

Audio Watermarking Using Pseudorandom Sequences Based on Biometric Templates

Malay Kishore Dutta

Department of Electronics Engineering, GCET, Greater Noida, India. Email: malay_kishore@rediffmail.com

Phalguni Gupta

Department of Computer Science and Engineering, IIT – Kanpur, India. Email: pg@cse.iitk.ac.in

Vinay K. Pathak

Department of Computer Science and Engineering, HBTI – Kanpur, India. Email: vinaypathak.hbti@gmail.com

Abstract— This paper proposes an efficient watermark generation method for audio copyright protection and digital right management. It proposes a method of generating pseudorandom sequences based on iris image templates. These biometric generated sequences (bio-keys) are found to be unique for distinct identification purposes. These bio-keys are used as the watermark for audio signals. The correlation of the extracted bio-key with a database of 150 bio-keys reveals that the best correlation is 1 while the next best correlation is less than 0.4 under no attack condition. Even under serious signal processing attacks, the bio-keys have distinctly been identified and mapped in a database. Experimental results of listening evaluation and robustness tests have confirmed that the use of bio-keys maintains good perceptual property and offers strong resistance to the typical signal processing attacks.

Index Terms— Audio Watermarking, Iris Recognition, Perceptual Transparency, Digital Right Management.

I. INTRODUCTION

Digital watermarking is one of the possible solutions of the multimedia data ownership problem. 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 are many folds such as copyright protection to resolve piracy disputes, proof of ownership, broadcast monitoring and secret communication.

Some of the popular audio watermarking methods are least significant bit (LSB) coding [1], echo hiding scheme [2] and spread spectrum watermarking [3]. An adaptive audio watermarking based on support vector regression is proposed in [4]. This method embeds the template information and watermark signal into the original audio by adaptive quantization according to the local audio correlation and human auditory masking. In [5] an improved model of echo hiding watermarking is proposed in which the analysis-by-synthesis approach, interlaced kernels and frequency hopping are adopted to achieve

high robustness, security and perceptual quality. In [6] two blind audio watermarking methods are proposed which use correlated quantization for data embedding with histogram based detector. In all these methods, the watermark is either generated from a pseudorandom number (PN) sequence or a chaotic sequence. The issue of ownership of a digital watermark has not been addressed in these methods. As a result, in case of piracy dispute, it may be difficult to prove ownership of a digital watermark.

This paper attempts to address the ownership issue of digital watermark. A digital watermark can be claimed for ownership only when it can be physically or logically owned. For example, if the watermark is generated from biometric data then it can be claimed for ownership since biometric features are unique for all individuals. This seems to be a potential solution to the problem of ownership of a digital watermark. In this paper features of iris image are used as the seed of the watermark and we call it as *bio-key*.

The paper is organized as follows. Section 2 describes the limitations of the existing watermarking schemes and a possible solution using bio-keys. Two methods of watermarking based on bio-keys have been proposed in Section 3. Experimental results are analyzed in the next section. Identification and authentication of the extracted bio keys are studied in Section 5. Finally, Section 6 concludes the paper.

II. PROPOSED METHOD FOR BIO KEY GENERATION

In this section limitations of the existing methods are discussed followed by a possible solution that integrates biometric features as the seed of the watermark. The correlations among the generated bio-keys are studied to illustrate that the bio-keys are unique in nature so that it can help in identification. It is practically impossible to take the iris image of a person in the required controlled environment without his knowledge or concern. This makes the issue of framing attacks out of question.

A. Limitations of the Existing Methods

In the existing methods the choice of watermark has been arbitrary in nature. In various methods, the

watermark is generated from random numbers or chaotic encryptions. 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 of the watermark, 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. In case an attacker is able to uncover the embedding algorithm then the watermark can easily be detected. 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. Also such secret keys cannot be patented or copyrighted because keys are to be secret for all reasons. These limitations of existing watermarking systems have been a cause of concern and there is a need for more secure and unique authentication methods.

B. Possible Solution

To overcome the above-mentioned limitations, there is a need of mapping a digital watermark to an entity that can be physically or logically owned. This entity should be such that it cannot be generated or copied and has to be unique for all reasons. Keeping this limitation in mind, one can think to incorporate biometric data as the seed of the watermark. Biometric features, termed as bio-key, can be used for the generation of the watermark key. Since the biometric features are unique for any individual and can easily be mapped in a database, biometric feature can be used as a key in a watermarking system. So the ownership issues can automatically be addressed.

C. Iris Feature Extraction

Haar wavelet technique is used to extract features from the iris image (Fig. 1). The inner iris boundary is localized on the iris image using circular Hough transformation [7], [8]. Once the inner iris boundary (which is also the boundary of the pupil) is obtained, outer iris is determined using intensity variation approach [9]. 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. 2. A d-dimensional feature vector A is obtained from the fourth level decomposition and can be expressed as:

