Robust Hiding of Fingerprint-Biometric Data into Audio Signals

Muhammad Khurram Khan[1,2], Ling Xie[2], and Jiashu Zhang[2]

[1] Research Group for Biometrics & Security Engineering,
Bahria University, Dept. of Computer Science & Engineering,
13- National Stadium Road, Karachi, Pakistan
khurram.khan@scientist.com
[2] Sichuan Key Lab of Signal & Information Processing,
Southwest Jiaotong University, Chengdu 610031, China

Abstract. This paper presents a novel fingerprint-biometric template protection scheme, in which templates are concealed into audio signals. Fingerprint templates are encrypted by chaotic encryption and then hid into the chaotically selected random sampling points of the host audio signal by a new non-uniform discrete Fourier transform (NDFT)-based data hiding method. The template extraction process is completely blind and does not require original audio signal, thus the extraction depends on the secret key. Experimental results show that the proposed scheme is robust against common signal processing attacks and achieves higher verification accuracy.

1 Introduction

With the recent advances of internet, the security and privacy issues in authentication systems have raised an important research concern. Applications such as electronic banking, e-commerce, m-commerce, ATM, and smart cards etc. require high attention of data security either data is stored in the database/token, or flow over the network. The implementation of automatic, robust, and secure person identification has become a hot research topic [1]. Traditional ID, PIN, and password-based authentication systems have been widely used for long time to authenticate a claimed identity [2]. The knowledge-based [password or personal identification number (PIN)] and token-based [ID card] identification systems are not secure enough, because passwords can be guessed or hacked, and ID cards can be stolen or lost. Only the citizens of USA loss more than 450 million dollars per annum because of credit card fraud [2].

The drawbacks of traditional identification systems have drawn attention towards secure and unique authentication method, in which biometrics has shown itself an emerging cutting edge identification and authentication technology. Biometric refers to identifying a person on the basis of his physiological or behavioral characteristics [1-4]. It includes fingerprint, hand geometry, palm print, voice, face, and iris recognition etc [3]. Among all the biometrics e.g., fingerprint, iris, face, hand geometry, retina, signature, keystroke dynamics, etc; fingerprint-based authentication is the most mature, proven, and widely used technique around the world [4].

S.-W. Lee and S.Z. Li (Eds.): ICB 2007, LNCS 4642, pp. 702–712, 2007.

Biometric indicators have an advantage over traditional security identification methods, because these inherent attributes cannot be easily shared and every person has unique biometric-attributes [5]. Biometric is of interest in any area where it is important to verify and authenticate the true identity of an individual. Biometric technologies are gaining more attraction because of secure authentication methods for user access, e-commerce, remote authentication, and access control. Biometric provides uniqueness, but the dilemma is that it is not secret and has some risks of being hacked, modified, and reused [6,7]. The integrity of biometric templates/data become more critical whenever it is sent over the network, so there is a need to protect biometric data from different attacks. The reliability and user acceptance of a biometric system depends on the effectiveness and the security of the system against intruders, unauthorized modification, and misuse [6-9]. A biometric-based verification system works properly only if the verifier system can guarantee that the templates come from the valid and legitimate user at the time of enrollment [8]. Although, there is a lot of work done in the pattern recognition and matching of biometric systems, unfortunately only few papers adhere to the security issues inherent with them. To promote worldwide implementation of biometric techniques, an increased security and secrecy of its data are necessary [6].

