Biometric Based Unique Key Generation for Authentic Audio Watermarking

Malay Kishore Dutta[1], Phalguni Gupta[2], and Vinay K. Pathak[3]

[1] Department of Electronics and Communication Engineering, Galgotias College of Engineering and Technology, Greater NOIDA, India
[2] Department of CSE, IIT-Kanpur, India
[3] Department of CSE, HBTI – Kanpur, India
malay_kishore@rediffmail.com, pg@cse.iitk.ac.in, vinaypathak.hbti@gmail.com

Abstract. This paper proposes a method of generating pseudorandom number sequences based on biometric templates of iris image. These sequences are found to be unique in nature. Such sequences can be stored in a database for distinct identification of the extracted keys and they can act as secret keys for audio watermarking with a stamp of ownership unlike arbitrary pseudorandom number sequences and chaotic sequences. Correlation scores achieved under signal processing attacks is more than 0.9 that is significant for identification.

Keywords: Audio watermarking, Biometric based keys, Perceptual transparency, Digital rights management.

1 Introduction

In Digital audio watermarking, embedding of watermark in audio signals is to be made in such a way that it does not degrade the audibility of the signal. Applications of watermarking involve copyright protection to resolve piracy disputes, proof of ownership, broadcast monitoring and secret communication. Several schemes of audio watermarking are proposed in different domains. [1], [2]. A popular method of audio watermarking employs spread spectrum techniques. In a number of the developed algorithms [3], [4] the watermark embedding and extraction is carried out using spread-spectrum technique. Pseudorandom sequences are used in spread spectrum audio watermarking techniques to spread the watermark data across the entire audible spectrum. These pseudorandom sequences are generally generated using methods like random number generator and chaotic maps. Sometime a logo or a symbol is used as a seed to generate the watermark. However if there is a piracy dispute on the ownership the symbol or the logo may not be considered as an adequate proof of ownership. In addition to that a malicious attacker may embed a watermark of a rival counterpart in an audio signal in pirated media files to mislead. As a general perspective a normal random number sequence or a pseudorandom sequence cannot be claimed for ownership until that sequence can be uniquely mapped to an entity that is logically or physically owned by the claimant. These limitations of existing watermarking systems have been a cause of concern and there is a need for more secure and unique authentication methods.

S. Chaudhury et al. (Eds.): PReMI 2009, LNCS 5909, pp. 458–463, 2009.

One way to overcome the above-mentioned limitations is to explore the possibility of mapping a digital watermark to an entity that can be physically or logically owned. Keeping these issues in mind this paper proposes to incorporate biometric data as the seed of the watermark. Biometric features are used for the generation of the watermark key (bio-key*)* for efficient use for identification and authentication. If biometric features are used as a key in a watermarking system then the authentication and ownership issues can automatically be addressed, as the biometric features are unique for any individual and can be mapped in a database.

In order to establish the proposed method of generating bio-key that can be incorporated in the audio signal, iris images are considered. From the iris images iris features are extracted and stored in a database. The method of iris feature extraction has been discussed in Section 2. The correlation between these feature vectors are discussed in section 3. The method of bio-key generation has been discussed in Section 4. The method proposed in [8] has been used to embed and recover the bio key from the audio signal is discussed in Section 5 along with robustness test results. Next section discusses the identification of the extracted bio-keys. Finally concluding remarks are given in the last section.

2 Iris Feature Extraction

Haar wavelet technique is used to extract features from the iris image. The inner iris boundary is localized on the iris image using circular Hough transformation [5], [6]. Once the inner iris boundary (which is also the boundary of the pupil) is obtained, outer iris is determined using intensity variation approach [7]. The annular portion of iris after localization is transformed into rectangular block to take into consideration the possibility of pupil dilation. This transformed block is used for feature extraction using Discrete Haar Wavelet Transform (DHWT). Haar wavelet operates on data by calculating the sums and differences of adjacent values. It operates first on adjacent horizontal values and then on adjacent vertical values. The decomposition is applied up to four levels on transformed rectangular iris block as shown in Fig. 1. A *d*-dimensional real feature vector A_1 is obtained from the fourth level decomposition and is given as

$$A_1 = [\, i_1, i_2 , ..i_d] \qquad (1)$$

Plot of a feature vector and its power spectral density (PSD) is shown in Fig 1 and Fig. 2 respectively. The PSD of the feature vector reveals that the power of the signal is approximately equally distributed in the entire frequency spectrum.