$$A = [i_1, i_2, \dots, i_d] \tag{1}$$


Fig. 1: Samples of Iris Image

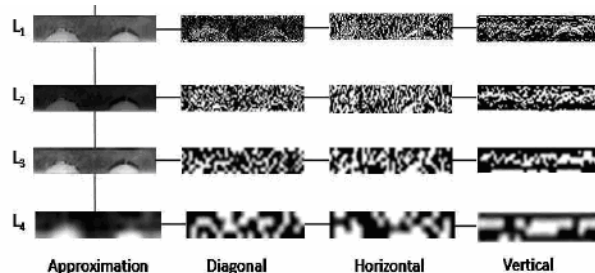


Fig. 2: Four Levels Discrete Haar Wavelet Transform on Iris

A plot of a sample iris vector is shown in Fig. 3. From a database of 150 iris sample images, 150 feature vectors have been generated. Let F be a matrix where the j th column represents the j th feature vector, for $j = 1, 2, \dots, 150$. Method of Gauss Jordan elimination with partial pivoting is used to obtain the reduced row echelon form of F . Experimentally, it is found that each column of this matrix is a pivot column and hence all the feature vectors are found to be linearly independent.

Fig. 4 shows the power spectral density (PSD) of the feature vector obtained in Fig. 3. The PSD of the feature vector reveals that the power of the signal is approximately evenly distributed in the entire frequency spectrum. Fig. 7 shows sixteen feature vectors generated from 16 samples of iris data while the PSD of these 16 feature vectors is shown in Fig. 8.

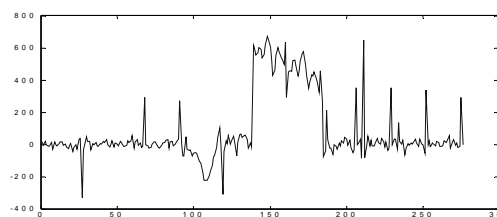


Fig. 3: Feature Vector of a Sample Iris Data.

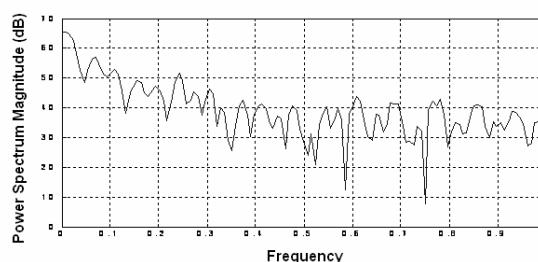


Fig. 4: PSD of the Feature Vector of Fig. 3

It is clearly seen from Fig. 8 that all the PSD curves have their power approximately distributed over the entire frequency range. This property is attractive for spread spectrum techniques [3] where the watermark is needed to be spread across the entire spectrum.

D. Bio-key generation from Iris data

In this section an approach to generate a bio-key from the feature vector of the iris data has been presented. The gray scale iris image is normalized with respect to its size. A feature vector A is generated from the iris image using Haar transformation. The feature vector is then

modified taking the absolute value of the elements. Vector B is defined using the median element of the vector A such that the element $B(i)$ is $+\alpha$ if $A(i)$ is larger or equal to the median element; otherwise it is set to $-\alpha$. Note that almost half of the elements of B are $+\alpha$. Hence a pseudorandom number (PN) sequence can be generated with mean equal to zero. This PN sequence is used as the key for watermarking. This key obtained from iris code becomes unique Steps involved in generating the bio-key using iris codes are given below.

1. Convert the gray scale iris image into a predefined size.
2. Obtain the feature vector A from the fourth level decomposition on iris data through Haar wavelet transformation.
3. Modify the vector A by replacing all negative values by their absolute ones.
4. Determine the median of A ; Let it be m .
5. Obtain vector B such that if $A[i] \geq m$ then $B[i] = \alpha$ otherwise $B[i] = -\alpha$ where α is chosen optimally to keep good signal to noise ratio (SNR).

It can be noted here that larger value of α improves the robustness while smaller value of α weakens the transparency. On the other hand decreasing the value of α , the robustness is weakened and the transparency is enhanced. The mean of these bio-keys are approximately equal to zero. Fig. 10 shows the power spectral densities (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 approximately evenly distributed throughout the spectrum.

In order to see whether all these feature vectors are uniquely distinct for identification, the correlation between any two feature vectors is found with all the feature vectors in the database of 150 samples. Fig.5 shows the normalized correlation (NC) of the 100th sample feature vector with every feature vectors in the database. 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 while average correlation is 0.72. It is seen from Fig.6 that the maximum, minimum and average normalized correlations of the bio- key of the 100th sample with rest of the bio-keys are 0.35, 0.1 and 0.225 respectively. It can be noted that this average correlation among the bio keys is significantly smaller than the normalized correlation of the corresponding feature vector. This reduction in the correlation allows us to have sufficient values of threshold for correlation-based detection of the bio-keys. Fig. 9 shows the correlation of the 70th feature vector with all other feature vectors of the database (solid line) and the correlation of the bio-key generated from the 70th feature vector with all other bio-keys in the database (dotted line). The highest spike is the autocorrelation of the feature vector and the bio-key. It is observed that correlation of the bio-key is comparatively much lesser than that of the feature vector. The arbitrariness of the bio-key is much more than that of the corresponding feature vector. These bio-keys with less correlation allow keeping a low threshold for detection of watermark.

