A Survey on Template Protection Scheme for Multimodal Biometric System

Praveer Tigga[1], **Akash Wanjari**[2]

Computer Science and Engineering (Information Security), DIMAT Raipur, India

Abstract: ***Multi-biometric systems are known to be universal and more accurate in biometric recognition. However, the storage of multiple biometric templates as separate entities pose major threats to user privacy and system security. The development of safe techniques in authentication systems is an important requirement in different fields of our modern interconnected society. Biometrics have long been used for various applications in the areas like access control to facilities and computers, criminal identification, border security, access to nuclear power plant, identity authentication in network environment, airport security, and issue of passports or driver licenses, forensic and medical databases. in now present time there is multimodal biometric is technique which is broadly used for the security in various area. There is various type attack present in biometric system. Many of the attack is applied on the template. In this paper we discuss about the various technique about template protection scheme and present a survey on the template protection scheme multimodal biometric system.***

Keywords: Cancellable biometrics, feature–level fusion, key generation discretisation, multimodal biometrics, template security.

1. Introduction

Biometrics has long been known as a robust approach for person authentication [1]. With new advances in technologies, biometrics has becoming emerging technology for authentication of individuals. Biometric system identifies or verifies a person based on his or her physiological characteristics such as fingerprint, face, palm print, iris etc or behavioral characteristics such as voice, writing style, and gait. Theoretically, any human physiological or behavioral characteristic can be used to make a personal identification as long as it satisfies features like universality, uniqueness, permanence and finally collectability. The biometric authentication system uses two kinds of approaches- Unimodal and Multimodal. Biometric systems used in real world applications are unimodal [2]. These unimodal biometric systems rely on the evidence of a single source of information for authentication of person. A unimodal biometric system has sensor module to capture the trait, feature extraction module to process the data to extract a feature set that yields compact representation of the trait, classifier module to compare the extracted feature set with reference database to generate matching scores and decision module to determine an identity or validate a claimed identity as shown in figure 1.

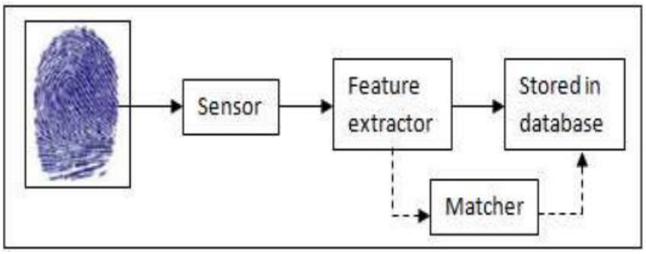

Figure 1: Unimodal biometric system

Though these unimodal biometric systems have many advantages, it has to face with variety problems like: Noise in sensed data, biometric data can be contaminated by noise due to imperfect acquisition conditions which may lead to false rejections. Non universality, meaningful data from a subset of individuals could not be acquired which results in failure to enroll error. Spoofing, behavioral traits are usually vulnerable to spoof attacks where an intruder mimics the trait corresponding to the enrolled subjects. Intra class variation, the biometric data acquired during verification will not be identical to the data used for generating template during enrollment for an individual. This is known as intra-class variation. Large intra-class variations increase the False Rejection Rate (FRR) of a biometric system. Interclass similarities, the overlap of feature spaces corresponding to multiple individuals. Large Inter-class similarities increase the False Acceptance Rate (FAR) of a biometric system. These problems were addressed by introducing multimodal biometric approach. It consolidates multiple sources of biometric information. This can be accomplished by fusing. Fusion can be done at different levels. The various levels of fusion in multimodal biometric are described in figure 2. A decision made by a multimodal biometric system is either a “genuine individual" type of decision or an “imposter" type of decision.

Sensor level fusion, this fusion refers to the consolidation of raw data obtained using multiple sensors or multiple snapshots of biometric using a single sensor. Feature level fusion, this fusion refers to the consolidation of features sets from different biometric traits into single feature set of features. Score level fusion, in this level of fusion, the match scores output by multiple matchers are combined to generate a new match score that can be subsequently used by verification or identification modules for rendering an identity decision. Decision level fusion, this fusion combines multiple decisions.

