ISSN:0975-9646

Digital Audio Watermarking for Copyright Protection

Chakradhar Kahalkar

Department of Computer Science
Manoharbhai Patel Institute of Engineering & Technology, Bhandara (MS), India

Abstract— **Digital Watermarking is the process of embedding data called watermark or signature into a multimedia object (image or audio or video) so that the watermark can be extracted for ownership verification or authentication. A visible watermark is a secondary translucent viewer on a careful inspection. In this paper presents new cryptographic scheme which use audio. The scheme is secret sharing scheme in which share is audio or images and is not suspect to a human censor. There are two decryption methods which are either based on the interference property of sound or based on the stereo perception of the human hearing system. The secret key encryption algorithm is used for embedding the watermark using LSB technique.**

Keywords— **Digital watermarking, Cryptography, Secret Key, Encryption, Decryption, Least Significant Bit (LSB). Mean Squared Error (MSE).**

I. INTRODUCTION

Digital Watermarking is the process of embedding data called watermark or signature into a multimedia object (image or audio or video) so that the watermark can be extracted for ownership verification or authentication. This technology is becoming important due to the popularity of usages of audio on web.

In general any watermarking algorithm consist of three parts [1]

- Watermark
- The encoder
- The decoder

Watermarking techniques can be divided into various categories in various ways [1]. Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows:

- Text Watermarking
- Image Watermarking
- Audio Watermarking
- Video Watermarking

In other way, the digital watermarks can be divided into three different types as follows:

- Visible watermark
- Invisible-Robust watermark
- Invisible-Fragile watermark

In Visible watermarking watermark appears visible to a casual viewer on a careful inspection. The invisible-robust watermark is embedded in such a way that alternations made to the pixel value are perceptually not noticed and it can be recovered only with appropriate decoding mechanism. The invisible-fragile watermark is embedded in such a way that any manipulation or modification of the audio would alter or destroy the watermark.

In this paper we used invisible watermarking. The watermark is encoded using secrete Key so that the ownership of the audio can be verified using the same key. In such a system, the owner of the audio inserts a watermark using a secret key K. In the watermark extraction procedure, the owner uses the same key [3] to prove ownership of the object. This technique is very useful for copyright protection, and it prevent illegal use of the multimedia content without the prior permission of owner. The proposed scheme is also capable of detecting any changes made in the pixel values of the audio, this is achieved by inserting the audio hash along with the encrypted message digest in the audio.

The rest of the paper is organised as follows: In section 2 the proposed scheme is described in detail; experimental results are presented in section 3 and conclusions are drawn in section 4.

II. PROPOSED SCHEME

The basic idea of proposed scheme is to provide Audio Integrity and Copyright protection which uses cryptographic functions such as encryption for copyright protection and hash function for Audio Integrity. The working of the proposed scheme involve following steps-

A. *Watermark Embedding Algorithm*

The watermark embedding process is stated in the following algorithm-

(1) Consider an audio X in which the watermark to be inserted and M be a message (owner's information's).

(2) Let H (.) be a cryptographic function such as MD5or SHA-1 [2]. The Message digest is computed as-

H (M) = (P1, P2, P3……Ps)

Where Pi denote the output bits of hash function and s is the size of the hash value that depends upon the type of the hash function such as s=128 for MD5 and s=160 bits for SHA-1.

(3) The Audio hash is computed as-

a) First the Binary audio B is crated from the original audio X.

b) Then Audio hash is computed using hash function such as MD5 or SHA-1

i.e. I = H(X)

(4) Then watermark W is generated by encrypting message digest Ps using symmetric key cryptosystem [3] as:

$$W = EK(Ps)$$

Where E (.) is an encryption function of the symmetric key system and K is the secrete key.

(5) Embed the watermark bits and Audio hash into LSB of original Audio X.

