A Reference Architecture for Biometric Template Protection based on Pseudo Identities

Jeroen Breebaart, Christoph Busch, Justine Grave, Els Kindt

jeroen.breebaart@philips.com; christoph.busch@hig.no;
justine.grave@sagem.com; els.kindt@law.kuleuven.be

Abstract: Biometric authentication is often considered to enhance identity verification. The use of biometrics also introduces new challenges to protect the privacy of the subjects while at the same time increasing the security of a verification system. In this paper, a set of requirements is proposed for biometric processing techniques to safeguard privacy and security. From these requirements, a reference architecture is derived that outlines processes and interfaces of biometric template protection methods in a high-level, technology-neutral way.

1 Introduction

The increasing demand for enhanced border control security, and the increasing amount of electronic transactions that are being sent across wired and wireless networks has created a strong need for more reliable identity management. In an identity management system, verifying the identity of a person is a critical task. Existing possession-based identification methods (an ID card, a token or a key) or knowledge-based methods (a PIN, or a password) can be forgotten, lost, shared or stolen, possibly resulting in identity theft or abuse.

In a financial application for example, identity theft may lead to account fraud, payment card spoofing, forgery of cheques or the use of stolen credit card numbers. In the healthcare domain, identity theft can result in access to medical records, unauthorized access to restricted areas, unauthorized use of medication or medical treatment, or health-insurance fraud. In government applications, identity theft may result in counterfeit or abused identity documents. This can have serious consequences since governmental identity documents are often used to authenticate identities for other applications as well.

According to [tw], every 3 seconds there will be a new victim of identity theft in the US and the total damage of identity theft is estimated at a USD 53 billion a year. The need for more reliable identity verification has resulted in an increased interest in biometrics to allow extension of the traditional possession and knowledge-based authentication methods. Biometrics can deliver an increased reliability for identity claim verification, while at the same time being more convenient since biometric characteristics are not easily forgotten or lost.

2 Challenges

1. **Privacy**. The use of biometrics as identity verification mechanism has also raised concerns. More specifically, the tight coupling of a biometric verification method and physical/anatomical properties allows the use of biometric measurement data for other purposes than intended, hence resulting in a privacy risk. This risk may be subdivided into four categories:

   - Unauthorized collection: collection of biometric samples without the subject's knowledge, for example using hidden cameras.
   - Unnecessary collection: biometrics that are employed in situations without or with little benefit from strong user verification.
   - Unauthorized use and disclosure: use of biometrics for purposes other than approved by the subject, such as forensic usage, linking or cross-matching databases, monitoring an individual's daily activity, and alike.
   - Function creep: expansion of a system into areas for which it was not originally intended, for example as occurred for national identity numbers.

   Unfortunately mechanisms to minimize one risk may cause another risk to increase. If for instance a system design includes stronger mechanisms that would prevent spoofing attacks by observing fingerprint patterns and finger-vein patterns at the same time the potential risk increases for a function creep i.e. that additional health-related information that is included in vein-images could be exploited.

   The Data Protection Directive 95/46/EC [EE95] on the protection of individuals with regard to the processing of personal data and on the free movement of such data which is applicable to the processing of biometric data, does not provide a clear answer to these and other privacy risks of biometrics. The Article 29 EU Advisory Body on Data Protection and Privacy therefore also underlined in its Working document on biometrics of 2003 [Par03] the importance of Privacy Enhancing Technologies in order to promote biometric systems that are constructed in a privacy and data protection friendly manner, minimize the collection of data and prevent unlawful processing.

2. **Security**. Biometrics are often employed to enhance the security of an application by improving the accuracy of an identity verification mechanism. One potential caveat is that the increased security may come with a decrease in privacy [CS07]. Furthermore, the incorporation of biometrics may even result in new security risks due to vulnerabilities present in the biometric subsystem. According to [JNN08], the security risks of a biometric verification system can be subdivided into four categories:

   - Intrinsic biometric failure due to incorrect decisions made by the biometric verification system, often expressed as a probability for false acceptance and/or rejection.
   - Administration attacks as a result of improper administration policies.

