BEAT

Biometrics Evaluation and Testing

http://www.beat-eu.org/

Funded under the 7th FP (Seventh Framework Programme)

Theme SEC-2011.5.1-1
[Evaluation of identification technologies, including Biometrics]

D5.5: Description of Metrics for the Evaluation of Privacy Preservation

Due date: 31/12/2012 **Submission date:** 31/12/2012
Project start date: 01/03/2012 **Duration:** 48 months
WP Manager: Cagatay Karabat **Revision:** 1

Author(s): Cagatay Karabat(TUBITAK), Julien Bringer (Morpho)

Project funded by the European Commission in the 7th Framework Programme (2008-2010)		
Dissemination Level		
PU	Public	Yes
RE	Restricted to a group specified by the consortium (includes Commission Services)	No
CO	Confidential, only for members of the consortium (includes Commission Services)	No

D5.5: Description of Metrics for the Evaluation of Privacy Preservation

Abstract:

This report is a literature survey on the metrics for privacy preservation. It will also describe the basic properties of the required quantitative and qualitative metrics by taking into account necessary security measures. In other words, it will deliver a requirement analysis for privacy preservation metrics.

The deliverable is structured as follows. The first section is devoted to the Introduction of the privacy preservation metrics. The second section addresses threat models. The third section covers privacy preservation metrics for biometric template protection methods. The forth section is related with the privacy preservation metrics for biometric systems. Finally, we give brief summary at the last section.

Contents

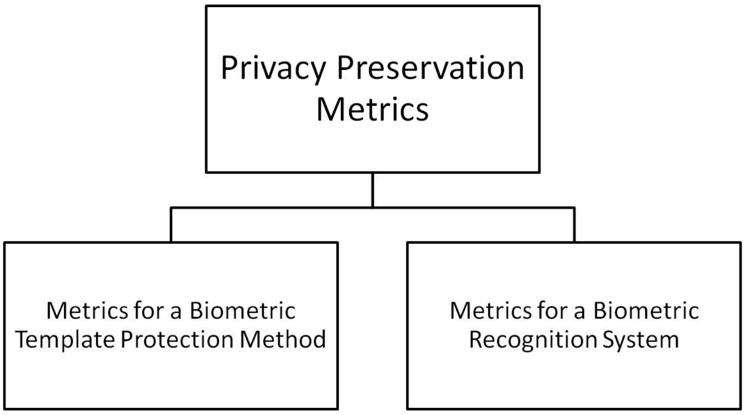

Privacy Preservation Metrics
Metrics for a Biometric Template Protection Method
Metrics for a Biometric Recognition System

Figure 1: Classification of privacy preservation metrics

1 Introduction

In recent years, biometrics have started being used in many real life applications. Widespread usage of biometrics, however, brings security and privacy problems. Since biometrics are derived from human bodies (e.g. face, fingerprint, iris) or activities of a human (e.g. gesture), it is personal information, hence, it is classified as sensitive information. The personal data is defined in the European Data Protection Directive 95/46/EC [1]: 'personal data shall mean any information relating to an identified or identifiable natural person ('data subject') and an individual have the right of access to and the right to rectify the data concerning him'.

Especially, it is really hard to assess either a biometric template protection method or a biometric recognition system in terms of privacy. There exists a need for a generalized privacy evaluation framework for both biometric template protection methods and biometric recognition systems. Privacy evaluation metrics are the main elements of a generalized privacy evaluation framework. In this deliverable, we discuss how to design an evaluation framework for biometric template protection methods and biometric recognition systems in terms of privacy. Therefore, we analyze potential privacy protection metrics for 1) Biometric template protection methods, 2)Biometric recognition systems as shown in Figure 1.

Privacy preservation ability of a biometric template protection scheme can be assessed via diversification, irreversibility, privacy leakage, and unlinkability. Irreversibility is related with the complexity to retrieve biometric features, while privacy leakage quantifies how much information about biometric data is contained in a secure biometric template. Another important criterion is unlinkability. Assume that an adversary obtains two secure templates. It should be difficult for him to verify whether they are generated from the same subject or not. Furthermore, combining two secure templates should not be helpful to estimate secrets or to retrieve biometric features. On the other hand privacy preservation ability of a biometric recognition system can be assessed via communication, storage, user and sensor requirements.

