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. 3, Issue 3, March 2015

Digital Watermarking of Audio in Time Domain Multiple Bit Plane based on Chaotic Scrambling

Jeebananda Panda[1], Indu Kumari[2], Nitish Goel[3]

Associate Professor, Department of ECE, Delhi Technological University, Delhi-42, India[1]

UG Student, Department of ECE, Delhi Technological University, Delhi-42, India[2]

UG Student, Department of ECE, Delhi Technological University, Delhi-42, India[3]

ABSTRACT: The swift progression in internet networking services has led to massive growth in various multimedia applications such as images, audio files, video files etc. This web revolution has made it feasible and simpler to transmit digital media from one point to another with paramount speed and accuracy. Besides this, it is easier to misuse and exploit the valuable information through hacking at the same time as the ownership and copyright of multimedia files are not usually protected. Hence, the technology needs to be enhanced to protect data from any unauthorized access. To protect intrusion of the intellectual property, digital watermarking becomes very significant. Many effective watermarking algorithms have been proposed, however, few algorithms have been proposed for audio watermarking. Digital Watermarking is a technique that allows the copyright protection of multimedia data by insertion of a signature.

This paper presents an audio watermarking scheme using multiple bit plan in which a binary image used as watermark signal is embedded into an audio sample in time domain using bit manipulation techniques simultaneously applied on 1st, 2nd, 3rd and 4th LSB. The watermark is subjected to chaotic scrambling before the process of embedding. Various attacks are also performed on watermarked audio and their impacts on quality of extracted message are also studied. This work has been implemented in MATLAB.

KEYWORDS: Audio watermarking, time domain, Multiple bit plane, chaotic scrambling, synchronisation code, Similarity, correlation, SNR

I. Introduction

With the boon of innovations in technology in telecommunication networks, the copyright and the ownership of various multimedia files is not protected against invasion by illicit sources [3][6] as the digital media is easily shared between various sources across the globe. Hence various techniques of watermarking have been proposed as a solution of this predicament. Digital Watermarking is a technology which is achieved by modifying the original content of a digital file by embedding a secret watermark as a proof of ownership, without the detection by the user. The watermark is not traceable to the user and does not influence the usability and quality of the original audio file. The extent of protection of the embedded watermark against a variety of attacks defines the robustness and efficiency of the applied algorithm. The watermarking presented in this paper is the Audio Watermarking in which the watermark is embedded in an audio signal. Audio watermarking [2] techniques can be grouped into two types; time-domain techniques and frequency-transform techniques [1]. In time-domain, the sample values of audio signal are directly modified whereas in frequency- transform domain, the bits of transform coefficients are modified and not the audio signal sample values. The best known Watermarking method that works in the time Domain is the Least Significant Bit (LSB), which replaces the least significant bits of pixels selected to hide the information. This method was used for image watermarking [6]. The same technique has been implemented for Digital Audio Signal [8] and the performance and robustness of the applied algorithm have been evaluated. In the present work, the embedding is done in 1st, 2nd, 3rd and 4th LSB (Multiple bit plane) of the audio samples simultaneously. To increase the robustness and security aspect of the proposed algorithm and to shield the watermark from illegitimate sources, the watermark is subjected to the process of chaotic scrambling [4][7] before it is embedded in the audio signal. The watermarked audio signal is then subjected to various attacks [3] before the watermark is extracted for checking the authenticity. The following paper has been

10.15680/ijircce.2015.0303093

divided into 8 sections. *Section II* gives the literature survey. *Section III* describes the model of digital watermarking scheme. *Section IV* presents the algorithm for Multiple bit plane method. *Section V* describes the method of chaotic scrambling. *Section VI* briefs about various attacks that can affect the audio signal and various assessment measures. *Section VII* contains summarised results followed by *Section VIII* that gives conclusions and future scope.