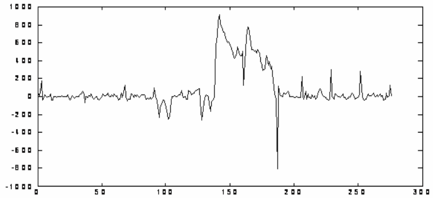

Fig. 1. Plot of an Iris Feature Vector

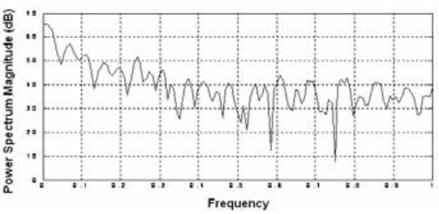

Fig. 2. PSD of the Sample Iris Feature Vector

It is clearly seen from the PSD curve that the power is approximately distributed over the entire frequency range. This property is attractive for spread spectrum techniques [3], [4] where the watermark is needed to be spread across the entire spectrum.

3 Correlation of Feature Vectors

Fig 3 shows the normalized correlation (NC) of the 100th sample feature vector with all other feature vectors in a database of 150 samples. The high spike indicates the autocorrelation of the feature vector. Subsequent to the highest spike in the figure the next highest spike is 0.79 that is the best correlation with some other feature vector in the database. The lowest correlation is found to be 0.61.

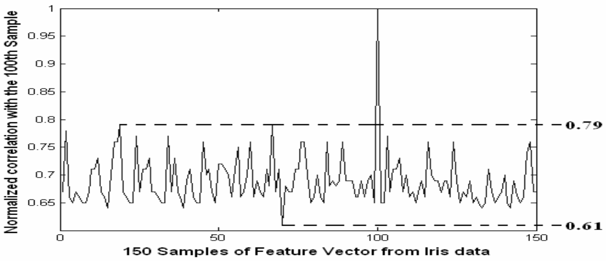

Fig. 3. NC of the 100th Feature Vector with All Others

4 Bio-key Generation From Iris Data

This section presents a novel approach to generate a bio-key from the feature vector of the iris data. The gray scale iris image is resized with 450 × 350 pixel resolution. Using the method described in Section 2 a feature vector *A* is generated from the iris image. The feature vector is then normalized taking the absolute value of the elements. The median element of the vector *A* is used to define a vector *B* such that the element *B(i)* is +1 if *A(i)* is larger or equal to the median element; otherwise it is set to –1. This bio-key that is generated form the feature vector becomes unique. The mean of these bio-keys are approximately equal to zero. Fig. 4 shows the power spectral density (PSD) of a bio-key generated by the method described above. It is clearly evident from the PSD of the bio-key that the power is evenly distributed throughout the spectrum.

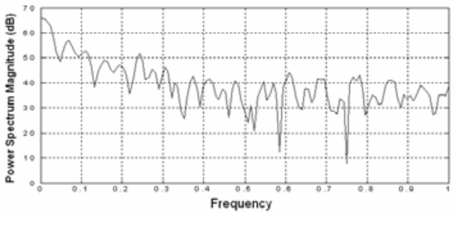

Fig. 4. PSD of a sample Bio-key

The NC between the 100th bio-key with all other samples is shown in Fig 5. The highest spike in the figure is the autocorrelation of the sample that is equal to one. It can be seen from the figure that the maximum correlation coefficient of the bio-key of the 100th sample with rest of the bio-keys is 0.35 while the minimum correlation is 0.1. This correlation is much lesser than the correlation of the same feature vector with other feature vectors. This reduction in the correlation allows having optimal values of threshold for unique detection of the watermark. Fig 6 shows the correlation of the 50th Feature vector with all the other feature vectors of the database (plot A , dotted line) and the correlation of the bio-key generated from the 50th feature vector with all other bio-keys in the database (plot B, solid line). It can be seen that the correlation of the bio-key is comparatively much lesser than the corresponding correlation of the feature vector. These bio-keys with less correlation allow deciding a judicious value of threshold for detection of watermark.