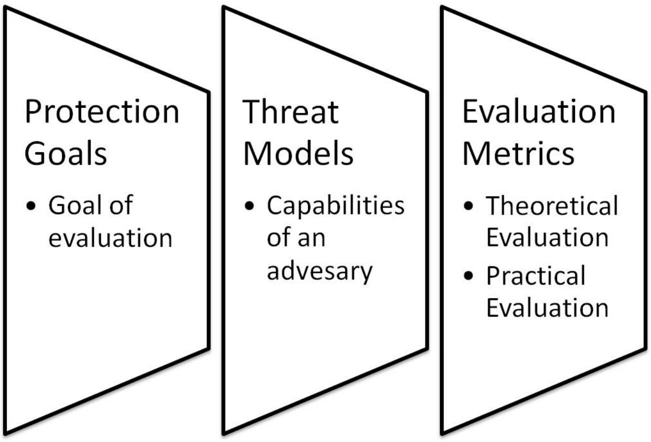


Figure 2: Generalized Privacy Evaluation Framework

2 Protection Goals

In a general privacy evaluation framework, the first step is to specify the objectives of the evaluation in order to properly determine metrics. The protection goals should be defined in order to clarify the aim of the evaluation. Within the concept of this deliverable, privacy is the protection goal of a biometric template protection method or a biometric recognition system.

The next step is to determine the threat models with respect to the abilities of an adversary. The last step is the evaluation. There are two types of evaluation: 1) Theoretical evaluation, 2)Practical evaluation. It should be noted that it is still unknown whether privacy preservation metrics are suitable for empirical evaluation and how these metrics can be measured in practice.

3 Threat Models

Choosing appropriate privacy preservation metrics is very important in order to evaluate the privacy preservation level of a biometric template protection method or biometric recognition system. The privacy preservation metrics should be identified with respect to the pre-defined threat models. Therefore, the first step is to specify the threat models. Some of the key check list questions in order to determine the threat models are as follows:

1. What are the abilities of an adversary?
2. What kind of information and system parameters an adversary can access in a practical attack?
3. How much computational power is available for an adversary?

Biometric template protection methods aim to increase the robustness of biometrics against internal and external attacks in a biometric recognition system. It is important to identify the power of an adversary before assessing the method in terms of privacy. In other words, the threat models are classified according to the information and computational resource available to an adversary. In this concept, three main threat models are defied as follows [20]:

- Naive Model
- Advanced Model
- Collision Model

Naive and advanced threat models are derived from the cryptanalysis which a cryptanalyst defines during assessment of cryptosystems. Naive threat model is the basic and the weakest threat model whereas advanced model is the most dangerous model which assess the privacy preservation level of a biometric protection method against a qualified adversary. On the other hand, collision model uses inherent weaknesses of biometrics (i.e. false acceptance rate). It is possible to refine threat models or extend new requisitions according to privacy requirements. It is worth to mention that the threat models are prerequisites for quantifying privacy.

3.1 Naive Model

In this threat model, an adversary has only access to secure biometric templates which are the outputs of a biometric template protection method (e.g. if biohashing method is used, an adversary is assumed to get biohashes). He has neither information of the underlying algorithm in a template protection system, nor owns a large biometric database. Besides, the biometric protection system is considered as a blackbox.

3.2 Advanced Model

In this threat model, an adversary has full knowledge of the underlying biometric template protection method as stated in Kerckhoff's principle of cryptology (A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.). In other words, adversary can access system internal parameters and can adjust them, he can obtain secure biometric templates from different biometric databases and he knows statistical properties of biometric features. Furthermore, it is assumed that an adversary also knows the secret information of a biometric template protection method. For example, this secret information can be a secret parameter i.e. transformation parameters in cancelable biometrics or projection matrix in biohashing. It is important to see whether leakage of biometric information exists, if secret information is compromised. In a nutshell, it is assumed that all system parameters are known to an adversary in this threat model.

3.3 Collision Model

In this threat model, an adversary has sufficiently large amount of biometric data in order to gain information about biometric data. He can exploit inaccuracy of biometric template protection method/biometric recognition method, make an exhaustive search in his own database and find biometric data, which have sufficient similarity to that of a target user. If False Accept Rate (FAR) is false acceptance rate of the system under a given setting, 1/FAR is the average number of biometric data from different users, which an adversary needs in his own database. This attack can be seen as a "Zero Effort" attack where an impostor provides one of its biometric sample to be authenticated as the user.

4 Privacy Preservation Metrics for Biometric Template Protection Methods

Biometric template protection methods are designed to preserve privacy and increase security of biometric templates against possible attacks using stored or transferred biometric data [6, 13, 11, 7, 8]. These methods have a number of useful properties i.e. revocation and renewing of biometric templates, which are the crucial functionalities in identity management [10]. The international standard ISO/IEC 24745 [2] defines a high-level architecture of biometric template protection, which can model various types of methods. It consists of the following functions:

1. The pseudonymous identifier encoder (PIE) generates a pseudonymous identifier (PI) and auxiliary data (AD) from a biometric data (B) in the enrolment session: $[PI; AD] = PIE(B)$ where PI denotes a protected identity of a user, B denotes biometric data and AD denotes user-specific data, which help to reproduce PI in an authentication process. Only PI and AD are stored as a secure template in the system. The biometric data B is deleted after the enrolment.

