

Blind Audio Watermarking for Tamper Detection Based on LSB

Alireza Ghobadi*, A.Boroujerdizadeh*, A.H. Yaribakht*, Roozbeh Karimi*

* Advance Information School, University Technology Malaysia, Malaysia

galireza3@live.utm.my, bali4@live.utm.my, hyamir2@live.utm.my, roozbeh83@gmail.com

Abstract— Recently, the attention of researchers has Audio because of the audio capability to hide data. There is some research to hide data in audio using watermarking technique. Some of them tried to use the watermark technique to protect the audio file of any tampering.

The current research defined in this chapter issue by using cheap audio watermarking and preserves audio files from any tampering. It will discuss more on previous study on tamper detection. The method provides both embedding and extraction solutions.

Keywords— LSB, DCT, Audio watermarking, Tamper detection

I. INTRODUCTION

Multimedia is involved in almost every aspect of human life, and many of us rely on various websites for information on events taking place all over the world. We form opinions based on the content of camera footage, phone conversations, and other recordings. Although some sources give us authentic information, others contain forged content. Concerns regarding how to authenticate multimedia data have led to research in forgery detection, but studies in audio are still limited compared to those in the image and video. Audio carrier includes the content of music, phone conversations, and other recording forms. Although some sources give us authentic information, others contain forged content. Audio forgery techniques could be used to conduct piracy over the Internet, falsify court evidence, or modify security device recordings of events taking place in different parts of the world. Real-world examples can best illustrate the importance of audio authentication.

This project proposed the new method which has been used LSB watermarking method to protect an Audio file from any manipulation. The solution not only has a tamper detection method but also can mark the audio location with highly accurate. It can detect any changes in the audio file less than 1/20000 seconds. For evaluation has been used BER to show the error rate during converting from frequency to bite and reverse and SNR to evaluate and quality changes.

II. RELATED WORK

In order to create a protective layer a self-embedding method has proposed in [1]. In this method audio signal will self-embedded into itself. To do so the signal is divided into 4 segments. The features of each segment are embedded into another segment using the least significant bit (LSB).

Choosing the target segment is randomly based on the secret key. By comparing the segments and their corresponding features, tamper detection is possible.

In [2], a multipurpose watermarking method is hired in order to provide copyright protection and authentication. For authentication a fragile watermark is embedded using the wavelet coefficients; and for copyright protection a robust watermark is embedded using discrete wavelet transform into the signal.

Due to the lack of proper plain text copyright protection, [3] has proposed a zero-watermarking method which is able to do the authentication as well as copyright protection. This algorithm is dedicated to text documenting. The algorithm is robust against modification and at the same time can detect whether the text is tampered or not.

In [4], based on Principal Component Analysis (PCA) a new audio watermarking algorithm is presented. In this algorithm wavelet packet decomposition is watermarked into the audio file. The decomposition itself is an encrypted matrix from PCA. This algorithm is able to detect and locate the tamper.

Since interpolation attack is one of the major known sources of audio tampering, a blind watermarking method with forensics approach is proposed in [5] in order to detect interpolation forgery. This attack causes statistical changes in linear dependencies. As singular value decomposition is a suitable method to express the linear dependencies, it is hired in this paper. By analyzing the audio file using SVD it is possible to find and locate any changes in the audio signal.

Another technique for tamper detection based on steganography is presented in [6]. In this method a watermark which is generated using integrated discrete cosine transform (in DCT) is embedded into the signal. Amplitude expansion in the high-frequency spectrum is hired to prepare a space for embedding. Comparing the extracted data with the original hash value can detect any tampering.

[7] is hired reversible watermarking in order to authenticate the transmitted signals and then removing watermark to reaching the original signal.

All of the researches which have been explained as above, with some more researches summarized in Table 1. The table shows the audio watermarking for tamper detection and recovery, measurement methods and the tax which was conducted experiment based on them. The table will be used on contribution section to show why the new method has been caused. The conduction experiment has been designed based on Table 1.

