Full text available at: http://dx.doi.org/10.1561/0100000051

Biometric Security from an Information-Theoretical Perspective

Biometric Security from an Information-Theoretical Perspective

Tanya Ignatenko

Eindhoven University of Technology
Eindhoven
The Netherlands
t.ignatenko@ieee.org

Frans M.J. Willems

Eindhoven University of Technology
Eindhoven
The Netherlands
f.m.j.willems@tue.nl

the essence of knowledge

Boston – Delft

Foundations and Trends® in Communications and Information Theory

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
USA
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is T. Ignatenko and F. M. J. Willems, Biometric Security from an Information-Theoretical Perspective, Foundations and Trends® in Communications and Information Theory, vol 7, nos 2–3, pp 135–316, 2010

ISBN: 978-1-60198-522-4

Foundations and Trends® in Communications and Information Theory
Volume 7 Issues 2–3, 2010

Editorial Board

Editorial Scope

Foundations and Trends® in Communications and Information Theory will publish survey and tutorial articles in the following topics:

- Coded modulation
- Coding theory and practice
- Communication complexity
- Communication system design
- Cryptology and data security
- Data compression
- Data networks
- Demodulation and Equalization
- Denoising
- Detection and estimation
- Information theory and statistics
- Information theory and computer science
- Joint source/channel coding
- Modulation and signal design
- Multiuser detection
- Multiuser information theory
- Optical communication channels
- Pattern recognition and learning
- Quantization
- Quantum information processing
- Rate-distortion theory
- Shannon theory
- Signal processing for communications
- Source coding
- Storage and recording codes
- Speech and Image Compression
- Wireless Communications

Information for Librarians
Foundations and Trends® in Communications and Information Theory, 2010, Volume 7, 6 issues. ISSN paper version 1567-2190. ISSN online version 1567-2328. Also available as a combined paper and online subscription.

Foundations and Trends® in
Communications and Information Theory
Vol. 7, Nos. 2–3 (2010) 135–316

DOI: 10.1561/0100000051

now
the essence of knowledge

Biometric Security from an Information-Theoretical Perspective

Tanya Ignatenko[1] and Frans M.J. Willems[2]

[1] *Eindhoven University of Technology, Den Dolech 2, Eindhoven, The Netherlands, t.ignatenko@ieee.org*
[2] *Eindhoven University of Technology, Den Dolech 2, Eindhoven, The Netherlands, f.m.j.willems@tue.nl*

Abstract

In this review, biometric systems are studied from an information theoretical point of view. In the first part biometric authentication systems are studied. The objective of these systems is, observing correlated enrollment and authentication biometric sequences, to generate or convey as large as possible secret keys by interchanging a public message, while minimizing privacy leakage. Here privacy leakage is defined as the amount of information that this public message contains about the biometric enrollment sequence. In this setting also the secrecy leakage, that is, the amount of information the public message leaks about the secret key, should be negligible. Next identification biometric systems are investigated. These systems should be able to identify as many individuals as possible while being able to assign as large as possible secret keys to each individual and again minimize the privacy leakage. To realize these systems public reference data are stored in the database.

Leakage is defined with respect to these reference data. For all these biometric systems fundamental limits are determined in the current work. Finally, a popular practical construction for biometric systems, fuzzy commitment, is analyzed with respect to both its theoretical performance and performance related to the code choice.

Contents

1

Introduction

1.1 Access Control Systems and Biometrics

Nowadays people live in the era of large-scale computer networks connecting huge numbers of electronic devices. These devices execute applications that use networks for exchanging information. Sometimes the information that is transmitted within these networks and stored by the devices is sensitive to misuse. Moreover, the networks and devices cannot always be trusted. This can lead to intrusions into the privacy of users by, for example, hackers, commercial parties, or even by governmental institutions. Also illegal copying of copyrighted content, illegal use of e-payment systems, and identity theft can be foreseen. In order to prevent all such malicious actions the security of networks and devices should be adequate.

Traditional systems for access control, which are based on the possession of secret knowledge (passwords, secret keys, etc.) or on a physical token (ID card, smart-card, etc.), have the drawback that they cannot guarantee that it is the legitimate user who, for example, enters

a password or presents a smart-card. Moreover, passwords can often be guessed, since people tend to use passwords which are easy to remember. Physical tokens in their turn can be lost, stolen, or copied.

Biometric systems offer a solution to most of the problems mentioned above. They could be either substituted for traditional systems or used to reinforce them. Biometric systems are based on physical or behavioral characteristics of human beings, like faces, fingerprints, voice, irises, gait, see Jain et al. [39]. The results of the measurement of these characteristics are called biometric data. Biometric data have the advantage that potentially they are unique identifiers of human beings, as was argued by Clarke [13]. They provide therefore a closer bond with the identity of their owner than a password or a token does. Moreover, biometric data cannot be stolen or lost. They potentially contain a large amount of information and therefore are hard to guess. All this makes biometrics a good candidate for substitution of traditional passwords and secret keys. A drawback of using biometrics is that the outcome of their measurements is, in general, noisy due to intrinsic variability, varying measurement conditions, or due to the use of different hardware. However, advanced signal-processing and error-correcting techniques can be applied to guarantee reliable overall behavior.

The attractive property of uniqueness, that holds for biometrics, also results in its major weakness. Unlike passwords and secret keys, biometric information, if compromised once, cannot be canceled and easily replaced by other biometric information, since people only have limited resources of biometric data. Theft of biometric data results in a partially stolen identity, and this is, in principle, irreversible. Therefore requirements for biometric systems should include *secure storage* and *secure communication* of biometric data in the applications where they are used.