II. LITERATURE SURVEY

Many watermarking algorithms have been proposed in last few years that ensure the security of the watermark signal and authenticity of the host message signal. The work presented in [8] by Prof. Jeebananda Panda et. al. is the Least Significant Bit (LSB) substitution method of audio watermarking in time-domain single bit plane. The watermark along with synchronisation bits is embedded in the 1st LSB of all the audio samples and the attained results are compared when the algorithm is recurred for 2nd, 3rd and 4th LSB. The watermarked signal is subjected to various attacks and by computing similarity between original and recovered watermark and SNR of audio signal, it is observed that algorithm is more robust corresponding to 3rd and 4th LSB substitution. Deepshikha Chopra et. al in [6] presented an invisible watermarking technique (lower LSB e.g. 1st) and a visible watermarking technique (higher LSB e.g. 7th) for image. The robustness of each technique is studied by Peak signal to noise ratio (PSNR) and mean square error (MSE). In [1], Ali Al-Haj et. al. presented an algorithm for audio watermarking in frequency-domain where the watermark image is embedded at LSB of the coefficients of transformed host audio signal. The transformed signal is obtain using Discrete Wavelet Transform (DWT). The proposed algorithm performed better than most traditional techniques. Prof. Samir Kumar in [5] worked on Audio Steganography techniques using LSB modification, phase encoding, parity coding and Spread Spectrum. In LSB coding technique, the least significant bit is modified to embed data. In phase encoding scheme, the phase of carrier file is replaced with reference phase which represents hidden data. In parity coding, signals are divided into regions and then parity bit of each region is calculated and matched with secret message bit. Depending on parity matching results, encoding is done. In spread spectrum method, secret information is spread over the audio signal frequency spectrum as much as possible. The work presented in [2] by Jeebananda Panda et. al. is energy efficient (frequency domain) watermarking of audio signal i.e. in audio samples, an energy efficient watermark is embedded which satisfies the power spectrum condition (PSC). In PSC compliant technique, the power spectrum of watermark is directly proportional to that of the original signal. Md. Moniruzzaman in [4] presented fragile watermarking technique based on chaotic scrambling. The watermarking scheme is based on Arnold's cat map which can be used for tamper detection. The performance of the scheme is evaluated using Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Error Bit Rate (EBR). Prof. Jeebananda Panda in [3] worked on empirical mode decomposition (EMD) based audio watermarking. The host audio signal is divided into segments with specific number of samples and then performed EMD separately on each segment to produce intrinsic mode functions (IMFs) that can be fully described by their extreme. The embedding of binary watermark is done into the extreme points of last IMF of all the segments concatenated together through Quantisation Index Modulation (QIM) embedding technique. Shao-Hui Liu et. al. in [7] presented a general framework for fragile watermark in which a difference image obtained by computing the difference between the host image and its chaotic pattern is mapped into a binary image. The binary image is then inserted into the LSB bit plane of the host image. Chaotic map is also proposed to generate the chaotic pattern image. The presented work is fast, secure and is tamper proof.

III. MODEL OF DIGITAL WATERMARKING

Digital Watermarking can be categorized into three sections; embedding, attacks in the channel and extraction.

1) *Embedding of Watermark:* In this phase, the original message used as watermark is hidden in the original digital file using Multiple bit plane method. The watermark can be further subjected to the process of scrambling i.e. encoding prior to the embedding.

2) *Attacks:* The contents of the watermarked signal can be amended or modified by unauthorized sources while transmitting, which are known as attacks. Various attacks that can alter the watermark data are additive Gaussian noise, re-sampling, cropping, mp3 compression and filtering.

3) *Extraction:* This makes use of the detection algorithm or the synchronisation code for extraction of the embedded watermark. It is then further processed for chaotic scrambling decoding.

