"3D Face": Biometric Template Protection for 3D Face Recognition

E.J.C. Kelkboom , B. Gökberk, T.A.M. Kevenaar, A.H.M. Akkermans, and M. van der Veen

Philips Research, High-Tech Campus 34, 5656AE, Eindhoven
{emile.kelkboom,berk.gokberk,tom.kevenaar,ton.h.akkermans, michiel.van.der.veen}@philips.com

Abstract. In this paper we apply template protection to an authentication system based on 3D face data in order to protect the privacy of its users. We use the template protection system based on the helper data system (HDS). The experimental results performed on the FRGC v2.0 database demonstrate that the performance of the protected system is of the same order as the performance of the unprotected system. The protected system has a performance of a FAR $\approx 0.19\%$ and a FRR $\approx$ 16% with a security level of 35 bits.

Keywords: Template protection, privacy protection, helper data system (HDS), 3D face recognition.

1 Introduction

Biometrics is used to recognize people for identification or verification purposes. It is expected that in the near future, biometrics will play an increasing role in many security applications. Today the market is dominated by fingerprint recognition, but for the near future market studies predict that face recognition technologies will also play an important role. This is driven by initiatives like the ePassport for which the ICAO standardized the face as being one of the modalities to be used for verification purposes. Following these trends, recently the European Project "3D Face"[1] was initiated. The principal goals of this project are to (i) improve the performance of classical face recognition techniques by extending it to 3D, (ii) integrate privacy protection technology to safeguard the biometric information and (iii) deploy the secure face recognition system at several international airports for the purpose of employee access control.

In this paper we concentrate on the privacy protection for 3D face recognition. In any biometric system, the storage of biometric information, also called biometric template, may be a privacy risk. To mitigate these risks, we see in recent literature different theoretical methods of privacy protection, e.g. *fuzzy commitment* [2], *fuzzy vault* [3], *cancelable biometrics* [4], *fuzzy extractors* [5], and the *helper data system* (HDS) [6,7]. The general goal of these systems is to (i) prevent *identity theft*, (ii) introduce *versatility*, and (iii) prevent *cross matching*. Also several attempts were made to integrate these techniques in practical systems for face [8] or fingerprint [9].

S.-W. Lee and S.Z. Li (Eds.): ICB 2007, LNCS 4642, pp. 566–573, 2007.

In our work we make use of the HDS template protection approach in the verification setting. We use a 3D face feature extraction algorithm that is based on the maximum and minimum principal curvature directions. The aim is to have at least the same verification performance in the protected case as in the unprotected case.

The remainder of the paper is organized as follows. In Section 2, we present a brief description of the feature extraction algorithm followed by the introduction of the HDS template protection system in Section 3. The results are given in Section 4 followed by the conclusions in Section 5.

2 3D Face Feature Extraction

In this work, we use a shape-based 3D face recognizer [10]. It has two main steps: 1) the alignment of faces, and 2) the extraction of surface features from 3D facial data. In the alignment step, each face is registered to a generic face model (GFM) and the central facial region is cropped. The GFM is computed by averaging correctly aligned images from a training set. After the alignment step, we can assume that all faces are transformed in such a way that they best fit the GFM, and have the same position in the common coordinate system.

After alignment, the facial surface is divided into 174 local regions. For each region, the maximum and minimum principal curvature direction are computed. Each of the two directions is presented by the azimuthal and the polar angle in the spherical coordinate system. Combining all the regions leads to a feature vector with $174 \times 2 \times 2 = 696$ entries. For matching two feature vectors, the distance is computed using the L_1 or the L_2 norm.

3 The Template Protection System: Helper Data System

The helper data system (HDS) is shown in Figure 1. It consists of the training, enrollment and verification stages. The inputs to all stages are real-valued feature vectors defined as, $\boldsymbol{z} \in \Re^k$, $\boldsymbol{x} \in \Re^k$ and $\boldsymbol{y} \in \Re^k$, respectively (k is the number of components of the feature vector). The feature vectors are derived from the 3D face image by the feature extraction algorithm described in Section 2. In each stage, users may have multiple images and therefore multiple feature vectors, which are defined as

