A Biometric Key-Binding and Template Protection Framework Using Correlation Filters

Vishnu Naresh Boddeti[1], Fei Su[2], and B.V.K. Vijaya Kumar[1]

[1] Carnegie Mellon University, Pittsburgh PA 15213, USA
naresh@cmu.edu, kumar@ece.cmu.edu
[2] Beijing University of Posts and Telecommunications, Beijing, China
sufei@bupt.edu.cn

Abstract. We describe a new framework to bind cryptographic keys with biometric signatures using correlation filters. This scheme combines correlation filter based biometric recognition with biometric key-binding while offering template protection, revocability, diversity and security. We demonstrate the effectiveness of our scheme via numerical results on the CMU-PIE face database.

Keywords: Encryption, Key-Binding, Correlation Filters, Face Recognition, Template Protection, Biometrics.

1 Introduction

The fundamental idea of cryptography is to encipher a "secret" or message into an intermediate form, also called "cipher text", in which the original message exists in a hidden state. The same message can be transformed into many intermediate forms by using different ciphers chosen by a key, called "cipher key". The original message can be recovered accurately by reversing this process only by using the correct decryption key. Most often these keys are very long and nonsensical making it very difficult for humans to remember. Hence they are stored either on a smart card or in a computer database and are released using some other form of authentication (usually a password).

While current cryptographic algorithms provide high security, they suffer from some limitations not due to weaknesses in the algorithms themselves but due to the setup of the whole security system. The decryption keys are only as secure as the password or smart card used for authentication to release the key. These passwords and smart cards can be lost or compromised, effectively nullifying the security provided by the cryptographic algorithms. Another concern is that there is no way of knowing if the password is being provided by a genuine person or an impostor.

Linking the decryption keys to the physiological and behavioral traits of a person like face, iris, fingerprint, gait etc. would address some of the above mentioned shortcomings of cryptographic authentication systems. These biometric characteristics cannot be lost or forgotten like passwords, thereby reducing the chances of being compromised. It is also not easy to copy, share or distribute the biometric signatures and more importantly they enable us to tie the key directly to the user. Hence biometric-based authentication systems are good candidates to either replace normal password-based systems or can be used in conjunction with them to provide two-factor authentication.

M. Tistarelli and M.S. Nixon (Eds.): ICB 2009, LNCS 5558, pp. 926–936, 2009.

Having said that, biometric authentication systems come with their own challenges. The main concern is that cryptographic systems require exactitude while biometric measurements are inherently noisy due to both natural variation and noise in acquiring biometric data. Hence combining cryptography with biometric recognition is challenging. Some requirements of biometric cryptographic systems are as follows:

1. ***Revocability:*** Lost or stolen passwords are easy to revoke and new passwords can be issued. Biometric authentication systems should have the same capability.
2. ***Security:*** Biometric authentication systems need to be as secure as password based systems. Also, it should be computationally hard to reverse engineer either the secret key or the raw biometric from the biometric template.
3. ***Performance:*** In order that only an authentic user be able to release the key, the error rates i.e., in terms of false accepts and false rejects should be low.
4. ***Diversity:*** Should have the ability to issue diverse templates, obtained from the same biometric, to be used for multiple applications.

The correlation filter based framework that we propose in this work has been designed keeping the above in mind. Correlation filters can be designed to tolerate a variety of sources of appearance variability in the image. Due to this property, correlation filters are suitable candidates for combining biometrics with cryptography. The filters used in this work, while performing their primary task of biometric matching, have the functionality of key-binding built into them. This is achieved by extending the traditional correlation filter design as explained in Section 2.

1.1 Related Work

Biometric security and privacy are important factors in the adoption and deployment of biometric authentication systems. There have been many approaches to address the issues in bringing together biometric authentication and traditional cryptography.

Soutar et al. [1][2][3] proposed a correlation-based key binding algorithm for fingerprint based authentication. They design a correlation filter from representative training images and then set the filter magnitude to 1 for all frequencies, while multiplying the filter by a random phase mask. Key-binding is done by linking the key to the binarized correlation plane. Though we also use correlation filters in our framework, our work differs from their's in both the correlation filter design and the key-binding algorithm.

