Encrypted Audio Watermarking in Frequency Domain

Uma R. Nair(✉) and Gajanan K. Birajdar

Department of Electronics and Telecommunication, Pillai HOC College
of Engineering & Technology, Raigad, Rasayani 410206, Maharashtra, India
uma.nair20@gmail.com, gajanan123@gmail.com

Abstract. Watermarking methods have been utilized for safeguarding contents against unlawful replication. New immune watermark introduction and retrieval mechanism constituting FFT based approach along with chaotic encryption is presented here. Encrypting the procedure develops a secure environment for the scheme. The primary audio undergoes Fast Fourier Transformation. Introduction of encrypted secret contents is accomplished adopting Fibonacci numbers. Retrieval of mark is achieved by non-informed scheme. Error rate as well as SNR outcomes are the execution specifications computed for this method. Here robust quality in opposition to distinct processing actions like reverberation, echo and smoothness is administered. Also greater imperceptibility procured by this method demonstrates the proprietary rights of initial content.

Keywords: Encryption · Audio watermarking · Fast fourier transform · Information security

1 Introduction

With the upswing in technology massive conveyance of digital contents has been actualized. It has also induced unlawful distribution of digitalized contents. Watermarking can be utilized as an effective method against unwanted reproduction of data to impart content verification. Digital audio watermarking is the mechanism of inserting a mark in initial audio [2].

A watermarking strategy must full fill the four indispensable prerequisites like perceptual transparency, robust aspect, payload along with security. Audio watermarking mechanism comprises of mark insertion and removal. Introduction of the secret data into the initial signal is exercised by embedding process while, extraction process is employed to acquire back the secret data [3]. Marking mechanism is divided in two types (a) time based techniques (b) transform based techniques.

The article proposes watermark scheme utilizing Fourier based approach and encryption. Here chaotic scheme is employed for encrypting the secret image since it accomplishes greater encryption capability. Here first host is sub-divided in blocks. Later the chaotic encrypted mark is introduced adopting Fibonacci

A. Unal et al. (Eds.): SmartCom 2016, CCIS 628, pp. 573–580, 2016.
DOI: 10.1007/978-981-10-3433-6_69

numbers into initial data. Chaotic scheme endeavours transmission of the mark securely. Fibonacci numbers on the other hand intensifies the imperceptibility of the scheme.

Remaining paper is put in order as enlisted: Sect. 2 contains survey of prior work. Section 3 puts forth the proposed system model. In Sect. 4 elaborates the chaotic scheme. In Sect. 5 experimental outcomes of scheme that is robust quality along with imperceptibility is considered. Section 6 winds up this article.

2 Literature Survey

Time based techniques performs insertion of mark without any transformation. In [15] GA scheme is demonstrated to overcome the inferior robust nature. Here data is introduced in deeper blocks and other contents are amended to reduce the faults. The prior echo schemes having inferior security outcomes are tackled in [10] by adopting pseudo noise distribution. Combination of pseudo noise distribution along with decipher action is suggested in it.

In transform domain the frequently adopted mechanisms are DWT, DCT as well as FFT. In [4] the initial information is disintegrated in lower and higher spectrum utilizing wavelet related approach. The mark is introduced employing maximized quantized index. Dependence between the successive aggregation of fragments is utilized in [12] for the watermark in DCT approach. Descriptive connection among the fragments is preserved in order to reveal the exact introduction of mark.

Employing FFT produces translation invariant characteristics for the mark. Two correlative insertion approaches are constructed utilizing the watermark mixture scheme as described in [9]. FFT related model is used to introduce correlative marks. Initial mark is introduced by affirmatively modulated method whereas the later one is introduced by anti-affirmatively modulated method. Variable byte geometric unvarying watermark method utilizing LCM is demonstrated in [6]. Scheme mentioned in [13] incorporates two condition which produces a superior quality mark. Acquisition of the intended spectrum being the initial one and adjusting the index extent being the other one. Data utilising FFT scheme is introduced by adjusting the index extent. The mark is introduced in coefficients through the above aspect employing a key produced capturing arrangement. A strategy to preserve the information by introducing a mark which can withstand distortions is considered in [8]. The mark insertion and retrieval is accomplished utilizing FFT transform based technique. The mark can be withdrawn employing hidden keys accompanying slight deformity. Mark method employing acoustic features along with fourier scheme is considered in [14]. Here mark is inserted in phase segments of contents following the transform. In [7] composition devoted watermark method to withstand TSM attacks is projected. Here the marks are introduced in the chosen stable greater energy locations. These locations intend to be unmodified for preserving greater audibility.