$$\begin{array}{l} (\boldsymbol{z}_{i,j})_t,\ i = 1, \ldots, N_T;\ \ j = 1, \ldots, M_{T_i};\ \ t = 1, \ldots, k, \\ (\boldsymbol{x}_{i,j})_t,\ i = 1, \ldots, N;\ \ \ j = 1, \ldots, M_{E_i};\ \ t = 1, \ldots, k, \\ (\boldsymbol{y}_{i,j})_t,\ i = 1, \ldots, N;\ \ \ j = 1, \ldots, M_{V_i};\ \ t = 1, \ldots, k, \end{array} \tag{1}$$

where N_T is the number of users in the training stage with user i having M_{T_i} images, and N is the number of users in the enrollment and verification stage with user i having M_{E_i} images in the enrollment and M_{V_i} images in the verification stage. The notation $(\boldsymbol{x}_{i,j})_t$ indicates the t-th component of vector $\boldsymbol{x}_{i,j}$.

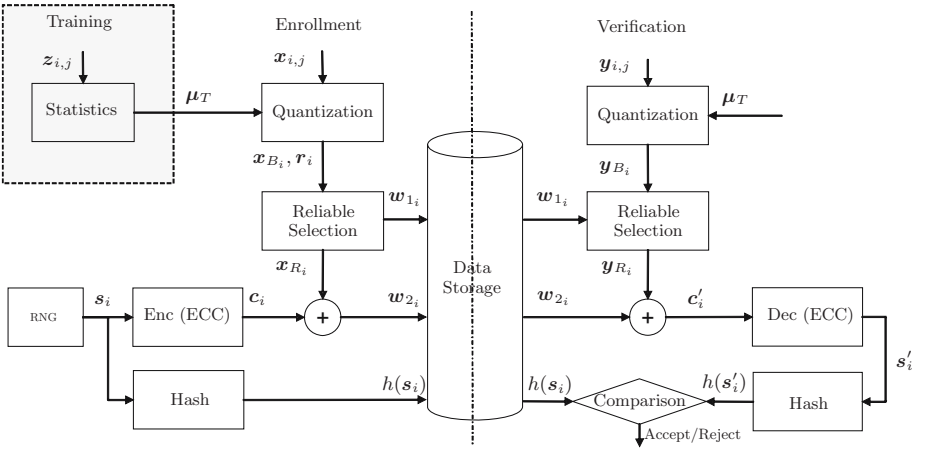

Fig. 1. The HDS template protection system; the enrollment (*left*), and verification stage (*right*). This figure is adapted from [8,9].

3.1 Training Stage

For template protection, binary feature vectors (binary strings) must be derived from the real-valued feature vectors. This is done by quantizing the feature vector with respect to a single threshold vector. In the training stage, this quantization threshold vector is calculated from the feature vectors of the training population $\boldsymbol{z}_{i,j}$. As threshold vector, we use the mean of the feature vectors defined as

$$\boldsymbol{\mu}_T = \frac{1}{\sum_{i=1}^{N_T} M_{T_i}} \sum_{i=1}^{N_T} \sum_{j=1}^{M_{T_i}} \boldsymbol{z}_{i,j}. \tag{2}$$

3.2 Enrollment Stage

In the enrollment stage, each user i has M_{E_i} feature vectors $\boldsymbol{x}_{i,j}$. In the *Quantization* block, the real-valued feature vectors are quantized into binary feature vectors $\boldsymbol{x}_{B_i}$ using the following equation

$$(\boldsymbol{x}_{B_i})_t = \begin{cases} 0, & \text{if } (\boldsymbol{\mu}_i)_t < (\boldsymbol{\mu}_T)_t \\ 1, & \text{if } (\boldsymbol{\mu}_i)_t \geq (\boldsymbol{\mu}_T)_t \end{cases}, \text{with } (\boldsymbol{\mu}_i)_t = \frac{1}{M_{E_i}} \sum_{j=1}^{M_{E_i}} (\boldsymbol{x}_{i,j})_t, \tag{3}$$

such that $(\boldsymbol{\mu}_i)_t$ is the mean of component t of the feature vectors of user i. The reliability $(\boldsymbol{r}_i)_t$ of each component $(\boldsymbol{x}_{B_i})_t$ is calculated as the ratio

$$(\boldsymbol{r}_i)_t = \frac{|(\boldsymbol{\mu}_T)_t - (\boldsymbol{\mu}_i)_t|}{(\sigma_i)_t}, \text{with } (\sigma_i)_t = \sqrt{\frac{1}{M_{E_i} - 1} \sum_{j=1}^{M_{E_i}} ((\boldsymbol{x}_{i,j})_t - (\boldsymbol{\mu}_i)_t)^2} \tag{4}$$

such that $(\sigma_i)_t$ is the standard deviation of component t of the feature vectors of user i. In the single image enrollment scenario, $M_{E_i} = 1$, we define $(\sigma_i)_t = 1$.

