Secured Digital Audio Watermarking and Recognition with Providing High Perceptual Transparency and Robustness

Ravi K Sheth[1], Dr. V V Nath[2]

[1] PhD scholar (Information Technology), Raksha Shakti University, Ahmedabad, Gujarat, India

[2] Professor, Nirma University, Ahmedabad, Gujarat, India

Email - [1]raviesheth@gmail.com [2]Vvnath01@gmail.com

Abstract : *In this paper, we suggested a new secured digital Audio watermarking technique that can be used for the data authentication and validation. The suggested method is secure and efficient. The secured digital watermark is added by the proposed method along with encryption technique (Arnold Transform). This technique provides strong robustness and perception transparency to the watermarked audio and original audio against different kind of attacks like cropping and noise.*

Keywords: *Digital audio watermarking, Arnold Transform, noise, cropping, PSNR, MSE, SF.*

1. INTRODUCTION:

In recent years, due to the growth of networked multimedia systems and the widespread use of personal computers, people have easy access to vast amounts of copyrighted digital data. This data, which includes text, digital audio, image and video, offers various advantages [1][2]. They can be reproduced without loss of quality, shared by multiple users, distributed over networks, and managed for long periods of time without any damage. However, unauthorized copying and distribution of digital data are serious threats to the rights of content owners [3]. Therefore, digital data protection and copyright issues have become more and more important in the face of today's technology. As a solution to copyright protection issues, digital watermarking technology is gaining attention as a new method of protecting copyrights for digital data [3].

In this paper we have inserted secrete message in data part of audio file and we kept header part of audio file as it is. We have used Arnold Transform to encrypt watermark data. In section II we have described basic methodology to implement Arnold transform. In section III we have discussed proposed method along with results based on different attacks like noise, cropping and scaling and finally we have given the conclusion based on our work.

2. ENCRYPTION ALGORITHM:

Here we have used Arnold transform as cryptographic algorithm for the encryption of M×M images. It is defined as [8]

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} a' \\ b' \end{bmatrix} (mod\ M) \quad (1)$$

Here (a, b) denotes the original values and (a', b') denotes the values of encrypted image, respectively. In equation (1), A denote the left matrix, A (a, b) and A (a', b') (m) stand for respected values of original image and the secured (encrypted) image after applying Arnold transform m times. Thus, image encryption using m times Arnold transform equation can be written as [8]

A (a', b') (l) = A (a, b) (l −1) (mod M) (2)

Where l= 1, 2… m, and A (a', b') (0) = A (a, b). It is Obvious to multiply the inverse matrix of A at each side of equation (2) to obtain A (a, b) (l −1). In other words, the encrypted image can be decrypted by iteratively calculating the following formula n times [8].

C (a, b) (k) = B−1 C (a', b') (l −1) (mod M) (3)

Where C (a', b') (0) is a pixel of the encrypted image, and C (a, b) (l) is a decrypted pixel by performing l iterations. Arnold Transform is basically periodic in nature. The extraction of image depends on alteration periods. Period changes in accordance with size of image. Here teration number is used as the encryption key. When Arnold Transformation is applied to data, the data can perform the iteration. The number of iteration count is used as a private key for extracting the secret image [8].This obviously is known only to the sender and receiver.

3. METHODOLOGY:

In this paper we have Proposed Secured Digital Audio Watermarking method as described below:

Basically, this method inserts a watermark data in data part of original image. While inserting a watermark we have applied Arnold Transform method for the better

security reason. The decryption method is as simple as the insertion method.

Watermark embedding procedure:

a. Select the audio file and secret message
b. Secrete data is converted in encrypted data using encryption algorithm
c. Audio file is divided in two parts: header and data
d. From the data part, number of samples are selected based on the size of secrete message
e. Selected sample values are converted in to its equivalent binary numbers
f. Encrypted message are embedded row by row inside the samples.
g. Finally watermarked audio file is prepared.

The entire above procedure is mentioned in figure 1.