Another popular technique is the Fuzzy Vault scheme proposed by Juels and Sudan [4]. This scheme has been used for fingerprint based recognition [5] and even in iris recognition [6]. While fuzzy vaults offer tolerance to biometric variability, they have many limitations [7][8], some of which are being addressed. The primary limitation with these schemes is the amount of security they provide, which is not on par with the present day encryption techniques like AES-128, triple DES etc.

Ratha et al. [9] and Savvides et. al. [10] proposed techniques for obtaining cancelable templates for fingerprints and faces respectively, which helps address the issues of revocability and diversity. In this work, we incorporate the later cancelability scheme.

Another approach to combining cryptography with biometrics has been the use of Error Correction Coding (ECC) to overcome the natural variability in biometrics. Hao et al. [11] use Hadamard and Reed Solomon codes for iris recognition while Sutcu et al. [12][13] use low density parity check (LDPC) codes on fingerprints. These methods require binary representation of the features to use ECC, which may not always be possible for biometrics like faces, gait, voice etc.

The rest of the paper is organized as follows. In Section 2, we describe the correlation filters used for matching. Our framework is presented in Section 3 followed by security analysis in Section 4. Experimental results are given in Section 5.

2 Correlation Filters

A correlation filter can be represented by a template that is specifically designed from a set of patterns (e.g., iris images) that are representative of a particular class. This template is matched against a query by performing a cross-correlation between the two. For computational efficiency this is done in the frequency domain,

$$C(x,y) = FT^{-1}\{FT\{I(x,y)\} \cdot F^{*}(u,v)\} \tag{1}$$

where *I(x,y)* is a query pattern and *F(u,v)* is the frequency domain representation of the correlation filter with u and v denoting the spatial frequencies.

The filter is constrained to give a sharp peak at the center of the correlation plane $C(x,y)$ for an authentic match and no such peak for an impostor as shown in Fig. 1. The degree of match is measured by the peak-to-correlation energy (PCE) ratio defined as:

$$PCE = \frac{peak - \mu}{\sigma} \tag{2}$$

μ and σ are the mean and the standard deviation, respectively of the correlation plane.

Correlation filters have been found to perform well in biometric recognition problems like face, iris, fingerprint and palm print recognition [14][15][16]. A variety of advanced correlation filters are available [17] and in this work we use a modified Minimum Average Correlation Energy (MACE) [18] filter. The MACE filter is given by,

$$\mathbf{h} = \mathbf{D}^{-1}\mathbf{X}(\mathbf{X}^{+}\mathbf{D}^{-1}\mathbf{X})^{-1}\mathbf{u} \tag{3}$$

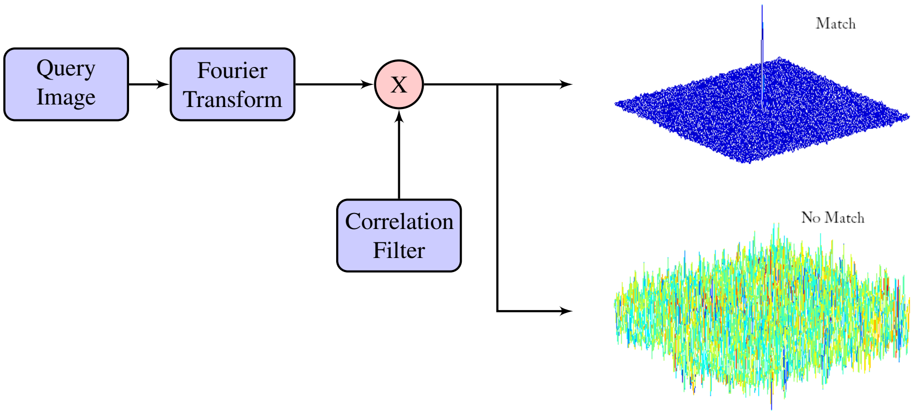

Fig. 1. Application of correlation filter on a query image

where $\mathbf{X} = [\mathbf{z_1} \ldots \mathbf{z_n}]$ contains the vectorized versions of the two-dimensional Fourier transforms (FT) of the training images, $\mathbf{h}$ is the frequency domain correlation filter, $\mathbf{u}$ contains the correlation plane origin constraints and $\mathbf{D}$ is a diagonal matrix with the average power spectrum of the training images along its diagonal.

