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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 2, March 2016

4th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '16)

10th-11th March 2016

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

SPIHT Based Compression Image Steganography Using LSB Encoding Method

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

PG Scholar, Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India[1]

Professor, Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India[2]

ABSTRACT: Steganography is came from the Greek word steganographic which means covered writing. It is the science of secret communication. steganography is used to hide the existence 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 major concern and thus data hiding technique has attracted people around the globe. Steganography techniques are used to address digital copyrights management, protect information, and conceal secrets. Data hiding techniques provide an interesting challenge for digital forensic investigators. Data is the backbone of today's communication. To ensure that data is secured and does not go to unintended destination, the concept of data hiding came up to protect a piece 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 confidentiality and data integrity are required to protect against unauthorized access and use. Steganography and cryptography are two different information hiding techniques, where we transform the message so as to make it meaning obscure to a malicious people who intercept it. Steganography relies on hiding message in unsuspected multimedia data and is generally used in secret communication between acknowledged 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 significantly 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 degree of redundancy are more suitable. The redundant bits of an object are those bits that can be altered without the alteration being detected easily

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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 2, March 2016

4th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '16)

10th-11th March 2016

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

II. OVERVIEW OF STEGANOGRAPHY

Types of Steganography

1.Text steganography: It consists of hiding 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.Image steganography:Hiding the data by taking 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 widely used cover source because there are number of bits presents in digital representation of an image. 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.

III. RESEARCH METHODOLOGY

3.1 LSB ALGORITHM

LSB (Least Significant Bit) substitution 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 8th bit of each byte of the image is changed 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:

$$S_n(T) = \begin{cases} 1, max_{(i,j)\epsilon T}\{|c_{i,j}|\} \geq 2^n| \\ 0, Otherwise \end{cases}$$

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 refinementas 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 wide 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.

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

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

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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 2, March 2016

4th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '16)

10th-11th March 2016

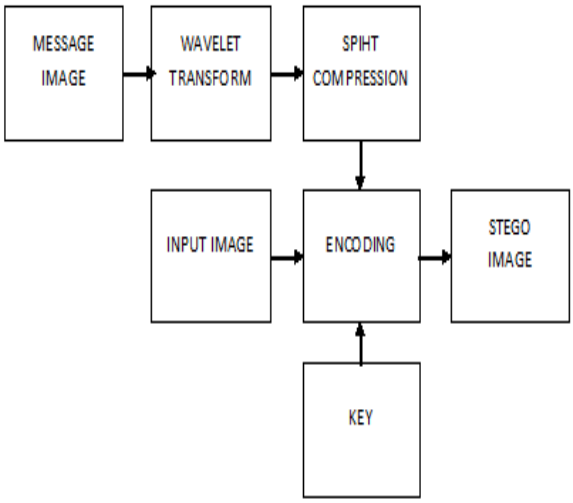
Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

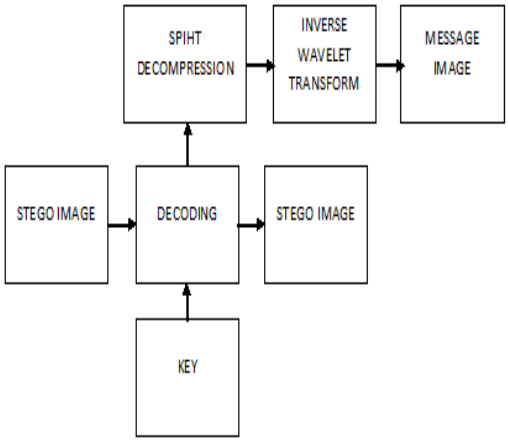
IV. PROPOSED METHOD

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 compression is made be the wavelet transform and then compress using the SPIHT coding.

BLOCK DIAGRAM OF ENCODING AND DECODING
ENCODING



DECODING



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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 2, March 2016

4th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '16)

10th-11th March 2016

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

SPIHT codes the individual bits of the image wavelet transform coefficients following a bit-plane sequence. Thus, it is capable of recovering 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.