(6) Finally obtain the watermark audio X_w

Watermark Embedding Scheme is shown in fig.1

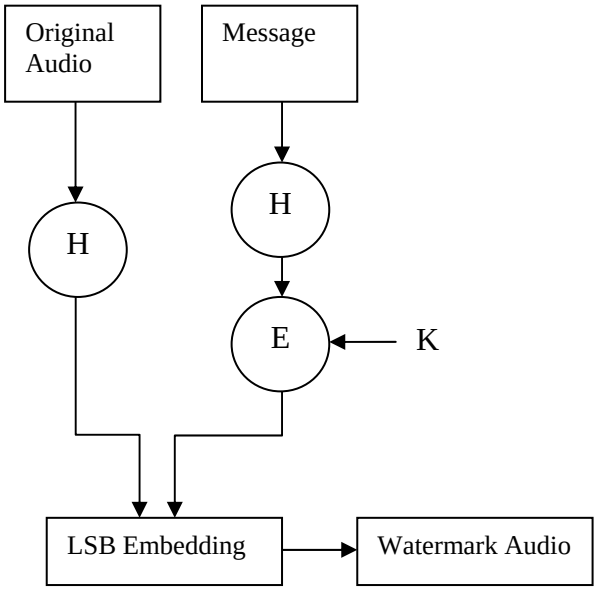

Fig. 1 Watermark Embedding

B. ***Watermark Extraction Algorithm***

The watermark extracting process is stated in the following algorithm-

(1) Extract encrypted Message digest and Audio hash from LSB of watermark Audio Xw.

(2) Obtain the hash value using symmetric key algorithm i.e. P's = DK(W')
Where D (.) is an decryption function and K is the owners secrete key.

(3) Compare P's with recomputed hash value of message to prove the ownership of the audio.

(4) Similarly the Audio hash is recomputed and compare for temper detection.

Watermark extraction and verification process is shown in fig.2.

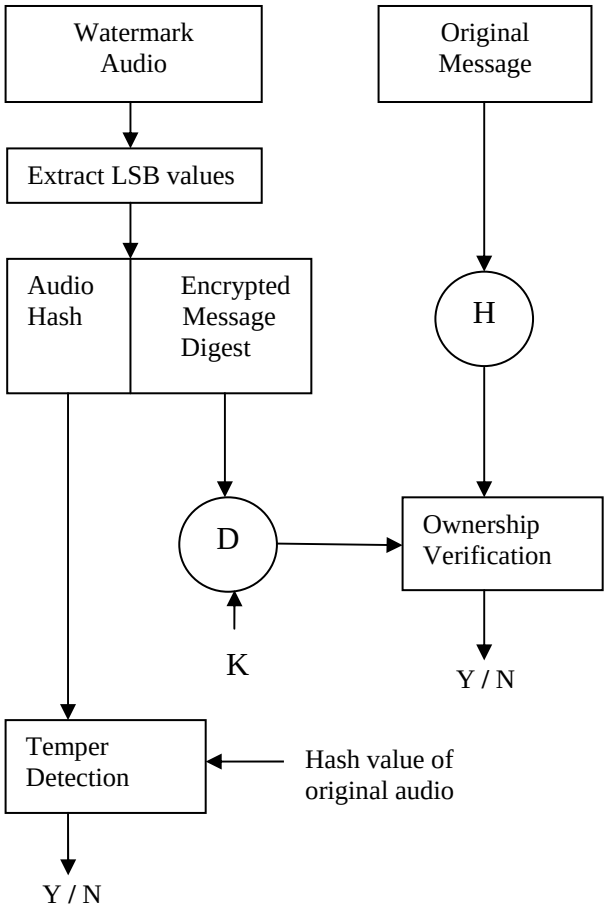

Fig. 2 Watermark extraction

III. IMPLEMENTATION AND EXPERIMENTAL RESULTS

The proposed idea is implemented using Java development kit (JDK1.6). The cryptographic primitives are implemented using JCA. JCA provide a set of classes for the implementation of cryptographic function such as encryption, decryption and hash.

The original audio is being watermarked using this proposed scheme (shown in fig. 3 and 4). The proposed algorithm is tested for different payloads.