2.1 Multi-peak Correlation Filter

Correlation filters have been traditionally designed to produce just one peak at the center of the correlation plane for an authentic match and no such peak for an impostor. We extend this by adding more constraints to the filter design to produce an arbitrary number of peaks at arbitrary locations for an authentic query and no discernible peaks for an impostor. This can be thought of as summing together multiple correlation planes, each having one peak at a pre-specified location which in turn can be obtained by shifting the peak in the traditional design (at the origin) to the specified location. See Fig. 2 for an illustration. Even though the absolute locations of the peaks may vary depending on the relative displacements between the gallery and probe images, the relative locations of these multiple peaks are, in general stable when using good quality images, thus approaching the exactness required by cryptography. This property together with the flexibility in designing the filter is exploited to bind the message with the biometric to give one template. The multi-peak MACE filter designed with n training images and m unique peak locations is of the same form as the MACE filter and is given by,

$$\mathbf{h} = \mathbf{D}^{-1}\mathbf{X}(\mathbf{X}^{+}\mathbf{D}^{-1}\mathbf{X})^{-1}\mathbf{u} \tag{4}$$

where $\mathbf{X} = [\mathbf{z_1 e^{-j(ux_1+vy_1)}} \ldots \mathbf{z_n e^{-j(ux_1+vy_1)}} \ldots \mathbf{z_1 e^{-j(ux_m+vy_m)}} \ldots \mathbf{z_n e^{-j(ux_m+vy_m)}}]$ now contains in the columns, the vectorized versions of the two-dimensional FT of the modulated training images. The modulation for each peak is $e^{-j(ux+vy)}$ where (x,y) is the desired location of the correlation peak. $\mathbf{D}$ is a diagonal matrix with the average power spectrum of the modulated training images along its diagonal.

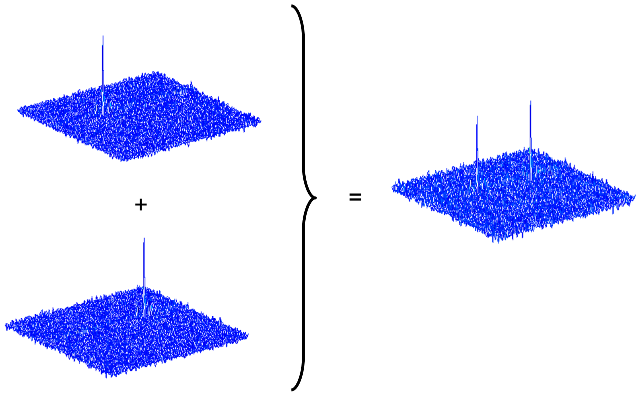

Fig. 2. A multi-peak correlation plane can be thought of as the sum of many correlation planes each producing one peak, but at distinct locations

3 Proposed Framework

The main idea behind our approach is to use correlation filters for the dual purpose of biometric matching and information hiding thereby binding the hidden information to the training images used to design the filter. During authentication this hidden information is released automatically if the match is determined to be an authentic match.

In an encryption system, two inputs, “secret” and “cipher key”, are algorithmically combined to give out one output, “cipher text”. The framework that we present here is flexible enough that we can hide either the “secret” or the “cipher key” in the filter. Each of the alternatives has its own advantages and disadvantages. Hiding the message directly would impose constraints on the maximum length of the message since there is a trade-off between how many peaks can be packed and how reliably we can recover the information. However it must be noted that recovering the information by brute force is as hard as decrypting a conventionally encrypted message. When hiding the encryption key, the message can now be of any length although the length of the encryption key is limited by the constraints in the performance of the filters. To allow for flexibility in the key length, we can use one more level of encryption to encrypt the “cipher key”. Now the key required for the second encryption is hidden in the correlation filter and the first “cipher key” now becomes the message in our framework. Such a scenario would arise when the key length required for the first encryption is beyond the capability of our framework (e.g., RSA-1024). In this initial work, we only consider the case where the key is hidden in the correlation filter.