Although biometric data may provide solutions to the problems discussed above, there are situations when they cannot be used. There is, for example, a small percentage of people whose fingerprints cannot be used due to intrinsic bad quality, see Dorizzi [25]. Also DNA recognition fails for identical twins. In such situations combination with standard cryptographic tools is needed to provide additional security.

1.2 From Traditional Biometric Systems to Biometric Secrecy Systems

1.2.1 Traditional Biometric Systems

The terms "Biometrics" and "Biometry" have been used since the first part of the 20th century to refer to the field of development of statistical and mathematical methods applicable to data analysis problems in biological sciences [8]. Relatively recently the term "Biometrics" has also been used to refer to the field of technology devoted to automatic identification of individuals using biological traits, such as those based on retinal or iris scans, fingerprints, faces, signatures, etc. Such biological traits are unique for individuals as noted in Jain et al. [39].

Traditionally, biometric recognition was used in forensic applications and performed by human experts. However, recent advantages in automated recognition resulted in the spreading of biometric applications, now ranging from border control at airports to access control in Walt Disney amusement parks (see Wayman et al. [83]).

A typical biometric system is essentially a pattern-recognition system, which performs one or more identity checks based on specific physiological or behavioral characteristics possessed by individuals. There are two different ways to resolve an individual's identity, that is, authentication and identification. Authentication (Am I who I claim I to be?) involves confirming or denying the individual's claimed identity. In identification, one has to establish the individual's identity (Who am I?). Each of these approaches has its own characteristics and could probably be solved best by biometric systems.

All biometric technology systems have certain aspects in common. All are dependent upon an accurate reference or enrollment data. If a biometric system is to identify or to authenticate an individual, it first must have these reference data positively linked to the subject. Modern biometric identification systems, based on digital technologies, analyze personal physical attributes at the time of enrollment and distill from them a series of numbers. Once this reference sample or template is in the system, future attempts to identify an individual rest on comparing "live" data to the reference data.

A perfect system would always recognize an individual, and always reject an impostor. However, biometric data are gathered from individuals under environmental conditions that cannot always be controlled, over equipment that may slowly be wearing out, and using technologies and methods that vary in their level of precision. Consequently, an ideal behavior of biometric systems cannot be realized in practice. Traditionally, the probability that an authorized individual is rejected by a biometric system is called False Rejection Rate (FRR), and the probability that an unauthorized individual is accepted by a biometric system is called False Acceptance Rate (FAR). There are also other performance measures that characterize biometric systems. For a complete overview and similar issues see Jain et al. [39], Maltoni et al. [50], or Wayman et al. [83].

Although biometric technologies have their advantages when they are applied in access control systems, privacy aspects of biometric data should not be ignored. Identification and authentication require storage of biometric reference data in some way. However, people feel uncomfortable with supplying their biometric information to a huge number of seemingly secure databases for various reasons, since

- practice shows that one cannot fully trust implementations of secure algorithms by third parties. Even governmental organizations that are typically trusted by the majority of the population cannot always guarantee that important sensitive data are securely stored;
- databases might be attacked from inside, which allows an owner of a database to abuse biometric information, for example, by selling it to third parties;
- people have limited resources of biometric data, that can be conveniently used for access control. Therefore an "identity theft" of biometric information has much more serious implications than a "simple" theft of a credit card. In the latter case, one can simply block and replace this credit card, while biometric information cannot be easily revoked and replaced by other biometric information.

It is often argued that privacy need not be a real issue in biometric systems, since biometric data are not secret and can easily be captured (faces, irises) or left in public (fingerprints), see Schneier [64]. However, this information, unlike the reference data, is typically of low quality and therefore cannot be easily used for impersonation. Even if it was of good quality, which might be the case with faces, connecting it to the corresponding database is not always an easy task.

Another important point is, that obtaining biometric data of a specific person as well as any other secret information belonging to him, is always possible when sufficient effort is exerted. In contrast, compromising a database, requires a comparable effort, but then provides immediate access to the biometric data of large number of individuals. Therefore, it makes sense to concentrate on protecting the database. It would be ideal if, in case the database becomes public, the biometric reference data could not be recovered.

1.2.2 Types of Security

To assess cryptographic protocols, two notions of security are commonly used, that is, information-theoretical security and computational security.

Computationally secure protocols rely on such an assumption as hardness of mathematical problems, for example, factoring and taking discrete logarithms, and assume that an adversary has bounded computing power. However, hardness of a problem is sometimes difficult to prove, and in practice certain problems are "assumed" to be hard.

Protocols whose security does not rely on computational assumptions, that is, they are secure even when the adversary has unbounded computing power, are called unconditionally or information-theoretically secure. Information-theoretically secure protocols are more desirable, but not always achievable. Therefore, in practice, cryptographers mostly use computational security.

In this review, we will treat security from an information-theoretical point of view. The key mathematical concept on which information theory is built and which is also relevant for considering information-theoretical security, is entropy. The notion of entropy comes from

Shannon [67]. Entropy is a measure of the information contained in a random variable. Although there are a number of alternative entropy concepts, for example, Rényi and min-entropy (Rényi entropy of order 2) [62], and smooth Rényi entropy [61], we will only use the classical (Shannon) notion of entropy here. Another Shannon-type concept is that of mutual information. Mutual information measures by how much the entropy of the first random variable decreases if access to the second random variable is obtained, and this notion can be defined in terms of entropies. For the exact definitions, properties and their proofs of entropy and mutual information we refer to Shannon [67] or, for example, Cover and Thomas [15].

