A Survey on Multimodal Biometrics and the Protection of Their Templates

Christina-Angeliki Toli, Bart Preneel

A Survey on Multimodal Biometrics and the Protection of their Templates

Christina-Angeliki Toli and Bart Preneel

Department of Electrical Engineering
ESAT/COSIC - KU Leuven
Kasteelpark Arenberg 10, bus 2452, B-3001 Leuven-Heverlee, Belgium
{christina-angeliki.toli,bart.preneel}@esat.kuleuven.be
http://www.esat.kuleuven.be/cosic/

Abstract. In order to guarantee better user-friendliness and higher accuracy, beyond the existing traditional single-factor biometric systems, the multimodal ones appear to be more promising. Two or more biometric measurements for the same identity are extracted, stored and compared during the enrollment, authentication and identification processes. Deployed multimodal biometric systems also referred to as multibiometrics or even as multimodalities are commonly found and used in electronic chips, embedded in travel documents. The widespread use of such systems, the nature of the shared data and the importance of applications introduce privacy risks. A significant number of approaches and very recent advances to the relevant protection technologies have been published. This paper illustrates a comprehensive overview of research in multibiometrics, the protection of their templates and the privacy issues that arise. Up-to-date review of the existing literature revealing the current state-of-art suggestions is provided, based on the different levels of fusion and the employed protection algorithms, while an outlook to future prospects is also discussed.

Keywords: multimodal biometric systems, multibiometrics, multimodalities, levels of fusion, biometric template protection scheme, biometric cryptosystem, privacy, security, cryptography

1 Introduction

Biometric authentication is the science of establishing the identity of a user, towards a system, based on his/her physical or behavioral attributes [1]. During the last decade, the field of biometric authentication has gained growing popularity as biometric traits are becoming the next generation method that will widely replace the user name and password as the primary way of authentication, in the next 2-3 years. In addition to the idea that biometric characteristics are only useful in forensics, the pronounced necessity for reliable day-to-day transactions, has led to a range of applications that verify the identity of a person using human properties. Systems are increasingly being deployed and used throughout the world [53], from limited simple home or business applications (the controlled

access to a room), to large-scale projects, which are involved in societal functions, such as user verification for on-line transactions (e.g. banking ePayments, mobile devices). Finally, it is a common secret that biometrics have been used in the scope of surveillance themes. Remarkably, not only the industry, but also the military, law enforcement, and security agencies invest in the development and manufacture of facial, iris and voice recognition technologies, capable of detecting and identifying anyone.

Traditional deployments are mainly uni-modal biometric systems and may have limited usage. The fact is that no single sample from the modality biometric is sufficiently accurate in real-world applications [28], where it is demanded from designers to produce robust systems with low error rates and sufficient tamper proof protection [43]. Nevertheless, they constitute the starting point of each research into the direction of multibiometric systems which seeks to reduce some of their drawbacks [20], by consolidating recognition process using multiple templates extracted from the same person (e.g., fingerprint, iris, face, hand geometry, gait, keystroke dynamics) [36, 37].

A biometric system is essentially a pattern recognition scheme that compares the tested features of a user with the stored ones, from the process of a previous enrollment. Each system can operate in identification or verification mode, where the system processes a measurement from which a biometrics template is extracted [19]. The concept of fusion in biometrics, helps to expand the feature space used to claim an identity, and thus, affects the matching accuracy of the system [24]. Multibiometric recognition in different levels of fusion can improve the performance, deter spoofing, and increase the overall accuracy of these systems. Considering these enrichments, the system will be more reliable and thus, more acceptable to be used in a number of related applications [4], [28] [42].

