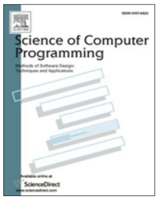
Science of Computer Programming 74 (2008) 43–51

Contents lists available at ScienceDirect

Science of Computer Programming

journal homepage: www.elsevier.com/locate/scico



The best of both worlds: Applying secure sketches to cancelable biometrics[☆]

Julien Bringer[a,*], Hervé Chabanne[a], Bruno Kindarji[a,b]

[a] Sagem Sécurité, Osny, France

[b] TELECOM ParisTech, Paris, France

ARTICLE INFO

Article history:
Received 26 March 2008
Received in revised form 30 September 2008
Accepted 30 September 2008
Available online 11 October 2008

Keywords:
Fingerprint biometrics
Cancelable biometrics
Secure sketches
Security

ABSTRACT

Cancelable biometrics and secure sketches have been introduced with the same purpose in mind: to protect the privacy of biometric templates while keeping the ability to match this protected data against a reference. The paradigm beyond cancelable biometrics is to perform an irreversible transformation over images and to make matching over transformed images. On one hand, a drawback of this technique is that for biometrics using a matching algorithm relying on some complex characteristics, such as the ones used for fingerprints, the irreversible transformation tends to break the underlying structure, thus degrading the performance accuracy. On the other hand, for secure sketches, matching is reduced to an error correction and we show here that applying secure sketch error correction to cancelable biometrics allows one to keep good matching performance. Moreover, the security's advantages of both schemes adds up together.

© 2008 Elsevier B.V. All rights reserved.

1. Introduction

In [28], Ratha et al. introduced the idea of applying an irreversible transformation to a fingerprint's picture in order to enhance the privacy of these biometric data. Indeed, this transformation prevents an adversary to find out who this transformed image belongs to. Moreover, as it is possible to change the transformation used at will, this allows one to renew it or to have different transformations for different applications. The question of the irreversibility of the transformation is raised in [1], and feedback on the performance accuracy of the matching is given in [26,27]. In fact, it is easy to understand that to be irreversible, the transformation has to destroy the characteristics of the biometric data and this will have an impact on the performance of the matching when one exploits this underlying structure.

We want to replace traditional matching algorithms with another one which can have a good performance when working with unstructured data. A natural candidate is the error-correcting procedure coming with secure sketches. Secure sketches are due to Juels and Wattenberg [18]. Since their introduction, some improvements have been made in order to allow their use with real biometric data. For instance, and as they will be used later in this paper, [6] deals with secure sketches for iris and [32] explains their application to fingerprints.

Our results show that we can have a transformation which completely breaks the fingerprint structure while still keeping good matching performances.

This paper is organized as follows. Section 2 recalls some theoretical facts about secure sketches and presents the practical constructions [6,32] for biometrics. Section 3 introduces our application of secure sketches to cancelable biometrics and the security's advantages. Section 4 describes our algorithm on fingerprints and the results we obtain. Finally, Section 5 concludes.

[☆] This work is partially supported by the French ANR RNRT project BACH.

[*] Corresponding author.
E-mail addresses: julien.bringer@sagem.com (J. Bringer), herve.chabanne@sagem.com (H. Chabanne), bruno.kindarji@sagem.com (B. Kindarji).

0167-6423/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.scico.2008.09.016

2. Secure sketches

2.1. Definitions

In [13], Davida et al. started pioneering work by combining error-correcting codes with biometrics to manage the natural variations which occur between two different measures of biometric data. A stronger notion, called the fuzzy commitment scheme, is introduced in [18], in order to handle noisy data in an authentication protocol. Dodis et al. [16] formalized this notion into two important concepts, namely secure sketch and fuzzy extractor, now widely studied. The general idea is to absorb the differences occurring between these two captures by viewing them as errors over a codeword. Afterward, many papers give applications of these techniques for cryptographic purposes in various contexts, e.g. remote biometric authentication [5] or authenticated key agreement [15]; see also [7,9,10,14,21,30,33].

Let $\mathcal{H}$ be a metric space with distance function d. In a few words, a secure sketch allows one to recover a string $w \in \mathcal{H}$ from any close string $w' \in \mathcal{H}$ thanks to known data P which does not leak too much information about w. The formal definition of secure sketching functions is the following.

Definition 1. A $(\mathcal{H}, m, m', t)$-secure sketch is a pair of functions $(\mathsf{SS}, \mathsf{Rec})$ where the sketching function SS takes $w \in \mathcal{H}$ as input, and outputs a sketch in $\{0, 1\}^*$, such that for all random variables W over $\mathcal{H}$ with min-entropy $\mathbf{H}_\infty(W) \geq m$, we have the conditional min-entropy $\overline{\mathbf{H}}_\infty(W \mid \mathsf{SS}(W)) \geq m'$.