1.1 Related Work

Recently some techniques based on encryption, watermarking, and data hiding are proposed for the security and secrecy of biometric templates or data. Among the published techniques for biometric encryption, first, Davida et al. [10] proposed a study on the feasibility of protecting the privacy of a user's biometric data on an insecure storage device. They suggest that providing additional privacy for the biometric data may provide stronger user acceptance. In their second work [10], they utilize the error correction codes and explain their role in the cryptographically secure biometric authentication scheme. They save the error correcting codes in the database, which leaks some information of user's biometric template, thus makes their system vulnerable. To enhance Davida's work, Soutar et al. [12,13] proposed an optical correlation-based fingerprint system, which binds a cryptographic key with the user's fingerprint images at the time of biometric enrollment. The cryptographic key is then retrieved only upon a successful identification. Later on, Andy [14] presented a scheme that appears to show vulnerabilities in Soutar et al.'s system. Andy's system extracts the secret code by applying hill-climbing attack on the enrolled image, which is then used to decrypt that code. Tuyls et al. [15-17] have also presented good work on the protection of biometric templates by quantizing secret extraction from significant components of the biometric traits. But, their system has less practicality and is sensitive to invariance, as mentioned in [18]. Uludag et al. [18] presented a comprehensive analysis on the biometric cryptosystems issues and challenges, and compared the performances of the biometric security pitfalls. This is a nice study on the security issues of the biometric systems.

On the other hand, digital watermarking and data hiding is also explored to secure the biometric data. At the beginning, Yeung-Pankanti [19] researched and presented the effects of watermarking fingerprint images on the overall system recognition and retrieval accuracy using an invisible fragile watermarking scheme for image verification applications on a fingerprint identification system. Yeung-Pankanti identified that using watermarking in the fingerprint images can provide a value-added protection and security, as well as copyright notification capability, to the fingerprint data collection processes and its usage. Their technique checks the watermark in the fingerprint images and verifies their integrity. Their scheme is useful before performing the identification, because system can check the fragile watermark embedded in the fingerprint images, but unfortunately it scheme can not be used for the secure transmission of biometrics over insecure network or communication channel.

In 2000, Sonia [20] investigated on a local average method where an executable compares block-by-block local average of the transmitted and the received image over the network. But this method does not provide or elaborate detailed experiments on the watermarked image, and Sonia did not give any signal or image processing attacks on her method during the transmission.

In 2002, Gunsel et al. [7] proposed two spatial domain-watermarking schemes. Their first scheme utilizes an image adaptive strength adjustment technique to make low visibility of embedded watermark, while their second method uses feature adaptive watermarking technique and is applicable before feature extraction. The pitfall of their system is that they did not perform encryption of watermarking data, so their method is susceptible to attack in case if an adversary extracts biometric template from the transmitted image over insecure network.

Recently, Jain-Uludag [6] published two application scenarios based on amplitude modulation watermarking method for hiding biometric data. Their first application is based on steganography, while another is embedding the facial data in fingerprint images. Their both applications embed the biometric template without performing encryption so it could also have the risk of biometric data copy attack [9] incase if an adversary is able to extract it from the transmitted host image. In addition, Jain-Uludag did not perform experiments for different kinds of noises and attacks on their method, so it is difficult to measure the performance of their system under different conditions over the network.

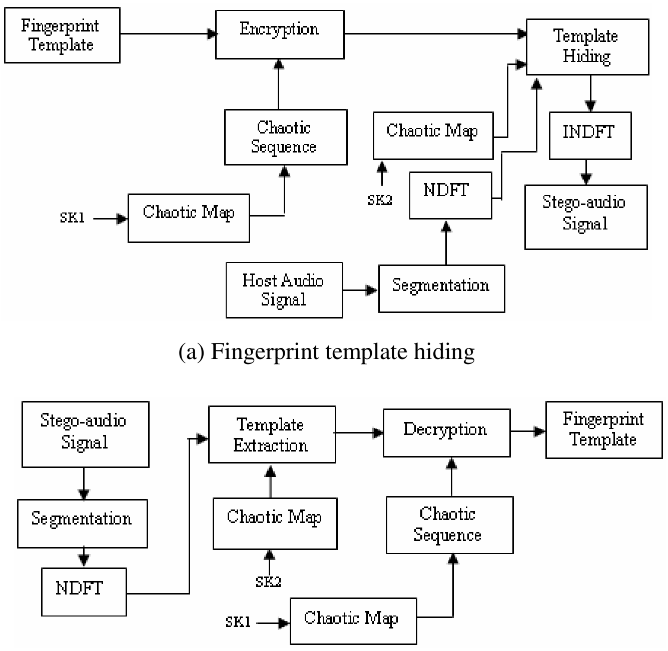
The problems of biometric template security raise concerns with the wide spread proliferation and deployment of biometric systems both commercially and in government applications, especially when its data flow in the air. So by keeping security and secrecy issues in concern for the template security enhancement, in this paper, we present a novel chaos and NDFT (Nonuniform Discrete Fourier Transform)-based biometric data hiding technique in the audio signals. For the experiments, we use fingerprint-biometric as a reference biometric because of its large-scale utilization in commonly used biometric-based authentication systems [1,4]. Fingerprint templates are encrypted by chaotic encryption, encoded by BCH codes, modulated by chaotic parameter modulation (CPM) scheme, and then hid by chaotically selected random frequency points in the original audio signal. Encryption and modulation of fingerprint templates, and chaotically selected hiding frequency points using secret key ensure the robustness against steganalysis attack [21]. Furthermore, proposed method is blind-hiding method and does not require original audio signal for the fingerprint template extraction at the server end. Experimental and simulation results show that the presented scheme: (i) accomplishes perceptual transparency, after template hiding, by exploiting the masking effects of the human auditory system (HAS), (ii) shows robustness against attacks, (iii) secure by using secret keys, (iv) and efficient in speed and hidden-template decoding performance.