Studies in these areas [5], [32], [37, 38], [45], aim to answer a crucial question: *How can the leakage of stored biometric characteristics, to unauthorized individuals, be prevented?* A variety of risks exist that call for protection of the stored elements, after the fusion of the templates. From a privacy viewpoint, most concerns against the common use of biometrics arise from the multiple modalities used to describe a single user, the sensitive nature of these data and the potential leakage of this information from devices that store it. Taking this into consideration, the security of the user's identity should be addressed, with a privacy perspective [21] and should be examined by different points of view. The elements that can reveal the identity of the user should be protected, while simultaneously, preventing him/her from opening multiple accounts using false data and covering the requirements for unique identifiers. Solutions such as the helper data system, fuzzy vault algorithms, cancelable biometrics and others come to promise improvements in this filed, while experimental studies have shown that these technologies can bring improved verification performance.

Multibiometric template protection is the source that has motivated numerous works in the field of the combination of pattern recognition methodologies with the world of cryptography. From research perspective, results about the significant advantages in accuracy, reliability and security of biometric systems

can promise protection of their storage. State-of-the-art proposals offer different scenarios to these concerns, while very recent experiments shift the target to the deployment of a unique generic category of systems [6], [52]. The idea behind this statement is that the systems development will be able to support many applications based on multiple pieces of evidence under one human identity, capable of performing well on large-scale datasets. They should be designed in such a smart way that can offer overall security, beyond well-known risks or the nature of the transactions.

This work is motivated by very recent advances in the areas of multibiometric recognition and biometric template protection, and its aim is to contribute to the studies of the interaction between biometrics and cryptography, presenting concrete, published results of the last four years. The time period of the works is carefully selected to serve the research in the entrance of biometrics in cryptography world, reflecting the increasing number of projects that aim to suggest solutions for the protection of user's identity, in case of risks during on-line transactions. These complementary security technologies can bring improvements in security and reliability of the systems, while strengthening public acceptance of the involved applications [7]. The remainder of this survey is organised as follows: In the next section, the importance of multimodalities against single modals is underlined, the different levels of fusion for multibiometric data are analysed, and template protection techniques are reviewed. Using this as the background of a new promising idea, the section of related work contains a comparative summary of multimodal biometrics and template protection in combination. The fourth section introduces the major privacy and security issues that arise. Finally, in the last section, a comprehensive conclusion, including the current approaches, is given and some remarks for discussion are presented.

2 Background

This section presents briefly the basic knowledge around the technology of biometric systems, starting from the way that these can be gathered, and suggesting the cryptographic methods that can be used for the protection of a biometric element in a database, in terms of security. The process, according to the application, the type of scenarios, the nature of the stored templates and their representation play an important role to the characterization of each system as a reliable and secure enough or not. The literature review in this area is extensive and it could not be fully addressed in this part. The target of the next subsections is to present the fusion of biometrics and the use of cryptographic techniques, introducing readers to enlightenment.

2.1 Multibiometric System Recognition

Data fusion in biometric systems is commonly an active area with numerous applications being not only a solution to the problems of uni-modalities, but also an active research field [3], [28]. Vendors are already deploying systems that

use two or three patterns for the same user, providing recognition even on large-scale datasets. Information fusion constitutes a way to enhance the matching accuracy of the system without resorting to other measurements or techniques, but just, being based only on the template.

Information Fusion. The three different factors of recognition performance of the gathered data are given in the following list.

Feature Level Fusion. The specific method comprises the strategies which pertain to the sensor, the set, rank and decision level. For the first one, in a concrete way, it is worth to be mentioned that this fusion level involves augmenting the vectors arising from the extractors and subjecting the vector to a transformation algorithm [35], [48]. The elements can enhance the performance.

Furthermore, information from multiple feature sets can be used to refine the template. Using the third category, a rank level fusion is suitable for biometric systems operating in the identification mode.

Finally, the last level fusion consists of artifacts coming from the final outputs of an individual sub-system, and wisely is mentioned as the simplest form of fusion. The correlation between the main inputs has to be examined, in order to evaluate the improvements in matching performance.

Score Level Fusion. On this level of fusion, matching scores are returned by each individual sub-system and the obtained output scores are combined. The suggested ways underline the necessity for a normalised score, aiming to improve the reliability of the system. There are three basic groups: density based, transformation based and classifier based schemes. The performance of each scheme depends on the quantity and the quality of the involved informative data. Major issues, like the limited number of the available training samples, or, the lack of homogeneity, can be further investigated, using the previously mentioned approaches [10].