The recovery function Rec takes a sketch P and a vector $w' \in \mathcal{H}$ as inputs, and outputs a word $w'' \in \mathcal{H}$, such that for any $P = \mathsf{SS}(w)$ and $d(w, w') \leq t$, it holds that $w'' = w$. Here, $\mathbf{H}_\infty(X) = -\log_2 \max_x \mathbb{P}(X = x)$ stands for the **min-entropy** and $\overline{\mathbf{H}}_\infty(X \mid Y) = -\log_2 \mathbf{E}_{y \leftarrow Y}(2^{-\mathbf{H}_\infty(X|Y=y)})$ for the **conditional min-entropy**.

In fact, the sketching function SS is a randomized function in order to introduce diversity in the sketches, otherwise $\overline{\mathbf{H}}_\infty(W \mid \mathsf{SS}(W))$ would equal 0.

Let $\mathcal{F}$ be a finite alphabet of size q. Let w_1, w_2 be two equal-length vectors over $\mathcal{F}$, then the **Hamming distance** $\mathrm{d}_H(w_1, w_2)$ is the canonical metric distance defined as the number of differences between w_1 and w_2. For some integer n, the set $\mathcal{F}^n$ equipped with the Hamming distance d_H is a **Hamming space**. A subset C of $\mathcal{F}^n$ is an $(n, k, d_{\min})_q$ **error-correcting code** over $\mathcal{F}$ if it contains exactly q^k elements (*i.e.* codewords) where the smallest distance between any two of them is $d_{\min}$. This implies that one can detect up to $d_{\min} - 1$ errors in a codeword. The capacity of correction t of C is the radius of the largest ball for which for any $w \in \mathcal{F}^n$ there is at most one codeword in the ball of radius t centered on w. For the Hamming distance d_H, $t = \lfloor (d_{\min} - 1)/2 \rfloor$. The parameters n, k and $d_{\min}$ are called respectively the length, the dimension and the minimum distance of C.

When $\mathcal{F}$ is a field, if C is a vector subspace of $\mathcal{F}^n$, then C is known as an $[n, k, d_{\min}]_q$ **linear code**.

In additive Hamming spaces, Juels and Wattenberg [18] have proposed a very practical construction, described below.

Definition 2 (*Code-Offset Construction*). Given C an $(n, k, 2t + 1)_q$ code, the secure sketch scheme is a pair of functions $(\mathsf{SS}_{\mathrm{JW}}, \mathsf{Rec}_{\mathrm{JW}})$ where

- the function $\mathsf{SS}_{\mathrm{JW}}$ takes w as input, and outputs the sketch $P = c - w$, where c is randomly taken from C.
- the function $\mathsf{Rec}_{\mathrm{JW}}$ takes w' and P as inputs, decodes $w' + P$ into a codeword c', and then outputs $c' - P$.

This yields a $(\mathcal{F}^n, m, m - (n - k) \log_2 q, t)$-secure sketch, which means that, given P, the entropy loss directly depends on the redundancy of the code. There is thus an obvious trade-off between the correction capacity t of the code and the security of the secure sketch.

The authentication protocol which naturally arises from this construction follows.

- During the registration, we store $P = \mathsf{SS}_{\mathrm{JW}}(w) = c - w$, where c is a random codeword in C, together with the hash value $H(c)$ of c (where H is a cryptographic hash function).
- To authenticate someone, we try to correct the corrupted codeword $w' + P = c + (w' - w)$ and if we obtain a codeword c', we then check if $H(c')$ equals $H(c)$.

Hence, in this construction, the code dimension must not be too small to reduce the entropy loss, and also to prevent an attacker from performing an exhaustive search on codewords to find the appropriate hash value.

Unfortunately, for biometric data, the security constraints of secure sketches are difficult to fulfil. First, we know that biometrics are not random data and that their entropy is hard to measure, so that the effects of entropy loss are not well understood in practice. Moreover, biometrics are widely considered as public data – think for instance about faces captured by cameras, fingerprints on glasses, ... – thus when P and $H(c)$ are known, an attacker would easily check whether it is associated with one of his own biometric database or try other kinds of cross-matching. Following the same idea, several works (e.g. [8,10,20,31]) underline the necessity to choose the parameters appropriately with the error rate of the system in order not to overestimate practical security.

2.2. Practical biometric schemes

2.2.1. Biometric matching

For typical configurations, a biometric-based recognition scheme consists of an enrollment phase and a verification phase. To register a user U, a biometric template b is measured from U and stored in a token or a database. When a new biometric sample b' is captured from U, it is compared to the reference data via a matching function. According to a similarity measure m and some recognition threshold τ, b' will be accepted as a biometric capture of U if $m(b, b') \leq \tau$, else rejected. If a legitimate user is rejected, the error is named a False Reject (**FR**), whereas a False Acceptance error (**FA**) is when a non-matching one, e.g. an impostor, is accepted. The FR and FA rates are the two principal measures of performance associated to biometric-based recognition. We also use the Equal Error Rate (**EER**) which is the point where FR and FA rates are equal.