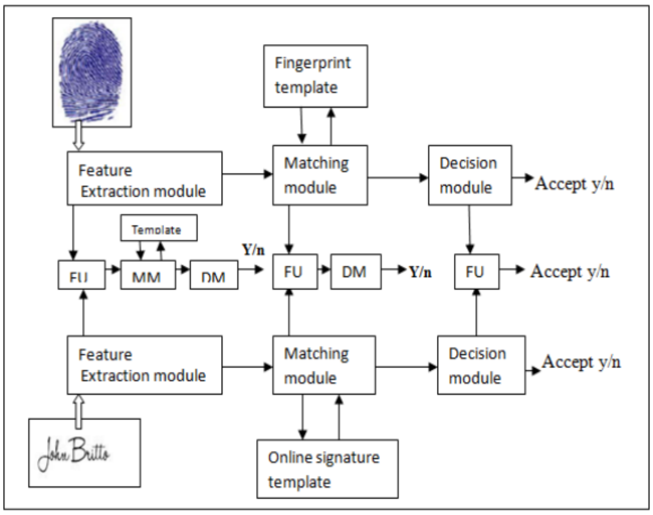

Figure 2: Multimodal biometric system.

Based on nature of these sources, a multi-biometric system can be broadly classified into one of the following six categories:

a. Multi-sensor systems
b. Multi-instance systems
c. Multi-algorithm systems:
d. Multi-sample systems
e. Multi-modal systems
f. Hybrid systems

2. Biometric Template Protection

The industry has long claimed that one of the primary benefits of biometric templates is that original biometric signals acquired to enrol a data subject cannot be reconstructed from stored templates. Several techniques (e.g. [8, 11]) have proven this claim wrong. Since most biometric characteristics are largely immutable, a compromise of raw biometric data or biometric templates might result in a situation that a subject's biometric characteristics are essentially burned and not usable any longer from the security perspective. Biometric template protection technologies offer significant advantages to enhance the privacy and security of biometric systems, providing reliable biometric authentication at a high security level. Traditional Encryption based methods like Advanced Encryption Standard(AES) or RSA cannot be applied to biometrics due to the intra-class variations in the biometric templates. The approaches for biometric template protection Methods can be classified as hardware based approach and software based approach. Hardware based approach include the usage of smartcards or standalone biometric system-on-devices. Such systems are called match-on-card or system-on-card technology. The main advantage of this solution is that the biometric information does not leak from the card. However, this solution is not suitable for the following reasons;

Not appropriate for large-scale applications

- They are expensive
- Users must carry the card with them all the time
- It is possible that the template can be gleaned from a stolen card

Therefore, even in hardware based solution like match-on-card, protecting biometric template is very crucial.

Approach	What imparts security to the template?	What entities are stored?	How are intra-user variations handled?
Salting	Secrecy of key K	Public domain: Transformed template $F(T;K)$ Secret: Key K	Quantization and matching in trans-formed domain $M(F(T;K),F(Q;K))$
Noninvertible transform	Non-invertibility of the transformation F	Public domain: Transformed template $F(T;K)$, Key K	Matching in transformed domain $M(F(T;K),F(Q;K))$
Key-binding biometric cryptosystem	Level of security depends on the amount of information revealed by the helper data H	Public domain: Helper Data $H = F(T;K)$	Error correction and user specific quantization $K = M(F(T;K),Q)$
Keygenerating biometric cryptosystem	Level of security depends on the amount of information revealed by the helper data H	Public domain: Helper Data $H = F(T)$	Error correction and user specific quantization $K = M(F(T),Q)$

3. Properties of Template Protection Methods

The following are the desirable characteristics of template protection schemes;

a) **Diversity:** To ensure privacy, secure template must not allow *crossmatching* or *function creep*.
b) **Revocability:** Compromised template should be revoked and it must be possible to reissue a new template from the same biometric data.
c) **Security:** It should not be possible to generate the original template from the secured template.
d) **Performance:** The operation of the protection scheme should not degrade the recognition performance (FAR and FRR) of the biometric system.

4. Classification of Biometric Template Protection Methods

Biometric template protection methods are broadly classified as:

1. Feature Transformation based methods
2. Biometric Cryptosystem based methods.

Feature transformation based methods are again categorized as salting based approach and non-invertible transformation based approach. Biometric Cryptosystem based methods are further classified as Key binding based method.