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. 3, Issue 3, March 2015

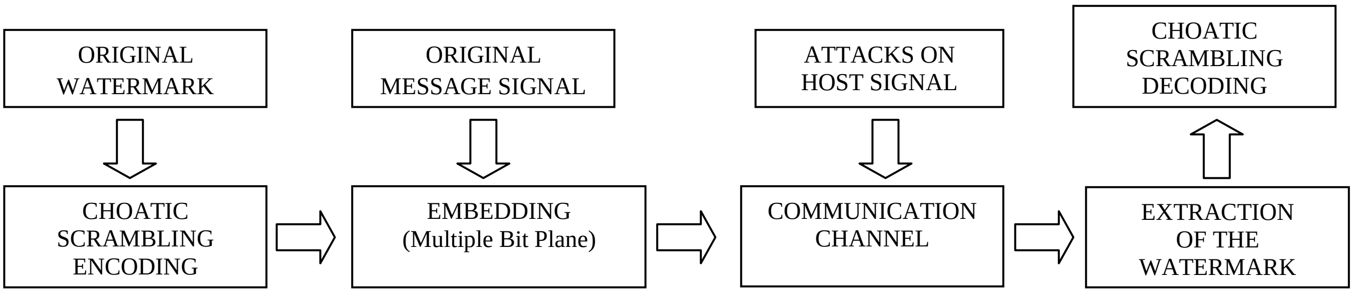

ORIGINAL WATERMARK
ORIGINAL MESSAGE SIGNAL
ATTACKS ON HOST SIGNAL
CHOATIC SCRAMBLING DECODING
CHOATIC SCRAMBLING ENCODING
EMBEDDING (Multiple Bit Plane)
COMMUNICATION CHANNEL
EXTRACTION OF THE WATERMARK

Figure 1. Basic Model of Watermarking

IV. AUDIO WATERMARKING

Digital audio watermarking [1][2] requires concealment of data within a discrete audio file. The protection of intellectual property forms the basis of research in this field of interest.

A. Watermark embedding process using Multiple Bit Plane

The extraordinary high channel capacity of audio signal permits a smaller watermark signal to be embedded multiple times. The probability of extraction of accurate watermark increases with the increase in the number of times the watermark is embedded into the digital file. In this paper, the watermark image used is a binary file of size 50 pixels x 50 pixels and the digital file used is an audio file of duration of 8 seconds sampled at a frequency of 44100 Hertz. The algorithm is as follows:

- The digital audio file of extension .wav is sampled at the frequency of 44100 Hertz. The audio samples by default are in double format. Hence, they are transformed into 16 bit format prior to the process of watermarking.

$$A = \{ A\ (1,j),\ 1 \le j \le K \}\ K = 352800 \qquad (1)$$

- The watermark image is a square matrix of size M x N where M,N = 50.

$$Img = \{ Img\ (k,j),\ 1 \le k \le M\ ,\ 1 \le j \le N \} \qquad (2)$$

- Reshape the binary image into a column array of length of 2500 pixels/bits.

$$C = \{ C(i) = Img(k,j),\ i = k\ x\ j \} \qquad (3)$$

- Additional 20 synchronization bits are inserted at the starting of the binary image array. The value of the additional bits is set to zero. Hence, the entire length of the image array to be inserted is modified to 2520 bits.

$$W = \{ W(i) = C(k),\ i = 20 + k \} \qquad (4)$$

- A total of 80 replicas of the watermark image are embedded into the audio file taken for our experiment.

$$I = W\ x\ k\ ,\ k = 80 \qquad (5)$$

- Multiple bit plane method is applied in which the 1st LSB of first sample, 2nd LSB of second sample, 3rd LSB of third sample, 4th LSB of fourth sample, then again 1st LSB of fifth sample till the end of all the samples of audio signal is set according to the binary image vector. Zero value of the image array sets the concerned LSB bit plane of audio file sample to 0 and non-zero value of image array sets it to 1.
- The modified watermark array obtained is stored as a new audio file with .wav extension before being used for transmission.

B. Watermark Retrieval Process

The received watermarked audio is subjected to the Watermark Recovery Algorithm for extraction of the embedded image from the original digital audio file. The audio file is subjected to distortion due to attacks. The extent of similarity of the extracted watermark binary image to the original binary image defines the robustness of the method used. The process of watermark retrieval is as follows:

- The reverse process of watermark embedding is applied in which the 1st, 2nd, 3rd and 4th LSB of the corresponding watermarked audio samples is extracted and stored in a different array.

10.15680/ijircce.2015.0303093

- The new array formed consists of 80 replicas of the watermark image along with 20 synchronization bit inserted at the starting of each binary image.
- For watermark recovery, a synchronization code is used which counts the number of synchronization bits in the resultant array. If the value of the counter attains 20 i.e. when 20 continuous synchronization bit of value 0 are encountered, the next 2500 pixels, which is the size of the embedded watermark image, are extracted and stored. As soon as the watermark image pixels are extracted, the synchronization code is terminated.
- The new array thus acquired is reshaped and scaled into a binary image of size M x N where M,N = 50.
  Thus, the hidden watermark is effectively extracted from the distorted watermarked audio signal and is subjected to various processing steps to find the similarity and correlation function values.