Assuming that the templates live in a Hamming space and that $m = \mathrm{d}_H$, the authentication protocol above is straight applicable to biometrics where the code-offset construction converts the matching step into an error-correcting problem. To keep the same performance, the correction capacity of the underlying code might thus be close to $n\tau$. However it is a challenging task in practice to find a good construction with respect to the structural constraints on codes and to the security requirements of secure sketches.

Although there are many propositions made on the subject, we only describe below the two practical constructions on which our scheme relies. In term of biometric performance, the following two algorithms, the first one for fingerprints and the second one for irises, are among the best known practical secure sketches constructions that we are aware of.

2.2.2. Reliable component scheme on fingerprints

Traditionally, fingerprint matching is made thanks to minutiae extraction [25] and comparisons of unordered sets of variable length. It is not well suited to secure sketches which are easier to construct for the Hamming distance with a q-ary code via Definition 2. To overcome this difficulty, Tuyls et al. [32] describe a smart algorithm, in the line of the previous works [21,33], to extract stable binary vectors from fingerprints and to apply secure sketches on it.

Firstly, the idea is to deal with fingerprint patterns rather than minutiae. It makes use of the techniques described in [3,2,4] to pre-align a fingerprint image thanks to its core [3] and to extract a real vector of length $L = 1536$. The first 512 coordinates are the values of the squared directional field defined in [2] taken on 256 positions. The remaining, inspired by [4] is the Gabor response of 4 complex Gabor filters with orientation 0, $\frac{\pi}{4}$, $\frac{\pi}{2}$ and $\frac{3\pi}{4}$.

Secondly, to increase the stability of the vectors, an enrollment database containing N users and M images per user is considered. From the NM real vectors $(X_{i,j})_{i=1..N, j=1..M}$ obtained as above, binary fixed-length strings are generated following some statistics.

- Statistical analysis: For each coordinates, the means by user and the mean of all the enrollment vectors are computed. The within-class covariance matrix Σ^w and the between-class covariance matrix Σ^b are also estimated.

$$\forall i \in \{1, \dots, N\}, \quad \mu_i = \frac{1}{M}\sum_{j=1}^{M} X_{i,j}, \qquad \mu = \frac{1}{N}\sum_{k=1}^{N} \mu_k. \tag{1}$$

- Quantization: For each feature $X_{i,j}$, the binary string $Q(X_{i,j})$ is defined by comparing the values of $X_{i,j}$ with the mean μ:

$$\forall t \in \{1, \dots, L\}, \quad (Q(X_{i,j}))_t = 0 \text{ if } (X_{i,j})_t \leq (\mu)_t,\ 1 \text{ if } (X_{i,j})_t > (\mu)_t.$$

- Selecting reliable components: Two notions of reliability are attached to a coordinate $t \in \{1, \dots, L\}$. For a user i, a coordinate t is said p-soft reliable if, for all j, all the $(Q(X_{i,j}))_t$ but p have the same value. Moreover the Signal-to-Noise Ratio (SNR) of the coordinate t is defined by $(\xi)_t = \frac{(\Sigma^b)_{t,t}}{(\Sigma^w)_{t,t}}$.

  Let $n < L$ be the number of reliable bits to select. For a user i, the strategy is to take the p-soft reliable components with highest SNR starting from $p = 0$ by increasing p progressively until it gives exactly n components. These indexes are saved in a vector $P_{1,i}$ and a new vector W_i of length n is constructed with the corresponding reliable bit values.

Finally, the code-offset construction is applied with a $[n, k, d]_2$ linear binary code. For a random codeword c_i, $P_{2,i} = \mathsf{SS}_{\mathrm{JW}}(W_i) = c_i \oplus W_i$ is computed and the public data $(i, P_{1,i}, P_{2,i}, H(c_i))$ are stored.

When a new fingerprint vector Y_i is captured and extracted for a user i, then the verification is straightforward. The quantized vector $Q(Y_i)$ is computed according to the comparison with the enrollment mean μ, and the vector W_i' is constructed by keeping only the indexes of $P_{1,i}$. Then we use the recovery function $\mathsf{Rec}_{\mathrm{JW}}$ to check if $H(\mathsf{Rec}_{\mathrm{JW}}(P_{2,i}, W_i') \oplus P_{2,i}) = H(c_i)$.

Some results are given on two fingerprint databases. The first one is the second FVC2000 database [23] which contains 8 images of 100 different fingers. For enrollment, $M = 6$ images per user are chosen and the 2 others for verification. They succeed in obtaining an Equal Error Rate (**EER**) of 5.3% with an $[511, 76, 171]_2$ BCH code (the EER decreases to 4.5% when the 13 worst reliable users are not taken in account). The second database, from the University of Twente, contains 5 images of 500 different fingers; with $M = 4$, the best EER is 4.2% for a secret size about 40 bits. In [32], it is also compared with a more classical matching algorithm on the original data without binarization nor secure sketches: a likelihood ratio-based algorithm yields an EER of 1.4% for the first database and 1.6% for the second one.