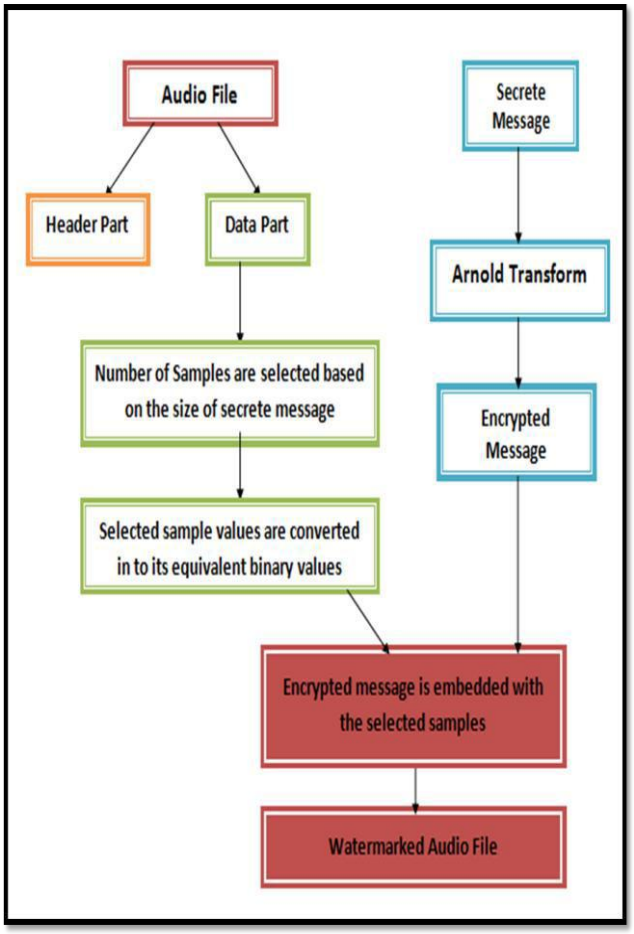

Figure 1: Watermark embedding procedure

Watermark retrieving procedure:

1. From the watermarked audio file, inserted values of secrete message is extracted
2. Message is reconstructed from the extracted values
3. Decryption algorithm is applied to decrypt the secrete message.
4. Finally original secrete message is retrieved.

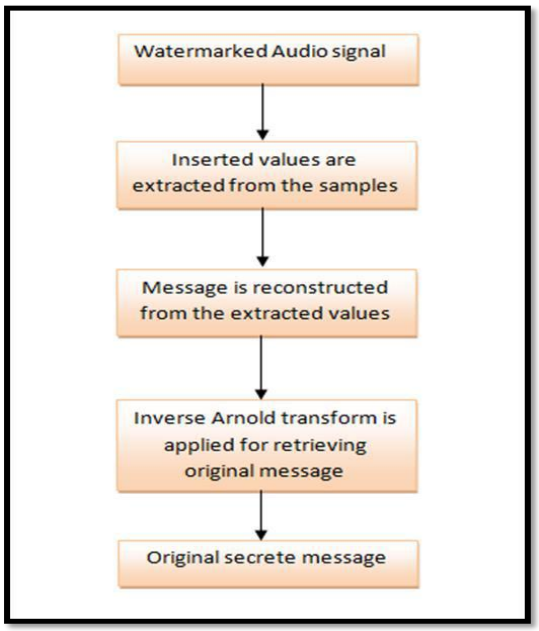

Figure 2: Watermark retrieving procedure

4. RESULTS:

In this research we have used open source dataset of audio files and images. From which we have used 5 different audio files as cover audio. We have tried different combination of cover audio as well as watermark image to validate the proposed method.

.

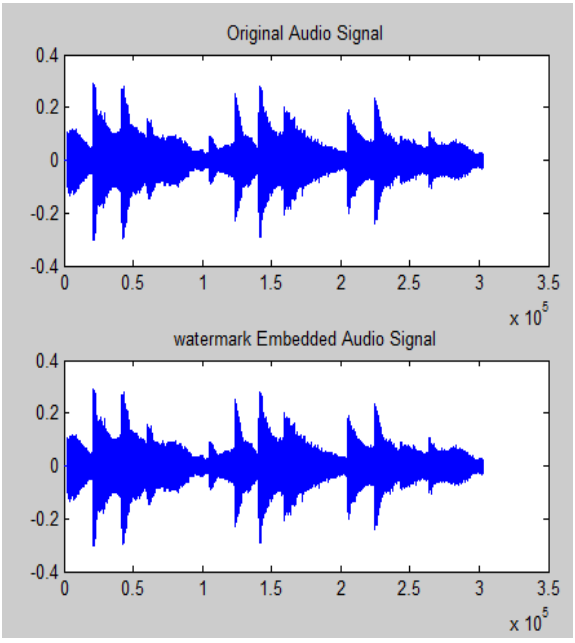

Figure 3: cover audio file and watermarked audio file

Figure 3 describes the results of proposed watermark insertion methods. The first part contains the original audio and second part contains the combination of watermarked and original audio. Same way figure 4 describes results of proposed watermark retrieval method.

