Open access Journal International journal of Emerging Trends in Science and Technology

# Secure Transmission of Information by LSB Encoding Technique using Audio Steganography and Cryptography

Authors

**Preeti Singh[1], Praveen Yadav[2]**

[1]Rungta College of Engineering and Technology,
CSVTU, Bhilai, Chhattisgarh, India
Email: *Preeti.116singh@gmail.com*
[2]Rungta College of Engineering and Technology,
Department of Electronics and Telecommunication, Chhattisgarh, India
Email: *Ypn.praveen@gmail.com*

**Abstract:**
*In this paper, we deal with Steganography where Steganography is the art and science of communicating in a way which hides the existence of the communication. [1]The goal of steganography is to hide messages inside other harmless message in a way that doesn't allow enemy to even detect that there is second message present. In an audio Steganographic method [2], we can adjust the bits in such a way so that the stego audio signal resulting from embedding data in higher LSB layer is perceptually indistinguishable from the host audio signal. In addition with Steganography, Cryptography has been added to provide more security for the message.*

**Keywords:** *Auditory System (HAS), LSB encoding, Cover Audio, Stego Audio.*

## 1. 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. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information. LSB coding is one of the earliest techniques studied in the information hiding and watermarking area of digital audio (as well as other media types). Here $4^{th}$ bit LSb coding technique is used where $4^{th}$ bit of selected sample is replaced by message bit. Also an adjustment algorithm has been provided which makes the Stego-audio and cover- audio less distinguishable. The main advantage of the LSB coding method is a very high watermark channel bit rate and a low computational complexity of the algorithm and in addition to this provides low quantization noise. The perceptual quality has been improved. Those who want a very secure private communication can combine encryption and Steganography. Encrypted data is more difficult to recognize from naturally occurring phenomena than plain text. There are several tools by which we can encrypt data before hiding it in the chosen medium. In some situations, sending an encrypted message will across suspicion while an invisible message will not do so. Both methods can be combined to produce better protection of the message. In case, when the Steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques.

## 2. Literature Review

Data hiding in the least significant bits (LSBs) of audio samples in the time domain is one of the simplest algorithms with very high data rate of

additional information. The LSB watermark encoder [5] usually selects a subset of all available host audio samples chosen by a secret key. The substitution operation on the LSBs is performed on this subset, where the bits to be hidden substitute the original bit values. Extraction process simply retrieves the watermark by reading the value of these bits from the audio stego object. Therefore, the decoder needs all the samples of the stego audio that were used during the embedding process. The random selection of the samples used for embedding introduces low power additive white Gaussian noise (AWGN) [6]. It is well known from the psychoacoustics literature that the human auditory system (HAS) is highly sensitive to AWGN. That fact limits the number of LSBs that can be imperceptibly modified during watermark embedding. The main advantage of the LSB coding method is a very high watermark channel bit rate; use of only one LSB of the host audio sample gives capacity of 44.1 kbps (sampling rate 44 kHz, all samples used for data hiding) and a low computational complexity. The obvious disadvantage is considerably low robustness, due to fact that simple random changes of the LSBs destroy the coded watermark. As the number of used LSBs during LSB coding increases or, equivalently, depth of the modified LSB layer becomes larger, probability of an easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it. Making the embedded message statistically detectable increases and perceptual transparency of stego objects is decreased. Therefore, there is a limit for the depth of the used LSB layer in each sample of host audio that can be used for data hiding [7]. Subjective listening test showed that, in average, the maximum LSB depth that can be used for LSB based watermarking without causing noticeable perceptual distortion is the fourth LSB layer when 16 bits per sample audio sequences are used. The tests were performed with a large collection of audio samples and individuals with different background and musical experience. None of the tested audio sequences had perceptual artifacts when the fourth LSB has been used for data hiding although in certain music styles, the limit is even higher than the fourth LSB layer. Robustness of the watermark, embedded using the LSB coding method, increases with increase of the LSB depth used for data hiding. Therefore, improvement of watermark robustness obtained by increase of depth of the used LSB layer is limited by perceptual transparency bound, which is the fourth LSB layer for the standard LSB coding algorithm.