An interesting special case of information-theoretical security is perfect security. This concept was introduced by Shannon [68]. He defined a secrecy system to be perfect if the mutual information between plaintext M and ciphertext C satisfies

$$I(M;C) = 0, \tag{1.1}$$

i.e., if a ciphertext C, which is a function of a plaintext M and a secret key S, provides no information about the plaintext M, in other words, if C and M are statistically independent. Shannon proved that perfect secrecy can only be achieved when the key-entropy and plaintext-entropy satisfy

$$H(S) \geq H(M). \tag{1.2}$$

An example of a perfectly secure system is the one-time pad system, also referred to as the Vernam cipher [80]. In one-time pad, a binary plaintext is concealed by adding modulo-2 (XOR-ing) a random binary secret key.

In practice it is quite possible and common for a secrecy system to leak some information. Although such a system is not perfectly secure, it can be information-theoretically secure up to a certain level.

1.2.3 Biometric Secrecy Systems with Helper Data

A perfect system for a secure biometric access control has to satisfy three requirements. Biometric data have to be private, namely, the reference information stored in a database should not reveal the actual

biometric data. Reference data that are communicated from a database to a point where access can be granted have to be resilient to eavesdropping. Reference data stored in a database have to be resilient to guessing, that is, to brute-force attacks.

Consider a biometric authentication system. A simple naive approach to satisfy both the first and the second requirements would be to use the biometric data as a password in a UNIX-password authentication scheme. In such a scheme, a user possesses a password x that gives access to his account. There is a trusted server that stores some information $y = f(x)$ about the password. The user gains access to the account only if he enters the password x', such that $f(x') = y$. The scheme has the requirement that nobody can figure out the password x from y in any way other than by guessing. To fulfill this requirement, a UNIX-password scheme relies on one-way functions. A one-way function $f(\cdot)$ is a function that is easy to compute but "hard to invert," where "hard to invert" refers to the property that no probabilistic polynomial-time algorithm can compute a pre-image of $f(x)$ with a better than negligible probability when x is chosen at random.

Thus, if we would use the UNIX-password authentication scheme and apply a one-way function to the biometric data, the storage of biometric data in the clear would be circumvented. However, there are a number of problems that would arise if we use biometric data in the UNIX scheme. First, the security properties that are guaranteed by one-way functions rely on the assumption that x is truly uniform, while we know that biometric data are far from uniform, although they do contain randomness of course. Moreover, one-way functions, as all cryptographic primitives, require their entries to be exactly reproducible for positive authentication,[1] while biometric data measurements are almost never identical. Therefore additional processing (e.g., error-correction and compression) is needed to realize a biometric UNIX-like authentication scheme that can tolerate a reasonable amount of errors in biometric measurements and results in uniform entries to the one-way function. One way of operating would be to use a collection of error-correcting

[1] Positive authentication can also be a result of an entry that produces a collision. However, here we do not consider collisions, since this is a problem associated with the design of one-way functions and therefore beyond the scope of this review.

codes such that for each observed biometric enrollment template there is a code that contains this template as a codeword. The index to this code is then stored in the database as helper data. Upon observing the individual for a second time, the helper can then be used to retrieve the enrollment template from the authentication template. The error-correcting code should be strong enough to correct the errors between the enrollment and authentication templates. From this, we may conclude that error-correcting techniques and helper data can be applied to combat errors. Subsequently compression methods can be used to achieve almost uniform entries.

Now that we have argued that helper data could be used to create a reliable system, the question arises what requirements ideal helper data should satisfy. Since helper data need to be stored (and communicated) for authentication, it would be advantageous if they could be made publicly available without compromising or leaking any information about the data that are used to get access to the system. We say that secrecy leakage from the helper data has to be negligible. Note that these data could be obtained using a one-way function as in the UNIX-scheme, but better procedures may exist as well. On the other hand, the helper data should leak as little information as possible about the observed biometric enrollment template. This would reduce privacy-related problems. Note that it might be impossible to make this leakage negligible, since helper data should contain some information about the biometric data in order to set up a reliable system. It will become clear later in this review that a notion of secret-key sharing originated from Information Theory, see Ahlswede and Csiszár [2], will be essential in designing and analyzing biometric systems in which public helper data are used. For these secret-key sharing systems, the problem of maximizing the size of the extracted secrets (the data needed to get access) was solved. This provides the solution for our third requirement, resilience to guessing.

In what we have discussed up to now, we have always assumed that keys were obtained as a result of a one-way operation on a password or on a biometric template. A biometric system would however be more flexible if we could choose the keys ourselves. We will show that the helper-data construction will make this possible. Therefore in this

review, we will distinguish between generated-key systems and chosen-key systems. Sometimes their performance will not differ that much, but in other situations the differences can be dramatic.

1.2.4 Protocols

In this subsection, we discuss examples of protocols for biometric authentication. Then we present two generic biometric models that constitute a core of biometric authentication systems. We will focus on these models and their modifications in our investigations of authentication systems. Moreover, we also sketch a protocol for biometric identification.

1.2.4.1 Protocols for Biometric Authentication

Protocol A

One of the typical protocols for secure authentication, also shown in Figure 1.1, reads as follows.