Table 1: Recently tamper detection papers based on methods

No.	Year	Title	Watermark Method	Purpose	Measurement Method
1	2008	A Fragile Watermarking Scheme for Audio Detection and Recovery	LSB	Fragile	BER SNR
2	2008	A multipurpose audio watermarking scheme for copyright protection and content authentication	DCT	Fragile	NC SNR
3	2010	A New Fragile Audio Watermarking Scheme	DCT		
4	2009	Audio Digital Signature Algorithm with Tamper Detection	SVD DCT		
5	2010	Detection of Audio Interpolation Based on Singular Value Decomposition	FFT, SVD	Semi-Fragile	SR AR
6	2004	Tamper Detection and Localization for Categorical Data Using Fragile Watermarks	DWT SVD	Fragile	BER
	2010	A New Approach of Reversible Acoustic Steganography for Tampering Detection	DCT	Semi-Fragile	SNR
8	2011	Reversible Watermarking for Digital Audio Based on Cochlear Delay Characteristics	PEAQ LSB	Fragile	MSE BER

This section explained audio watermarking, audio watermark characteristics, attacks on audio watermarking, and tamper detection definitions. It is continuing with the related work. The section organized by two sections. First section abstracts recently audio watermarking techniques. The second section includes especially explained the tamper detection methods. Both of the section concluded by the table to summarize related works. The next chapter will be explained the methodology, operational methods, and list down the phases to implements of the research.

III. ALGORITHM AND IMPLEMENTATION

WTDM is the new idea to use fragile watermark and detect and tampering with the audio file. Based on the previous chapter, the most of the researchers have been used frequency and time masking to detect the tampering. The proposed algorithm produces a small hash signature by computing a limited number of random projections of a perceptual, time-frequency representation of the original audio stream. The other researcher works on Wavelet packet decomposition were implemented to audio files. All the terminal coefficients of the wavelet packet decomposing tree were used as the data matrix.

Based on the input request, the output of the system could be the audio file with the tampering file or reports of the tampering places.

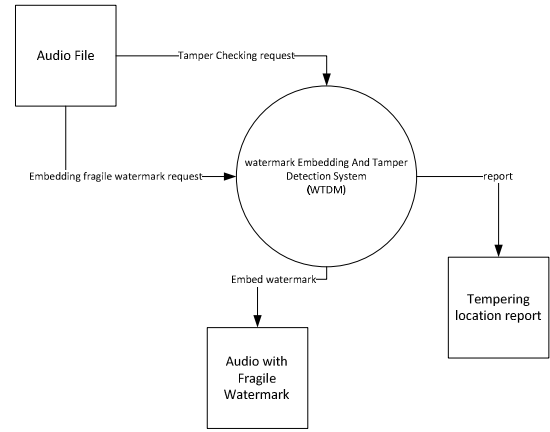


Figure 1: WTDM architecture

The Algorithm consists of two parts; embedding Algorithm embed the LSB and Matrix (focusing on adding watermarks to the audio); and extract watermarking (to do detect tampering processes).

A. WTDM Embedding watermark process

In the embedding methods, explains as a detail of process from converting audio file to the vector, normalization of the vector, converting the matrix form, calculation of mean for each column and embedding the mean by LSB method. For more understanding, each part is explained by the mathematical model.

The wavelet audio of a signal x is calculated by passing it through a series of filters. The size of the vector is s . At the first the audio convert to the vector x as below:

$$\forall s \in N, \forall s \in R, v(s) = \{v_1, v_2, \dots, v_s\} \quad (1)$$

The vector range belongs to the Real number. Because the embedding process needs to have a range of Natural number then needs to be limited to the natural number (The limitation is defined as 0 to 255, Because the vector number converts to the eight bit number, it is necessary to be in this range). To arrange the limitation, all members multiple to ten thousand (To reduce error) and then using mode function by 255 (mode helps to remove negative number and also has the numbers in the range 0 to 255). The calculation has been defined as (2).