2. The pseudonymous identifier recorder (PIR) takes a queried biometric data (B') and the stored auxiliary data (AD) as inputs and computes a pseudonymous identifier PI' in the verification session: $[PI'] = PIR(B'; AD)$.

3. The pseudonymous identifier comparator (PIC) compares PI' with the stored PI : $v = PIC(PI; PI')$. Depending on comparators, comparison result v is either a hard decision (yes/no) or a similarity score v.

The Figure 3 illustrates the construction of biometric template protection with PIE, PIR and PIC. Biometric recognition systems use the biometric data collected at the enrollment session B and the biometric data collected at the verification session B'. In real life applications, enrollment and verification stations are not placed at the same location. If the biometric data are centrally stored, database easily becomes attack target. In remote enrollment or authentication, biometric data needs to be transported, e.g. over Internet. From security point of view, transferring and storing PI, which cannot conceal biometric information, are better than using biometric templates themself. Please note that AD is allowed to be public in some algorithms, however, in others AD is a secret parameter. The desired properties of biometric template protection methods are:

1. **Irreversibility**: It is either computationally hard or impossible to deduce the underlying biometric data from PI.

2. **Robustness**: Biometric data vary due to acquisition noise, environment changes, aging effect, etc. The derived PIs should be robust to variation of input biometric data and PIC can compare PIs directly. Additionally, applying template protection should not influence the recognition performance in comparison with the original biometric system.

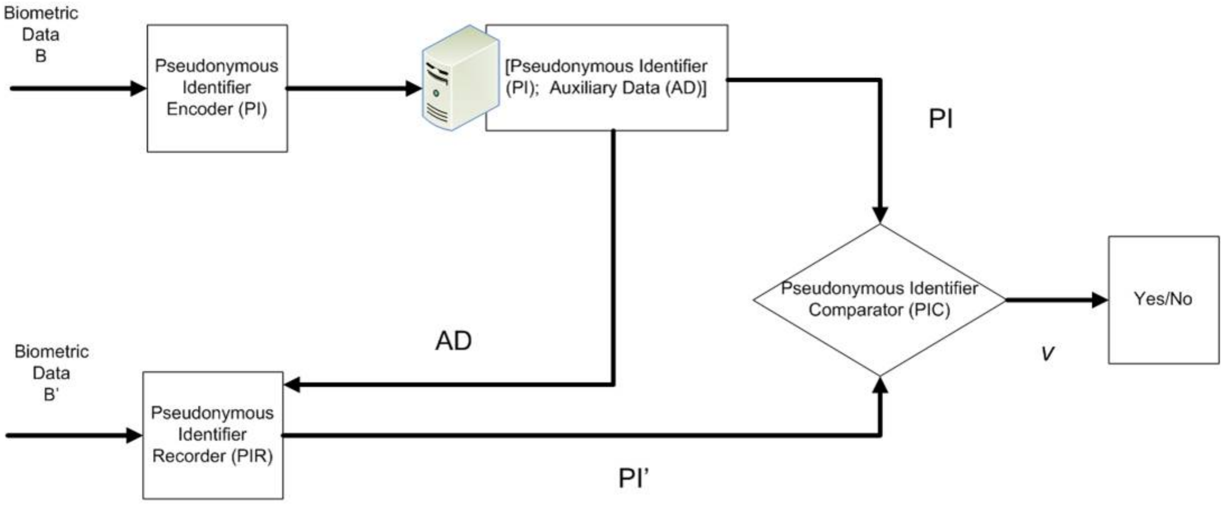

Biometric Data B
Pseudonymous Identifier Encoder (PI)
[Pseudonymous Identifier (PI); Auxiliary Data (AD)]
PI
Pseudonymous Identifier Comparator (PIC)
Yes/No
V
AD
Biometric Data B'
Pseudonymous Identifier Recorder (PIR)
PI'

Figure 3: ISO reference architecture of biometric template protection

3. **Diversity**: Number of independent protected templates can be generated from one biometric characteristic.

4. **Unlinkability**: Knowledge of one protected template does not yield information on other protected templates derived from the same characteristics.

The Figure 4 shows the examples of functions used in the biometric template protection methods and the meaning of PI and AD. Various functions and constructions are used to meet the aforementioned requirements. Besides, all these methods can be described with the ISO architecture.