- Non-secure infrastructure resulting in vulnerabilities related to non-secure hardware, software, or communication channels.
- Biometric overtness facilitating means to covertly acquire a biometric sample from a genuine user and use that to create artifacts or any other means to influence the result of the identity verification system.

3. **Trust**. A third factor that is important for acceptance of biometric verification systems is trust. Trust differs from objective measurements such as false acceptance rates in the sense that is is a subjective property. Trust is a prediction or reliance on an action and its consequences, based on what a subject knows about an application or technology. Examples of (a lack of) trust are concerns such as health effects induced by biometric measurements (for example frequent illumination of the retina), hygiene issues (on fingerprint sensors), or the risk of stolen body parts containing a biometric characteristic (such as fingers). Some biometric modalities may also suffer from negative associations (for example fingerprints and crime).

4. **Risk mitigation**. The persistence of biometric characteristics has important consequences for the ability to mitigate risks associated with identity theft or exploited security vulnerabilities. Once a biometric characteristic has been subject to theft or abuse, it is virtually impossible to renew this characteristic. For the biometric characteristic itself, this problem is difficult to solve. However, a significant reduction of the risks associated with stolen or abused biometric characteristics can be obtained by ensuring that the biometric templates, i.e., the representation of the biometric characteristic in an identity verification system, is *renewable*.

5. **Interoperability**. Last but not least, given the large range of biometric modalities, sensor types, feature extraction types and template formats, an interoperable scheme that supports all technology permutations of sensor, feature and template types is difficult to realize. Interoperability is especially important for large-scale open applications (e.g., biometric passports, biometric banking cards). There are efforts for standardization [37, tcM, AI, ISOa, ISOb, 17], but their scope does currently not cover a complete, end-to-end, interoperable, biometric verification system that employs techniques to protect the privacy of the subjects.

   A related issue is the risk of a vendor lock in. Many biometric verification solutions exist today that are based on proprietary sensors, template formats and comparison algorithms. Switching to another vendor hence may create substantial switching costs.

3 Requirements for biometric templates

Given the challenges described in the previous section we can derive a set of requirements for a biometric verification system to ensure that privacy and security result in a positive sum [CS07], and to allow risk mitigation.

1. **Protected templates**. The representation of biometric templates that is used in a privacy-protected verification system should satisfy the following constraints:

   - It is impossible to retrieve or decode the original biometric sample(s), features or (unprotected) template from the protected template or any derivative that reveals private information from the biometric sample (such as health data, racial or ethnic origin, and alike).
   - It is impossible to uniquely link subjects within and across databases through comparison of templates.
   - A biometric template represents identity verification data for a specific, predefined purpose or application only.

   These constraints should be satisfied for storage, transmission and comparison operations on templates. If a template representation satisfies these constraints, the template is referred to as a "protected biometric template".

2. **Revocable, renewable, and diversifiable protected templates**. Protected biometric templates should support mechanisms for revocation (for example using certificates from a certificate authority). Furthermore, the template encoding process should have means for generation of multiple independent protected templates from the same, or very similar biometric characteristics. The process of generating multiple independent protected templates from the same biometric characteristics is referred to as "diversification". This diversification property is also required to prevent cross-matching of subjects across databases, and to prevent searching for subjects with very similar biometric characteristics.

3. **Universal approach**. The protected biometric templates approach should in principle be applicable to any biometric modality, and support combinations of biometric modalities (fusion) to obtain a high verification performance. Preferably, biometric modalities can be selected and/or combined for each enrollee individually within the same application to resolve potential problems with weak biometric characteristics for a certain group of enrollees.

4. **Interoperability**. Although interoperability in general is regarded as increasing privacy risks, the biometric protected template will not allow linking data subjects across databases or across applications (see above).

   Interoperability dictates that a biometric verification system should be based on a predefined format and method that satisfies the constraint given above. This format should be compatible with a wide range of sensor types and feature extraction types. It is foreseen that such interoperability can be obtained by a two-stage approach:

- Convert a biometric sample into a modality-dependent, predefined biometric feature data format that is preferably in line with existing (and/or standardized) template formats;
- Convert the modality-dependent, predefined biometric feature data to a protected template using a predefined format and method.