## 3. Audio Steganography and Cryptography

Audio steganographic system is characterized by three features viz. transparency, capacity and robustness. While modification, the transparency of the signal gets distorted. Perceptual transparency is defined as inaudibility of distortion in cover audio file. The perceptual distortion caused due to embedding should be below the masking threshold value estimated based on the HAS and the host media [1].

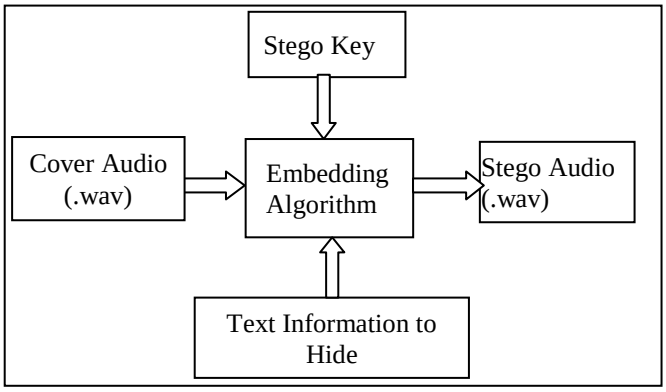


**Figure 1**: Basic principle of Audio Steganography (Embedding)

When hiding information inside Audio files the technique usually used is **low bit encoding** which is somewhat similar to LSB that is generally used in Images. The problem with low bit encoding is that it is usually noticeable to the human ear, so it is a rather risky method for someone to use if they are trying to mask information inside of an audio file. In this paper, a novel method that is able to shift the limit for transparent data hiding in audio from the 1st LSB layer to the fourth LSB layer, using a two-step approach. In the first step, a watermark bit is embedded into the $4^{th}$ LSB layer of the host audio using a novel LSB coding method. In the second step, the impulse noise caused by watermark embedding is shaped in order to change its white noise properties.

The major task of the audio steganography is to provide the user the flexibility of passing the information implementing the algorithms proposed and store the information in a form that is undetectable. This Application has a reversal

process, which is used to de-embed the data file from audio file and convert the data to its original format upon the proper request by the user.

The Fig.2 is the basic block diagram of the extraction process. The information to be embedded into the LSB layer has been extracted using the same Stego key and using the same algorithm.

The embedding and extraction uses the shares the same keys.

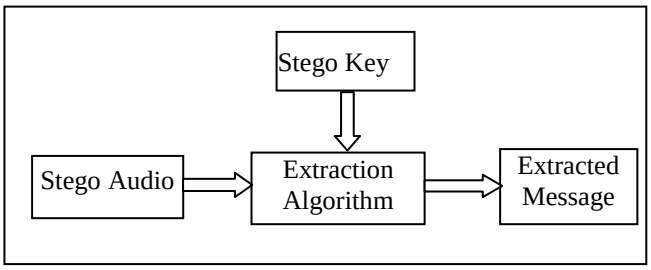


**Figure 2:** Basic principle of Audio Steganography (Extraction)

The above were the steganography embedded and extraction method by which one can hide and extract the data using proposed algorithm. Before hiding, the data can be encrypted using symmetric key cryptography and same can be decrypted at the receiver side using the same key. This method of hiding and encrypting provides greater security in data transmission. Cryptography is the study of methods of sending messages in distinct form so that only the intended recipients can remove the disguise and read the message. The message we want to send is called Plain text & the disguised message is called Cipher text. The process of converting the plain text into cipher text is called Enciphering/Encryption whereas the process of converting the cipher text into plain text is called Deciphering/ Decryption. [5]