2 Proposed Scheme

2.1 Template Generation and Encryption

Our proposed scheme is depicted in Figure 1. Fig. 1(a) delineates the fingerprint template hiding method, and Fig. 1(b) shows the template extraction process at the server end.

The presented scheme starts with capturing fingerprint images from the sensor. In the proposed scheme, fingerprint images are preprocessed by the image processing and pattern recognition algorithms. Fingerprint features are extracted by the Gabor filter bank-based technique [4]. The extracted feature vector is composed of both the global and local characteristics of ridges and valleys of fingerprint image. The extracted fingerprint-biometric feature vector $x \in R^M$ is reduced down to a set of single bits $b \in \{0,1\}^N$ where, N is length of the bit string; in actual it is the template size of the extracted fingerprint [4].



(a) Fingerprint template hiding

(b) Fingerprint template extraction

Fig. 1. Proposed fingerprint template hiding scheme

After feature extraction, fingerprint-biometric template is encrypted by chaotic encryption method. For the encryption, we employed skew tent map, which is a piecewise-linear Markov chaotic map that shows superiority against the some widely used pseudorandom sequences and have controllable correlation properties [5].

$$s(x) = \begin{cases} \frac{1}{a}x, & 0 \le x \le a \\ \frac{1}{a-1}x + \frac{1}{1-a}, & a \le x \le 1 \end{cases} \tag{1}$$

where, $a \in (0,1)$ and used as the encryption/decryption-key of fingerprint template. The sequence generated by Tent map is composed of real numbers, so the output sequence of equation (1) is quantized into binary stream by the following threshold:

$$c(n) = \begin{cases} 1, & x_n \ge 0.5 \\ 0, & x_n < 0.5 \end{cases} \tag{2}$$

The normalized sequence is $c(n) \in \{0,1\}$. We use XOR operation to encrypt the fingerprint template, and the encrypted template is obtained by:

$$e(n) = E(b(n) = \sum_{n=1}^{N} b(n) \oplus c(n) \tag{3}$$

where N is size of template and chaotic sequence, $b(n)$ is the normalized fingerprint template, $c(n)$ is the pseudorandom key sequence generated by Tent map, $E(b(n))$ is the encrypted template, and $\oplus$ denotes the Exclusive-OR operation.

2.2 Fingerprint Template Hiding Algorithm

The nonuniform discrete Fourier transform (NDFT) has been widely used in signal processing applications where nonuniform spaced samples in the frequency domain are needed [6,23]. Nonuniform distribution of sampling points in the NDFT makes it a good candidate for the data hiding applications.

One dimension NDFT and its inverse transform (INDFT) are [22]:

$$\begin{cases} F(k_m) = \sum_{n=0}^{N-1} f(n) e^{-jk_m n} \\ f(n) = \frac{1}{N} \sum_{n=0}^{N-1} F(k_m) e^{-jk_m n} \end{cases}, \ \mathrm{m} = 1, \cdots, M \tag{4}$$

Where, k_m may choose any real number and M expresses the number of sampling points.