$$\forall 0 \leq i < s, s \in N, x(i) = (v(i) * 10000) \bmod 255 \quad (2)$$

As previously explained, the first issue is to find the relation between the vector members. The solution for this issue defines a matrix. To create the matrix, first has to find the number of the row and column. The number and column define as (3), and (4).

$$\forall c \in N, \begin{cases} c = \lfloor \frac{s}{9} \rfloor & \text{if } s \bmod 9 \neq 0 \\ c = \lfloor \frac{s}{9} \rfloor + 1 & \text{if } s \bmod 9 = 0 \end{cases} \quad (3)$$

$$\forall r \in N, r = \{1, 2, 3, \dots, 9\} \quad (4)$$

$$\forall i, j \in N, i = s \bmod 9, j = \frac{s}{9} \Rightarrow$$

$$\begin{cases} m(i, j) = x(s) & \text{if } i \neq 0 \\ m(i, j) = \text{mean}(\sum_{k=1}^8 m(k, j)) & \text{if } i = 0 \end{cases} \quad (5)$$

For more understanding, give an example. The test is five seconds wave format audio. When convert it to vector x, the size of the vector is 19100. Then can define a matrix as below:

$$s \bmod 9 = 2 \quad (6)$$

$$(2) \text{ and } (5) \Rightarrow C = \lfloor 19100/8 \rfloor + 1 = 2387 + 1 = 2388(7)$$

The matrix should be $m(9, 2388)$. The next step is to transfer vector's member x to this matrix by formula (5). The matrix should be as below:

$$m_{9 \times 2388} = \begin{pmatrix} x_1 & \dots & x_{19099} \\ \text{mean}(\sum_{k=1}^8 m(k, 1)) & \dots & \text{mean}(\sum_{k=1}^8 m(k, 1)) \end{pmatrix} \quad (8)$$

The mean is the strong connection between eight members. If there are any changes on one of them, then the mean is changing. Figure 2: The vector's member's relation. shows how the members are related by Mean.

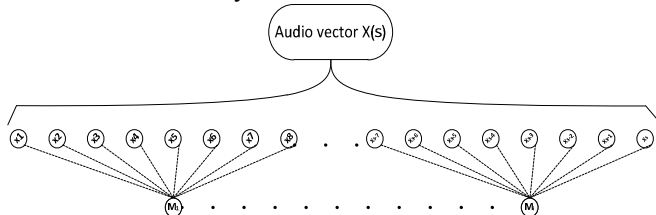


Figure 2: The vector's member's relation.

After calculate mean and create matrix $m_{i \times j}$ to make a relation to these eight members. For this reason, convert matrix $m_{i \times j}$ from decimal to the binary and insert to matrix $n_{i \times j}$. Then, embed each of eight binary members of the mean of the eight members of the same column. The Figure shows the process in phase to embed mean binary to the same column members.