V. Chaotic Scrambling

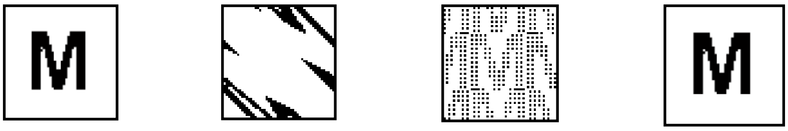
In order to raise the safety of watermark against unauthorized access, chaotic scrambling i.e. encryption of watermark image before embedding process is used. As security issues are a major concern, chaotic maps generate chaotic patterns for increasing the security. *Arnold's cat map transformation* [4] algorithm is used for generating scrambled sequence. Two dimensional Arnold's cat map shuffles the pixels of the image matrix without affecting the grey level intensities.

The 2D Arnold cat map [7] is obtained as:

$$x' = [x + py] \bmod (N) \tag{6}$$

$$y' = [qx + (pq + 1)y] \bmod (N) \tag{7}$$

where (x', y') are the new positions of point (x, y) after the Arnold's cat transformation and N is the dimension of the image. p and q are the initial values on which sensitivity of cat map depends and can be used as keys. Here, p and q are taken as 1.



(a) *(b)* *(c)* *(d)*

(a) Original Image (50x50) (b) & (c) are scrambled images after iterations T = 1 & 100.
(d) Original image after completing a cycle (T=149)
Figure 2. Periodic pattern of Arnold's cat map

Each scrambled image is different from each other depending upon number of iterations T. Also, Arnold's cat map is periodic in nature as the original image is obtained after successive iterations since pixels return to original positions after being transformed T times. The periodicity of the algorithm is shown in Figure 2. In this paper, the watermark image is transformed T=1 times before embedding in the host signal.

VI. Tests Against Attacks

Audio file watermarked using the above algorithm was subjected to various attacks such as *additive noise, mp3 compression, re-sampling, cropping* and *low pass filtering.* The extracted watermark is compared with the original watermark image to study the efficiency of the proposed algorithm.

1) **Noise:** Average White Gaussian Noise (AWGN) is added to make Signal to Noise (SNR) ratio of signal to 104 dB.
2) **Re-sampling:** The watermarked signal is subjected to decimation (reduction in number of samples).
3) **Cropping:** Segments of 441 samples are removed at 3 locations and are replaced with segments contaminated with AWGN (100dB).
4) **Compression:** The watermarked signal compressed and eventually decompressed using MP3 compression at 320 kbps.
5) **Filtering:** The signal is passed through a low pass filter (LPF) .

The extracted watermark W' and the original watermark W are compared through a Similarity function(SIM). The mathematical expression is as follows:-

$$SIM(W,W') = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(W(i,j)*W'(i,j))}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}(W'(i,j))^2}}$$

where W = Original Watermark
W' = Extracted Watermark
m,n = Number of rows and columns

The correlation factor is given by:

$$Correlation \quad Factor = \frac{\sum_{i=1}^{MN} f_i f'_i}{\sqrt{\sum_{i=1}^{MN} f_i^{\,2}}\sqrt{\sum_{i=1}^{MN} f'^{\,2}_i}}$$

where f = Original Watermark
f ' = Extracted Watermark
M,N = Number of rows and columns

For watermarked audio signal quality, signal to noise ratio (SNR) is defined as follows:

$$SNR(Y,Y^*) = 10\log_{10}\left(\frac{\sum_{i=0}^{length-1} y^2(i)}{\sum_{i=0}^{length-1}[y(i)-y^*(i)]^2}\right)$$

where Y = Original Audio Signal
Y*= Watermarked Audio Signal

VII. Experimental results And Comparisons

Audio samples used here are 16 bit unsigned samples. 50 x 50 bit binary image is used as Watermark image and 20 bit "00000000000000000000" as synchronization code. In this paper, 352800 16-bit audio samples are used for embedding 80 segments of watermark image each of 2500 bit size along with 20 bit synchronization code. Hence total size of the watermark signal is 2520 bits. Figure 3 gives the normalized plot of the original audio signal and watermarked audio signal with y axis ranging from [-1,1] and x axis showing the number of samples i.e. 352800. Figure 4 shows the recovered watermarks in case of attacks and no attack after applying the proposed algorithm.