To conclude, always considering that a multibiometric system is affected by the correlation [50], the combination of the weak uncorrelated biometric matchers can lead to better performance, than combining the strong ones, positively correlated. Using this starting point, score level becomes the most popular level among the others, and uncorrelated traits are applied in recognition systems, increasing, successfully, the desirable accuracy [40].

Decision Level Fusion. This level fusion is termed so because it depends on the final, acceptance or rejection, decisions. Auxiliary information is available to systems with high dependence from the application. Gathering the information by independent sub-systems, and fusing the results, constitutes a way to increase the overall precision, supporting the idea for universality of the entire system [13]. Mainly, the conducted research in this area is still immature. Fusion schemes that incorporate parts into a whole final scheme have not been yet explored [9]. Suggestions for combining soft biometric characteristics [48], like the

gender, age or the ethnicity of the user, with the inputs of biometric samples, can be used to verify the person's identity.

The presented themes provide an overview of the first tendency to the direction of covering the problematic areas of conventional biometric systems. The combination of popular traits, such as the iris and the fingerprints, is embedded in many applications. The conducted tests demonstrate advantages, while introducing new tasks. The evaluation of a complete biometric system is a complex issue and requires stronger user involvement for feature level schemes [31]. Compact multibiometric templates need to be generated, offering, in this way, an improved concrete content of information. Nevertheless, the most important drawback of fusion is the central storage of the data, coming from the same or different sources. This is a complex characteristic that should be addressed in order to prevent further privacy threats. Last, but not least, the precision of the model feature distributions, and the estimation of the possibilities to practice the theory in large databases, are still intricate issues [33].

2.2 Biometric Template Protection

Template Protection can be simply described as a straightforward and novel cryptographic construction. Biometrics can be found where personal information is employed to authenticate users, and here the readings are inherently noisy, not only because of their nature, but also, because of the pattern recognition techniques [14], [31]. However, such architectures have been used in a number of real-world, error-prone environments. Due to security concerns that arise from the storage of these data, several techniques [26] provide mechanisms, that can face the technical weaknesses of parameterization, representing a primitive with a special property of error-tolerance. The final aim is to improve the reliability of the systems and enlarge the chances for public acceptance and user confidence [17].

Categories Biometric characteristics are largely immutable and any kind of compromise is undesirable [1], [27]. The standard encryption algorithms do not support a comparison of biometric templates in an encrypted domain, leaving important personal information totally exposed, during the authentication. While user authentication is based on possession of secret keys, key management is performed introducing another layer of authentication. In this way, encryption of data inherits the security of according biometrics applied to release correct decrypting keys. Biometric template protection schemes are usually categorised in two main groups and are designed to meet the requirements of biometric data protection [48]. Schematic illustration is shown in Fig. 1.

Cancelable Biometrics also referred to as feature transformations are designed in a way, that it should be computationally difficult to recover the original information [37], [56]. The idea is to apply transformations that do not affect the

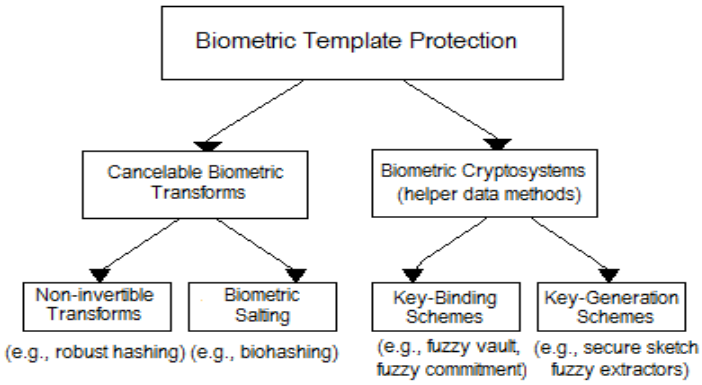

Fig. 1. Categorisation of Template Protection Schemes.

elements, while are tolerant to variations. The basic fact, in this category, is that cancelable biometrics consist of intentional distortions of signals that are repeatedly transformed, similarly to those between templates in the transformed domain.

