Template Protection for PCA-LDA-based 3D Face Recognition Systems

Daniel Hartung

Email: hartung.dani@gmail.com

Abstract: Authentication based on biometrics became significantly important over the last years. Privacy and security concerns arise by the extensive deployment of biometrics. The used biometric features itself have to be secured. We propose a security mechanism that solves privacy related problems in 3D facial verification systems. Our solution combines PCA/LDA feature extraction with the Helper Data Scheme for template protection. The evaluation shows recognition rates at the same level for secured and unsecured templates, which leads to a win-win scenario for users and providers of the adapted systems.

1 Introduction

No matter how safely data is stored, attacks based on insider-information or security holes are difficult to avoid. For example, SecurityFocus reported in 2005 about the theft of 40 million mastercard accounts. Compromising biometric data does not yet mean a substantial loss of properties; however, biometric technology is an evolving field and consequently, this could become a severe problem in the future. For example, vein pattern recognition is already used in several Japanese financial institutions for verifying identity at ATMs. Moreover, biometric data can yield private and medical information and should therefore be deemed worthier to protect [JB00]. As a result, template protection systems for privacy-enhanced storage and usage of biometric data are being developed. Biometric features, the compact person-specific representation of biometric characteristics, are not saved directly, but are transformed into a secure reference. These systems approve new functionality which levels disadvantages of biometric authentication systems compared to classic password or token-based variants.
Revocation and renewability management is possible with template protection: if a template is compromised, the same biometric characteristic can be used again to construct a new secure template that can easily replace the old one. Another issue concerning privacy is handled when merging information gained from different databases: profiling is not possible if different templates were used in different contexts. These templates will be independent from each other, so cross-checks cannot succeed.
The advantages of biometric systems using template protection are strong, but there are still unsolved questions which have not yet been investigated for every biometric modality, for example: Is template protection feasible and what is the influence on the recognition rates? This paper describes how 3D face features can be combined with the Helper Data

Scheme (HDS) [Gos04, vdVKea06] for template protection. The features will be extracted using Principal Component Analysis (PCA) [TP92] in combination with Linear Discriminant Analysis (LDA) [BHK97]. Those feature extraction algorithms provide excellent recognition rates in 2D face recognition systems. Using 3D data instead requires various adaptions, but recognition rates are not dependent on light or pose variations anymore, also liveness detection is easier, overcoming the systems gets more elaborate. HDS uses standard cryptographic functions to secure the features. Therefore extracting enough stable bits out of the biometric data to cope with actual security-constraints, is one goal of this investigation. 3D face scans seem to offer the needed biometric entropy resulting in superb recognition rates [NIS08]. The next goal is to make sure that template protection does not substantially affect the recognition performance.

The paper shows how to merge HDS with the prepared 3D data to build a biometric verification system that gains additional benefits from the template protection system without suffering from lower recognition rates.

2 Template Protection

Much effort was spent on this topic of research since 1994. Dr. George Tamko, founder of Mytec Technologies Inc., invented a concept named Biometric Encryption for key revelation and securing fingerprint data [SRea99]. A non-exhaustive overview of existing systems is given in [SC07]. The concept of Cancelable Biometrics [RCB01] uses template protection as an alternative to watermarking techniques to authenticate the sensors responsible for capturing the biometric characteristic. Sensors perform a non-invertible deformation of the data to guarantee privacy of the biometric feature. Fuzzy Extractors [DRS04] are turning biometric information into cryptographic keys taking into account the noise in biometric data. Fuzzy Vault [JS06] is a scheme to protect unordered features like fingerprint minutiae data based on the complexity of polynomial reconstruction. Fuzzy Commitment Scheme [JW99] introduced shielding functions to secure biometric data. These functions add error correction to biometric data through mapping binarized biometric feature vectors into higher dimensional sets. All vectors pointing into a certain area are mapped exactly to one point. So even if the bit vector is distorted, it can be mapped to a certain bit vector.

Helper Data Scheme uses the principle of Fuzzy Commitment Scheme to protect biometric features. An overview is given in Figure 1. In the **enrolment phase** the users biometric characteristic M is captured. The biometric sample is the input of the HDS. The binarization unit transforms M – in order to be able to use standard cryptography functions – into a bit string of length m. The next block extracts the $n \leq m$ most reliable bits X by analyzing the templates statistics to ensure the robustness of the system. The positions R of these reliable bits are stored in the database. The vector containing the reliable bits (X) is merged with a random secret S – that is error encoded (C) for robustness reasons; C and X both having the same size. This conglomerate $W = X \oplus S$, which does not reveal any information about X is stored in the database together with a hash value of the secret ($h(S)$) and the index of the reliable bits (R).

