EURASIP Journal on Information Security
a SpringerOpen Journal

RESEARCH Open Access

A survey on biometric cryptosystems and cancelable biometrics

Christian Rathgeb* and Andreas Uhl

Abstract

Form a privacy perspective most concerns against the common use of biometrics arise from the storage and misuse of biometric data. Biometric cryptosystems and cancelable biometrics represent emerging technologies of biometric template protection addressing these concerns and improving public confidence and acceptance of biometrics. In addition, biometric cryptosystems provide mechanisms for biometric-dependent key-release. In the last years a significant amount of approaches to both technologies have been published. A comprehensive survey of biometric cryptosystems and cancelable biometrics is presented. State-of-the-art approaches are reviewed based on which an in-depth discussion and an outlook to future prospects are given.

Keywords: biometrics, cryptography, biometric cryptosystems, cancelable biometrics, biometric template protection

1. Introduction

The term biometrics is defined as "*automated recognition of individuals based on their behavioral and biological characteristics*" (ISO/IEC JTC1 SC37). Physiological as well as behavioral biometric characteristics are acquired applying adequate sensors and distinctive features are extracted to form a biometric template in an enrollment process. At the time of verification or identification (identification can be handled as a sequence of verifications and screenings) the system processes another biometric input which is compared against the stored template, yielding acceptance or rejection [1]. It is generally conceded that a substitute to biometrics for positive identification in integrated security applications is non-existent. While the industry has long claimed that one of the primary benefits of biometric templates is that original biometric signals acquired to enroll a data subject cannot be reconstructed from stored templates, several approaches [2,3] have proven this claim wrong. Since biometric characteristics are largely immutable, a compromise of biometric templates results in permanent loss of a subject's biometrics. Standard encryption algorithms do not support a comparison of biometric templates in encrypted domain and, thus, leave biometric templates exposed during every authentication attempt [4] (homomorphic and asymmetric encryption, e.g., in [5-7], which enable a biometric comparison in encrypted domain represent exceptions). Conventional cryptosystems provide numerous algorithms to secure any kind of crucial information. While user authentication is based on possession of secret keys, key management is performed introducing a second layer of authentication (e.g., passwords) [8]. As a consequence, encrypted data inherit the security of according passwords applied to release correct decrypting keys. Biometric template protection schemes which are commonly categorized as biometric cryptosystems (also referred to as helper data-based schemes) and cancelable biometrics (also referred to as feature transformation) are designed to meet two major requirements of biometric information protection (ISO/IEC FCD 24745):

- *Irreversibility*: It should be computationally hard to reconstruct the original biometric template from the stored reference data, i.e., the protected template, while it should be easy to generate the protected biometric template.
- *Unlinkability*: Different versions of protected biometric templates can be generated based on the same biometric data (renewability), while protected templates should not allow cross-matching (diversity).

* Correspondence: crathgeb@cosy.sbg.ac.at
Multimedia Signal Processing and Security Lab (Wavelab), Department of Computer Sciences, University of Salzburg, A-5020 Salzburg, Austria

"*Biometric cryptosystems (BCSs) are designed to securely bind a digital key to a biometric or generate a digital key from a biometric*" [9] offering solutions to biometric-dependent key-release and biometric template protection [10,11]. Replacing password-based key-release, BCSs brings about substantial security benefits. It is significantly more difficult to forge, copy, share, and distribute biometrics compared to passwords [1]. Most biometric characteristics provide an equal level of security across a user-group (physiological biometric characteristics are not user selected). Due to biometric variance (see Figure 1), conventional biometric systems perform "fuzzy comparisons" by applying decision thresholds which are set up based on score distributions between genuine and non-genuine subjects. In contrast, BCSs are designed to output stable keys which are required to match a 100% at authentication. Original biometric templates are replaced through biometric-dependent public information which assists the key-release process.

"*Cancelable biometrics (CB) consist of intentional, repeatable distortions of biometric signals based on transforms which provide a comparison of biometric templates in the transformed domain*" [12]. The inversion of such transformed biometric templates must not be feasible for potential imposters. In contrast to templates protected by standard encryption algorithms, transformed templates are never decrypted since the comparison of biometric templates is performed in transformed space which is the very essence of CB. The application of transforms provides irreversibility and unlinkability of biometric templates [9]. Obviously, CB are closely related to BCSs.

As both technologies have emerged rather recently and corresponding literature is dispersed across different publication media, a systematic classification and in-depth discussion of approaches to BCS and CB is given. As opposed to existing literature [4,8], which intends to review BCSs and CB at coarse level, this article provides the reader with detailed descriptions of all existing key concepts and follow-up developments. Emphasis is not only placed on biometric template protection but on cryptographic aspects. Covering the vast majority of published approaches up to and including the year 2010 this survey comprises a valuable collection of references based on which a detailed discussion (including performance rates, applied data sets, etc.) of the state-of-the-art technologies is presented and a critical analysis of open issues and challenges is given.

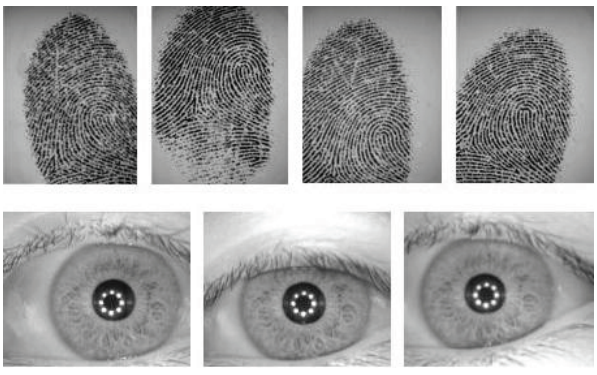

Figure 1 Biometric variance (images taken from FVC'04 and CASIAv3-interval database).

This survey is organized as follows: BCSs (Section 2) and CB (Section 3) are categorized and concerning literature is reviewed in detail. A comprehensive discussion including the current state-of-the-art approaches to both technologies, security risks, privacy aspects, and open issues and challenges is presented and concluding remarks are given (Section 4).

2. Biometric Cryptosystems

The majority of BCSs require the storage of biometric-dependent public information, applied to retrieve or generate keys, which is referred to as helper data [4]. Due to biometric variance it is not feasible for most biometric characteristics to extract keys directly. Helper data, which must not reveal significant information about original biometric templates, assists in reconstructing keys. Biometric comparisons are performed indirectly by verifying key validities, where the output of an authentication process is either a key or a failure message. Since the verification of keys represents a biometric comparison in encrypted domain [11], BCSs are applied as a means of biometric template protection [4], in addition to providing biometric-dependent key-release. Based on how helper data are derived, BCSs are classified as key-binding or key-generation systems (see Figure 2):

(1) *Key-binding schemes*: Helper data are obtained by binding a chosen key to a biometric template. As a result of the binding process a fusion of the secret key and the biometric template is stored as helper data. Applying an appropriate key retrieval algorithm, keys are obtained from the helper data at authentication [8]. Since cryptographic keys are independent of biometric features these are revocable while an update of the key usually requires re-enrollment in order to generate new helper data.
(2) *Key-generation schemes*: Helper data are derived only from the biometric template. Keys are directly generated from the helper data and a given biometric sample [4]. While the storage of helper data are not obligatory the majority of proposed key-generation schemes does store helper data (if key-generation

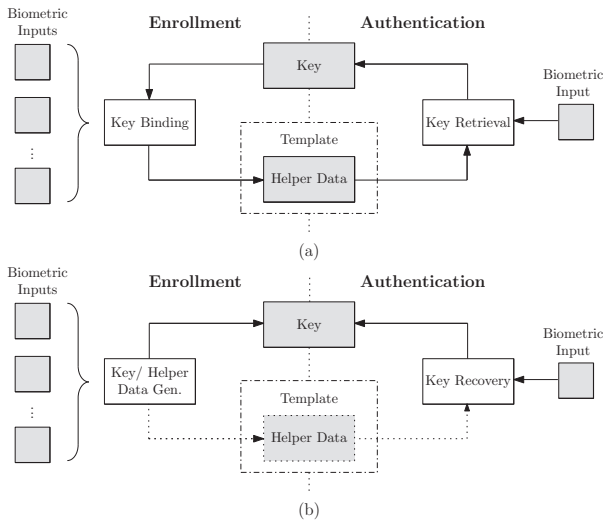

Figure 2 The basic concept of biometric (a) key-binding and (b) key-generation.

schemes extract keys without the use of any helper data these are not updatable in case of compromise). Helper data-based key-generation schemes are also referred to as "fuzzy extractors" or "secure sketches", for both primitives formalisms (and further extensions) are defined in [13,14]. A fuzzy extractor reliably extracts a uniformly random string from a biometric input while stored helper data assist the reconstruction. In contrast, in a secure sketch, helper data are applied to recover the original biometric template.

Several concepts of BCSs can be applied as both, key-generation and key-binding scheme [15,16]. Hybrid approaches which make use of more basic concepts [17] have been proposed, too. Furthermore, schemes which declare different goals such as enhancing the security of an existing secret [18,19] have been introduced. In contrast to BCSs based on key-binding or key-generation, key-release schemes represent a loose coupling of biometric authentication and key-release [8]. In case of successful biometric authentication a key-release mechanism is initiated, i.e., a cryptographic key is released. The loose coupling of biometric and cryptographic systems allows to exchange both components easily. However, a great drawback emerges, since the separate plain storage of biometric templates and keys offers more vulnerabilities to conduct attacks. Key-release schemes do not meet requirements of biometric template protection and, thus, are hardly appropriate for high security applications and not usually considered a BCS. Another way to classify BCSs is to focus on how these systems deal with biometric variance. While some schemes apply error correction codes [15,16], others introduce adjustable filter functions and correlation [20] or quantization [21,22].

Even though definitions for "biometric keys" have been proposed (e.g., in [23,24]), these terms have established as synonyms for any kind of key dependent upon biometrics, i.e., biometric features take influence on the constitution of keys (as opposed to key-binding schemes). Like conventional cryptographic keys, biometric keys have to fulfill several requirements, such as key-randomness, stability, or uniqueness [25,26].

A. Performance measurement

When measuring the performance of biometric systems widely used factors include False Rejection Rate (FRR), False Acceptance Rate (FAR), and Equal Error Rate (EER) [1,27] (defined in ISO/IEC FDIS 19795-1). As score distributions overlap, FRR and FAR intersect at a certain point, defining the EER of the system (in general, decreasing the FRR increases the FAR and vice versa).

These performance metrics are directly transferred to key-release schemes. In the context of BCSs the meaning of these metrics change since threshold-based "fuzzy comparison" is eliminated. Within BCSs acceptance requires the generation or retrieval of hundred percent correct keys, while conventional biometric systems response with "Yes" or "No". The fundamental difference between performance measurement in biometric systems and BCSs is illustrated in Figure 3. The FRR of a BCS defines the rate of incorrect keys untruly generated by the system, that is, the percentage of incorrect keys returned to genuine users (correct keys are user-specific and associated with according helper data). By analogy, the FAR defines the rate of correct keys untruly generated by the system, that is, the percentage of correct keys returned to non-genuine users. A false accept corresponds to the an untrue generation or retrieval of keys associated with distinct helper data at enrollment.

Compared to biometric systems, BCSs generally reveal a noticeable decrease in recognition performance [8]. This is because within BCS in most cases the enrolled

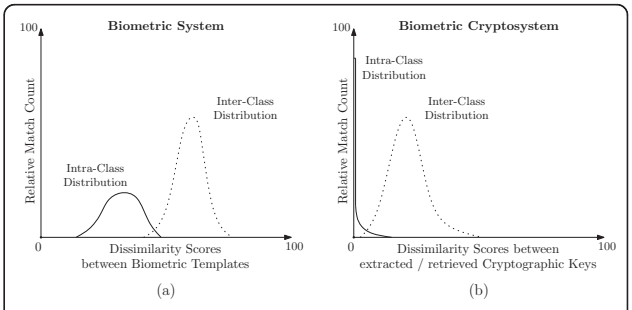

Figure 3 Performance measurement in (a) biometric systems and (b) BCSs.

template is not seen and, therefore, cannot be aligned properly at comparison. In addition, the majority of BCSs introduce a higher degree of quantization at feature extraction, compared to conventional biometric systems, which are capable of setting more precise thresholds to adjust recognition rates.

B. Approaches to biometric key-binding

1) Mytec1 and Mytec2 (Biometric Encryption™)

The first sophisticated approach to biometric key-binding based on fingerprints was proposed by Soutar et al. [28-30]. The presented system was called Mytec2, a successor of Mytec1 [20], which was the first BCS but turned out to be impractical in terms of accuracy and security. Mytec1 and Mytec2 were originally called Biometric Encryption™, the trademark was abandoned in 2005. The basis of the Mytec2 (and Mytec1) algorithm is the mechanism of correlation.

Operation mode (see Figure 4): at enrollment a filter function, $H(u)$, is derived from $f_0(x)$, which is a two-dimensional image array (0 indicates the first measurement). Subsequently, a correlation function $c(x)$ between $f_0(x)$ and any other biometric input $f_1(x)$ obtained during verification is defined by $c(x) = FT^{-1}\{F_1(u)F_0^*(u)\}$, which is the inverse Fourier transform of the product of the Fourier transform of a biometric input, denoted by $F_1(u)$, and $F_0^*(u)$, where $F_0^*(u)$ is represented by $H(u)$. The output $c(x)$ is an array of scalar values describing the degree of similarity. To provide distortion tolerance, the filter function is calculated using a set of T training images $\{f_0^1(x), f_0^2(x), \ldots, f_0^T(x)\}$. The output pattern of $f_0^t(x)$ is denoted by $c_0^t(x)$ with its Fourier transform $F_0^t(u)H(u)$. The complex conjugate of the phase component of $H(u)$, $e^{i\varphi}(H(u))$, is multiplied with a random phase-only array of the same size to create a secure filter, $H_{stored}(u)$, which is stored as part of the template while the magnitude of $H(u)$ is discarded. The output pattern $c_0(x)$ is then linked with an N-bit cryptographic key k_0 using a linking algorithm: if the n-th bit of k_0 is 0 then L locations of the selected part of $c_0(x)$ which are 0 are chosen and the indices of the locations are written into the n-th column of a look-up table which is stored as part of the template, termed BioScrypt. During linking, redundancy is added by applying a repetitive code. Standard hashing algorithms are used to compute a hash of k_0, termed id_0 which is stored as part of the template, too. During authentication a set of biometric images is combined with $H_{stored}(u)$ to produce an output pattern $c_1(x)$. With the use of the look-up table an appropriate retrieval algorithm calculates an N-bit key k_1 extracting the constituent bits of the binarized output pattern. Finally, a hash id_1 is calculated and tested against id_0 to check the validity of k_1.

The algorithm was summarized in a patent [31], which includes explanations of how to apply the algorithm to other biometric characteristics such as iris. In all the publications, performance measurements are omitted.

2) Fuzzy commitment scheme

In 1999 Juels and Wattenberg [15] combined techniques from the area of error correcting codes and cryptography to achieve a type of cryptographic primitive referred to as fuzzy commitment scheme.

Operation mode (see Figure 5): A fuzzy commitment scheme consists of a function F, used to commit a codeword $c \in C$ and a witness $x \in \{0, 1\}^n$. The set C is a set of error correcting codewords c of length n and x represents a bitstream of length n, termed witness (biometric data). The difference vector of c and x, $\delta \in \{0, 1\}^n$, where $x = c + \delta$, and a hash value $h(c)$ are stored as the commitment termed $F(c, x)$ (helper data). Each x', which is sufficiently "close" to x, according to an appropriate metric, should be able to reconstruct c using the difference vector δ to translate x' in the direction of x. A hash of the result is tested against $h(c)$. With respect to biometric key-binding the system acquires a witness x at enrollment, selects a codeword $c \in C$, calculates and stores the commitment $F(c, x)$ (δ and $h(c)$). At the time of authentication, a witness x' is acquired and the system checks whether x' yields a successful decommitment.

Proposed schemes (see Table 1): The fuzzy commitment scheme was applied to iris-codes by Hao et al. [32]. In their scheme, 2048-bit iris-codes are applied to

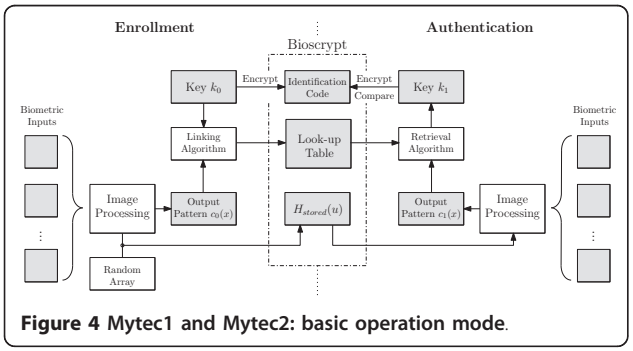

Figure 4 Mytec1 and Mytec2: basic operation mode.