During enrollment, the biometric data of a subject are captured and analyzed, and the template X^N is extracted. A secret S is chosen or generated from these data. Then the template X^N is linked to the

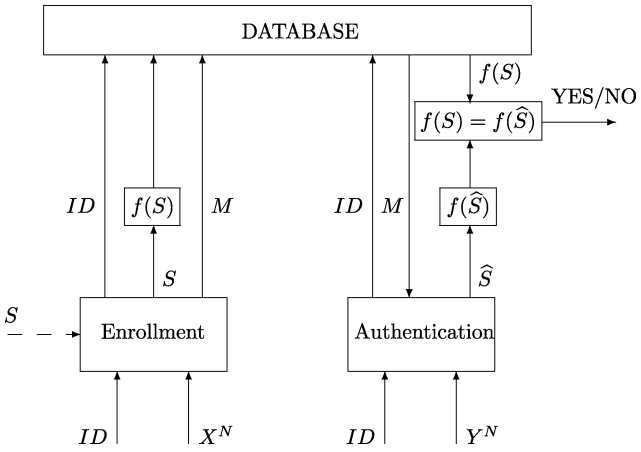

Fig. 1.1 Secure authentication. The dotted arrow indicates the possibility that the secret key is chosen, not generated from X^N.

key S via a helper message M. The key is encrypted using a one-way function and stored in a database as $f(S)$, together with an ID of the subject and the helper message M.

During authentication, the subject claims his ID. His biometric data are captured and preprocessed again, resulting in the template Y^N. The key $\widehat{S}$ is estimated based on Y^N and the helper message M that corresponds to the claimed ID. This estimated key is encrypted and then matched against the encrypted key $f(S)$ corresponding to the claimed ID. Only if $f(\widehat{S})$ is the same as $f(S)$ the subject is positively authenticated.

Protocol B

A variation of the first protocol is a protocol for biometric authentication with distributed storage. The first step of Protocol B is similar to the enrollment procedure in Protocol A. Here, however, the secret key is not stored anymore in the database, but on a smartcard. The startcard is given to the individual.

During authentication the subject provides a measurement of his biometrics. This measurement is preprocessed, resulting in a noisy template Y^N. The template and the helper message M are now used to derive a key $\widehat{S}$. The key $\widehat{S}$ is then compared to the secret key S on the smartcard.

1.2.4.2 Two Generic Settings

From the discussions above we may conclude that in order to design a good biometric secrecy system, we can focus on a number of generic structures, that is, models that constitute the core of any biometric secrecy system. These generic, secret-key sharing models can be subdivided into a class of models with generated keys, see Figure 1.2(a), and a class of models with chosen keys, see Figure 1.2(b). This subdivision also appears in the overview paper of Jain et al. [40]. In both models S is a randomly generated/chosen secret key, X^N and Y^N are biometric enrollment and authentication sequences having length N, M is a helper message, and $\widehat{S}$ is an estimated secret key. The channel between an encoder and decoder is assumed to be public. We only

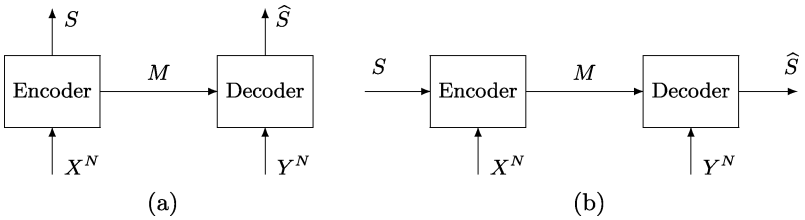

Fig. 1.2 Generic settings, generated and chosen keys.

assume that passive attacks are possible, namely, an attacker can see all public information but cannot change it. The information leakage is characterized in terms of mutual information, and the size of the secret keys in terms of entropy. The generic models must satisfy the following requirements

$$\begin{aligned} \Pr(S \neq \widehat{S}) &\approx 0 \quad \text{(reliability)}, \\ \frac{1}{N}H(S) &\approx \frac{1}{N}\log_2|\mathcal{S}| \quad \text{(secret uniformity)}, \\ \frac{1}{N}H(S) &\text{ is as large as possible} \quad \text{(secret-key rate)}, \\ \frac{1}{N}I(S;M) &\approx 0 \quad \text{(secrecy leakage)}, \\ \frac{1}{N}I(X^N;M) &\text{ is as small as possible} \quad \text{(privacy leakage)}. \end{aligned} \tag{1.3}$$

1.2.4.3 Protocol for Biometric Identification

A typical protocol for identification systems, see Figure 1.3 consists of the following steps.

During enrollment, the biometric data of $|\mathcal{V}|$ subjects are captured and analyzed, resulting into biometric templates $X^N(v), v = 1,2,\ldots,|\mathcal{V}|$. Based on these templates, secure templates or helper data $M(1), M(2),\ldots,M(|\mathcal{V}|)$ are extracted and then stored in the database together with the subjects IDs.

During identification, a subject presents his biometric data, which are captured and preprocessed again, resulting in the template Y^N. The identity label $\widehat{v}$ of the individual is estimated based on Y^N and all helper data $M(1), M(2),\ldots,M(|\mathcal{V}|)$ from the database. The result of this step is ID-label $\widehat{v}$ of the subject or "no found" error.

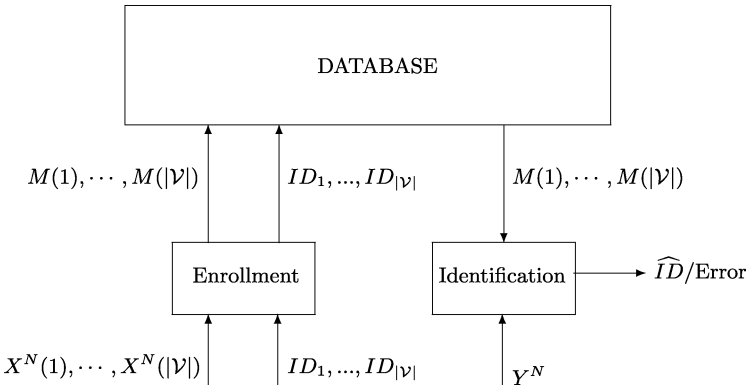

Fig. 1.3 Secure identification.