Template protection is achieved by convolving the images with a random kernel as proposed by Savvides et.al [10]. Fig. 3 shows an example.

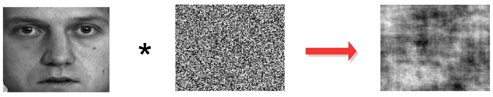

Fig. 3. Image encryption with a random convolution kernel

The resulting image looks very different from the original image, effectively securing the original images. It also helps us achieve revocability and diversity by assigning different kernels for different people and different applications. One way to do this would be by asking the user for a password and using it as a seed for the random number generator from which the random kernel is obtained. It was shown theoretically and empirically in [10] that matching in this encrypted domain does not lead to any loss of performance. We design the modified MACE filter introduced in the previous section with these encrypted images.

3.1 Enrollment

Fig. 4 shows the block diagram of the enrollment process. During enrollment the user provides multiple samples of his/her biometric (shown as ”Training Data” in Fig. 4), the “secret” that is sought to be protected and a password to create the random kernel to encrypt the images. The number of peaks in the output correlation plane for a user

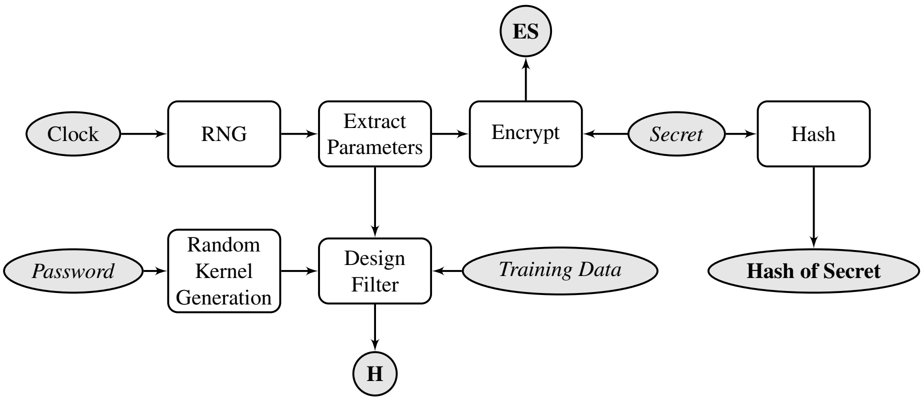

Fig. 4. Block diagram of the enrollment process. Uncolored blocks denote internal processing. Colored blocks with *italicized* text denote input and **bold** text denote output.

is selected at random between some minimum and maximum number depending on the desired level of security. Then the locations of the peaks are selected at random depending on the resolution of the images. We further choose the polarity of each peak (± 1) at random. This set of numbers representing the number of peaks, the polarity of the peaks and the locations of the peaks are concatenated to form the encryption key for that user and is used to encrypt the message. This whole process is captured in the blocks labeled “clock”, “RNG” and “Extract Parameters”.

The peak locations are used as constraints while designing the multi-peak MACE filter described in the previous section. The filter is the cancelable template for the user and is stored in the database along with the encrypted message. We also store the hash value of the message using a one-way hash function. Thus each user has their own cancelable template designed with a random number of peaks, polarity of peaks and peak locations.

To get stable correlation planes with sharp peaks, the peak locations for designing the filter are chosen such that there is at least a 3 pixel separation between adjacent peaks. We also do not allow the peaks to be within 5 to 10 pixels from the boundary of the image. Sharper peaks corresponds to better recognition performance and greater number of peaks provides more security. Both of these cannot be achieved simultaneously since there exists a trade-off between how many peaks one can pack in the correlation plane and the sharpness of the peaks.