NDFT of N points can be represented by arbitrary N points on unit circle in the Z-plane [6]. It can be expressed by:

$$X(z_k) = \sum_{n=0}^{N-1} x(n) z_k^{-n}, \quad \mathrm{k = 0,1,\ldots N - 1} \tag{5}$$

Where, z_0, $z_1,\ldots z_{N-1}$ are arbitrary N different points in the Z-plane. Equation (5) can be further represented in matrix form by:

$$X = Dx \tag{6}$$

$$X = \begin{bmatrix} X(z_0) \\ X(z_1) \\ \vdots \\ \mathrm{X(z_{N\text{-}1})} \end{bmatrix}, \quad x = \begin{bmatrix} x(0) \\ x(1) \\ \vdots \\ x(N-1) \end{bmatrix}, \quad D = \begin{bmatrix} 1 & \mathrm{z}_0^{-1} & \mathrm{z}_0^{-2} & \cdots & \mathrm{z}_0^{-(N-1)} \\ 1 & \mathrm{z}_1^{-1} & \mathrm{z}_1^{-2} & \cdots & \mathrm{z}_1^{-(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \mathrm{z}_{N\text{-}1}^{-1} & \mathrm{z}_{N\text{-}1}^{-2} & \cdots & \mathrm{z}_{N\text{-}1}^{-(N-1)} \end{bmatrix},$$

where, Matrix D is Vandemone matrix and entirely determined by N points z_k, $(k = 1,2,..., N - 1)$. Expression of matrix D can be shown as:

$$\det(D) = \prod_{i \neq j, i > j} (z_i^{-1} - z_j^{-1}) \tag{7}$$

where, D is nonsingular, so INDFT (inverse NDFT) exists and is unique, that is: $x = D^{-1} X$.

2.2.1 Embedding Details

The original audio signal has the sampling frequency of 44.1 KHZ and the quantization ratio is 16 bits. The amplitude of the original audio signal is 0~65535 (2^{16}-1). The total length of the samples is 4096.

The details of embedding biometric data are as follows:

(1). To embed the data in the NDFT domain, first we segment the host/cover original audio signal into 8 samples per segment. For each segment, a frequency point in the selectable frequency range is chosen by the secret key to carry on NDFT transform, which keeps privacy of embedding position. We use Logistic map to generate the specific frequency chosen rule.

$$x_{n+1} = g(x_n) = \mu x_n (1 - x_n) \tag{8}$$

where, $n = 1,2,3,...$ is the map iteration index and μ is the parameter value. For $3.57 < \mu \leq 4.0$, the generated real number sequence is non-periodic, non-convergent, and very sensitive to its initial value [3].

(2). After segmenting and choosing the frequency points, we quantize the frequency coefficient to embed the template. The quantization rule is as follows:

For the coefficient $f(k)$ to be embedded, the modulus and residual are $m = \lfloor | f(k) | / \Delta \rfloor$, $r = | f(k) | - m \times \Delta$. Where, m is the modulus, r is the residual, and Δ is the quantization step.

$$| f(k)^w | = \begin{cases} \frac{\Delta}{2} & WW(k) = 1 \\ \frac{3\Delta}{2} & WW(k) = 0 \end{cases} \qquad m = 0 \tag{9}$$

$$| f(k)^w | = \begin{cases} \begin{cases} 2k\Delta + \frac{1}{2}\Delta & if\ m = 2k \\ 2k\Delta + \frac{1}{2}\Delta & if\ m = 2k + 1 and | r | \le \frac{1}{2}\Delta \\ 2k\Delta + 2\Delta + \frac{1}{2}\Delta & if\ m = 2k + 1 and | r | > \frac{1}{2}\Delta \end{cases} & WW(k) = 1 \\ \begin{cases} (2k+1)\Delta + \frac{1}{2}\Delta & if\ m = 2k + 1 \\ 2k\Delta - \frac{1}{2}\Delta & if\ m = 2k\ and | r | \le \frac{1}{2}\Delta \\ (2k+1)\Delta + \frac{1}{2}\Delta & if\ m = 2k\ and | r | > \frac{1}{2}\Delta \end{cases} & WW(k) = 0 \end{cases} \qquad m \neq 0$$

where, $| f(k)^w |$ are the stego-coefficients, which contain the fingerprint template.