1.3 Modeling Biometric Data

Throughout this review, we will consider two types of biometric data. First we assume that our biometric sequences (feature vectors) are discrete, independent and identically distributed (i.i.d.). Fingerprints and irises can be modeled as such biometric sources. A discrete representation of other biometric modalities can be obtained using quantization. Then we also consider systems based on Gaussian i.i.d. biometric sequences. We may assume Gaussian biometric data distribution, since it is well-known that most transmission channels can be modeled as additive white Gaussian noise channels. The independence of biometric features is not unreasonable to assume, since Principal Components Analysis (PCA), Linear Discriminant Analysis (LDA) and other transforms, which are applied to biometric measurements during feature extraction (see Wayman et al. [83]) result in more or less independent features. In general, different components of biometric sequences may have different ranges of correlation. However, for reasons of simplicity we will only discuss i.i.d biometrics here. Finally, we assume that biometric sequences are aligned.

1.4 Related Work

Privacy concerns related to the use of biometric data in various secrecy systems were raised more than a two decade ago. Schneier [64] pointed

out that biometric data are not standard secret keys and cannot be easily canceled. Ratha et al. [60] investigated the vulnerability points of biometric secrecy systems. In Prabhakar et al. [56] security and privacy concerns were raised. Linnartz and Tuyls [48] looked at the problem of achieving biometric systems with no secrecy leakage. Finally, at the DSP forum [81] secrecy- and privacy-protecting technologies were discussed. The extent to which secrecy and privacy problems were investigated in literature also received attention there.

Considerable interest in the topic of biometric secrecy systems resulted in the proposal of various techniques. Recent developments in the area of biometric secrecy systems led to methods grouped around two classes: cancelable biometrics and "fuzzy encryption." Detailed summaries of these two approaches can be found in Uludag et al. [77] and in Jain et al. [40]. These works concentrate on biometric authentication systems.

It is the objective of cancelable biometrics, introduced by Ratha et al. [59, 60], Ang et al. [3], and Maiorana et al. [49], to avoid storage of reference biometric data in the clear in biometric authentication systems. These methods are based on non-invertible transformations that preserve the statistical properties of biometric data and rely on the assumption that it is hard to exactly reconstruct biometric data from the transformed data and applied transformation. However, hardness of a problem is difficult to prove, and, in practice, the properties of these schemes are assessed using brute-force attacks. Moreover, visual inspection shows that transformed data, for example, the distorted faces in Ratha et al. [59], still contain a lot of biometric information. Therefore, in this review we concentrate on the second class of systems.

The "fuzzy encryption" approach focuses on generation and binding of secret keys from/to biometric data. These secret keys are used to regulate access to, for example, sensitive data, services, and environments in key-based cryptographic applications and, in particular, in biometric authentication systems (all referred to as biometric secrecy systems). In biometric secrecy systems a secret key is generated/chosen during an enrollment procedure in which biometric data are observed for the first time. This key is to be reconstructed after these biometric data are observed again during an attempt to obtain access (authentication).

Since biometric measurements are typically noisy, reliable biometric secrecy systems also extract so-called helper data from the biometric observation at the time of enrollment. These helper data facilitate reliable reconstruction of the secret key in the authentication process. The helper data are assumed to be public, and therefore they should not contain information on the secret key. We say that the secrecy leakage should be negligible. Important parameters of a biometric secrecy system include the size of the secret key and the information that the helper data contain (leak) on the biometric observation. This latter parameter is called privacy leakage. Ideally the privacy leakage should be small, to avoid the biometric data of an individual to become compromised. Moreover, the secret-key length (also characterized by the secret-key rate) should be large to minimize the probability that the secret key is guessed and unauthorized access is granted.

Implementations of "fuzzy encryption" include methods based on various forms of Shamir's secret sharing [66]. These methods are used to harden passwords with biometric data (Monrose et al. [52, 53]). Methods based on error-correcting codes, that bind uniformly distributed secret keys to biometric data and that tolerate (biometric) errors in these secret keys, were formally defined by Juels and Wattenberg [43]. Less formal approaches can be found in Davida et al. [20, 21]. Error-correction based methods were extended to the set difference metric developed by Juels and Sudan [42]. Some other approaches focus on continuous biometric data and provide solutions which are based on quantization of biometric data as in Linnartz and Tuyls [48], Denteneer et al. [22] (with emphasis on reliable components), Teoh et al. [73], and Buhan et al. [10].

Finally, a formal approach for designing secure biometric systems for three metric distances (Hamming, edit and set), called fuzzy extractors, was introduced in Dodis et al. [24] and further elaborated in [23]. Dodis et al. [23, 24] were the first ones who addressed the problem of code construction for biometric secret-key generation in a systematic information-theoretical way. Although their works provide results on the maximum secret-key rates in biometric secrecy systems, they also give the corresponding results for the maximum privacy leakage. In biometric setting, however, the goal is to minimize the privacy leakage.

The need for quantifying the exact information leakage on biometric data was also stated as an open question in Sutcu et al. [70].

Another branch of work on "fuzzy encryption" focuses on combination of biometric and cryptographic keys. Methods in this direction include attempts to harden the fuzzy vault scheme of Juels and Sudan [42] with passwords by Nandakumar et al. [54] and dithering techniques that were proposed by Buhan et al. [9].