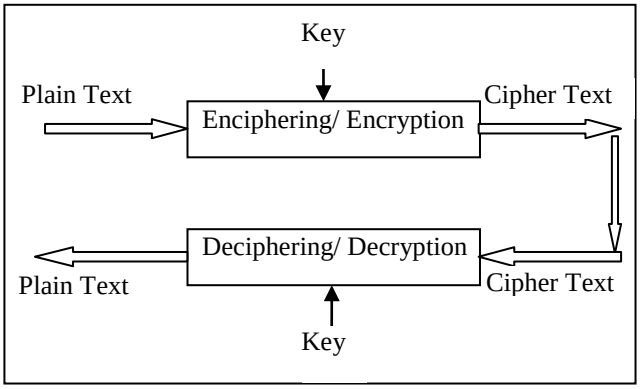


**Figure 3:** Symmetric Key Cryptography

Encryption protects contents during the transmission of data from the sender to receiver. However after receipt and decryption, the data is no longer protected and is clear. Steganography hides messages rather than encrypting the message, it is embedded in the data (that has to be protected) and doesn't require secret transmission. The message is carried inside data. Symmetric cryptography has been used here as sharing the same key for encryption and decryption purposes shown in Figure 3.

## 4. Proposed Methodology

**Data Hiding**

1. Select Audio Wave file.
2. Select Key File.
3. Select Secrete data.
4. Encrypt Secrete data using Symmetric key cryptography.
5. Select audio Samples as per key file content.
6. Hide encrypted data in selected audio samples.
7. Save Audio Data.

**Data Extraction**

1. Select Audio File.
2. Select Key file.
3. Extract data (Encrypted).
4. Decrypt Data.
5. Save Data.

### 3.1 Proposed LSB Method for Hiding

We developed a novel method that is able to shift the limit for transparent data hiding in audio from the fourth LSB layer to the sixth LSB layer, using a two-step approach. In the first step, a watermark bit is embedded into the I $^{th}$ LSB layer of the host audio using a novel LSB coding method. In the second step, the impulse noise caused by watermark embedding is shaped in order to change its white noise properties. The standard LSB coding method simply replaces the original host audio bit in the I $^{th}$ layer (i=1, 16) with the bit from the watermark bit stream. In the case when the original and watermark bit are different and I th LSB layer is used for embedding the error caused by watermarking is 2^i-1 quantization steps (QS) [9] (amplitude range is [-32768 to 32767]). The embedding error is positive if the original bit was

0 and watermark bit is 1 and vice versa. The key idea of the proposed LSB algorithm is watermark bit embedding that causes Minimal embedding distortion of the host audio. It is clear that, if only one of 16 bits in a sample is fixed and equal to the watermark bit, the other bits can be flipped in order to minimize the embedding error [10].

**Algorithm Working:**

If host sample a>0
If bit 0 is to be embedded
If $a_{i-1}$ =0 then $\underline{a}_{i-1}\underline{a}_{i-2}$-----$\underline{a}_0$ = 11....1
If $a_{i-1}$ =1 then $\underline{a}_{i-1}\underline{a}_{i-2}$-----$\underline{a}_0$ = 00....0
If $a_{i+1}$ =0 then $\underline{a}_{i+1}$ =1
Elseif $a_{i+2}$ =0 then $\underline{a}_{i+2}$ = 1
.....
Elseif $a_{15}$ =0 then $a_{15}$ =1
Else if bit 1 is to be embedded
If $a_{i-1}$ =1 then $\underline{a}_{i-1}$ $\underline{a}_{i-2}$ ----- $\underline{a}_0$ =00....0
If $a_{i-1}$ = 0 then $\underline{a}_{i-1}$ $\underline{a}_{i-2}$ ----- $\underline{a}_0$ = 11.....1 and
If $a_{i+1}$ = 1 then $\underline{a}_{i+1}$ =0
Else if $a_{i+2}$ =1 then $\underline{a}_{i+2}$ = 0
.....
Else if $a_{15}$ =1 then $a_{15}$ =0
Else if bit 1 is to be embedded
If host sample a<0
If bit 0 is to be embedded
If $a_{i-1}$ =0 then $\underline{a}_{i-1}$ $\underline{a}_{i-2}$ ----- $\underline{a}_0$ = 11....1
If $a_{i-1}$ =1 then $\underline{a}_{i-1}\underline{a}_{i-2}$-----$\underline{a}_0$ = 00....0 and
If $a_{i+1}$ =0 then $\underline{a}_{i+1}$ =1
Else if $a_{i+2}$ =0 then $\underline{a}_{i+2}$ = 1
.....
Else if $a_{15}$ =0 then $a_{15}$ =1
Else if bit 1 is to be embedded
If $a_{i-1}$ =1 then $\underline{a}_{i-1}\underline{a}_{i-2}$-----$\underline{a}_0$ =00....0
If $a_{i-1}$ =0 then $\underline{a}_{i-1}\underline{a}_{i-2}$-----$\underline{a}_0$ = 11.....1
If $a_{i+1}$ =1 then $\underline{a}_{i+1}$ =0
Elseif $a_{i+2}$ =0 then $\underline{a}_{i+2}$ = 1
.....
Elseif $a_{15}$ =1 then $a_{15}$ =0
Else if bit 1 is to be embedded