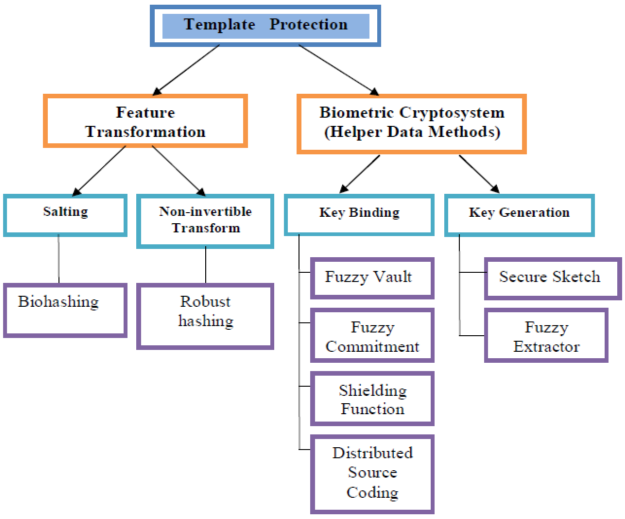

Figure 3: Categories of Template Protection Methods

5. Related Work

As it was mentioned above, the limited security of multimodal recognition systems, the drawbacks of biometric template protection technologies and the major absence of practicality to the recognition algorithms, involved in these creations, have motivated researchers to examine the possibilities for a fortunate combination of the two areas [2,37]. From an academic perspective, multi biometric template protection has several different facets [20]. At the same time, industrial actions attempt to establish a framework that can be effectively used to understand the issues and progress in the area while evaluating the needs of the applications [29,50]. At any rate, the relation between biometrics and protection techniques brings new challenges and illustrates efforts for further scenarios which can promise better overall accuracy of the system [19,32]. Literature survey has revealed a number of experimental works or approaches that are focused on the most frequently used biometrics (iris, fingerprint, face pattern) and aim at reducing the errors and providing higher security [15,50]. This section, briefly, refers to the most notable architectures, according to current methods that aim to equip sensors used in environments, where the personal data constitute a sensitive element [2,14,39,40].

A. Multi biometric Template Protection

Current literature in biometric template protection, key approaches to cryptosystems or cancelable biometrics and multiple biometric templates from the same source have been examined. Early studies, which required an alignment of biometric templates, have demonstrated efficiency with specific combinations of personal data. Different techniques have been proposed to overcome the shortcomings of pre-alignment methods [9,45]. Some of the schemes have been applied to physiological or behavioral biometrics [46]. Respecting the necessity for use the most easily captured biometric features, from a pattern recognition aspect, biometrics have been selected to map bio hashing, block permutation, fuzzy vaults and commitments schemes [41,44]. As a second approach, the collaboration of template protection with multi biometrics can be achieved with several notable approaches that have been proposed and evaluated according to the ability to correct the error ratio. For example, multi-algorithm fusion at feature level, multi biometric cryptosystem fuzzy vault based on fingerprint and iris [51], fuzzy commitments for face [49] and other ideas for score fusion level were successfully applied to fingerprints with security advances and many other combinations under various scenarios have been proposed during the last three years [23,51]. The target is to provide a uniform distribution of errors [30], combining successfully the data and covering research gaps of previous works, and thus, contributing to secure, stable systems [25,54], while offering, a fast comparison of protected templates suitable for biometric recognition in identification mode.

B. Ideas for Incorporation

Industrial projects are focused on the creation of a generic framework, similar to the one schematically presented below. The system should be capable of incorporating n templates, without the necessity to follow specific fusion levels for their representation, (k representations could be involved). The process is continued with a common representation and then the generic system is applied for the protection of the template (Fig. 2). Analyzing the idea from the levels aspect, focusing on the first part of this representation, it seems that biometrics fusion on feature level is the most suitable approach for the protection of the templates. Of course, score level fusion is not enough, besides the approaches of a solutions that offers to many systems. Nevertheless, cancelable biometric systems based on score level fusion can be reconstructed, in an analogous way to conventional, but their use to cryptosystems applications is not really popular [55]. Decisions based on final decisions can be successfully implemented to both system protection areas. Following the design of this framework, some issues arise, such as the template alignments, the way of the combination for modalities, the implementation in applications for the representation of the features [16], the level of the obtained recognition performance, the correction of the errors and the overall security of the system, and the way the latter comes to solve any privacy related themes [11].