Also, a secret $\boldsymbol{s}_i$ of L_S bits is randomly generated by the *Random Number Generator* (*RNG*) block. The security level of the system is higher at larger secret lengths L_S. A codeword $\boldsymbol{c}_i$ of an error correcting code with L_C bits is obtained by encoding $\boldsymbol{s}_i$ in the *ENC* block. In our case we use the "Bose, Ray-Chaudhuri, Hocquenghem" (BCH) Error Correction Code (ECC) [11]. For the BCH code, the codeword length is equal to $L_C = 2^n - 1$, where n is a natural number. The most common codeword lengths for our application are 127, 255, and 511 bits and can be freely chosen as long as it is smaller than or equal to the feature vector length k. Examples of some BCH parameter combinations are given in Table 1. In the *Reliable Component* block, the reliable binary string $\boldsymbol{x}_{R_i}$ is created by cropping the binary feature vector $\boldsymbol{x}_{B_i}$ to the same length as the codeword by selecting the L_C components having the largest reliability $(\boldsymbol{r}_i)_t$. The indices of the L_C most reliable components are collected in the public helper data $\boldsymbol{w}_{1_i}$. Hereafter, the reliable binary feature vector $\boldsymbol{x}_{R_i}$ is bitwise XOR-ed with codeword $\boldsymbol{c}_i$. This XOR operation leads to the second helper data $\boldsymbol{w}_{2_i}$. The third and last helper data is the hashed value of secret $\boldsymbol{s}_i$, indicated as $h(\boldsymbol{s}_i)$. The cryptographic hash function can be considered as a one-way function which makes it computationally hard to retrieve the secret $\boldsymbol{s}_i$ from its hashed value $h(\boldsymbol{s}_i)$. The protected template corresponds to the three helper data denoted as: $[X]_i = \{h(\boldsymbol{s}_i), \boldsymbol{w}_{1_i}, \boldsymbol{w}_{2_i}\}$. The protected template can be considered as public and reveals only a minimum amount of information of $\boldsymbol{s}_i$ and $\boldsymbol{x}_{i,j}$. Therefore it can be easily stored on a less secure local data storage device or on a centralized database, depicted here as the *Data Storage*.

Table 1. Some examples of BCH parameter combinations

Codeword (L_C)	Secret (L_S)	Correctable bits (η)	BER $= \eta/L_C$
127	36	15	11.8%
	64	10	7.9%
255	37	45	17.7%
	63	30	11.8%
511	31	109	21.3%
	67	87	17.0%

3.3 Verification Stage

In the verification stage, a single feature vector $\boldsymbol{y}_{i,j}$ is used. As in classical biometric systems, this feature vector is compared to the reference data stored in the system. In the current setup, $\boldsymbol{y}_{i,j}$ is compared to the protected template $[X]_i$ derived in the enrollment stage using a dedicated matching method as follows. In the *Quantization block*, the binary feature vector $\boldsymbol{y}_{B_i}$ is obtained by quantizing $\boldsymbol{y}_{i,j}$ using Eq. 3, where $(\boldsymbol{\mu}_i)_t$ is replaced by $(\boldsymbol{y}_{i,j})_t$. The same threshold $\boldsymbol{\mu}_T$ is used as in the enrollment stage. In the *Reliable Component* block, the helper data

$\boldsymbol{w}_{1_i}$ is used to select components in $\boldsymbol{y}_{B_i}$ to obtain $\boldsymbol{y}_{R_i}$. The recovered codeword $\boldsymbol{c}'_i$ is the output of the XOR operation between the helper data $\boldsymbol{w}_{2_i}$ and $\boldsymbol{y}_{R_i}$. Next, this codeword is decoded to recover the (candidate) secret $\boldsymbol{s}'_i$, which is hashed into $h(\boldsymbol{s}'_i)$. In the *Comparison* block, $h(\boldsymbol{s}'_i)$ is matched bitwise with $h(\boldsymbol{s}_i)$ as obtained from the protected template $[X]_i$. If the hashes are bitwise exact the user is accepted, otherwise rejected. We have a match only if the following is true