For example, if the original sample value was 0...010002=810, and the watermark bit is zero is to be embedded into 4th LSB layer, instead of value 0...000002=010, that would the standard algorithm produce, the proposed algorithm produces sample that has value 0...001112=710, which is far more closer to the original one.

However, the extraction algorithm remains the same; it simply retrieves the watermark bit by reading the bit value from the predefined LSB layer in the watermarked audio sample. In the embedding algorithm, the (i+1) $^{th}$ LSB layer (bit $a_i$) is first modified by insertion of the present message bit [11, 12]. Then, the algorithm given below is run. In case that the bit $a_i$ need not be modified at all due to being already at a correct value, no action is taken with that signal sample. Underlined bits ($a_i$) represent bits of watermarked audio.

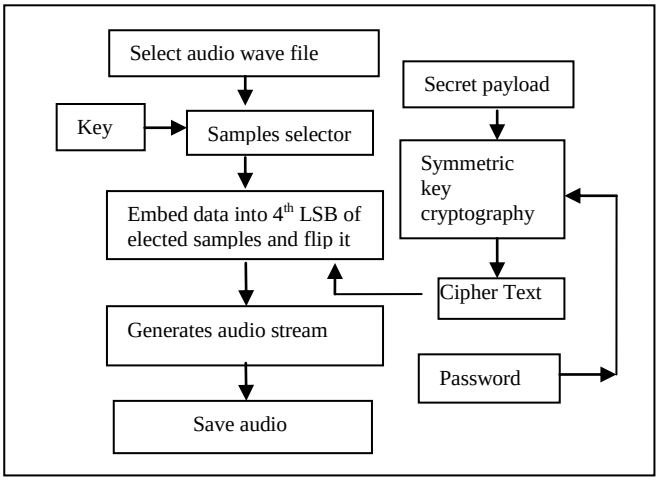


**Figure 4**: Data Hiding

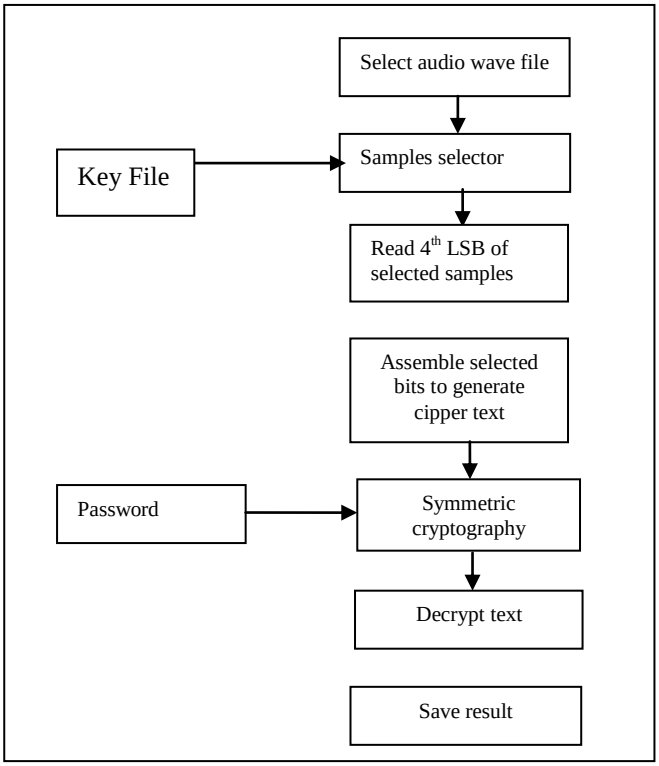


**Figure 5:** Data Extraction

## 5. Result and Discussions

The proposed technique has been implemented, tested and verified. During testing we consider large target messages and successfully hide those in an audio file without create any detectable

perception of human being. But here for better understanding we show the results of our technique using a message file hidden within an audio clip.