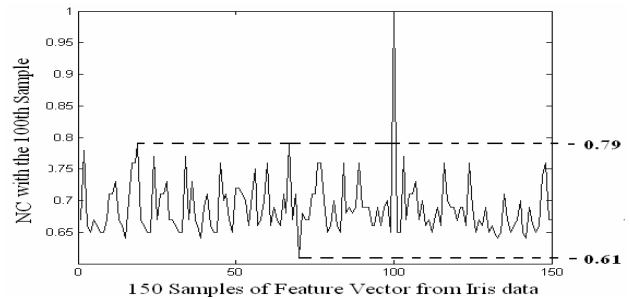


Fig. 5: Correlation Coefficients of 100th Feature Vector with Others

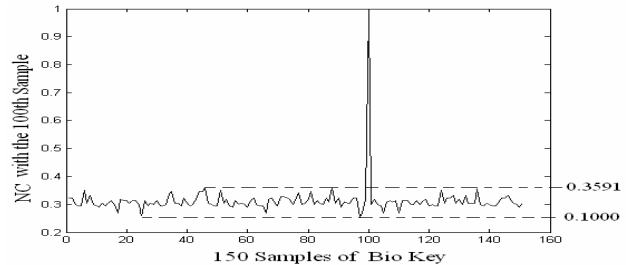


Fig. 6: Correlation Coefficients of 100th Bio-key with Others

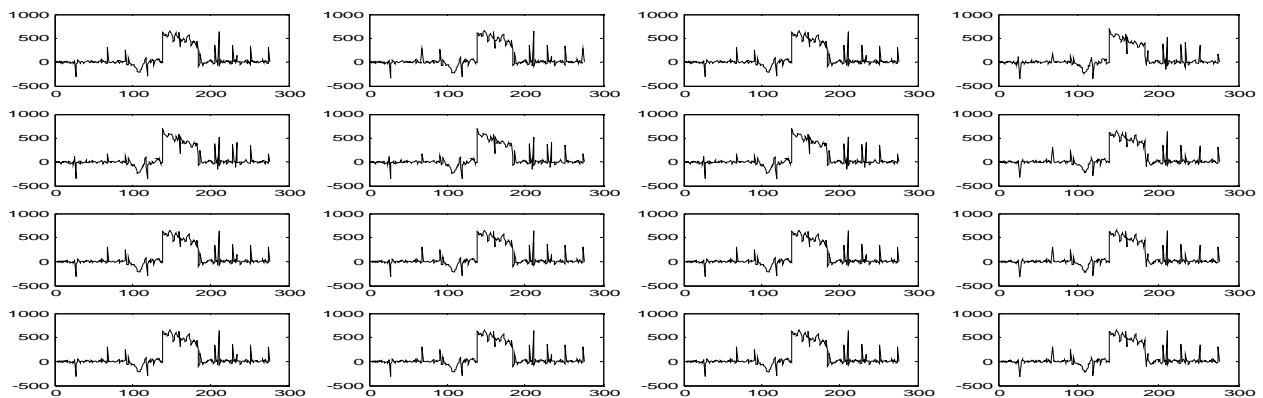


Fig 7: Iris Feature Vector for 16 Different Samples

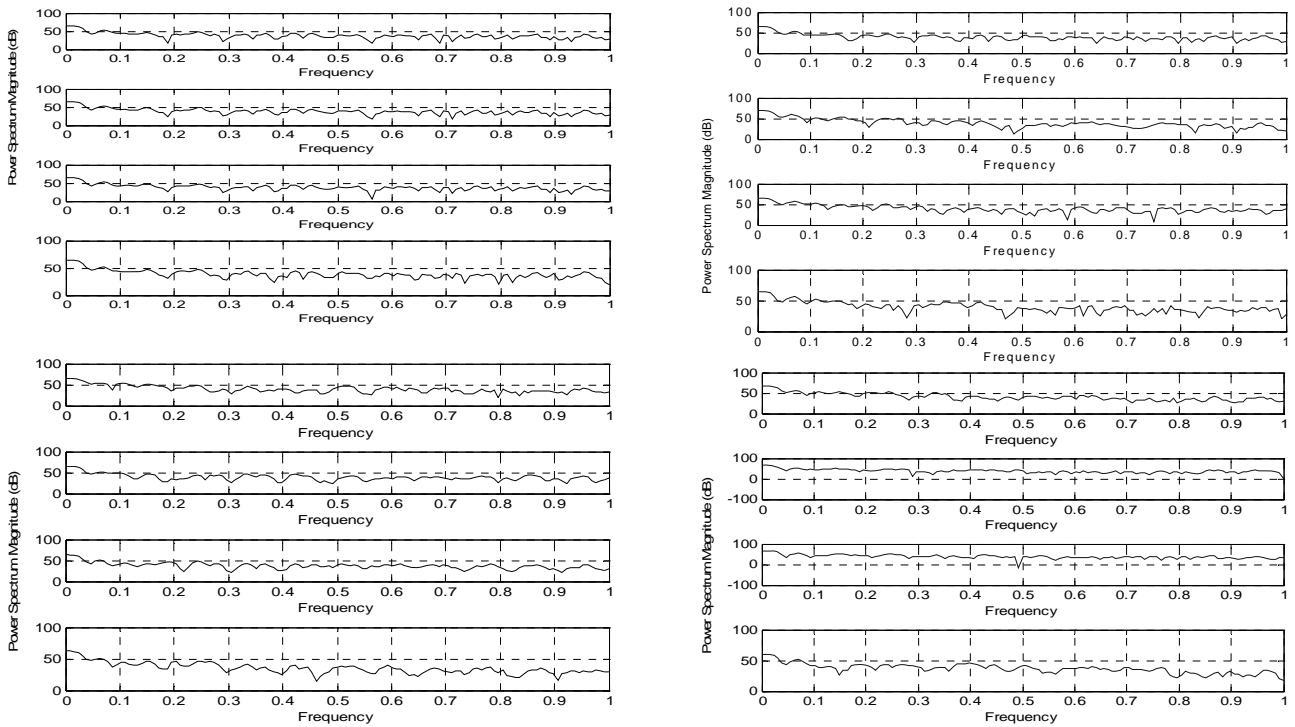


Fig 8: The PSD of the 16 samples of iris feature vectors shown in figure 5.

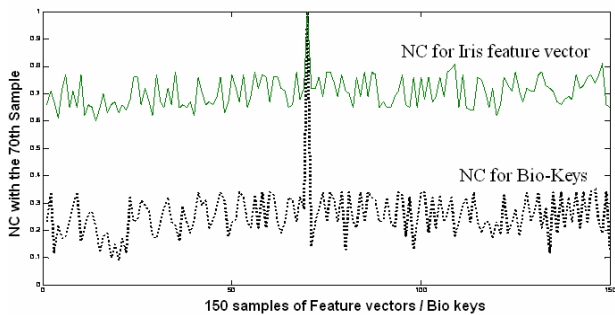


Fig 9: Correlation of 70th Bio-key, Feature Vector with Others

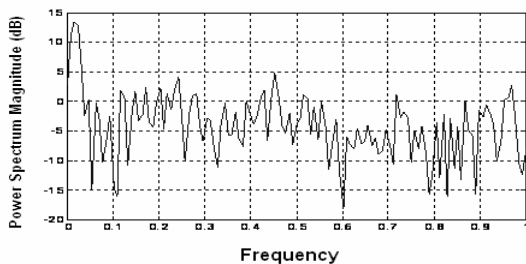


Fig. 10: PSD of a Sample Bio-key

III. WATERMARK EMBEDDING AND DETECTION.

To demonstrate the application of the bio-key as a digital watermark for audio signals, following two methods

1. A method to embed watermark in high energy regions of the audio signal.
2. A watermarking method in wavelet domain. A sub-band is strategically chosen for watermark embedding in the audio signals.

have been proposed for its functional validation.

A. Method 1: Peak Point Reference Method

Prominent instruments like drum, tabla (an Indian instrument) and piano play a very important role in contemporary music and they control the rhythm of the music. They are so dominant that the sounds of other musical instruments and vocal sounds are normally masked at that instant.

1) Watermark Embedding

This method chooses all high-energy peaks and these peaks act as reference points. For selecting high-energy peaks a threshold is chosen above which all such peaks are considered as reference points. This threshold is taken as a fraction of the maximum value of the sample in the time domain signal. The locations of these reference points are stored in a vector D. A new vector C is formed from the vector D with those elements having a distance between them greater than the length of the bio-key i.e. the number of elements in A. The watermark is embedded in the audio signal keeping these reference points as the center of the embedding regions.

The embedding regions R_i can be defined as follows:

$$R_i = [C(i) - |A|/2 : C(i) + |A|/2 - 1] \quad (2)$$