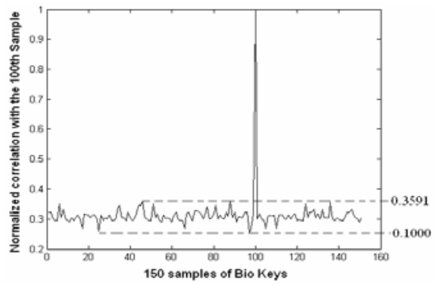

Fig. 5. The NC of the 100th Bio-key with all others

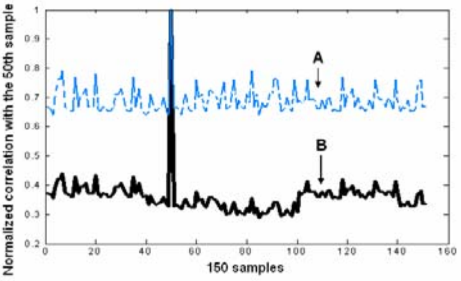

Fig. 6. NC of the 50th Bio-key and 50th Feature Vector

5 Watermark Embedding and Detection

Following the method proposed in [8] an attempt has been made to embed and to recover the bio-keys from the given audio signal. The method selects embedding regions on the original audio waveform based on a threshold in the time domain. The length of the bio-key used in the experiments is 276. A database of 150 bio-keys used for experiments to embed and then recover them from audio signals under signal processing attacks. The robustness test for survival of the bio-keys is shown in Table 1.

6 Identification

Bio keys were picked from a database of 150 samples for embedding in audio signals. These audio signals were then subjected to signal processing attacks and then the bio-key was detected and recovered from the audio signal. For the mapping of the extracted bio- key normalized correlation (NC) is used. The NC of the extracted bio-key is determined with all the keys available in the database. If there is a large difference between the highest NC coefficient and the next highest NC coefficient then we can conclude that the bio key is uniquely mapped in the database.

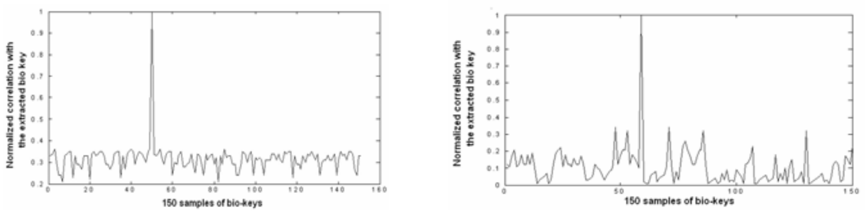

Fig. 7. NC of the extracted bio-key with a database of 150 for two samples (under attack free condition)

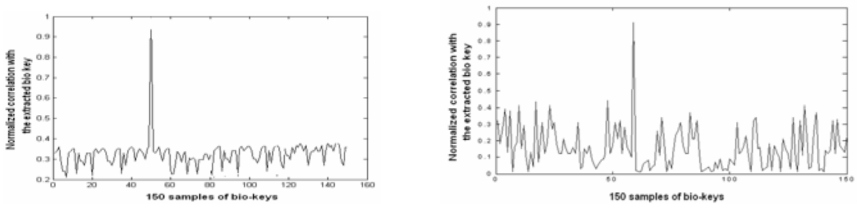

Fig. 8. NC of the extracted bio-key with a database of 150 for two samples. (under TSM attack of + 10%).