Techniques of transformation modify the template in a user specific way. During authentication, the same transformation is applied to the biometric query, and the matching is performed in the already transformed area, so as to avoid the exposition of the original stored template [47].

A weak point of the system is that the transformation key is stored along with the biometric template. One solution for this can be the non-invertibility of the used transformation function, even in those cases, where the attacker knows the key. Furthermore, assuming beforehand that the transformed biometric data may be compromised, the parameters should be changed, in order to secure the template. Finally, to prevent the tracking subjects by cross-matching databases processes, recent studies have tested methods for applying different transformations for different applications [9], [33].

Cancelable biometrics are distinguished in two categories: non-invertible transforms and biometric salting. Academic research in this area consists of numerous works that can be further classified. It is worth mentioning that published works, in this area, apply the techniques of robust hashing systems and biohashing in specific modalities, studying the error rates, with remarkable results. These examinations also include analysis of the design from a constructional and security aspect, and evaluating the behavior of those schemes against potential attacks [35].

Biometric Cryptosystems are designed to securely bind a digital key to a biometric feature or generate a key from it. The idea, for a design of robust keys, started as a solution to threats like copying, sharing and distributing biometrics from the initial genuine storage. This is the reason for their second name, as

helper data methods. Based on schemes which perform fuzzy comparisons, using decision thresholds, original templates are replaced through biometric-dependent public information. Specifically, secure sketches are derived from the biometric template after the enrollment process. This sketch is stored in the system, instead of the original template, in a form of a function. This mixture is obtained by binding the template with an error-correcting code, which itself is defined by a key. The strength, in terms of security, is the absence of the user's data, which however is a drawback for this design. Security relies on the difficulty to recover the template, using as attacks an authentication query or an error-correcting code. Some examples of biometric cryptosystems are fuzzy vault schemes, fuzzy extractors, and secret sharing approaches, secure sketches and others. Typically, these are separated into two main categories according to the schemes, as key-binding or key-generation [17].

Both technologies aimed to meet some requirements like non-invertibility where, given a protected template, it should be difficult for the attacker to find a biometric feature set that will match with the initial one. Second, we need revocability where versions of protected templates can be generated from the same biometric data and, concurrently, the protected templates should not allow cross-matching process, obeying to the necessity for diversity of data representations [40]. The use of these techniques can offer advantages, taking into account the uses cases, a fact that is also underlined in some published works [13], [16], [21], [54], where different approaches and combinations can be presented. In general, comparing the two methods of protection, cryptosystems tending to have stronger non-invertibility transformation schemes also offer unlinkability. Separately, or using hybrid products of their connection, several traditional attacks against systems have been prevented and the generated template is usually strong enough to be reconstructed, which is a feature that increases privacy and, consequently, the social acceptance [38].

3 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, multibiometric 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].

3.1 Multibiometric 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 biohashing, block permutation, fuzzy vaults and commitments schemes [41], [44].

As a second approach, the collaboration of template protection with multibiometrics 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, multibiometric 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.

3.2 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.

Analysing 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

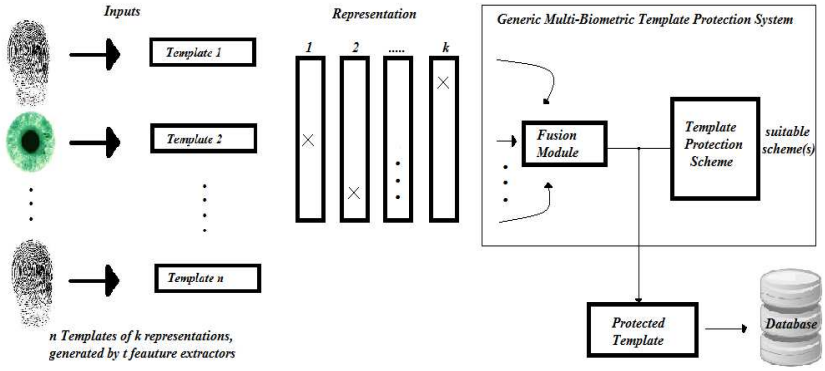

Fig. 2. A Framework of a Generic Multibiometric Template Protection at Feature Level.