The quality of the watermark audio against the embedding payload is tested in terms of three parameters: Histograms, Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). Larger is the PSNR better is the quality of audio and smaller is the MSE better is quality of audio. The MSE is obtain using following formula-

$$MSE = \frac{1}{N}\sum_i |x(i) - e(i)|^2$$

Here x and e are the encrypted watermarked audio signals respectively and N is the number of samples in the audio signal.

The PSNR values are obtain using following formula-

$$PSNR = 20\log_{10}\left(\frac{65535}{\sqrt{MSE}}\right)$$

An extremely high value of MSE of 7.157E8 and a corresponding low PSNR of 7.77dB were obtained.
The high MSE stood for complete deviation of the encrypted data from the signal, as is also apparent from the ACF plot, shown in Figure 5.

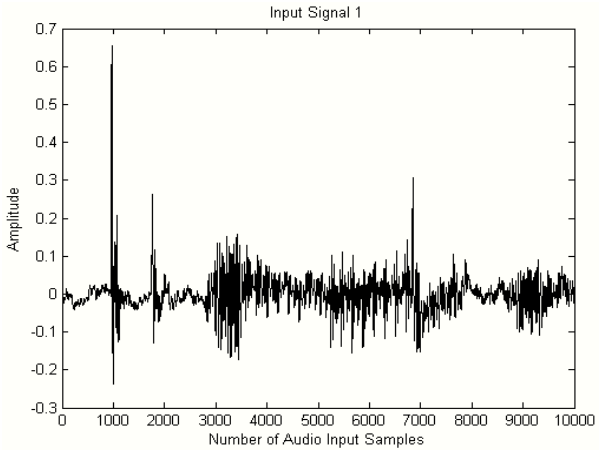

Fig. 3: Original Audio

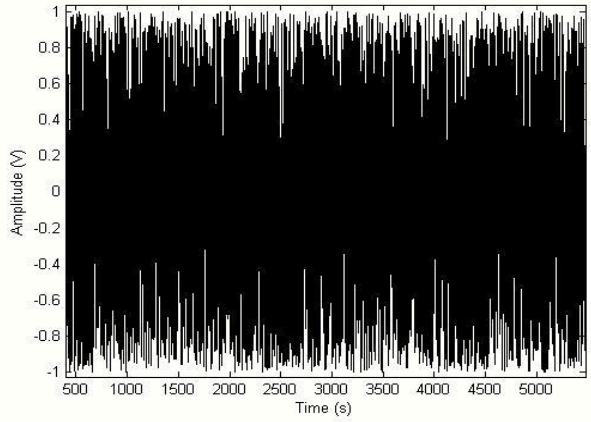

Fig. 4: Digital Watermark Audio

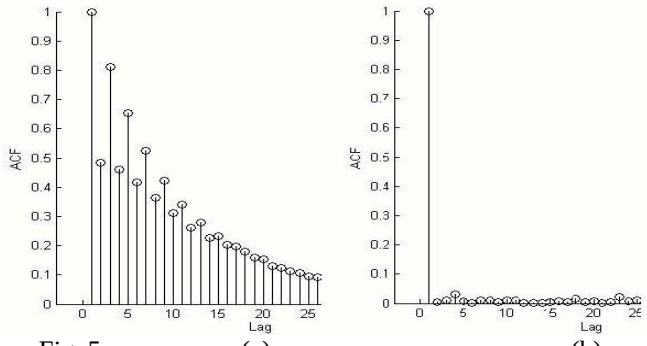

Fig. 5 (a) (b)
Autocorrelation function of Original and Digital Watermark Audio respectively.

The algorithm proposed in Section – II operates on the mode of Electronic Codebook (ECB). The times required for performing encryption and decryption using the proposed algorithm is shown in Table 1 as a function of number of audio input samples. As the audio file size becomes bigger, there is a linear rise of the time required for computations. Moreover decryption is found to be more prolonged than encryption as a sequential search is performed amidst 65536 index values to determine the actual audio sample. Faster search algorithms like the binary search also are unsuitable as they require a sorted list.