During the embedding process, two aspects should be paid more attention:

(2a). To guarantee embedded coefficients are also real number by way of INDFT manipulation, the embedding data is implemented under positive symmetric condition similar to DFT-based embedding method. That is: on the chosen frequency point, let $X(k) = X^*(N - k)$. The positive symmetric condition is defined as:

$$| X(k) | \leftarrow | X(k) | + \varepsilon \tag{10}$$

$$| X(N-k) | \leftarrow | X(N-k) | + \varepsilon \tag{11}$$

(2b). Choosing quantization step Δ: The quantization step $\Delta = 5120$ is used in the proposed scheme. This quantization value ensures the robustness of the algorithm and sensitivity to audible that is an important issue in human auditory system (HAS).

At the end of embedding fingerprint template, we carry out INDFT of the stego-coefficients to get the stego-audio signal. Now this stego-audio signal, which hides fingerprint template, can be securely transmitted to authentication server for the identification of a person.

2.3 Fingerprint Template Extraction and Verification

At the authentication server end, we perform NDFT on the stego-signal to extract the fingerprint template. Extracting data does not need original audio signal, because template/data is embedded by quantizing NDFT amplitude coefficients. The process of extracting hidden data is the inverse of the embedding process; the detailed steps are as follows:

(a) Perform segmentation of the received audio signal;
(b) Carry out NDFT on segmented stego-audio signal by secret key;
(c) Extract fingerprint template by quantization rule in the chosen frequency point;

After performing extraction, the biometric template is decrypted by the same method as described in subsection 2.1. At the end, we perform verification of the extracted fingerprint template, $t'(n)$, against the pre-stored template database by the following equation:

$$M = \frac{1}{N}\sum_{i=1}^{N} t'(n) \oplus t(n) \tag{12}$$

where, N is the size of the fingerprint template, $t(n)$ is original fingerprint template stored in the database, while $t'(n)$ is an extracted template from the stego-audio signal.

3 Experimental Results and Discussions

Experiments are conducted on the public domain fingerprint images dataset, DB3, FVC2004 that contains a total of 120 fingers and 12 impressions per finger (1440 impressions) using 30 volunteers. The size of fingerprint images is 300×480 pixels captured at a resolution of 512 dpi.

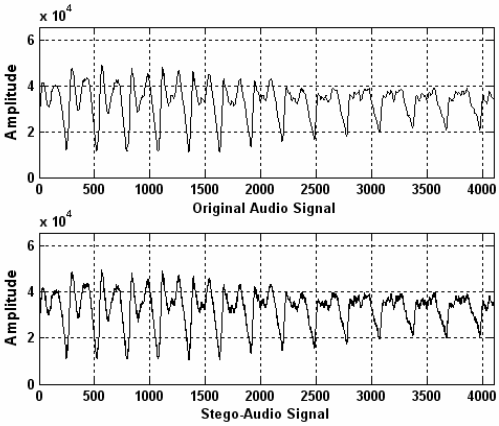


Fig. 2. Original audio signal without fingerprint template and Stego-audio signal with hidden fingerprint template

To evaluate the performance of the proposed scheme, in terms of robustness and inaudibility, we performed a set of experiments including Gaussian noise, low pass filtering, Mp3 compression, re-sampling, and re-quantization on the stego-transmitted signal that contains hidden biometric-fingerprint template. The original audio signal and stego-audio signal containing hidden biometric-fingerprint template are depicted in figure 2, and their signal difference is shown in figure 3.