$$\begin{gathered} h(\boldsymbol{s}_i) = h(\boldsymbol{s}'_i) \text{ iff } \boldsymbol{s}_i = \boldsymbol{s}'_i \text{ iff} \\ ||\boldsymbol{c}_i \oplus \boldsymbol{c}'_i||_1 = ||(\boldsymbol{x}_{R_i} \oplus \boldsymbol{w}_{2_i}) \oplus (\boldsymbol{w}_{2_i} \oplus \boldsymbol{y}_{R_i})||_1 = ||\boldsymbol{x}_{R_i} \oplus \boldsymbol{y}_{R_i}||_1 \leq \eta \end{gathered} \tag{5}$$

where η is the number of bits the ECC can correct and $||\boldsymbol{x}_{R_i} \oplus \boldsymbol{y}_{R_i}||_1$ is the hamming distance (HD) between $\boldsymbol{x}_{R_i}$ and $\boldsymbol{y}_{R_i}$. This means that the number of bit differences between $\boldsymbol{x}_{R_i}$ and $\boldsymbol{y}_{R_i}$ should be equal or less than η for a match.

4 Verification Performance Results

To analyze the verification performance of the system, we use the FRGC v2.0 database [12], which has 465 subjects having between 1 or 22 3D face images with a total of 4007 images. The 1st version, FRGC v1.0, is used to derive the GFM in the feature extraction algorithm. When applying our feature extraction algorithm to the FRGC images, we obtain feature vectors with $k = 696$ (see Section 2). Our verification performance test is complex, because the template protection system uses multiple enrollment images. The test protocol we use is elaborated next followed by the verification performance results.

4.1 Test Protocol

We first divide the FRGC v2.0 database into a training and a test set. The training set is used to obtain the quantization threshold $\boldsymbol{\mu}_T$, while the test set is used to analyze the verification performance. The optimal number of enrollment images, N_{enrol}, is not known and has to be verified. Its range is set to [1, 10], and two images of each subject are used in the verification stage. In the FRGC v2.0 database, subjects have varying numbers of 3D face images. In order to have the same subjects in each test, only the subjects having at least 12 images are selected for the test set, while the rest is used as the training set. This results into a test set containing 145 subjects with a total of 2347 images. For each N_{enrol} and codeword length {127, 255, 511} case, 20 verification runs are performed. Each run consists of randomly selecting $(N_{enrol} + 2)$ images of each subject and performing experiments for the $\binom{N_{enrol}+2}{N_{enrol}}$ possible combination of dividing the selected images into N_{enrol} enrollment images and two verification images. The results are averaged over all combinations and runs.

We evaluate the verification performance for both the protected and the unprotected case. For the template protection system, we evaluate its performance by studying the reliable binary feature vectors $\boldsymbol{x}_{R_i}$ and $\boldsymbol{y}_{R_i}$ and assuming a hamming distance classifier given as

$$HD = ||\boldsymbol{x}_{R_i} \oplus \boldsymbol{y}_{R_i}||_1. \tag{6}$$

The verification performance test is performed for feature lengths of 127, 255, and 511 bits, corresponding to possible codeword lengths of the ECC code. We also look at the verification performance of the full binary feature vectors $\boldsymbol{x}_{B_i}$ and $\boldsymbol{y}_{B_i}$, indicated as the "696" bits case. For the unprotected case, we use the real-valued feature vectors $\boldsymbol{x}_{i,j}$ and $\boldsymbol{y}_{i,j}$ and the L_1 and the L_2 norm as distance measure.

4.2 Performance Results: Protected and Unprotected Templates

Figure 2(a) shows the Equal Error Rate (EER) at different choices of N_{enrol}. It is clear that N_{enrol} has influence on the performance and we observe that at 7 or more images the performance stabilizes. For the real-valued (unprotected) case the EER is around 7.2%, while for binary (protected) case the EER is between 3-4%. This shows that in this case our binarization method itself leads to a significant performance improvement. We assume that the performance gain is achieved due to the filtering property of the binarization method on the real-valued feature vectors. The influence of N_{enrol} on the False Acceptance Rate

