International Journal of Soft Computing and Engineering (IJSCE)
ISSN: 2231-2307, Volume-2, Issue-6, January 2013

Digital Watermarking with Secret Audio Sharing

Supriyo De, Subijit Mondal, Dibyendu Chowdhury

Abstract -- In today's society with the increased use of computers, internet, and wireless communications, the need for safety and security has raised dramatically. The phenomenal growth of E-communication and new technologies has furnished to the need of secured communication and secure data transmission. The information can be a confidential document, it may be in form of image, audio, text etc. Some of the information transmitted can be intercepted illegally, such as personal information and private or secure messages. In this paper, implementation of secret sharing scheme is used to achieve the goal. We have proposed a technique to hide shared data into a digital image using the basics of cryptography to prepare a cipher key and meanwhile using the definition of digital watermarking to hide the fact that data is hidden. This helps to prevent the participant from incidental or intentional provision of a false or tampered stego-image. Consequently, the proposed scheme offers a high secure and cost effective mechanism for secret sharing.

Keywords – Image processing, Secret sharing, Secure message transfer, Security watermarking, Steganography.

I. INTRODUCTION

A digital watermark is a signal that is embedded in a digital image or a video session to identify the ownership or provide any additional information regarding the content [1]-[3]. For several years, watermarking tended to be used in new kinds of applications besides just digital security: watermarking is no longer necessarily used to hide information related to the content owners/users; it can also be used as a means to transmit information useful for users (e.g. "enriched-content" databases). For example, in, watermarking is used to embed into a mixture audio signal metadata that guide the separation of the source signals composing the (watermarked) audio mix.

In certain application cases, it is a risk if a set of secret data is held by only one person without extra copies because the secret data set may be lost incidentally or modified intentionally.

Manuscript received on January, 2013.

Supriyo De, Department Of Electronics and Communication Engineering, Saroj Mohan Institute of Technology (Degree Engineering Division), Hooghly, India.

Subijit Mondal, Department Of Electronics and Communication Engineering, Saroj Mohan Institute of Technology (Degree Engineering Division), Halisahar , India.

Dibyendu Chowdhury, Department Of Electronics and Communication Engineering,, Haldia Institute of Technology ,Haldia, India.

The first idea of secret sharing was proposed individually by Adi Shamir and George Blakley in1979. Shamir's[4] scheme based on polynomial interpolation where as Blakley[5] scheme based on hyper plane geometry. After the scheme was proposed, many related topics have been studied (Sun and Shieh, 1994; Chang and Lee, 1993). However, the resulting methods are suitable for only a few types of digital data, such as text files, passwords, encryption/decryption keys, etc. In 2004, Lin and Tsai[6] proposed a method that used Steganography for generation of meaningful shares with secret image sharing. But this study used polynomial-based secret sharing approach which led to high computational complexity.

In this paper we have suggested a secret sharing scheme absolutely different from any of the schemes discussed so far, where simple ANDing operation[7] is used for n no of share generation and then each share data embedded into a single digital image. Reconstruction can be done simply ORing the k ($k \leq n$) no of share data which are retrieved from digital image at receiving end. Sending the single digital image through the channel indicates low costing although it will prevent attacks or illicit access more effectively.

This paper is organized as follows: the first section is a general overview of the proposed system and the second section is a detailed presentation of the main functioning structure of the system. Results are presented in the third section and the last section concludes this article.

II. SYSTEM DESCRIPTION

A. Design Concept

The proposed system is basically a digital signal processing based system (Fig. 1). The user has to provide the inputs e.g. the audio file to be used as the message signal and the image file to be used as the cover file. Here we use secret sharing scheme which employs simple graphical masking method, performing by simple ANDing for share generation & reconstruction can be done by the performing simple ORing the predefined minimal number of shares of audio sample. The generated shares are kept into a meaningful cover image but the novelty of the scheme depends upon the technique of generating individual masks to be used for ANDing over the original secret for share generation. The shared sample values of audio data are hidden into random positions of the image using random position generator algorithm employed by a secret key. A set wise algorithm is suggested for such mask design for any (n, k) scheme where *n* number of masks are designed to generate n different shares & any *k* shares (k<n) on ORing reconstruct the original secret and *key* by which the random positions [8] were generated.

