ABSTRACT
In this paper we present a short overview of results that have been achieved on template protecting biometric authentication systems.

1. INTRODUCTION
The increasing demand for more reliable and convenient security systems generates a renewed interest in human identification based on biometric identifiers such as fingerprints, iris, voice and gait. Since biometrics cannot be lost or forgotten like e.g. computer passwords, biometrics have the potential to offer higher security and more convenience for the users.

A common approach to biometric authentication is to capture the biometric templates of all users during the enrollment phase and to store the templates in a reference database. During the authentication phase new measurements are matched against the database information.

The fact that biometric templates are stored in a database introduces a number of security and privacy risks. We identify the following threats.

1. Impersonation. An attacker steals templates from a database and constructs artificial biometrics that pass authentication.
2. Irrevokability. Once compromised, biometrics cannot be updated, reissued or destroyed.
3. Exposure of sensitive personal information.

The first threat was recognized by several authors [3, 11, 17]. When an authentication system is used on a large scale, the reference database has to be made available to many different verifiers, who, in general, cannot be trusted. Especially in a networked environment, attacks on the database pose a serious threat. It was shown explicitly by Matsumoto et al. [12] that template information stored in a database, can be abused to construct artificial biometrics meant to impersonate people. Construction of artificial biometrics is possible even if only part of the template is available. Hill [7] showed that if only minutiae templates of a fingerprint are available, it is still possible to successfully construct artificial biometrics that pass authentication. The second threat was first addressed by Schneier [19]. The problem is concisely paraphrased by: “Theft of biometrics is theft of identity.” The third threat is caused by the fact that biometrics contain sensitive personal information. It is shown in [2, 14, 16] that fingerprints contain certain genetic information. From [4] on the other hand it follows that retina scans reflect information about diseases like diabetes and strokes.

We present a general architecture that guarantees privacy protection of biometric templates. Examples of architectures that achieve protection of templates are private biometrics [6], fuzzy commitment [9], cancelable biometrics [18], fuzzy vault [8], quantizing secret extraction [10] and secret extraction from significant components [21].

All these systems are based on the use of a one-way transform to achieve protection of the biometric templates. The systems proposed in [6, 8–10, 21] are all based on the use of helper data. In this paper we discuss the principle behind all these systems, identify fundamental performance bounds and propose an algorithm that achieves these bounds.

2. MODEL AND DEFINITIONS

2.1 Security Assumptions
In this paper, we make the following security assumptions.

- Enrollment is performed at a trusted Certification Authority (CA).
- The database is vulnerable to attacks as well from the outside as from the inside (malicious verifier).
- During the authentication phase an attacker is able to present artificial biometrics at the sensor.
- All capturing and processing during authentication is tamper resistant and reveals no information.
- The communication channel between the sensor and the verification authority is assumed to be public and authenticated.

2.2 Biometrics
Biometric templates are processed measurement data, i.e. feature vectors. We model biometric templates as realizations of a random process. Biometrics of different individuals are independent realizations of a random process that is equal for all individuals. We assume that the processing of the biometrics results in templates that can be described by n independent identically distributed (i.i.d.) random variables with a known distribution $P_X$. Noisy measurements of biometrics are modelled as observations through a memoryless noisy channel, characterized by the conditional distribution $P_{Y|X}$. 
2.3 Secret Extraction Codes (SECs)

In order to deal with noisy measurements, we introduce the notion of Secret Extraction Codes (SECs). For a precise definition we refer to [20]. A SEC code is used to derive a secret S from a biometric Xn such that S can be reconstructed from Yn, a noisy version of Xn, during authentication. Loosely speaking, it is defined as a set of encoding regions that are surrounded by larger decoding regions. The size of the decoding regions is defined such that the secret S is correctly reconstructed during the authentication phase.

Note that SECs are strongly related to geometric codes [5]. Furthermore, when the encoding regions are points, the SECs are normal error correcting codes.