2.2.3. *Optimal Iris fuzzy sketches*

Iris biometrics are better suited to secure sketches: the matching, which is already made on binary vectors, is close to a Hamming distance classifier, and thus code-offset construction is easier to apply than for fingerprints. From one iris image, a 256-bytes iris template and a 256-bytes mask can be constructed (cf. [12]) where the mask filters out the unreliable positions of the iris template, such as eyelashes, eyelids and reflection positions. And matching between two irises merely consists of computing the relative binary Hamming distance over all the non-erased positions.

Hence, contrary to the fingerprint case above, we can try to use secure sketches without any restriction on the enrollment database. There are very few existing works [6,17] which investigate what are the best codes for the underlying decoding problem. Here, the real difficulty is the number of errors and erasures that an error-correcting code would be able to correct. For instance, classical binary linear codes such as BCH codes are not sufficient for attaining low FR rates (lower than 10%) with a non-negligible transmission rate (k/n). To overcome this problem, [6] describes a specific coding/decoding scheme which succeeds in being close to classical matching performances.

The idea is to use an iterative min-sum decoding algorithm on a 2D product code. The product code C is constructed from two binary Reed–Muller codes (see [24,29]) of order 1, to form a code of length 2048 bits. A binary Reed–Muller code of order 1 in m variables, $RM(1, m)$, is an $[2^m, m + 1, 2^{m-1}]_2$ code. The example given in [6] is the product code $C = RM(1, 6) \otimes RM(1, 5)$, which means that codewords of C are matrices of size $2^6 \times 2^5$ whose rows are codewords of $RM(1, 6)$ and columns are codewords of $RM(1, 5)$. It is an $[2048, 7 \times 6, 2^5 \times 2^4]_2$ code. The principle of the iterative min-sum decoding algorithm is to alternate iterations on lines and on columns to update progressively some cost functions which represent the cost to put a 0 or a 1 at a given position.

Starting with a received message $(m_{i,j})$, an initial cost function is defined as $\kappa^0_{ij}(x) = x \oplus m_{i,j}$ or $1/2$ if $m_{i,j}$ is erased, $x \in \{0, 1\}$. And each iteration takes input costs κ^{in}_{ij} and produces output costs κ^{out}_{ij}. For instance, a row iteration updates the costs by computing

$$\kappa^{out}_{ij}(x) = \min_{c \in RM(1,6), c_j = x} \sum_{k=1}^{2^6} \kappa^{in}_{ik}(c_k)$$

while a column iteration works with codewords of RM(1, 5) and computes the sum of costs by column. After an iteration, the decoding message m' defined by $m'_{i,j} = x$ if $\kappa^{out}_{ij}(x) < \kappa^{out}_{ij}(1 \oplus x)$ is constructed. If it is a codeword then the algorithm ends else it continues, with a maximum number of iterations.

3. Applying secure sketches to cancelable biometrics

3.1. *Cancelable biometrics*

Although cancelable biometrics [28] have been introduced with similar objectives to biometric secure sketches, *i.e.* to limit the privacy threats raised by biometric authentication, the methods are somewhat opposed. The idea is to transform biometric data with an irreversible transformation and to perform the matching directly on the transformed data. The advantage pointed out by [28,26,27] is the capability of using existing feature extraction and matching algorithms. However, the main drawback is that, with classical matching algorithms, the performance quickly decreases when the transformation breaks the structure of biometrics. For instance for fingerprints, if the matching uses minutiae then a random permutation of image's blocks leads to bad FR rates (cf. [26, Fig. 7(a) Cartesian case]). There is thus a compromise between irreversibility and performances.

More precisely, let a matching algorithm associated with the similarity measure m and f be a transformation, which acts either on biometric images or on biometric features. Given two biometric data w and w', the matching score will be computed directly on transformed data by $m(f(w), f(w'))$. One first constraint is for f not to degrade the performances too much, and from a security point of view the requirements are:

- w and $f(w)$ do not match together,
- for two different transformations $f_1, f_2, f_1(w)$ and $f_2(w)$ do not match together,
- a pre-image of $f(w)$ must be hard to compute.

In practice, these requirements are difficult to estimate and it seems hard to achieve a good irreversibility with good performances. Anyway, these security properties are really interesting as it allows diversity and revocability of biometric templates when they are verified.

Remark 1. As an attacker, who tries to match two data, may choose himself the similarity measure, the two first conditions should be satisfied for any similarity measure m. It means that, for any m, it should be hard to distinguish $m(w, f(w))$ from $m(w, f(w'))$ and $m(f_1(w), f_2(w))$ from $m(f_1(w), f_2(w'))$ for two non-matching biometric data $w,\ w'$.

Note that the security does not concern the same layer as secure sketches does. Indeed, with cancelable biometrics the matching is performed on transformed data and so the original data are never computed after the enrollment. Thus, it protects the representation of biometrics whereas secure sketch is a clever way to protect the storage of your biometric data until you present a close template.