This section introduces the basic properties of required privacy preservation metrics for a biometric template protection method by taking into account necessary security measures. The potential criteria and requirements for privacy preservation metrics are defined as follows: [20, 16, 3]:

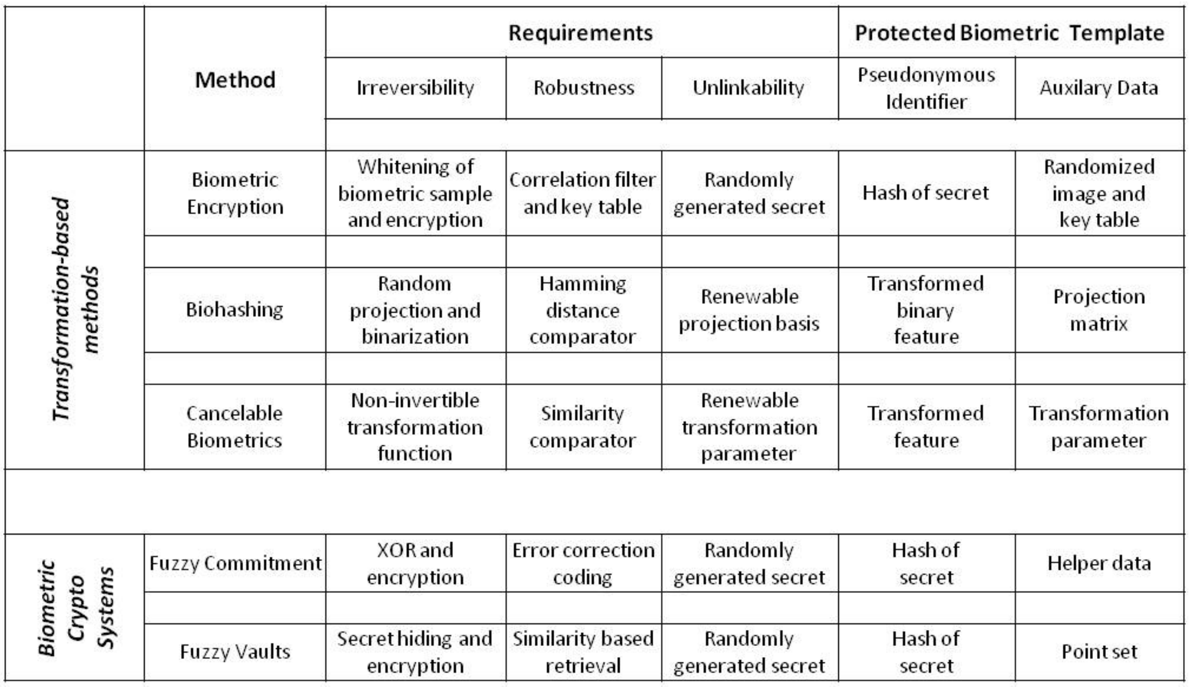
1. Diversification

2. Irreversibility

3. Unlinkability

4. Privacy Leakage

There exists number of potential metrics (e.g. min-entropy, average min-entropy, guessing entropy, conditional guessing entropy and statistical distance) in privacy assessment of a biometric template protection methods as shown in Table 1. These metrics evaluate the privacy from different aspects. Min-entropy, $H_\infty(B)$ where B denotes biometric



	Method	Requirements			Protected Biometric Template	
		Irreversibility	Robustness	Unlinkability	Pseudonymous Identifier	Auxilary Data
Transformation-based methods	Biometric Encryption	Whitening of biometric sample and encryption	Correlation filter and key table	Randomly generated secret	Hash of secret	Randomized image and key table
	Biohashing	Random projection and binarization	Hamming distance comparator	Renewable projection basis	Transformed binary feature	Projection matrix
	Cancelable Biometrics	Non-invertible transformation function	Similarity comparator	Renewable transformation parameter	Transformed feature	Transformation parameter
Biometric Crypto Systems	Fuzzy Commitment	XOR and encryption	Error correction coding	Randomly generated secret	Hash of secret	Helper data
	Fuzzy Vaults	Secret hiding and encryption	Similarity based retrieval	Randomly generated secret	Hash of secret	Point set

Figure 4: Examples of functions used in the biometric template protection methods and the meaning of PI and AD [20]

data, refers to the probability of the most frequently occurring element of a variable. The irreversibility can be measured via min-entropy in advanced model without taking AD into account. Average min-entropy, $\widetilde{H}_\infty(B|PI)$ where B denotes biometric data and PI denotes pseudonymous identifier, can be used to measure the irreversibility in advanced model. It corresponds to the probability of the most likely biometric data given protected template. Guessing entropy, $G(B)$, and conditional entropy measure the average number of attempts needed to retrieve user's biometric data with and without the help of AD respectively. Statistical distance measures the distance between two distributions. In the secret-based biometric template protection methods, the secrets are expected to be random even if auxiliary data is given. The statistical distance can show the deviation of the secret distribution from an ideal uniform distribution.

Apart from the aforementioned metrics, capacity of a biometric template protection method can be used as a metric for privacy preservation [20]. Capacity refers to the number of different users that a biometric template protection method can accommodate. In the literature, Willems proposed a general capacity analysis method for biometric identification systems. [19]. Tuyls works on capacity analysis for biometric template protection methods [18]. Besides, Karabat proposes a capacity analysis framework especially for biohashing methods [9] which are used as an authentication system.

