17

Template Protection For 3D Face Recognition

Xuebing Zhou, Arjan Kuijper and Christoph Busch
Fraunhofer Institute for Computer Graphics Research IGD
Germany

Abstract

The human face is one of the most important biometric modalities for automatic authentication. Three-dimensional face recognition exploits facial surface information. In comparison to illumination based 2D face recognition, it has good robustness and high fake resistance, so that it can be used in high security areas. Nevertheless, as in other common biometric systems, potential risks of identity theft, cross matching and exposure of privacy information threaten the security of the authentication system as well as the user's privacy. As a crucial supplementary of biometrics, the template protection technique can prevent security leakages and protect privacy.

In this chapter, we show security leakages in common biometric systems and give a detailed introduction on template protection techniques. Then the latest results of template protection techniques in 3D face recognition systems are presented. The recognition performances as well as the security gains are analyzed.

1. Introduction

Biometrics is technique to automatically recognize a person based on his/her physiological or behavior characteristics. Since the characteristics used are unique to each individual, biometrics can create a direct link between users and their identity. From this point of view, it can provide more secure authentication in comparison to password and token based methods. Moreover, it is very convenient to use.

Applications of biometrics have spread rapidly in last decade and are still growing. In European e-passports, images of faces and fingerprints are stored. Many countries employ biometric information in citizen cards. In the US visit program, 10 fingers and the facial image are also acquired to support visa application and border control. It is efficient to prevent identity fake and increase the security against terrorists. Additionally, biometrics are widely used in access control, payment, banking and so on.

As biometrics markets are blooming, novel security and privacy leakages, such as exposure of private sensitive information, unchangeability and impersonate of biometric identities, and profiling, attract a lot of attention from public sectors, data protection officers, service providers and end users. After carefully analyzing the weakness of biometrics and summarizing requirements for secure biometric authentication, template protection techniques have been developed as an important supplement to common biometric system with improved security and enhanced privacy protection.

In this chapter we address the template protection techniques for 3D face recognition systems. Among fingerprints and iris, face is one of the most popular biometric modalities. So far, facial information is mainly acquired as 2D illumination based images, 3D surfaces, or 2D near infra-red images. In comparison with other methods, 3D face recognition utilizes rich geometric information of facial surfaces, is less sensitive to ambient light conditions and robust to face variation due to different poses. Especially due to its resistance to fake attack it is very attractive in high security applications. Recently, 3D scanners become more and more efficient and economically priced. A sufficiently precise 3D face scan can be accomplished in several milliseconds. 3D face recognition shows a better recognition performance than 2D face recognition and other kinds of biometrics modalities. By implementing template protection techniques for 3D facial information not only the 3D facial information itself is protected. Also potential risks are avoided and high secure authentication systems become realizable.

2. Motivation

As biometrics is applied in manifold areas and users enjoy its benefits, vulnerabilities of biometric system and potential security risks cannot be neglected or underestimated as shown in following example.

Bob is a frequent traveller. He does not like waiting in long queues including the queue in front of a border control desk. Thus, he registers at the airport for the automatic verification system that is based on 3D face recognition. When crossing the border, the system reads his travel document, performs a 3D scan of his face and compares it with the stored information. This saves the busy businessmen Bob a lot of time. He gets enthusiastic about biometrics and enrols himself in 3D face recognition in the bank for cash points. Later he visits a casino and leaves his 3D face information to access the casino.

In this example, he used the same biometric information in different areas. Some of them are trustworthy. But can he really trust all the different service providers? What will happen, if his biometric information is compromised? In the following we elaborate the privacy and security issues in biometrics.

Aggravation of identity theft/fraud Biometric characteristics can not be stolen or handed over like token or password, but they can be faked. For example, it is shown in (2; 20) how effortless it is to make a gummy or laminate finger using a trace left on a glass. With one more surveillance camera, facial information can be completely exposed even without knowledge or consent of victims. Also, a synthetic artifact can be created with stored biometric templates (4; 10; 15). Remote authentication systems based on digital transmitted biometric data can be even attacked without reconstructing biometric modalities. As a consequence, on the one hand integrating liveness detection techniques in sensors is essential to prevent impersonation. On the other hand, protection of stored and transmitted biometric data is significant.

3D face recognition has advantages in comparison with other modalities from a security point of view. It is hard to obtain 3D face information, since it can not leave a trace like fingerprints. Besides the up-to-now minor risk of deriving a 3D face surface from photos, there is the risk to reconstruct a 3D face surface from stored biometric templates. [1]

Unchangeability On the one hand, one of the advantages using biometrics is that users and their identity are linked together with their personal unique biometric characteristics. On the other hand, the exposure of biometric data is critical since it can not be easily revoked or renewed as in common password or toked based authentication. One

[1] It is difficult to keep some biometric modalities such as fingerprint, 2D face images, ''secret''. In applications requiring high security, using these modalities should be avoided.

can only choose another biometric modality or try to modify the exposed one. Unfortunately, both are not suitable solutions: we only have a limited number of biometric modalities, e.g. ten fingers, one face and two irises. And alteration of our biometric modalities is only possible with very complicated methods such as transplantation or cosmetic surgery. In the report of defense science board (3) , it is also emphasized that revocation of biometric keys used for identity or privilege is indispensable.

Cross matching As the same biometric modality is adopted in multiple applications, all these applications are potentially coupled. A untrustworthy data collector can track the activities of a subject in external applications and misuse these informations. Additionally, if the biometric identity is compromised in one application, all the others get in danger.