3.2. Cancelable and secure biometrics

We now apply secure sketches to cancelable biometrics. In so doing, our goals are to add the security of both schemes together and to switch from the matching step of cancelable biometrics to an error-correction problem. It helps to keep good biometric performance.

Assume that the biometric templates are in the metric space $\mathcal{H}$, let f be a transformation on $\mathcal{H}$, we propose to use an $(\mathcal{H}, m, m', t)$-secure sketch with functions $(\mathsf{SS}, \mathsf{Rec})$ as follows. We define the enrollment function Enrol by

$$\mathsf{Enrol}(w; f) = \mathsf{SS}(f(w)).$$

And the verification function Verif takes an enrolled data P, a vector $w' \in \mathcal{H}$ and the function f as inputs and outputs $\mathsf{Rec}(P, f(w'))$, *i.e.* $f(w)$ whenever $d(f(w'), f(w)) \leq t$.

It keeps the correction's principle of secure sketches and the recovery of w from $\mathsf{Enrol}(w; f)$ is at least as hard as the recovery of $f(w)$ from the sketch $\mathsf{SS}(f(w))$. And the more f helps to hide w, the more the security increases. A more formal analysis is done in Section 3.3 to discuss these points. Another advantage of this construction is to enhance the diversity of the enrolled data, as different functions can be used for different users or for different applications by the same user.

As for classical cancelable biometrics, transformations can be applied either on the biometric images, or on the extracted features in $\mathcal{H}$. It can also be applied on both at the same time to increase the irreversibility.

Remark 2. Here, one additional benefit compared with Section 3.1, from converting matching into a decoding procedure, is that an attacker cannot compute directly the distance between transformed and original data. Thus, even if $f(w)$ is closer to w than to another biometric data w', it is not straightforward to distinguish $(w, f(w))$ from $(w', f(w))$ if decoding fails in both cases.

Moreover, it is worth noting that in some applications, f could be stored in a token directly by the user – especially when f is invertible – so that the transformation is unknown to the server and from the outside. Indeed, the cancelable transformations can be computed by the user before sending data for enrollment or verification.

3.2.1. Anonymous protocol

To avoid any tracking of authentications, we can also change the transformation used for a user after each succeeded verification. The transmitted data $f(w')$ will then be unrelated to the next ones and thus it allows one to achieve an anonymous authentication protocol. This can be done by applying a new transformation g on the recovered data $f(w)$ and thereafter to transmit $g \circ f$ for the next verification.

3.3. Security analysis

We consider the functions Enrol and Verif which are defined in Section 3.2 via an $(\mathcal{H}, m, m', t)$-secure sketch with functions $(\mathsf{SS}, \mathsf{Rec})$ and a transformation f on $\mathcal{H}$. Two situations are possible: f can be public or secret.

In both cases, the following lemma is straightforward. We underline that it implies that the protection of w is at least as strong as the protection of $f(w)$ achieved by the secure sketch, under the condition that the entropy of $f(w)$ is sufficiently high.

Lemma 1. *For all random variables W on $\mathcal{H}$,*

$$\overline{\mathbf{H}}_\infty(W \mid \mathsf{Enrol}(W; f)) \geq \overline{\mathbf{H}}_\infty(f(W) \mid \mathsf{SS}(f(W))).$$

If f is invertible, it is an equality.

Proof. For $w \in \mathcal{H}$, we have $\mathbb{P}(W = w) = \mathbb{P}(W = w \wedge f(W) = f(w)) \leq \mathbb{P}(f(W) = f(w))$, which implies that

$$\overline{\mathbf{H}}_\infty(W \mid \mathsf{Enrol}(W; f)) \geq \overline{\mathbf{H}}_\infty(f(W) \mid \mathsf{Enrol}(W; f))$$

with $\mathsf{SS}(f(W)) = \mathsf{Enrol}(W; f)$. □

Via Definition 1, we deduce that for all random variables W on $\mathcal{H}$ with $\mathbf{H}_\infty(f(W)) \geq m$, then

$$\overline{\mathbf{H}}_\infty(W \mid \mathsf{Enrol}(W; f)) \geq m'.$$

We also see that the more f is irreversible, the more it would be difficult to recover w in general. For instance, if f is such that

$$\mathbb{P}(W = w) \leq \frac{\mathbb{P}(f(W) = f(w))}{\lambda}$$

with $\lambda \geq 1$, we obtain

$$\overline{\mathbf{H}}_\infty(W \mid \mathsf{Enrol}(W; f)) \geq \overline{\mathbf{H}}_\infty(f(W) \mid \mathsf{SS}(f(W))) + \log_2 \lambda. \tag{2}$$

If the entropy of $f(W)$ is sufficiently large, it means that the security of both schemes are added together.