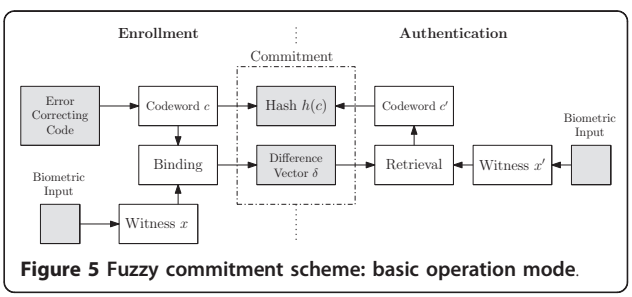

Figure 5 Fuzzy commitment scheme: basic operation mode.

Table 1 Experimental results of proposed fuzzy commitment schemes.

Authors	Char.	FRR/FAR	Remarks
Hao et al. [32]		0.47/0	Ideal images
Bringer et al. [34]	Iris	5.62/0	Short key
Rathgeb and Uhl [39]		4.64/0	-
Teoh and Kim [40]		0.9/0	User-specific tokens
Tong et al. [44]	Fingerprint	78/0.1	-
Nandakumar [45]		12.6/0	-
Van der Veen et al. [46]		3.5/0	>1 enroll. sam.
Ao and Li [43]	Face	7.99/0.11	-
Lu et al. [47]		~30/0	Short key
Maiorana and Ercole [48]	Online Sig.	13.07/4	>1 enroll. sam.

bind and retrieve 140-bit cryptographic keys prepared with Hadamard and Reed-Solomon error correction codes. Hadamard codes are applied to eliminate bit errors originating from the natural biometric variance and Reed-Solomon codes are applied to correct burst errors resulting from distortions. The system was tested with 700 iris images of 70 probands obtaining rather impressive results which were not achieved until then. In order to provide an error correction decoding in an iris-based fuzzy commitment scheme, which gets close to a theoretical bound, two-dimensional iterative min-sum decoding is introduced by Bringer et al. [33,34]. Within this approach a matrix is created where lines as well as columns are formed by two different binary Reed-Muller codes. Thereby a more efficient decoding is available. The proposed scheme was adapted to the standard iris recognition algorithm of Daugman to bind and retrieve 40-bit keys. Due to the fact that this scheme was tested on non-ideal iris images a more significant performance evaluation is provided. Rathgeb and Uhl [35] provide a systematic approach to the construction of iris-based fuzzy commitment schemes. After analyzing error distributions between iris-codes of different iris recognition algorithms, Reed-Solomon and Hardamard codes are applied (similar to [32]). In other further work [36] the authors apply context-based reliable component selection in order to extract keys from iris-codes which are then bound to Hadamard codewords. Different techniques to improve the performance of iris-based fuzzy commitment schemes have been proposed [37-39]. Binary iris-codes are suitable to be applied in a fuzzy commitment scheme, in addition, template alignment is still feasible since it only involves a one-dimensional circular shift of a given iris-code. Besides iris, the fuzzy commitment scheme has been applied to other biometrics as well, which always requires a binarization of extracted feature vectors.

Teoh and Kim [40] applied a randomized dynamic quantization transformation to binarize fingerprint features extracted from a multichannel Gabor filter. Feature vectors of 375 bits are extracted and Reed-Solomon codes are applied to construct the fuzzy commitment scheme. The transformation comprises a non-invertible projection based on a random matrix derived from a user-specific token. It is required that this token is stored on a secure device. Similar schemes based on the feature extraction of BioHashing [41] (discussed later) have been presented in [42,43]. Tong et al. [44] proposed a fuzzy extractor scheme based on a stable and order invariant representation of biometric data called Fingercode reporting inapplicable performance rates. Nandakumar [45] applies a binary fixed-length minutiae representation obtained by quantizing the Fourier phase spectrum of a minutia set in a fuzzy commitment scheme, where alignment is achieved through focal point of high curvature regions. In [46] a fuzzy commitment scheme based on face biometrics is presented in which real-valued face features are binarized by simple thresholding followed by a reliable bit selection to detect most discriminative features. Lu et al. [47] binarized principal component analysis (PCA) based face features which they apply in a fuzzy commitment scheme.

A method based on user adaptive error correction codes was proposed by Maiorana et al. [48] where the error correction information is adaptively selected based on the intra-variability of a user's biometric data. Applying online signatures this seems to be the first approach of using behavioral biometrics in a fuzzy commitment scheme. In [49] another fuzzy commitment scheme based on online signatures is presented.

While in classic fuzzy commitment schemes [15,32] biometric variance is eliminated applying error correction codes, Zheng et al. [50] employ error tolerant lattice functions. In experiments a FRR of ~3.3% and a FAR of ~0.6% are reported. Besides the formalism of fuzzy extractors and secure sketches, Dodis et al. [13] introduce the so-called syndrome construction. Here an error correction code syndrome is stored as part of the template and applied during authentication in order to reconstruct the original biometric input.

3) Shielding functions

Tuyls et al. [51] introduced a concept which is referred to as shielding functions.

Operation mode (see Figure 6): It is assumed that at enrollment a noise-free real-valued biometric feature vector X of fixed length is available. This feature vector is used together with a secret S (the key) to generate the helper data W applying an inverse δ-contracting function G^{-1}, such that $G(W, X) = S$. Like in the fuzzy commitment scheme [15], additionally, a hash $F(S) = V$ of the secret S is stored. The core of the scheme is the δ-contracting function G which calculates a residual for

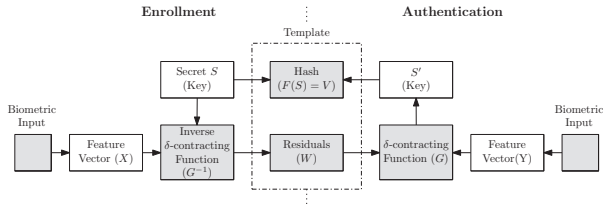

Figure 6 Shielding functions: basic operation mode.

each feature, which is the distance to the center of the nearest even-odd or odd-even interval, depending on whether the corresponding bit of S is 0 or 1. W can be seen as correction vector which comprises all residuals. At authentication another biometric feature vector Y is obtained and $G(W, Y)$ is calculated. In case $||X - Y|| \leq \delta$, $G(W, Y) = S' = S = G(W, X)$. In other words, noisy features are added to the stored residuals and the resulting vector is decoded. An additional application of error correction is optional. Finally, the hash value $F(S')$ of the reconstructed secret S' is tested against the previously stored one (V) yielding successful authentication or rejection. In further work [52] the authors extract reliable components from fingerprints reporting a FRR of 0.054% and a FAR of 0.032%.

Buhan et al. [53] extend the ideas of the shielding functions approach by introducing a feature mapping based on hexagonal zones instead of square zones. No results in terms of FRR and FAR are given. Li et al. [54] suggest to apply fingerprint in a key-binding scheme based on shielding functions.

4) Fuzzy vault

One of the most popular BCSs called fuzzy vault was introduced by Juels and Sudan [16] in 2002.

Operation mode (see Figure 7): The key idea of the fuzzy vault scheme is to use an unordered set A to lock a secret key k, yielding a vault, denoted by V_A. If another set B overlaps largely with A, k is reconstructed, i.e., the vault V_A is unlocked. The vault is created applying polynomial encoding and error correction. During the enrollment phase a polynom p is selected which encodes the key k in some way (e.g., the coefficients of p are formed by k), denoted by $p \, \Re \, k$. Subsequently, the

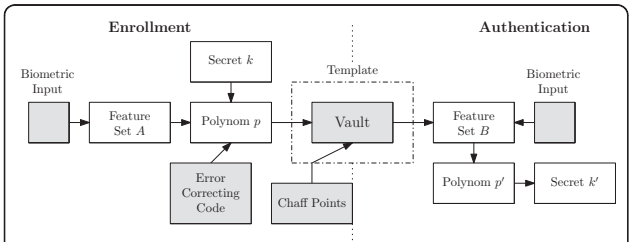

Figure 7 Fuzzy vault scheme: basic operation mode.

elements of A are projected onto the polynom p, i.e., $p(A)$ is calculated. Additionally, chaff points are added in order to obscure genuine points of the polynom. The set of all points, R, forms the template. To achieve successful authentication another set B needs to overlap with A to a certain extent in order to locate a sufficient amount of points in R that lie on p. Applying error correction codes, p can be reconstructed and, thus, k. The security of the whole scheme lies within the infeasibility of the polynomial reconstruction and the number of applied chaff points. The main advantage of this concept is the feature of order invariance, i.e., fuzzy vaults are able to cope with unordered feature set which is the case for several biometric characteristics (e.g., fingerprints [27]).

Proposed schemes (see Table 2): Clancy et al. [55] proposed the first practical and most apparent implementation of the fuzzy vault scheme by locking minutiae points in a "fingerprint vault". A set of minutiae points, A, are mapped onto a polynom p and chaff points are randomly added to construct the vault. During authentication, Reed-Solomon codes are applied to reconstruct the polynom p out of which a 128-bit key is recreated. An pre-alignment of fingerprints is assumed which is rarely the case in practice (feature alignment represents a fundamental step in conventional fingerprint recognition systems). To overcome the assumption of pre-alignment, Nandakumar et al. [56] suggest to utilize high curvature points derived from the orientation field of a fingerprint as helper data to assist the process of alignment. In their fingerprint fuzzy vault, 128-bit keys are bound and retrieved. Uludag et al. [8,57,58] propose a line-based minutiae representation which the authors evaluate on a test set of 450 fingerprint pairs. Several other approaches have been proposed to improve the alignment within fingerprint-based fuzzy vaults [59-61]. Rotation and translation invariant minutiae representations have been suggested in [62].

Numerous enhancements to the original concept of the fuzzy vault have been introduced. Moon et al. [63] suggest to use an adaptive degree of the polynomial. Nagar and Chaudhury [64] arrange encoded keys and biometric data of fingerprints in the same order into separate grids, which form the vault. Chaff values are inserted into these grids in appropriate range to hide information.

In other work, Nagar et al. [17,65] introduce the idea of enhancing the security and accuracy of a fingerprint-based fuzzy vault by exploiting orientation information of minutiae points. Dodis et al. [13] suggest to use a high-degree polynomial instead of chaff points in order to create an improved fuzzy vault. Additionally, the authors propose another syndrome-based key-generating scheme which they refer to as PinSketch. This scheme is

Table 2 Experimental results of proposed fuzzy vault schemes.

Authors	Char.	FRR/FAR	Remarks
Clancy et al. [55]		20-30/0	Pre-alignment
Nandakumar et al. [56]		4/0.04	-
Uludag et al. [57]	Fingerprint	27/0	-
Li et al. [61]		~7/0	Alignment-free
Nagar et al. [17]		5/0.01	Hybrid BCS
Lee et al. [67]		0.775/0	-
Wu et al. [68]	Iris	5.55/0	-
Reddy and Babu et al. [72]		9.8/0	Hardend vault
Wu et al. [70]		0.93/0	-
	Palmprint		
Kumar and Kumar [73]		~1/0.3	-
Wu et al. [71]	Face	8.5/0	-
Kholmatov and Yanikoglu [75]	Online Sig.	8.33/2.5	10 subjects

based on polynomial interpolation like the fuzzy vault but requires less storage space. Arakala [66] provides an implementation of the PinSketch scheme based on fingerprints.

Apart from fingerprints, other biometric characteristics have been applied in fuzzy vault schemes. Lee et al. [67] proposed a fuzzy vault for iris biometrics. Since iris features are usually aligned, an unordered set of features is obtained through independent component analysis. Wu et al. [68,69] proposed a fuzzy vault based on iris as well. After image acquisition and preprocessing, iris texture is divided into 64 blocks where for each block the mean gray scale value is calculated resulting in 256 features which are normalized to integers to reduce noise. At the same time, a Reed-Solomon code is generated and, subsequently, the feature vector is translated to a cipher key using a hash function. In further work, Wu et al. [70] propose a system based on palmprints in which 362 bit cryptographic keys are bound and retrieved. A similar approach based on face biometrics is presented in [71]. PCA features are quantized to obtain a 128-bit feature vector from which 64 distinguishable bits are indexed in a look-up table while variance is overcome by Reed-Solomon codes. Reddy and Babu [72] enhance the security of a classic fuzzy vault scheme based on iris by adding a password with which the vault as well as the secret key is hardened. In case passwords are compromised the systems security decreases to that of a standard one, thus, according results were achieved under unrealistic preconditions. Kumar and Kumar [73,74] present a fuzzy vault based on palmprints by employing real-valued DCT coefficients of palmprint images binding and retrieving 307 bit keys. Kholmatov and Yanikoglu [75] propose a fuzzy vault for online signatures.

C. Approaches to biometric key-generation

The prior idea of generating keys directly out of biometric templates was presented in a patent by Bodo [76]. An implementation of this scheme does not exist and it is expected that most biometric characteristics do not provide enough information to reliably extract a sufficiently long and updatable key without the use of any helper data.

1) Private template scheme

The private template scheme, based on iris, was proposed by Davida et al. [77,78] in which the biometric template itself (or a hash value of it) serves as a secret key. The storage of helper data which are error correction check bits are required to correct faulty bits of given iris-codes.

Operation mode (see Figure 8): In the enrollment process M, 2048-bit iris-codes are generated which are put through a majority decoder to reduce the Hamming distance between them. The majority decoder computes the vector $V\,ec(V) = (V_1, V_2, ..., V_n)$ for a n-bit code vector, denoted by $V\,ec(\nu_i) = (\nu_{i,1}, \nu_{i,2}, ..., \nu_{i,n})$, where $V_j = majority(\nu_{1,j}, \nu_{2,j}, ..., \nu_{M,j})$ is the majority of 0's and 1's at each bit position j of M vectors. A majority decoded iris-code T, denoted by $V\,ec(T)$, is concatenated with check digits $V\,ec(C)$, to generate $V\,ec(T)||V\,ec(C)$. The check digits $V\,ec(C)$ are part of an error correction code. Subsequently, a hash value Hash (Name, Attr, $V\,ec(T)||V\,ec(C)$) is generated, where Name is the user's name, Attr are public attributes of the user and Hash(·) is a hash function. Finally, an authorization officer signs this hash resulting in Sig(Hash(Name, Attr, $V\,ec(T)||V\,ec(C)$)). During authentication, several iris-codes are captured and majority decoded resulting in $V\,ec(T')$. With the according helper data, $V\,ec(C)$, the corrected template $V\,ec(T'')$ is reconstructed. Hash(Name, Attr, $V\,ec(T'')||V\,ec(C)$) is calculated and compared against Sig (Hash(Name, Attr, $V\,ec(T'')||V\,ec(C)$)). Experimental results are omitted and it is commonly expected that the proposed system reveals poor performance due to the fact that the authors restrict to the assumption that only 10% of bits of an iris-code change among different

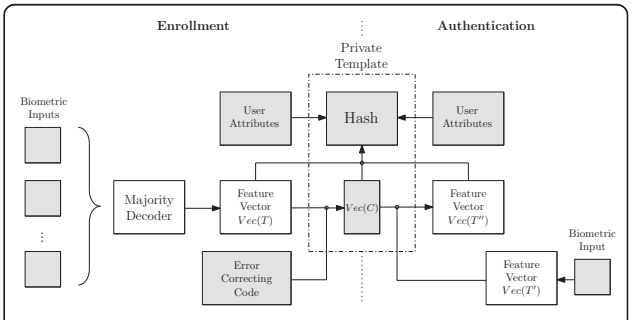

Figure 8 Private template scheme: basic operation mode.

iris images of a single subject. In general, average intra-class distances of iris-codes lie within 20-30%. Implementations of the proposed majority decoding technique (e.g., in [79]) were not found to decrease intra-class distances to that extent.

2) Quantization schemes

Within this group of schemes, helper data are constructed in a way that is assists in a quantization of biometric features in order to obtain stable keys.

Operation mode (see Figure 9): In general quantization schemes, which have been applied to physiological as well as behavioral biometric characteristics, process feature vectors out of several enrollment samples and derive appropriate intervals for each feature element (real-valued feature vectors are required). These intervals are encoded and stored as helper data. At the time of authentication, again, biometric characteristics of a subject are measured and mapped into the previously defined intervals, generating a hash or key. In order to provide updateable keys or hashes, most schemes provide a parameterized encoding of intervals. Quantization schemes are highly related to shielding functions [51] since both techniques perform quantization of biometric features by constructing appropriate feature intervals. In contrast to the shielding functions, generic quantization schemes define intervals for each single biometric feature based on its variance. This yields an improved adjustment of the stored helper data to the nature of the applied biometrics.