Privacy Biometric data is derived from human bodies or the behavior of a person. Per-se this personal information is sensitive information. For example, in (30) it is shown that some diseases and sexual orientation have influence on fingerprint. The disease such as free-floating iris cyst, diffuse Iris Melanoma, can change iris pattern. From a face photo, gender and race of users can be recognized. DNA-analysis can expose sensitive genetic information. 3D face information is widely used in medical analysis. Moreover, many genetic syndromes can effect the facial trait. Therefore, 3D face scans is used to analyze facial morphology (13) as well as to diagnose some gene syndromes (29). Such private information is not relevant for the authentication purpose. But it is contained in every 3D face scan and therefore retrievable from the scan results.

Legislation Since biometrics belongs to personal information, usage of biometrics including storage and collection is very critical from the legislation point of view. In the European data protection directive (1), it is emphasized to protect individuals regarding to the processing of their personal data. In the white paper of TeleTrustT Deutschland e.V. (7), it is elaborated the importance of data protection in biometrics in compliance with the legislation.

Hill climbing Decision of biometric authentication rests on the similarity (or distance) measurement between stored templates and a live derived template. A feedback of a comparison can be obtained, e.g. directly from the authentication response, or from a Trojan horse embedded in a computer. An attacker can exploit such information to reconstruct the stored biometric template or the biometric sample recursively (33). It is so called hill climbing attack

The above issued security and privacy problems arise from the uncertainty of stored or transmitted biometric data. The Information and Privacy Commissioner/Ontario also dwelt on the problems of biometrics and drew the conclusions that applying biometrics causes ''a zero-sum game" for this reason: biometrics provide additional security guarantees, meanwhile, it brings also new leakages. Therefore techniques to protect biometric data is necessary(11). In the next session we introduce the possible solutions to overcome these drawbacks.

3. Template Protection Techniques

Recently template protection techniques – also known as biometric encryption, untraceable biometrics, cancelable or revocable biometrics – have been developed in order to meet the requirements of protecting stored biometric data. These methods convert biometric data elements into multiple (ideally) uncorrelated references, from which it is infeasible to retrieve the original information. Template protection is a generalized and efficient method to preserve privacy and to enhance the security of biometric data by limiting the exposure of template data which must not be revoked. They have the following key properties:

One-Way and Robustness The computational complexity of deriving a secure reference from a biometric datum (template) is limited, while it is either computationally hard or impossible to deduce the template from such a reference. The derivative references can be compared to a biometric datum under similarity metrics for the underlying biometric template. This allows the successful comparison of measurements exhibiting small variations or measurement errors to a derivative reference.

Diversity and Randomness Template protection can create numerous secure references from one biometric feature with the references independent of each other, i.e. knowledge of one reference does not yield information on other references derived from the same template.

The resulting various references are also called pseudo identities (9). Different methods to protect the biometrics data exist. They can be classified into four categories: cancelable biometrics, biometric salting, fuzzy encryption and biometric hardening passwords (36). *Cancelable biometrics* modifies the original biometric features or samples with "non-invertible" functions such as scrambling, morphing so that the original data is no longer to be recognized (26), (8), (27). *Biometric salting* randomizes biometric data with random patterns. For example, in biometric encryption (28) , biometric data is convoluted with randomly generated code and in the biohashing algorithm (16), biometric features are projected into different orthogonal spaces generated from large amount random sequences. *Biometric hardening passwords* fuses password-based authentication with biometrics (22), (21). Finally, *fuzzy encryption* combines cryptographic hashing or secret sharing protocol with error correction codes (ECC) (17; 18). Among these methods, fuzzy commitment is one of the most successful algorithm. In the next section, we give detailed introduction on the helper data scheme, a practical realization of fuzzy commitment.

4. Template Protection with Helper Data Scheme

In 1999, Juels et al. proposed the "fuzzy commitment" to protect biometric information by using an existing cryptographic scheme (18). It is similar to password authentication system on Unix computers. There, passwords are never stored or compared in a plain text form but in an encrypted form. The system can authenticate a user without knowing the original password. Accordingly, a fuzzy template can be generated from biometric information and can be safeguarded with cryptographic functions. Yet, the protection scheme must have tolerance to variation of biometric data due to measurement noise or alteration of modalities. To overcome this problem, error correction coding is used.

Later, the Helper Data Scheme (HDS) has been developed to make the idea of fuzzy commit feasible for biometric systems. HDS can extract secure templates from biometric data. This secure template is stable to biometric variation and it is impossible to retrieve original biometric information from it. The mathematical formulation of these properties is summarized as delta-contracting and epsilon-revealing by J. P. Linnartz et al. (19). The block diagram of the HDS is depicted in figure 1.

In figure 1 M is a biometric template extracted from a biometric measurement. In the enrollment process, the binarization converts the biometric template M into a binary vector Q. Ideally, the binarization results in a binary string that is uniformly distributed for different users and invariant for an identical user. The detailed description of binarization is given

