ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Efficient Data Hiding Scheme Using Image Steganography

Nitesh H. Shenare

M.E Student (VLSI and Embedded System), DPCOE, Savitribai Phule Pune University, Pune, India

ABSTRACT: Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. OR Stenography is an art of secret communication. It is sub discipline of information hiding that focuses on concealing the existence of messages. In this paper this is to develop an algorithm to embed secret message in the form of Text, Image, Audio and Video into a cover (host) image without causing significant perceptual distortion in the stego-image. Further the objective is to extract the embedded secret message from the stego- image without loss of information. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. The carrier image file is taken to hide the data. The carrier file contains LSB bits. Some of the bits the carrier file is replaced by secured data file. The operation of recovering data is done in similar manner. The steganography hides the file data to give more security.

KEYWORDS: Steganography, Image processing, LSB (Least Significant Bit)

I. INTRODUCTION

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity or Stenography is an art of secret communication. It is a sub discipline of information hiding that focuses on concealing the existence of messages. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Encryption remains the primary method used to protect information in the event it is accessed or obtained illegally. It involves encrypting the vital information into an undecipherable form. Only a recipient with the correct key will be able to decipher the information. The downside of encryption is that is immediately apparent to anyone acquiring the file that there is hidden information within the file. Another option is steganography. Rather that encrypting the information, it is hidden inside another, apparently innocuous file. The benefit of this method is that someone acquiring the file might not even know that there is valuable information contained within it. As the world becomes more anxious about the use of any secret communication, and as regulations are created bygovernments to limit uses of encryption, steganography role is gaining prominence.

We could think of steganography as a form of robust encryption. It attempts to hide the message in such a way that the observer may not even realize that the message is being exchanged. Unlike encryption, steganography cannot be detected. Often, steganography is used to supplement encryption. Through its combination of encryption and invisibility of the encrypted data it keeps the message completely protected form data espionage.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

II. LITERATURE SURVEY

A. *Steganography*

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message; this is in contrast to Cryptography, where the existence of the message itself is not disguised, but the meaning is obscured. "Steganography" is a Greek word and means 'covered or hidden writing'. Its origins can be traced back to 440 BC. Steganography has been widely used in historical times, especially before crypto graphical systems were developed.

There are various methods in steganography text in image, text in audio and video. The Fig. 1 shows the standard steganography operation on the different-different file format.

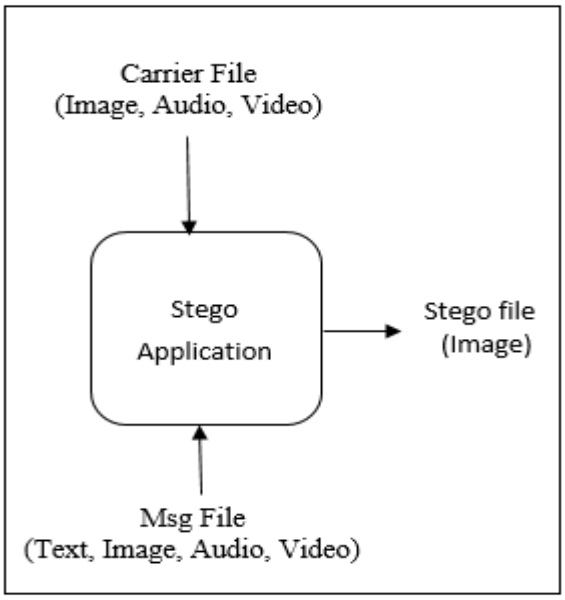


Fig. 1 Standard Steganography Method.

B. *Types*

There are basically two types of steganography

1. Physical Steganography

Physical Steganography includes message written on an element and another element covers that message. For example Demaratus used the wooden plate with covering of wax on it. There are other steganography examples like some kings used the message written in tattoo on head and then cover head with hair and on recovery side shaved head. Modern day's steganography is done on glass.

2. Digital Steganography

In this kind of steganography data in digital format is hidden. There are several techniques to do this like LSB steganography, compression based steganography.

Steganography can be done in different domains. Time domain is one of the common domains used for steganography. Time domain steganography is usually simple and fast.