Firstly we choose the target message and the cover audio file. (.wav file)

### 5.1 Input Wave Segment of the cover audio:

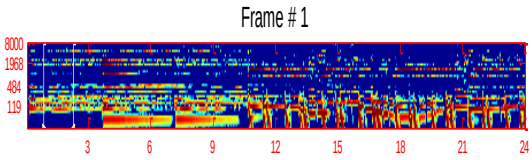


**Figure 6:** Wave Segment (cover Audio)

Due to large cover audio the total file has been divided into segments. Here it has been divided into two segments whose power spectrum, Fourier transforms and sound spectrum has shown below in the following figures.

### 5.2 Power Spectrum of Input Wave Segment:

The power spectrum of one of the segment of input carrier audio is as shown in figure 7.

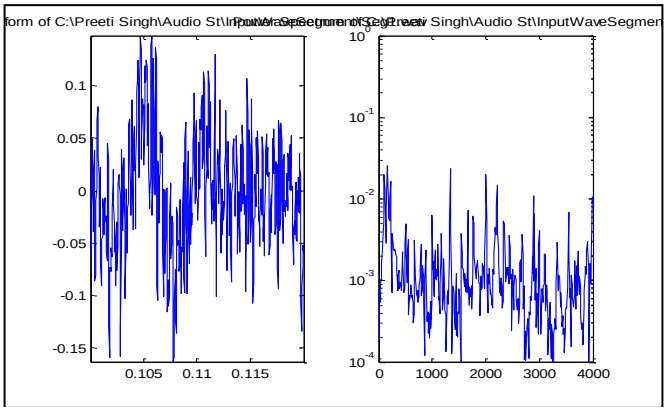


**Figure 7:** Power Spectrum of cover Audio

### 5.3 Fourier Transform of Input Wave Segment:

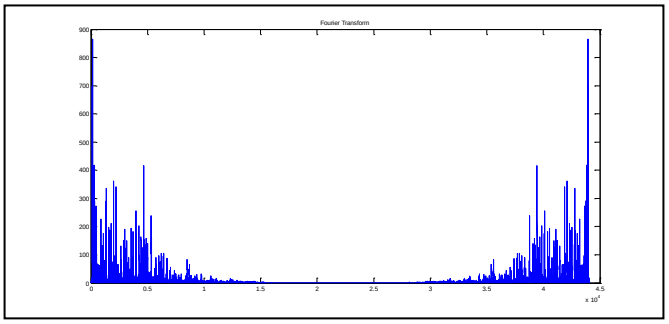

**Figure 8:** Fourier Transform (Cover Audio)

### 5.4 Sound Spectrum of Input Wave Segment:

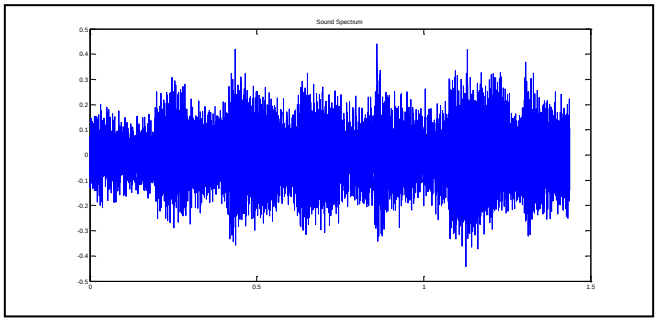

**Figure 9:** Sound Spectrum (cover audio)

The sound spectrum of one of the segment of segmented cover audio is shown in figure 9.

### 5.5 Result Wave Segment of the Stego File

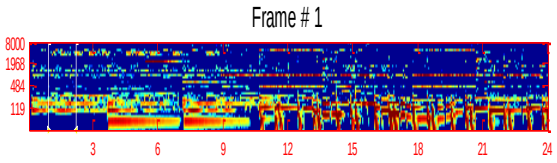


**Figure 10:** Wave Segment (Stego-Audio)

Due to large Stego or resultant audio, the whole file has been divided into segments.