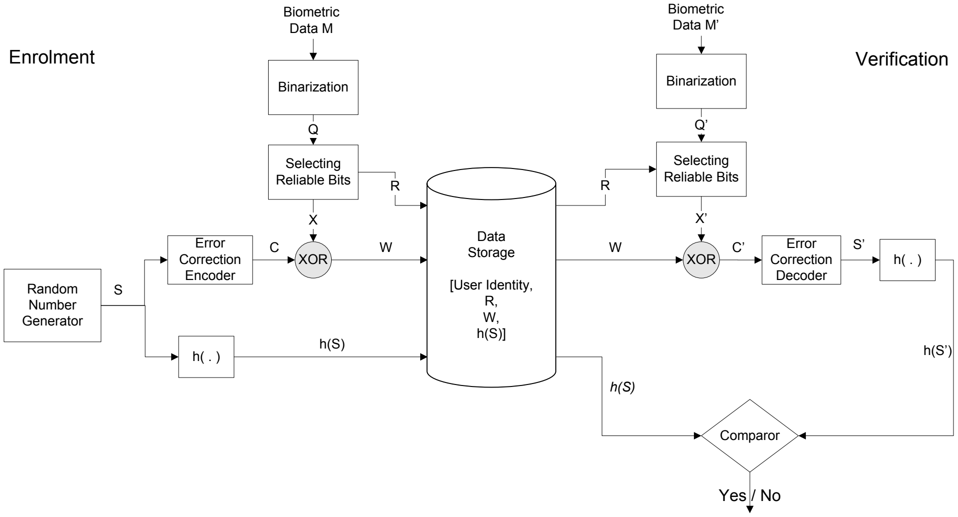

Fig. 1. Block diagram of the helper data scheme

in section 4.1. In parallel, a random number generator creates a secret code S. First, S is hashed and stored. Thus, it enables randomness in the system so that distinct references can be created from the same biometric characteristics for different applications. Second, a error correction encoder adds redundancy in the secret S. As a consequence, the resulting codeword C is longer than S. Depending on the characteristics of the bit errors, different error correction codes can be adopted. Foe example, when bit errors are uniformly distributed in the codeword, a BCH-code, which has a codeword length of $2^L - 1$[2], can be employed. If the length of the binarized vector Q extends the length of the codeword C, then the most reliable bits in Q are selected so that the resulting binary string X is as long as the codeword C and robustness is improved. R indicates the position of reliable bits. W, the result of the bitwise XOR-function of X and C, is so called helper data. With help of W and for a suitable input, the secret S can be recovered in the verification process. Instead of storing the secret S, the position vector R, the helper data W, the hashed secret code $h(S)$ and user identity information are stored in data storage. It can be proved that both W and $h(S)$ reveal little information about S, X as well as the biometric template M (32).
During the verification process, with claimed identity, R, W and $h(S)$ are retrieved from the data storage. The binary string Q' is extracted from biometric template M', which is M potentially distorted by noise. The binary string X' is estimated with Q' and R. A potentially distorted codeword C' can be acquired from W and X'. The following error correction decoder removes errors in C' and results in the reconstructed secret code S'. By comparing $h(S)$ with $h(S')$, a positive or negative response for a verification query can be given. In contrast to common biometrics system, only a "hard decision" (rejected or accepted) is given and no similarity score is available in the comparator of the template protection system due to the applied hash function. The previously described hill climbing attack, which iteratively reconstructs biometrics using matching scores (5)′ (31), is not applicable.

[2] L is a natural number

The length of the secret code is one security issue. If the length of the codeword is fixed, the length of the secret code is restricted by the error correction ability. The maximum length of the codeword relies on the entropy for the considered biometric characteristics. Obviously, the processes of binarization and selection of reliable bits strongly affects the performance of the template protection scheme. In the following sections we introduce their functionalities and construction.

4.1 Binarization

Binarization is the core component of the helper data scheme. The requirements of its output binary vector can be summarized as follows: binarized vectors of different users should be uniformly and independently distributed, and the binary vector of a specific user should be robust to variation of biometric data. It guarantees that no prediction of a binary vector is possible and the discriminability of binary vector is optimized. And no information of a user can be obtained using binary vectors of other users. The binarized features have certain resilience to noise.

Moreover, binarization tries to extract a long binary vector from biometric template without any degradation of authentication performance. The construction of binarization depends on the statistical analysis of the input biometric templates. Assuming that a training template set contains N users and each user has K samples and $M_{n,k} = \left[m_{n,k,1}, m_{n,k,2}, \cdots, m_{n,k,T}\right]$ is the template with T components extracted from the k-th samples of the user n with $k \in \{1, \cdots, K\}$ and $n \in \{1, \cdots, N\}$. If each component is statistically independent and at least one bit can be extracted from each component, the binarization function can be defined as:

$$q_{n,t} = B\left\{m_{n,k,t} | k \in [1, \cdots, K]\right\} = \begin{cases} 1 & \text{if} \quad \mu_{n,t} \geq \mu_t \\ 0 & \text{if} \quad \mu_{n,t} < \mu_t \end{cases} \tag{1}$$

where $\mu_{n,t}$ is an estimation of the real template for user n and μ_t is the threshold of binarization. In order to achieve uniform distribution of the binary vector, μ_t could be the median of $\mu_{n,t}$ of all the users. Instead of the median, the mean can also be adopted. If the training data set is large enough, there is no significant difference between median and mean. In practice, we suggest to use the median, which is resistant to extreme values caused by measure errors.

4.2 Selecting Reliable Bits

Selecting reliable bits contributes to the robustness of the system. It is based on the estimation of the error probability for each bit. Only the bits with the lowest error probability are selected. In the previously presented binarization method, the error probability depends on the distance between $\mu_{n,t}$ and μ_t as shown in equation 1. $\mu_{n,t}$ of a relative stable bit should derive from μ_t. On the other hand, intra-class variation also affects the error probability. The smaller the intra-class variation is, the more reliable the corresponding bit is.