In this two-step approach, the intermediate predefined biometric feature data format allows the use of technology from various vendors (including sensors and feature extraction algorithms) within one system. A good example of such intermediate feature data format is the use of fingerprint minutiae data [ISOc].

The same argument holds for the second step. If the formats of the inputs and outputs to create a protected template are standardized, and the process to create protected templates is well defined (either by describing the process itself, or by using conformance criteria), the complete chain from biometric sensor to protected template could be fully interoperable.

5. **Data minimization**. For efficient storage, transmission and matching of protected templates, and to ensure maximum privacy, the amount of binary data associated with the template should be minimized while minimizing negative effects on the identity verification performance.

6. **Intrinsic security**. The verification performance of protected templates should be preferably in line with state-of-the-art biometric verification methods. A limited amount of verification performance degradation is however expected and acceptable as long as this is balanced with the gain in privacy protection. Furthermore, the trade-off between false acceptance and false rejection rates should be adjustable on an application level, and preferably also on a personal level. The latter is especially important to prevent repeating (rejection) inconvenience for persons with weak or noisy biometric characteristics.

   The degree of similarity (comparison score) that was obtained during a comparison may be derived and communicated to an application, but only if there is a strong need or benefit of such information, and only in the case of a match. For a non-match, it is preferably intrinsically impossible to derive a comparison scores to thwart certain attack types that threaten security and privacy (such as hill-climbing attacks).

7. **Seamless integration with existing verification methods**. The biometric architecture should fit seamlessly to existing 2 or 3-factor verification methods (i.e., possession and knowledge-based authentication). The combination of multiple verification methods should result in a multiplicative effect on the difficulty of a zero-effort attack. The use of both application as well as user-specific secrets should be supported. The balance between possession-based, knowledge-based, and biometric security should be controllable on an application or data subject level to assure maximum system flexibility and personal convenience.

Since data subjects have in particular circumstances the right to object against the processing of biometric data on compelling legitimate grounds relating to their particular situation [EE95] such as privacy concerns, difficulty to enroll or false rejections, an authentication system should provide alternative means for authentication that is not based on biometrics. Such means should preferably be specified for failures to enroll, failures to acquire, and false rejects.

8. **Architecture flexibility**. The template protection scheme may support both online verification (using a central database) as well as off-line (local) verification. The architecture may provide a mode that requires both centrally stored protected template information as well as locally stored template information for successful verification.

The approach outlined in this paper is intended to provide additional security and privacy. It should be noted that some applications offer secure storage and processing by storing data on personal tokens. Such token based systems store a biometric template in a secure environment of smart cards and compare on the card [Ber08]. These applications are currently standardized in ISO/IEC JTC1 SC17 [ISOd].

4 Reference architecture

To facilitate a common vocabulary and to outline architectural aspects to meet the requirements described in the previous sections, a reference architecture for protected templates is described below. This architecture is based on so-called "pseudo identities" (or PIs). The pseudo identity life cycle, its embedding in a reference architecture and the associated interfaces and processes will be described in the next sections. The architecture is meant to be technology neutral, i.e., it should provide a generic framework for many existing template protection techniques that currently exist and is preferably future proof. Depending on the biometric application different technical requirements will apply. Thus for a specific implementation single functional components might be left out from this reference architecture or might need to be added to it.

4.1 Pseudo identities

Pseudo identities (cf. [DCB+08]) are diversifiable, protected identity verification strings within a predefined context (i.e., the protected biometric ecosystem). A pseudo identity (PI) does not reveal any information that allows retrieval of the original biometric measurement data, biometric template or true identity of its owner by any other person than the enrolled subject. Within a protected biometric ecosystem, pseudo identities follow 4 distinct phases that are visualized in Fig. 1:

1. Creation (or renewal) of PIs from biometric reference data during an enrollment phase;
2. Verification of a PI based on a recognition sample;
3. Expiration of the validity of a PI;
4. Revocation of a PI if its validity is expired.