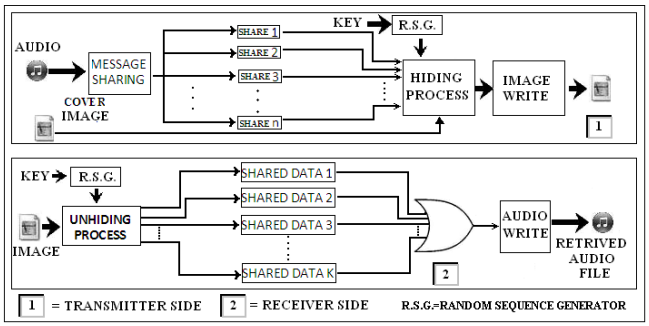

Fig. 1: The basic block diagram for the proposed system [Both the transmitter (or encoder) and the receiver (or extractor) side]

B. Detailed Algorithm

1) Sender side algorithm –

STEP 1:- The audio file to be transferred is read into an array(length=L)(Fig. 2). The audio signal[9] is then adjusted according to the need (DC value adjustment) (Fig. 3) and quantized for the ease of use through some algorithm. 6-bit dynamic but linear quantization[9] (Fig. 4) is used here. So, each audio data sample has been quantized into 64 levels.

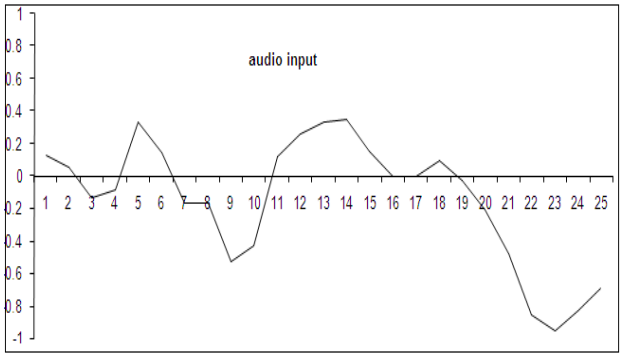

Fig. 2: The input audio array

STEP 2:- MESSAGE SHAREING:- Here we design 4 masks to generate 4 different shares (n) & any 3 shares (k) on ORing reconstruct the original secret. List of row vectors of size 4 bits with 2 no of 0's & 1's. Then, we take the transpose of the matrix & we get the desired masks for four shares as listed in the form of matrix of dimension $n \times {}^{n}C_{k-1}$ i.e. 4×6. The masks are shown below:

Mask 1: 1 1 1 0 0 0
Mask 2: 1 0 0 0 1 1
Mask 3: 0 1 0 1 0 1
Mask 4: 0 0 1 1 1 0

Now, we take '0 1 1 0 1 0' as a sample audio message(6 bit). Then, we are ANDing the audio message with each mask to generate the secret shares. The shares are shown below:

Share 1: 0 1 1 0 0 0
Share 2: 0 0 0 0 1 0
Share 3: 0 1 0 0 0 0
Share 4: 0 0 1 0 1 0

One can easily check that ORing any three(k) or more shares we get the original audio message but with less than three shares some positions still have missed. We can design n number of masks to generate n different shares and any k shares (k<n) on ORing reconstruct the original message.

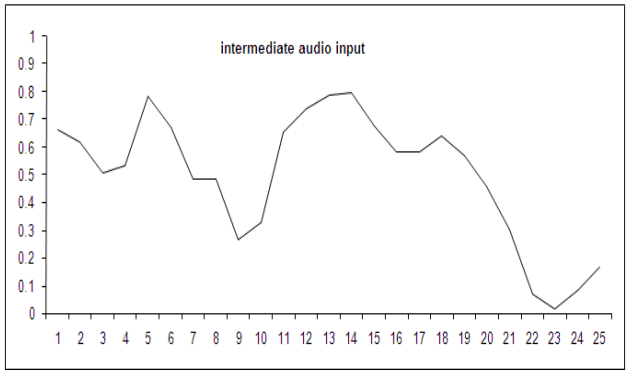

Fig. 3: Audio array after DC shift

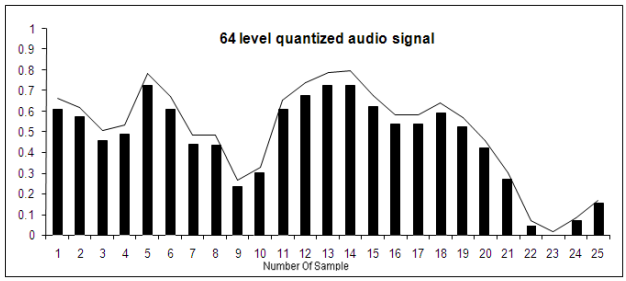

Fig. 4: Audio array after quantization

STEP 3:- A colour [RGB] image is taken ,according to the audio file size. The image file is read into an array in a way similar to step 1.