3.2 Authentication and Identification

Fig. 5 shows a block diagram of the authentication process. In the authentication stage, the user provides the biometric (denoted as ”probe” in Fig. 5) along with the password for his/her random kernel. The biometric is convolved with the random kernel derived from the password. The resulting image is then correlated with the filter stored in the database. If the match is authentic, the resulting correlation plane would have sharp peaks at the locations that the filter was constrained to produce peaks at. From the peak locations, the key is retrieved and is used to decrypt the stored encrypted message. For

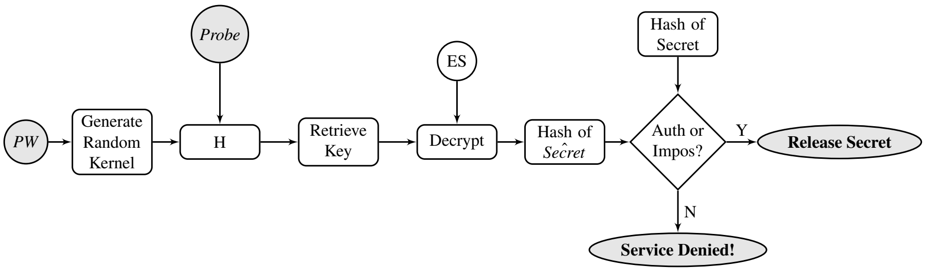

Fig. 5. Block diagram of the authentication process. Uncolored blocks denote internal processing. Colored blocks with *italicized* text denote input and **bold** text denote output.

an authentic match, the retrieved key would be correct while for an impostor, it would be wrong leading to incorrect message decryption. This is confirmed by comparing the stored hash value of the original message with the hash value of the recovered message. Only when the two match, the "secret" is released. For an impostor the decryption would fail because there would not be any sharp peaks in the correlation result when either the password is wrong or the biometric is wrong or both are wrong.

4 Security Analysis

In the proposed framework, protection is provided at two levels, password and biometric. Both the biometric and the password have to be correct for correct decoding of the protected message. We consider three kinds of possible attack strategies. In all the scenarios, we assume that the attacker has access to the database i.e., the encrypted message, the biometric template and the hash value of the message.

4.1 Brute Force

This corresponds to the scenario when the attacker does not have access to both the password and the biometric. The attacker now has to guess the decryption key which means he must guess the number of peaks, polarity of the peaks and the peak locations. Once the number of peaks and their peak locations are correctly guessed, the attacker gets the decryption key and can decrypt the encrypted message. For an image size of MxN pixels and a filter design with Q peaks, the entropy $L(Q)$ in bits is given by:

$$L(Q) = \sum_{i=1}^{Q} [\log_2\{(M-q)(N-q)-(i-1)p^2\}-1] \tag{5}$$

where q is the size of the boundary region that is ignored and p is the minimum separation between the peaks in the correlation plane. The $(M-q)(N-q)$ term quantifies the number of available peak locations for the first peak. Now since there is a minimum required separation of p in either direction between the peaks, the number of peak locations for the subsequent peaks reduces by p^2. We also allow for the retrieved peak location to be off by 1 in either x or y direction which is accounted for by subtracting 2 bits per peak and adding one bit for the sign of the peak.

To provide equal amount of security to all the users of the system in the same application, each user is assigned the same number of peaks depending on the security and performance trade-off. Thus the amount of security is $L(Q)$ with Q peaks per user. In situations where more flexibility is needed and equal security for all users is not required, each user can be assigned different number of peaks. It must be noted that there is no storage or computational cost associated with using different number of peaks. However, the amount of security and the recognition performance would be different.

4.2 Compromised Biometric

This is the scenario where the attacker does not know the password but obtains the biometric, for example a face image from the subject's web site or fingerprints from the objects the subject touches etc. In this case, the security depends on how guessable the password is and also on the quality of the biometric stolen by the hacker. Without the password, the random mask would be wrong and the decoding will fail. So the amount of security is equal to the strength of the user's password or the complexity of the encryption used, whichever is lower.