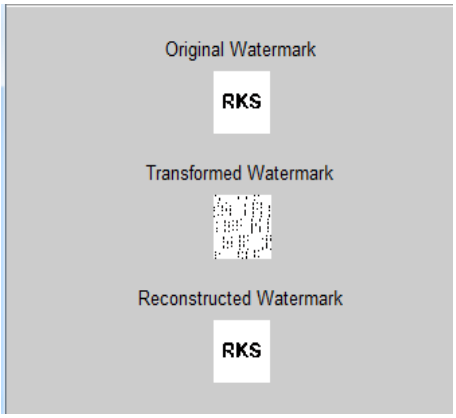

Figure 4: Retrieved watermark images

5. ANALYSIS OF RESULTS:

To check robustness and perception transparency we have calculated mean square error (MSE), peak signal-to-noise ratio (PSNR) similarity factor (SF)

A. *Mean Square Error*

The Mean Squared Error (MSE) is maybe the most significant measure used to evaluate the performance of an analyst or an estimator. (The subtle distinction between analyst and estimators is that arbitrary variables are analyzed and values are projected). For the calculation of this function we need to focus on original values and values retrieved after the experiment. It is defined as below [6].

$$MSE = \frac{1}{xy}\sum_{a=0}^{x-1}\sum_{b=0}^{y-1}[A(a,b) - K(a,b)]^2$$

B. *Peak Signal to Noise Ratio*

The *Peak Signal to Noise Ratio* (PSNR) mass computes the peak signal-to- noise ratio between two images. This ratio is regularly used as a value capacity between the original and retrieved image. The high value of PSNR indicates the superior quality of reformed image [6]. The PSNR is the ratio between two images used to compare the image quality. PSNR for image with size L x M is given by [7]:

$$PSNR = 10 * \log_{10}\left(\frac{255}{\sqrt{\frac{\sum_{a=1}^{L}\sum_{b=1}^{M}[A(a,b) - A'(a,b)]^2}{L * M}}}\right)$$

Where A (a, b) is the original Audio, A'(a, b) is watermarked Audio and L, M are the size coordinates of the images. In general for gray scale image, the maximum pixel value is 255 and they are represented with 8bits. In general, more than 28 values of PSNR are acceptable for images [6].

C. *Similarity Factor*

The Similarity Factor (SF) used for finding the similarity or to find the perception transparency between original and retrieved watermark, the scientist named Cox et. al. provides the equation as described below[4]

$$SF(A, A') = \frac{A * A'}{\sqrt{A' * A'}}$$

In which A is the original and A' is the retrieved watermark image.

Table 1: Information of Audio files and watermark image

Audio File Type	Duration	No of samples	Hiding size (No. of Pixels)
Clock_mantle.wav	00:00:13	302697	3600
Bogos_Drum.wav	00:00:08	177200	3600
duck.wav	00:00:04	411072	3600
FlagRaising.wav	00:00:24	538100	3600
Taps.wav	00:00:32	353430	3600

Table 2: Audio file And Watermark before Embedding

Audio File name	Audio file size (No. of samples)	Watermark file size
Clock_mantle.wav	302697	3600
Bogos_Drum.wav	177200	3600
duck.wav	411072	3600
FlagRaising.wav	538100	3600
Taps.wav	353430	3600

Table 3: Audio file and Watermark after Extraction

Audio File name	Audio file size (No. of Samples)	Watermark file size
Clock_mantle.wav	302697	3600
Bogos_Drum.wav	177200	3600
duck.wav	411072	3600
FlagRaising.wav	538100	3600
Taps.wav	353430	3600

Table 4: Results obtained using Secured Audio watermarking method for uncompressed Audio file

Audio File Name	Watermark Image	MSE	PSNR	SF
Clock_mantle.wav	rks.jpg	0.1414	55.718	0.9998
Bogos_Drum.wav		0.1414	55.718	0.9998
duck.wav		0.1414	55.718	0.9998
FlagRaising.wav		0.1414	55.718	0.9998
Taps.wav		0.1414	55.718	0.9998

Table 5: Effect of noise attack

Audio File Name	Watermark	MSE	PSNR	SF
Clock_mantle.wav	rks.jpg	0.1414	55.718	0.9944
Bogos_Drum.wav		0.1414	55.718	0.9944
duck.wav		0.1414	55.718	0.9944
FlagRaising.wav		0.1414	55.718	0.9944
Taps.wav		0.1414	55.718	0.9944

Table 6: Effect of cropping attack (cropping initial 10% of samples)

Audio File Name	Watermark Image	MSE	PSNR	SF
Clock_mantle.wav	rks.jpg	0.4323	45.234	0.9998
Bogos_Drum.wav		0.4323	45.234	0.9998
duck.wav		0.4323	45.234	0.9998
FlagRaising.wav		0.4323	45.234	0.9998
Taps.wav		0.4323	45.234	0.9998

Table 7: Effect of cropping attack (cropping last 10% of samples)