Proposed schemes (see Table 3): Feng and Wah [21] proposed a quantization scheme applied to online signatures in order to generate 40-bit hashes. To match signatures, dynamic time warping is applied to x and y-coordinates and shapes of x, y waveforms of a test sample are aligned with the enrollment sample to extract correlation coefficients where low ones indicate a rejection. Subsequently, feature boundaries are defined and encoded with integers. If a biometric sample passed the shape-matching stage, extracted features are fitted into boundaries and a hash is returned out of which a public and a private key are generated. Vielhauer et al. [22,24] process online signatures to generate signature hashes, too. In their approach an interval matrix is generated

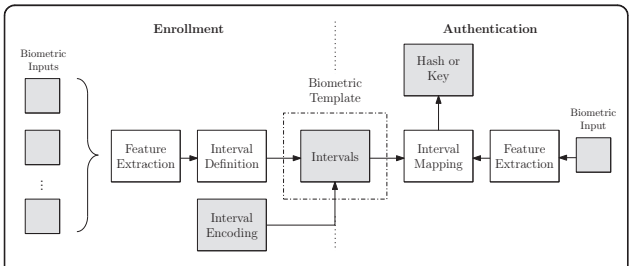

Figure 9 Quantization scheme: basic operation mode.

Table 3 Experimental results of proposed quantization schemes.

Authors	Char.	FRR/FAR	Remarks
Feng and Wah [21]	Online Sig.	28/1.2	
Vielhauer et al. [22]		7.05/0	
Li et al. [83]	Fingerprint	20/1	>1 enroll. sam.
Sutcu et al. [85]	Face	5.5/0	
Rathgeb and Uhl [87]	Iris	4.91/0	

for each subject such that hashes are generated by mapping every single feature against the interval matrix. In [80] the authors adopt the proposed feature extraction to an online signature hash generation based on a secure sketch. Authors report a decrease of the FRR but not of the EER. An evaluation of quantization-based key-generation schemes is given in [81]. Sutcu et al. [82] proposed a quantization scheme in which hash values are created out of face biometrics. Li et al. [83] study how to build secure sketches for asymmetric representations based on fingerprint biometrics. Furthermore, the authors propose a theoretical approach to a secure sketch applying two-level quantization to overcome potential pre-image attacks [84]. In [85] the proposed technique is applied to face biometrics. Rathgeb and Uhl [86] extended the scheme of [82] to iris biometrics generating 128-bit keys. In [87] the authors apply a context-based reliable component selection and construct intervals for the most reliable features of each subject.

D. Further investigations on BCSs

Besides the so far described key concepts of BCSs, other approaches have been proposed. While some represent combinations of basic concepts, others serve different purposes. In addition, multi-BCSs have been suggested.

1) Password hardening

Monrose et al. [19] proposed a technique to improve the security of password-based applications by incorporating biometric information into the password (an existing password is "salted" with biometric data).

Operation mode (see Figure 10): The keystroke dynamics of a user a are combined with a password pwd_a resulting in a hardened password $hpwd_a$ which can be tested for login purposes or used as cryptographic key. $\varphi(a, l)$ denotes a single biometric feature φ acquired during the l-th login attempt of user a. To initialize an account, $hpwd_a$ is chosen at random and $2m$ shares of $hpwd_a$, denoted by $\{S_t^0, S_t^1\}$, $1 \leq t \leq m$, are created by applying Shamir's secret-sharing scheme. For each $b \in \{0,1\}^{\frac{a}{m}}$ the shares $\{S_t^{b(t)}\}$, $1 \leq t \leq m$, can be used to reconstruct $hpwd_a$, where $b(i)$ is the i-th bit of b. These shares are arranged in an instruction table of

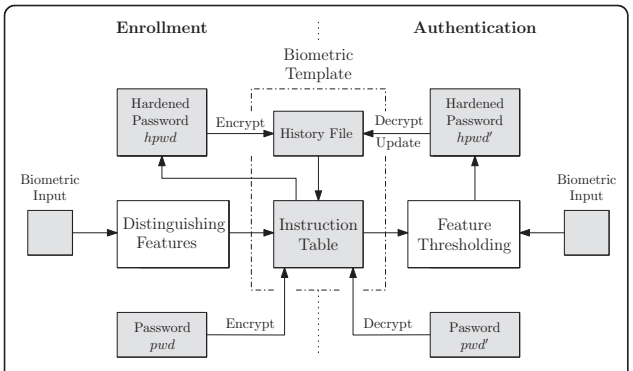

Figure 10 Password hardening: basic operation mode.

dimension $2 \times m$ where each element is encrypted with pwd_a. During the l-th login, pwd'_a, a given password to access account a, is used to decrypt these elements (the correctness of pwd'_a is necessary but not sufficient). For each feature φ_i, comparing the value of $\varphi_i(a, l)$ to a threshold $t_i \in \mathbb{R}$ indicates which of the two values should be chosen to reconstruct $hpwd_a$. Central to this scheme is the notion of *distinguishable features*: let μ_{ai} be the mean deviation and σ_{ai} be the standard deviation of the measurement $\varphi_i(a, j_1) \ldots \varphi_i(a, j_h)$ where $j_1, ..., j_h$ are the last h successful logins of user a. Then, φ_i is a distinguishable feature if $|\mu_{ai} - t_i| > k\sigma_{ai}$ where $k \in \mathbb{R}^+$. Furthermore, the feature descriptor b_a is defined as $b_a(i) = 0$ if $t_i > \mu_{ai} + k\sigma_{ai}$, and 1 if $t_i < \mu_{ai} - k\sigma_{ai}$. For other features, b_a is undefined. As distinguishing features φ_i develop over time, the login program perturbs the value in the second column of row i if $\mu_{ai} < t_i$, and vice versa. The reconstruction of $hpwd_a$ succeeds only if distinguishable features remain consistent. Additionally, if a subject's typing patterns change slightly over time, the system will adapt by conducting a constant-size history file, encrypted with $hpwd_a$, as part of the biometric template. In contrast to most BCSs the initial feature descriptor is created without the use of any helper data.

Proposed schemes: In several publications, Monrose et al. [18,23,88] apply their password-hardening scheme to voice biometrics where the representation of the utterance of a data subject is utilized to identify suitable features. A FRR of approximately 6% and a FAR below 20% was reported. In further work [25,26] the authors analyze and mathematically formalize major requirements of biometric key generators, and a method to generate randomized biometric templates is proposed [89]. Stable features are located during a single registration procedure in which several biometric inputs are measured. Chen and Chandran [90] proposed a key-generation scheme for face biometrics (for 128-bit keys), which operates like a password-hardening scheme [19], using Radon transform and an interactive chaotic bispectral one-way transform. Here, Reed-Solomon codes are used instead of shares. A FRR of 28% and a FAR of 1.22% are reported.

2) BioHashing

A technique applied to face biometrics called "BioHashing" was introduced by Teoh et al. [41,91-93]. Basically, the BioHashing approach operates as key-binding scheme, however, to generate biometric hashes secret user-specific tokens (unlike public helper data) have to be presented at authentication. Prior to the key-binding step, secret tokens are blended with biometric data to derive a distorted biometric template, thus, BioHashing can be seen as an instance of "Biometric Salting" (see Section 3).

Operation mode (see Figure 11): The original concept of BioHashing is summarized in two stages while the first stage is subdivided in two substages: first the raw image is transformed to an image representation in log-polar frequency domain $\Gamma \in \Re^M$, where M specifies the log-polar spatial frequency dimension by applying a wavelet transform, which makes the output immune to changing facial expressions and small occlusions. Subsequently, a Fourier-Mellin transform is applied to achieve translation, rotation and scale invariance. The generated face feature $\Gamma \in \Re^M$ is reduced to a set of single bits $b \in \{0, 1\}^{l_b}$ of length l_b via a set of uniform distributed secret random numbers $r_i \in \{-1, 1\}$ which are uniquely associated with a token. These tokenized random numbers, which are created out of a subject's seed, take on a central role in the BioHashing algorithm. First the user's seed is used for generating a set of random vectors $\{r_i \in \Re^M | i = 1, ..., l_b\}$. Then, the Gram-Schmidt process is applied to the set of random vectors resulting in a set of orthonormal vectors $\{r_{\perp_i} \in \Re^M | i = 1, \ldots, l_b\}$. The dot product of the feature vector and all orthonormal vectors $\{\langle \Gamma | r_{\perp_i} \rangle \in \Re^M | i = 1, \ldots, l_b\}$ is calculated. Finally a l_b-bit FaceHash $b \in \{0, 1\}^{l_b}$ is calculated, where b_i, the i-th bit of b is 0 if $\langle \Gamma | r_{\perp_i} \rangle \leq \tau$ and 1 otherwise, where τ is a predefined threshold. In the second stage of BioHashing a key k_c is generated out of the BioHash b. This is done by applying Shamir's secret-sharing scheme.

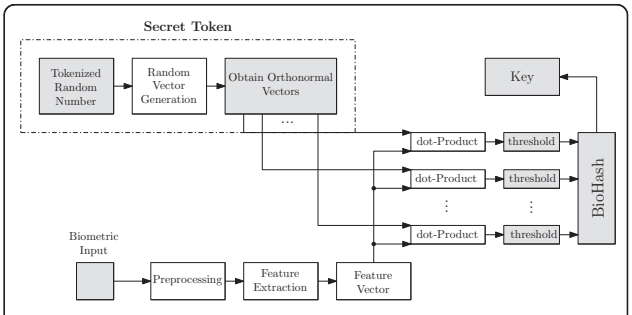

Figure 11 BioHashing: basic operation mode.

Proposed schemes: Generating FaceHashes, a FRR of 0.93% and a zero FAR are reported. In other approaches the same group adopts BioHashing to several biometric characteristics including fingerprints [94,95], iris biometrics [96,97] as well as palmprints [98] and show how to apply generated hashes in generic key-binding schemes [99,100]. The authors reported zero EERs for several schemes.

Kong et al. [101] presented an implementation of FaceHashing and gave an explanation for the zero EER, reported in the first works on BioHashing. Zero EER were achieved due to the tokenized random numbers, which were assumed to be unique across subjects. In a more recent publication, Teoh et al. [102] address the so-called "stolen-token" issue evaluating a variant of BioHashing, known as multistage random projection (MRP). By applying a multi-state discretization the feature element space is divided into 2^N segments by adjusting the user-dependent standard deviation. By using this method, elements of the extracted feature vector can render multiple bits instead of 1 bit in the original BioHash. As a result, the extracted bitstreams exhibit higher entropy and recognition performance is increased even if impostors are in possession of valid tokens. However, zero EERs were not achieved under the stolen-token scenario. Different improvements to the BioHashing algorithm have been suggested [103,104].

3) Multi-BCSs and hybrid-BCSs

While multi-biometric systems [105] have been firmly established (e.g., combining iris and face in a single sensor scenario) a limited amount of approaches to BCSs utilize several different biometric traits to generate cryptographic keys. Nandakumar and Jain [106] proposed the best performing multibiometric cryptosystem in a fuzzy vault based on fingerprint and iris. The authors demonstrate that a combination of biometric modalities leads to increased accuracy and, thus, higher security. A FRR of 1.8% at a FAR of ~0.01% is obtained, while the corresponding FRR values of the iris and fingerprint fuzzy vaults are 12 and 21.2%, respectively. Several other ideas of using a set of multiple biometric characteristics within BCSs have been proposed [107-114].

Nagar et al. [17,65] proposed a hybrid fingerprint-based BCS. Local minutiae descriptors, which comprise ridge orientations and frequency information, are bound to ordinate values of a fuzzy vault applying a fuzzy commitment scheme. In experiments FRR of 5% and a FAR of 0.01% is obtained, without minutiae descriptors the FAR increased to 0.7%. A similar scheme has been suggested in [115].

4) Other approaches

Chen et al. [116] extract keys from fingerprints and bind these to coefficients of n-variant linear equations. Any n ($n < m$) elements of a m-dimensional feature vector can retrieve a hidden key where the template consists of true data, the solution space of the equation, and chaff data (false solutions of the equation). A FRR of 7.2% and zero FAR are reported. Bui et al. [117] propose a key-binding scheme based on face applying quantization index modulation which is originally targeted for watermarking applications. In [118,119], approaches of combining biometric templates with syndrome codes based on the Slepian-Wolf theorem are introduced. Boyen et al. [120] presented a technique for authenticated key exchange with the use of biometric data. In order to extract consistent bits from fingerprints a locality preserving hash is suggested in [121]. Thereby minutiae are mapped to a vector space of real coefficients which are decorrelated using PCA. Kholmatov et al. [122] proposed a method for biometric-based secret sharing. A secret is shared upon several users and released if a sufficiently large number of the user's biometric traits is presented at authentication. Similar approaches have been proposed in [123,124].

E. Security of biometric cryptosystems

Most BCSs aim at binding or generating keys, long enough to be applied in a generic cryptographic system (e.g., 128-bit keys for AES). To prevent biometric keys from being guessed, these need to exhibit sufficient size and entropy. System performance of BCSs is mostly reported in terms of FRR and FAR, since both metrics and key entropy depend on the tolerance levels allowed at comparison, these three quantities are highly interrelated.

Buhan et al. [53,125] have shown that there is a direct relation between the maximum length k of cryptographic keys and the error rates of the biometric system. The authors define this relation as $k \leq -\log_2(\mathrm{FAR})$, which has established as one of the most common matrices used to estimate the entropy of biometric keys. This means that an ideal BCS would have to maintain an $\mathrm{FAR} \leq 2^{-k}$ which appears to be a quite rigorous upper bound that may not be achievable in practice. Nevertheless, the authors pointed out the important fact that the recognition rates of a biometric system correlate with the amount of information which can be extracted, retaining maximum entropy. Based on their proposed quantization scheme, [22]. Vielhauer et al. [126] describe the issue of choosing significant features of online signatures and introduce three measures for feature evaluation: intrapersonal feature deviation, interpersonal entropy of hash value components and the correlation between both. By analyzing the discriminativity of chosen features the authors show that the applied feature vector can be reduced by 45% maintaining error rates [127]. This example underlines the fact that BCSs

may generate arbitrary long keys while inter-class distances (= Hamming distance between keys) remain low. Ballard et al. [25,26] propose a new measure to analyze the security of a BCS, termed guessing distance. The guessing distance defines the number of guesses a potential imposter has to perform in order to retrieve either the biometric data or the cryptographic key. Thus, the guessing distance directly relates to intra-class distances of biometric systems and, therefore, provides a more realistic measure of the entropy of biometric keys. Kelkboom et al. [128] analytically obtained a relationship between the maximum key size and a target system performance. A increase of maximum key size is achieved in various scenarios, e.g., when applying several biometric templates at enrollment and authentication or when increasing the desired false rejection rates. In theory-oriented work, Tuyls et al. [129,130] estimate the capacity and entropy loss for fuzzy commitment schemes and shielding functions, respectively. Similar investigations have been done by Li et al. [131,132] who provide a systematic approach of how to examine the relative entropy loss of any given scheme, which bounds the number of additional bits that could be extracted if optimal parameters were used. A method for arranging secret points and chaff points in fuzzy vaults such that entropy loss is minimized is presented in [133].

Obviously, key lengths have to be maximized in order to minimize the probability that secret keys are guessed [128]. A second factor which affects the security of biometric cryptosystems is privacy leakage, i.e., the information that the helper data contain (leak) about biometric data [134]. Ideally, privacy leakage should be minimized (for a given key length), to avoid identity fraud. The requirements on key size and privacy leakage define a fundamental trade-off within approaches to BCSs, which is rarely estimated. In [135] this trade-off is studied from in an information-theoretical prospective and achievable key length versus privacy leakage regions are determined. Additionally, stored helper data have to provide unlinkability.

3. Cancelable biometrics

Cancelable biometric transforms are designed in a way that it should be computationally hard to recover the original biometric data (see Figure 12). The intrinsic strength (individuality) of biometric characteristics should not be reduced applying transforms (constraint on FAR) while on the other hand transforms should be tolerant to intra-class variation (constraint on FRR) [12]. In addition, correlation of several transformed templates must not reveal any information about the original biometrics (unlinkability). In case transformed biometric data are compromised, transform parameters are changed, i.e., the biometric template is updated. To prevent impostors from tracking subjects by cross-matching databases it is suggested to apply different transforms for different applications. Two main categories of CB are distinguished [4]:

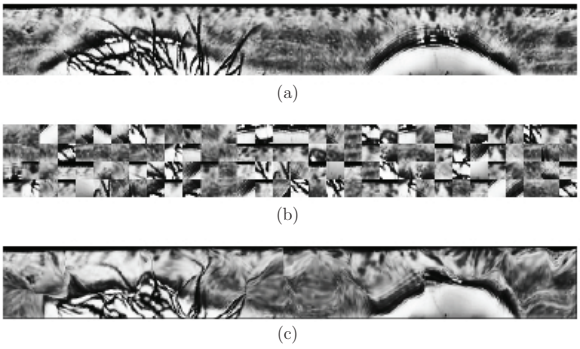

Figure 12 CB: (a) iris texture, (b) block permutation, (c) surface folding.