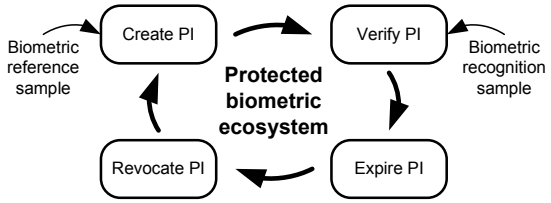

Figure 1: Pseudo identity lifecycle in a protected biometric ecosystem.

4.2 Pseudo identity creation

The Pseudo identity creation process is outlined in Fig. 2. During an enrollment phase a biometric reference is generated for an individual. In this process, a biometric capture device creates one (or more) biometric sample(s), for example in the form of an image of a fingerprint or a photo of a face. Subsequently, a feature extractor creates biometric feature data from the biometric sample. Preferably, but not necessarily, these feature data are in line with existing (standardized) template formats. Finally, a pseudo identity encoder (PIE) generates a pseudo identity and possibly additional auxiliary data (AD). Depending on the employed method and algorithms, the auxiliary data may serve the following purposes:

- It allows generation of multiple independent pseudo identities for the same individual within an application to provide renewable templates;
- it allows generation of independent pseudo identities across applications to prevent database cross-matching and linking;
- it allows generation of independent pseudo identities for subjects that have very similar biometric characteristics to prevent impersonation through spotting of biometric look-a-likes;
- it provides means for template data separation to enhance security and privacy; and
- it allows individualized comparison parameters to optimize the verification performance.

Method	Pseudo identity	Auxiliary data
Fuzzy commitment [JW99]	Hash of secret string	offset
Cancelable biometrics [RCCB07]	Transformed template	Transform parameters
Helper data systems [TAK$^+$05]	Hash of secret string	helper data
Biometric encryption [SRS$^+$98]	Cryptographic key	Filter and key link
Fuzzy vault [JW02, NJP07]	Hash of secret string	Point set P
Shielding functions [LT03]	Hash of secret string	Authentication challenge W
Fuzzy extractors [DRS04]	Hash of secret string	Public string P
Extended PIR [BCPT07]	Encrypted template	n/a

Table 1: Overview of template protection methods and their relation to pseudo identities and auxiliary data.

If the auxiliary data contain data elements that are associated with the diversification process, these data elements are correspondingly referred to as "diversification data". The auxiliary data could result from various approaches that provide renewable and protected templates[1]. Table 1 provides an overview of some existing template protection methods and their relation to pseudo identities and auxiliary data.

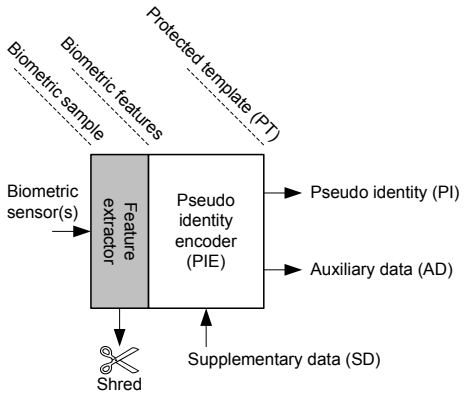

Figure 2: Creation of protected templates.

The combination of PI and AD is referred to as a protected template and hence the requirements mentioned in Sect. 3 apply to this template. Both PI and AD are stored, while the biometric sample and the biometric features are destroyed. The PI and AD can be stored in different ways that can be grouped into three categories: central storage (both PI and AD stored on a database), local storage (both PI and AD stored on a token) and hybrid storage by separating these data elements (for example by storing the AD on a token and the PI in a database). The advantages for central storage of at least one of the data elements are blacklist and audit functionalities, and simple revocation. For local storage, the advantages are the absence of security risks related to central databases and that the subject has

[1]There may exist methods that do not strictly use auxiliary data; in that case the AD is assumed to be an empty string.

full control over the template data. For hybrid storage, the advantages are that the subject and the provider have control over the use of the template data and that is could decrease potential security risks related to central databases (for certain attack types).