Recently, Prabhakaran and Ramchandran [57], and Gündüz et al. [30] studied source-coding problems where the issue of (biometric) leakage was addressed. In their work, though, it is not the intention of the users to produce a secret but to communicate a (biometric) source sequence in a secure way from the first to the second terminal.

From information-theoretical point of view biometric identification systems were studied by O'Sullivan and Schmid [55] and Willems et al. [87]. They derived the corresponding identification capacity, that is, the maximum number of individuals that a systems can reliably identify. They assumed, however, storage of the biometric enrollment sequences in the clear. Later Tuncel [74] analyzed the trade-off between the capacity of a biometric identification system and the space required to store the biometric templates. Tuncel's method realizes a kind of template protection.

1.5 Organization of This Review

In the current review, we study a number of problems related to the design of biometric secrecy systems for both authentication and identification.

First, in Section 2 we review the problem of secret sharing in order to set theoretical grounds for our investigation of secret-key rates and privacy leakage in biometric secrecy systems. In this section, we revisit the classical Ahlswede and Csiszár [1] and Maurer [51] problem of generating a secret from two dependent sequences but in the biometric setting. In this section, the biometric source is assumed to be discrete memoryless, however stationary ergodic biometric sources are also discussed there. Moreover, we investigated the question of which FRR and FAR can be achieved with biometric secret generation systems.

Next in Section 3 we continue to study secret-key rates and privacy leakage. We concentrate on biometric authentication systems. In this section we study a more general situation. One of the challenges in designing biometric secrecy systems is to minimize the privacy leakage for a given secret-key rate. Therefore, in Section 3, we focus on finding the fundamental trade-off between secret-key rates and privacy leakage for a number of biometric models. In this section we assume that our biometric source is discrete memoryless. In Section 4 we extend the results found in Section 3 to the Gaussian biometric sources.

The following section, Section 5, is devoted to biometric identification systems with protected templates. Since biometric data are typically used for both identification and authentication purposes, we determine there the trade-off between identification, secret-key and privacy-leakage rates. In this section we again assume our biometric source and channel to be discrete memoryless.

Next we turn to practical constructions. In Section 6 a popular realization of binary biometric authentication systems with chosen secret keys, called fuzzy commitment [43], is analyzed. There we present theoretical performance analysis of the scheme. The following section investigates how binary quantization of biometric sequences influences the performance of biometric secrecy systems with respect to secret-key rates and privacy leakage. Also there we study the effect of the code choice and binary quantization in fuzzy commitment.

Section 8 concludes this review and present some discussions on the future directions in the area of biometric secrecy systems.

References

[1] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography — part I: Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, pp. 1121–1132, July 1993.

[2] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography — part II: CR capacity," *IEEE Transactions on Information Theory*, vol. 44, pp. 225–240, January 1998.

[3] R. Ang, R. Safavi-Naini, and L. McAven, "Cancelable key-based fingerprint templates," in *ACISP*, pp. 242–252, 2005.

[4] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," in *IEEE International Symposium on Information Theory*, Trondeheim, Norway, 1994.

[5] T. Berger, "Multiterminal source coding, *the information theory approach to communications*," in *CISM Courses and Lectures*, vol. 229, (G. Longo, ed.), pp. 171–231, Springer-Verlag, 1978.

[6] P. Bergmans, "A simple converse for broadcast channels with additive white gaussian noise (corresp.)," *IEEE Transactions on Information Theory*, vol. 20, no. 2, pp. 279–280, March 1974.

[7] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error–correcting coding and decoding: Turbo-codes," vol. 2, pp. 1064–1070, May 1993.

[8] *BIOMETRICS, Journal of the International Biometric Society.*

[9] I. Buhan, J. Doumen, and P. Hartel, "Controlling leakage of biometric information using dithering," in *EUSIPCO*, 2008.

[10] I. Buhan, J. Doumen, P. H. Hartel, Q. Tang, and R. N. J. Veldhuis, "Embedding renewable cryptographic keys into continuous noisy data," in *ICICS*, pp. 294–310, 2008.

[11] P. Campisi, E. Maiorana, M. Prats, and A. Neri, "Adaptive and distributed cryptography for signature biometrics protection," in *SPIE Conference on Security, Steganography and Water-Making of Multimedia Contents IX*, vol. 6505, San Jose, CA, 2007.

[12] C. Chen, R. Veldhuis, T. Kevenaar, and A. Akkermans, "Multi-bits biometric string generation based on the likelihood ratio," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Workshop on Biometrics*, pp. 1–7, Anchorage, Alaska, US, June 24–28 2008.

[13] R. Clarke, "Human identification in information systems: Management challenges and public policy issues," *Information Technology and People*, vol. 7, no. 4, pp. 6–37, 1994.

[14] T. Cover, "A proof of the data compression theorem of Slepain and Wolf for ergodic sources," *IEEE Transactions on Information Theory*, vol. 22, pp. 226–228, March 1975.

[15] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: John Wiley and Sons Inc., 2nd ed., 2006.

[16] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. New York: Academic, 1982.

[17] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 344–366, 2000.

[18] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3047–3061, December 2004.

[19] J. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148–1161, November 1993.

[20] G. Davida, Y. Frankel, and B. Matt, "On enabling secure applications through off-line biometric identification," in *Proceedings of the IEEE 1998 Symposium on Security and Privacy*, 1998.

[21] G. Davida, Y. Frankel, and B. Matt, "On the relation of error correction and cryptography to an off-line biometric based identification scheme," in *Proceedings of WCC99, Workshop on Coding and Cryptography*, 1999.