Statistical analysis of intra class characteristics for each user has a major effect on the performance of selecting reliable bits. If biometric templates are Gaussian distributed, then:

$$\mu_{n,t} = E\left\{m_{n,k,t} | k \in [1, \cdots, K]\right\} \tag{2}$$

$$p_{n,t} \propto \frac{|\mu_{n,t} - \mu_t|}{\sigma_{n,t}} \tag{3}$$

where E is the function calculating the expected value, $p_{n,t}$ is the error probability of the t-th component of user n, and $\sigma_{n,t}$ is the standard deviation of $m_{n,k,t}$ for $k \in [1, \cdots, K]$ (see also (34)).

If biometric templates are not Gaussian distributed or it is impossible to estimate intra class variation, then:

$$\mu_{n,t} = MEDIAN_{k=1}^{K} \{m_{n,k,t}\} \tag{4}$$

$$p_{n,t} \propto |\mu_{n,t} - \mu_t| \tag{5}$$

Actually, the reliable estimation of error probabilities can only be achieved with a sufficient number of samples. In the next section we show how the template protection using the helper data scheme is integrated in 3D face recognition system.

5. An Example of Secure 3D Face Recognition System

The above sections stressed the importance of protecting biometric data and introduced to the details of template protection systems. In this section, we show how such a method can be integrated in a 3D face recognition system. Our experimental results show the effect on the performance. At first, we will give an introduction on 3D face recognition algorithm.

5.1 3D Face Recognition Algorithm

In a 3D face recognition system, a 3D face image can be acquired by using a structured light projection approach. To compensate pose variation during acquisition, the 3D face images are normalized in a pre-processing step to a frontal view. The normalized facial image represents the face geometry and can be used as a biometric feature. For example, the normalized images can be compared using the Hausdorff distance classifier ((24), (23)). This normalized data, however, cannot directly be utilized in the template protection, since these features are strongly correlated and very sensitive to noise. A process to extract compact and robust features is required. The Eigenface and Fisherface feature extraction algorithms (e.g. (12), (14) and (6)) are widely used to reduce dimensions of the original data. These statistics-based algorithms achieve a good verification performance, however, the size of the features is strongly reduced and it is difficult to extract binary vectors of sufficient length, which is required for an input for the helper data scheme.

In our experiments, we use a histogram-based feature extraction algorithm. It is based on the distribution of depth-values of the face region to characterize facial geometry. In this algorithm, a three dimensional rectangular region of a normalized image is used to limit the considered facial surface points. In Figure 2, the intermediate processes of the proposed algorithm is depicted. The algorithm consists of the following processing steps:

1. The facial surface points to be evaluated are selected from a normalized range image as shown in the dark area of the image at the lower left of Figure 2.
2. The selected facial region is further divided into J disjunct horizontal stripes S_j, where $j \in [1, \cdots, J]$ (see the image at the lower right of Figure 2). By this, the algorithm evaluates local geometric surface information. Due to the symmetric properties of a human face, the stripes are perpendicular to the symmetry plane.
3. The distribution of the facial points p_i in stripe S_j is counted. If $\{d_0, \cdots, d_L\}$ is a vector with $L + 1$ elements. This vector is used to partition the surface points in the horizontal stripes according to their depth-value. d_0 and d_L indicate the upper band and lower band of depth limit, the l-th feature of the stripe S_j is given as follows:

$$f_{l,j} = \frac{\left|\left\{p_i = (x_i, y_i, z_i) | p_i \in S_j, d_{l-1} < z_i < d_l\right\}\right|}{\left|S_j\right|}, \tag{6}$$