However, as we stated before, the entropy of biometric data is difficult to estimate, and the more f will be irreversible, the more the entropy of $f(w)$ will decrease. In terms of entropy, there is thus a kind of compensation between security of secure sketches and security of cancelable transformation. In this way, for the code-offset construction where the loss of entropy does not depend on the input's entropy, the loss of entropy stays the same after introduction of the cancelable transformation:

Proposition 1. *Given a code-offset $(\mathcal{F}^n, m, m-(n-k)\log_2 q, t)$-secure sketch, let $\alpha \geq 0$ such that for all random variables W on $\mathcal{F}^n$, $\mathbf{H}_\infty(f(W)) \geq \mathbf{H}_\infty(W) - \alpha$, then*

$$\overline{\mathbf{H}}_\infty(W \mid \mathsf{Enrol}_{\mathsf{JW}}(W;\, f)) \geq \mathbf{H}_\infty(W) - (n-k)\log_2 q.$$

Proof. We have $\overline{\mathbf{H}}_\infty(f(W) \mid \mathsf{SS}_{\mathsf{JW}}(f(W))) \geq \mathbf{H}_\infty(f(W)) - (n-k)\log_2 q$. And, as in (2),

$$\overline{\mathbf{H}}_\infty(W \mid \mathsf{Enrol}_{\mathsf{JW}}(W;\, f)) \geq \overline{\mathbf{H}}_\infty(f(W) \mid \mathsf{SS}_{\mathsf{JW}}(f(W))) + \alpha,$$

so it leads to the result. □

For the specific case where f is invertible and secret, the security of secure sketches and cancelable biometrics also add up together: an attacker would try to recover $f(w)$ from the sketch and thereafter to construct w from $f(w)$.

Moreover, the construction brings to secure sketches the advantages of cancelable biometrics, of which an important one is the protection against cross-matching attacks. Indeed, starting from 2 sketches $\mathsf{SS}(f_1(w))$ and $\mathsf{SS}(f_2(w))$, it seems difficult to establish a link between them as $f_1(w)$ might not match with $f_2(w)$. Finally, contrary to secure sketches where a successful attack of a sketch compromises forever the underlying biometric data, here cancelable biometrics act as a second layer of protection.

4. An example for fingerprints

To underline the feasibility and the interest of this construction, we experiment it on the fingerprint FVC2000 second database [23]. In fact, we merge three techniques, a cancelable biometrics transformation is applied and both schemes described Section 2.2 are used: an enrollment algorithm adapted from the reliable component scheme [32], slightly modified with techniques from [19], to extract binary features and the coding/decoding algorithm of the optimal iris fuzzy sketch [6] for the secure sketch.

4.1. Algorithm

4.1.1. Feature extraction

We use similar methods to Section 2.2 (pre-alignment,[1] directional field and Gabor response) but with a slight modification. In the second FVC2000 database, the image size is 256 by 364 pixels and we observe that pre-alignment can be very important in some cases, so we decide to embed images in larger images of 768 by 1092 pixels to avoid any loss of information. Moreover, the images are rectangular thus we do not restrict ourselves to squared directional field and Gabor response, which gives us real vectors with 1984 components of information embedded in a vector of length $L = 17\,952$. All the 15 968 null components are marked as erasures for the sequel.

4.1.2. Enrollment

It follows three steps below.

- Cancelable transformation: As in Section 2.2, we set an enrollment database with NM real vectors $(X_{i,j})_{i=1..N,j=1..M}$ from N users. For all $i \in \{1,\ldots,N\}$, a random permutation f_i of $\{1,\ldots,L\}$ is chosen and we applied them on the database to obtain the transformed database containing new vectors $(Y_{i,j})_{i=1..N,j=1..M}$ where for all i, j we set

  $$\forall t \in \{1,\ldots,L\}, \quad (Y_{i,j})_t = (X_{i,j})_{f_i(t)},$$

  which means that we applied[2] the transformations f_i on all templates of user i to construct cancelable templates $Y_{i,*}$. These transformations are stored either by a server or by the relating users for future verifications. Here, we will consider them as secrets.

[1] Note that here this pre-alignment was done manually for all the database to simplify the experiment.

[2] This operation is in fact equivalent to the application of a random permutation of $\{1,\ldots,n\}$ on the binary template W_i after reliable bit selection.

- Reliable bit selection: This step is similar to the one from [32] but we use instead the method described in [19] for face recognition, which is quite softer to adapt to our context. The statistical analysis is not modified except that the erased positions of a vector are not counted. Hence, for a given user i, the number $(M_i)_t$ of non-erased components at an index t is no more constant:

  $$\forall i \in \{1, \dots, N\}, t \in \{1, \dots, L\}, \quad 0 \le (M_i)_t \le M.$$