Audio File Name	Watermark Image	MSE	PSNR	SF
Clock_mantle.wav	rks.jpg	0.4323	45.234	0.9998
Bogos_Drum.wav		0.4323	45.234	0.9998
duck.wav		0.4323	45.234	0.9998
FlagRaising.wav		0.4323	45.234	0.9998
Taps.wav		0.4323	45.234	0.9998

Table 8: Effect of Cropping attack (cropping middle 10% of samples)

Audio File Name	Watermark Image	MSE	PSNR	SF
Clock_mantle.wav	rks.jpg	0.4323	45.234	0.5628
Bogos_Drum.wav		0.4323	45.234	0.5628
duck.wav		0.4323	45.234	0.5628
FlagRaising.wav		0.4323	45.234	0.5628
Taps.wav		0.4323	45.234	0.5628

Table 9: Effect of attacks on proposed method (Summary)

Attacks	MSE	PSNR	SF
Noise	0.1414	55.718	0.9944
Cropping (Initial	0.4323	45.234	0.9998
Cropping (Last 10%	0.4323	45.234	0.9998
Cropping (middle	0.4323	45.234	0.5628

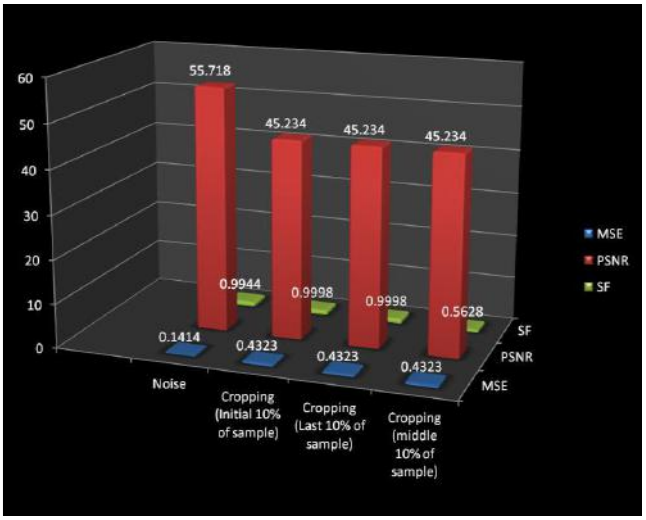

Figure 5: Effect of attacks on proposed method (Summary)

6. CONCLUSION:

We have implemented proposed technique in MATLAB environment. Looking at the Mean Square Error (MSE), Peak Signal Noise Ration (PSNR) and Similarity Factor (SF) it is clearly and safely concluded that the suggested technique provides stronger robustness and perception transparency to the watermarked image and original image against different kind of attacks like noise and cropping.

7. LIMITATIONS:

This experiment has been conducted in the laboratory under controlled environment using MATLAB. It is also important to note that there is nothing to suggest that the same principle may not work in the actual real time environment and give similar results. However this needs to be studied in actual field trial.

8. ACKNOWLEDGEMENT:

Authors acknowledge DG & DY DG of Raksha Shakti University, Ahmedabad for allowing this research work at the aegis of Institute of R&D, Raksha Shakti University, Ahmedabad & we are grateful for their support and guidance.

REFERENCES:

1. Himeur, Yassine, and Bachir Boudraa. "Secure and robust audio watermarking system for copyright protection." Microelectronics (ICM), 2012 24th International Conference on. IEEE, 2012.
2. Yang, Bailong, et al. "Lossless and secure watermarking scheme in MP3 audio by modifying redundant bit in the frames." Information Management, Innovation Management and Industrial Engineering (ICIII), 2013 6th International Conference on. Vol. 1. IEEE, 2013
3. Kabir, Hussain Mohammed Dipu, and Syed Bahauddin Alam. "Hardware based realtime, fast and highly secured speech communication using FPGA."Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on. IEEE, 2010
4. Pooya Monshizadeh Naini, A tutorial on "Digital Watermarking Using MATLAB" University of Tehran, Iran.
5. Deepayan Bhowmik, "Digital watermarking techniques for JPEG2000 scalable image coding" The University of Sheffield, Sheffield, UK
6. MathWorks, "PSNR". [Online]. Available: http://in.mathworks.com/. [Accessed: 01-Nov2015].
7. Seema Malshe (Gondhalekar), Hitesh Gupta, Saurabh Mandloi, "Survey of Digital Image Watermarking Techniques to achieve Robustness", International Journal of Computer Applications (0975 – 8887) Volume 45– No.13, May 2012
8. Z. Tang and X. Zhang, "Secure Image Encryption without Size Limitation Using Arnold Transform and Random Strategies", Journal of Multimedia, vol. 6, no. 2, pp. 202-206, 2011.