3 Proposed System

Sound perceiving characteristic of human ear diminishes while approaching higher spectrum so in the considered method secret information is introduced in higher spectrum. Two specifications (i) frequency band (ii) frame size are arranged prior to insertion procedure. Frame size influences the robust nature while frequency band influences imperceptibility as well as capacity. Here high frequency is adjusted as 16 kHz or lesser at the beginning. In addition, division of higher segments in frames of span, s = 7 is implemented.

3.1 Inserting Watermark

In the method put forward watermark employing fourier based scheme and chaotic encryption is accomplished. Figure 1 lays out the insertion procedure.

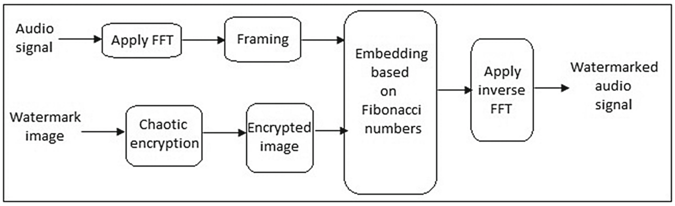

Fig. 1. Watermark insertion procedure of considered method

Steps of introducing the mark is observed as below.

1. Execute fourier transform to compute the FFT coefficients.
2. Separate fourier constituents in frames.
3. Encrypt the watermark image using chaotic encryption.
4. The y-th greatest Fibonacci number for FFT fragment is estimated which is less than FFT coefficients magnitude.
5. FFT marked fragments are acquired by (1) and (2).
   If encrypted mark bit is obtained as zero, then

$$A^{'} = \begin{cases} A_y, & \text{if } y\,mod\,2 = 0; \\ A_{y+1}, & \text{if } y\,mod\,2 = 1. \end{cases} \tag{1}$$

   here y stands for y-th Fibonacci number.
   If encrypted mark bit is obtained as one, then

$$A^{'} = \begin{cases} A_{y+1}, & \text{if } y\,mod\,2 = 0; \\ A_y, & \text{if } y\,mod\,2 = 1. \end{cases} \tag{2}$$

6. Marked data is achieved by inverse FFT.

3.2 Recovering Mark

Non informed approach of watermarking is applied, as initial information is not necessary throughout the retrieval procedure. Figure 2 lays out the retrieval procedure.

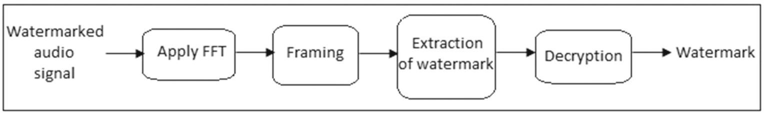

Fig. 2. Watermark retrieval procedure of considered method

Steps of retrieving the mark is observed as below.

1. Execute fourier transform to compute the FFT coefficients.
2. Separate fourier constituents in frames.
3. In the chosen frequency group for individual FFT element acquire nearest Fibonacci number with respect to magnitude of FFT coefficients.
4. Select lesser Fibonacci number as long as distance of FFT elements from two Fibonacci numbers is equal.
5. The retrieval of mark is estimated as:

$$C^{'} = \begin{cases} 0, \text{ if } y \, mod \, 2 = 0; \\ 1, \text{ if } y \, mod \, 2 = 1. \end{cases} \tag{3}$$

   where $C^{'}$ is mark bit recovered from every element.
6. Mark is secured depending on constituents tally that signify either zero or one is acquired following the acquisition of specification regarding the constituents. The identified bit is "0", considering the constituents tally designated as "0" is proportionate or above halved frame extent or else "1" is acquired. Execute the procedure for entire frames.
7. The mark is retrieved securely by decrypting the above obtained information.

4 Chaotic Encryption Technique

Chaotic Baker map is employed for accomplishing chaotic encryption for the mark. The permuted form of the square matrix of information is created by this map which jumbles a square matrix in its discrete format. The map in discretized format considered for J × J matrix is given by (4)

$$D(x,y) = [\frac{J}{w_i}(x - J_i) + y \, mod \, (\frac{J}{w_i}), \frac{w_i}{J}(y - y \, mod \, (\frac{J}{w_i})) + J_i] \tag{4}$$

Here D(x,y) are recent indices of information, $J_i = w_1 + w_2 + ... + w_i, J_i \leq x < J_i + w_i$ and $0 < y < J$. Chaotic encryption is employed since it accomplishes greater encryption capability. Book of the Abacas [5] was formulated by Leonard of Pisa who brought the string recognized as Fibonacci numbers that are 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89. In accordance with [11] musical rhythm comprises Fibonacci sequence.