  We also compute the variance σ_i of the components of the user i:

  $$(\sigma_i)_t = \frac{1}{(M_i)_t} \sum_{j=1}^{(M_i)_t} \left((X_{i,j})_t - (\mu_i)_t\right)^2,$$

  if $(M_i)_t \ge 1$, otherwise we will consider the position as an erasure. Now, the quantization step is to construct the binary string Q_i by comparing the values of the mean μ_i with the overall mean μ:

  $$\forall t \in \{1, \dots, L\}, \quad (Q_i)_t = 0 \text{ if } (\mu_i)_t \le (\mu)_t, \ 1 \text{ if } (\mu_i)_t > (\mu)_t,$$

  if $(M_i)_t \ge 1$. Then we select the n most reliable components thanks to the reliability vector R_i which coordinate t is defined as

  $$(R_i)_t = \frac{1}{2}\left(1 + \operatorname{erf}\left(\frac{|(\mu_i)_t - (\mu)_t|}{\sqrt{2(\sigma_i)_t}}\right)\right)$$

  when $(M_i)_t \ge 1$, where erf is the error function. Hence, we obtain for a user i the binary template W_i of length $n < L$ and the vector $P_{1,i}$ of indexes, potentially with a few erasures if the number of non-erased components was insufficient.
- Sketching: The code-offset construction is applied with a binary product code C of length n. Let c_i be a random codeword of C and compute $P_{2,i} = c_i \oplus W_i$. The data $(i, P_{1,i}, P_{2,i}, H(c_i))$ are stored in a database.

4.1.3. Verification

When a user i wants to authenticate itself, a new fingerprint image is captured and a real vector Z_i of length L is extracted, once again with 1984 components of information and 15 968 erasures.

- Cancelable transformation: In order to compute the cancelable representation of Z_i, the transformation f_i is recovered from its storage location – e.g. a server or the user's token – then we construct T_i as $(T_i)_t = (Z_i)_{f_i(t)}$ for all $t \in \{1, \dots, L\}$.
- Quantization and selection of n bits: From T_i, the quantized vector $Q(T_i)$ is constructed thanks to the comparisons with the mean μ and the binary string W_i' of length n is obtained by restricting $Q(T_i)$ to the indexes of $P_{1,i}$. Here, an important difference with the enrollment is that more erasures may be selected.
- Recovery and verification: $P_{2,i} \oplus W_i' = c_i \oplus (W_i \oplus W_i')$ is computed and the min-sum decoding algorithm of Section 2.2 is run to recover a message c_i'. One nice feature is that it enables efficient decoding of errors and erasures at the same time. Finally, we compare the value $H(c_i')$ with the stored value $H(c_i)$.

Note that here the use of secret permutations of $\{1, \dots, n\}$ to transform the extracted features fulfills the condition of cancelability. It is clear that, with a high probability, it allows to match neither a data x with a transformed version $f(x)$ nor two transformed versions $f_1(x)$ and $f_2(x)$ together. And, even if they are not irreversible functions by construction, they are computationally irreversible thanks to their secrecy and randomness.

Following an observation of [26], for each individual, we assume that a new random permutation is assigned at each enrollment. Hence, due to the large number of possibilities, a given permutation will only, with an overwhelming probability for n large (e.g. $n > 500$), be used once during the system's life (for all users together). So that, given a transformed template $f(x)$, there is no other available information on f which would have permit to interpolate f and to recover x. Moreover, it implies that an adversary could distinguish $(x_1, f(x_1))$ from $(x_2, f(x_1))$ only with a negligible probability when x_1 and x_2 have the same binary weight.

Of course, a truly irreversible function would be preferable than a secret one for some applications but we think that the results achieved below worth considering this slight constraint.

4.2. Results

To follow the cancelable biometrics configuration, all the results are always computed by assuming that the right transformation is used in verification; *i.e.* that when the verification involves the reference data of a user i, then the new template is always[3] transformed via f_i, even if it concerns a non-legitimate user $j \ne i$.

[3] Otherwise, with the wrong transformations f_j, the FA rate would be almost 0%.

We choose randomly $M = 6$ images per user for enrollment and the 2 remaining for the verification. We construct binary templates of length $n = 2048$ and we consider the $[2048, 42, 512]_2$ product code $C = RM(1, 6) \otimes RM(1, 5)$. It yields a FR rate of 3% and a FA rate of 5.53%. With respect to the performance announced in [32, Fig. 5] (for comparable FR rate or FA rate), it compares favourably to the results obtained with the $[511, 67, 175]_2$ BCH code, 5.2% of FR for 5.5% of FA, and it is even sligthly better than the 3.4% of FR and 6.1% of FA given by the restriction to the 87 most reliable users.

We also check the Hamming distance distribution to evaluate the performance of a Hamming distance classifier, which has the same effect of a BCH decoder, by adding the number of errors to the half of erasures. For similar rates, we need a very large threshold: with a threshold of 0.4×2048 it gives a FR rate of 3% for a FA rate of 6.40%. First, it means that we cannot achieve this performance with a BCH code with the same dimension: for the length 2048 and a capacity of correction of 0.4×2048, the dimension must be smaller than 2 thanks to the Plotkin bound — cf. [22]. And it also underlines that the min-sum algorithm helps to improve the performance.

Note that, even if here the dimension of the code could appear as quite small, it has the merit of proving that to include cancelable biometrics into secure sketches still permits having good discrimination between matching fingerprints and non-matching fingerprints.