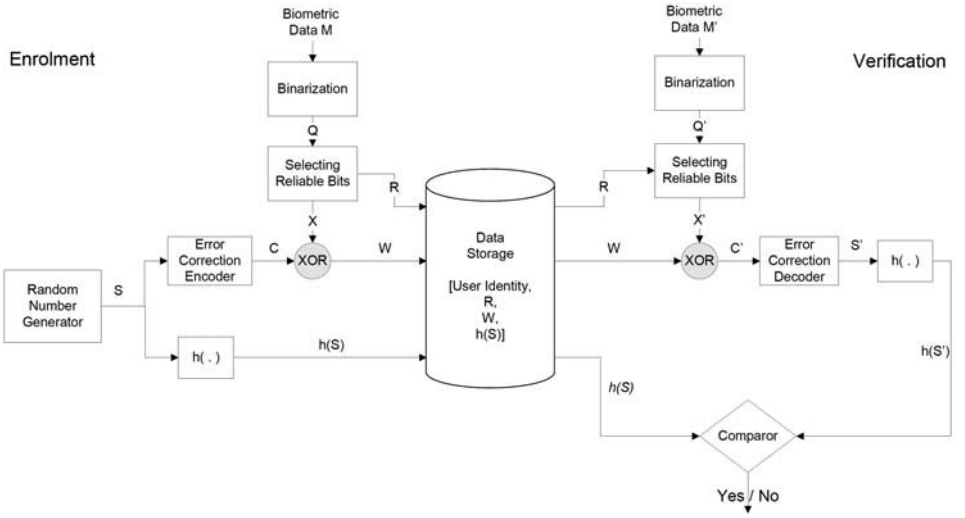

Figure 1: HDS overview [Zho07]

In the **verification phase** the noisy biometric data $M^{'}$ is binarized. After claiming the identity, the corresponding set of R, W and $h(S)$ is retrieved from the database. The bits at positions R of the binarized M' are extracted ($X^{'}$). The XOR-operation is applied to the $X^{'}$ and the stored $W(= X \oplus S)$. If X and $X^{'}$ match exactly the system verifies the user, as the stored and the calculated hash-value are the same $h(S) = h(S^{'}) = h(decode(C = W \oplus X))$. Usually the noise in biometric features forces the error decoding function to correct those bits differing in the reference and the noisy version of X. If C and $C^{'}$ differ not in more bits than the capability of the error correction system the hash-value of $S^{'}$ will match the stored $h(S)$. In this case – all errors could be corrected – the user is verified. This result is a simple binary decision. Equivalent to the length of the secret value S the security of the system will increase or decrease. A boundary is given only by the entropy of the biometric modality.

3 Combining HDS with PCA/LDA

The Helper Data Scheme supports improved privacy for the users in biometric systems and offers new functionality like revocation and renewability to the operator. HDS has one restriction: the used biometric features must provide the extraction of many reliable bits to use long secrets for high security applications. In order to achieve this goal, 3D facial depth data is used and features are extracted with well known gold standard algorithms for 2D face recognition (PCA/LDA). Two tactics are used: Improving the quality of the feature extraction system and the 3D samples as well as the extraction of many bits per component.