Table 1: A Generalized Framework for Privacy Assessment

Metric	Threat Model	Requirement
Entropy	Naive	Diversification
Min-Entropy	Advanced	Irreversibility
Conditional Entropy	Advanced	Irreversibility
Mutual Information	Advanced	Privacy leakage

4.1 Diversification

Biometric template protection methods can generate a number of protected template from the same biometric feature of a user. Diversification can be defined as the maximum number of independent protected biometric templates that can be generated from the same biometric feature of a user by using a biometric template protection method. For instance, the number of biohash vectors that can be generated from the same biometric feature of a user by using the same biohashing method. The diversification can be measured via entropy of pseudonymous identifier PI (i.e. $H(PI)$).

4.2 Irreversibility

Irreversibility refers to the secrecy of the biometric data from which the protected template was created. In other words, the irreversibility means that the difficulty of determining (exactly or with tolerable margin) the biometric features of a user from a protected template. For instance, let us assume that a biohash vector (protected template) is generated by using a biohashing method (biometric template protection method). Here, irreversibility problem occurs if an attacker can obtain the biometric data from the biohash vector.

The irreversibility of biometric data is equivalent to security of pseudonymous identifier PI. The security of PI can be measured with conditional entropy $H(S|AD)$ where S denotes secret of a biometric template protection method (i.e. secret key for a biohashing method) and AD denotes auxilary data (i.e. projection matrix for biohashing methods). Besides, the irreversibility can be measured by conditional entropy $H(B|PI)$ where B denotes biometric data and PI pseudonymous identifier (i.e. biohash vector for biohashing methods as shown in Figure 4). Here, the conditional entropy measures the uncertainty about B given PI. With this construction, privacy of the biometric data B depends on the secret S. Thus, the uncertainty about B is equal to the uncertainty about S with known AD. It is proved for fuzzy commitment schemes as follows [4, 20]:

$$\begin{aligned} H(S|AD) &= H(S) - I(S;AD) \\ &= H(S) + H(B) - H(AD) \\ &= H(B|AD) \end{aligned} \tag{1}$$

where B denotes biometric feature vector of a user.

4.3 Unlinkability

Biometric template protection methods generate protected templates from biometric features. These protected templates are used for either authentication or identification purposes in a biometric recognition system. One of the main goals of the biometric template protection methods is to preserve privacy of the user via protected templates. An adversary, however, may not need to generate the original biometric feature of a user in order threaten the privacy. If the adversary links the protected template with the user, he can be successful. Unlinkability between the protected template and the user means that within the biometric template protection method, from the adversary's perspective, these items of interest are no more and no less related after his observation. In other words, it means that the probability of those items (the protected template and the user) being related from the attacker's perspective stays the same before and after attacker's observation (attacker gets the protected template of the user). Actually, unlinkability has two aspects which are defined as follows:

1. **Cross matching**: When an adversary obtains two protected biometric templates, it should be hard for him to verify whether they are generated from the same user or not. On the other hand, if protected biometric templates contain personal identifiable information, cross matching can happen. For example, AD is generated by PIE and required in PIR. If AD is not random and contains user-specific information, identification of a user is feasible with AD. It is necessary to measure whether and how much personally identifiable information is contained in AD.

2. **Leakage amplification**: Combing two or more protected biometric templates should not be helpful to estimate secrets or to retrieve biometric features. Whether combination of several secure templates can increase privacy leakage and reduce security needs to be analysed. Leakage amplification limits long term applications and multiple uses of biometrics.

4.4 Privacy Leakage

The privacy leakage quantifies how much information about biometric data contained in a protected template [15]. The probability distribution of biometric data plays a very important role in privacy assessment. It is expected that binary biometric features have uniform distribution where a bit's probability being 1 or 0 is equal. In other words, binary biometric feature B is expected to be uniformly and independently distributed (u.i.d.), namely any element b_i of B with $p(b_i = 0) = p(b_i = 1) = 0.5$. On the other hand, the dependency of binary features is ignored in many biometric template protection methods. Thus, security and privacy are suspected to be highly overestimated. It is necessary to know the distribution of biometric data in theoretical analysis. When bits extracted from biometric features are uniformly and independently distributed, it is possible to achieve perfect security from information-theoretical point of view. However, this strict condition is difficult to fulfill in real-life application and privacy leakage is unavoidable [21]. There exist privacy leakage in many biometric template protection methods in order to compensate variation of biometric data [17, 5]. The protected biometric template should contain as little biometric information as possible since exposure of biometric information is not only threat for privacy but also a serious security shortcoming. It can also be exploited to retrieve activities of a subject in other biometric applications. In the literature, Ignatenko analyses the privacy leakage in term of the mutual information between the public helper data and biometric features in a biometric template protection method. In this work, a trade-off between maximum secret key rate and privacy leakage is given [5].