C. Image steganography

Image files are probably the most common medium for hiding files. Most of the stego techniques that use image files involve manipulation of the image's colour tables.

8-bit images use a colour table of 256 RGB values. Each pixel is represented by a byte, which is then used to pick out the pixel's RGB value from the colour table. In order to hide data in 8-bit images, S-Tools modifies the image to only use a 32-colour palette instead of 256. These 32 colours are duplicated 8 times in order to fill the colour table. The duplicate entries are then used to store the secret message in the three least significant bits for each RGB entry. This all means that each colour in the modified image can be represented in eight different ways, which leaves redundant representations in which information can be hidden.

Image Steganography algorithms exploit the limited powers of Human Visual System (HVS), to embed data in images. Psycho visually, human do not react very promptly and sharply to very small changes in what we see. This relative insensitivity and the versatility of today's digital multimedia can be exploited to make small changes to make small changes in digital multimedia data without getting noticed.

D. LSB steganography

There are various types of steganography LSB node selection methods. There is modified bit selection algorithm is proposed in research of modified bit steganography. There is another approach proposed in the

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

wave steganography of modifying whole LSB data of all bits. In third approach modification of least bit of MSB is done. Problem in first and third approach is less data can be hidden anddistortion part is increasingrespectively as MSB contains the maximum information of the carrier file.

The LSB technique involves the following steps:-

1. Select pixels of carrier image file.
2. Get the pixel value of each pixel one by one.
3. Replace pixels of carrier image file to input message file.

1. Select pixels of carrier image file.

The process of converting a carrier file into its binary equivalent is explained here. So the contents of the carrier file are converted into its corresponding binary equivalent using the mentioned technique. Also the carrier file may be masked before replacing it in the pixels of the image. The Masking Technique is shown in Fig 3 below. In this technique each byte of the carrier file's binary equivalent is binary ANDed with the binary equivalent of 254. Then the bits are exchanged with the image pixels. This will provide additional security. The masking technique is shown below.

2. Get the pixel value of each pixel one by one.

After masking has been done, each bit of the message file is replaced in the LSB position of the pixels in the image. Here LSB refers to the Least Significant Bit i.e. the last bit of the pixel value. Since only the LSB is changed the difference between the original image and the stego image will be so small, that the difference cannot be detected by human eyes.

3. Replace pixels of carrier image file to input message file.

The LSB technique can also be briefly explained with the help of bits. In Fig. 5 the LSB technique is explained with the help of binary values. As shown in the figure the last bits of the pixels are replaced with the bits of the message file. So the final image will resemble the original image.

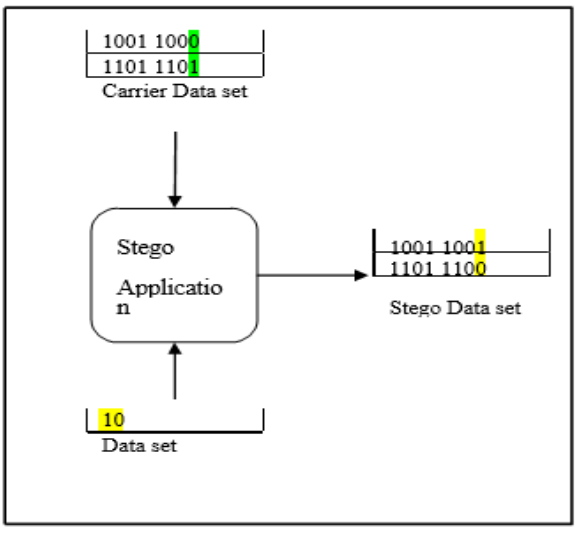


Fig. 2 LSB Steganography Method.