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].

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 unlinkability, 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.

4 Security and Privacy Issues

A great number of biometric characteristics are being used in various applications. The nature of each biometric trait makes it eligible for a variety of applications. Beyond, the well-known, common seven factors that underline the suitability of the data, that is universality, uniqueness, permanence, measurability, performance, acceptability, circumvention [37], there are, also, other factors that should be taken into consideration, especially when biometric systems are deployed in real-world applications [22], [39, 40]. Computing environments present security challenges related to aspects of multimodality [28] while extending and facilitating the ways of accessing may cause security threats [7]. The system must, at the same time, behave according to a certain policy of biometrics and be properly instrumented against attacks and actions performed by non-expert users, in order to protect information, thus meeting the requirements of irreversibility and unlinkability.

After overcoming engineering and technical performance issues [6], the primary research question to be addressed with regards to a multibiometric system is: *How does the system address privacy concerns regarding its level of provided security to the relevant application?* A starting point is the idea that with improvements of security, privacy as well as systems reliability of two or more biometrics could be combined in a method that enhances the efficiency. Following this assumption, multibiometric systems not only can reduce some threats, but also can be compromised in many ways [18]. In that sense, the leakage of template information to unauthorized individuals becomes a serious theme. One should bear in mind, however, that the storage of multiple biometric records of a fused template of elements, extracted from different traits, under the same identity, may offer a solution to many risks, but still, this storage has to be protected [9].

Multibiometric Systems

A multibiometric system increases the degree of confidence while the accuracy, throughput and scalability could be well estimated. Approximately, using the proposed fusion levels for different biometric traits in unconstrained environments and after the experimental performance analysis, there is an ability to reduce the levels of noise [6], [48]. On the other hand, multimodalities overcome limitations such as error-correcting capability and non-universality and this is a field which requires improvements [12], [42].

Biometric Template Protection Technologies

Biometric template protection technologies present several advantages over generic biometric systems. In particular, attention is paid to immutability, because it is

the basic characteristic of biometrics. The schemes, as these are previously categorised using this point, enhance privacy providing reliable authentication at a significant level. Specifically, the original template is concealed, the reconstruction becomes extremely efficient [9], [42] and the methods ensure, in some sort, the revocability and renewability of the template. Published studies provide tests using traditional attacks against the systems and introduce not only the strong fundamental spots, but also, the obscured ones [21], [42], [49]. For biometric cryptosystems, the key entropy, the tolerance levels, during the processes, and the metrics are the quantities that lack further investigation [9], [19]. Then, the amount of the applicable parameters should be examined closely, considering their important role in the definition of a restricted key space, something that puts at risk the security of the methods which use cancelable biometrics. In conclusion, in order to avoid fraud, privacy leakage should be decreased and the major requirement of unlinkability must be met. Furthermore, the alignment affects the recognition performance, the absence of a unified architecture brings confusion across the applications [25] and the desired properties for error-correction codes remain unattained.