The Pseudo identity encoder takes as input some supplementary data (SD). This input can be used for various purposes, such as security enhancement by possession or knowledge-based secrets to be entered by the enrollee (cf. biometrically hardened passwords, [MRW99]); security enhancement by application or system specific secrets or signatures; limiting the scope of a PI by incorporating time and/or place-specific information for which the PI is valid and digital signature or certification of data. In any case, the supplementary data string itself is not stored with the template; it is destroyed when the PI is generated.

Some protected template technologies could be used to perform secure identification as well. This could help in a duplicate enrollment check scenario for instance.

4.3 Pseudo identity verification: PI recoder (PIR) approach

The verification process can be divided in two different classes. The first class of verification processes is based on a "pseudo identity recoder" (PIR) approach. This approach is based on the re-creation (or recoding) of a pseudo identity during the verification process, which is subsequently compared to the pseudo identity that was generated during enrollment (for example [SRS+98, JW99, LT03, DRS04, TAK+05, ST06, NJP07, RCCB07]). The verification is obtained by transforming a captured recognition biometric data sample to a new pseudo identity (PI*) based on the provided auxiliary data (see the left panel of Fig. 3) by a pseudo identity recoder (PIR). If supplementary data input was provided to the pseudo identity encoder during enrollment, the same supplementary data should be provided as input for the pseudo identity recoder. When the PI* is created, all input data, such as the biometric sample, the feature data and the supplementary data, are destroyed. The PI* is provided to a pseudo identity comparator (PIC) that compares both PI and PI*. Only if PI is equal to PI*, verification is successful. The advantage of this approach is that the exchange of information between the PIR (which could for example be integrated in a biometric sensor or a local terminal) and the PIC (which could reside at the application or service provider level) is in protected form (cf. [CS07]).

4.4 Pseudo identity verification: PI verification (PIV) approach

The second class of verification methods does not rely on re-creation of a PI* during verification but rather directly verifies a PI based on a provided recognition sample (cf. [DKM+07, BCI+07, BCPT07]). The corresponding scheme is visualized in the right panel of Fig. 3. Given a protected template consisting of PI and AD and a sample from a biometric sensor, a pseudo identity verifier (PIV) provides the verification result. If supplementary data were provided during enrollment, the same supplementary data should be

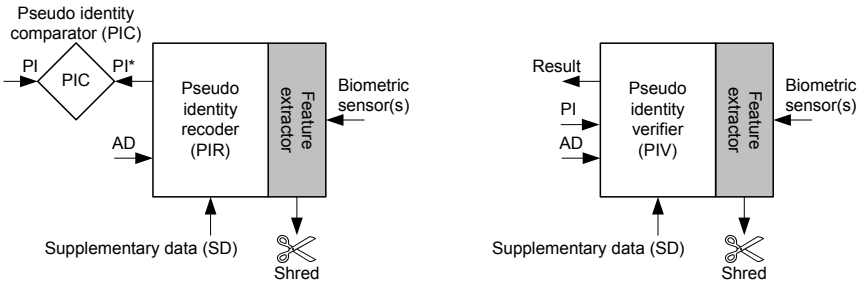

Figure 3: Verification of protected templates by PI recoding and comparison (PIR and PIC; left panel) and by direct PI verification (PIV; right panel).

provided during the verification process to allow a successful verification. If the verification result is published, all input data is destroyed. The advantage of this approach is that no exchange or transmission of template information is required if the PIV module and the protected template are implemented on the same device, for example in a Match-On-Card solution [17, ISOd].

4.5 Pseudo Identity expiration

Pseudo identities may expire for several reasons. For example, it may have been issued for a limited period only, or may require renewal because it was compromised. Furthermore, aging effects might impact the biometric characteristic, as it is the case for the human face, which requires a renewal of the biometric reference. Validity checks and expiration can be controlled by means of watch lists. Alternatively, in some cases a validity period can be used as supplementary data for the Pseudo Identity creator resulting in an intrinsic validity check.

4.6 Pseudo Identity revocation

Depending on the implementation of a verification system, pseudo identities can be revoked by deleting the pseudo identity from a database, and/or removing the authorization to use a pseudo identity. Subsequent to revocation, re-enrollment may result in a new protected template. Depending on the architecture, this may require capturing of new biometric reference samples.