Input sample size	ECB MODE		CBC MODE	
	Encryption Time (s)	Decryption Time (s)	Encryption Time (s)	Decryption Time (s)
1e3	0.039	1.75	0.046	1.765
1e4	0.047	16.904	0.078	15.969
2e4	0.062	34.312	0.115	33.969
3e4	0.069	61.605	0.125	52.843
5e4	0.078	80.79	0.187	84.968
1e5	0.109	168.703	0.297	169.609

Table 1: Times required for encryption and decryption processes as a function of the number of input samples in the ECB and CBC modes.

IV. CONCLUSIONS

One of the most secure techniques of audio watermarking is spread spectrum audio watermarking. The key factor for detection of hidden information from SSW is the PN sequence. Here, an intelligent guided technique via an adaptive fuzzy similarity analysis is adopted in order to accelerate the process of evolutionary based recovering of PN sequence. A fuzzy supervisor such as the auto tuning algorithm is introduced in order to avoid the tuning of parameters used in this approach. This paper presented invisible watermarking scheme for copyright protection of audio. The watermark is generated by encrypting the message digest using symmetric key algorithm. Then the generated watermark along with the audio hash is embedded into LSB of original audio.

The verification process uses the same key as in encryption and hence it can be used for the copyright protection of the audio. During the verification process the received hash is compared with the recomputed hash to prove the ownership. Similarly the audio hash is compared with the recomputed audio hash for detecting any modifications made in the audio pixels. This technique provides high capacity and minimum computations. Further we can improve this method by embedding the watermark into DCT coefficients.

REFERENCES

[1] N. Cvejic, T. Seppanen "Algorithms for Audio Watermarking and St eganography", PHD thesis, oulu University of technology, June 2004.

[2] K. Gopulan "Audio steganography using bit modification", Proceedings of the 2003 International conference on Acoustic Speech and signal Processing, 2003.

[3] R. Ansari, H. Malik, A. Khikhar "Data hiding in audio using frequency selective phase alteration", Proceedings of the IEEE International Conference on Acoustic Speech and signal processing, 2004.

[4] H. Joong, Y. H. Choi, "a novel echo-hiding scheme with forward ba ckward kernels" IEEE Transactions on Circuits and Systems for Video Technology, Volume 13, No 8, Aug 2003.

[5] Z. Liu, A. Inue, "Spread spectrum watermarking of audio signals", IE EE Transactions on Circuits and System for Video Technology, Volume 13, NO. 8, Aug 2003.

[6] Saeed Sedghi, Habib Rajabi Mashhadi, Morteza Khademi"Detecting Hidden Information from a Spread Spectrum Watermarked Signal by Genetic Algorithm", IEEE Congress on Evolutionary Computation, pp. 480-485, July 16-21, 2006

[7] J.-H. Chen, D. Goldberg, S.-Y. Ho, and K. Sastry, "Fitness inheritan ce in multi objective optimization", Proceedings of the 2002 International conference on Genetic and Evolutionary Computation Conference, pp. 319–326, 2002.

[8] Margarita Reyes-Sierra , Carlos A. Coello Coello, "Dynamic fitness i nheritance proportion for multi objective particle swarm optimization", Proceedings of the 8th annual conference on Genetic and Evolutionary Computation, July 08-12, 2006, Seattle, Washington, USA.

[9] Mehrdad Salami , Tim Hendtlass, "The Fast Evaluation Strategy for Evolvable Hardware", Genetic Programming and Evolvable Machines, Volume 6, NO. 2, p.139-162, June 2005.

[10] R. Myers and D. Montgomery. "Response Surface Methodology", Jo hn Wiley & Sons, Inc., New York, 1995.

[11] Y.-S. Hong, H.Lee, and M.-J. Tahk, "Acceleration of the convergenc e speed of evolutionary algorithms using Multi layer neural networks", Journal of Engineering Optimization, Volume 35, NO 1, pp. 91–102, 2003.

[12] Won, K. S. and Ray, T., "A Framework for Design Optimization usi ng Surrogates", Journal of Engineering Optimization, pp.685-703, 2005.

[13] Gunn S.R., "Support Vector Machines for Classification and Regres sion", Technical Report, School of Electronics and Computer Science, University of Southampton, (Southampton, (U.K.), 1998.