Combination of Cryptography and Multimodalities

It is an undeniable fact that the combination of cryptography and multibiometrics introduces a number of successful mechanisms that ensure information privacy. Some of the approaches presented in the previous paragraphs of this section may be adopted as solutions, but, still other situations will occur. Precisely, the alignment of the protected templates is an essential task [9], and the representation of feature vectors remains an important line of research. Experiments on protected biometric data [42] lead to the assumption that the low boundaries between the false rejection rates and the error-correction capacities compound a more vulnerable system and at the same time, the requirements for stable biometric features are, definitely, non-trivial. Some of the approaches show that the protocols in the literature do not secure the encoding procedures [25] while others provide multiple suggestions for the distribution of reliability, or concentrate the efforts to the improvement of recognition rates [34]. With respect to the different multimodal biometrics template protection schemes, the interesting side contains the concentrated trials for a generic framework, focused on unified representation of biometric features, under the combination of the suggested protection designs. Relevant to the mechanisms and for the improvement of security and privacy, the requirements, according to Biometric Template Protection Standardization ISO/IEC 24745 [58] need to be covered and clearly addressed, while the accuracy of each concept should be tested.

The last element in this list is some of the most popular introduced privacy methods and the security issues currently on debate. Beyond all the technical cases that arise from the use of multimodalities, when those are applied to template protection schemes, their fusion leads to a number of issues. While,

researchers suggest the use of multimodalities, other approaches [57] induce different findings and set the dilemma about the choice of the use of multimodal biometrics instead of uni-modal ones, in order to contribute to a protection of the user against undesired biometric checking. Some other open research questions from privacy aspect, which need to be further examined are: *Does the system exclude the threats that can arise, considering the possibility to perform the biometric procedure without notice and/or against the will of the user? How can the user protect himself/herself against undesired biometric checking?* One step further, the biometric databases, created to support a range of applications, the possibility of data correlation with health information [7, 8], [40], [49], and the security requirements for data, stored in ePassports or ID cards, cause a risky uncertainty. Also, the very nature of template protection schemes, introduce questions about their efficiency for on-line fast identifications, or situations that involve government applications, and these are some of the areas that need to be covered extensively.

5 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 multibiometric 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 organised 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 generalised multimodal

way, are highly counter-intuitive and deserve a deeper exposition and evaluation of the ways that could significant to the problematic areas.

Summarising, 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 multibiometrics need to be further investigated.

Acknowledgments. This research will contribute to FIDELITY (Fast and trustworthy Identity Delivery and check with ePassports 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] A. Abaza, A. Ross, C. Hebert, M. A. F. Harrison, and M. S. Nixon. A survey on ear biometrics. ACM Comput. Surv., 45(2):22, 2013.

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

[3] C. Adams. Achieving non-transferability in credential systems using hidden biometrics. Security and Communication Networks, 4(2):195-206, 2011.

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

[5] A. Nagar, K. Nandakumar, and A. K. Jain. Multibiometric cryptosystems based on feature-level fusion. Information Forensics and Security, IEEE Transactions on, 7(1):255-268, 2012.

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

[7] F. Hao, R. Anderson, and J. Daugman. Combining crypto with biometrics effectively. Computers, IEEE Transactions on, 55(9):1081-1088, 2006.

[8] A. K. Jain, K. Nandakumar, and A. Nagar. Biometric template security. EURASIP Journal on Advances in Signal Processing, 2008:113, 2008.

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

[10] E. Argones Rua, E. Maiorana, J. L. Alba Castro, and P. Campisi. Biometric template protection using universal background models: An application to online signature. Information Forensics and Security, IEEE Transactions on, 7(1):269-282, 2012.