Table 1. Robustness Tests against Signal Processing Attacks

Audio File	Type of attack	NC	BER %	Type of attack	NC	BER %
Sample 1 **Tabla** (Indian musical instrument) 18 Sec, 44.1 KHz Sampling, 16 bits/ sample	Attack free Low pass (4 KHz) Low pass (8 KHz) Re-sampling(22 KHz) Re-sampling (11. 5KHz) Add Gaussian Noise	1 0.988 0.991 0.962 0.956 1	0 0 0 0 8 0	TSM (+5%) TSM (+10%) TSM (-5%) TSM(-10%) MP3 (32(kbps) Cropping	0.922 0.911 0.927 0.914 0.997 1	13 16 21 17 1 0
Sample2 **Multiple musical Instruments** 18 Sec, 44.1 KHz Sampling, 16 bits/ sample	Attack free Low pass (4 KHz) Low pass (8 KHz) Re-sampling(22 KHz) Re-sampling (11. 5KHz) Add Gaussian Noise	1 0.981 0.992 0.967 0.942 1	0 0 0 0 11 0	TSM (+5%) TSM (+10%) TSM (-5%) TSM(-10%) MP3 (32(kbps) Cropping	0.922 0.901 0.921 0.904 0.990 1	14 21 16 21 2 0
Sample 3 Classical1 18 Sec, 44.1 KHz Sampling, 16 bits/ sample	Attack free Low pass (4 KHz) Low pass (8 KHz) Re-sampling(22 KHz) Re-sampling (11. 5KHz) Add Gaussian Noise	1 0.978 0.989 0.987 0.949 1	0 0 0 2 10 0	TSM (+5%) TSM (+10%) TSM (-5%) TSM(-10%) MP3 (32(kbps) Cropping	0.922 0.90 0.923 0.901 0.98 1	13 24 13 24 4 0
Sample 4 Piano 18 Sec, 44.1 KHz Sampling, 16 bits/ sample	Attack free Low pass (4 KHz) Low pass (8 KHz) Re-sampling(22 KHz) Re-sampling (11. 5KHz) Add Gaussian Noise	1 0.976 0.932 0.983 0.961 1	0 0 0 2 9 0	TSM (+5%) TSM (+10%) TSM (-5%) TSM (-10%) MP3 (32(kbps) Cropping	0.932 0.913 0.931 0.914 0.991 1	16 19 16 19 1 0
Sample 5 Country 18 Sec, 44.1 KHz Sampling, 16 bits/ sample	Attack free Low pass (4 KHz) Low pass (8 KHz) Re-sampling(22 KHz) Re-sampling (11. 5KHz) Add Gaussian Noise	1 0.943 0.912 0.978 0.954 1	0 0 0 6 0 0	TSM (+5%) TSM (+10%) TSM (-5%) TSM (-10%) MP3 (32(kbps) Cropping	0.95 0.901 0.962 0.909 0.990 1	6 21 8 20 2 0

Results of two such experiments are presented in Fig 7. The high spike with NC of 1 suggests that the key is mapped to one of the sample. The next highest correlation is below 0.35. Hence the mapping of the extracted bio-key is very distinct for identification purpose. In Table 1 it is mentioned that the most serious signal processing attack is Time scale modification (TSM). To test the identification of the bio-keys under this attack the watermarked signal was subjected to a TSM attack of 10%. Then the NC of the extracted bio-key was done with all samples in the database as shown in Fig 8. It can be seen that in the TSM attack of 10% the extracted watermark has a correlation of 0.9 with a sample in the database and the next best correlation is less than 0.5 which is good enough for identification.

7 Conclusion

This paper has proposed a method to generate the watermark (bio-key) from biometric data for audio signals. The proposed method addresses an important limitation in ownership of digital watermarks for identification and authentication. The bio-keys generated have a correlation less than 0.3 among themselves and could survive signal-processing attacks. The extracted bio-keys from watermarked audio signals were subjected to identification from the database from which it was picked. Under no-attack condition the correlation score of 1 was achieved which clearly maps the extracted key to the database. Under serious synchronization attacks like time scale modification (10%) the bio-key a correlation score of 0.9 was achieved which is good enough for identification purpose. The results indicate distinct identification of an extracted bio-key from a database. If the owner is not an individual but a legal entity then such keys has to be generated by a combination of biometric data from multiple subjects. This is left for future work in this area.

References

1. Fridrich, J., Goljan, M., Du, R.: Distortion-Free Data Embedding. LNCS, vol. 2173, pp. 27–41. Springer, Heidelberg (2001)
2. Bender, W., Gruhl, D., Morimoto, N., Lu, A.: Techniques for Data Hiding. IBM Systems Journal 35(3-4), 313–336 (1996)
3. Kirovski, D., Malvar, H.S.: Spread-spectrum Watermarking of Audio Signals. IEEE Transactions on Signal Processing 51(4), 1020–1033 (2003)
4. Bassia, P., Pitas, I., Nikolaidis, N.: Robust Audio Watermarking in the Time Domain. IEEE Transactions on Multimedia 3(2), 35–41 (2001)
5. Chen, T.C., Chung, K.L.: An Efficient Randomized Algorithm for Detecting Circles. Computer Vision and Image Understanding 83(2), 172–191 (2001)
6. He, X., Shi, P.: A Novel Iris Segmentation Method for Hand-held Capture Device. In: Zhang, D., Jain, A.K. (eds.) ICB 2005. LNCS, vol. 3832, pp. 479–485. Springer, Heidelberg (2005)
7. Ma, L., Tan, T., Zhang, D., Wang, Y.: Local Intensity Variation Analysis for Iris Recognition. Pattern Recognition 37(6), 1287–1298 (2004)
8. Li, W., Xue, X., Lu, P.: Localized Audio Watermarking Technique Robust against Time Scale Modification. IEEE Transactions on Multimedia 8(1), 61–69 (2006)