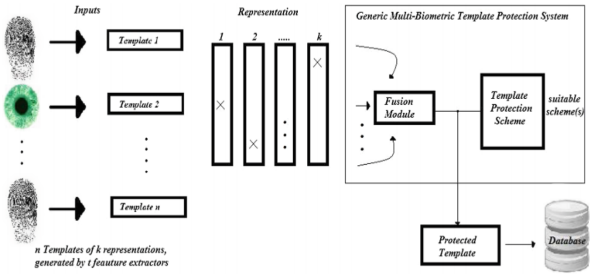
Inputs
Template 1
Template 2
Template n
n Templates of k representations, generated by t feauture extractors
Representation
1
2
.....
k
Generic Multi-Biometric Template Protection System
Fusion Module
Template Protection Scheme
suitable scheme(s)
Protected Template
Database

Figure 4: A framework of a generic multi biometric template protection at feature level.

More precisely, a construction of an align-invariant biometric cryptosystem or cancelable biometrics is not yet fully investigated. Feature level fusion of templates hinders a proper alignment of protected templates, while auxiliary data for the use of alignment may leak information on stored templates. Helper data techniques can probably provide some solution, but this is still unsure. The desired code length also remains evasive, and this comes to affect the necessity for error-correction codes. The fact that false rejection rates are lower bounded by error-correction capacities emerges as a great challenge since each change can make the system more vulnerable. The representation of the feature can bring better results but it may necessitate extended efforts in the direction of combination of many different templates using the fuzzy vault schemes methodology. Finally, from a biometric template protection perspective, the length of the keys remains a major topic for discussion. In conclusion, experiments that have been carried out in different studies with use of multiple combinations of biometric samples from the same identity and implemented in several template protection technologies, illustrate significant improvements with regards to reliability of the relevant applications. Different proposals of frameworks for the design of cryptosystems or cancelable biometrics that contain many modalities, have been presented enriching this research field. In spite of the encouraging results, several other issues might occur and demand further investigation [23]. Current literature studies are focused on the possibility to establish a generic model, which will cover the necessity for irreversibility and unlink ability, and secure enough to be used in many applications. The next section is dedicated to the emerging issues, from biometrics recognition to the protection categories, as those were presented above.

6. Conclusions and Discussion

In this work, we have presented a concrete approach on the protection of multimodal biometric templates, underlying critical privacy issues, while focusing on the suggestions for future research. Multimodal biometric systems are mostly discussed for the impact of their use on publicly accepted, reliable identification systems [31,53], overcoming the obstacles of uni-modal ones. Researchers propose different methods for combination of biometric traits, testing the possibilities that can induce to an effective fusion scheme for highly accurate recognition systems. During this study, there is an analysis of the three main fusion levels, in terms of theoretical [37] and recently published experimental knowledge [6,43]. The limitations of the single characteristic as a verification tool are revealed, while the vitality of multimodalities against fraudulent technologies is under examination. While biometric vendors are deploying multi biometric systems, at the same time concerns arise from the storage and misuse of the data [9]. The security of the templates is especially crucial for the confidentiality and integrity of this sensitive information. In the direction of facing a number of threats, works on the two main categories of biometric template protection schemes offer important advantages [19]. However, the significant number of studies on single biometric data [51] and the lack of security for multimodalities beyond their advantages, shift the organized and dedicated efforts to the connection of these areas. The incorporation of multiple biometrics in template protection schemes seems that can offer suggestions for solution against many drawbacks, while new security interrogations arise. During the last years, studies attempt to generate a compact generic framework and evaluate each proposed multimodal cryptosystem on large-scale datasets. In this line, there are still many open research questions, and the merit of biometric cryptosystems should ideally be expanded. The nature and privacy properties of a system, that can be used in a generalized multimodal way, are highly counter-intuitive and deserve a deeper exposition and evaluation of the ways that could significant to the problematic areas. Summarizing, the selection of the optimal fusion level and the choice for the appropriate modals as well as their combination present special interest, because they are the basic challenges in the requirements of each system according to the application design. After all, biometrics is the new digital enabler in a fast advancing technological world and their greatest strength is their uniqueness, which is also one of their greatest weakness. And if biometric elements are compromised during the verification process, the identity of the user is the primary concern. And it is at this point where cryptographic issues for multi biometrics need to be further investigated.