4.3 Compromised Password

This is the scenario where the attacker knows the password but does not have the biometric. In this case since the biometric would be wrong, the result of the correlation with the filter would either not produce any peaks or produce them at the wrong location which causes the decryption to fail. The amount of security in this case would depend on the complexity associated with guessing the biometric (e.g., by hill climbing technique [19]) or the complexity of the encryption used, whichever is lower.

5 Numerical Results

We used the CMU-PIE database to evaluate the effectiveness of the proposed scheme and we allowed for illumination changes only in our experiments. We believe that since biometric key-binding would be used for applications such as access control, e-commerce etc., it is reasonable to expect user cooperation while presenting their biometric. Illumination is something that can't really be controlled very well (even for cooperative users) and hence becomes one of the sources of variability in appearance. Further we use both the PIE-lights and PIE-nolights for our evaluation and present the verification results. The PIE-lights database consists of 68 classes with 24 images per class while PIE-nolights consists of 66 classes with 21 images per class. In our experiments we used 3 images for training the MACE filter and the rest of the images for testing. The 3 training images were chosen such that one has illumination from the left, another has illumination from the right and the third has illumination from the front.

We conducted numerical experiments corresponding to two different levels of security. In one case we use both the password and the biometric for authentication (referred to as whole), while in the other case we use only the biometric i.e., the images are not convolved with a random mask which is the scenario when the password is compromised (referred to as part). Table 1 summarizes our results for both subject verification

Table 1. Performance with 5 Peaks and Image Size 256

Exp. Type	Recognition		Decryption			
	Lights	No Lights	Lights		No Lights	
	EER (%)	EER (%)	DFR (%)	FDR (%)	DFR (%)	FDR(%)
Whole	0.0	0.083	1.4	0.0	3.2	0.0
Part	0.072	0.65	2.3	3.2	3.5	1.6

and successful message decryption. We show equal error rates (EER) for verification performance and to quantify key-retrieval performance we look at the decryption failure rate (DFR) for the authentic users and the false decryption rate (FDR) for the impostors i.e., impostors who could retrieve the key of another user.

When the whole system is used, i.e., when both password and biometric are available, the FDR is very close to zero, while in the case where only the biometric is used, the FDR is higher at about 3.2% in the case of PIE-lights. This is because of the presence of users who look similar to each other. When the password is used, since the images are convolved with a random mask the effect of the similarity in the face images is reduced by the randomness of the mask thereby reducing the FDR. Hence the use of the random mask not only protects the template but also helps reduce the FDR.

The results in Table 1 used images of resolution 256x256 with 5 peaks for each user. A region of 10 pixels near the boundary was ignored and the minimum distance between the pixels was set to 5. The entropy for 5 peaks is 74 bits which is the amount of security of the system since all the users have the same number of peaks.

Table 2 summarizes results for both subject verification and successful message decryption when the number of peaks is increased to 7 using images of size 256x256 giving 103 bits of security. Increasing the number of peaks from 5 to 7 increases the amount of security. However there is a performance degradation in both DFR and FDR. The FDR when using the whole system is still 0% which is very desirable.

Table 2. Performance with 7 Peaks and Image Size 256

Exp. Type	Recognition		Decryption			
	Lights	No Lights	Lights		No Lights	
	EER (%)	EER (%)	DFR (%)	FDR (%)	DFR (%)	FDR(%)
Whole	0.0	0.12	2.0	0.0	3.4	0.0
Part	0.1	1.0	2.6	3.8	3.9	3.0

Table 3 shows results for both subject verification and successful message decryption with 6 peaks with the resolution of the images being 128x128 which amounts to 75 bits of security. Using images of smaller size reduces the security and also since the peaks are more closely packed there is a performance degradation.