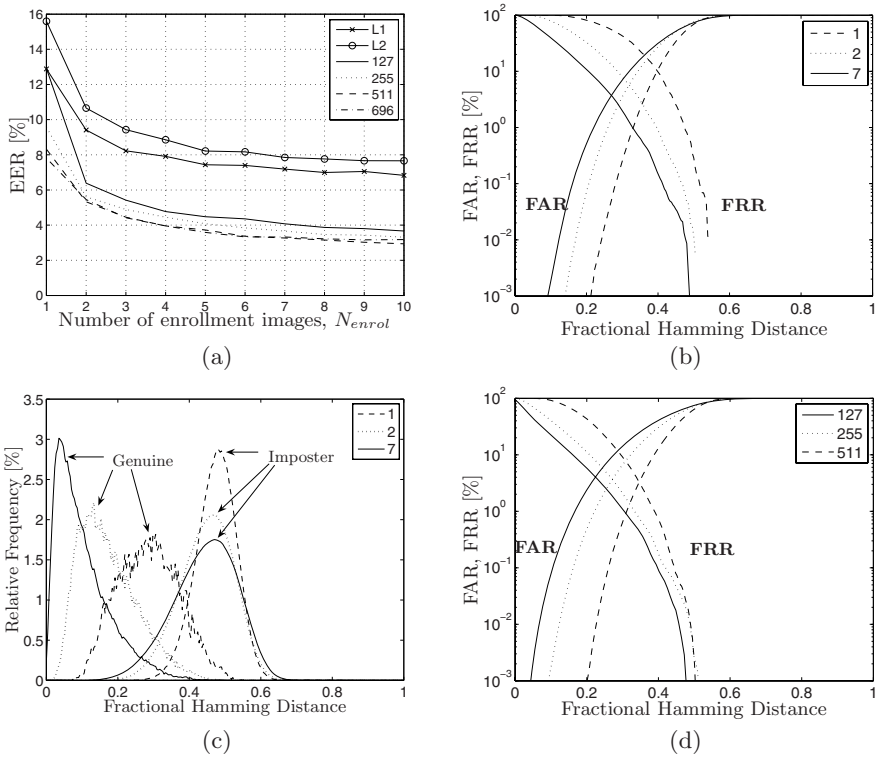

Fig. 2. At different N_{enrol} values (a) shows the EER for each case, (b) the FAR and FRR curves for the 255 bits case, and (c) gives the genuine and imposter distribution. For different codeword lengths, (d) gives the FAR and FRR curves.

Table 2. Verification performance for the protected (reliable binary feature vectors) and unprotected (real-valued and full binary feature vectors). N_{enrol} is set to 7.

Protected Templates				Unprotected Templates			
case	EER	FAR, FRR @ $L_S \approx 65$	FAR, FRR @ $L_S \approx 35$	case	EER	FRR @ FAR $\approx 0.25\%$	FAR @ FRR $\approx 2.5\%$
127	4.1	0.023%, 30.0%	0.18%, 17.7%	Binary "696"	3.3%	14.9%	4.7%
255	3.7	0.007%, 32.8%	0.19%, 15.6%	Real, L_1	7.2%	25.3%	25.2%
511	3.2	$\approx 0\%$, 58.5%	$\approx$0%, 36.8%	Real, L_2	7.8%	28.3%	27.5%

(FAR) and False Rejection Rate (FRR) curves is shown in Figures 2(b) for the 255 bits case and is representative for the other cases. It can be seen that with a larger N_{enrol}, both the EER and the corresponding threshold value, given as the Fractional Hamming Distance (FHD), decreases. FHD is defined as the hamming distance divided by the feature vector length. The EER threshold value also stabilizes at a N_{enrol} larger than 7.

The shift of the EER threshold can be explained with Figure 2(c). The genuine distribution shifts to a smaller FHD when N_{enrol} is increased. By increasing N_{enrol}, $(\sigma_i)_t$ and $(\boldsymbol{\mu}_i)_t$ can be better estimated and consequently the reliable components can be selected more accurately. A better selection of the most reliable components leads to a smaller FHD at genuine matches, as it is seen by the shift. On the other hand, when the most reliable components are selected, the imposter distribution curve also shifts to the left. However, the genuine distribution shift is greater than the imposter distribution, resulting in a EER at a smaller FHD.