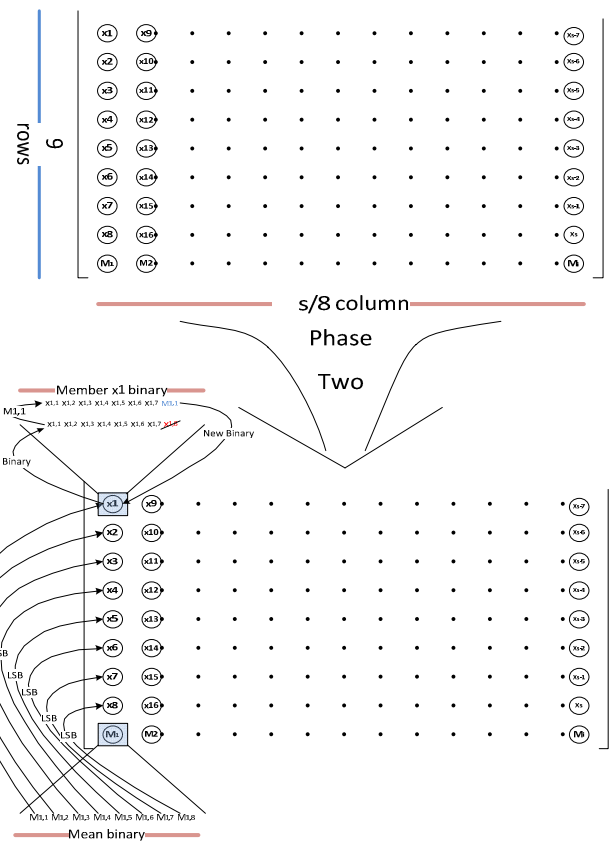


Figure 4: Embedding LSB watermarking process in phase two

The last phase is to return to the vector $y(s)$. The process is the reverse process of the first phase. The data read from the first member of the matrix and restore on a new vector. The Figure 3 shows the way that convert matrix to vector.

$$\forall t \in N, j \in N, t \in N, t = i \bmod 9, j = i/8 \quad (9)$$

$$y(i) = m(t, j) \quad \text{if } i \neq 0 \quad (10)$$

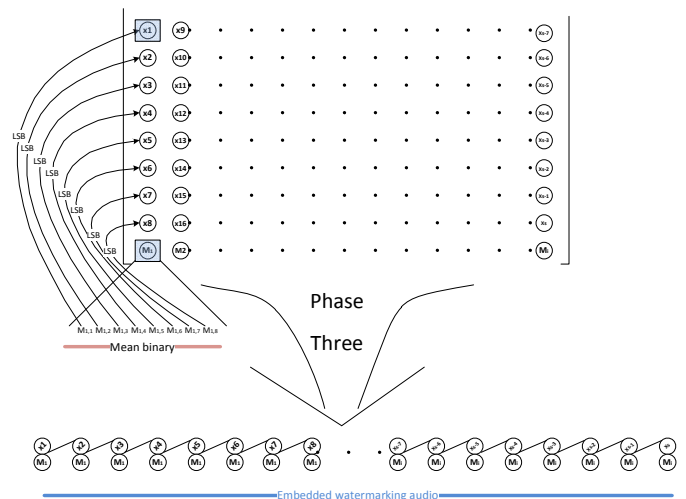


Figure 3: Convert matrix to the new audio vector

After transfer audio wave to the vector, in the step one first collect first eight members of and calculate N_1 (Mean of eight members). In step two, extract first binary number of each member and arrange it. Then convert it to decimal M_1 compare M_1 and N_1 based on (10) equation.

$$N_1 - 1 \leq M_1 \leq N_1 + 1 \quad (11)$$

If the mathematical relation (11) established, then the tampering not detected then will be selected the next eight members return to step one. If (11) is not established the tampering, then choose the members from Y (2) until X (11) return to step one. In this tampering detection find keep the position of the first member collection. The step three repeats until the (11) relation established, and then record the new position. The tampering happened from the first member position until the new member position. Figure 45 shows the process in one shot.