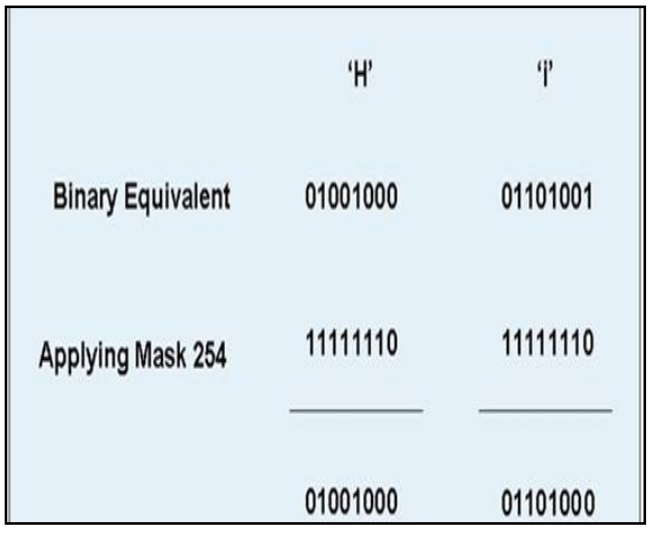


Fig.3 Masking Technique

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

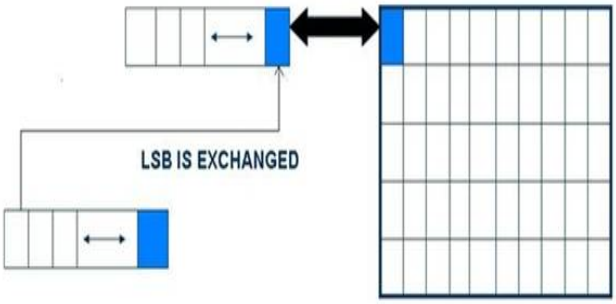


Fig. 4 LSB Technique

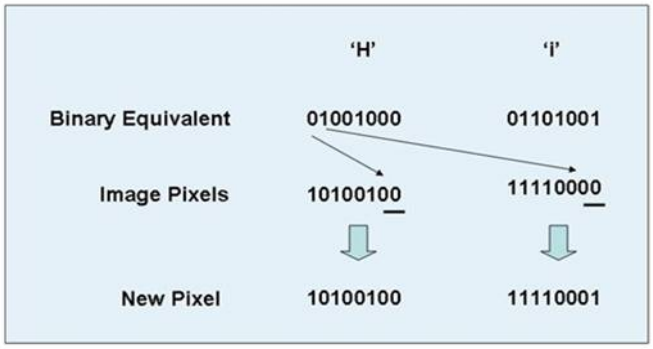


Fig. 5. LSB Technique Illustration

E. Lossy and Lossless Steganography

There are two approaches present to hide data as lossy and lossless. In lossy method, only MSB of data set is hidden in carrier data set where as in the lossless method MSB as well as LSB of data set is hidden in the carrier data set.As shown in Fig. 6 and Fig. 7 the lossy and lossless method can be applied. In lossy method maximum data can be hiddenbut at the time of recovery, some of the data may be lost where as in lossless method percentage of the data hidden is half but the recovery is full.The percentage of data hide in carrier file. This figure shows the difference in lossy and lossless, as lossy uses only MSB of message file which do not require space to store the LSB of message file, whilein lossless there is a requirementto embed data both as MSB as well as LSB of message data.

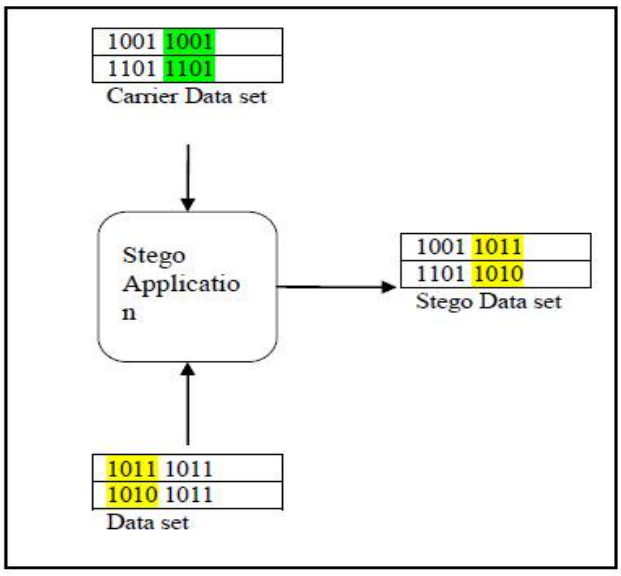


Fig. 6 LSB Lossy Method.