STEP 4:- A secret Key (key) is taken for generating random number[10] to set the position.

STEP 5:- The shared audio sample values are split into three parts of 2-bit each, and are used to replace two of the LEAST SIGNIFICANT BITs of each plane of image pixel (Fig. 5). For example, d_0 and d_1 bits of audio signal sample replace the D_0 and D1 bits of RED plane. This process is repeated until the original image pixel value is modified for all the sample value of modified audio file.

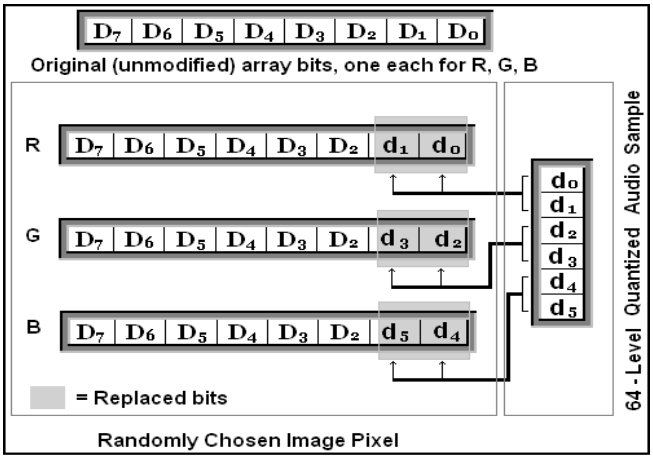

Fig. 5: The pixel value replacement concept (steganography)

STEP 6:- Now, the generated image can be transferred through any public-purpose communication channel.

2) Receiver side algorithm –

STEP 1:- Upon receiving the image and the secret key, the decryption or extraction process can be started. Then random positions are generated using the secret key. These positions are exactly the same set of positions of the sender side.

STEP 2:- It is the step to extract the last two bits of each plane from the selected pixels. Now, combined the bit-pattern in the similar manner of the sender side to get back the 6-bit quantized data. This process is repeated for L times.

STEP 3:- Now, any k shares data (k<n) on ORing reconstruct the original audio file.

STEP 4:- After getting the extracted signal values, a filtering method (LPF) is to be applied to remove the noise present in those samples.

STEP 5:- Then the final extracted audio array is written into an audio file. Then the audio information is audible at the receiver side.

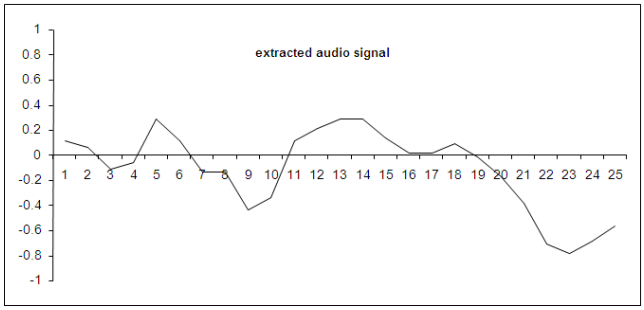

Fig. 6: Extracted and reconstructed audio array

III. Experimental Results

TABLE I List Of Values For The Audio Array

No. of Sample	Quantized Data (qD)	Share 1 (A)	Share 2 (B)	Share 3 (C)	Share 4 (D)
01	100100	100000	100000	000100	000100
02	100010	100000	100010	000000	000010
03	011011	011000	000011	010001	001010
04	011101	011000	000001	010101	001100
05	101011	101000	100011	000001	001010
06	100100	100000	100000	000100	000100
07	011010	011000	000010	010000	001010
08	011010	011000	000010	010000	001010
09	001110	001000	000010	000100	001110
10	010010	010000	000010	010000	000010
11	100100	100000	100000	000100	000100
12	101000	101000	100000	000000	001000
13	101011	101000	100011	000001	001010
14	101011	101000	100011	000001	001010
15	100101	100000	100001	000101	000100
16	100000	100000	100000	000000	000000
17	100000	100000	100000	000000	000000
18	100011	100000	100011	000001	000010
19	011111	011000	000011	010101	001110
20	011001	011000	000001	010001	001000
21	010000	010000	000000	010000	000000
22	000011	000000	000011	000001	000010
23	000000	000000	000000	000000	000000
24	000100	000000	000000	000100	000100
25	001001	001000	000001	000001	001000

Besides giving high authentication ability and good robustness, this proposed scheme obtains good recoverability. Experiments have been performed many times and exhaustively for the reliability and robustness of the total system. For illustration purpose, the consecutive 25 samples are taken from the audio source file and the corresponding tabular representations of the values at different stages of the algorithm are shown in TABLE I.