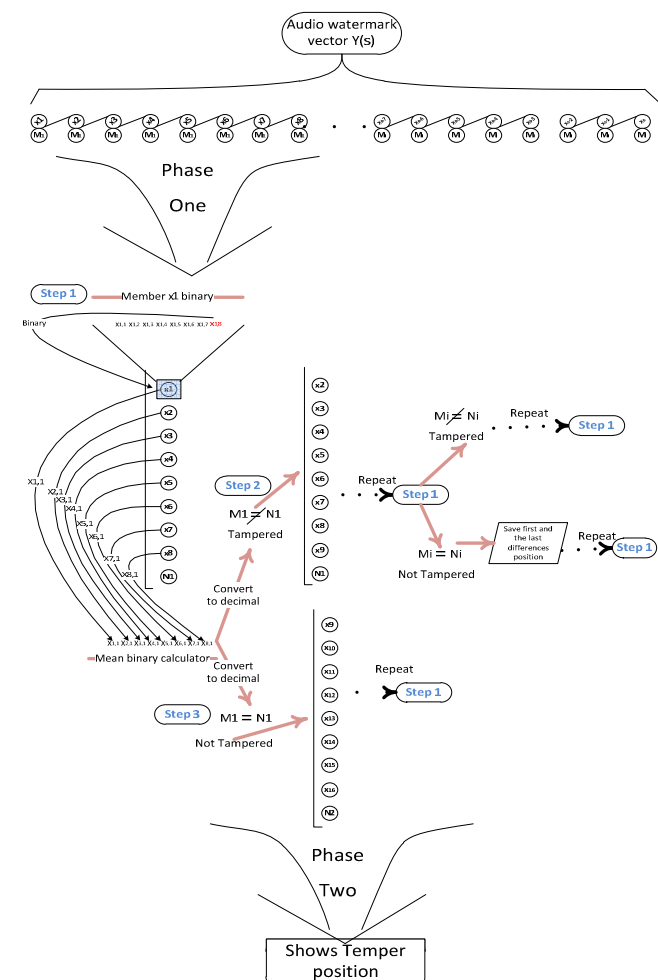


Figure 4: Extraction process

IV. EXPERIMENTAL RESULTS AND ANALYSES

WTDM was implemented using the Matlab programming language, implemented on windows. It was tested under the

setup and configuration shown in Figure 1. The experiments were conducted using several audio files and attacks. The files classified by the numbering. It helps easily understand and trace. To numbering on Each tamper file, using the original file number with different tampering numbers which consider as the kind of attack (Table 4). For example if the original file name is “1.wav”, then the tampering files related to it are “1.1.wav”, “1.2 wav”, and “1.3.wav”. The file with the name “1.1.wav” is the tampering model by attack croppingThe attack selectors refer to the other research attacks have been used by other researchers.

Table 2: Attack classification number

No	Attack name	Attack number
1	Cropping (deleting some part of Audio)	1
2	Cropping (Change time frequency)	2
3	Low and high filtering	3

All of the original files, tampering files and detail information to conduct experiments have been shown in Table 3. This table shows that the vector size, and the duration size.

Table 3: List of sample audio files for test

No.	The original audio		Audio watermark name	Audio tamper name		
	Name	Size (s)	Vector size	Name	Size (s)	Vector size
1	1.wav	5	90309	1.1.wav	3.5	84364
2				1.2.wav	5	90309
3				1.3.wav	5	90123
4	2.wav	3	56066	2.1.wav	4.3	77679
5				2.2.wav	3	57023
6				2.3.wav	3	75294
1	3.wav	7	126603	3.1.wav	7.9	142688
2				3.2.wav	7	125622
3				3.3.wav	7	126328

A. Sample Testing Process

The testing of the system was done based on the Table 3. In this section, explains the input original and tamper audio files. To do shows them, using a graph. The graph is not only showing them graphically, but also can find the differences between these two files. To embed watermarks and showing the quality result has been conducting based on SNR and BER. BER shows any error during converting data on after embedding watermark method, and extracting the audio tampering location. The next section shows original and tampering files using Matlab tools. These files are used as the input files to the system. In this section extracts information about original and tampering file include the graph of the wave figure.

B. Original audio file before watermarking

Based on the. Original file (named 1.wave) has been used. Based on

Figure 5, the number of this file vector member's value is 90309 members.

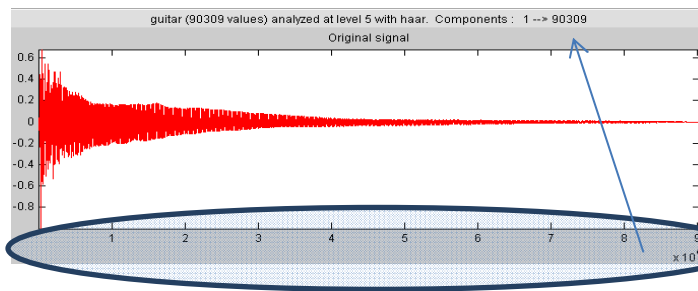


Figure 5: The original audio wave file.