[22] D. Denteneer, J. Linnartz, P. Tuyls, and E. Verbitskiy, "Reliable (robust) biometric authentication with privacy protection," in *Proceedings of IEEE Benelux Symposium on Information Theory*, Veldhoven, The Netherlands, 2003.

[23] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM Journal on Computing*, vol. 38, no. 1, pp. 97–139, 2008.

[24] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Advances in Cryptology — Eurocrypt*, 2004.

[25] B. Dorizzi, "Biometrics at the frontiers, assessing the impact on society, technical impact of biometrics," European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE), Technical Report, 2005.

[26] S. C. Draper, A. Khisti, E. Martinian, A. Vetro, and J. S. Yedidia, "Using distributed source coding to secure fingerprint biometrics," in *IEEE International Conference on Acoustics, Speech and Signal Processing*, vol. 2, pp. 129–132, 2007.

[27] G. D. Forney, "Information theory," 1972, course notes (unpublished), Stanford University.

[28] R. Gallager, *Information Theory and Reliable Communcation*. New York: Wiley, 1968.

[29] R. G. Gallager, "Low density parity check codes," *IRE Transactions on Information Theory*, vol. 8, pp. 21–28, January 1962.

[30] D. Gündüz, E. Erkip, and H. V. Poor, "Secure lossless compression with side information," in *Proceedings of the IEEE Information on Theory Workshop*, Porto, Portugal, 2008.

[31] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081–1088, 2006.

[32] S.-W. Ho, "On the interplay between shannon's information measures and reliability criteria," in *IEEE International Symposium on Information Theory (ISIT)*, pp. 154–158, Seoul, Korea, June 28–July 3 2009.

[33] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. New York, NY, USA: Cambridge University Press, 2003.

[34] T. Ignatenko, "Secret-key rates and privacy leakage in biometric systems," Ph.D. dissertation, Eindhoven University of Technology, 2009.

[35] T. Ignatenko and F. Willems, "Achieving secure fuzzy commitment scheme for optical PUFs," in *Proceedings of the International Conference on Intelligent Information on Hiding and Multimedia Signal Processing, September 12–14, 2009, Kyoto, Japan*, pp. 1185–1188, 2009.

[36] T. Ignatenko and F. Willems, "Biometric systems: Privacy and secrecy aspects," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 4, December 2009.

[37] T. Ignatenko and F. Willems, "Fundamental limits for biometric identification with a database containing protected templates," in *Proceedings of the IEEE International Symposium on Information Theory and its Applications (ISITA)*, Taichung, Taiwan, October 17–20 2010.

[38] T. Ignatenko and F. Willems, "Secret-key and identification rates for biometric identification systems with protected templates," in *Proceedings of Symposium on Information on Theory in the Benelux*, pp. 337–348, Rotterdam, The Netherlands, May 11–12 2010.

[39] A. Jain, R. Bolle, and S. Pankanti, eds., *Biometrics: Personal Identification in a Networked Society*. Kluwer Academic Publishers, 1999.

[40] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, 2008.

[41] R. Johannesson and K. S. Zigangirov, *Fundamentals of Convolutional Coding*. Wiley-IEEE Press, 1999.

[42] A. Juels and M. Sudan, "A fuzzy vault scheme," in *IEEE International Symposium on Information Theory*, p. 408, 2002.

[43] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *ACM Conference on Computer and Communications Security*, pp. 28–36, 1999.

[44] E. Kelkboom, G. G. Molina, T. Kevenaar, R. Veldhuis, and W. Jonker, "Binary biomterics: An analytic framework to estimate the bit error probability under gaussian assumption," in *IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS)*, pp. 1–6, September–October 2008.

[45] T. A. M. Kevenaar, G. J. Schrijen, M. van der Veen, A. H. M. Akkermans, and F. Zuo, "Face recognition with renewable and privacy preserving binary templates," in *AutoID*, pp. 21–26, 2005.

[46] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy-security tradeoffs in reusable biometric security system," in *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Dallas, TX, March 2010.

[47] Q. Li, Y. Sutcu, and N. Memon, "Secure sketch for biometric templates," in *Asiacrypt, LNCS*, vol. 4284, Shanghai, China, December 2006.

[48] J.-P. M. G. Linnartz and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates," in *AVBPA*, pp. 393–402, 2003.

[49] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia, and A. Neri, "Template protection for HMM-based on-line signature authentication," in *Computer Vision and Pattern Recognition Works, IEEE Computer Society Conference*, pp. 1–6, June 2008.

[50] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. New York: Springer, 2003.

[51] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, pp. 733–742, May 1993.

[52] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel, "Cryptographic key generation from voice," in *IEEE Symposium on Security and Privacy*, pp. 202–213, 2001.

[53] F. Monrose, M. K. Reiter, and S. Wetzel, "Password hardening based on keystroke dynamics," in *ACM Conference on Computer and Communications Security*, pp. 73–82, 1999.

[54] K. Nandakumar, A. Nagar, and A. Jain, "Hardening fingerprint fuzzy vault using password," in *ICB07*, pp. 927–937, 2007.

[55] J. A. O'Sullivan and N. A. Schmid, "Large deviations performance analysis for biometrics recognition," in *Proceedings of Annual Allerton Conference on Communication, Control, and Computing*, Allerton House Monticello, IL, USA, October 2–4 2002.

[56] S. Prabhakar, S. Pankanti, and A. Jain, "Biometric recognition: Security and privacy concerns," *Security and Privacy, IEEE*, vol. 1, no. 2, pp. 33–42, March–April 2003.

[57] V. Prabhakaran and K. Ramchandran, "On secure distributed source coding," *IEEE Information on Theory Workshop*, pp. 442–447, September 2007.