(1) *Non-invertible transforms*: In these approaches, biometric data are transformed applying a noninvertible function (e.g., Figure 12b,c). In order to provide updatable templates, parameters of the applied transforms are modified. The advantage of applying non-invertible transforms is that potential impostors are not able to reconstruct the entire biometric data even if transforms are compromised. However, applying non-invertible transforms mostly implies a loss of accuracy. Performance decrease is caused by the fact that transformed biometric templates are difficult to align (like in BCSs) in order to perform a proper comparison and, in addition, information is reduced. For several approaches these effects have been observed [12,136].

(2) *Biometric salting*: Biometric salting usually denotes transforms of biometric templates which are selected to be invertible. Any invertible transform of biometric feature vector elements represents an approach to biometric salting even if biometric templates have been extracted in a way that it is not feasible to reconstruct the original biometric signal [137]. As a consequence, the parameters of the transform have to be kept secret. In case user-specific transforms are applied, the parameters of the transform (which can be seen as a secret seed [102] have to be presented at each authentication. Impostors may be able to recover the original biometric template in case transform parameters are compromised, causing a potential performance decrease of the system in case underlying biometric algorithms do not provide high accuracy without secret transforms. While approaches to biometric salting may maintain the recognition performance of biometric

systems non-invertible transforms provide higher security [4].

Approaches to CB can be classified further with respect parts of biometric systems in which transforms are applied. In the signal domain, transformations are either applied to raw biometric measurements (e.g., face image [12]) or to preprocessed biometric signals (e.g., iris texture [138]). In case transforms are applied in signal domain comparators do not need to be adapted. In feature domain extracted biometric features (e.g., face features in [102]) are transformed, thus, a compromise of transforms requires further effort in reconstructing the original biometric from the template. Experimental results of key concepts of CB are summarized in Table 4.

A. The issue of performance evaluation

While in the majority of proposed approaches to CB template alignment is non-trivial and applied transforms are selected to be non-invertible, still some schemes (e.g., in [72,102]), especially to biometric salting, report an increase in performance. In case user-specific transforms are applied at enrollment and authentication, by definition, two-factor authentication is yielded which may increase the security but does not effect the accuracy of biometric authentication.

Table 4 Experimental results of proposed approaches to CB.

Authors	Char.	FRR/FAR	Remarks
Non-invertible transforms			
Ratha et al. [140]		$15/10^{-4}$	-
	Fingerprint		
Boult et al. [147]		~0.08 EER	-
Hammerle-Uhl et al. [138]		1.3 EER	-
	Iris		
Zuo et al. [136]		0.005/0	perf. increase
Maiorana et al. [146]	Online Sig.	10.81 EER	-
Biometric salting			
Savvides et al. [137]		4.64/0	Non-stolen token
Teoh et al. [91]	Face	$2{\cdot}10^{-3}$ EER	Non-stolen token
Wang et al. [157]		6.68 EER	-
Zuo et al. [136]		$0.005/<10^{-3}$	perf. increase
	Iris		
Ouda et al. [159]		1.3 EER	-
Teoh et al. [151]	Fingerprint	5.31 EER	-
Other CB			
Jeong et al. [161]	Face	14 EER	-
Tulyakov et al. [162]		25.9/0	-
	Fingerprint		
Ang et al. [164]		4 EER	-

A significant increase of recognition rates can be caused by unpractical assumptions during performance evaluations. If user-specific transforms are applied to achieve CB these transforms have to be considered compromised during inter-class comparisons. Otherwise, biometrics becomes meaningless as the system could rely on secret tokens parameters without any risk [101]. Secret tokens, be it transform parameters, random numbers or any kind of passwords are easily compromised and must not be considered secure [1]. Thus, performance evaluations of approaches to CB have to be performed under the so-called "stolen-token scenario" where each impostor is in possession of valid secret tokens (the same applies to BCSs in case secret tokens are applied). Figure 13 illustrates how inter-class distances may change with or without considering the stolen-token scenario. If different tokens are applied for each subject a clear separation of intra-class and inter-class distributions is achieved by adopting a new threshold. In contrast, if secret tokens are considered compromised accuracy decreases. Performance is untruly gained if this scenario is ignored during experiments causing even more vulnerable systems in case of compromise [139].

B. Approaches to non-invertible transforms

1) IBM approaches

Ratha et al. [12] were the first to introduce the concept of CB applying noninvertible transforms.

Operation mode (see Figure 14): Generally, at enrollment, non-invertible transforms are applied to biometric inputs choosing application-dependent parameters. During authentication, biometric inputs are transformed and a comparison of transformed templates is performed.

Several types of transforms for constructing multiple CB from pre-aligned fingerprints and face biometrics

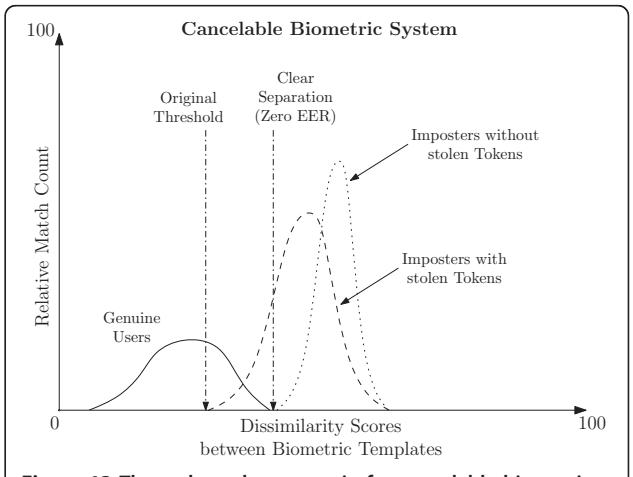

Figure 13 The stolen-token scenario for cancelable biometrics.

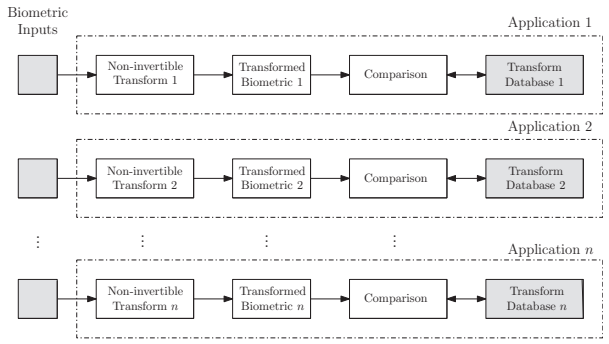

Figure 14 The basic concept of CB based on non-invertible transforms.

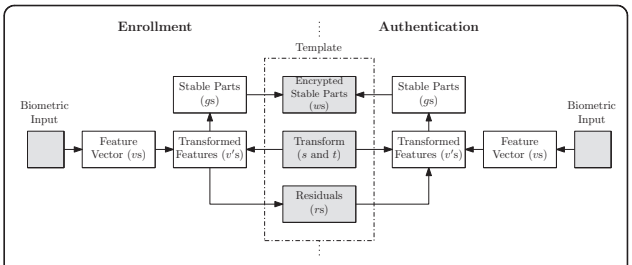

Figure 15 Biotokens: basic operation mode.

have been introduced in [12,140,141] including cartesian transform and functional transform. In further work [136], different techniques to create cancelable iris biometrics have been proposed. The authors suggest four different transforms applied in image and feature domain where only small performance drops are reported. Hammerle-Uhl et al. [138] applied classic transformations suggested in [12] to iris biometrics. Furthermore, in [142] it is shown that applying both transforms to rectangular iris images, prior to preprocessing, does not work. Similar to [136] Rathgeb and Uhl [143] suggest to apply row permutations to iris-codes. Maiorana et al. [144-146] apply non-invertible transforms to obtain cancelable templates from online signatures. In their approach, biometric templates, which represent a set of temporal sequences, are split into non-overlapping sequences of signature features according to a random vector which provides revocability. Subsequently, the transformed template is generated through linear convolution of sequences. The complexity of reconstructing the original data from the transformed template is computationally as hard as random guessing.

2) Revocable biotokens

Boult et al. [147,148] proposed cryptographically secure biotokens which they applied to face and fingerprints. In order to enhance security in biometric systems, biotokens, which they refer to as Biotope™, are adopted to existing recognition schemes (e.g., PCA for face).

Operation mode (see Figure 15): Each measured biometric feature v is transformed via scaling and translation resulting in $v' = (v - t) \cdot s$. The key idea is to split v' into a stable part g termed integer and an unstable part r. For face biometrics the authors suggest to simply split real feature values into an integer part and a fractional part (e.g., 15.4 is splitted into 15 and 0.4). Since g is considered stable, and a "perfect matching" is claimed to be feasible at authentication, comparisons can be performed in the encrypted domain. A one-way transform of g, denoted by w is stored as first part of the secure biometric template. As second part of the template the unencoded r which has been obscured via the transform, as well as s and t are stored. At authentication, features are transformed applying s and t onto a residual region defined by r. Then, the unencrypted r is used to compute the local distance within a "window", which is referred to as robust distance measure, to provide a perfect match of w. However, since a perfect match is required only for a number of features defined by the system threshold, biotokens are not matched exactly. Additionally, user-specific passcodes can be incorporated to create verification-only systems. Although the authors ideas seem promising, several questions with respect to the presented approaches are left open, for instance, the design of the helper function which separates biometric features into stable and unstable parts and the adoption of this scheme to other biometric characteristics (which is claimed to be feasible). In further work, bipartite biotokens [149,150] are introduced and applied to fingerprints in order to provide secure communication via an untrusted channel, where cryptographic keys are released based on successful comparisons of biotokens.

C. Approaches to biometric salting

Savvides et al. [137] generate cancelable face biometrics by applying so-called minimum average correlation filters which provide non-invertibility. User-specific secret personal identification numbers (PINs) serve as seed for a random basis for the filters similar to [31]. As previously mentioned, BioHashing [41] without key-binding provides cancelable biometric templates, too. Early proposals of the BioHashing algorithm did not consider the stolen-token scenario. In more recent work [151] it is demonstrated that the EER for the extraction of cancelable 180-bit fingercodes increases from 0% to 5.31% in the stolen-token scenario. The authors address this issue by proposing a new method which they refer to as MRP [152,153]. It is claimed that MRP (which is applied to face and speech) retains recognition performance in the stolen-token scenario. Furthermore, the authors proposed a method to generate cancelable keys out of dynamic hand signatures [154,155] based on the random mixing step of BioPhasor and user-specific 2^N discretization. To

provide CB, extracted features are randomly mixed with a token T using a BioPhasor mixing method. Kim et al. [156] apply user-specific random projections to PCA-based face features followed by an error minimizing template transform. However, the authors do not consider a stolen-token scenario. Another approach to biometric salting was presented by Wang et al. [157] in which face features are transformed based on a secret key. Non-invertibility is achieved by means of quantization. Ouda et al. [158,159] propose a technique to obtain cancelable iris-codes. Out of several enrollment templates a vector of consistent bits (BioCode) and their positions are extracted. Revocability is provided by encoding the BioCode according to a selected random seed. Pillai et al. [160] achieve cancelable iris templates by applying sector random projection to iris images. Recognition performance is only maintained if user-specific random matrices are applied.

D. Further investigations on cancelable biometrics

Jeong et al. [161] combine two different feature extraction methods to achieve cancelable face biometrics. PCA and ICA (independent component analysis) coefficients are extracted and both feature vectors are randomly scrambled and added in order to create a transformed template. Tulyakov et al. [162,163] propose a method for generating cancelable fingerprint hashes. Instead of aligning fingerprint minutiae, the authors apply order invariant hash functions, i.e., symmetric complex hash functions. Ang et al. [164] suggest to apply a key-dependent geometric transform to fingerprints. In the first step a core point is selected in the fingerprint image and a line is drawn through it where the secret key defines the angle of the line ($0 \leq \text{key} \leq \pi$). Secondly, all minutiae below the line are reflected above the line to achieve a transformed template. Yang et al. [165] apply random projections to minutiae quadruples to obtain cancelable fingerprint templates. In further work [166] the authors address the stolen-token scenario by selecting random projection matrices based on biometric features. Lee et al. [167] presented a method for generating alignment-free cancelable fingerprint templates. Similar to [59,162,163], orientation information is used for each minutiae point. Cancelability is provided by a user's PIN and the user-specific random vector is used to extract translation and rotation invariant values of minutiae points. Hirata and Takahashi [168] propose CB for finger-vain patterns where images are transformed applying a Fourier-like transform. The result is then multiplied with a random filter where the client stores the inverse filter on some token. At authentication the inverse filter is applied to regenerate the transformed enrollment data and correlation-based comparison is performed. A similar scheme is applied to fingerprints in [169]. Bringer et al. [170] presented an idea of generating time-dependent CB to achieve untraceability among different identities across time.

E. Security of cancelable biometrics

While in the vast majority of approaches, security is put on a level with obtained recognition accuracy according to a reference system, analysis with respect to irreversibility and unlinkability is rarely done. According to irreversibility, i.e., the possibility of inverting applied transforms to obtain the original biometric template, applied feature transformations have to be analyzed in detail. For instance, if (invertible) block permutation of biometric data (e.g., fingerprints in [140] or iris in [138]) is utilized to generate cancelable templates the computational effort of reconstructing (parts of) the original biometric data has to be estimated. While for some approaches, analysis of irreversibility appear straight forward for others more sophisticated studies are required (e.g., in [145] irreversibility relies on the difficulty in solving a blind deconvolution problem).

In order to provide renewability of protected biometric templates, applied feature transformations are performed based on distinct parameters, i.e., employed parameters define a finite key space (which is rarely reported). In general, protected templates differ more as more distant the respective transformation parameters are [146]. To satisfy the property of unlinkability, different transformed templates, generated from a single biometric template applying different parameters, have to appear random to themselves (like templates of different subjects), i.e., the amount of applicable parameters (key space) is limited by the requirement of unlinkability.

F. Cancelable biometrics versus biometric cryptosystems

The demand for cancelable biometric keys results in a strong interrelation between the technologies of BCSs and CB [8]. Within common key-binding schemes in which chosen keys are bound to biometric templates, keys are updatable by definition. In most cases, revoking keys require re-enrollment (original biometric templates are discarded after enrollment). In case a key-binding system can be run in secure sketch mode (e.g., [15,16]), original biometric templates can be reconstructed from another biometric input. With respect to key-generation schemes, revoking extracted keys require more effort. If keys are extracted directly from biometric features without the application of any helper data (e.g., as suggested in [76]), an update of the key is not feasible. Within helper data-based key-generation schemes stored helper data has to be modified in a way that extracted keys are different from previous ones (e.g., changing the encoding of intervals in quantization schemes). Alternatively, the key-generation process could comprise an additional

stage in which biometric salting performed prior to the key-generation process [171,172]. In [173] it is suggested to combine a secure sketch with cancelable fingerprint templates. While CB protect the representation of the biometric data, the biometric template is reconstructed from the stored helper data. Several other approaches to generating cancelable biometric keys have been proposed in [174-177].

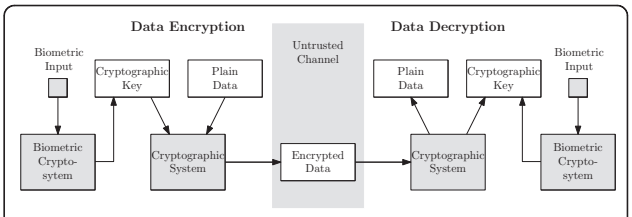

Figure 16 Encryption and decryption of information with keys of BCSs.

4. Discussion and outlook

Based on the presented key concepts of BCSs and CB a concluding discussion is done, including advantages and applications, potential attacks to both technologies, the current state-of-the-art, commercial vendors, and open issues and challenges.

A. Advantages and applications

BCSs and CB offer several advantages over generic biometric systems. Most important advantages are summarized in Table 5. In order to underline the potential of both technologies, two essential use cases are discussed.

1) Encryption/decryption with biometric keys

The most apparent application of BCSs is biometric-dependent key-release within conventional cryptosystems, replacing insecure password- or PIN-based key-release [8]. Eliminating this weak link within cryptosystems, biometric-dependent key-release results in substantial security benefits making cryptographic systems more suitable for high security applications.

Operation mode (see Figure 16): Any subject registered with the BCS is able to release cryptographic keys upon presenting biometric characteristics. Biometric-dependent keys are then transferred to the applied cryptographic algorithm to encrypt plain data. While several approaches to BCSs fulfill the requirement of generating sufficiently long cryptographic keys to be used in symmetric cryptosystems, most schemes fail in extracting an adequate amount of information to construct public key infrastructures (with few exceptions, e.g., [178]). Subsequently, encrypted data are transmitted via any untrusted channel. To decrypt the cipher text again, biometrics are presented to release decrypting keys. It is important to point out that by using biometric keys in generic cryptosystems the generated cipher text is not harder to decipher (in fact it will be even easier to decipher since biometric keys often suffer from low entropy).