5 Experimental Outcomes

The album Rust by No, Really [1] is employed for examining the outcomes of the intended method. All elements employ 44.1 kHz accompanying 2 channels in addition to 16 bits for each element. Here 32 × 32 binary image is employed as mark. Outcome is determined by employing SNR, BER and payload.

Plot employing stop payment host is demonstrated in Fig. 3 and marked content is set out in Fig. 4. Initial mark is laid out in Fig. 5 while encrypted mark is demonstrated in Fig. 6. Extracted encrypted mark is laid out in Fig. 7 while decrypted mark is set out in Fig. 8

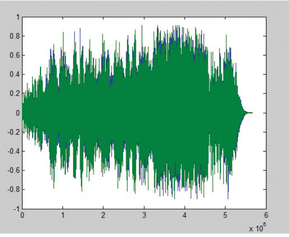

Fig. 3. Host information

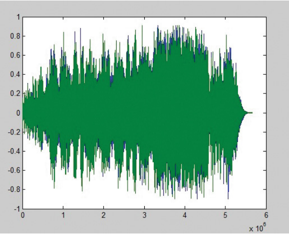

Fig. 4. Marked content

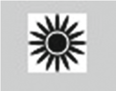

Fig. 5. Mark

Fig. 6. Encrypted mark

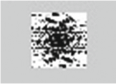

Fig. 7. Extracted encrypted mark

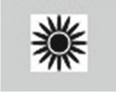

Fig. 8. Obtained decrypted mark

5.1 Robustness Test

Calculation of robust nature of audio signal is performed by Bit Error Rate as:

$$BER(E, E') = \frac{\sum_{y=0}^{Y-1} E(y) \oplus E'(y)}{Y} \tag{5}$$

where length of mark is indicated by Y, yth bit of introduced mark is indicated by $E(y)$ and yth bit of recovered mark is indicated by $E'(y)$. To assess robust feature of suggested mechanism, five separate activities outlined below were implemented.

1. Fusion with noise: Marked content is mixed AWGN.
2. Low-pass filtering: Low pass with termination 15 kHz.
3. Echo: Impairment factor denoting 50 percent with wait time of 100 ms.
4. Reverberation: Marked content with reverberate period 1 s along with extent of −24 dB.
5. Smoothness filtering: Evenly seep through marked content.

Table 1. BER Results for signal processing attacks

Attack name	Stop Payment	Rust	Do You Know
Echo	0.0077	0.0117	0.013
Noise addition	0.0075	0.012	0.012
Smoothness filtering	0.0069	0.010	0.0114
Reverberation	0.0065	0.0104	0.011
Lowpass filtering	0.0072	0.011	0.0114

Table 1 demonstrates that BER vary from 0.0065 to 0.013 during distinct activities for three files that is Stop Payment, Rust and Do You Know Where Your Children Are and hence suggests that mechanism contributes superior outcomes.

5.2 Imperceptibility Test and Payload

Here assessment of perceptual nature regarding audio signal is calculated utilizing SNR. It is computed as:

$$SNR = 10log_{10}\frac{\sum_{y=1}^{Y} E^2(y)}{\sum_{y=1}^{Y}[E(y) - E'(y)]^2} \tag{6}$$

where $E(y)$ is initial content and $E'(y)$ is marked content.

Perceptual transparency of watermark scheme becomes superior by incrementing SNR. The outcomes considering SNR of three files are laid out in Fig. 9. We accomplish that suggested mechanism contributes SNR up to 67.9 decibels from Fig. 9. Content payload specifies content insertion extent of mechanism. Figure 10 displays the content payload for the three audio files with the mechanism attaining payload of 3000 bps.

From the results of Table 2, it is achieved that proposed mechanism produces improved results compared to other mechanisms. Robust nature obtained here is higher along with greater imperceptibility than the other algorithms.

