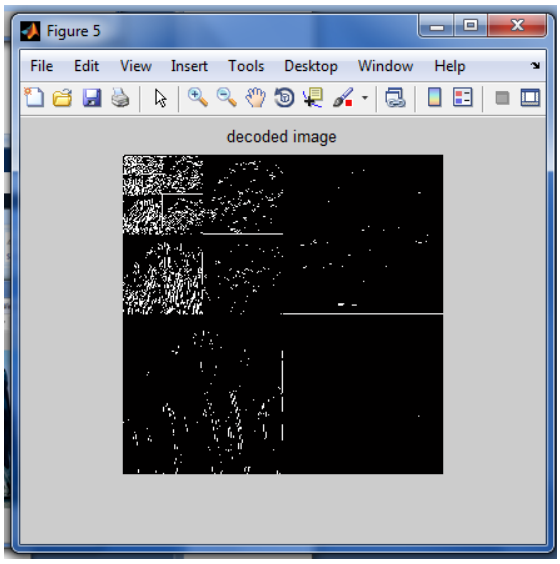


FIG:5. DECODED IMAGE

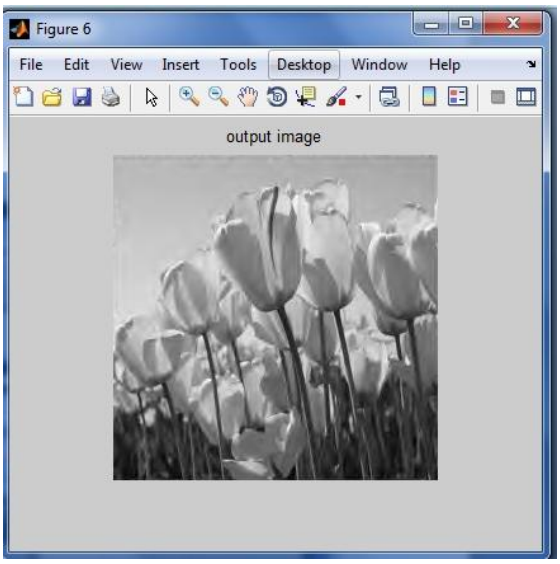


FIG:6. OUTPUT IMAGE

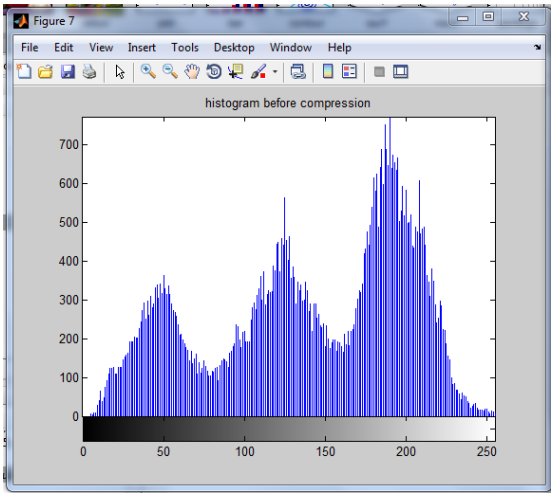


FIG:7. HISTOGRAM BEFORE COMPRESSION

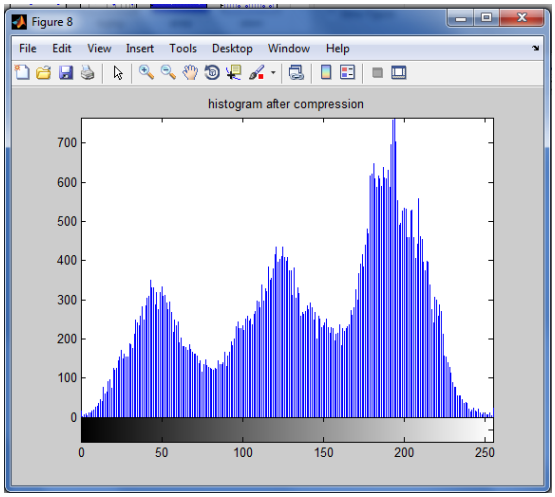


FIG:8. HISTOGRAM AFTER COMPRESSION

TABULATION

S. no	Image	PSNR	MSE
1	Chrysanthemum	25.1	192
2	Desert	25.6	177
3	Hydrangeas	29	80
4	Jelly fish	32.7	35
5	Kola	34.3	24

Any Steganography technique is characterized mainly by two attributes, imperceptibility and capacity. Imperceptibility means the embedded data must be imperceptible to the observer (perceptual invisibility) and computer analysis (statistical invisibility). In this paper we proposed the method of compress image steganography. The input image is compressed using the SPIHT algorithm, which is wavelet based compression method. Then the compressed image is encoded in to the cover image using LSB algorithm. The decoding process is inverse of the encoding which first decode and get the image and then

decompress using SPIHT. Peak Signal to Noise Ratio (PSNR) between the stego image and its corresponding cover image are analyzed.