2) Pseudonymous biometric databases

BCSs and CB meet the requirements of launching pseudonymous biometric databases [9] since both technologies provide biometric comparisons in encrypted domain while stored helper data or transformed templates do not reveal significant information about original biometric templates.

Operation mode (see Figure 17): At enrollment, biometric characteristics of a subject are employed as input for a BCS or CB (as suggested in [12] diverse obscured templates are generated for different databases). Depending on the type of application further encrypted records are linked to the template where decryption could be applied based on biometric-dependent keys. Since biometric templates are not exposed during comparisons [4], the authentication process is fully pseudonymous and, furthermore, the activities of any subject are untraceable.

Several other applications for the use of BCSs and CB have been suggested. In [10], biometric ticketing, consumer biometric payment systems and biometric boarding cards are suggested. VoIP packages are encrypted applying biometric keys in [179]. A remote biometric authentication scheme on mobile devices based on biometric keys is proposed in [180] and a framework for an alternative PIN service based on CB is presented in [181]. In [182], helper data-free key-generation is utilized for biometric database hashing. Privacy preserving video surveillance has been proposed in [183].

Table 5 Major advantages of BCS and CB.

Advantage	Description
Template protection	Within BCSs and CB the original biometric template is obscured such that a reconstruction is hardly feasible.
Secure key release	BCSs provide key release mechanisms based on biometrics.
Pseudonymous Auth.	Authentication is performed in the encrypted domain and, thus, is pseudonymous.
Revocability of templates	Several instances of secured templates can be generated.
Increased security	BCSs and CB prevent from several traditional attacks against biometric systems.
More social acceptance	BCSs and CB are expected to increase the social acceptance of biometric applications.

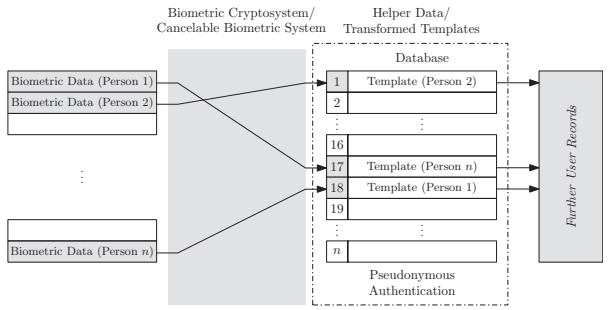

Figure 17 The concept of pseudonymous biometric databases.

B. Potential attacks

Several attacks have been encountered to infiltrate conventional biometric systems [4,184]. The technologies of BCS and CB prevent from different traditional attacks while they appear still vulnerable to some. The most common points of attacks to a biometric system are shown in Figure 18. In addition, numerous techniques have been especially designed to attack key approaches to BCSs and CB.

BCSs and CB do not prevent from classic spoofing attacks [184] (presenting fake physical biometrics). However, there are other possibilities to detect fake biometric inputs (e.g., liveness detection [185]) which can be integrated in both technologies, the same holds for replay attacks. Performing substitution attacks to BCSs is more difficult compared to conventional biometric systems since biometric templates are either bound to cryptographic keys or used to extract helper data (the original biometric template is discarded). Substitution attacks against BCSs require additional knowledge (e.g., of bound keys in case of key-binding schemes). In case of CB substitution, attacks are feasible if impostors are in possession of secret transform parameters or secret keys within approaches to biometric salting. Both technologies are more resilient to masquerade attacks [10,186]. Since reconstruction of original biometric templates should not be feasible the synthetization of original biometric inputs is highly complicated (e.g., [187]). Performance rates of both technologies decrease compared to conventional biometric systems which makes BCSs and CB even more vulnerable to false acceptance attacks. In contrast to CB, overriding final yes/no responses in a tampering scenario is hardly feasible within BCSs as these return a key instead of binary decisions (intermediate score-based attacks could still be applied [188]).

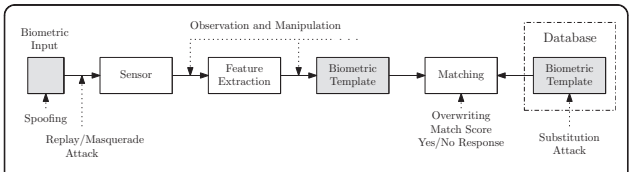

Figure 18 Potential points of attack in generic biometric systems.

In Table 6 an overview of specific attacks proposed against BCSs and CB technologies is given.

1) Attacks against BCSs

Boyen [189] was the first to point out the vulnerability of secure sketches and fuzzy extractors in case an impostor is in possession of multiple invocations of the same secret which are combined to reconstruct secrets and, furthermore, retrieve biometric templates. This (rather realistic) scenario is considered as basis for several attacks against BCSs and CB. Similar observations have been made by Sceirer and Boult [190] which refer to this attack as "attack via record multiplicity". Moreover, the authors point out that if the attacker has knowledge of the secret, the template can be recovered. In addition, a blended substitution attack is introduced in which a subjects and the attackers template are merged into one single template used to authenticate with the system. The Biometric Encryption™algorithm [20] is highly impacted or even compromised by these attacks. Adler [187] proposed a "hill-climbing" attack against the Biometric Encryption™algorithm in which a sample biometric input is iteratively modified while the internal comparison score is observed. Nearest impostor attacks [188] in which distinct parts of a large set of biometric templates is combined to obtain high match scores could be applied even more effectively.

Keys bound in fuzzy commitment schemes [15] have been found to suffer from low entropy (e.g., 44 bits in [32]) reducing the complexity for brute force attacks [40]. Attacks which utilize the fact that error correction codes underlie distinct structures have been suggested [10,188]. Attacks based on error correction code histograms have been successfully conducted against iris-based fuzzy commitment schemes in [191]. In [134], privacy and security leakages of fuzzy commitment schemes are investigated for several biometric data statistics. It is found that fuzzy commitment schemes leak information in bound keys and non-uniform templates. Suggestions to prevent from information leakage in fuzzy commitment schemes have been proposed in [192]. In addition, attacks via record multiplicity could be applied to decode stored commitments [193,194]. Kelkboom et al. [195] introduce a bit-permutation process to prevent from this attack in a fingerprint-based fuzzy commitment scheme. In addition, it has been found that a permutation of binary biometric feature vectors improves the performance of fuzzy commitment scheme [34], i.e., not only the entropy of the entire biometric template (which is commonly estimated in "degrees-of-freedom" [196]) but the distribution of

Table 6 Potential attacks against BCS and CB.

Technology	Proposed attack(s)
Biometric cryptosystems	
Biometric encryption™[20]	Blended substitution attack, attack via record multiplicity, masquerade attack (hill climbing)
Fuzzy commitment scheme [15]	Attacks on error correcting codes
Shielding functions [51]	Attack via record multiplicity
Fuzzy vault scheme [16]	Blended substitution attack, attack via record multiplicity, chaff elimination
Key-Gen. Schemes [77,126]	False acceptance attack, masquerade attack, brute force attack
Biometric hardend passwords [19]	Power consumption observation
Cancelable Biometrics	
Non-invertible transforms [12]	Overwriting final decision, Attack via Record Multiplicity, Substitution Attack (known Transform)
Biometric salting [41]	Overwriting final decision, with Stolen Token: False Acceptance Attack, Substitution Attack, Masquerade Attack

entropy across feature vectors contributes to the security of the system. As a successive encoding of chunks of biometric templates is essential to bind sufficiently long keys distinct parts of the commitment may suffer from low entropy and, thus, are easily decoded [188], i.e., an adaption of biometric templates (e.g., [195]) or an improved use of error correction (e.g., [48]) is necessary.

Applying shielding functions to fingerprints, Buhan et al. [197] estimate the probability of identifying protected templates across databases. It is demonstrated that any kind of quantization approaches do not meet the requirement of unlinkability in general.

Against fuzzy vaults [16], several attacks have been discovered. Chang et al. [198] present an observation to distinguish minutiae from chaff points attacking fuzzy vaults based on fingerprints. Since chaff points are created one-by-one, those created later tend reveal smaller empty surrounding areas which is verified experimentally, i.e., the security of a fuzzy vault highly relies on the methodology of generating chaff points. Scheirer and Boult [190] introduce an attack via record multiplicity. If more instances of a fuzzy vault (generated using different keys) are obtained minutiae are likely recoverable, i.e., unlinkability represents a major issue constructing fuzzy vaults. A method for inserting chaff points with a minimal entropy loss has been proposed in [133]. A brute force attack against fuzzy vaults was proposed in [199]. A collusion attack where the attacker is assumed to be in possession of multiple vaults locked by the same key is presented in [200]. It is demonstrated how to effectively identify chaff points which are subsequently remove to unlock the vault. In [201], vulnerabilities within the concept of a hardened fuzzy vaults are pointed out. In contrast to other concepts (e.g., the fuzzy commitment scheme) the fuzzy vault scheme does not obscure the original biometric template but hides it by adding chaff points, i.e., helper data comprise original biometric features (e.g., minutiae) in plain form. Even if practical key retrieval rates are provided by proposed systems, impostors may still be able to unlock vaults in case the helper data does not hide the original biometric template properly, especially if attackers are in possession of several instances of a single vault.

Helper data-based key-generation schemes [77,126] appear to be vulnerable to attack via record multiplicity. If an attacker is in possession of several different types of helper data and valid secret keys of the same user, a correlation of these can be utilized to reconstruct an approximation of biometric templates acquired at enrollment. In addition, key-generation schemes tend to extract short keys which makes them easier to be guessed in brute force attacks within a realistic feature space. Methods to reconstruct raw biometric data from biometric hashes have been proposed in [202]. Since key-generation schemes tend to reveal worse accuracy compared to key-binding approaches (unless a large number of enrollment samples are applied) these are expected to be highly vulnerable to false acceptance attacks.

The password-hardening scheme [19] has been exposed to be vulnerable to power consumption observations. Side channel attacks to a key generator for voice [18,23] were performed in [203]. Demonstrating another way of attacking biometric key generators, tolerance functions were identified, which either decide to authorize or reject a user. Another side channel attack to a BCS based on keystroke dynamics was presented in [204]. It is suggested to add noise and random bitmasks to stored parts of the template in order to reduce the correlation between the original biometric template and the applied key. A similar attack to initial steps of error correction decoding in BCSs is proposed in [205].

2) Attacks against CB

The aim of attacking CB systems is to expose the secret transform (and parameters) applied to biometric templates. Thereby potential attackers are able to apply substitution attacks. If transforms are considered invertible, original biometric templates may be reconstructed. In case of non-invertible transforms, attackers may reconstruct an approximation of the original biometric

template. Comparison scores, calculated in encrypted domain, could be overwritten [184] and hill-climbing attacks [186] could be performed. In [206,207], attacks against the block re-mapping and surface-folding algorithm of [12] based on fingerprints are proposed.

Since most approaches to biometric salting become highly vulnerable in case secret tokens are stolen [101], false accept attacks could be effectively applied. If the salting process is invertible, templates may be reconstructed and applied in masquerade attacks. Approaches to biometric salting which do not comprise a key-binding step are vulnerable to overwriting final decisions. Several vulnerabilities in the original concept of the BioHashing algorithm [41] have been encountered in [103]. The main drawback of BioHashing (and other instances of biometric salting) resides in exhibiting low performance in case attackers are in possession of secret tokens.

C. Privacy aspects

Subjects can no longer be trusted based on credentials; however, credentials can be revoked and reissued. In order to abolish credential-based authentication, biometrics are increasingly applied for authentication purposes in a broad variety of commercial (e.g., fingerprint door locks) and institutional applications (e.g., border control). Therefore, biometric authentication requires more stringent techniques to identify registered subjects [208]. Besides the fact that subjects share biometric traits rather reluctantly, the common use of biometrics is often considered as a threat to privacy [209]. Most common concerns include abuse of biometric data (e.g., intrusion by creating physical spoofs) as well as permanent tracking and observation of activities (e.g., function creep by cross-matching).

BCSs and CB are expected to increase the confidence in biometric authentication systems (trusted identification). Both technologies permanently protect biometric templates against unauthorized access or disclosure by providing biometric comparisons in the encrypted domain, preserving the privacy of biometric characteristics [8,27]. BCSs and CB keep biometric templates confidential meeting security requirements of irreversibility, and unlinkability.

D. The state-of-the-art

The state-of-the-art of BCSs and CB is estimated according to several magnitudes, i.e., reported performance rates, biometric modalities, applied test sets, etc., and the best performing and evaluated approaches are compared and summarized.

In early approaches to BCSs [31,77], performance rates were omitted. Moreover, most of these schemes have been found to suffer from serious security vulnerabilities [8,190]. Representing one of the simplest key-binding approaches the fuzzy commitment scheme [15] has been successfully applied to iris [32] (and other biometrics). Iris-codes appear to exhibit sufficient information to bind and retrieve long cryptographic keys. Shielding functions [51] and quantization scheme [22,82] have been applied to several physiological and behavioral biometrics, while focusing on reported performance rates, these schemes require further studies. The fuzzy vault scheme [16] which represents one of the most popular BCS has frequently been applied to fingerprints. Early approaches [55], which required a pre-alignment of biometric templates, have demonstrated the potential of this concept. Recently, several techniques [56,57] to overcome the shortcoming of pre-alignment have been proposed. In addition, the feature of order-invariance offers solutions to implement applications such as biometric-based secret sharing in a secure manner [122]. Within the BioHashing approach [41], biometric features are projected onto secret domains applying user-specific tokens prior to a key-binding process. Variants of the BioHashing approach have been exposed to reveal unpractical performance rates under the non-stolen-token scenario [101]. While generic BCSs are designed to extract or bind keys from or to a biometric the password-hardening scheme [19] aims at "salting" an existing password with biometric features.

An overview of key approaches of BCSs, with respect biometric characteristics, applied data sets etc., is given in Table 7. Best results are achieved for fingerprints and iris (e.g., in [32,56]). Both characteristics seem to provide enough information to release sufficiently long keys at practical performance rates while an alignment of templates is feasible. In [32] a FRR of 0.42% at zero FAR is achieved for the first iris-based fuzzy commitment scheme. Performance rates decrease applying scheme to larger datasets captured under unfavorable conditions [34]. Focusing on fingerprints the first implementations of fuzzy vaults [55] have been significantly improved. In [56] a FRR of 4.0% is achieved at a negligible FAR without pre-alignment. Multi-biometric schemes [106] were found improve accuracy even for binding rather long keys. Quantization schemes, which are mostly applied to behavioral biometric characteristics, are limited to generating rather short keys or hashes (e.g., 24 bits in [22]) while performance rates are found unpractical (e.g., FRR of 28.0% in [21]). With respect to recognition rates, the vast majority of BCSs are by no means comparable to conventional biometric systems. While numerous approaches to BCSs generate too short keys at unacceptable performance rates, several enrollment samples may be required as well, (e.g., four samples in [55]). Approaches which report practical rates are tested on

Table 7 Summarized experimental results of key approaches to BCSs.

Author(s)	Applied scheme	Char.	FRR/FAR (%)	Data Set	Key Length	Remarks
Hao et al. [32]	Fuzzy commitment	Iris	0.42/0.0	70 subjects	140-bit	-
Bringer et al. [33]			5.62/0.0	ICE 2005 (244 subjects)	40-bit	-
Clancy et al. [55]	Fuzzy vault	Fingerprints	20-30/0.0	not given	224-bit	pre-alignment, >1 enroll sam.
Nandakumar et al. [56]			4.0/0.004	FVC2002-DB2 (110 subjects)	128-bit	>1 enroll sam.
Wu et al. [68,70]		Iris	5.5/0.0	CASIA v1 (108 subjects)	256-bit	-
		Palmprint	0.73/0.0	PolyU DB (386 subjects)	292-bit	-
Feng and Wah [21]	Quantization	Online signature	28.0/1.2	750 subjects	40-bit	>1 enroll sam.
Vielhauer et al. [22]			7.05/0.0	10 subjects	24-bit	
Monrose et al. [23]	Password-hardening	Voice	>2.0/2.0	90 subjects	~ 60-bit	-
Teoh et al. [92]	BioHashing	Face	0.0/0.0	ORL-DB/Faces94 (194 subjects)	80-bit	Non-stolen token
Nandakumar et al. [106]	Multibiometric Fuzzy Vault	Fingerprint and Iris	1.8/0.01	MSU-DBI and CASIA v1 (108 subjects)	224 bits	-

rather small datasets (e.g., 70 persons in [32]) which must not be interpreted as significant. The introduction of additional tokens, be it random numbers or secret PINs, often clouds the picture of reported results (e.g., zero EER in [92]).