### 5.6 Power Spectrum of Result Wave Segment:

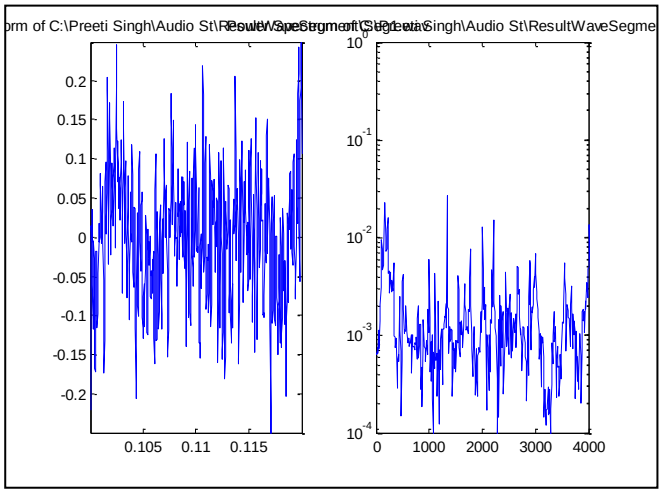


**Figure 11:** Power Spectrum (Stego-Audio)

The power spectrum of one of the segment of segmented stego audio is as shown in figure 11.

### 5.7 Fourier Transform of Result Wave Segment:

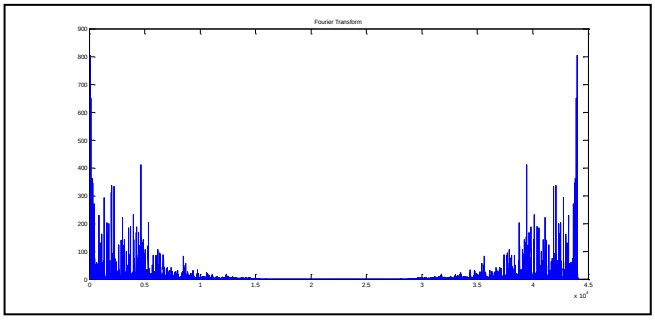

**Figure 12:** Fourier Transform (Stego-Audio)

### 5.8 Sound Spectrum of Result Wave Segment:

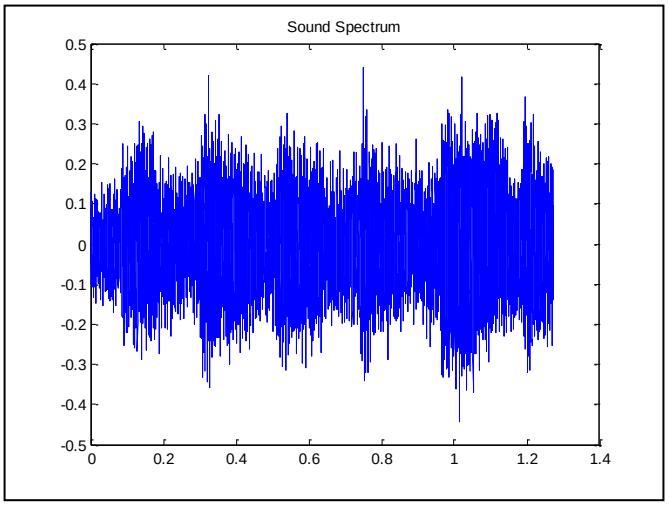


**Figure 12:** Sound Spectrum (Stego audio)

Experimental results indicate that our proposed watermarking system shows strong imperceptibility against several kinds of attacks such as noise accumulation, cropping, re-sampling, re-quantization, and MP3 density and achieves similarity values ranging from 95 to 99. Here the achieved similarty factor between cover audio and stego audio is 99.

## 6. References

[1] Jangra, Taruna, and Dinesh Singh. "Message guided random Audio Steganography using Modified LSB Technique" INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY 12.5 (2014): 3464-3469.