where $|A|$ is the length of A. Once the watermark embedding regions are selected, the watermark is embedded in the selected regions. The embedding is done in frequency domain for increased robustness to signal processing attacks. Fast Fourier Transform (FFT) is used to convert the embedding region R_i into frequency domain and the watermark is embedded. After the watermark is embedded in the region R_i , inverse Fast Fourier Transform (IFFT) is performed to revert back to the time domain.

The steps in watermark embedding are as follows:

1. Rescale the generated bio-key with a weighting factor α
2. Read the sample audio file as a vector X .
3. Find the maximum value of the samples $X(i)_{\max}$ in X .
4. Find all values of samples that are above the threshold which is a fraction of $X(i)_{\max}$.
5. Generate a vector D with the locations of the samples above the threshold.
6. A new vector C is created as
for $n=1: |D|$
 if $D(i+1) - D(i) > |A|$ **then** $C(i) = D(i)$;
7. **for** $j=1: |C|$
 $l = C(j) - |A|/2$; $h = C(j) + |A|/2 - 1$;
 $F = \text{FFT}(X(l:h))$;
 $W = \text{IFFT}(F + \alpha * A)$; $X(l:h) = W$;

2) Watermark Detection and Recovery

Similar to the embedding process the reference points are determined and stored as a vector. In this case, we use $D1$ for D and $C1$ for C for clear distinction. Once the reference points are detected, the watermark is found as the difference between the watermarked and the original signals in the frequency domain for the corresponding points around the reference points. Steps in the watermark detection and recovery are as follows:

1. Read the watermarked file as Y .
2. Find the max value of the samples $Y(i)_{\max}$ in Y .
3. Use the same threshold as used in embedding which is a fraction of $Y(i)_{\max}$.
4. Find all values of samples that are above the threshold.
5. Generate a vector $D1$ with the locations of the samples above the threshold.
6. A new vector $C1$ is created as
for $n=1: |D1|$
 if $D1(i+1) - D1(i) > |A|$ **then** $C1(i) = D1(i)$
7. Read the length of the vector $C1$.
8. **for** $j=1: |C1|$
 $l = C1(j) - |A|/2$; $h = C1(j) + |A|/2 - 1$
 $R = \text{FFT}(Y(l:h)) - \text{FFT}[X(l:h)]$

The vector R is the recovered watermark and this is subjected to the performance analysis of the method.