Any k shares (k<n) on ORing reconstruct the original audio signal. In this experiment, the peak signal-to-noise ratio (PSNR) is used to evaluate the quality of the restored audio file. A higher PSNR means that the quality of the restored signal is better.

Here MSE is the mean square error between the original signal and the recovered one. For a host signal with a length of n, the formula for MSE is

$$MSE = \frac{1}{n}\sum_{N=1}^{n}\left(f(x) - f'(x)\right)^2$$

where, f(x) is the original signal and f'(x) is the recovered signal. TABLE II displays the quality of images with five different audio files which are evaluated by PSNR values. Here, all the audio files are sampled in 8 KHz (Here, all the different images have same PSNR for the same audio file used.)

The robustness of the process depends upon how well the steganographic approached has worked out, i.e. the least of difference between the original image and the newly generated image, both visually and features-wise, i.e. structurally. Some of the experimental results are listed in TABLE III.

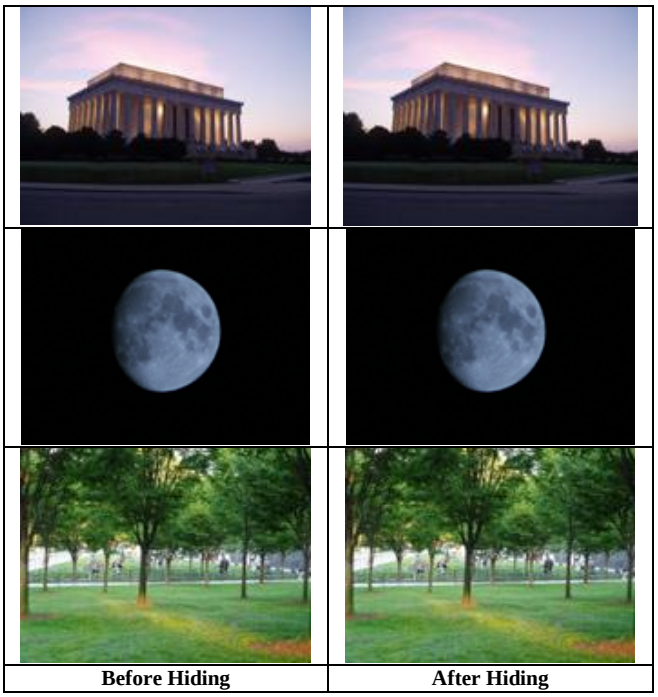

Fig7: Original and Modified Image

TABLE II PSNR (For Various Audio Signals With IDs)

hello_computer. wav (1)	hello.wav (2)	alright. wav (3)	as_you_ wish.wav (4)	program_ complete. wav (5)
73.803	65.748	68.522	69.023	78.76

TABLE III
FEATURE UNDER TEST: CONTRAST
[LISTED AS THE % OF VARIATION IN OUTPUT WITH RESPECTTO INPUT]

File ID	korean1024. bmp	moon.bmp	lincoln 1024.bmp	boat1024X768.bmp
1	0.56%	5.7%	2.97%	6.54%
2	0.56%	4.98%	2.90%	6.46%
3	0.56%	4.89%	2.89%	6.46%
4	0.57%	6.00%	3.01%	6.57%
5	0.59%	5.90%	2.99%	6.56%

From the table and images above, it is evident that the data hiding has taken place successfully and the change after the hiding process is almost invisible to bare-eyed user having no prior knowledge of the steganographic approach.

IV. RESTRICTIONS, CONCLUSIONS & PERSPECTIVES

The main restriction of this system is the image size compatibility. The length of the audio file array will be the key factor determining the dimension of the cover image to be used. Another factor, which may affect the decoding process hugely, is the modification in the image dimension after the watermarking process, as the random positions generated by the algorithm is based upon the image dimension. If we collect less than threshold (k) number of shares then the generated audio file will be completely different from the original. If the number of n and k is high then some difficulties will arise. The method is tested under Windows Xp OS and MATLAB 7.0.0.19920 platform with 3 Gb RAM.