[58] J. Proakis, *Digital Communications*. McGraw-Hill, 4th ed., (Int.), 2001.

[59] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 561–572, April 2007.

[60] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[61] R. Renner and S. Wolf, "Smooth Renyi entropy and its properties," in *IEEE International Symposium on Information Theory (ISIT)*, 2004.

[62] A. Rényi, "On measures of entropy and information," in *Proceedings of Berkeley Symposium on Mathematics Statistics and Probability*, vol. 1, pp. 547–561, 1961.

[63] N. A. Schmid and J. A. O'Sullivan, "Performance prediction methodology for biometric systems using a large deviations approach," *IEEE Transactions on Signal Processing*, vol. 52, no. 10, pp. 3036–3045, October 2004.

[64] B. Schneier, "Inside risks: The uses and abuses of biometrics," *Communications of the ACM*, vol. 42, no. 8, p. 136, 1999.

[65] S. Shamai and A. Wyner, "A binary analog to the entropy-power inequality," *IEEE Transactions on Information Theory*, vol. 36, no. 6, pp. 1428–1430, November 1990.

[66] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612–613, 1979.

[67] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, pp. 623–656, 1948.

[68] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[69] A. Smith, "Maintaining secrecy when information leakage is unavoidable," Ph.D. Dissertation, MIT, 2004.

[70] Y. Sutcu, Q. Li, and N. Memon, "How to protect biometric templates," in *SPIE Conference on Security, Steganography and Water-making of Multimedia Contents IX*, vol. 6505, 2007.

[71] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric templates with sketch: Theory and practice," *IEEE Transactions on Information Forensic and Security*, vol. 2, no. 3, pp. 503–512, September 2007.

[72] Y. Sutcu, S. Rane, J. Yedidia, S. Draper, and A. Vetro, "Feature extraction for a slepian-wolf biometric system using ldpc codes," in *IEEE International Symposium on Information Theory (ISIT)*, pp. 2297–2301, Toronto, Canada, July 6–11 2008.

[73] A. Teoh, A. Goh, and D. Ngo, "Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 1892–1901, 2006.

[74] E. Tuncel, "Capacity/storage tradeoff in high-dimensional identification systems," pp. 1929–1933, July, 2006.

[75] P. Tuyls, A. Akkermans, T. Kevenaar, G.-J. Schrijen, B. A, and R. Veldhuis, "Practical biometric authentication with template protection," in *International Conference on Audio- and Video-Based Personal Authentication (AVBPA)*, pp. 436–446, 2005.

[76] P. Tuyls and J. Goseling, "Capacity and examples of template-protecting biometric authentication systems," in *ECCV Workshop BioAW*, pp. 158–170, 2004.

[77] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948–960, 2004.

[78] S. Verdu and D. Guo, "A simple proof of the entropy power inequality," *IEEE Transactions on Information Theory*, vol. 52, no. 5, pp. 2165–2166, May 2006.

[79] S. Verdu and T. S. Han, "A general formula for channel capacity," *IEEE Transactions on Information Theory*, vol. 40, no. 4, pp. 1147–1157, July 1994.

[80] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Journal of the IEEE*, vol. 55, pp. 109–115, 1926.

[81] A. Vetro, (moderator), contributors: A. K. Jain, R. Chellappa, S. C. Draper, N. Memon, and P. J. Phillips, "Forum on signal processing for biometric systems," *IEEE Signal Processing Magazine*, vol. 24, no. 6, pp. 146–152, November 2007.

[82] A. J. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," *IEEE Transactions on Information Theory*, vol. 13, pp. 260–269, April 1967.

[83] J. Wayman, A. Jain, and D. Maltoni, eds., *Biometric Systems: Technology, Design and Performance Evaluation*. London: Springer-Verlag, 2005.

[84] F. Willems, "Coding theorem for the AWGN channel in terms of jointly typical sequences," in *Symposium on Information Theory in the Benelux*, pp. 13–18, Houthalen, Belgium, May 25 & 26 1989.

[85] F. Willems and T. Ignatenko, "Fundamental limits for biometric identification with a database containing protected templates," in *Proceedings of the IEEE Workshop on Information Forensics and Security*, pp. 1185–1188, Seattle, U.S.A., December 12–15 2010.

[86] F. Willems and T. Ignatenko, "Identification and secret-key generation in biometric systems with protected templates," in *Proceedings of the ACM Workshop on Multimedia and Security*, pp. 63–66, Rome, Italy, 2010.

[87] F. Willems, T. Kalker, J. Goseling, and J.-P. Linnartz, "On the capacity of a biometrical identification system," in *Proceedings of 2003 IEEE International Symposium on Information Theory*, 2003.

[88] F. M. J. Willems and T. Ignatenko, "Quantization effects in biometric systems," in *Proceedings of Workshop ITA (Information Theory and its Applications), 8–13 February 2009*, San Diego, CA, USA, 2009.

[89] J. Wolfowitz, *Coding Theorems of Information Theory*. Berlin: Springer-Verlag, 1961.

[90] A. Wyner and J. Ziv, "A theorem on the entropy of certain binary sequences and applications–I," *IEEE Transactions on Information Theory*, vol. 19, no. 6, pp. 769–772, November 1973.

[91] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Transactions on Information Theory*, vol. 22, no. 1, pp. 1–10, January 1976.

[92] S. Yang and I. Verbauwhede, "Secure iris verification," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, vol. 2, pp. 133–136, 2007.

[93] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from gaussian random variables," in *IEEE International Symposium on Information Theory (ISIT)*, pp. 2593–2597, Seattle, USA, July 9–14 2006.