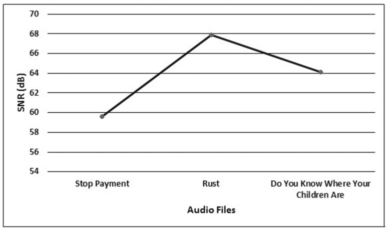

Fig. 9. SNR results

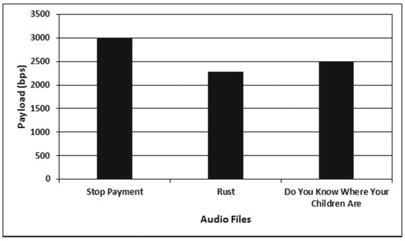

Fig. 10. Payload results

Table 2. Comparison of the proposed method with other schemes

Algorithm	SNR [dB]	BER
[6]	38.8	0.015
[13]	-	0.01
[8]	45.25	-
[14]	43.5	-
[7]	29.5	0.03
Proposed	67.9	0.0065

6 Conclusion

Highly imperceptible watermark inclusion scheme considering audio contents, that contributes robust feature with respect to processing activities is introduced. Greater encryption capability is accomplished utilizing chaotic encryption. Encrypting the procedure develops secure environment for the method. For mark insertion, FFT is exercised on host and later FFT elements are adjusted utilising Fibonacci numbers with encrypted watermark. Scheme utilized here imparts superior SNR and decreased BER along with high content payload. Here we apply non-informed scheme. Outcome of projected mechanism is calculated by employing BER, payload with SNR. By monitoring outcomes and contrasting with existing procedures, it is achieved that audio marking using FFT, chaotic encryption and Fibonacci numbers gives enhanced outcomes.

References

1. No really, rust. http://www.jamendo.com/en/album/7365. 17 July 2014
2. Boney, L., Tewfik, A.H., Hamdy, K.N.: Digital watermarks for audio signals. In: Proceedings of the Third IEEE International Conference on Multimedia Computing and Systems, pp. 473–480, June 1996
3. Cvejic, N., Seppanen, T.: Digital Audio Watermarking Techniques and Technologies: Applications and Benchmarks. IGI Global, Hershey (2007)

4. Hemis, M., Boudraa, B., Merazi-Meksen, T.: Intelligent audio watermarking algorithm using multi-objective particle swarm optimization. In: 4th International Conference on Electrical Engineering (ICEE), pp. 1–5, December 2015
5. Horadam, A.F.: A generalized fibonacci sequence. Am. Math. Mon. **68**(5), 455–459 (1961)
6. Kang, X., Yang, R., Huang, J.: Geometric invariant audio watermarking based on an LCM feature. IEEE Trans. Multimedia **13**(2), 181–190 (2011)
7. Li, W., Xue, X., Lu, P.: Localized audio watermarking technique robust against time-scale modification. IEEE Trans. Multimedia **8**(1), 60–69 (2006)
8. Loytynoja, M., Cvejic, N., Seppanen, T.: Audio protection with removable watermarking. In: 6th International Conference on Information, Communications Signal Processing, pp. 1–4, December 2007
9. Lu, C.S., Liao, H.Y.M., Chen, L.H.: Multipurpose audio watermarking. In: Proceedings of the 15th International Conference on Pattern Recognition, vol. 3, pp. 282–285 (2000)
10. Natgunanathan, I., Xiang, Y.: A novel pseudonoise sequence for time-spread echo based audio watermarking. In: Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM), pp. 1–6, November 2009
11. Nickel, J.: Mathematics: Is God Silent?. Ross House Books, Vallecito (2001)
12. Roy, S., Sarkar, N., Chowdhury, A.K., Iqbal, S.M.A.: An efficient and blind audio watermarking technique in DCT domain. In: Proceedings of the 18th IEEE International Conference on Computer and Information Technology (ICCIT), vol. 1, pp. 362–367, December 2015
13. Seo, Y., Cho, S., Chong, U.: Audio watermarking alogrithm using subband energy. In: 7th International Forum on Strategic Technology (IFOST), pp. 1–4, September 2012
14. Wen, X., Ding, X., Li, J., Gao, L., Sun, H.: An audio watermarking algorithm based on fast fourier transform. In: Proceedings of the IEEE International Conference on Information Management, Innovation Management and Industrial Engineering, vol. 1, pp. 363–366, December 2009
15. Zamani, M., Manaf, A.B.A., Ahmad, R.B., Zeki, A.M., Magalingam, P.: A novel approach for audio watermarking. In: Proceedings of the Fifth IEEE International Conference on Information Assurance and Security (IAS), vol. 2, pp. 83–86, August 2009