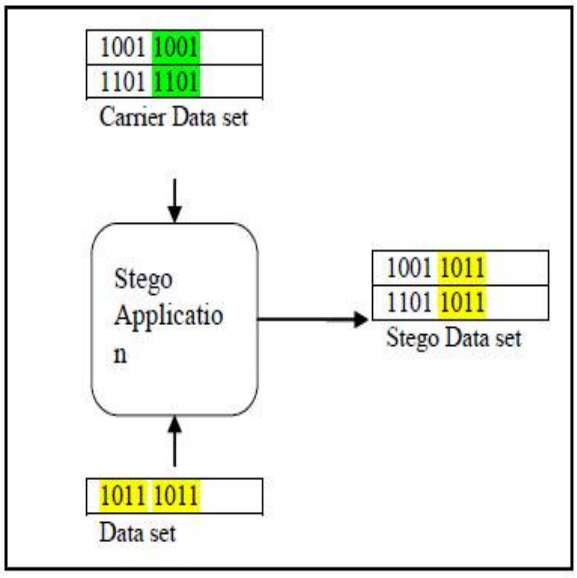


Fig. 7 LSB Lossless Method.

III.STEPS OF IMAGE STEGANOGRAPHY

System uses the following algorithm to hide data in Image file.

Hiding Side:-

Step: 1. Select Image file for hiding data.
Step: 2. Read and open file data for binary read access.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Step: 3. Select pixels of carrier image file.
Step: 4. Select message file to hide.
Step: 5. Read and open file data for binary read access.
Step: 6. Apply LSB lossless steganography at stego applicationBlock.

Recovery Side:-

Step: 1. Select stego file for recovering data.
Step: 2. Read and open file data for binary read access.
Step: 3. Select pixels of stego image file.
Step: 4. Apply recovery stego application.
Step: 5. Recover the message file.