C. Audio file after watermarking

Figure 7 shows the wave frequency format (file name is "guitar1.wav"). The Figure 66 shows the graph of the original wave file based on the Haar model. The Figure 66 shows the number of this file vector member's value is 90309 members, which is not changing the watermark. Also, this figure shows that the waveforms is not changing much. The part where the wave part higher than 0.8 has some small changes. To have less effect compare with original files used the LSB model.

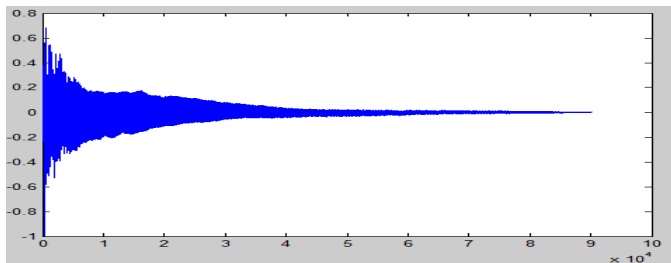


Figure 6: The audio watermark wave file.

This table shows that these measurement methods are NC, PSNR, SDG, ODG, MSE, PSR, SIM, BER, and SNR.

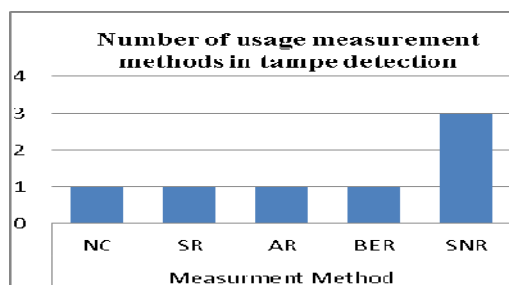


Figure 7: The measurement methods statistic for tamper detection

D. Result and discussion

The result has been checked by BER which is check any changes during converting audio to vector and vector to audio and SNR to check the quality after embedding watermarking. Based on "implementation section" explanation and Figure 3, because has been used LSB as embedding Mean to each eight member, expected that is not watermarked on the audio watermarking. This theory has been proved by the conducted experiments result.

Table 4: Measurement table based on SNR and BER

No.	File name	Vector size	SNR	BER
1	1.1.wav	84364	39.41	0.9341
2	1.2.wav	90309	42.96	1
3	1.3.wav	90623	36.23	0.996
4	2.1.wav	77679	39.36	0.722
5	2.2.wav	57023	47.68	0.978
6	2.3.wav	75294	40.19	0.745
7	3.1.wav	142688	39.28	0.877
8	3.2.wav	125622	50.14	0.992
9	3.3.wav	126328	39.09	0.997

The result focuses on two parts, the tampering detection location and also the quality of the audio which is watermarked. The SNR result has been accepted if the SNR is between 30 (db) until 70 (db). Table 3 shows the audio quality result based on SNR measurement. The result is between acceptable ranges.

The BER column shows that the differences Bite error Rate. This error rate also shows that the quality is not changed much when the watermark applies to the original file. The last table which explains the differences between other research there are two comparable graphs. The first comparison graph shows that the SNR evaluation method. The SNR has been calculated by below formula:

$$SNR(S, S') = 10 \log \frac{\sum_{n=1}^L s(n)^2}{\sum_{n=1}^L [s(n) - s'(n)]^2} \quad (12)$$

Figure 8 shows the SNR result the original and the watermarked audio for the past three papered (review in related work) new purposed model. The result shows that the proposed method achieves better transparency of work.