Privacy leakage can be measured with the mutual information as follows;

$$I(B; AD) = H(B) - H(B|AD) \tag{2}$$

where B denotes biometric feature vector of a user and AD denotes auxilary data [4].

5 Privacy Preservation Metrics for Biometric Recognition Systems

In addition to the biometric template protection methods (cf. Section 4), that can be seen as a protection at the template level, several studies have been made for protection layers at the system level to preserve privacy of the users. We here discussed the threats, goals and metrics that can be considered with respect to the analysis of a system solution.

This section introduces possible privacy preservation evaluation metrics for biometric recognition systems when seen at the system level. In other words, this section addresses the basic properties of required privacy preservation metrics for a biometric recognition system by taking into account necessary security measures.

The potential criteria for privacy preservation are derived mainly from the framework described in [14] but some general ideas are also given in [20, 16].

5.1 Biometric Components

In the literature, the basic components of a biometric recognition system have been defined as illustrated by Figure 5.

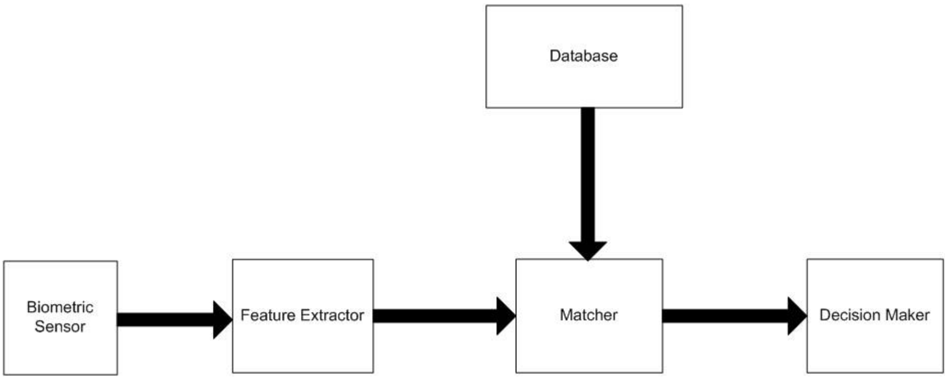


Figure 5: Basic elements of a biometric recognition system

The basic components are:

1. Biometric sensor
2. Feature extractor
3. Matcher
4. Database
5. Decision maker

These biometric components can be executed in the same location or not. When it is not possible to consider some of them as independent of the others, we have to rely on the template protection at the template level for privacy metrics. Whereas if some components are distributed in different physical or logical locations, we can elaborate a more complex system view to analyse the privacy properties.

Ten possible attack points to a biometric recognition system have been defined in [12] as shown in Figure 6.

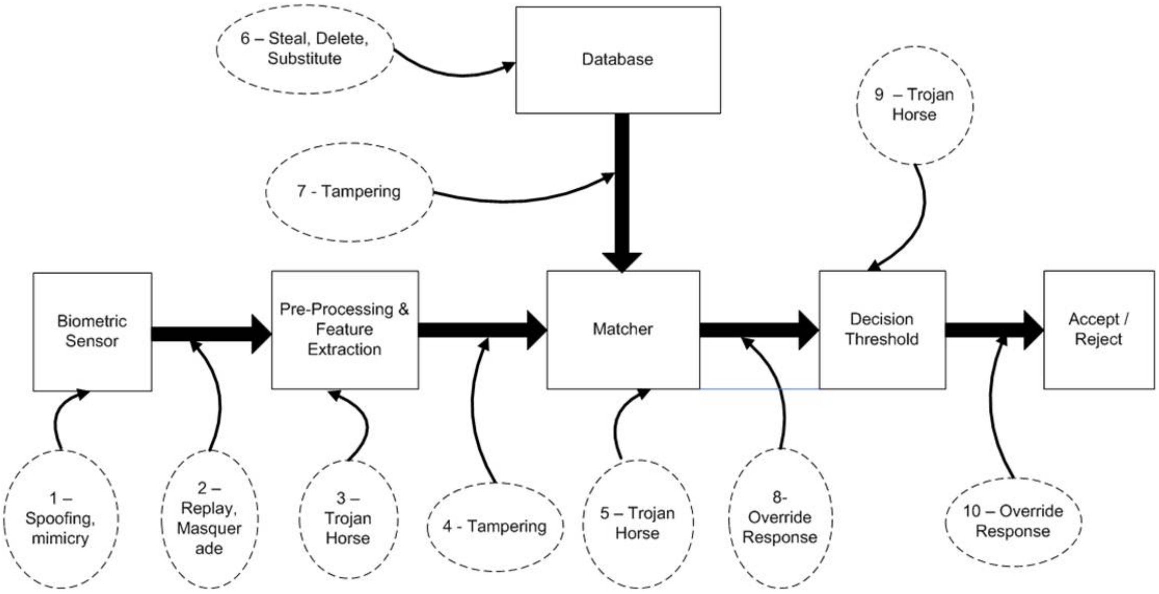


Figure 6: Attacks against a biometric recognition system (adapted from [12])