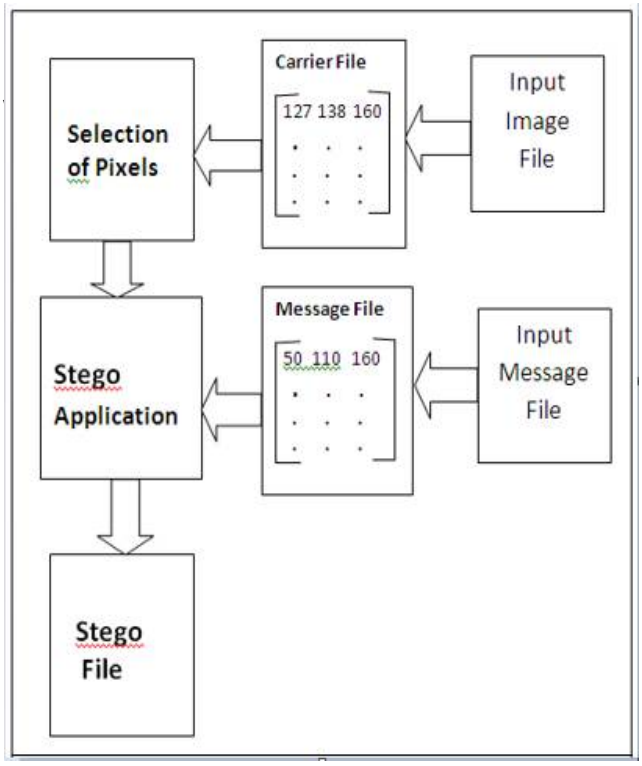


Fig.9 System Architecture of hiding of data

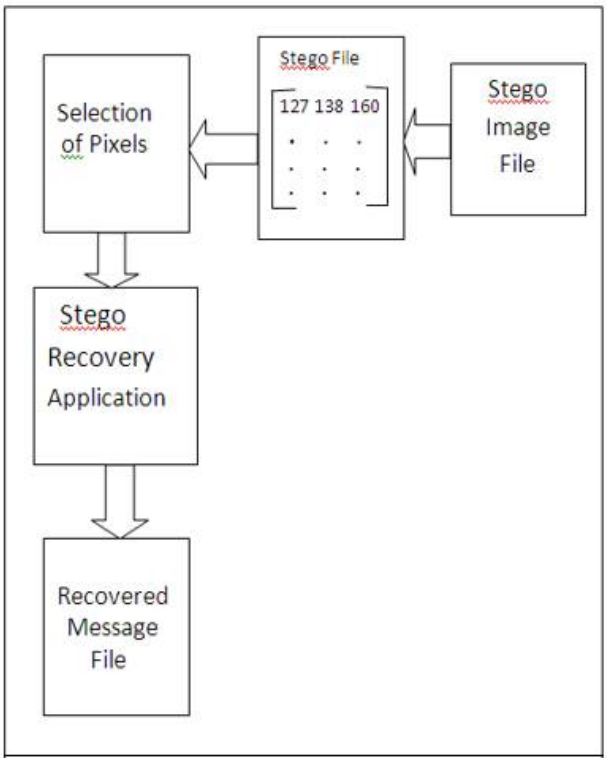


Fig.9 System Architecture of Recovery of data

III. RESULT IMPLEMENTATION

The carrier image file is taken to hide the data. The carrier file contains LSB bits. Some of the bits of the carrier file is replaced by secured data file. The operation of recovering data is done in similar manner. The steganography hides the file data to give more security.

In this project this is to develop an algorithm to embed secret message in the form of Text, Image, Audio and Video into a cover (host) image without causing significant perceptual distortion in the stego-image. Further the objective is to extract the embedded secret message from the stego- image without loss of information.

The carrier image file is taken to hide the data. The carrier file contains LSB bits. Some of the bits the carrier file is replaced by secured data file. The operation of recovering data is done in similar manner. The steganography hides the file data to give more security.

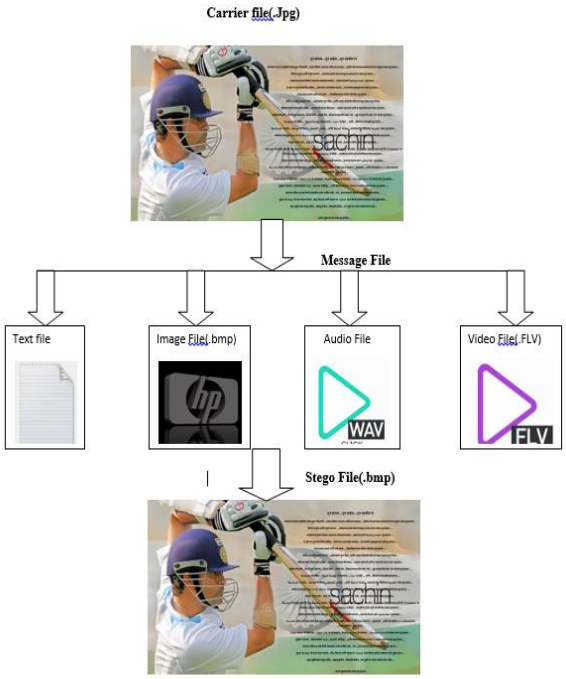
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

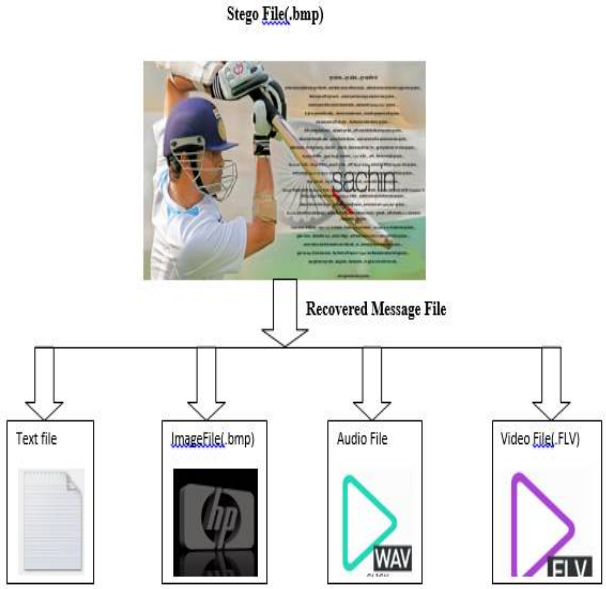
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Hiding Operation:-



Recovery Operation:-



IV. CONCLUSION

Steganography has its place in security. Hiding message with steganography methods reduces the chance of a message being detected. We could think of steganography as a form of robust encryption. It attempts to hide the message in such a way that the observer may not even realize that the message is being exchanged.