Cancelable biometrics schemes are summarized in Table 8. First approaches to non-invertible transforms [12], which have been applied to face and fingerprints, include block permutation and surface folding. Diverse proposals [136,138] have shown that recognition performance decreases noticeably compared to original biometric systems while sample images of transformed biometric images render non-invertibility doubtable. Within the biotoken approach [147] a performance increase is claimed to be achieved due to the application of the robust distance measure. An EER of ~ 0.08% showed an improvement of ~ 36% compared to the original system (this is likely the only approach to CB that claims to perform better in transformed domain).

BioHashing [41] (without key-binding) represents the most popular instance of biometric salting which represents a two-factor authentication scheme [139]. Since additional tokens have to be kept secret [137,157] result reporting turns out to be problematic. Perfect recognition rates have been reported (e.g., in [91]) while the opposite is true [101].

E. Deployments of BCSs and CB

Though BCSs and CB are still in statu nascendi, first deployments are already available.

priv-ID[a], an independent company that was once part of Philips specializes in biometric encryption. By applying a one-way function, which is referred to as BioHASH®, to biometric data pseudonymous codes are obtained. PerSay[b], a company that provides voice biometric speaker verification collaborates with priv-ID to integrate priv-ID engine to voice biometrics. Genkey[c], a Norway company (which has a large deployment in

Table 8 Summarized experimental results of key approaches to CB.

Author(s)	Technique	Char.	Performance	Data Set	Remarks
Ratha et al. [140]	Block permutation,	Fingerprints	FRRs: ~35, ~15, ~15 (FARs: 10^{-4})	188 subjects	-
Boult et al. [147]	Radial transform, surface folding Revocable BioTokens		~ 0.08 EER	FVC 2004 (200 subjects)	-
Maiorana et al. [146]	BioConvolving	Online Sig.	10.81 EER	MYCT (330 subjects)	-
Teoh et al. [91]	BioHashing	Face	0.0002 EER	ORL-DB/Faces94 (194 subjects)	Non-stolen token

New Delhi), offers solutions to fingerprint-based key-generation. The company utilized a concept, which is referred to as FlexKey, where several enrollment samples are applied to select only the most discriminating features in order to extract longer keys. Precise Biometrics[TMd] is a Swedish company which offers solutions to secure match-on-card fingerprint verification. Securics: The science of security[TMe], founded by T. Boult, provide revocable biometric tokens based on the BioToken approach [147].

The EU project TURBINE [210] which aims to transform a description of fingerprints through cryptobiometrics techniques received a EU funding of over $9 million.

F. Open issues and challenges

With respect to the design goals, BCSs and CB offer significant advantages to enhance the privacy and security of biometric systems, providing reliable biometric authentication at an high security level. Techniques which provide provable security/privacy, while achieving practical recognition rates, have remained elusive (even on small datasets). Additionally, several new issues and challenges arise deploying these technologies [10]. One fundamental challenge, regarding both technologies, represents the issue of alignment, which significantly effects recognition performance. Biometric templates are obscured within both technologies, i.e., alignment of obscured templates without leakage is highly non-trivial. While for some biometric characteristics (e.g., iris) alignment is still feasible, for others (e.g., fingerprints) additional information, which must not lead to template reconstruction, has to be stored. Within conventional biometric systems, align-invariant approaches have been proposed for several biometric characteristics. So far, hardly any suggestions have been made to construct align-invariant BCSs or CB. Feature adaptation schemes that preserve accuracy have to be utilized in order to obtain common representations of arbitrary biometric characteristics (several approaches to extract binary fingerprint templates have been proposed, e.g., [211,212]) allowing biometric fusion in a form suitable for distinct template protection schemes. In addition, several suggestions for protocols providing provable secure biometric authentication based on template protection schemes have been made [150,192,213,214].

Focusing on BCSs it is not actually clear which biometric characteristics to apply in which type of application. In fact it has been shown that iris or fingerprints exhibit enough reliable information to bind or extract sufficiently long keys providing acceptable trade-offs between accuracy and security, where the best performing schemes are based on fuzzy commitment and fuzzy vault. However, practical error correction codes are designed for communication and data storage purposes such that a perfect error correction code for a desired code length has remained evasive (optimal codes exist only theoretically under certain assumptions [215]). In addition, a technique to generate chaff points that are indistinguishable from genuine points has not yet been proposed. The fact that false rejection rates are lower bounded by error correction capacities [216] emerges a great challenge since unbounded use of error correction (if applicable) makes the system even more vulnerable [188]. Other characteristics such as voice or keystroke dynamics (especially behavioral characteristics) were found to reveal only a small amount of stable information [18,19], but can still be applied to improve the security of an existing secret. In addition, several characteristics can be combined to construct multi-BCSs [107], which have received only little consideration so far. Thereby security is enhanced and feature vectors can be merged to extract enough reliable data. While for some characteristics, extracting of a sufficient amount of reliable features seems to be feasible it still remains questionable if these features exhibit enough entropy. In case extracted features do not meet requirements of discriminativity, systems become vulnerable to several attacks (e.g., false acceptance attacks). In addition, stability of biometric features is required to limit information leakage of stored helper data. Besides, several specific attacks to BCSs have been proposed. While key approaches have already been exposed to fail high security demands, more sophisticated security studies for all approaches are required since claimed security of these technologies remains unclear due to a lack formal security proofs and rigorous security formulations [135]. Due to the sensitivity of BCSs, more user-cooperation (compared to conventional biometric systems) or multiple enrollment samples [216] are demanded in order to decrease intra-class variation, while sensoring and preprocessing require improvement as well.

Cancelable biometrics require further investigations as well. Transformations and alignment of transformed templates have to be optimized in order to maintain the recognition performance of biometric systems. Additionally, result reporting remains an issue since unrealistic preconditions distort performance rates.

As plenty different approaches to BCSs and CB have been proposed a large number of pseudonyms and acronyms have been dispersed across literature such that attempts to represented biometric template protection schemes in unified architectures have been made [217]. In addition, a standardization on biometric template protection is currently under work in ISO/IEC FCD 24745.

Endnotes

[a]priv-ID B.V., The Netherlands, http://www.priv-id.com/.

[b]PerSay Ltd., Israel, http://www.persay.com/.

[c]Genkey AS, Norway (BioCryptics), http://genkeycorp.com/.

[d]Precise Biometrics AB, Sweden, http://www.precise-biometrics.com/.

[e]Securics Inc., Colorado Springs, CO, http://www.securics.com/.

Acknowledgements
This work has been funded by the Austrian Science Fund, project no. L554-N15. We thank all the reviewers who significantly helped to improve this work.

Competing interests
The authors declare that they have no competing interests.

Received: 18 February 2011 Accepted: 23 September 2011
Published: 23 September 2011

References

1. Jain AK, Ross A, Prabhakar S: **An introduction to biometric recognition.** *IEEE Trans Circ Syst Video Technol* 2004, **14**:4-20.
2. Cappelli R, Lumini A, Maio D, Maltoni D: **Fingerprint image reconstruction from standard templates.** *IEEE Trans Pattern Anal Mach Intell* 2007, **29(9)**:1489-1503.
3. Ross A, Shah J, Jain AK: **From template to image: reconstructing fingerprints from minutiae points.** *IEEE Trans Pattern Anal Mach Intell* 2007, **29(4)**:544-560.
4. Jain AK, Nandakumar K, Nagar A: **Biometric template security.** *EURASIP J Adv Signal Process* 2008, 1-17.
5. Luo Y, Cheung SS, Ye S: **Anonymous biometric access control based on homomorphic encryption.** *ICME'09: Proc of the 2009 IEEE Int Conf on Multimedia and Expo* 2009, 1046-1049.
6. Upmanyu M, Namboodiri AM, Srinathan K, Jawahar CV: **Efficient biometric verification in encrypted domain.** *ICB '09: Proc of the Third Int Conf on Biometrics* 2009, 899-908.
7. SPEED: **(Signal Processing in the Encrypted Domain) project.**[http://www.speedproject.eu/], Accessed Apr 2011.
8. Uludag U, Pankanti S, Prabhakar S, Jain AK: **Biometric cryptosystems: issues and challenges.** *Proc IEEE* 2004, **92(6)**:948-960.
9. Cavoukian A, Stoianov A: **Biometric encryption.** *Encyclopedia of Biometrics* Springer; 2009.
10. Cavoukian A, Stoianov A: **Biometric encryption: the new breed of untraceable biometrics.** *Biometrics: Fundamentals, Theory, and Systems* Wiley, London; 2009.
11. Jain AK, Ross A: **U Uludag, Biometric template security: Challenges and solutions.** *Proc of European Signal Processing Conf (EUSIPCO)* 2005.
12. Ratha NK, Connell JH, Bolle RM: **Enhancing security and privacy in biometrics-based authentication systems.** *IBM Syst J* 2001, **40**:614-634.
13. Dodis Y, Ostrovsky R, Reyzin L, Smith A: **Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data.** *Proc Eurocrypt* 2004, **2004**:523-540, (LNCS: 3027).
14. Verbitskiy EA, Tuyls P, Obi C, Schoenmakers B, Škorić B: **Key extraction from general nondiscrete signals.** *IEEE Trans Inf Forensic Secur* 2010, **5(2)**:269-279.
15. Juels A, Wattenberg M: **A fuzzy commitment scheme.** *6th ACM Conf on Computer and Communications Security* 1999, 28-36.
16. Juels A, Sudan M: **A fuzzy vault scheme.** *Proc 2002 IEEE Int Symp on Information Theory* 2002, 408.
17. Nagar A, Nandakumar K, Jain A: **A hybrid biometric cryptosystem for securing fingerprint minutiae templates.** *Pattern Recogn Lett* 2010, **31**:733-741.
18. Monrose F, Reiter MK, Li Q, Wetzel S: **Cryptographic key generation from voice.** *SP '01: Proc of the 2001 IEEE Symp on Security and Privacy* 2001, 12.
19. Monrose F, Reiter MK, Wetzel S: **Password hardening based on keystroke dynamics.** *Proc of 6th ACM Conf on Computer and Communications Security, CCCS* 1999, 73-82.
20. Soutar C, Tomko GJ, Schmidt GJ: **Fingerprint controlled public key cryptographic system.** *US Patent* 1996, 5541994.
21. Feng H, Wah CC: **Private key generation from on-line handwritten signatures.** *Inf Manag Comput Secur* 2002, **10(18)**:159-164.
22. Vielhauer C, Steinmetz R, Mayerhöfer A: **Biometric hash based on statistical features of online signatures.** *Proc of the 16 th Int Conf on Pattern Recognition (ICPR'02)* 2002, **1**:10123.
23. Monrose F, Reiter MK, Li Q, Wetzel S: **Using Voice to Generate Cryptographic Keys.** *Proc 2001: A Speaker Odyssey, The Speech Recognition Workshop* 2001, 6.
24. Vielhauer C: **Biometric User Authentication for IT Security.** In *Advances in Information Security. Volume 18.* Springer; 2006.
25. Ballard L, Kamara S, Monrose F, Reiter M: **On the requirements of biometric key generators, Technical Report TR-JHU-SPARBKMR- 090707.** *Submitted and available as JHU Department of Computer Science Technical Report* 2007.
26. Ballard L, Kamara S, Reiter MK: **The practical subtleties of biometric key generation.** *SS'08: Proc of the 17th Conf on Security symposium* 2008, 61-74.
27. Jain AK, Flynn PJ, Ross AA: **Handbook of Biometrics.** Springer; 2008.
28. Soutar C, Roberge D, Stoianov A, Gilroy R, Kumar BV: **Biometric encryption–enrollment and verification procedures.** *Proc SPIE, Optical Pattern Recognition IX* 1998, **3386**:24-35.
29. Soutar C, Roberge D, Stoianov A, Gilroy R, Kumar BV: **Biometric encryption using image processing.** *Proc SPIE, Optical Security and Counterfeit Deterrence Techniques II* 1998, **3314**:178-188.
30. Soutar C, Roberge D, Stoianov A, Gilroy R, Kumar BV: **Biometric encryption, ICSA Guide to Cryptography.** 1999.
31. Soutar C, Roberge D, Stoianov A, Gilroy R, Kumar BV: **Method for secure key management using a biometrics.** *US Patent* 2001, 6219794.
32. Hao F, Anderson R, Daugman J: **Combining cryptography with biometrics effectively.** *IEEE Trans Comput* 2006, **55(9)**:1081-1088.
33. Bringer J, Chabanne H, Cohen G, Kindarji B, Źemor G: **Optimal iris fuzzy sketches.** *Proc 1st IEEE Int Conf on Biometrics: Theory, Applications, and Systems (BTAS'07)* 2007, 1-6.
34. Bringer J, Chabanne H, Cohen G, Kindarji B, Źemor G: **Theoretical and practical boundaries of binary secure sketches.** *IEEE Trans Inf Forensic Secur* 2008, **3**:673-683.
35. Rathgeb C, Uhl A: **Systematic construction of iris-based fuzzy commitment schemes.** *Proc of the 3rd Int Conf on Biometrics 2009 (ICB'09)* 2009, 947-956, LNCS: 5558.
36. Rathgeb C, Uhl A: **Context-based texture analysis for secure revocable iris-biometric key generation.** *Proc of the 3rd Int Conf on Imaging for Crime Detection and Prevention, ICDP '09* 2009.
37. Zhang L, Sun Z, Tan T, Hu S: **Robust biometric key extraction based on iris cryptosystem.** *Proc of the 3rd Int Conf on Biometrics 2009 (ICB'09)* 2009, 1060-1070, LNCS: 5558.
38. Ignatenko T, Willems F: **Achieving secure fuzzy commitment scheme for optical pufs.** *Int Conf on Intelligent Information Hiding and Multimedia Signal Processing* 2009, 1185-1188.
39. Rathgeb C, Uhl A: **Adaptive fuzzy commitment scheme based on iris-code error analysis.** *Proc of the 2nd European Workshop on Visual Information Processing (EUVIP'10)* 2010, 41-44.
40. Teoh A, Kim J: **Secure biometric template protection in fuzzy commitment scheme.** *IEICE Electron Express* 2007, **4(23)**:724-730.
41. Goh A, Ngo DCL: **Computation of cryptographic keys from face biometrics.** *Communications and Multimedia Security* 2003, 1-13, (LNCS: 2828).
42. Zeng Z, Watters PA: **A novel face hashing method with feature fusion for biometric cryptosystems.** *European Conference on Universal Multiservice Networks* 2007, 439-444.
43. Ao M, Li SZ: **Near infrared face based biometric key binding.** *Proc of the 3rd Int Conf on Biometrics 2009 (ICB'09)* 2009, 376-385, LNCS: 5558.
44. Tong V, Sibert H, Lecoeur J, Girault M: **Biometric fuzzy extractors made practical: a proposal based on fingercodes.** *Int Conf on Biometrics* 2007, (LNCS: 4642).
45. Nandakumar K: **A fingerprint cryptosystem based on minutiae phase spectrum.** *Proc of IEEE Workshop on Information Forensics and Security (WIFS)* 2010.