3. PROTECTION OF TEMPLATES

3.1 Requirements

The requirements for an architecture that does not suffer from the threats mentioned in the introduction are:

1. The reference information that is stored in the database does not give sufficient information to make successful impersonation possible.
2. The reference information reveals as little information as possible about the original biometrics, in particular it reveals no sensitive information.

Note that an architecture that meets those requirements, guarantees that the biometric cannot be compromised.

3.2 The Helper Data Architecture

The privacy protecting biometric authentication architecture that is proposed in [10,21] is inspired by the protection mechanism used for computer passwords. Passwords are stored in a computer system in a cryptographically hashed form. This makes it computationally infeasible to retrieve the password from the information stored in the database. During the authentication phase the same hash function is applied to the user input and matching is based on the equality of the hashed values. This approach, however, cannot be used for the protection of biometric templates in a straightforward way, because the measurements in the authentication phase are inherently noisy. Since small differences at the input of one-way functions result in completely different outputs, the hashed versions of the enrollment and the noisy authentication measurements will be different with high probability.

In order to combine biometric authentication with cryptographic techniques, we derive helper data during the enrollment phase. The helper data guarantees that a unique string can be derived from the biometrics of an individual as well during the authentication as during the enrollment phase. Since the helper data is stored in the database it should be considered publicly available. In order to prevent impersonation we need to derive reference data from the biometric that is statistically independent of the helper data. In order to keep the reference data secret for somebody having access to the database, we store the reference data in hashed form. In this way impersonation becomes computationally infeasible.

A schematic representation of the architecture described in this section is presented in Fig. 1.

During the enrollment phase a secret S, belonging to an alphabet $\mathcal{S} = \{1, 2, \ldots, |\mathcal{S}|\}$, is extracted from a sequence $X^n$. In order to guarantee robustness to noise, the CA derives helper data $W$ that will be used during the authentication phase to achieve noise robustness.

During the authentication phase a noisy version $Y^n$ of the enrollment sequence $X^n$ is obtained. Using the helper data $W$, which is provided to the verifier, a secret $V \in S$ is derived. The scheme is designed such that $V$ equals $S$ with high probability. Note that in contrast to usual biometric systems, we perform an exact match on $F(S)$ and $F(V)$.

The first requirement given in Section 3.1, is to prevent abuse of database information for impersonation. To this end the system is designed such that the mutual information between the helper data and the secret is sufficiently small and the secrets are uniformly distributed. Furthermore the set of secrets has to be sufficiently large to exclude an attack by exhaustive trial.

The helper data architecture was introduced as an architecture for verification; i.e. a situation in which an identity claim is verified. The helper data architecture can, however, also be used in an identification setting. In that case a biometric measurement is matched against the database information of all enrolled users. In the remaining part of this paper, algorithms will be proposed in a verification setting. The extension to the identification setting is left implicit.

3.3 Relation with Secret Extraction from Common Randomness

There is a strong relation between the protection of biometric templates and secret extraction from common randomness [1,13]. The term common randomness is used for the situation that two parties possess sequences of correlated random variables. The secret extraction problem arises when the parties want to extract a common secret from the correlated data by communicating over a public channel. As the communication channel is public, the secret extraction protocol has to be designed such that no information about the secret is revealed to an eavesdropper.

Fig. 2 gives an alternative representation of the situation that was already visualized in Fig. 1. In the case of biometrics a secret $S$ is derived from $X^n$ during the enrollment phase together with helper data $W$. During the authentication phase $Y^n$ a noisy version of $X^n$ (and hence correlated with $X^n$) is obtained and a secret $V$ is computed using the public helper data $W$. The helper data is designed such that $V$ equals $S$ with very high probability and such that no information on $S$ is revealed.

4. BOUNDS: SECRECY AND IDENTIFICATION CAPACITY

4.1 Secret Extraction

An important parameter of a template protecting biometric authentication system is the maximum size (bit length) of the secrets that can be achieved under the requirements,
stored in a database. In the authentication phase a noisy version
of the biometric template is captured. The helper data is used to derive a secret from the noisy version. If the authentication measurement matches, the authentication is successful.