Paper present an effective steganography method on LSB technique. This Method replaces the least significant bits according to the Percentage of the data to be hidden. This method has high capacity for hiding data. Another advantage of the technique is that the hidden information is extracted by methods lossless and lossy.

The paper introduces a tiny part of the art of steganography. Steganography goes well beyond simply hiding text information in an image. Steganography applies not only to digital images but to other media as well, such asAudio files, communication channels, and other text and binary files.

REFERENCES

1. Jagtap V.G., Prof. Pande S.S., Dr. Parag Kulkarni,Intelligent Silhouette Wave Steganography (I-SiWaS), CiiT International Journal of Artificial Intelligence Systems and Machine Learning: Issue: January 2013, DOI: AIML012013003
2. Los Alamos Nat. Lab., NM, “Digital steganography: hiding data within data”, Internet Computing, IEEE, May/Jun 2001, Volume: 5, Issue:
3. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, “Secure spreadspectrum watermarking for images, audio and video,” in Proc. IEEE Int.Conf. Image Processing, Lausanne, Switzerland, Sept. 1996, vol. 111, pp.243-246.
4. Xinpeng Zhang, “Separable Reversible Data Hiding in Encrypted Image”, IEEE TRANSACTIONS ON INFORMATION FORENSICSAND SECURITY, VOL. 7, NO. 2, APRIL 2012.
5. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, vol. 35, issue 3-4, September 1996, pp.313-336.
6. I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for images, audio and video,” in Proc. IEEE Int. Conf. Image Processing, Lausanne, Switzerland, Sept. 1996, vol. 111, pp.243-246.
7. L. Gang, A.N. Akansu, and M. Ramkumar, "MP3 resistant oblivioussteganography," Proceedings of 2001 IEEE International Conference onAcoustics, Speech, and Signal Processing (ICASSP'01), May 2001 vol.3,pp. 1365-1368.
8. Y. Linde, A. Buzo, R. M. Gray, “An Algorithm for Vector QuantizerDesign”, IEEE Trans. on Communications, Vo1.28, [7] N. M. Nasrabadiand R. A. King, “Image coding using vector quantization: A review”,IEEE Trans. Commun., vol. 36, pp. 84-95, 1980.
9. Xinpeng Zhang, “Separable Reversible Data Hiding in Encrypted Image”, IEEE TRANSACTIONS ON INFORMATION

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

FORENSICSAND SECURITY, VOL. 7, NO. 2, APRIL 2012.

10. Anant Umbarkar, Abhijit Joshi, Ajay Jadhav, "Wave Steganography",2010 IEEE International Conference on Computational Intelligence andComputing Research (ICCIC).
11. K. Gopalan, "Audio steganography by cepstrum although the algorithm isapplicable to other resolution modification," In Proc. IEEE Int. Conf.Acoustics, Speech, levels of wavelet and Signal Processing, Vol. 5, pp.481-484, March 2005.
12. T. Cedric, R. Adi, I. Mcloughlin "Data concealment in audio using anonlinear frequency distribution of PRBS coded data andfrequency-domain LSB insertion", Proc. IEEE Region 10 InternationalConference on Electrical and Electronic Technology, Kuala Lumpur,Malaysia, September 2000, pp. 275-278.

BIOGRAPHY

Mr. Nitesh Havgirao Shenare born in Latur (Maharastra, India) on 5th April1989. He completed his Bachelor ofEngineering (B.E.) in Electronics and Telecommunication (E&TC) fromMarathwada Mitra Mandal College of Engineering, Pune (India), under Pune University, Pune in June 2014. He ispursuing Masters of Engineering (M.E.) in VLSI and Embedded System from DPCOE College (India) under University of Pune.His research areas are Data Security, Computation,and Image Processing.