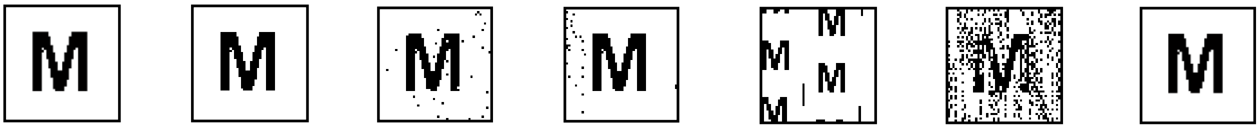
1
0.5
0
-0.5
-1
0
0.5
1
1.5
2
2.5
3
3.5
4
x 10^5

(a) Original Audio Signal

(b)Watermarked Audio Signal

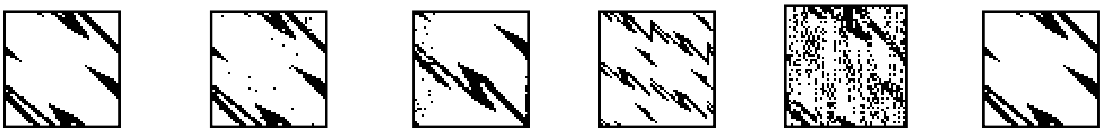
Figure 3. Plot of original and watermarked signal

The recovered watermarks when chaotic scrambling is not used in case of no attack and in case of different attacks are summarized as follows:-



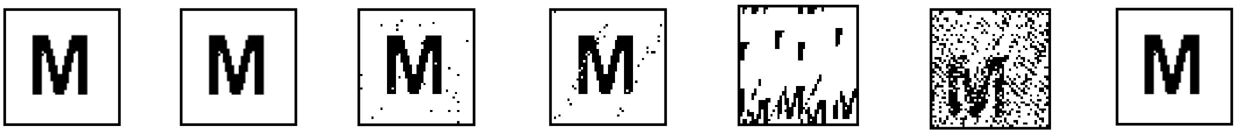
(a) Original *(b) No Attack* *(c) AWGN (104 dB)* *(d) Cropping* *(e) Decimation* *(f) LPF* *(g) mp3 compression*

The recovered watermarks when chaotic scrambling is used in case of no attack and in case of different attacks are summarized. The following are the scrambled watermarks which are then transformed using the periodic property of the Arnold cat transformation.



(a) No Attack *(b) AWGN (104 dB)* *(c) Cropping* *(d) Decimation* *(e) LPF* *(f) mp3 compression*

The watermarks when transformed using chaotic scrambling when the recovered scrambled watermark is transformed for number of iterations T =149 are :-



(a) Original *(b) No Attack* *(c) AWGN (104 dB)* *(d) Cropping* *(e) Decimation* *(e) LPF* *(f) mp3 compression*

Figure 4. Recovered Watermarks

It has been observed that the embedded watermark is successfully extracted from the watermarked audio signal with the proposed algorithm. The performance of the proposed scheme has also been evaluated under various attacks and it is observed that watermark can be efficiently extracted from the watermarked audio signal even when the audio quality is tampered due to different distortions. This establishes the robustness and advantage of the proposed scheme over the existing algorithms. The results of various comparison measures of multiple bit plane technique with and without the use of chaotic scrambling are compared with the method of watermarking specified in our previous paper [8] in which the watermark is embedded only in the 1st LSB of all the audio samples.

Table I and Table II summarize the results for *Correlation Factor* and *Similarity Measure* respectively between the original watermark and the extracted watermarks using the three methods whereas Table III summarizes the results for *Signal to noise ratio* between the original audio signal and the watermarked audio signals using the three methods.

Method 1: LSB Substitution Method in [8]
Method 2: Multiple bit plane without chaotic scrambling
Method 3: Multiple bit plane with chaotic scrambling.