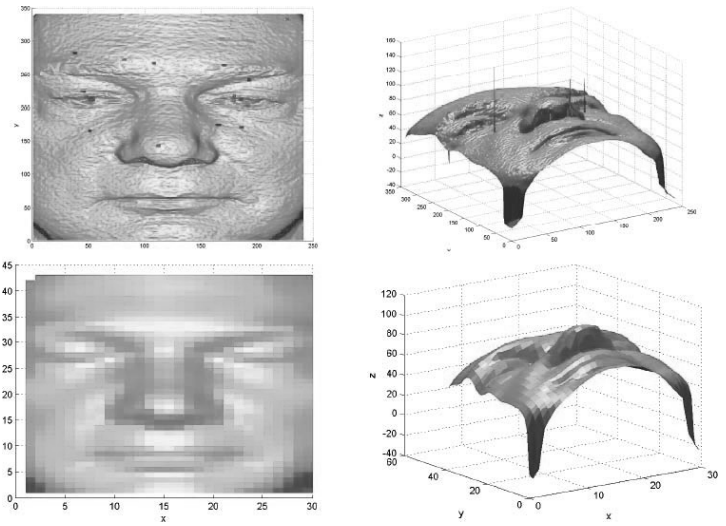

Figure 2: Shrinked 3D face scan

The preparation of the dataset has a major impact on the performance of the system. After gridding the data and normalizing the faces further processing is needed. Not defined points must be eliminated to extract the features. In order to achieve this, all samples are analyzed and a bit mask is created that defines a point valid or not. Also a soft decision is possible, a point is set as invalid if a certain threshold of samples contains not defined values. In this case not defined values need to be set to a certain value. The next problem to cope with are spikes, local errors in the depth measurement (Figure 2 shows the impact of our algorithm). Different algorithms are tested for eliminating those spikes, we applied a solution that is a local pixel block based algorithm that computes the mean value of this pixel block considering only values not differing too much from its blocks' median. We chose pixel blocks from size 2x2 up to 6x6 – also unchanged data was taken into account. After this step the feature extraction is optimized.
PCA and LDA in combination offer an additional degree of freedom when choosing the level of dimension reduction. Nonetheless the reduction is good for the robustness of the features and the computational effort, the requirements of HDS has to be fulfilled. The selection of the training set also effects the results, especially because PCA/LDA and HDS need separate trainings – those sets can not be used for validation. As metric for the optimization the equal error rate was used. We evaluated standard PCA and PCA in combination with LDA, differing the training sets systematically from 2 scans per person up to 22.

The next step was to optimize the HDS. The binarization block was extended to enable multi bit extraction. Instead of creating one bit out of each real valued component the proposed algorithm is able to extract many of them to satisfy the requirements of HDS. The level of reliability of those bits is set as the ratio between intra- and inter class variation. The simple version of the algorithm calculates the median of every component of the

feature vectors from a given training set. The result is one threshold vector – having the same size as every feature vector – containing those median values. Feature vectors are binarized comparing each component to the related component of the threshold vector. If the value is greater or equal than the threshold it is mapped to 1, in the other case to 0. We proposed an algorithm that calculates not only the median values of each component but also their quantiles. So each real value can be compared against $2^n - 1$ quantiles resulting in n uniformly distributed bits per component (for $n \geq 1$).
The error correction of HDS offers potential for optimization – in this implementation BCH-codes [BRC60] are used. HDS uses a binary decision for the verification, the error correction block is the only possibility to manipulate the behavior of the overall system – high levels of robustness have to be leveled against high false match rates. Different configurations for BCH are tested, fixing the code word length and differing the encoded secret.
We also tested the impact of the recognition rates when using several 3D scans for the verification of one user. So if one of those samples could be verified with the HDS, the user was verified.

After pointing out the parts of the system that are essential to our solution we want to discuss the results briefly.