![Figure 1](image1.png)

Figure 1: The proposed authentication architecture. In the enrollment phase, the biometric template $X^n$ is used for the derivation of a secret $S$ and helper data $W$. A hashed version $F(S)$ of the secret and the helper data $w$ are stored in a database. In the authentication phase a noisy version $Y^n$ of the biometric template is captured. The helper data $w$ is used to derive a secret $V$ from $Y^n$. If $F(S) = F(V)$, the authentication is successful.

![Figure 2](image2.png)

Figure 2: The sequence $X^n$ denotes the enrollment measurements and $Y^n$ the authentication measurements. The computed secrets $S$ and $V$ as well as the communication of the helper data is indicated.

1. During authentication and enrollment the same secret $S$ is derived with very high probability.
2. The helper data $W$ gives as little information as possible about $S$.

This quantity is called the secrecy capacity and denoted by $C_s$. For a precise definition we refer to [20].

The second requirement guarantees that impersonation becomes infeasible if $C_s$ is sufficiently large and the secrets are randomly chosen.

According to requirement 2 from Section 3.1, $I(W; X^n)$ should be small. It was proven in [21], that in order to guarantee correctness and a large number of secrets, the helper data $W$ should depend on the biometric template $X^n$. Hence $I(W; X^n)$ cannot be zero. In Section 5 we show, however, that it is possible to keep $I(W; X^n)$ small. More in particular, it will not be possible to derive from the helper data $W$ a good estimate of $X^n$. It was proven in [20] that $C_s = I(X; Y)$.

4.2 Biometric Identification

In the enrollment phase of an identification setting, a database is created with data from a set of $|M|$ enrolled users, each identified with an index $m \in \{1, 2, \ldots, |M|\}$. In the identification phase, a measurement $Y^n$ and the information in the database are used to find the identity of an unknown (but properly enrolled) individual $m$. The identifier output is denoted by $M$.

Reliability of the identification is expressed by the average error probability, assuming that the individual is chosen at random. Performance in terms of the number of users in the system is expressed by the rate $R$. The maximum number of users that can be reliably identified is given by the identification capacity $C_{id}$. For a precise definition, we refer again to [20].

It was proven in [15, 22] that all biometric identification systems satisfy $C_{id} = I(X; Y)$.

5. EXAMPLES

5.1 Secret Extraction from Significant Components

For a precise description of this construction we refer to [20] and [21].

In words it can be explained as follows. Given a vector $X^n$ of $n$ components we look for its large components, i.e. the components $i$ such that $|X_i| > \delta$, where $\delta > 0$. The idea is that those components can be encoded in such a manner that the decoding will not be perturbed by the noise. The encoding scheme works as follows: if $X_i$ is larger than zero then the $i$-th component of $S_i$ is set equal to one, otherwise if $X_i < 0$, $S_i = 0$. The helper data are given by a vector $W$ that indicates the large components of $X$ that have to be used for decoding during authentication. It was shown in [21] that this scheme is robust to noise and that the helper data reveals no information on the secret string $S$.

5.2 Secret Extraction on Discrete Biometrics

This example assumes that the biometric data can be modeled as sequences of binary random variables and that the measurement process is modeled as a binary symmetrical channel with cross-over probability $p$. The starting point is to choose a suitable error correcting code. From this error-correcting code, we construct a new set $C$ of error correcting codes (using appropriate helper data) such that each biometric is a codeword of one of the codes in $C$. The helper data is a pointer to the code in $C$ that has to be used for decoding.

It was shown in [20] that this scheme can achieve secrecy capacity equal to $\exp[n(1 - H(p) - \epsilon)]$ while being zero revealing ($I(W; S) = 0$). On the other hand $W$ reveals $n - \log |S|$ bits on $X^n$.

REFERENCES