The method of finding embedding regions is the most important step of Method 1. It makes the method robust against Time scale modification (TSM). TSM algorithms stretch audio signals only in regions where there is minimum transient information and strive to preserve high-energy spikes.

B. Method 2: Wavelet Domain Approach

Successful functional validation of the bio-keys as digital watermark for audio signal in Method 1 has encouraged to propose and to study another watermarking method which is in wavelet transform domain. This is a blind watermarking method where the original host audio signal is not required for the watermark recovery.

1) Watermark Embedding

This proposed method selects embedding regions on the original audio waveform in the high-energy regions. The method utilizes the wavelet high-energy band (CD) to embed the bio-key in the host audio signal. The original audio signal is decomposed in wavelet domain at level L and then the decomposition vector is obtained as:
 $X = \{CA_L, CD_L, CD_{L-1}, CD_{L-2} \dots \dots CD_1\}$ (3)
 where CA_L is the low frequency coefficients at level L and CD_K is the detailed coefficients at level K , $1 \leq K \leq L$.

To make the watermark imperceptible and robust, CD_L is chosen (detailed coefficients) as the embedding area. N strongest coefficients with large magnitude are selected to generate the vector P and then their positions are marked in a vector K . These two vectors, P and K , can serve as keys in the detection of the watermark.

$$CD'_L(K(i)) = CD_L(K(i)) + W(i) \quad (4)$$

where $K(i)$ represents the index of the i^{th} strongest coefficient where $1 \leq i \leq N$. After the embedding of watermark in the detailed coefficients as shown in (4), inverse wavelet transform is performed to reconstruct the watermarked audio signal as:

$$X_j = \{CA_L, CD'_L, CD_{L-1}, CD_{L-2} \dots \dots CD_1\} \quad (5)$$

The N strongest detailed coefficients are chosen for the embedding of the watermark where N is the length of the bio-key. Depending on the length of the bio-key and the length of the host audio signal, the watermark can be embedded in multiples of N . In such situation, the key vector P or K has to carry the details of such information. In this proposed method, redundant bits are used in key vector K to carry this information. This slightly decreases the data but increases the security of the method against signal-processing attacks.

2) Watermark Detection and Recovery

In the watermark detection and recovery process, the original host audio signal is not required and hence the method is blind watermarking. The two key vectors, P and K , are adequate for the extraction of the watermark. Discrete wavelet transform is done at level L to the signal $X1$. The detailed coefficients CD'_L are extracted from which the watermark is to be detected. The transformed coefficients of CD'_L are found in corresponding locations as per vector K and vector P' is generated. The vector P contains those elements whose indices are marked in vector K . After the formation of vector P' , the bio-key can be extracted according to the equation:

$$W' = (P' - P) / \alpha \quad (6)$$

It can be noted that the original host audio signal is not required for watermark detection and hence is a blind method.

IV EXPERIMENTAL RESULTS

In this section the experimental results for listening evaluations and robustness against signal processing attacks separately for Method 1 and Method 2 have been discussed. Signal to noise ratio (SNR), Normalized correlation (NC) and Bit error rater (BER) are the parameters used for performance analysis.

A. Experimental Results for Method 1

In the experiment the value of α is taken as 2.5×10^{-2} that gives a decent SNR for various thresholds chosen in determining the embedding regions. Threshold between 0.95 and 0.65 of the maximum sample value is chosen for experiments. The original and the watermarked signal for the first three samples are shown in Fig. 11 for a threshold value of 0.7. Signal to noise ratio (SNR) is calculated for each value of threshold and is shown in Table 1. To evaluate the audio quality, subjective listening tests have been performed using the mean opinion score (MOS). The definitions of the scores are defined as: 0 for Imperceptible, -1 for Perceptible but not Annoying, -2 for Slightly Annoying, -3 for Annoying, -4 for Very Annoying. Ten listeners of different age groups are provided with the original and the watermarked audio signal and they have been asked to classify the difference in terms the MOS grades. The result of the subjective quality evaluation is averaged and tabulated in Table 2.

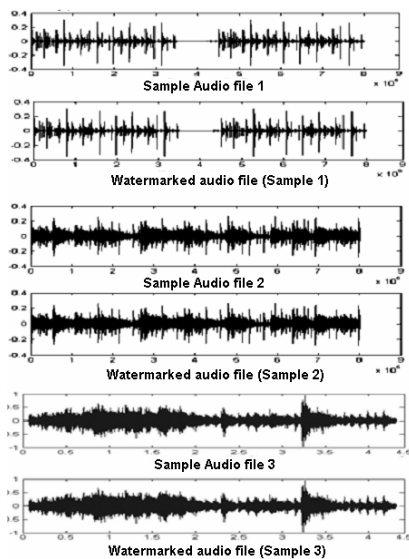


Fig. 11: Original and Watermarked Signal (Method 1)

Thres hold	SNR (dB)					
	Sample 1	Sample 2	Sample 3	Sample 4	Sample 5	Sample 6
0.95	67.50	56.2	61.9	58.4	54.3	56.4
0.90	66.25	55.1	60.2	56.3	52.1	55.1
0.85	61.86	53.2	57.4	54.3	50.0	52.3
0.80	60.81	50.3	56.1	52.9	49.3	49.3
0.75	58.47	46.7	54.2	51.7	46.2	46.1
0.70	56.71	45.3	52.1	48.1	45.5	45.2
0.65	53.82	44.5	50.1	47.3	42.1	42.2

Table 1: Variation of SNR for different values of thresholds.