These attacks points are originally introduced to undermine the operationnal goals of the system (ensuring an accurate decision). But they can also be a threats for the privacy of users. These attacks are as follows:

1. Spoofing attacks
2. Attack against the communication channel between sensor and feature extractor
3. Attack against feature extractor
4. Attack against the communication channel feature extractor and matcher
5. Attack against matcher
6. Attack against database
7. Attack against the communication channel between matcher and database

8. Attack against the communication channel between matcher and decision maker
9. Attack against the decision maker
10. Attack against the communication channel between decision maker and application

5.2 System Model

We give now a point of view mainly based on a synthesis of the general privacy framework for a biometric authentication system that is described in [14]. This recent framework considers insider attacks of biometric authentication protocols with respect to user and data privacy. In fact, even in the case of a biometric system with several distributed entities, it is important to circumvent function creep of the system, where an adversary might try to learn information either on biometric data or on users that are in the system.

This framework gives a general system model involving four logical entities on which the biometric components introduced above will be implemented: a sensor, an authentication server, a database and a matcher.

And the difficult point is to analyze whether one or a combination of these entities could exploit potential privacy leakages when they have a malicious behavior. Security against external eavesdroppers is handled via quite classical security measures (confidentiality, integrity, secure communication).

5.2.1 Enrolment

In the system, a user, who has previously registered his biometric data b_i during the enrollment procedure, wishes to authenticate to a particular service. In the context of the service, the user has been assigned an identifier ID_i, which only has meaning within this context. The biometric reference data b_i are stored by the database, who links the data to identifier i. The mapping from ID_i to i is only known by the authentication server, if relevant. Note that in some applications it is possible that the same user is registered for the same service or in the same database with different samples, b_i and b_j, and different identities, i.e., $ID_i \neq ID_j$ in the service context or $i \neq j$ in the database context. The property of not being able to relate queries under these different identities is called *identity privacy*.

5.2.2 Authentication

During the authentication procedure the sensor captures a fresh biometric sample b'_i from the user and sends the sample to the authentication server. The authentication server manages authorizations and controls access to the service. To make the authorization decision, the authentication server will rely on the result of the biometric verification (or possibly identification) procedure that is obtained via the matcher. It is assumed that there is no direct link between the matcher and the database. As such, the authentication server requests from the database the reference data that are needed by the matcher and forwards them to the matcher.

5.3 Attackers

Two types of attackers are possible: internal attackers are corrupted components in the system and external attackers are entities that only have access to a communication channel. It is important to verify that the system ensures the security of the scheme against any external attacker. This can be achieved by an external security layer, generally independent of the core protocol specification, for instance with encryption for confidentiality of the communication channels and of the data when at rest. This is a first privacy level to measure on the system: Is there a privacy leakage with respect to an external adversary?

There are also two types of internal attackers: passive ones (that follow the protocol but are happy to learn information from the data that pass through them) and active ones that can deliberately deviate from the protocol to create information leakage. This is a second privacy level to measure on the system: Is there a privacy leak with respect to an internal passive adversary or to an active one?

The sequel of this section discussed the potential criteria for privacy preservation. The first ones correspond merely to external attackers or, honest-but-curious and isolated internal entities (part of those criteria are mentioned in [20, 16]). Then more details are given with respect to complex privacy issues related to combination of internal malicious entities (as described in [14]).

5.4 Basic Requirements

5.4.1 Communication Requirements

Since private information are communicated between the different entities, confidentiality and integrity mechanisms that thwart attacks based on distinguishing private data and perturbing any data by an external adversary.

5.4.2 Storage Requirements

Since private information are stored in a database for authentication or identification purposes in a biometric recognition system, the database should ensure confidentiality of the data in such a way that it is possible neither to distinguish private data (irreversibility and unlinkability), nor to modify them (in order to avoid privacy leakage after potential perturbations).

5.4.3 User and Sensor Requirements

The user and the sensor should be limited in their possible actions, in particular to avoid them searching for a collision (as described in Section 3).

5.5 Advanced Privacy Requirements

To analyse precisely the potential privacy issues, the following attack goals are defined:

- Learn reference b_i (fully or partially): the full leakage is the recovery of the full template, authorization leakage is to construct a sample close (i.e. that would result on a successful authentication) to b_i and minimum leakage is the retrieval of information that enables to link references. If the system thwarts this attack, we say that it achieves **biometric reference privacy**.

  This attack is a threat with respect to the authentication server, the matcher, potentially the database (if the system is designed to make confidential the data stored in the database), and a combination of those entities.