46. Van der Veen M, Kevenaar T, Schrijen G-J, Akkermans TH, Zuo F: **Face biometrics with renewable templates.** *SPIE Proc on Security, Steganography, and Watermarking of Multimedia Contents* 2006, **6072**:205-216.
47. Lu H, Martin K, Bui F, Plataniotis K, Hatzinakos D: **Face recognition with biometric encryption for privacy-enhancing self exclusion.** *Proc of the 16th Int Conf on Digital Signal Processing (DSP 2009)* 2009.
48. Maiorana E, Campisi P, Neri A: **User adaptive fuzzy commitment for signature templates protection and renewability.** *SPIE J Elec Imaging Spec Sect Biomet Adv Secur Usability Interoper* 2008, **17(1)**:1-12.
49. Maiorana E, Campisi P: **Fuzzy commitment for function based signature template protection.** *IEEE Signal Process Lett* 2010, **17(3)**:249-252.
50. Zheng G, Li W, Zhan C: **Cryptographic key generation from biometric data using lattice mapping.** *18th Int Conf on Pattern Recognition (ICPR 2006)* 2006, **4**:513-516.
51. Linnartz J-P, Tuyls P: **New shielding functions to enhance privacy and prevent misuse of biometric templates.** *Proc 4th Int Conf Audio- And Video-Based Biometric Person Authentication* 2003, 393-402.
52. Tuyls P, Akkermans AHM, Kevenaar TAM, Schrijen GJ, Bazen AM, Veldhuis RNJ: **Practical biometric authentication with template protection.** *Proc Audio-and Video-Based Biometrie Person Authentication* 2005, **3546**:436-446.
53. Buhan IR, Doumen JM, Hartel PH, Veldhuis RNJ: **Constructing practical fuzzy extractors using QIM, Centre for Telematics and Information Technology, University of Twente, Enschede, Technical Report TR-CTIT-07-52.** 2007.
54. Li H, Wang M, Pang L, Zhang W: **Key binding based on biometric shielding functions.** *IAS* 2009, 19-22.
55. Clancy TC, Kiyavash N, Lin DJ: **Secure smartcard-based fingerprint authentication.** *Proc ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop* 2003, 45-52.
56. Nandakumar K, Jain AK, Pankanti S: **Fingerprint-based fuzzy vault: implementation and performance.** *IEEE Trans Inf Forensic Secur* 2007, **2**:744-757.
57. Uludag U, Jain AK: **Fuzzy fingerprint vault.** *Proc Workshop: Biometrics: Challenges Arising from Theory to Practice* 2004, 13-16.
58. Uludag U, Jain AK: **Securing fingerprint template: fuzzy vault with helper data.** *Proc IEEE Workshop on Privacy Research In Vision* 2006.
59. Yang S, Verbauwhede I: **Automatic secure fingerprint verification system based on fuzzy vault scheme.** *Proc of IEEE Int Conf Audio, Speech and Signal Processing (ICASSP'05)* 2005, **5**:609-612.
60. Chung Y, Moon D, Lee S, Jung S, Kim T, Ahn D: **Automatic alignment of fingerprint features for fuzzy fingerprint vault.** *Proc of Conf on Information Security and Cryptology* 2005, 358-369.
61. Li P, Yang X, Cao K, Tao X, Wang R, Tian J: **An alignment free fingerprint cryptosystem based on fuzzy vault scheme.** *J Netw Comput Appl* 2010, **33**:207-220.
62. Jeffers J, Arakala A: **Minutiae-based structures for a fuzzy vault.** *Proc of the Biometric Consortium Conf 2006* 2006, 1-6.
63. Moon D, Choi W-Y, Moon K, Chung Y: **Fuzzy fingerprint vault using multiple polynomials.** *IEEE 13th Int Symposium on Consumer Electronics, ISCE '09* 2009, 290-293.
64. Nagar A, Chaudhury S: **Biometrics based Asymmetric Cryptosystem Design Using Modified Fuzzy Vault Scheme.** *18th Int Conf on Pattern Recognition (ICPR'06)* 2006, **ICPR 4**:537-540.
65. Nagar A, Nandakumar K, Jain AK: **Securing fingerprint template: Fuzzy vault with minutiae descriptors.** *Int Conf on Pattern Recognition (ICPR'08). IEEE* 2008, 1-4.
66. Arakala A: **Secure and private fingerprint-based authentication.** *Bull Aust Math Soc* 2009, **80**:347-349.
67. Lee YJ, Bae K, Lee SJ, Park KR, Kim J: **Biometric key binding: Fuzzy vault based on iris images.** *Proc of Second Int Conf on Biometrics* 2007, 800-808.
68. Wu X, Qi N, Wang K, Zhang D: **A Novel Cryptosystem based on Iris Key Generation.** *Fourth Int Conf on Natural Computation (ICNC'08)* 2008, 53-56.
69. Wu X, Qi N, Wang K, Zhang D: **An iris cryptosystem for information security.** *IIH-MSP '08: Proc of the 2008 Int Conf on Intelligent Information Hiding and Multimedia Signal Processing* 2008, 1533-1536.
70. Wu X, Wang K, Zhang D: **A cryptosystem based on palmprint feature.** *19th Int Conf on Pattern Recognition, (ICPR 2008)* 2008, 1-4.
71. Wu Y, Qiu B: **Transforming a pattern identifier into biometric key generators.** *Proc of Int Conf on Multimedia and Expo (ICME)* 2010, 78-82.
72. Reddy E, Babu I: **Performance of Iris Based Hard Fuzzy Vault.** *Int J Comput Sci Netw Secur (IJCSNS)* 2008, **8(1)**:297-304.
73. Kumar A, Kumar A: **A palmprint based cryptosystem using double encryption.** *Proc SPIE Conf Biometric Technology for human identification* 2008, **6944**:69440D-1-69440D-9.
74. Kumar A, Kumar A: **Development of a new cryptographic construct using palmprint-based fuzzy vault.** *EURASIP J Adv Signal Process* 2009, 11.
75. Kholmatov A, Yanikoglu B: **Biometric cryptosystem using online signatures.** *Comput Inf Sci ISCIS 2006 (LNCS)* 2006, **4263**:981-990.
76. Bodo A: **Method for producing a digital signature with aid of a biometric feature.** *German patent DE 4243908 A1* 1994.
77. Davida G, Frankel Y, Matt B: **On enabling secure applications through off-line biometric identification.** *Proc of IEEE, Symp on Security and Privacy* 1998, 148-157.
78. Davida G, Frankel Y, Matt B: **On the relation of error correction and cryptography to an off line biometric based identication scheme.** *Proc of WCC99, Workshop on Coding and Cryptography* 1999, 129-138.
79. Yang S, Verbauwhede I: **Secure Iris Verification.** *Proc of the IEEE Int Conf on Acoustics, Speech and Signal Processing, (ICASSP 2007)* 2007, **2**:II-133-II-136.
80. Scheidat T, Vielhauer C, Dittmann J: **An iris-based interval mapping scheme for biometric key generation.** *Proc of the 6th Int Symposium on Image and Signal Processing and Analysis, ISPA '09* 2009, 550-555.
81. Hoque S, Fairhurst M, Howells G: **Evaluating biometric encryption key generation using handwritten signatures.** *Proc of the 2008 Bio-inspired, Learning and Intelligent Systems for Security* 2008, 17-22.
82. Sutcu Y, Sencar HT, Memon N: **A secure biometric authentication scheme based on robust hashing.** *MMSec '05: Proc of the 7th Workshop on Multimedia and Security* 2005, 111-116.
83. Li Q, Guo M, Chang E-C: **Fuzzy extractors for asymmetric biometric representations.** *IEEE Workshop on Biometrics (In association with CVPR)* 2008, 1-6.
84. Li Q, Chang E-C: **Robust, short and sensitive authentication tags using secure sketch.** *MM&Sec '06: Proc of the 8th workshop on Multimedia and security* 2006, 56-61.
85. Sutcu Y, Li Q, Memon N: **Protecting biometric templates with sketch: Theory and practice.** *IEEE Trans Inf Forensic Secur* 2007, **2**:503-512.
86. Rathgeb C, Uhl A: **An iris-based interval-mapping scheme for biometric key generation.** *Proc of the 6th Int Symposium on Image and Signal Processing and Analysis, ISPA '09* 2009.
87. Rathgeb C, Uhl A: **Privacy Preserving Key Generation for Iris Biometrics.** *Proc of the 11th Joint IFIP TC6 and TC11 Conf. on Communications and Multimedia Security, CMS '2010* 2010, 191-200, LNCS: (6109).
88. Monrose F, Reiter MK, Lopresti DP, Shih C: **Toward speech generated cryptographic keys on resource constrained devices.** *Proc 11th USENIX Security Symposium* 2002, 283-296.
89. Ballard L, Kamara S, Monrose F, Reiter MK: **Towards practical biometric key generation with randomized biometric templates.** *CCS '08: Proc of the 15th ACM Conf on Computer and Communications Security* 2008, 235-244.
90. Chen BC, Chandran V: **Biometric based cryptographic key generation from faces.** *Proc. Digital Image Computing: Techniques and Applications (DICTA)* 2007, 394-401.
91. Goh A, Teoh ABJ, Ngo DCL: **Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs.** *IEEE Trans Pattern Anal Mach Intell* 2006, **28(12)**:1892-1901.
92. Teoh ABJ, Ngo DCL, Goh A: **Personalised cryptographic key generation based on face hashing.** *Comput Secur* 2004, **2004(23)**:606-614.
93. Teoh ABJ, Ngo DCL, Goh A: **Biometric Hash: High-Confidence Face Recognition.** *IEEE Trans Circ Syst Video Technol* 2006, **16(6)**:771-775.
94. Song OT, Teoh AB, Ngo DCL: **Application-specific key release scheme from biometrics.** *Int J Netw Secur* 2008, **6(2)**:122-128.
95. Teoh ABJ, Ngo DCL, Goh A: **Biohashing: two factor authentication featuring fingerprint data and tokenised random number.** *Pattern Recogn* 2004, **37**:2245-2255.
96. Chong SC, Jin ATB, Ling DNC: **High security iris verification system based on random secret integration, Comput.** *Vision Image Understanding* 2006, **102(2)**:169-177.
97. Chong SC, Jin ATB, Ling DNC: **Iris authentication using privatized advanced correlation filter.** In *Proc of the 1st Int IAPR Conf on Biometrics (ICB'06). Volume 4642.* Springer Lecture Notes on Computer Science; 2006:382-388.

98. Connie T, Teoh A, Goh M, Ngo D: **Palmhashing: a novel approach for cancelable biometrics.** *Inf Process Lett* 2005, **93(1)**:1-5.
99. Song OT, Teoh ABJ, Ngo DCL: **Application-specific key release scheme from biometrics.** *Int J Netw Secur* 2008, **6(2)**:127-133.
100. Beng A, Teoh J, Toh K-A: **Secure biometric-key generation with biometric helper.** *3rd IEEE Conf on Industrial Electronics and Applications (ICIEA 2008)* 2008, 2145-2150.
101. Kong A, Cheunga K-H, Zhanga D, Kamelb M, Youa J: **An analysis of BioHashing and its variants.** *Pattern Recogn* 2006, **39**:1359-1368.
102. Teoh ABJ, Kuan YW, Lee S: **Cancellable biometrics and annotations on biohash.** *Pattern Recogn* 2008, **41(6)**:2034-2044.
103. Lumini A, Nanni L: **An improved biohashing for human authentication.** *Pattern Recogn* 2007, **40(3)**:1057-1065.
104. Nanni L, Lumini A: **Random subspace for an improved biohashing for face authentication.** *Pattern Recogn Lett* 2008, **29(3)**:295-300.
105. Jain AK, Flynn PJ, Ross AA: **Handbook of Biometrics.** Springer, New York; 2008.
106. Nandakumar K, Jain AK: **Multibiometric template security using fuzzy vault.** *IEEE 2nd Int Conf on Biometrics: Theory, Applications, and Systems, BTAS '08* 2008, 1-6.
107. Voderhobli K, Pattinson C, Donelan H: **A schema for cryptographic key generation using hybrid biometrics.** *7th annual postgraduate symp.: The convergence of telecommunications, networking and broadcasting, Liverpool* 2006.
108. Sutcu Y, Li Q, Memon N: **Secure biometric templates from fingerprint-face features.** *IEEE Conf on Computer Vision and Pattern Recognition, CVPR '07* 2007, 1-6.
109. Cimato S, Gamassi M, Piuri V, Sassi R, Scotti F: **A multibiometric verification system for the privacy protection of iris templates.** *Proc of the Int Workshop on Computational Intelligence in Security for Information Systems CISIS08* 2008, 227-234.
110. Kanade S, Petrovska-Delacretaz D, Dorizzi B: **Multi-biometrics based cryptographic key regeneration scheme.** *IEEE 3rd Int Conf on Biometrics: Theory, Applications, and Systems, BTAS '09* 2009, 1-7.
111. Kanade S, Camara D, Petrovska-Delacrtaz D, Dorizzi B: **Application of biometrics to obtain high entropy cryptographic keys.** *Proceedings of World Academy on Science, Engineering, and Technology, Hong Kong* 2009, **52.**
112. Meenakshi VS, Padmavathi G: **Security analysis of password hardened multimodal biometric fuzzy vault.** *Proceedings of World Academy of Science, Engineering and Technology* 2009, **56.**
113. Jagadeesan A, Thillaikkarasi T, Duraiswamy K: **Cryptographic key generation from multiple biometric modalities: Fusing minutiae with iris feature.** *Int J Comput Appl* 2010, **2(6)**:16-26.
114. Zhang M, Yang B, Zhang W, Takagi T: **Multibiometric based secure encryption and authentication scheme with fuzzy extractor.** *Int J Netw Secur* 2011, **12(1)**:50-57.
115. Chafia F, Salim C, Farid B: **A biometric crypto-system for authentication.** *Proc of Int Conf on Machine and Web Intelligence (ICMWI)* 2010, 434-438.
116. Chen H, Sun H, Lam K-Y: **Key management using biometrics.** *Int Symposium on Data, Privacy, and E-Commerce* 2007, **1**:321-326.
117. Bui FM, Martin K, Lu H, Plataniotis KN, Hatzinakos D: **Fuzzy key binding strategies based on quantization index modulation (QIM) for biometric encryption (BE) applications.** *Trans Inf Forensic Secur* 2010, **5**:118-132.
118. Draper S, Khisti A, Martinian E, Vetro A, Yedidia J: **Secure storage of fingerprint biometrics using slepian-wolf codes.** *Inform Theory and Apps Work (UCSD)* 2007.
119. Martinian SYE, Yedidia JS: **Secure biometrics via syndromes.** *43rd Annual Allerton Conf on Communications, Control, and Computing* Monticello, IL, USA; 2005.
120. Boyen X, Dodis Y, Katz J, Ostrovsky R: **A Smith, Secure remote authentication using biometric data.** *Proc Eurocrypt 05 (LNCS)* 2005, **3494**:147-163.
121. Chang E-C, Roy S: **Robust extraction of secret bits from minutiae.** *Proc of the 2nd Int Conf on Biometrics 2007 (ICB'07)* 2007, 750-759.
122. Kholmatov A, Yanikoglu B, Savas E, Levi A: **Secret sharing using biometric traits.** *Proc of SPIE* 2006, **6202**:62020W.
123. Hirschbichler M, Boyd C, Boles W: **A multiple-control fuzzy vault.** *PST '08: Proc of the 2008 Sixth Annual Conf on Privacy, Security and Trust* 2008, 36-47.
124. Margarov G, Tolba M: **Biometrics based secret sharing using fuzzy vault.** *7th Int Conf on Computer Science and Information Technologies (CSIT'09)* 2009.
125. Buhan IR, Doumen JM, Hartel PH, Veldhuis RNJ: **Fuzzy extractors for continuous distributions.** *University of Twente, Technical Report* 2006.
126. Vielhauer C, Steinmetz R: **Handwriting: feature correlation analysis for biometric hashes.** *EURASIP J Appl Signal Process* 2004, **2004(1)**:542-558.
127. Scheidat T, Vielhauer C: **Biometric hashing for handwriting: entropy based feature selection and semantic fusion.** *Proc of SPIE* 2008, **6819**:68190N.1-68190N.12.
128. Kelkboom EJC, Breebaart J, Buhan I, Veldhuis RNJ: **Analytical template protection performance and maximum key size given a Gaussian modeled biometric source.** *Proc of SPIE defense, security and sensing* 2010.
129. Verbitskiy E, Tuyls P, Denteneer D, Linnartz JP: **Reliable biometric authentication with privacy protection.** *Paper presented at the SPIE Biometric Technology for Human Identification Conference* 2004.
130. Tuyls P, Goseling J: **Capacity and examples of template protecting biometric authentication systems.** *Proc ECCV Workshop BioAW (LNCS)* 2004, **3087**:158-170.
131. Li Q, Sutcu Y, Memon N: **Secure sketch for biometric templates.** *Adv. Cryptology Asiacrypt* 2006, **99-113, (LNCS:4284).**
132. Sutcu Y, Li Q, Memon N: **How to Protect Biometric Templates.** *Proc of SPIE SPIE Conf on Security, Steganography and Watermarking of Multimedia Contents IX* 2007, **6505**:11.
133. Li Q, Chang E-C: **Hiding secret points amidst chaff.** *Proc of the Eurocrypt '06* 2006, 59-72, (LNCS 4004).
134. Ignatenko T, Willems FMJ: **Information leakage in fuzzy commitment schemes.** *Trans Inf Forensic Secur* 2010, **5(2)**:337-348.
135. Ignatenko T, Willems FMJ: **Biometric systems: privacy and secrecy aspects.** *Trans Inf Forensic Secur* 2009, **4(4)**:956-973.
136. Zuo J, Ratha NK, Connel JH: **Cancelable iris biometric.** *Proc of the 19th Int Conf on Pattern Recognition 2008 (ICPR'08)* 2008, 1-4.
137. Savvides M, Kumar B, Khosla P: **Cancelable biometric filters for face recognition.** *ICPR '04: Proc of the Pattern Recognition, 17th Int Conf on (ICPR'04)* 2004, **3**:922-925.
138. Hämmerle-Uhlr J, Pschernig E, Uhl A: **Cancelable iris biometrics using block re-mapping and image warping.** *Proc of the Information Security Conf 2009 (ISC'09) LNCS* 2009, **5735**:135-142.
139. Rathgeb C, Uhl A: **Two-factor authentication or how to potentially counterfeit experimental results in biometric systems.** *Proc of the Int Conf on Image Analysis and Recognition (ICIAR'10), Part II* **6112**:296-305, LNCS 2010.
140. Ratha NK, Connell JH, Chikkerur S: **Generating cancelable fingerprint templates.** *IEEE Trans Pattern Anal Mach Intell* 2007, **29(4)**:561-572.
141. Ratha NK, Connell JH, Bolle RM, Chikkerur S: **Cancelable biometrics: a case study in fingerprints.** *ICPR '06: Proc of the 18th Int Conf on Pattern Recognition* 2006, 370-373.
142. Färberböck P, Hämmerle-Uhl J, Kaaser D, Pschernig E, Uhl A: **Transforming rectangular and polar iris images to enable cancelable biometrics.** In *Proc of the Int Conf on Image Analysis and Recognition (ICIAR'10). Volume 6112.* Springer LNCS; 2010:276-386.
143. Rathgeb C, Uhl A: **Secure iris recognition based on local intensity variations.** In *Proc of the Int Conf on Image Analysis and Recognition (ICIAR'10). Volume 6112.* Springer LNCS; 2010:266-275.
144. Maiorana E, Martinez-Diaz M, Campisi P, Ortega-Garcia J, Neri A: **Template protection for HMM-based on-line signature authentication.** *Proc Workshop Biometrics CVPR Conference* 2008, 1-6.
145. Maiorana E, Martinez-Diaz M, Campisi P, Ortega-Garcia J, Neri A: **Cancelable biometrics for hmm-based signature recognition.** *Proc of the 2nd IEEE Int Conf on Biometrics: Theory, applications and systems (BTAS'08)* 2008, 1-6.
146. Maiorana E, Campisi P, Fierrez J, Ortega-Garcia J, Neri A: **Cancelable templates for sequence-based biometrics with application to on-line signature recognition.** *Trans Syst Man Cybernet A Syst Hum* 2010, **40(3)**:525-538.
147. Boult T: **Robust distance measures for face-recognition supporting revocable biometric tokens.** *FGR '06: Proc of the 7th Int Conf on Automatic Face and Gesture Recognition* 2006, 560-566.
148. Boult T, Scheirer W, Woodworth R: **Revocable fingerprint biotokens: Accuracy and security analysis.** *IEEE Computer Society Conference on Computer Vision and Pattern Recognition* 2007, **1**:1-8.
149. Boult T, Scheirer W: **Bio-cryptographic protocols with bipartite biotokens.** *Proc of the IEEE Biometric Symposium, BSYM '08* 2008, 9-16.
150. Boult T, Scheirer W: **Bipartite biotokens: definition, implementation, and analysis.** *Proc of the 3rd Int Conf on Biometrics 2009 (ICB'09)* **5558**:775-785, LNCS: 2009.