V. EXPERIMENTAL RESULT

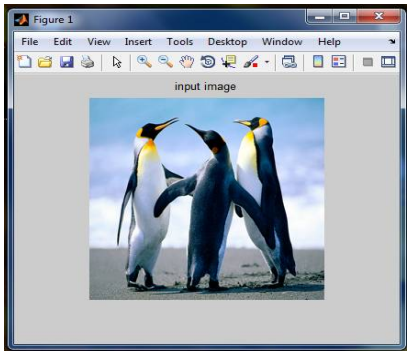


Fig:1.Input image

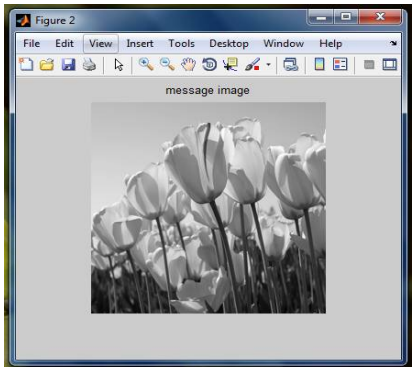


Fig:2.Message image

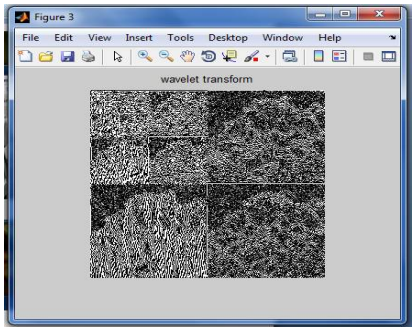


Fig:3.Wavelet transform

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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 2, March 2016

4th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '16)

10th-11th March 2016

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

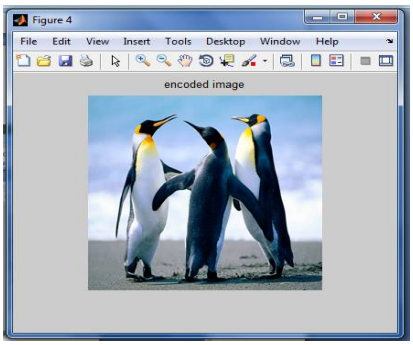


Fig:4.Encoded image

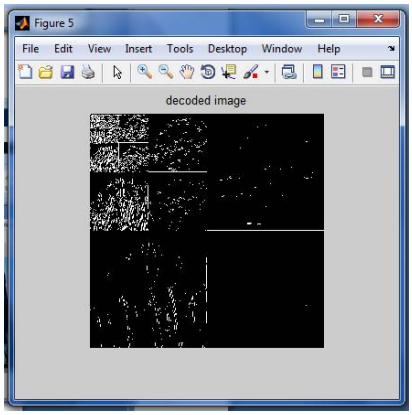


Fig:5.Decoded image

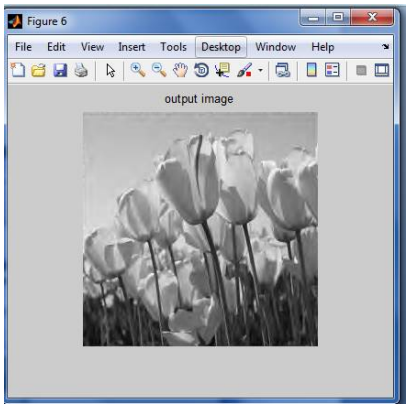


Fig:6.Output image

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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 2, March 2016

4th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '16)

10th-11th March 2016

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

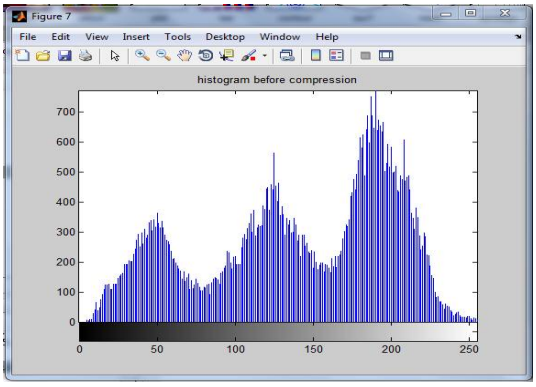


Fig:7.Histogram before compression

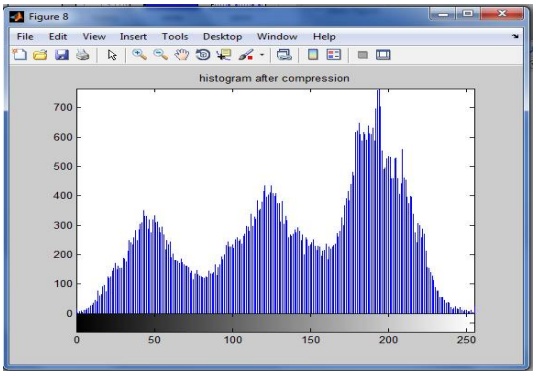


Fig:8.Histogram after compression

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). 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 desired 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 negligible 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 validate 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] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," Computer, vol. 31, no. 2, pp. 26–34, 1998.

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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 2, March 2016

4th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '16)

10th-11th March 2016

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

[2] 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.
[3] 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.
[4] 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.
[5] 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.
[6] 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.
[7] 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.