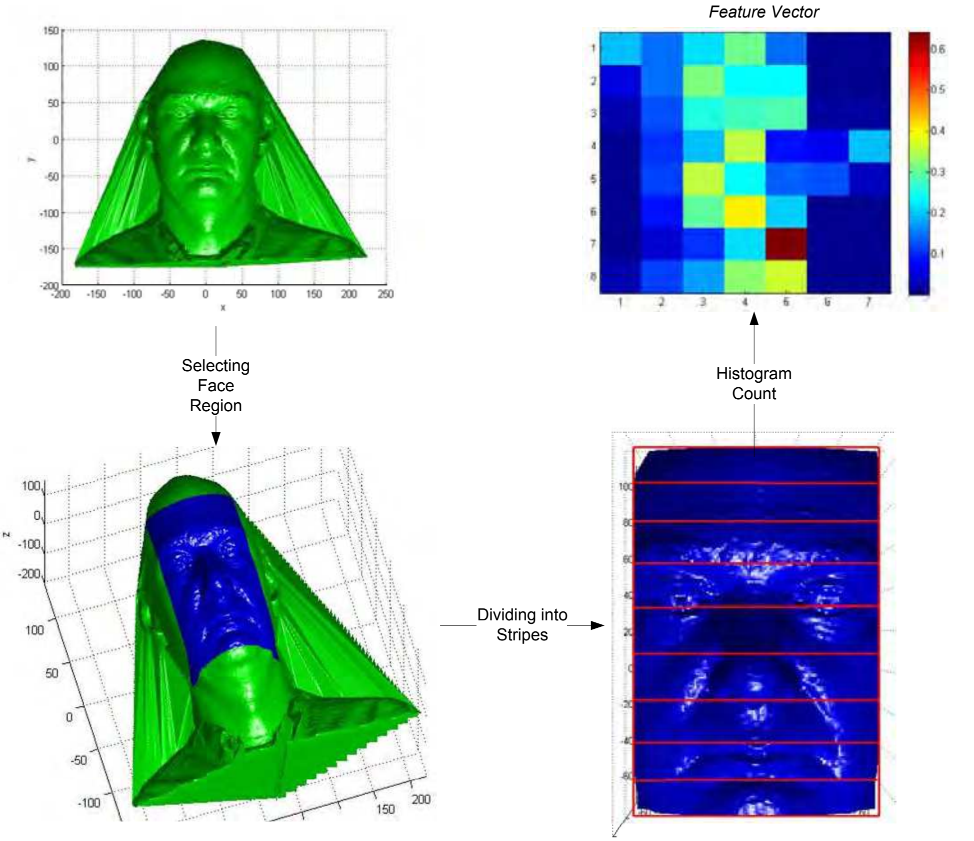

Fig. 2. An overview of the histogram-based face recognition algorithm

where $l \in [1, \cdots, L]$, $j \in [1, \cdots, J]$, z_i is the depth value (z-value) of point p_i, $\left|S_j\right|$ is the number of the facial points in S_j. $f_{l,j}$ represents the proportions of the points in S_j, whose z-values are located in the region $[d_{l-1}, d_l]$.

The resulting feature corresponds to the histogram count of the stripe. Therefore the proposed algorithm is called histogram-based face recognition algorithm. An example of feature values is shown in the image at the top right of Figure 2, where the feature vector corresponding to each stripe is represented as a row in the image and the color indicates their absolute feature values.

The algorithm adopts a simple statistical analysis to describe the geometrical character of a facial surface. This algorithm efficiently filters noise and reduces the correlation in the range image. The resulting feature vectors can be used as an input to the quantizer preceding the template protection scheme. More details about this algorithm are shown in (35).

5.2 Experimental Results

We have implemented HDS in the 3D face recognition system. The 3D facial images of face recognition grant challenge (FRGC) (25) database version 2 are used as testing data. The 3507 samples from 454 subjects are correctly normalized. During the test, only the users, who have at least 4 samples, are chosen. Three samples per user are chosen as enrollment data and one sample as verification data. A different sample for the verification is chosen for each test and the tests are repeated 4 times.

The preciously described feature extraction process is applied with the following parameters. The 3D facial data is normalized to compensate the pose variation in the acquisition. The normalized 3D facial data is projected into regular grids. Then a fixed face region is selected for each resulting range image. The selected face region is divided into 68 sub-areas. A histogram-based extraction algorithm is applied in each sub-area. A feature vector containing $68 \times 6 = 408$ real values is obtained. The false acceptance rate (FAR) and the false rejection rate (FRR) using the correlation classifier is plotted in figure 3. The equal error rate (EER) is equal to 3.38%.

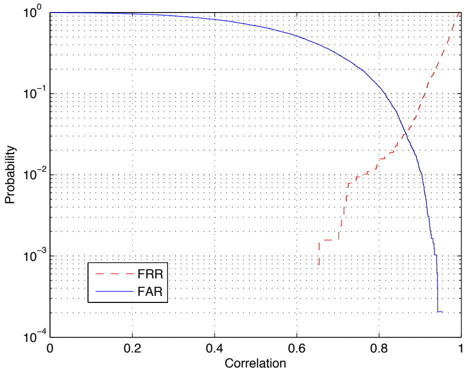

Fig. 3. Classification results of the histogram-based face recognition algorithm

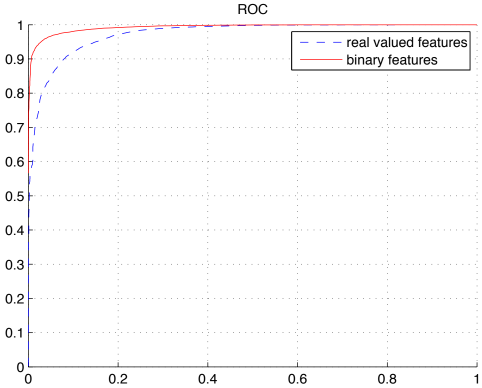

Fig. 4. ROC curves of real-valued feature vectors and binary feature vectors

Then, we use the above mentioned binarization function to convert the extracted feature vectors into binary strings. To compare the authentication performance before and after binarization, we show the receiver operation characteristic (ROC) curves in figure 4. The solid line of the binary feature vectors is obviously above the dashed line of the real-valued feature vector. That is to say, binarization function improves slightly the authentication performance. Generally, a good binarization can be applied with acceptable changing on the authentication performance.

If we compare the distribution of interclass and intraclass distance before and after binarization process as shown in figure 5 and figure 6, the binarization has much stronger influence on the distribution of the inter-class distance than on the intra-class distance. After binarization, the inter-class distance becomes more symmetrical and concentrates on 50%.

In the above binarization process, the median was adopted to calculate the binarization threshold. If we compare the FAR and FRR curves of the binarization using median (figure 7) and mean (figure 8), there is no significant difference regarding authentication performance. Both

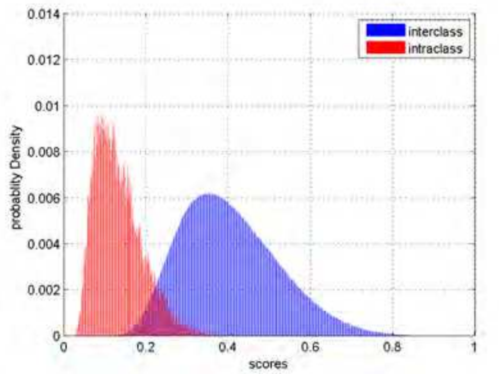

Fig. 5. Probability density of interclass and intraclass distance of real valued features