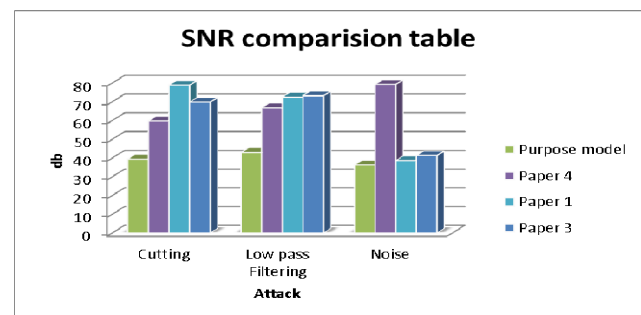


Figure 8: SNR comparison table between previous work and new algorithm

The other measurement methods (which are related to quality) are BER. The BER calculate based on the bit error rate between the original file and the watermark file based on below formula:

$$BER = \sum_{n=1}^L s(n) / s(n') \quad (13)$$

The result shows the new purpose model has been reduced bit error rate compare to next three previous models. The most significant factor is that the new model using bit vectors instead of the frequency model. In the frequency mode,

converting noise effected and the bite rate normally is not the same between original and watermark file. Figure 910 shows the attacks based on the experiment which conducted an experiment.

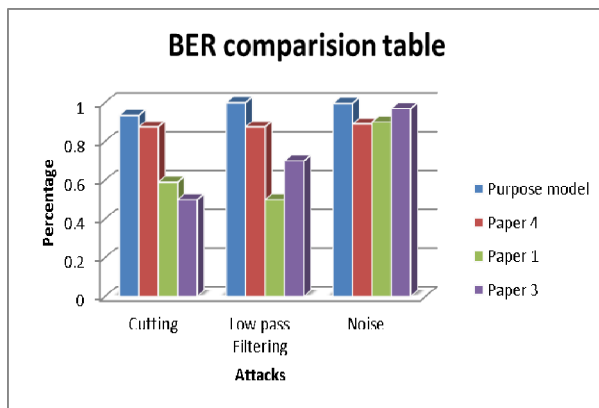


Figure 9: BER comparison table between previous work and new algorithm

V. CONCLUSION AND FUTURE WORK

The most of the methods on the audio tamper detection has been used the frequency masking and threshold to find the tamper location (FFT). There is a new idea to novelized frequency for the low and high and change frequency data to the matrix model. There are three issues that have to consider in the new methods. First of all has to find the way to transfer wave format to the descriptive format. The second issue is to find the strong relation between these discrete members. The late one find the fragile watermarking easy implement, detect and extract with less effective to the audio quality (As mention before, the audio is easily detected by human).

This paper focuses on the audio tamper detection method in the wavelet format. The project goal is to use a fragile watermark algorithm to detect any changes in the audio file. The method should detect any tampering and show the tamper location.

The new enhance algorithm, combined DCT, FFT, and DWT methods and introducing an algorithm that provides a strong connection between audio vector members. The result shows that the new enhance algorithm, has less effect to the audio size and audibility is detected by the ears.

The solution more attention to quality to keep the originality of the files, reduces the bit error rate in the process, and increase accuracy of tamper detection. This severity with another model which has been tested just shows the area of tampering. The new purposed methods can find tampering in less than 1/20000 (S).