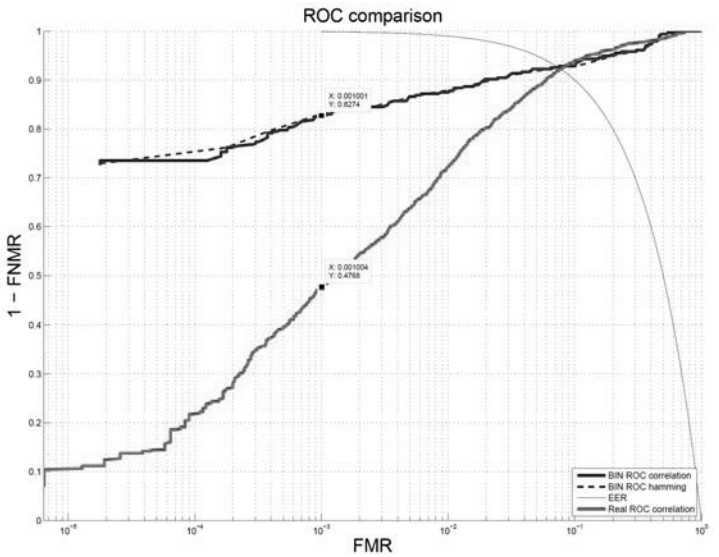

Figure 3: ROC of binarized / real valued features

4 Results

More than 4.000 recordings from the FRGC 2.0 database [PFS+05] could be used for optimization and evaluation.
Best results – at an operation point of 6.6% – could be achieved with data reduced to a resolution of 43 $\times$ 30 pixels. PCA/LDA parameters are set to a dimension reduction of 512/256 components. The performance between standard features and the binarised versions are at the same level (Figure 3 shows the receiver operation characteristics). The operation point using the different features is roughly the same. In the area of low false match rates (FMR), which is of interest for high security applications, the binarized features can even outperform their real valued equivalent: the false non match rate (FNMR) is substentially lower (52% vs. 17% FNMR @ 0.1% FMR). When using the HDS indeed only small secret sizes are appropriate to correct the bit errors that occur in the used biometric face data (Table 1). Taking into account three samples of one user for validation improves the results to a false match rate between 0.69 and 6.25% depending on the length of the used secret without any measurable false match rate. Extracting many bits out of the features was indeed not successful – recognition rates decreased in all configurations, the number of reliable bits could not be raised in this way. Anyway 3D facial biometric data can be secured against various kinds of attacks without decreasing the recognition performance.

Codeword length (in bits)	255	255	255	255	255
Secret length (in bits)	29	63	71	79	87
Correctable BER(in %)	18.4	11.8	11.4	10.6	10.2
FNMR(in %)	13.66	25.93	26.16	28.47	28.70
$FNMR_3$(in %)	0.69	2.08	3.47	4.17	6.25
FMR (in %)	0	0	0	0	0

Table 1: Performance results for codewords of 255 bits length

5 Conclusions

In this paper we combined and optimized various algorithms for securing 3D facial data. With our approach, biometric data is stored securely after the enrolment of the user and can be used as good as unsecured biometric features for verification. Evaluation shows that both secured and unsecured biometric data provide the same recognition rates. Using secured biometric information additionally enables the revocation of lost or compromised biometric templates, it also increases the acceptance of the user and helps the providers to manage their biometric systems.

Our work can be extended by multimodal biometrics and sensor data fusion techniques to overcome the limitations of small secrets. Also 3D video capturing devices could help providing many recordings in a short period of time to enhance the verification process.

References

[BHK97] Peter N. Belhumeur, João P. Hespanha, and David J. Kriegman. Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection. *IEEE Trans. Pattern Anal. Mach. Intell*, 19(7):711–720, 1997.

[BRC60] R. C. Bose and D. K. Ray-Chaudhuri. On A Class of Error Correcting Binary Group Codes. *Information and Control*, 3(1):68–79, March 1960.

[DRS04] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. In *Advances in Cryptology – EUROCRYPT ' 2004*, LNCS. Springer-Verlag, 2004.

[Gos04] P. Goseling, J. Tuyls. Information-theoretic approach to privacy protection of biometric templates. In *ISIT 2004. Proceedings. International Symposium on Information Theory*. Philips Research, Eindhoven, Netherlands, June 2004.

[JB00] M.D. James Bolling. A window to your health. *Jacksonville Medicine, Special issue: Retina diseases*, 51, September 2000.

[JS06] Ari Juels and Madhu Sudan. A Fuzzy Vault Scheme. *Des. Codes Cryptography*, 38(2):237–257, 2006.

[JW99] Ari Juels and Martin Wattenberg. A Fuzzy Commitment Scheme. In *ACM Conference on Computer and Communications Security*, pages 28–36, 1999.

[NIS08] NIST. FRVT 2006 and ICE 2006 Large Scale Results, 2006 National Institute of Standards and Technology, Gaithersburg, MD 20899, NISTIR 7408.

[PFS+05] P. Jonathon Phillips, Patrick J. Flynn, W. Todd Scruggs, Kevin W. Bowyer, Jin Chang, Kevin Hoffman, Joe Marques, Jaesik Min, and William J. Worek. Overview of the Face Recognition Grand Challenge. In *CVPR*, pages 947–954. IEEE Computer Society, 2005.

[RCB01] Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614–634, 2001.

[SC07] A. Stoianov and A. Cavoukian. Biometric Encryption: A positive-sum technology that achieves strong authentication, security and privacy. In *Office of the Information and Privacy Commissioner of Ontario*, March 2007.

[SRea99] C. Soutar, D. Roberge, and A. Stoianov et al. Biometric Encryption. In *ICSA - Guide to Cryptography*, chapter 22. McGraw-Hill, 1999.

[TP92] M. A. Turk and A. P. Pentland. Face Recognition Using Eigenfaces. In *Proceedings IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, pages 586–590, 1992.

[vdVKea06] M. van der Veen, T. Kevenaar, and G. Schrijen et al. Face biometrics with renewable templates. In *Security, Steganography, and Watermarking of Multimedia Contents VIII*, January 2006.

[Zho07] Xuebing Zhou. Template protection and its implementation in 3D face recognition systems. In *Conference Biometric Technology for Human Identification*, April 2007.