Threshold	MOS					
	Sample 1	Sample 2	Sample 3	Sample 4	Sample 5	Sample 6
5	0	0	0	0	0	0
0.90	0	0	0	0	0	0
0.85	0	0	0	0	0	0
0.80	0	-0.2	0	0	0	0
0.75	-0.1	-0.2	0	-0.2	-0.1	-0.2
0.70	-0.1	-0.3	-0.1	-0.2	-0.1	-0.2
0.65	-0.2	-0.3	-0.2	-0.3	-0.3	-0.3

Table 2: Average MOS of the Subjective Listening Test. (Method1)

It is seen from Table 2 that the MOS is good quality that means the perceptual properties of the human auditory system may not be able to detect the change in the signal due to the insertion of the watermark. The performances of the watermarking method under various signal-processing attacks are shown in Table 3.

Audio File	Type of attack	NC	BER %
Sample 1 Tabla (Indian musical instrument)	Attack free	1	0
	Low pass (8 KHz)	0.97	2
	Re-sampling (22 KHz)	0.95	4
	Addition of Gaussian Noise	0.92	10
	MP3 (32(kbps)	0.91	14
	TSM (10%)	0.90	16
Sample 2 Flute	Attack free	1	0
	Low pass (8 KHz)	0.97	4
	Re-sampling (22 KHz)	0.96	10
	Addition of Gaussian Noise	0.98	3
	MP3 (32(kbps)	0.98	3
	TSM (10%)	0.91	15
Sample 3 Classical 1	Attack free	1	0
	Low pass (8 KHz)	0.93	11
	Re-sampling (22 KHz)	0.95	9
	Addition of Gaussian Noise	0.92	12
	MP3 (32(kbps)	0.91	14
	TSM (10%)	0.90	16
Sample 4 Country 1	Attack free	1	0
	Low pass (8 KHz)	0.94	14
	Re-sampling (22 KHz)	0.94	14
	Addition of Gaussian Noise	0.91	17
	MP3 (32(kbps)	0.98	5
	TSM (10%)	0.91	16
Sample 5 Blues	Attack free	1	0
	Low pass (8 KHz)	0.92	16
	Re-sampling (22 KHz)	0.91	18
	Addition of Gaussian Noise	0.95	12
	MP3 (32(kbps)	0.96	9
	TSM (10%)	0.90	16
Sample 6 Pop	Attack free	1	0
	Low pass (8 KHz)	0.97	4
	Re-sampling (22 KHz)	0.96	6
	Addition of Gaussian Noise	0.95	9
	MP3 (32(kbps)	0.91	17
	TSM (10%)	0.91	15

Table 3: Robustness Tests against Signal Processing Attacks for Method 1 (Threshold Condition of 0.75)

B. Experimental Results for Method 2

The same audio files have been used for experiments as used in Method 1. Experiments are performed to find an optimum value of α that makes the watermark imperceptible. The value of α is taken as 2.5×10^{-2} that gives a decent value of SNR.

The first three elements of vector K are used to carry the information on number of times that the bio-key is embedded in the host audio file. In doing so the watermark data rate decreases by around 1% but this increases the security of the watermark as many times the watermark is embedded. The length of P is a multiple of N of the bio-key. Wavelet decomposition is implemented by Daubechies-4 wavelet base with 3rd level. To make the watermark imperceptible the watermark is embedded into the low frequency part of the large magnitude detailed coefficients of the audio signal. The first N

elements in the vector P are the N-strongest detailed coefficients of level 3. The next N elements are the next N strongest detailed coefficients of level 3 and so on.

Audio File	Type of attack	NC	BER %
Sample 1 Tabla (Indian musical instrument)	Attack free	1	0
	Low pass (8 KHz)	0.96	8
	Re-sampling (22 KHz)	0.97	5
	Addition of Gaussian Noise	0.94	11
	MP3 (32(kbps)	0.92	14
	TSM (10%)	0.90	15
Sample 2 Flute	Attack free	1	0
	Low pass (8 KHz)	0.96	7
	Re-sampling (22 KHz)	0.96	10
	Addition of Gaussian Noise	0.98	3
	MP3 (32(kbps)	0.98	5
	TSM (10%)	0.91	14
Sample 3 Classical 1	Attack free	1	0
	Low pass (8 KHz)	0.97	10
	Re-sampling (22 KHz)	0.95	12
	Addition of Gaussian Noise	0.92	16
	MP3 (32(kbps)	0.97	7
	TSM (10%)	0.90	16
Sample 4 Country 1	Attack free	1	0
	Low pass (8 KHz)	0.95	13
	Re-sampling (22 KHz)	0.96	11
	Addition of Gaussian Noise	0.91	17
	MP3 (32(kbps)	0.98	5
	TSM (10%)	0.90	16
Sample 5 Blues	Attack free	1	0
	Low pass (8 KHz)	0.92	16
	Re-sampling (22 KHz)	0.93	15
	Addition of Gaussian Noise	0.95	12
	MP3 (32(kbps)	0.97	7
	TSM (10%)	0.91	14
Sample 6 Pop	Attack free	1	0
	Low pass (8 KHz)	0.96	6
	Re-sampling (22 KHz)	0.96	6
	Addition of Gaussian Noise	0.94	10
	MP3 (32(kbps)	0.91	17
	TSM (10%)	0.92	12