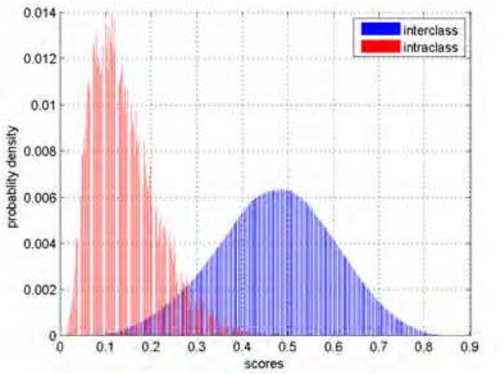

Fig. 6. Probability density of interclass and intraclass distance of binary features

EERs are around 3%. However, the FRR-curve of the mean-based binary vectors deviates from the probability-axis in comparison with the one of the median-based binary vectors. The median-based binarization has higher robustness to noise. This is an advantage over the mean-based binarization, since the performance of template protection is restricted by errors occurring in the binary feature vectors.

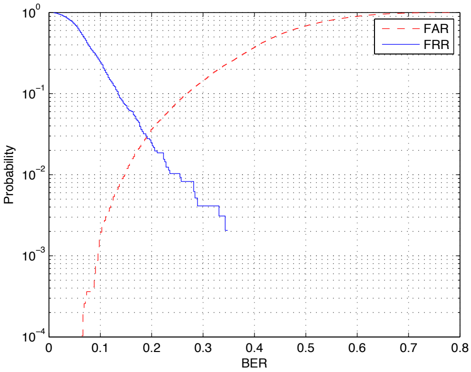

Fig. 7. The classification results for the binary vectors using the median-based binarization

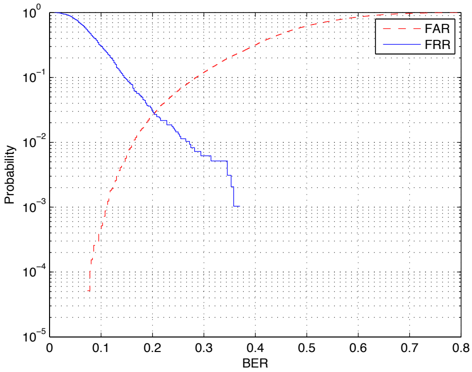

Fig. 8. The classification results for the binary vectors using the mean-based binarization

In the implemented scheme, a BCH- code is chosen as error correction code. The binary features have the length of 408. The maximum length of a codeword under 408 is 255. The 255 most reliable bits is chosen from the 408-bits long binary vector. The classification results under the assumption of uniquely distributed templates and Gaussian distributed templates are shown in Figure 9 and in Figure 10. Both classification results are similar. Under the assump-

tion of uniquely distributions, the robustness is better than under the assumption of Gaussian distributions, however, the discriminative power is slightly worse.
With codeword of 255 bits, only a discrete set of the secret code length s and the correctable errors length e is possible. Several examples and their corresponding bit error rate (BER), FRR and FAR are given in Table 1. The FRR under the assumption of a uniquely distribution is significantly better than under the assumption of a Gaussian distribution, while its FAR decreases slightly.

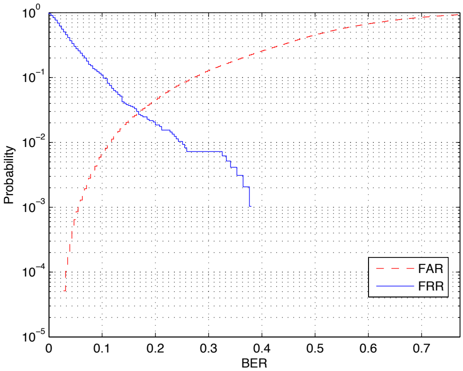

Fig. 9. The classification results for the selected binary vectors under the assumption of uniquely distributed templates

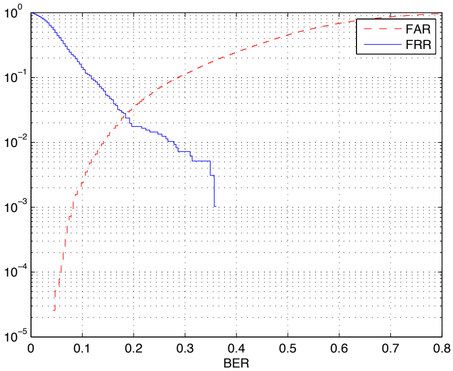

Fig. 10. The classification results for the selected binary vectors under the assumption of Gaussian distributed templates

BCH $(c/s/e)$	Correctable BER	Results for uniquely distribution	Results for Gaussian distribution
255/107/22	8.6%	FRR=12%; FAR=0.4%	FRR=21%; FAR≈ 0
255/91/25	9.8%	FRR=11%; FAR=0.6%	FRR=16%; FAR=0.2%
255/79/27	10.5%	FRR=10%; FAR=0.7%	FRR=13%; FAR=0.3%

Table 1. Examples of possible BCH codes and the corresponding FRR and FAR

6. Discussion

Template protection techniques can derive different secure independent references from biometric data. Secure references can not reveal information of biometric data. No biometric related information is available in authentication systems. Not only biometric data is protected, security leakages such as crossing match, impersonation or cross matching are also avoided. Moreover, they enable revocation and renewing of templates, which are crucial functionalities for authentication process.
Our implementation of a 3D face recognition system shows the general feasibility of a template protection technique. A minor performance degradation is observed in the experimental

results. This might originate in the binarization process and feature selection process: Converting continuously distributed feature vectors into binary vectors can result in information lost.