In this paper a novel approach is presented for secure transfer of an audio message with the help of a cover image using both secret sharing and watermarking. This method possesses low computational complexity, high security, no distortion as well as less cost. This method is more robust than other simple cryptographic or simple steganographic approach, as it includes the best of both. Watermarking is mainly used as a tool to achieve copyright protection, ownership trace, and authentication. Usually, the data used for watermarking is of less importance. This research paper focuses on using the audio message as the watermarking data to achieve secret sharing and steganographic approach side by side. This approach makes this technique unique in its field. This uniqueness adds an extra mile to its level of security.

However, this system is not future-proof in case of further modifications. There are still possibilities for increasing the level of security. Instead of using the spatial and time domain for the image and audio signal processing, discreet cosine transform of the values can be considered for a stronger approach. Also, the concept of non-linear quantization may be incorporated to the system in order to make the system to be almost invincible to possible attacks. There seems to be another shortcoming of this algorithm. The random positions used in this system are based upon the image size (or pixel count). So, it might be possible to have a hint of the random positions by applying brute force attack if the image (used as cover) is too small compared to the number of audio file samples used. So, to increase the security level, the pixel count of image should be in much higher proportion to the audio file samples. In this paper, the algorithm is so designed that it will automatically generate random positions and checks them for their random nature. Sender should use the different value of *n*, *k* and *key* for the betterment of the security. Thus it guarantees to maintain the random nature of the positions as well as secret sharing technique.

ACKNOWLEDGMENTS

Authors are thankful and express their gratitude to the Digital Signal Processing Laboratory of Saroj Mohan Institute of Technology [Degree Engineering Division], Guptipara, Hooghly to be of immense help carrying out the work of this project. We thank Dr. A. K. Nath, Jadavpur University for many useful comments.

REFERENCES

[1] J. Cox, M. L. Miller and J. A. Bloom. Digital Watermarking,Research Report, New York: Academic Press, 2002.
[2] Adelson, E., 1990. Digital signal encoding and decoding apparatus, US Patent no. 4,939,515, 1990.
[3] Hsu, C.T., Wu, J.L., 1999. Hidden digital watermarks in images. IEEE Transactions of Image Processing 8, 58–68.
[4] A. Shamir: "How to share a secret ?" Comm ACM, 22(11):612-613, 1979.
[5] G. Blakley : "Safeguarding cryptographic keys", Proc. of AFIPS National Computer Conference, 1979.
[6] Chang-Chou Lin, Wen-Hsiang Tsai, "Secret image sharing with steganography and authentication", Journal of Systems and software, vol. 73, no. 3, pp. 405-414, 2004.
[7] P.K. Naskar, A. Chaudhuri, A. Chaudhuri, "Image Secret Sharing with Steganography", Proc. of Second National Conference on Computing and Systems – 2012, pp. xv-xix.
[8] S De, D Choudhury, S Ghosh, P Maity, "A New Digital watermarking Scheme for Secret Audio Message Transmission", Proc. of National Conference on Advanced Communication Systems and Design Techniques, 2011, pp. 118-122.
[9] L. Boney, T. Ahmed and H. Khaled. Digital watermarks for audio signals. *Third IEEE Int. Conf. on Multimedia Computing and Systems*, pp.473-480, June 1996.
[10] S. Manchanda, M. Dave, S.B. Singh, *Customized and secure image steganography through random number logic*, signal processing: An International Journal, Volume 1, Issue 1.

Mr. Supriyo De is the Assistant Professor of Department of Electronics & Communication Engineering and Applied Electronics & Instrumentation Engineering, Saroj Mohan Institute of Technology.He was born on the 2nd day of November, 1983 at Kolkata. He obtained his B.Tech degree from JIS College of Engineering in 2006 and M.Tech degree from Haldia Institute of Technology in 2009.The broad area of his research interest is in Digital Signal Processing, Digital Image Processing and Pattern Recognition.

Mr. Subijit Mondal is an Electronics engineer. He was born on the 25th day of April, 1990 at Halisahar.He obtained his Bachelor of Technology degree from Saroj Mohan Institute of Technology (Techno India) under West Bengal University of Technology in the Year 2012.The broad area of his research interest is in digital signal processing, cryptography and digital watermarking.

Mr. Dibyendu Chowdhury is working as an Assistant Professor in the department of Electronics & Communication Engineering, Haldia Institute of Technology, Haldia. He received his B.Sc and M.Sc in Electronics under Vidyasagar University in the year of 2004 and 2006 respectively. He received his M.Tech in Electronics & Communication Engineering under West Bengal University of Technology in the year of 2009. He also received **Gold Medal** (For M.Sc) from Vidyasagar University. His area of research interest includes VLSI and Embedded Systems. He is working towards his Ph.D. degree.