7. Acknowledgments

This research will contribute to FIDELITY (Fast and trustworthy Identity Delivery and check with e Passports leveraging Traveler privacy), project funded by the European Commission, under the Security theme of the Seventh Framework Programme (Grant agreement no: 284862). The authors would like to thank the reviewers for their ideas and support, regarding improvements for this survey.

References

[1] Abaza, A., Ross, A., Hebert, C., Harrison, M.A.F., Nixon, M.S.: A survey on ear biometrics. ACM Comput.Surv. 45(2), 22 (2013)

[2] Maiorana, E., Campisi, P., Fierrez, J., Ortega-Garcia, J., Neri, A.: Cancelable templates for sequence-based biometrics with application to on-line signature recognition. IEEE Trans. Syst. Man Cybern. Part A: Syst. Humans 40(3), 525–538 (2010)

[3] Adams, C.: Achieving non-transferability in credential systems using hidden biometrics. Secur.Commun.Netw. 4(2), 195–206 (2011)

[4] Dodis, Y., Ostrovsky, R., Reyzin, L., Smith, A.: Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. SIAM J. Comput. 38(1), 97–139 (2008)

[5] Nagar, A., Nandakumar, K., Jain, A.K.: Multibiometric cryptosystems based on feature-level fusion. IEEE Trans. Inf. Forensics Secur. 7(1), 255–268 (2012)

[6] Sim, H.M., Asmuni, H., Hassan, R., Othman, R.M.: Multimodal biometrics: weighted score level fusion based on non-ideal iris and face images. Expert Syst. Appl. 41(11), 5390–5404 (2014)

[7] Hao, F., Anderson, R., Daugman, J.: Combining crypto with biometrics effectively. IEEE Trans. Comput. 55(9), 1081–1088 (2006)

[8] Jain, A.K., Nandakumar, K., Nagar, A.: Biometric template security. EURASIP J. Adv. Signal Process. 2008, 113 (2008)

[9] Rathgeb, C., Busch, C.: Multi-biometric template protection: Issues and challenges. In: New Trends and Developments in Biometrics, pp. 173–190 (2012)

[10] ArgonesRua, E., Maiorana, E., Alba Castro, J.L., Campisi, P.: Biometric template protection using universal background models: an application to online signature. IEEE Trans. Inf. Forensics Secur. 7(1), 269–282 (2012)

[11] Isobe, Y., Ohki, T., Komatsu, N.: Security performance evaluation for biometric template protection techniques. Int. J. Biometrics 5(1), 53–72 (2013)

[12] Simoens, K.: Security and privacy challenges with biometric solutions. LSEC Biometrics (2011)

[13] Lu, L., Peng, J.: Finger multi-biometric cryptosystem using feature-level fusion (2014)

[14] Hoang, T., Choi, D.: Secure and privacy enhanced gait authentication on smart phone. Sci. World J. Article ID 438254, 8 p. (2014). doi:10.1155/2014/438254

[15] Peng, J., Li, Q., El-Latif, A.A.A., Niu, X.: Finger multibiometric cryptosystems: fusion strategy and template security. J. Electron. Imaging 23(2), 023001–023001 (2014) 16. Chin, Y., Ong, T., Teoh, A., Goh, K.: Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion. Inf. Fusion 18, 161–174 (2014)

[16] Maiorana, E.: Biometric cryptosystem using function based on-line signature recognition. Expert Syst. Appl. 37(4), 3454–3461 (2010)

[17] Bringer, J., Chabanne, H., Patey, A.: Privacy-preserving biometric identification using secure multiparty computation: an overview and recent trends. IEEE Sig. Process. Mag. 30(2), 42–52 (2013)

[18] Rathgeb, C., Uhl, A.: A survey on biometric cryptosystems and cancelable biometrics. EURASIP J. Inf. Secur. 2011(1), 1–25 (2011)

[19] Kumar Ramachandran Nair, S., Bhanu, B., Ghosh, S., Thakoor, N.S.: Predictive models for multibiometric systems. Pattern Recogn. 47(12), 3779–3792 (2014)

[20] Simoens, K., Bringer, J., Chabanne, H., Seys, S.: A framework for analyzing template security and privacy in biometric authentication systems. IEEE Trans. Inf. Forensics Secur. 7(2), 833–841 (2012)

[21] Cavoukian, A., Stoianov, A.: Privacy by design solutions for biometric one-tomany identification systems (2014)