Table 3. Performance with 6 Peaks and Image Size 128

Exp. Type	Recognition		Decryption			
	Lights	No Lights	Lights		No Lights	
	EER (%)	EER (%)	DFR (%)	FDR (%)	DFR (%)	FDR(%)
Whole	0.0	0.08	0.21	0.0	4.3	0.0
Part	0.07	1.2	0.14	0.25	4.4	0.05

6 Limitations

To understand the true effectiveness of our scheme, one must think of all possible attack strategies. However due to space constraints we will briefly mention only some limitations of the proposed framework.

- Key retrieval is tied strongly to subject verification which means this scheme is effective only when the verification performance is acceptable.
- Stealing biometrics is not too difficult (e.g., one can easily obtain face images from a personal web site), in which case it may turn out that our system is only as strong the password used to encrypt the images. However all biometric-based authentication systems would also face the same problem.
- Once the password in our scheme is compromised, it might become vulnerable to a hill climbing attack. However, it must be noted that the hidden message can be recovered only by a very good estimate of the biometric via hill climbing.
- If the database is not very secure the stored template can be tampered with leading to a denial of service attack or more seriously, a blended substitution attack is also possible. A simple scheme to prevent both of these attacks is to check if the template has been tampered before using it or by making the database read-only.

7 Conclusions

We presented a novel framework for biometric key-binding and template protection using correlation filters and demonstrated its effectiveness in terms of recognition performance and security. Our framework provides great flexibility and scope for expansion. The presented scheme also addresses other important issues like cancelability and diversity and offers two-factor authentication.

Acknowledgements

This work was supported in part by US Army Research Office (ARO) support to CyLab at Carnegie Mellon University.

References

1. Soutar, C., et al.: Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques II, vol. 3314, pp. 178–188 (1998)
2. Soutar, C., et al.: Proc. SPIE, Optical Pattern Recognition IX, vol. 3386, pp. 24–35 (1998)

3. Soutar, C., et al.: Biometric encryption. In: Nichols, R.K. (ed.) ICSA Guide to Cryptography. McGraw-Hill, New York (1999)
4. Juels, A., Sudan, M.: Proc. of IEEE Intl. Symp. on Info. Theory, Lausanne, Switzerland, p. 408 (2002)
5. Uludag, U., et al.: Fuzzy vault for fingerprints. In: Kanade, T., Jain, A., Ratha, N.K., et al. (eds.) AVBPA 2005. LNCS, vol. 3546, pp. 310–319. Springer, Heidelberg (2005)
6. Lee, Y.J., et al.: IEEE Transactions on Systems, Man, and Cybernetics-Part B 38, 1302–1313 (October 2008)
7. Scheirer, W.J., Boult, T.E.: Proc. of Biometrics Symposium, September 2007, pp. 1–6 (2007)
8. Kholmatov, A., Yanikoglu, B.: Proc. of SPIE Symposium on Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, San Jose, USA, vol. 6819, pp. 68190O–68190O-7 (2008)
9. Ratha, N.K., et al.: IEEE Trans. Pattern Anal. Mach. Intell., 561–572 (2007)
10. Savvides, M., et al.: International Conference on Pattern Recognition, pp. 922–925 (2004)
11. Hao, F., et al.: IEEE Trans. Computers, 1081–1088 (2006)
12. Sutcu, Y., et al.: IEEE International Symposium on Information Theory (ISIT), pp. 2297-2301 (July 2008)
13. Sutcu, Y., et al.: IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), June 2008, vol. 23, pp. 1–6 (2008)
14. Vijaya Kumar, B.V.K., et al.: Proceedings of International Conference of Image Processing, September 2002, pp. 53–56 (2002)
15. Savvides, M., Vijaya Kumar, B.V.K.: Proceedings of IEEE Conference on Advanced Video and Signal Based Surveillance, July 2003, pp. 45–52 (2003)
16. Thronton, J., et al.: Proceedings of International Conference on Image Analysis and Recognition, September 2005, pp. 1098–1105 (2005)
17. Vijaya Kumar, B.V.K.: Applied Optics 31, 4773–4801 (1992)
18. Mahalanobis, A., et al.: Applied Optics 26, 3633–3640 (1987)
19. Adler, A.: Audio and Video Based Biometric Person Authentication, pp. 1100–1109 (2005)