Presented system shows 100% fingerprint template decoding accuracy without any attacks as shown in Table 1. We evaluated the performance of our system by calculating Signal-to-Noise Ratio (SNR), Mean Squared Error (MSE), and Bit Error Rate (BER), and their mathematical formulae are shown in equations (13) to (15), respectively.

$$SNR(dB) = 10\log_{10}\frac{\sum_{i=0}^{N-1} x^2(n)}{\sum_{i=0}^{M-1}\left[x(n)-y(n)\right]^2} \tag{13}$$

$$MSE = \frac{1}{N}\sum_{i=0}^{M-1}\left[x(n)-y(n)\right]^2 \tag{14}$$

$$BER = \frac{1}{N}\sum_{i=0}^{N-1} x(n)\oplus y(n) \tag{15}$$

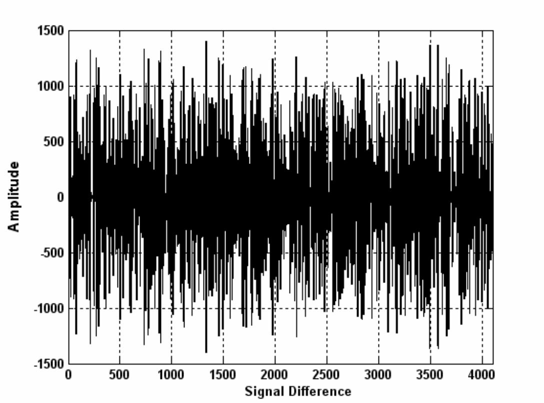


Fig. 3. Signal difference of original and stego-audio signals

where, N is size of the template, $x(n)$ is the original/host audio signal and $y(n)$ is the stego-audio signal in which, fingerprint template is hidden.

Hence, it is apparent from the experimental results that the proposed system is an ideal candidate for secure transmission of biometric templates over insecure communication network. Moreover, it achieves an outstanding decoding performance, even under different kinds of attacks which could be possible during the transmission.

Table 1. Experimental Results

Attack	SNR (dB)	MSE	BER	Accuracy (%)
No Attack	34.9622	3.4076e-004	0	100
Gaussian Noise	32.7750	5.6386e-004	0.0059	99.41
Low-pass Filtering	34.8085	3.5304e-004	0.0020	99.80
128K Mp3 Compression	34.5605	3.7379e-004	0.0000	100
Re-Sampling	34.8861	3.4679e-004	0.0020	99.80
Re-Quantization	34.8991	3.4575e-004	0.0000	100

4 Conclusion

We have presented a novel covert-transmission scheme of biometric-fingerprint templates, in which audio signal hid templates as container to protect from attacks and kept secret the existence of fingerprint templates from the communication eavesdropping. We used chaos and NDFT-based template hiding scheme and proved that biometric template in audio signal could not affect the identification performance of the biometric recognition system. In addition, we performed a series of experiments to evaluate the performance of the system and the experimental results have shown that the proposed system is robust against noises and attacks, and achieves better verification accuracy. Our future work would focus on hiding different type of biometrics templates e.g. face, iris etc; into audio signal to evaluate the robustness of our system.

Acknowledgements

This project is supported by 'Sichuan Youth Science and Technology Funds' under grant number: 03ZQ026-033 and ‘Southwest Jiaotong University Doctors Innovation Funds 2005’.

References

1. Anil, K.J., Prabhakar, S., Hong, L., Pankanti, S.: Filterbank-based fingerprint matching. IEEE Transactions On Image Processing 9, 846–859 (2000)
2. Anil, K.J., Pankanti, S., Bolle, R.: Biometrics: Personal Identification in Networked Society. Kluwer, USA (1999)
3. Khan, M.K., Jiashu, Z., Lei, T.: Chaotic secure content-based hidden transmission of biometrics templates. In: Chaos, Solitons, and Fractals, vol. 32(5), pp. 1749–1759. Elsevier Science, Amsterdam (2007)
4. Anil, K.J., Prabhakar, S., Hong, L.: A multichannel approach to fingerprint classification. IEEE Transactions on Pattern Analysis and Machine Intelligence 21, 348–359 (1999)
5. Daugman, J.: High confidence visual recognition of persons by a test of statistical independence. IEEE Transactions on Pattern Analysis and Machine Intelligence 15, 1148–1161 (1999)
6. Anil, K.J., Umut, U.: Hiding biometric data. IEEE Transactions on Pattern Analysis and Machine Intelligence 25, 1494–1498 (2003)