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. 3, Issue 3, March 2015

Attack Type	CORRELATION FACTOR		
	Method 1	Method 2	Method 3
Original Watermark	1.0000	1.0000	1.0000
No attack	1.0000	1.0000	1.0000
AWGN (104 dB)	0.9900	0.9926	0.9933
Cropping	0.8684	0.9938	0.9749
Mp3 compression	0.9928	1.0000	1.0000
Low-Pass Filtering	0.9986	0.8560	0.7636
Decimation	0.8390	0.8390	0.8242

TABLE I. CORRELATION FACTOR FOR DIFFERENT METHODS

Attack Type	SIMILARITY MEASURE (%)		
	Method 1	Method 2	Method 3
Original Watermark	100	100	100
No attack	100	100	100
AWGN (104 dB)	99.00	99.26	99.33
Cropping	86.84	99.38	97.49
Mp3 compression	99.28	100	100
Low-Pass Filtering	99.86	85.60	76.36
Decimation	83.90	83.90	82.42

TABLE II. SIMILARITY MEASURE FOR DIFFERENT METHODS

Attack Type	SIGNAL TO NOISE RATIO (dB)		
	Method 1	Method 2	Method 3
No attack	104.6	88.27	93.08
AWGN (104 dB)	162.68	166.20	160.32
Cropping	176.10	189.22	195.24
Mp3 compression	83.30	93.23	93.09
Low-Pass Filtering	139.7	156.57	165.27
Decimation	75.50	92.32	75.40

TABLE III. SIGNAL TO NOISE RATIO FOR DIFFERENT METHODS

From the above results, it has been observed that the signal to noise ratio of the watermarked audio signal has been significantly improved from the existing method specified in [8]. Also the quality of the extracted watermark has also been improved showing the robustness of the applied algorithm. It is found that the SNR with chaotic scrambling is better than that without chaotic scrambling in some cases.

VIII. CONCLUSIONS AND FUTURE SCOPE

The results of the proposed method in this paper are enhanced as compared to that obtained in [8] thereby showing the efficiency and effectiveness of the algorithm. The watermark is impercievable and inaudible by Human Auditory System(HAS). In this paper, the watermark is embedded at the 1st, 2nd, 3rd and 4th LSB consecutively of all audio samples with and without chaotic scrambling. Hence, each audio sample is altered in one bit position in its 16 bit value.

10.15680/ijircce.2015.0303093

Since each sample is affected, the payload is increased and SNR is reduced. As a future research, the watermark can be embedded in a random manner in which random audio samples are affected and remaining samples remain impervious to the watermark. This decreases the payload, increases the SNR of watermarked signal and also increases the security of the embedded image.

REFERENCES

[1] Ali Al-Haj et. al., "DWT–Based Audio Watermarking", The International Arab Journal of Information Technology, Vol. 8, No. 3, July 2011.

[2] Jeebananda Panda et. al.," Application of Energy Efficient Watermark on Audio Signal for Authentication" 2011 International Conference on Computational Intelligence and Communication Systems.

[3] Jeebananda Panda, Karan Raj Gera and Asok Bhattacharyya, "Non-Blind Audio Watermarking Scheme Based on Empirical Mode Decomposition", International Journal of Advanced Science, Engineering and Technology.ISSN 2319-5924 Vol 3, Issue3, 2014, pp38-43

[4] Md. Moniruzzaman, Md. Abul kayum hawlader and Md. Foisal hossain, "An image fragile watermarking scheme based on Chaotic system for image tamper detection", 3rd international conference on informatics, electronics & vision 2014

[5] Prof. Samir Kumar, Bandyopadhyay Barnali, Gupta Banik, "LSB Modification and Phase Encoding Technique of Audio Steganography Revisited", International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 4, June 2012

[6] Deepshikha Chopra et. al., "LSB Based Digital Image Watermarking For Gray Scale Image", IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727 Volume 6, Issue 1 (Sep-Oct. 2012), PP 36-41.

[7] Shao-Hui Liu, Hong-Xun Yao, Wen Gao, Yong-Liang Liu, "An image fragile watermark scheme based on chaotic image pattern and pixel pairs", Applied Mathematics and Computation, vol. 185, pp. 869–882, 2007.

[8] Jeebananda Panda, Indu Kumari and Nitish Goel, " Digital Watermarking of Audio using LSB Substitution", National Conference on Advanced Computing Research (NCACR)-2015

BIOGRAPHY

Jeebananda Panda
Designation: Associate Professor
Qualification: ME
Specilization: Applied Electronics
Email: jpanda@dce.ac.in

Indu Kumari
Designation:Student
Qualification: UG
Department: Electronics and Communication Engineering
Email: indukumari2795@gmail.com

Nitish Goel
Designation:Student
Qualification: UG
Department: Electronics and Communication Engineering
Email:ngoel0108@gmail.com

10.15680/ijircce.2015.0303093