Table 4: Robustness Tests against Attacks for Method 2

Experiments have been performed with embedding the bio-key as many as eight times in the samples. In this method, the marked coefficients have indices spread out throughout the signal depending upon the content of the audio signal. In case the signal has sound of percussion instruments throughout then it can have high-energy peaks in the signal throughout. Strategically selecting the sub bands can contain these peaks that allow the watermark to spread in the signal making the method robust against signal processing attacks.

No. of coeff marked	MOS					
	Sample 1	Sample 2	Sample 3	Sample 4	Sample 5	Sample 6
N	0	0	0	0	0	0
2N	0	0	0	0	0	0
3N	0	0	0	0	0	0
4N	0	-0.2	0	0	-0.2	0
5N	-0.1	-0.2	0	-0.2	-0.2	-0.2
6N	-0.1	-0.3	-0.1	-0.2	-0.3	-0.2
7N	-0.2	-0.3	-0.2	-0.3	-0.3	-0.3
8N	-0.3	-0.4	-0.2	-0.3	-0.4	-0.5

Table 5: Average MOS of the subjective listening test.

The subjective listening tests have been performed in a similar way to as discussed in Method 1. The result of the subjective quality evaluation is averaged and tabulated in Table 5. The performance of the second method under signal processing attacks is shown in Table 4. In case multiples number of watermark is embedded the value of the highest NC and lowest BER is presented.

V IDENTIFICATION AND AUTHENTICATION

The objective of this paper is to embed a watermark in an audio signal so that after extraction it can be uniquely mapped in a database of an entity that can be physically or logically owned. It becomes essential to uniquely map the extracted bio-key to a sample in a database.

Bio-keys are picked from this database of 150 samples for embedding it in the samples of audio signals. These audio signals are then subjected to signal processing attacks and then the bio-key is detected and recovered from the audio signal. This extracted bio-key has to be used to identify its identity in the given database. For the mapping these bio-keys in the database, normalized correlations (NC) of the extracted bio-key with all the bio-keys in the database are obtained. For distinct identification, there has to be a NC having very large value compared to all other coefficients. If such a coefficient is found, it can easily be inferred that the bio-key is mapped to a sample in the database and the ownership is authenticated. Results of the experiment performed with the 70th bio-key in Sample 1 are given in Fig. 12 (for Method 1) and Fig. 13 (Method 2). After extraction of the bio-key, it is subjected to NC with all samples in the database. It can be seen that there is a high spike in the figure. It means that the NC with one of the sample in the database is extraordinarily high in comparison to all others. Under no-attack condition, the highest NC obtained is 1 and next highest NC is below 0.4. This clearly maps the extracted bio-key to one of the sample of the database.

Type of Attack	Highest NC	Next Highest NC
Attack Free	1	0.4
LPF (4 KHz)	1	0.4
Resampling (22KHz)	1	0.41
Gaussian Noise	1	0.42
MP3 Compression	0.85	0.44
TSM 5%	0.82	0.44
TSM 10%	0.8	0.46

Table 6: NC based identification of Bio-Keys (Method 1)

To test the identification of the bio-keys under signal processing attacks the watermarked signal (Method 1) has been subjected to low pass filtering, MP3 compression, Gaussian noise, resampling and Time Scale Modification. Results for identification under signal processing attacks are presented in Fig. 12. It can be seen that under these types of attacks, the extracted bio-key has a correlation more than 0.8 with a sample in the database and the next

best correlation is less than 0.5. The experimental results are presented in Table 6 which shows that an optimum threshold can be used for correlation-based identification of the bio keys. Based on this method distinct identification of an extracted bio-key can be done from a given database.

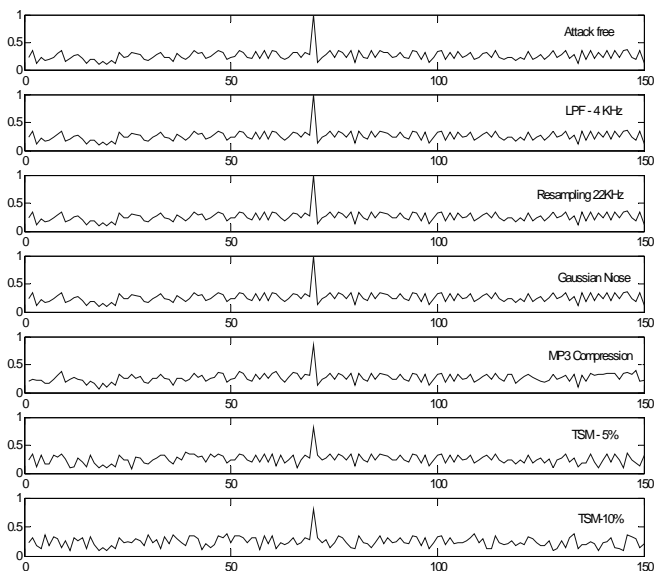


Fig. 12: Normalized Correlation of Extracted Bio-key with Database of 150 Samples under Various Signal Processing Attacks (Method 1)