The performance results for each case are given in Table 2, where N_{enrol} is set to 7. For the protected case it shows the EER, the FRR and FAR at the error correction capability of the ECC when $L_S \approx 65$ bits and $L_S \approx 35$ bits. For the unprotected case the EER, FRR at a FAR $\approx 0.25\%$, and FAR at a FRR $\approx$ 2.5% are shown. It can be seen that the binarization improves the performance in terms of EER. At a secret length of around 65 bits, codeword lengths 127 and 255 have the best performance, but the FRR is still high ($\approx$ 30%). At a smaller secret length of 35 bits, FRR decreases to $\approx$ 15% while maintaining a good FAR $\approx 0.20\%$. The smaller codewords have a better performance because the threshold corresponding to the EER point shifts to a smaller FHD (see Figure 2(d)). This decrease is larger than the decrease of the error correcting capabilities of the ECC due to smaller codeword lengths (see Table 1).

5 Conclusions

In this work, we successfully combined the HDS template protection system with a 3D face recognition system. The verification performance of the protected templates is of the same order as the performance of the unprotected, real-valued, templates. In order to achieve this improvement we proposed a special

binarization method, which uses multiple enrollment images. In a HDS template protection system, the choice of the operating point is limited by the number of bits the ECC can correct. Using multiple images and varying the number of binary features (corresponding to the codeword length of the ECC) the operating point can be brought closer to the EER point. We obtained the best verification performances at a codeword length of 255 bits with a FAR $\approx 0.19\%$ and a FRR $\approx 16\%$ at 35 bits of security. This is better than the FAR $= 0.25\%$ and FRR $\approx 26\%$ performance of the real-valued case.

It is expected that if the performance of the real-valued feature vectors is improved, it will further improve the performance of the protected templates. Furthermore, the verification performance of the protected templates can be enhanced with a more robust binarization algorithm. If the resulting binary templates are more robust, the EER will be achieved at a lower fractional Hamming distance. This will give the template protection system the flexibility to choose different operating points, leading to a more secure or a more convenient system.

References

1. 3DFace: (http://www.3dface.org/home/welcome)
2. Juels, A., Wattenberg, M.: A fuzzy commitment scheme. In: 6th ACM Conference on Computer and Communications Security, pp. 28–36. ACM Press, New York (1999)
3. Juels, A., Sudan, M.: A fuzzy vault scheme. In: Proc. of the 2002 International Symposium on Information Theory (ISIT 2002), Lausanne (2002)
4. Ratha, N.K., Connell, J.H., Bolle, R.M.: Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal 40, 614–634 (2001)
5. Dodis, Y., Reyzin, L., Smith, A.: Fuzzy extractors: How to generate strong secret keys from biometrics and other noisy data. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 532–540. Springer, Heidelberg (2004)
6. Verbitskiy, E., Tuyls, P., Denteneer, D., Linnartz, J.P.: Reliable biometric authentication with privacy protection. In: Proc. of the 24th Symp. on Inf. Theory in the Benelux, Veldhoven, The Netherlands, pp. 125–132 (2003)
7. Linnartz, J.-P., Tuyls, P.: New shielding functions to enhance privacy and prevent misuse of biometric templates. In: 4th Int. Conf. on AVBPA (2003)
8. Kevenaar, T.A.M., Schrijen, G.-J., Akkermans, A.H.M., van der Veen, M., Zou, F.: Face recognition with renewable and privacy preserving binary templates. In: 4th IEEE workshop on AutoID, Buffalo, New York, USA, pp. 21–26. IEEE Computer Society Press, Los Alamitos (2005)
9. Tuyls, P., Akkermans, A.H.M., Kevenaar, T.A.M., Schrijnen, G.J., Bazen, A.M., Veldhuis, R.N.J.: Pratical biometric authentication with template protection. In: 5th International Conference, AVBPA, Rye Brook, New York (2005)
10. Gökberk, B., Irfanoglu, M.O., Akarun, L.: 3D shape-based face representation and feature extraction for face recognition. Image and Vision Computing 24, 857–869 (2006)
11. Purser, M.: Introduction to Error-Correcting Codes. Artech House, Boston (1995)
12. Phillips, P.J., Flynn, P.J., Scruggs, T., Bowyer, K.W., Chang, J., Hoffman, K., Marques, J., Min, J., Worek, W.: Overview of the face recognition grand challenge. In: IEEE CVPR, vol. 2, pp. 454–461. IEEE Computer Society Press, Los Alamitos (2005)