Although the performance after binarization is improved in our experiments, this can not be generalized for other cases. If feature extraction and the corresponding comparator are optimal, using the biometric features directly has the best performance characteristics. Similarly, the performance degradation for an optimal binarization method is expected to be very small. The selection of reliable components is the requirement of the coding schemes. Additionally, the error probabilities of biometric features normally are not equal. The filtering of unreliable features is helpful to increase the code rate of ECC and secret length. The reduced feature vector, however, may lose discriminative power in comparison to the unabridged feature vector. Although the performance degradation after integrating template protection in the 3D face recognition exist, the resulting performance is still acceptable and comparable with the system without template proction. Moreover, there is potential for improvement: data-source specific adaptation of the coding scheme or the binarization method. Furthermore, the fusion of different modalities or different feature extraction algorithms – in other words deriving more biometric features for one user – can enhance the security and performance.

As the security of template protection schemes is crucial, their evaluation and analysis should not be limited to their performance. In the given experiment, the security evaluation is based on the length of the secret. However, different security levels can be defined depending on the information that is available and accessible to the attacker. If the attacker has only access to individual entries in database, the only way to obtain the secret or the biometric related information is the brute-force attack for the desired hash value. The length of secret is representative to security. However, if they know the details of the template protection algorithm and also distribution of biometric features, the risk of tracking system with much lower complexity is possible. In the second case, the security is over-estimated if security is simply defined by the secret length. Even worse, an attacker with a sufficiently large biometric database can exploit the false acceptance. By doing this, he can identify individual users which share similar biometric data, i.e. biometric twins.

7. Conclusions

In this chapter we show the privacy and security of common biometric systems, which can not be neglected. Template protection techniques are introduced. They can safeguard biometric data and prevent exposing user's private information. They can stop crossing matching, impersonation and hill climbing problems, meanwhile they enable renewing and revocation of identities. They are an very important supplementary to biometric technique.

An implementation in 3D face recognition is demonstrated. 3D face recognition has good resistance to counterfeit and is widely used in high security area. The experimental results show feasibility of template protection technique. The system performance after integration is comparable with the one without template protection. High security can be achieved with sufficient length of the secret. However, it is possible to improve performance and security with optimized binarization and coding methods. Hopeful this work can draw more attention of security enhancement in biometrics and motivate more research in this area.

8. References

[1] Directive 95/46/ec of the european parliament and of the council. *Offical Journal of the European Communities*, L 281 (1995).

[2] How to fake fingerprints? *Chaos Computer Club e.V.* (2004).

[3] Report of the defense science board task force on defense biometrics. Tech. Rep. 20301-3140, Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, Washington, D.C., March 2007.

[4] ADLER, A. Sample images can be independently restored from face recognition templates. In *Proceedings of Canadian Conference on Electrical and Computer Engineering* (Montreal, Canada, 2003), pp. 1163–1166.

[5] ADLER, A. Reconstruction of source images from quantized biometric match score data. In *In Biometrics Conference, Washington, DC* (September 2004).

[6] BAI, X.-M., YIN, B.-C., AND SUN, Y.-F. Face recognition using extended fisherface with 3d morphable model. In *Proceedings of the Fourth International Conference on Machine Learning and Cybernetics* (2005), pp. 4481–4486.

[7] BIERMANN, H., BROMBA, M., BUSCH, C., HORNUNG, G., MEINTS, M., AND QUIRING-KOCK, G. White paper zum datenschutz in der biometrie. TELETRUST Deutschland e.V., March 2008.

[8] BOLLE, R., CONNELL, J. H., AND RATHA, N. System and method for distorting a biometric for transactions with enhanced security and privacy. US 6836554 B1, Dec 2004.

[9] BREEBAART, J., BUSCH, C., GRAVE, J., AND KINDT, E. A reference architecture for biometric template protection based on pseudo identities. In *BIOSIG 2008: Biometrics and Electronic Signatures* (2008).

[10] BROMBA, M. On the reconstruction of biometric raw data from template data. *Bromba Biometrics* (2006).

[11] CAVOUKIAN, A., AND STOIANOV, A. Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy. Tech. rep., Information and Privacy Commissioner/Ontario, March 2007.

[12] CHANG, K., BOWYER, K., AND FLYNN., P. Face recognition using 2d and 3d facial data. *In IEEE International Workshop on Analysis and Modeling of Faces and Gestures, Nice, France.* (2003).

[13] HAMMOND, P., HUTTON, T. J., ALLANSON, J. E., CAMPBELL, L. E., HENNEKAM, R. C., HOLDEN, S., MURPHY, K. C., PATTON, M. A., SHAW, A., TEMPLE, K., TROTTER, M., AND WINTER, R. M. 3d analysis of facial morphology. *American Journal of Medical Genetics Part A*, 126(4) (2004), 339–348.

[14] HESELTINE, T., PEARS, N., AND AUSTIN, J. Three-dimensional face recognition: A fishersurface approach. Springer Belin / Heidelberg.

[15] HILL, C. J. Risk of masquerade arising from the storage of biometrics. Master's thesis, The Department of Computer Science, Australian National University, November 2001.

[16] JIN, A. T. B., LING, D. N. C., AND GOH, A. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition Issue 11 37* (November 2004), 2245–2255.

[17] JUELS, A., AND M.SUDAN. A fuzzy vault scheme. In *IEEE International Symposium on Information Theory* (2002).

[18] JUELS, A., AND WATTENBERG, M. A fuzzy commitment scheme. In *6th ACM Conference on Computer and Communications Security* (1999), pp. 28–36.