5 Architecture overview

The PI creation, storage and verification architecture is shown in Figs. 4 and 5 for the PI recoder and PI verification approach, respectively. Pseudo Identities are created during an enrollment phase. The biometric sample, biometric features and supplementary data (if these are being used by the application) are deleted when a PI is generated (or stored in a vault for later use, e.g., renewal without physical presence of the data subject). The PI and AD are published and stored on a suitable medium or different media (such as databases, smart cards, bar codes, etc). During verification in case of a recoding approach, a new PI* is generated (recoded) from the issued AD, a biometric measurement and supplementary data (if these are being used by the application). Both PI and PI* are communicated to an application to verify the claimed identity. For the PIV approach, the PIV generates a verification result without recoding a PI.

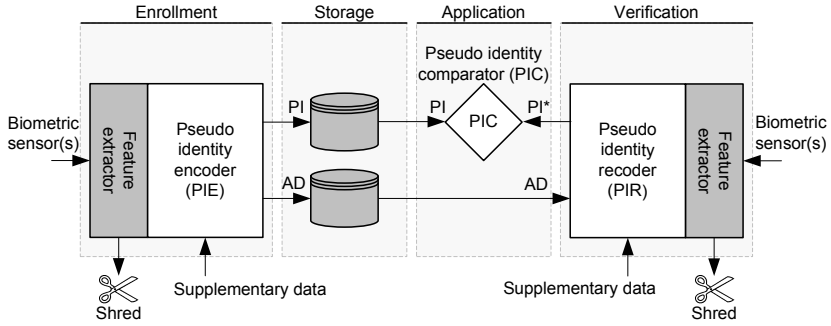

Figure 4: Reference architecture for biometric template protection based on pseudo identity recoding and comparison.

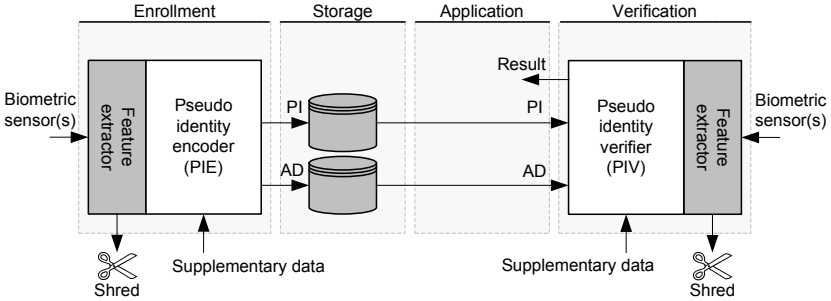

Figure 5: Reference architecture for biometric template protection based on direct pseudo identity verification.

6 Conclusions

In this paper, challenges and resulting requirements for biometric template protection methods were outlined. Based on the requirements, a reference architecture was described that describes the relevant interfaces and processes for template protection in a technology-neutral way.

7 Acknowledgments

The authors would like to thank Ton Akkermans, Julien Bringer, Jens-Petter Glittenberg, Berk Gokberk, Koen de Groot, Alty van Luijt, Johannes Midgren, Koen Simoens, Menno Treffers, Michiel van der Veen, and Bian Yang for their very helpful comments and suggestions to improve the proposed architecture and this manuscript. This work is supported by funding under the Seventh Research Framework Programme of the European Union, Project TURBINE (ICT-2007-216339). This document has been created in the context of the TURBINE project. All information is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. The European Commission has no liability in respect of this document, which is merely representing the authors' view.

References

[17] ISO/IEC JTC 1 SC 17. Application of biometrics to cards and personal identification.

[37] ISO/IEC JTC 1 SC 37. Biometrics.

[AI] ANSI/NIST-ITL. American national standards for biometrics. http://fingerprint.nist.gov/standard/.

[BCI+07] J. Bringer, H. Chabanne, M. Izabachene, D. Pointcheval, Q. Tang, and S. Zimmer. An application of the Goldwasser-Micali cryptosystem to biometric authentication. In *ACISP*, 2007.