[11] Y. Isobe, T. Ohki, and N. Komatsu. Security performance evaluation for biometric template protection techniques. International Journal of Biometrics, 5(1):53-72, 2013.
[12] K. Simoens. Security and privacy challenges with biometric solutions. LSEC Biometrics, 2011.
[13] L. Lu and J. Peng. Finger multi-biometric cryptosystem using feature-level fusion. 2014.
[14] T. Hoang and D. Choi. Secure and privacy enhanced gait authentication on smart phone. The Scientific World Journal, 2014, 2014.
[15] J. Peng, Q. Li, A. A. A. El-Latif, and X. Niu. Finger multibiometric cryptosystems: fusion strategy and template security. Journal of Electronic Imaging, 23(2):023001-023001, 2014.
[16] Y. Chin, T. Ong, A. Teoh, and K. Goh. Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion. Information Fusion, 18:161-174, 2014.
[17] E. Maiorana. Biometric cryptosystem using function based on-line signature recognition. Expert Systems with Applications, 37(4):3454-3461, 2010.
[18] J. Bringer, H. Chabanne, and A. Patey. Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends. Signal Processing Magazine, IEEE, 30(2):42-52, 2013.
[19] C. Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security, 2011(1):1-25, 2011.
[20] S. Kumar Ramachandran Nair, B. Bhanu, S. Ghosh, and N. S. Thakoor. Predictive models for multibiometric systems. Pattern Recognition, 2014.
[21] K. Simoens, J. Bringer, H. Chabanne, and S. Seys. A framework for analyzing template security and privacy in biometric authentication systems. Information Forensics and Security, IEEE Transactions on, 7(2):833-841, 2012.
[22] A. Cavoukian and A. Stoianov. Privacy by design solutions for biometric one-to-many identification systems. 2014.
[23] C. Rathgeb and C. Busch. Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters. Computers & Security, 42:1-12, 2014.
[24] A. Cavoukian and A. Stoianov. Biometric encryption. In Encyclopedia of Cryptography and Security, pages 90-98. Springer, 2011.
[25] Y. Sutcu, Q. Li, and N. Memon. Secure sketches for protecting biometric templates. In Security and Privacy in Biometrics, pages 69-104. Springer, 2013.
[26] J. Breebaart, B. Yang, I. Buhan-Dulman, and C. Busch. Biometric template protection. Datenschutz und Datensicherheit-DuD, 33(5):299-304, 2009.
[27] P. Tuyls, A. H. Akkermans, T. A. Kevenaar, G.-J. Schrijen, A. M. Bazen, and R. N. Veldhuis. Practical biometric authentication with template protection. In Audio-and Video-Based Biometric Person Authentication, pages 436-446. Springer, 2005.
[28] D. G. Lee, S. Hussain, G. Roussos, and Y. Zhang. Editorial: Special issue on security and multimodality in pervasive environments. Wireless personal communications, 55(1):1-4, 2010.
[29] M. Butt, O. Henniger, A. Nouak, and A. Kuijper. Privacy protection of biometric templates. In HCI International 2014-Posters' Extended Abstracts, pages 153-158. Springer, 2014.
[30] N. Wang, Q. Li, A. A. A. El-Latif, J. Peng, X. Yan, and X. Niu. A novel template protection scheme for multibiometrics based on fuzzy commitment and chaotic system. Signal, Image and Video Processing, pages 1-11, 2014.

[31] N. Buchmann, C. Rathgeb, H. Baier, and C. Busch. Towards electronic identification and trusted services for biometric authenticated transactions in the single euro payments area. In Privacy Technologies and Policy, pages 172-190. Springer, 2014.

[32] R. Connaughton, K. W. Bowyer, and P. J. Flynn. Fusion of face and iris biometrics. In Handbook of Iris Recognition, pages 219-237. Springer, 2013.

[33] A. I. Awad and A. E. Hassanien. Impact of some biometric modalities on forensic science. In Computational Intelligence in Digital Forensics: Forensic Investigation and Applications, pages 47-62. Springer, 2014.

[34] P. Campisi. Security and Privacy in Biometrics. Springer, 2013.

[35] R. R. Jillela, A. A. Ross, V. N. Boddeti, B. V. K. V. Kumar, X. Hu, R. J. Plemmons, and P. Pauca. Iris segmentation for challenging periocular images. In Burge andBowyer [11], pages 281-308.

[36] M. J. Burge and K. W. Bowyer, editors. Handbook of Iris Recognition. Advances in Computer Vision and Pattern Recognition. Springer, 2013.

[37] A. A. Ross, K. Nandakumar, and A. K. Jain. Handbook of multibiometrics, volume 6. Springer, 2006.