VI. CONCLUSION

A secured LSB technique for image steganography with compression of message image using SPIHT has been presented in this paper. It proposed a new Steganographic scheme to hide an image into a same sized cover image. The image is compressed into preferred level using SPIHT and is then hidden to the cover image using LSB steganograpy scheme compression. The image resolution doesn't change much and is insignificant when we embed the message into the image and the image is protected with the personal key. Different experiments were conducted on the different size images to authenticate the proposal. Image quality was retained with high PSNR values. Similarity in the Histograms of the Cover and Stego images confirms the closeness of these images. This abides by the objective of our study on Image Steganography.

REFERENCES

[1] Kuo-Chen Wu and Chung-Ming Wang,Steganography Using Reversible Texture Synthesis, IEEE Trans,image processing, Vol. 24, no. 1, January 2015
[2] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," Computer, vol. 31, no. 2, pp. 26–34, 1998.
[3] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," IEEE Security Privacy, vol. 1, no. 3, pp. 32–44,May/Jun. 2003.
[4] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding survey," Proc. IEEE, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.
[5] Y.-M. Cheng and C.-M. Wang, "A high-capacity steganographic approach for 3D polygonal meshes," Vis. Comput., vol. 22, nos. 9–11,pp. 845–855, 2006.
[6] S.-C. Liu and W.-H.Tsai, "Line-based cubism-like image—A new type of art image and its application to lossless data hiding," IEEE Trans.Inf. Forensics Security, vol. 7, no. 5, pp. 1448–1458, Oct. 2012.
[7] I.-C. Dragoi and D. Coltuc, "Local-prediction-based difference expansion reversible watermarking," IEEE Trans. Image Process., vol. 23,no. 4, pp. 1779–1790, Apr. 2014.
[8] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color, and gray-scale images," IEEE MultiMedia, vol. 8, no. 4,pp. 22–28, Oct./Dec. 2001.
[9] Y. Guo, G. Zhao, Z. Zhou, and M. Pietikäinen, "Video texture synthesis with multi-frame LBP-TOP and diffeomorphic growth model," IEEETrans. Image Process., vol. 22, no. 10, pp. 3879–3891, Oct. 2013.
[10] L.-Y. Wei and M. Levoy, "Fast texture synthesis using tree-structured vector quantization," in Proc. 27th Annu. Conf. Comput. Graph.Interact.Techn., 2000, pp. 479–488.
[11] A. A. Efros and T. K. Leung, "Texture synthesis by non-parametric sampling," in Proc. 7th IEEE Int. Conf. Comput. Vis., Sep. 1999,pp. 1033–1038.
[12] C. Han, E. Risser, R. Ramamoorthi, and E. Grinspun, "Multiscale texture synthesis," ACM Trans. Graph., vol. 27, no. 3, 2008, Art. ID 51.
[13] H. Otori and S. Kuriyama, "Data-embeddable texture synthesis," in Proc.8th Int. Symp. Smart Graph., Kyoto, Japan, 2007, pp. 146–157.
[14] H. Otori and S. Kuriyama, "Texture synthesis for mobile data communications,"IEEEComput.Graph. Appl., vol. 29, no. 6, pp. 74–81,Nov./Dec. 2009.
[15] M. F. Cohen, J. Shade, S. Hiller, and O. Deussen, "Wang tiles for image and texture generation," ACM Trans. Graph., vol. 22, no. 3, pp. 287–294,2003.
[16] K. Xuet al., "Feature-aligned shape texturing," ACM Trans. Graph.,vol. 28, no. 5, 2009, Art. ID 108.
[17] L. Liang, C. Liu, Y.-Q.Xu, B. Guo, and H.-Y. Shum, "Real-time texture synthesis by patch-based sampling," ACM Trans. Graph., vol. 20, no. 3,pp. 127–150, 2001.
[18] A. A. Efros and W. T. Freeman, "Image quilting for texture synthesis and transfer," in Proc. 28th Annu. Conf. Comput. Graph. Interact. Techn.,2001, pp. 341–346.
[19] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding,"IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362,Mar. 2006.
[20] X. Li, B. Li, B. Yang, and T. Zeng, "General framework to histogramshifting-based reversible data hiding," IEEE Trans. Image Process.,vol. 22, no. 6, pp. 2181–2191, Jun. 2013.
[21] J. L. Rodgers and W. A. Nicewander, "Thirteen ways to look at the correlation coefficient," Amer. Statist., vol. 42, no. 1, pp. 59–66, 1988.