REFERENCES

- [1] al-Yaman, M. S., Al-Taei, M. A., And Alshammas, H. A. Audio-Watermarking Based Ownership Verification System Using Enhanced Dwt-Svd Technique.
- [2] Anastasijevic, A., And Coja, D. (2011). Audio Watermarking Using Frequency Hopping Method 1586-1589.
- [3] Anderson, R. (1996). Information Hiding: First International Workshop, Cambridge, Uk, May 30-June 1, 1996: Proceedings. (Vol. 1): Springer Verlag.
- [4] Anderson, R. J., Kuhn, M. G., And Petitcolas, F. A. P. (1998). Attacks On Copyright Marking Systems 218-238.
- [5] Arnold, M. (2000). Audio Watermarking: Features, Applications And Algorithms 1013-1016 Vol. 1012.
- [6] Arnold, M. K., Schmucker, M., And Wolthusen, S. D. (2003). Techniques And Applications Of Digital Watermarking And Content Protection. Artech House Publishers.
- [7] Barni, M., And Bartolini, F. (2004). Data Hiding For Fighting Piracy. Signal Processing Magazine, Ieee. 21(2), 28-39.
- [8] Bender, W., Gruhl, D., Morimoto, N., And Lu, A. (1996). Techniques For Data Hiding. Ibm Systems Journal. 35(3.4), 313-336.
- [9] Busch, C., Funk, W., And Wolthusen, S. (1999). Digital Watermarking: From Concepts To Real-Time Video Applications. Computer Graphics And Applications, Ieee. 19(1), 25-35.
- [10] Chen, F., He, H. J., And Wang, H. X. (2008). A Fragile Watermarking Scheme For Audio Detection And Recovery 135-138.
- [11] Depovere, G., Kalker, T., Haitsma, J., Maes, M., De Strycker, L., Termont, P., Et Al. (1999). The Viva Project: Digital Watermarking For Broadcast Monitoring 202-205 Vol. 202.
- [12] Fastl, H., And Zwicker, E. (2007). Psychoacoustics: Facts And Models. (Vol. 22): Springer-Verlag New York Inc.
- [13] Fotopoulos, V., And Skodras, A. N. (2003). Digital Image Watermarking: An Overview. Eurasp Newsletter. 14(4), 10-19.
- [14] Hartung, F., And Kutter, M. (1999). Multimedia Watermarking Techniques. Proceedings Of The Ieee. 87(7), 1079-1107.
- [15] Jalil, Z., Mirza, A. M., And Iqbal, T. (2010). A Zero-Watermarking Algorithm For Text Documents Based On Structural Components 1-5.
- [16] Kim, J., And Lee, Y. An Inaudible Pseudonoise Sequence Generation For Digital Audio Watermarking.
- [17] Koenig, B. E., And Lacey, D. S. (2009). Forensic Authentication Of Digital Audio Recordings. J. Audio Eng. Soc. 57(9), 662-695.
- [18] Kozaczuk, W., And Kasperek, C. (1984). Enigma: How The German Machine Cipher Was Broken, And How It Was Read By The Allies In World War Two. University Publications Of America.
- [19] Kraetzer, C., Oermann, A., Dittmann, J., And Lang, A. (2007). Digital Audio Forensics: A First Practical Evaluation On Microphone And Environment Classification 63-74.
- [20] Le, T. H. N., Nguyen, K. H., And Le, H. B. (2010). Literature Survey On Image Watermarking Tools, Watermark Attacks And Benchmarking Tools 67-73.
- [21] Maha, C., Maher, E., And Chokri, B. A. (2008). A Blind Audio Watermarking Scheme Based On Neural Network And Psychoacoustic Model With Error Correcting Code In Wavelet Domain 1138-1143.
- [22] Maher, R. (2010). Overview Of Audio Forensics. Intelligent Multimedia Analysis For Security Applications, 127-144.
- [23] Moriya, T., Harada, N., Kamamoto, Y., And Sekigawa, H. (2006). Mpeg-4 Als—International Standard For Lossless Audio Coding. Nit Technical Review. 4(8), 40-45.
- [24] Salma, M., Maha, C., And Chokri, B. A. (2010). A Robust Audio Watermarking Technique Based On The Perceptual Evaluation Of Audio Quality Algorithm In The Multiresolution Domain 326-331.
- [25] Shi, Q., And Ma, X. (2011). Detection Of Audio Interpolation Based On Singular Value Decomposition 287-290.
- [26] Tibbitts, J., And Lu, Y. (2009). Forensic Applications Of Signal Processing. Signal Processing Magazine, Ieee. 26(2), 104-111.
- [27] Unoki, M., And Miyauchi, R. (2011). Reversible Watermarking For Digital Audio Based On Cochlear Delay Characteristics 314-317.
- [28] Yang, R., Shi, Y. Q., And Huang, J. (2009). Defeating Fake-Quality Mp3 117-124.
- [29] Yang, X., Wu, X., And Zhang, M. (2009). Audio Digital Signature Algorithm With Tamper Detection 15-18.
- [30] Zhao, X., Guo, Y., Liu, J., And Yan, Y. (2011). A Spread Spectrum Audio Watermarking System With High Perceptual Quality 266-269.