[19] LINNARTZ, J. P., AND TUYLS, P. New shielding functions to enhance privacy and prevent misuse of biometric templates. In *4th international conference on audio- and video-based biometric person authentication* (2003).

[20] MATSUMOTO, T., MATSUMOTO, H., YAMADA, K., AND HOSHINO, S. Impact of artificial "gummy" fingers on fingerprint systems. In *Optical Security and Counterfeit Deterrence Techniques IV* (2002), vol. SPIE Vol. 4677, pp. 275–289.

[21] MONROSE, F., REITER, M. K., LI, Q., LOPRESTI, D. P., AND SHIH, C. Toward speech-generated cryptographic keys on resource constrained devices. In *in Proc. 11th USENIX Security Symp* (2002), p. 283ñ296.

[22] MONROSE, F., REITER, M. K., AND WETZE, S. Password hardening based on keystroke dynamics. In *International Journal on Information Security, Springer* (2002), vol. 1, pp. 69–83.

[23] PAN, G., WU, Y., WU, Z., AND LIU, W. 3D face recognition by profile and surface matching. In *Proc. International Joint Conference on Neural Networks* (Portland, Oregon, 2003), pp. 2168–2174.

[24] PAN, G., AND WU, Z. Automatic 3d face verification from range data. In *ICASSP* (2003), pp. 193–196.

[25] PHILLIPS, P. J., FLYNN, P. J., SCRUGGS, T., BOWYER, K. W., CHANG, J., HOFFMAN, K., MARQUES, J., MIN, J., AND WOREK, W. Overview of the face recognition grand challenge. In *In IEEE CVPR* (http://face.nist.gov/frgc/, June 2005), vol. 2, pp. 454–461.

[26] RATHA, N., CONNELL, J., AND BOLLE, R. Enhancing security and privacy of biometric-based authentication systems. *IBM Systems Journal 40*, 3 (2001), 614–634.

[27] RATHA, N. K., CHIKKERUR, S., CONNELL, J. H., AND BOLLE, R. M. Generating cancelable fingerprint templates. In *IEEE Transactions on Pattern Analysis and Machine Intelligence* (April 2007), vol. 29.

[28] ROBERGE, C. S. D., STOIANOV, A., GILROY, R., AND KUMAR, B. V. Biometric encryption. *ICSA Guide to Cryptography, Chapter 2* (1999).

[29] SCIENCE, R. M. 3d face scans spot gene syndromes. *BBC News* (September 2007), http://news.bbc.co.uk/2/hi/science/nature/6982030.stm.

[30] SEIDEL, J. Zusatzinformationen in fingerbildern. Master's thesis, Hochschule Darmstadt, 2006.

[31] SOUTAR, C. Biometric system security. In *Information Technology Security Symposium* (2002).

[32] TUYLS, P., AND GOSELING, J. Capacity and examples of template protecting biometric authentication systems. In *Biometric authentication workshop (BioAW 2004)* (Prague, 2004), LNCS, Ed., no. 3087, pp. 158–170.

[33] ULUDAG, U., AND JAIN, A. K. Attacks on biometric systems: a case study in fingerprints. In *SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents VI* (San Jose, CA, 2004), pp. 622–633.

[34] VAN DER VEEN, M., KEVENAAR, T., SCHRIJEN, G.-J., AKKERMANS, T. H., AND ZUO, F. Face biometrics with renewable templates. In *Security, Steganography, and Watermarking of Multimedia Contents VIII* (San Jose, California, USA).

[35] ZHOU, X., SEIBERT, H., BUSCH, C., AND FUNK, W. A 3d face recognition algorithm using histogram-based features. In *Eurographics Workshop on 3D Object Retrieval* (Crete, Greece, 2008), pp. 65–71.

[36] ZHOU, X., WOLTHUSEN, S. D., BUSCH, C., AND KUIJPER, A. A security analysis of biometric template protection schemes. In *International Conference on Image Analysis and Recognition ICIAR 2009* (2009), L. 5627, Ed., pp. 29–38.

Face Recognition
Edited by Milos Oravec

ISBN 978-953-307-060-5
Hard cover, 404 pages
Publisher InTech
Published online 01, April, 2010
Published in print edition April, 2010

This book aims to bring together selected recent advances, applications and original results in the area of biometric face recognition. They can be useful for researchers, engineers, graduate and postgraduate students, experts in this area and hopefully also for people interested generally in computer science, security, machine learning and artificial intelligence. Various methods, approaches and algorithms for recognition of human faces are used by authors of the chapters of this book, e.g. PCA, LDA, artificial neural networks, wavelets, curvelets, kernel methods, Gabor filters, active appearance models, 2D and 3D representations, optical correlation, hidden Markov models and others. Also a broad range of problems is covered: feature extraction and dimensionality reduction (chapters 1-4), 2D face recognition from the point of view of full system proposal (chapters 5-10), illumination and pose problems (chapters 11-13), eye movement (chapter 14), 3D face recognition (chapters 15-19) and hardware issues (chapters 19-20).

How to reference
In order to correctly reference this scholarly work, feel free to copy and paste the following:

Xuebing Zhou, Arjan Kuijper and Christoph Busch (2010). Template Protection For 3D Face Recognition, Face Recognition, Milos Oravec (Ed.), ISBN: 978-953-307-060-5, InTech, Available from: http://www.intechopen.com/books/face-recognition/template-protection-for-3d-face-recognition

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

© 2010 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike-3.0 License, which permits use, distribution and reproduction for non-commercial purposes, provided the original is properly cited and derivative works building on this content are distributed under the same license.