[BCPT07] J. Bringer, H. Chabanne, D. Pointcheval, and Q. Tang. Extended private information retrieval and its application in biometrics authentications. In *CANS*, 2007.

[Ber08] C. Bergman. Match-on-card for secure and scalable biometric authentication. In N. K. Ratha and V. Govindaraju, editors, *Advances in biometrics*. Springer, London, 2008.

[CS07] A. Cavoukian and A. Stoianov. Biometric encryption: a positive-sum technology that achieves strong authentication, security and privacy. *Whitepaper information and Privacy Commissioner/Ontario*, 2007. available from www.ipc.on.ca.

[DCB+08] N. Delvaux, H. Chabanne, J. Bringer, B. Kindarji, P. Lindeberg, J. Midgren, J. Breebaart, T. Akkermans, M. van der Veen, R. Veldhuis, E. Kindt, K. Simoens, C. Busch, P. Bours, D. Gafurov, B. Yang, J. Stern, C. Rust, B. Cucinelli, and D. Skepastianos. Pseudo idenitities based on fingerprint characteristics. In *IEEE 4th international conference on intelligent information hiding and multimedia signal processing (IIH-MSP)*, Harbin, China, 2008.

[DKM+07] S. Draper, A. Khisti, E. Martinian, A. Vetro, and J. Yedidia. Using distributed source coding to secure fingerprint biometrics. In *Mitsubishi Electric Research Labs*, 2007.

[DRS04] Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *Eurocrypt*, 2004.

[EE95] European Parliament and European Council. Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML, 1995. Last visited: May 24, 2008.

[ISOa] ISO/IEC. 19092:2008 - Financial services - Biometrics - Security framework.

[ISOb] ISO/IEC. 19794 - Information technology - biometric data interchange formats.

[ISOc] ISO/IEC. 19794-2:2005 - Information technology - biometric data interchange formats part 2: Finger minutiae data.

[ISOd] ISO/IEC. CD 24787 - Identification cards - On-Card matching.

[JNN08] A. K. Jain, K. Nandakumar, and A. Nagar. Biometric template security. *EURASIP J. Advances in signal processing*, 2008. (To appear).

[JW99] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In *ACM Conference on Computer and Communications Security*, pages 28–36, 1999.

[JW02] A. Juels and M. Wattenberg. A fuzzy vault scheme. In *Proc. IEEE Int. Symposium on Information Theory*, 2002.

[LT03] Jean-Paul M. G. Linnartz and Pim Tuyls. New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates. In *AVBPA*, pages 393–402, 2003.

[MRW99] F. Monrose, M. K. Reiter, and R. Wetzel. Password hardening based on keystroke dynamics. In *Proc. 6th ACM CCCS*, pages 73–82, 1999.

[NJP07] K. Nandakumar, A. K. Jain, and S. Pankanti. Fingerprint-based fuzzy vault: Implementation and performance. In *IEEE transactions on information forensics and security*, 2007.

[Par03] ARTICLE 29 Data Protection Working Party. Working document on biometrics Working Document on Biometrics. http://ec.europa.eu/justice-home/fsj/privacy/docs/wpdocs/2003/wp80-en.pdf, 2003. Last visited: May 24, 2008.

[RCCB07] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle. Generating cancelable fingerprint templates. *IEEE Trans. pattern analysis and machine intelligence*, 29(4):561–572, 2007.

[SRS+98] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. V. K. Vijaya Kumar. Biometric Encryption using image processing. In *Proc. SPIE 3314*, pages 178–188, 1998.

[ST06] B. Schoenmakers and P. Tuyls. Efficient binary conversion for Paillier encrypted values. In *Eurocrypt*, 2006.

[TAK+05] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G. J. Schrijen, A. M. Bazen, and R. N. J. Veldhuis. Practical biometric authentication with template protection. In *Audio and video-based biometric person authentication*, pages 436–446. Springer, Berlin, Germany, 2005.

[tcM] ANSI/INCITS technical committee M1. Biometrics. http://m1.incits.org/.

[tw] Identity theft website. http://www.idtheft.com.