[22] Rathgeb, C., Busch, C.: Cancelable multi-biometrics: mixing iris-codes based on adaptive bloom filters. Comput.Secur. 42, 1–12 (2014)

[23] Cavoukian, A., Stoianov, A.: Biometric encryption. In: van Tilborg, H.C.A., Jajodia, S. (eds.) Encyclopedia of Cryptography and Security, pp. 90–98. Springer, US (2011) 25.Sutcu, Y., Li, Q., Memon, N.: Secure sketches for protecting biometric templates. In: Campisi, P. (ed.) Security and Privacy in Biometrics, pp. 69–104. Springer, London (2013)

[24] Breebaart, J., Yang, B., Buhan-Dulman, I., Busch, C.: Biometric template protection. Datenschutz und Datensicherheit-DuD 33(5), 299–304 (2009)

[25] Tuyls, P., Akkermans, A.H.M., Kevenaar, T.A.M., Schrijen, G.-J., Bazen, A.M., Veldhuis, R.N.J.: Practical biometric authentication with template protection. In: Kanade, T., Jain, A., Ratha, N.K. (eds.) AVBPA 2005. LNCS, vol. 3546, pp. 436–446. Springer, Heidelberg (2005)

[26] Lee, D.G., Hussain, S., Roussos, G., Zhang, Y.: Editorial: special issue on security and multimodality in pervasive environments. Wireless Pers. Commun. 55(1), 1–4 (2010)

[27] Butt, M., Henniger, O., Nouak, A., Kuijper, A.: Privacy protection of biometric templates. In: Stephanidis, C. (ed.) HCI 2014, Part I. CCIS, vol. 434, pp. 153–158. Springer, Heidelberg (2014)

[28] Wang, N., Li, Q., Ahmed, A., El-Latif, Abd.,Peng, J., Yan, X., Niu, X.: A novel template protection scheme for multibiometrics based on fuzzy commitment and chaotic system. Sig. Image Video Process., 1–11 (2014). doi:10.1007/ s11760-014-0663-2

[29] Buchmann, N., Rathgeb, C., Baier, H., Busch, C.: Towards electronic identification and trusted services for biometric authenticated transactions in the single euro payments area. In: Preneel, B., Ikonomou, D. (eds.) APF 2014. LNCS, vol. 8450, pp. 172–190. Springer, Heidelberg (2014)

[30] Connaughton, R., Bowyer, K.W., Flynn, P.J.: Fusion of face and iris biometrics. In: Burge, M.J., Bowyer, K.W. (eds.) Handbook of Iris Recognition, pp. 219–237. Springer, London (2013)

[31] Awad, A.I., Hassanien, A.E.: Impact of some biometric modalities on forensic science. In: Muda, A.K., Choo, Y.-H., Abraham, A., Srihari, S.N. (eds.) Computational Intelligence in Digital Forensics: Forensic Investigationand Applications, pp. 47–62. Springer, Switzerland (2014)

[32] Campisi, P.: Security and Privacy in Biometrics. Springer, London (2013)

[33] Jillela, R.R., Ross, A.A., Boddeti, V.N., Kumar, B.V.K.V., Hu, X., Plemmons, R.J., Pauca, P.: Iris segmentation for challenging periocular images. In: Burge and Bowyer [11], pp. 281–308

[34] Burge, M.J., Bowyer, K.W. (eds.): Handbook of Iris Recognition. Advances in Computer Vision and Pattern Recognition. Springer, London (2013)

[35] Ross, A.A., Nandakumar, K., Jain, A.K.: Handbook of Multibiometrics, vol. 6. Springer, New York (2006)

[36] Kong, A., Zhang, D., Kamel, M.: Palmprint identification using feature-level fusion. Pattern Recogn. 39(3), 478–487 (2006)

[37] Wouters, K., Simoens, K., Lathouwers, D., Preneel, B.: Secure and privacy-friendly logging for egovernment services. In: Third International Conference on Availability, Reliability and Security, ARES 2008, pp. 1091–1096. IEEE (2008)

[38] Juels, A., Molnar, D., Wagner, D.: Security and privacy issues in e-passports. In: First International Conference on Security and Privacy for Emerging Areas in Communications Networks, SecureComm 2005, pp. 74–88. IEEE (2005)

[39] Techniques - Biometric Information Protection (2011).