- Learn sample b'_i: Similar as in the attack goal above but for the fresh samples. When the system is resistant, we have **biometric sample privacy**.

  This attack is a threat with respect to the authentication server, the matcher, the database and a combination of those entities.

- Trace users with different identities: This corresponds to the case when different references from the same user, possibly coming from different systems, can be linked together. We have **identity privacy** when the system avoids such leakage.

  This attack is a threat with respect to the authentication server, the matcher, potentially the database (if the system is designed to make confidential the data stored in the database), and a combination of those entities.

- Trace users over different queries: This attack refers to the possibility of linking queries, either anonymised or not, based on i, ID_i, b_i or b'_i. When this attack is prevented, we say that the system ensures **transaction anonymity**.

  This attack is a threat with respect to the database, the matcher, potentially the authentication server (if the system is designed to make private the identities on the service side), and a combination of those entities.

Privacy leakage with respect to the user or the sensor is not generalized as above but should also be investigated (in particular in combination with the other insider attack points: authentication server, database, matcher).

6 Summary

In this deliverable, literature review for privacy metrics of biometrics has been achieved. The number of potential candidates for privacy metrics have already been identified for both biometric template protection methods and biometric recognition systems. The more detailed analysis and implementation will be achieved in the next deliverable (D5.6 Metrics for the evaluation of privacy preservation).

References

[1] Directive 95/46/ec of the european parliament and of the council. In *Offical Journal of the European Communities*, page 281, 1995.

[2] I. J. S. 27. Iso/iec 24745 information technology - security techniques - biometric template protection. June 2011.

[3] R. Belguechi, E. Cherrier, and C. Rosenberger. How to evaluate transformation based cancelable biometric systems? In *NIST International Biometric Performance Testing Conference (IBPC)*, 2012.

[4] T. Ignatenko. Secret-key rates and privacy leakage in biometric systems, 2009.

[5] T. Ignatenko and F. Willems. Secret rate - privacy leakage in biometric systems. In *Proceedings of the 2009 IEEE international conference on Symposium on Information Theory - Volume 4*, ISIT'09, pages 2251–2255, Piscataway, NJ, USA, 2009. IEEE Press.

[6] A. K. Jain, A. Ross, and S. Prabhakar. An introduction to biometric recognition. *IEEE Trans. on Circuits and Systems for Video Technology*, 14:4–20, 2004.

[7] C. Karabat and H. Erdogan. Discriminative projection selection based face image hashing. *IEICE Transactions*, 95-D(5):1547–1551, 2012.

[8] C. Karabat and H. Erdogan. Error-correcting output codes guided quantization for biometric hashing. *IEICE Transactions*, 95-D(6):1707–1712, 2012.

[9] C. Karabat, H. Erdogan, and M. Mihcak. Information theoretic capacity analysis for biometric hashing methods. In *Digital Signal Processing (DSP), 2011 17th International Conference on*, pages 1 –6, july 2011.

[10] A. Nagar, K. Nandakumar, and A. K. Jain. Biometric template transformation: a security analysis. In *Media Forensics and Security*, page 75410, 2010.

[11] S. Prabhakar, S. Pankanti, and A. K. Jain. Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*, 1(2):33–42, 2003.

[12] N. K. Ratha, J. H. Connell, and R. M. Bolle. An analysis of minutiae matching strength. In *Proc. 3rd AVBPA*, pages 223–228, 2001.

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

[14] K. Simoens, J. Bringer, H. Chabanne, and S. Seys. A framework for analyzing template security and privacy in biometric authentication systems. *IEEE Transactions on Information Forensics and Security*, 7(2):833–841, 2012.

[15] K. Simoens, P. Tuyls, and B. Preneel. Privacy weaknesses in biometric sketches. In *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, SP '09, pages 188–203, Washington, DC, USA, 2009. IEEE Computer Society.

[16] 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 *ICB*, pages 498–505, 2012.

[17] A. D. Smith. Maintaining secrecy when information leakage is unavoidable, 2001.

[18] P. Tuyls and J. Goseling. Capacity and examples of template-protecting biometric authentication systems. In *ECCV Workshop BioAW*, pages 158–170, 2004.

[19] F. Willems, T. Kalker, S. Baggen, and J. paul Linnartz. J.p.: On the capacity of a biometrical identification system. In *In: Proc. of the 2003 IEEE Int. Symp. on Inf. Theory*, pages 8–2, 2003.

[20] X. Zhou. Privacy and security assessment of biometric template protection. *it - Information Technology*, 54(4):197–, 2012.

[21] X. Zhou, A. Kuijper, R. Veldhuis, and C. Busch. Quantifying privacy and security of biometric fuzzy commitment. In *Proceedings of the 2011 International Joint Conference on Biometrics*, IJCB '11, pages 1–8, Washington, DC, USA, 2011. IEEE Computer Society.