[2] Anderson and Petitcolas 2001 Anderson, R; Petitcolas, F.: On the limits of the steganography, IEEE Journal Selected Areas in Communications, Volume 16(4), Page(s) 4,474-481.

[3] Bassia June 2001 Bassia; P., Pitas, I; Nikolaidis, N.: Robust audio watermarking in the time domain, IEEE Transactions on Multimedia, Volume 3, Issue 2, Page(s):232 – 241.

[4] Cedric 2000 Cedric, T.; Adi, R.,Mcloughlin, I.: Data concealment in audio using a nonlinear frequency distribution of PRBS coded data and frequency-domain LSB insertion, Proc. IEEE Region 10 International Conference on Electrical and Electronic Technology, Kuala Lumpur, Malaysia, pp 275-278

[5] Dumitrescu 2002 Dumitrescu, S.; Wu, W; Memon, N.: On steganalysis of random LSB embedding in continuous-tone images, Proc. International Conference on Image Processing, Rochester, NY, pp 641-644.

[6] Fridrich 2002 Fridrich; J., Goljan; M., Du, R.:Lossless Data Embedding New Paradigm in Digital Watermarking, Applied Signal Processing, 2002, 2, pp 185-196

[7] Lee and Chen 2000 Lee; Y., Chen : High capacity image steganographic model, IEEE Proceedings on Vision, Image and Signal Processing, 147, 3, pp 288-294.

[8] Mintzerl ; Mintzer, F.; Goertzil, G.; Thompson, G.; "Display of images with calibrated colour on a system featuring monitors with limited colour palettes", Proceeding. SID International Symposium, pp 377-380;1988.

[9] Mobasseri 1998] Mobasseri, B.: Direct sequence watermarking of digital video using m-frames, Proceeding International Conference on Image Processing, Chicago, IL, pp 399- 403.

[10] [Yeh and Kuo 1999] Yeh, C., Kuo, C.: Digital Watermarking through Quasi m-Arrays, Proc. IEEE Workshop on Signal Processing Systems, Taipei, Taiwan, 456-461. [Zwicker 1982] Zwicker, E.: Psychoacoustics, Springer Verlag, Berlin, Germany.

[11] Ahuja, B.; Kaur, M., "High Capacity Filter Based Steganography", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, 2009

[12] Maitra, I. K.; Nag, S.; Datta, B.; Bandyopadhyay, S. K., "Digital Steganalysis: Review on Recent Approaches", Journal of Global Research in Computer Science, Vol. 2, No. 1, 2011

[13] Mohammed, A. F., "Image Steganography by

Mapping Pixels to Letters", Journal of Computer Science 5 (1): pp. 33-38, 2009

[14] David, K., "The History of Steganography", Proc. of First Int. Workshop on Information Hiding, Cambridge,UK, May30-June1 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson (Ed.), pp.1-7

[15] Bender, W.; Gruhl, D.; Morimoto, N.; Lu, A., "Techniques for data hiding", IBM Systems Journal, vol. 35, Issues 3&4, 1996, pp. 313-336.

[16] Kharrazi, M.; Sencar, H. T.; Memon, N., "Image Steganography: Concepts and Practice", WSPC, April 22, 2004

**Author Profile**

**Preeti Singh** received her B.E. degree in Electronics & Telecommunication Engineering from M.P.Christian College of Engineering & Technology (affiliated to Pt. Ravishankar Shukla University), Raipur in 2008 and pursuing her Mtech degree in Digital Electronics from Rungta College of Engineering & Technology(Affiliated to CSVTU), Bhilai. She is a lecturer in Electronics & Telecommunication department at G.D. Rungta college of engineering & Technology, Bhilai. She has published her one research paper.

**Professor Praveen Yadav** B.E. from SSCET Bhilai, M.Tech(Digital electronics) from RCET Bhilai, assistant professor of Electronics & Telecommunication, RCET, Bhilai, India. His research interests signal processing and communication. He has 6 yrs of experience at the Post-graduate and under-graduate teaching in Chhattisgarh Swami Vivekanand University, Bhilai. He has already got several Academic Distinctions in Degree level/Recognition/Awards from various prestigious Institutes and Organizations. He has published 3 Research papers in International & Indian Journals.