7. Gunsel, B., Umut, U., Tekalp, A.M.: Robust watermarking of fingerprint images. In: Pattern Recognition, vol. 35, pp. 2739–2747. Elsevier Science Ltd., Amsterdam (2002)
8. Khan, M.K., Jiashu, Z., Lei, T.: Protecting biometric data for personal identification. In: Li, S.Z., Lai, J.-H., Tan, T., Feng, G.-C., Wang, Y. (eds.) SINOBIOMETRICS 2004. LNCS, vol. 3338, pp. 629–638. Springer, Heidelberg (2004)
9. Ratha, N., Connell, J., Bolle, R.: Enhancing security and privacy in biometrics-based authentication systems. IBM System Journal 40, 614–634 (2001)
10. Davida, G.I., Frankel, Y., Matt, B.J.: On enabling secure applications through online biometric identification. In: IEEE Symposium on Security and Privacy, pp. 148–157 (1998)
11. Davida, G.I., Frankel, Y., Matt, B.J., Peralta, R.: On the relation of error correction and cryptography to an offline biometric based identification scheme. In: Proc. Workshop Coding and Cryptography, pp. 129–138 (1999)
12. Soutar, C., Roberge, D., Stojanov, S.A., Gilroy, R., Vijaya Kumar, B.V.K.: Biometric encryption using image processing. In: Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques II, vol. 3314, pp. 178–188 (1998)
13. Soutar, C., Roberge, D., Stojanov, S.A, Gilroy, R., Vijaya Kumar, B.V.K.: Biometric encryption, enrollment and verification procedures. In: Proc. SPIE, Optical Pattern Recognition IX, vol. 3386, pp. 24–35 (1998)
14. Andy, A.: Vulnerabilities in biometric encryption systems. In: Kanade, T., Jain, A., Ratha, N.K. (eds.) AVBPA 2005. LNCS, vol. 3546. Springer, Heidelberg (2005)
15. Linnartz, J.P., Tuyls, P.: New shielding functions to enhance privacy and prevent misuse of biometric templates. In: Proc. of the 4th Int. Conf. on Audio and Video Based Biometric Person Authentication, UK, pp. 393–402 (2004)
16. Verbitskiy, E., Tuyls, P., Denteneer, D., Linnartz, J.P.: Reliable biometric authentication with privacy protection. In: Proc. of the 24th Symposium on Inf. Theory, pp. 125–132 (2003)
17. Tuyls, P., Gosling, J.: Capacity and examples of template-protecting biometric authentication systems. In: Maltoni, D., Jain, A.K. (eds.) BioAW 2004. LNCS, vol. 3087, pp. 158–170. Springer, Heidelberg (2004)
18. Uludag, U., Pankanti, S., Prabhakar, S., Jain, A.K.: Biometric cryptosystems: issues and challenges. Proceedings of the IEEE 92, 948–960 (2004)
19. Yeung, M.M., Pankanti, S.: Verification watermarks on fingerprint recognition and retrieval. Journal of Electronic Imaging 9, 468–476 (2000)
20. Sonia, J.: Digital watermarking techniques: a case study in fingerprints and faces. In: Proc. Indian Conference on Computer Vision, Graphics, and Image Processing, pp. 139–144 (2000)
21. Andrew, D.K.: Steganalysis of LSB matching in grayscale images. IEEE Signal Processing Letters 12, 441–444 (2005)
22. Bagchi, S., Mitra, S.K.: The Nonuniform Discrete Fourier Transform and its application in filter design. IEEE Trans. on Circuits and System: Analog and Digital Signal Processing 43, 422–433 (1996)
23. Ling, X., Jiashu, Z., Hong-Jie, H.: NDFT-based Audio Watermarking Scheme with High Security. In: IEEE ICPR, vol. 4, pp. 270–273 (2006)