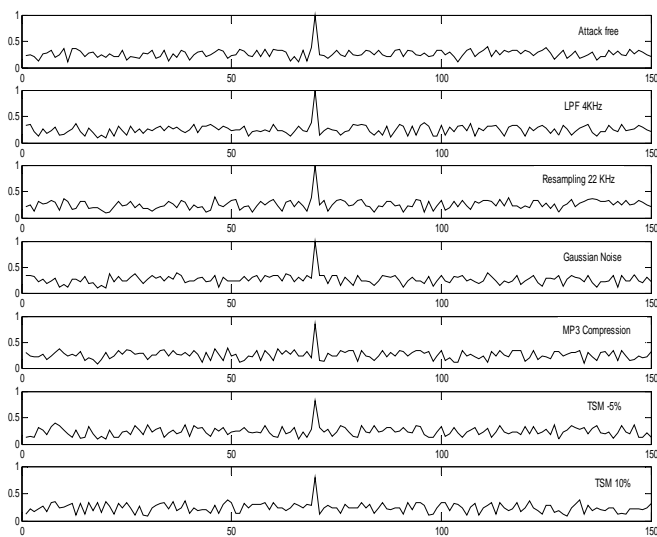


Fig. 13: Normalized Correlation of Extracted Bio-key with Database of 150 Samples under Various Signal Processing Attacks (Method 2)

Type of Attack	Highest NC	Next Highest NC
Attack Free	1	0.41
LPF (4 KHz)	1	0.39
Resampling (22KHz)	1	0.4
Gaussian Noise	1	0.39
MP3 Compression	0.84	0.44
TSM 5%	0.81	0.41
TSM 10%	0.82	0.42

Table 7: NC based identification of Bio-Keys (Method 2)

From Fig. 13 it is clearly seen that the NC of the extracted bio-key with one of the sample is very high in comparison to others (Method 2). The highest NC and the next highest NC is presented in Table 7. It is clearly seen that there is a large difference between the highest and the next highest NC. This means an optimum threshold can be used for correlation based identification and authentication of these extracted bio keys.

VI CONCLUSION

This paper has proposed a method to generate the watermark (bio-key) from biometric data. The proposed method addresses an important limitation in ownership of digital watermarks for identification and authentication. Experimental validation of the application of bio-key has been done using two different methods. The results obtained using both the methods are encouraging. The bio-keys survived under signal processing attacks and distinct identification has been done after the bio-key extraction from the watermarked signal. The normalized correlation of the extracted bio-key with a database 150 bio-keys reveals that the best correlation is 1 followed by a next best below 0.4 under no attack condition. Even under the challenging Time Scale Modification (TSM) attack up to +10%, the best correlation is 0.8 followed by a next best correlation less than 0.5. This clearly indicates a significant development in identification and proof of ownership.

REFERENCES

- [1] Miroslav Goljan, Jessica J. Fridrich and Rui Du, "Distortion-free Data Embedding for Images" LNCS 2137, 2001 pp. 27-41.
- [2] Bender, Gruhl, Morimoto and Lu, "Techniques for Data Hiding" IBM Systems Journal 35(3), 1996, pp.- 313-336.
- [3] Kirovski D and Malvar H, "Spread-spectrum Watermarking of Audio Signals" IEEE Transactions on Signal Processing 51(4), 2003, pp. 1020-1033.
- [4] Xiangyang Wang, Wei Qi, and Panpan Niu, "A New Adaptive Audio Watermarking based on Support Vector Regression" IEEE Transactions on Audio, Speech, and Language Processing, 15 (8), 2007, pp. 2270-2277.
- [5] Oscar T.-C. Chen and Wen-Chih Wu, "Highly Robust, Secure, and Perceptual-Quality Echo Hiding Scheme" IEEE Transactions on Audio, Speech, and Language Processing, 16 (3), 2008, pp.629-638.
- [6] Mohammad A. Akhaee, Mohammad J. Saberian, Soheil Feizi, and Farokh Marvasti, "Robust Audio Data Hiding Using Correlated Quantization With Histogram-Based Detector" IEEE Transactions on Multimedia, 2009 - (In press).
- [7] Chen and Chung, "An Efficient Randomized Algorithm for Detecting Circles" Computer Vision and Image Understanding 83(2) 2001, pp. 172-191.
- [8] He, X., and Shi, P, "A Novel Iris Segmentation Method for Hand-held Capture Device" LNCS: 0302-9743, 2005 pp. 479-485.
- [9] L Ma, T N Tan, Y.H.W. and Zhang, D, "Local Intensity Variation Analysis for Iris Recognition" Pattern Recognition, 37(6) 2004, pp. 1287-1298.