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

[39] K. Wouters, K. Simoens, D. Lathouwers, and B. Preneel. Secure and privacy-friendly logging for egovernment services. In Availability, Reliability and Security, 2008. ARES 08. Third International Conference on, pages 1091-1096. IEEE, 2008.

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

[41] E. J. Kelkboom, J. Breebaart, I. Buhan, and R. N. Veldhuis. Analytical template protection performance and maximum key size given a gaussian-modeled biometric source. In SPIE Defense, Security, and Sensing, pages 76670D-76670D. International Society for Optics and Photonics, 2010.

[42] C. Rathgeb, A. Uhl, and P. Wild. Reliability-balanced feature level fusion for fuzzy commitment scheme. In Biometrics (IJCB), 2011 International Joint Conference on, pages 1-7. IEEE, 2011.

[43] A. M. Siddiqui, R. Telgad, and P. D. Deshmukh. Multimodal biometric systems: Study to improve accuracy and performance. 2014.

[44] K. Nandakumar and A. K. Jain. Multibiometric template security using fuzzy vault. In Biometrics: Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on, pages 1-6. IEEE, 2008.

[45] E. Kelkboom, X. Zhou, J. Breebaart, R. Veldhuis, and C. Busch. Multi-algorithm fusion with template protection. In Biometrics: Theory, Applications, and Systems, 2009. BTAS'09. IEEE 3rd International Conference on, pages 1-8. IEEE, 2009.

[46] Y. Sutcu, Q. Li, and N. Memon. Secure biometric templates from fingerprint-face features. In Computer Vision and Pattern Recognition, 2007. CVPR'07. IEEE Conference on, pages 1-6. IEEE, 2007.

[47] K. Radhika, G. Sekhar, and M. Venkatesha. Pattern recognition techniques in online hand written signature verification-a survey. In Multimedia Computing and Systems, 2009. ICMCS'09. International Conference on, pages 216-221. IEEE, 2009.

[48] M. Rajibul Islam, M. Shohel Sayeed, and A. Samraj. Multimodality to improve security and privacy in fingerprint authentication system. In Intelligent and Ad-

vanced Systems, 2007. ICIAS 2007. International Conference on, pages 753-757. IEEE, 2007.

[49] B. Yang, D. Hartung, K. Simoens, and C. Busch. Dynamic random projection for biometric template protection. In Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on, pages 1-7. IEEE, 2010.

[50] K. Simoens, B. Yang, X. Zhou, F. Beato, C. Busch, E. M. Newton, and B. Preneel. Criteria towards metrics for benchmarking template protection algorithms. In Biometrics (ICB), 2012 5th IAPR International Conference on, pages 498-505. IEEE, 2012.

[51] K. Nandakumar. A fingerprint cryptosystem based on minutiae phase spectrum. In Information Forensics and Security (WIFS), 2010 IEEE International Workshop on, pages 1-6. IEEE, 2010.

[52] J. Bringer, H. Chabanne, D. Pointcheval, and S. Zimmer. Generation and use of a biometric key, Mar. 11 2014. US Patent 8,670,562.

[53] B. Yang, C. Busch, J. Bringer, E. Kindt, W. R. Belser, U. Seidel, E. Springmann, U. Rabeler, A. Wolf, and M. Aukrust. Towards standardizing trusted evidence of identity. In Proceedings of the 2013 ACM workshop on Digital identity management, pages 63-72. ACM, 2013.

[54] R. M. Bolle, S. S. Chikkerur, J. H. Connell, and N. K. Ratha. Methods and apparatus for generation of cancelable fingerprint template, Sept. 17 2013. US Patent 8,538,096.

[55] W. Cheng and G. An. Face template protection using chaotic encryption. 2013.

[56] S. Abt. Assessing Semantic Conformance of Minutiae-based Feature Extractors. PhD thesis, M. Sc Thesis, 2011.

[57] http://www.cl.cam.ac.uk/ jgd1000/combine/combine.html

[58] ISO/IEC 24745/2011, Information Technology - Security Techniques - Biometric Information Protection, 2011.