151. Teoh ABJ, Ngo DCL: **Biophasor: token supplemented cancellable biometrics.** *Proc of the Int Conf on Control, Automation, Robotics and Vision (ICARCV'06)* 2006, 1-5.
152. Teoh ABJ, Yuang CT: **Cancellable biometrics realization with multispace random projections.** *IEEE Trans SMC B Recent Adv Biomet Syst* 2007, **37(5)**:1096-1106.
153. Teoh ABJ, Chong L-Y: **Secure speech template protection in speaker verification system.** *Speech Commun* 2010, **52(2)**:150-163.
154. Kuan YW, Teoh ABJ, Ngo DCL: **Secure hashing of dynamic hand signatures using wavelet-Fourier compression with biophasor mixing and 2^N discretization.** *EURASIP J Appl Signal Process* 2007, **2007(1)**:32.
155. Yip WK, Teoh ABJ, Ngo DCL: **Replaceable and securely hashed keys from online signatures.** *IEICE Electron Express* 2006, **3(18)**:410-416.
156. Kim Y, Toh K: **A method to enhance face biometric security.** *IEEE Int Conf on Biometrics: Theory, Applications, and Systems, BTAS '07* 2007, 1-6.
157. Wang Y, Plataniotis K: **Face based biometric authentication with changeable and privacy preservable templates.** *Proc of the IEEE Biometrics Symposium* 2007, 11-13.
158. Ouda O, Tsumura N, Nakaguchi T: **Bioencoding: a reliable tokenless cancelable biometrics scheme for protecting iris codes.** *IEICE Trans Inf Syst* 2010, **E93.D**:1878-1888.
159. Ouda O, Tsumura N, Nakaguchi T: **Tokenless cancelable biometrics scheme for protecting iris codes.** *Proc of the 20th Int. Conf. on Pattern Recognition (ICPR'10)* 2010, 882-885.
160. Pillai JK, Patel VM, Chellappa R, Ratha NK: **Sectored random projections for cancelable iris biometrics.** *Proc of the IEEE Int Conf. on Acoustics Speech and Signal Processing (ICASSP)* 2010, 1838-1841.
161. Jeong MY, Lee C, Kim J, Choi JY, Toh KA, Kim J: **Changeable biometrics for appearance based face recognition.** *Proc of Biometric Consortium Conf, 2006 Biometrics Symposium* 2006, 1-5.
162. Tulyakov S, Farooq F, Govindaraju V: **Symmetric hash functions for fingerprint minutiae.** *Int Workshop on Pattern Recognition for Crime Prevention (LNCS: 3687), Security and Surveillance* 2005, 30-38.
163. Tulyakov S, Farooq F, Mansukhani P, Govindaraju V: **Symmetric hash functions for secure fingerprint biometric systems.** *Pattern Recogn Lett* 2007, **28(16)**:2427-2436.
164. Ang R, Safavi-Naini R, McAven L: **Cancelable key-based fingerprint templates.** *Proc of the Australasian Conf. on Information Security and Privacy ACISP'05* 2005, 242-252, (LNCS 3574).
165. Yang B, Busch C, Gafurov D, Bours P: **Renewable minutiae templates with tunable size and security.** *Proc of the 20th Int Conf on Pattern Recognition (ICPR'10)* 2010, 878-881.
166. Yang B, Hartung D, Simoens K, Busch C: **Dynamic random projection for biometric template protection.** *Proc of the 4th IEEE Int Conf on Biometrics: Theory, applications and systems (BTAS'10)* 2010, 1-7.
167. Lee C, Choi J, Toh K, Lee S, Kim J: **Alignment-free cancelable fingerprint templates based on local minutiae information.** *IEEE Trans Syst Man Cybern B Cybern* 2007, **37(4)**:980-992.
168. Hirata S, Takahashi K: **Cancellable biometrics with perfect secrecy for correlation-based matching.** *Proc of the 3rd Int Conf on Biometrics 2009 (ICB'09), LNCS* 2009, **5558**:868-878.
169. Takahashi K, Hirata S: **Generating provably secure cancelable fingerprint templates based on correlation-invariant random filtering.** *IEEE 3rd Int Conf on Biometrics: Theory, Applications, and Systems, BTAS '09* 2009, 1-6.
170. Bringer J, Chabanne H, Kindarji B: **Anonymous identification with cancelable biometrics.** *Proc of the 6th Int Symposium on Image and Signal Processing and Analysis, ISPA '09* 2009, 494-499.
171. Feng YC, Yuen PC, Jain AK: **A hybrid approach for face template protection.** *Proc of SPIE* 2008, **6944**:694408-1-694408-11.
172. Prasanalakshmi B, Kannammal A: **A secure cryptosystem from palm vein biometrics.** *ICIS '09: Proc of the 2nd Int Conf on Interaction Sciences* 2009, 1401-1405.
173. Bringer J, Chabanne H, Kindarji B: **The best of both worlds: applying secure sketches to cancelable biometrics.** *Paper presented at the WISSec* Luxembourg City, Luxembourg; 2007.
174. Gaddam SVK, Lal M: **Efficient cancellable biometric key generation scheme for cryptography.** *Int J Netw Secur* 2010, **11(2)**:61-69.
175. Lalithamani N, Soman K: **Irrevocable cryptographic key generation from cancelable fingerprint templates: an enhanced and effective scheme.** *Eur J Sci Res* 2009, **31**:372-387.
176. Lalithamani N, Soman K: **An effective scheme for generating irrevocable cryptographic key from cancelable fingerprint templates.** *Int J Comput Sci Netw Secur* 2009, **9(3)**:183-193, (IJCSNS 09).
177. Lalithamani N, Soman KP: **Towards generating irrevocable key for cryptography from cancelable fingerprints.** *Int Conf on Computer Science and Information Technology* 2009, 563-568.
178. Gong Y, Deng K, Shi P: **Pki key generation based on iris features.** *Int Conf on Computer Science and Software Engineering* 2008, **6**:166-169.
179. Arul P, Shanmugam A: **Generate a key for AES using biometric for VOIP network security.** *J Theoretical Appl Inf Technol* 2009, 107-112.
180. Khan MK, Zhang J, Wang X: **Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices.** *Chaos Solitons Frac* 2008, **35(3)**:519-524.
181. Han B-J, Shin Y-N, Jeun I-K, Jung H-C: **A framework for alternative pin service based on cancellable biometrics.** *Joint Workshop on Information Security, JWIS'09* 2009.
182. Rathgeb C, Uhl A: **Iris-biometric hash generation for biometric database indexing.** *Proc of the 20th International Conference on Pattern Recognition (ICPR'10)* 2010, 2848-2851.
183. Upmanyu M, Namboodiri AM, Srinathan K, Jawahar C: **Efficient privacy preserving video surveillance.** *Proc of the IEEE Int Conf on Computer Vision (ICCV'09)* 2009.
184. Ratha NK, Connell JH, Bolle RM: **An analysis of minutiae matching strength.** *AVBPA '01: Proc of the Third Int Conf on Audio- and Video-Based Biometric Person Authentication* 2001, 223-228.
185. Schuckers S, Hornak L, Norman T, Derakhshani R, Parthasaradhi S: **Issues for liveness detection in biometrics.** *Biometric Consortium Conference, 2002 Biometrics Symposium* 2002.
186. Adler A: **Sample images can be independently restored from face recognition templates.** *Proc of the Canadian Conf on Electrical and Computer Engineering* 2003, **2**:1163-1166.
187. Adler A: **Vulnerabilities in biometric encryption systems.** *Audio- and video-based Biometric Person Authentication (AVBPA)* 2005, 1100'1109.
188. Stoianov A, Kevenaar T, van der Veen M: **Security issues of biometric encryption.** *Proc of the Toronto Int. Conf. Science and Technology for Humanity (TIC-STH)* 2009, 34-39.
189. Boyen X: **Reusable cryptographic fuzzy extractors, CCS'2004 Proc. of the 11th ACM Conf. on Computer and Communications Security.** 2004, 82-91.
190. Scheirer W, Boult T: **Cracking fuzzy vaults and biometric encryption.** *Biomet Symp* 2007, **2007**:1-6.
191. Rathgeb C, Uhl A: **Statistical attack against iris-biometric fuzzy commitment schemes.** *Proc of the IEEE Computer Society and IEEE Biometrics Council Workshop on Biometrics (CVPRW'11)* 2011, 25-32.
192. Failla P, Sutcu Y, Barni M: **esketch: a privacy-preserving fuzzy commitment scheme for authentication using encrypted biometrics.** *Proc of the 12th ACM workshop on Multimedia and security MM&Sec '10* 2010, 241-246.
193. Simoens K, Tuyls P, Preneel B: **Privacy weaknesses in biometric sketches.** *Proc of the 30th IEEE Symposium on Security and Privacy* 2009, 188-203.
194. Buhan-Dulman I, Merchan JG, Kelkboom E: **Efficient strategies for playing the indistinguishability game for fuzzy sketches.** *Proc of IEEE Workshop on Information Forensics and Security (WIFS)* 2010.
195. Kelkboom ERC, Breebaart J, Kevenaar TAM, Buhan I, Veldhuis RNJ: **Preventing the decodability attack based crossmatching in a fuzzy commitment scheme.** *Trans Inf Forensic Secur* 2011, **6(1)**:107-121.
196. Daugman J: **The importance of being random: statistical principles of iris recognition.** *Pattern Recogn* 2003, **36(2)**:279-291.
197. Buhan IR, Breebaart J, Guajardo J, de Groot K, Kelkboom E, Akkermans T: **A quantitative analysis of indistinguishability for a continuous domain biometric cryptosystem.** *Proc of the First Int. Workshop Signal Processing in the Encrypted Domain (SPEED '09)* 2009, 82-99.
198. Chang E-C, Shen R, Teo FW: **Finding the original point set hidden among chaff.** *ASIACCS '06: Proc of the 2006 ACM Symposium on Information, Computer and Communications Security* 2006, 182-188.
199. Mihailescu P: **The fuzzy vault for fingerprints is vulnerable to brute force attack.** *CoRR* 2007, **abs/0708.2974.**
200. Miri A, Poon HT: **A collusion attack on the fuzzy vault scheme.** *ISC Int J Inf Secur* 2009, **1(1)**:27-34.
201. Hong S, Jeon W, Kim S, Won D, Park C: **The vulnerabilities analysis of fuzzy vault using password.** *FGCN '08: Proc of the 2008 Second Int Conf on Future Generation Communication and Networking* 2008, 76-83.

202. Kümmel K, Vielhauer C: **Reverse-engineer methods on a biometric hash algorithm for dynamic handwriting.** *Proc of the 12th ACM workshop on Multimedia and security, MM&Sec '10* 2010, 67-72.
203. Delivasilis DL, Katsikas SK: **Side channel analysis on biometric-based key generation algorithms on resource constrained devices.** *Int J Netw Secur* 2005, **3(1)**:44-50.
204. Tao Z, Ming-Yu F, Bo F: **Side-channel attack on biometric cryptosystem based on keystroke dynamics.** *The First International Symposium on Data, Privacy, and E-Commerce, (ISDPE 2007)* 2007, 221-223.
205. Karakoyunlu D, Sunar B: **Differential template attacks on PUF enabled cryptographic devices.** *Proc of IEEE Workshop on Information Forensics and Security (WIFS)* 2010.
206. Quan F, Fei S, Anni C, Feifei Z: **Cracking cancelable fingerprint template of Ratha.** *Int Symposium on Computer Science and Computational Technology* 2008, **2**:572-575.
207. Shin SW, Lee M-K, Moon D, Moon K: **Dictionary attack on functional transform-based cancelable fingerprint templates.** *ETRI J* 2009, **31(5)**:628-630.
208. Cimato S, Gamassi M, Piuri V, Sassi R, Scotti F: **Privacy in biometrics.** *Biometrics: Fundamentals, Theory, and Systems* Wiley, London; 2009.
209. Jain AK, Ross A, Pankanti S: **Biometrics: a tool for information security.** *IEEE Trans Inf Forensic Secur* 2006, **1**:125-143.
210. Delvaux N, Chabanne H, Bringer J, Lindeberg P, Midgren J, Breebaart J, Akkermans T, van der Veen M, Veldhuis R, Kindt E, Simoens K, Busch C, Bours P, Gafurov D, Yang B, Stern J, Rust C, Cucinelli B, Skepastianos D: **Pseudo identities based on fingerprint characteristics.** *IIH-MSP '08: Proc of the 2008 Int Conf on Intelligent Information Hiding and Multimedia Signal Processing* 2008, 1063-1068.
211. Bringer J, Despiegel V: **Binary feature vector fingerprint representation from minutiae vicinities.** *Proc of the 4th IEEE Int Conf on Biometrics: Theory, Applications and Systems (BTAS'10)* 2010, 1-6.
212. Xu H, Veldhuis RN: **Binary representations of fingerprint spectral minutiae features.** *Proc of the 20th Int Conf on Pattern Recognition (ICPR'10)* 2010, 1212-1216.
213. Barni M, Bianchi T, Catalano D, Di RM, Donida LR, Failla P, Fiore D, Lazzeretti R, Piuri V, Scotti F, Piva A: **Privacy preserving fingercode authentication.** *Proc of the 12th ACM workshop on Multimedia and security MM&Sec '10* 2010, 231-240.
214. Upmanyu M, Namboodiri AM, Srinathan K, Jawahar CV: **Blind authentication: a secure crypto-biometric verification protocol.** *Trans Inf Forensic Secur* 2010, **5(2)**:255-268.
215. Willems F, Ignatenko T: **Identification and secret-key binding in binary-symmetric template-protected biometric systems.** *Proc of IEEE Workshop on Information Forensics and Security (WIFS)* 2010.
216. Kelkboom EJC, Molina GG, Breebaart J, Veldhuis RNJ, Kevenaar TAM, Jonker W: **Binary biometrics: an analytic 22 framework to estimate the performance curves under Gaussian assumption.** *Trans Syst Man Cybern A Syst Hum* 2010, **40(3)**:555-571.
217. Breebaart J, Busch C, Grave J, Kindt E: **A reference architecture for biometric template protection based on pseudo identities.** *Proc of the BIOSIG 2008: Biometrics and Electronic Signatures* 2008, 25-38.

doi:10.1186/1687-417X-2011-3
Cite this article as: Rathgeb and Uhl: **A survey on biometric cryptosystems and cancelable biometrics.** *EURASIP Journal on Information Security* 2011 **2011**:3.