At last, we underline that these error rates improvement are reported when biometric templates are binarized and the similarity measure uses Hamming distance whereas, without any quantization, biometric templates such as fingerprints can be compared with more efficient matching mechanisms. For instance, as explained in [32], a likelihood ratio-based algorithm would yield here an EER of 1.4%.

5. Conclusion

We showed how to apply secure sketches to cancelable biometrics in order to take advantage of both schemes. From a security point of view, it allows one to augment the protection of biometric data by combining together the security properties of each scheme. We also explained a specific algorithm which gives good performance on a fingerprint database by mixing several sketching techniques and a cancelable transformation. We really think that this first example underlines the interest and the feasibility of the technique. In our opinion, it will help to greatly improve the security of biometric data.

One can also think of adding a physical layer of protection by embedding an enrolled template and the matching algorithm in a smart card, as in general, computations rely on a decoding algorithm.

Acknowledgments

The authors gratefully thank the valuable reviewers' comments which helped a lot to improve the presentation of the paper.

References

[1] R. Ang, R. Safavi-Naini, L. McAven, Cancelable key-based fingerprint templates, in: C. Boyd, J.M.G. Nieto (Eds.), ACISP, in: LNCS, vol. 3574, Springer, 2005.

[2] A.M. Bazen, S.H. Gerez, Systematic methods for the computation of the directional fields and singular points of fingerprints, IEEE Trans. Pattern Anal. Mach. Intell. 24 (7) (2002) 905–919.

[3] A.M. Bazen, R.N.J. Veldhuis, Detection of cores in fingerprints with improved dimension reduction, in: 4th IEEE Benelux Signal Processing Symposium, SPS-2004, Hilvarenbeek, The Netherlands, 2004 (IEEE Benelux Signal Processing Chapter).

[4] A.M. Bazen, R.N.J. Veldhuis, Likelihood-ratio-based biometric verification, IEEE Trans. Circuits Syst. Video Technol. 14 (1) (2004) 86–94.

[5] X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky, A. Smith, Secure remote authentication using biometric data, in: Cramer [11], pp. 147–163.

[6] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, G. Zémor, Optimal iris fuzzy sketches, in: IEEE First International Conference on Biometrics: Theory, Applications and Systems, BTAS'07, 2007.

[7] J. Bringer, H. Chabanne, Q.D. Do, A fuzzy sketch with trapdoor, IEEE Trans. Inf. Theory 52 (5) (2006) 2266–2269.

[8] I. Buhan, J. Doumen, P.H. Hartel, R.N.J. Veldhuis, Fuzzy extractors for continuous distributions, in: F. Bao, S. Miller (Eds.), ASIACCS, ACM, 2007.

[9] G. Cohen, G. Zémor, Generalized coset schemes for the wire-tap channel: Application to biometrics, in: IEEE International Symposium on Information Theory, Chicago, 2004.

[10] G. Cohen, G. Zémor, Syndrome-coding for the wiretap channel revisited, in: IEEE Information Theory Workshop, ITW'06, Chengdu, 2006.

[11] R. Cramer (Ed.), Advances in Cryptology — EUROCRYPT 2005, Proceedings, Aarhus, Denmark, May 22–26, 2005, in: LNCS, vol. 3494, Springer, 2005.

[12] J. Daugman, The importance of being random: Statistical principles of iris recognit., Pattern Recognit. 36 (2) (2003) 279–291.

[13] G. Davida, Y. Frankel, B. Matt, On enabling secure applications through offline biometric identification, in: Proc. IEEE Symp. Security and Privacy, 1998.

[14] G.I. Davida, Y. Frankel, Perfectly secure authorization and passive identification for an error tolerant biometric system, in: M. Walker (Ed.), IMA Int. Conf, in: LNCS, vol. 1746, Springer, 1999.

[15] Y. Dodis, J. Katz, L. Reyzin, A. Smith, Robust fuzzy extractors and authenticated key agreement from close secrets, in: C. Dwork (Ed.), CRYPTO, in: LNCS, vol. 4117, Springer, 2006.

[16] Y. Dodis, L. Reyzin, A. Smith, Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, in: C. Cachin, J. Camenisch (Eds.), EUROCRYPT, in: LNCS, vol. 3027, Springer, 2004.

[17] F. Hao, R. Anderson, J. Daugman, Combining crypto with biometrics effectively, IEEE Trans. Comput. 55 (9) (2006) 1081–1088.

[18] A. Juels, M. Wattenberg, A fuzzy commitment scheme, in: ACM Conference on Computer and Communications Security, 1999.

[19] T.A.M. Kevenaar, G.J. Schrijen, M. van der Veen, A.H.M. Akkermans, F. Zuo, Face recognition with renewable and privacy preserving binary templates, in: Proceedings of the Fourth IEEE Workshop on Automatic Identification Advanced Technologies, AUTOID'05, IEEE Computer Society, Washington, DC, USA, 2005.

[20] Q. Li, Y. Sutcu, N. Memon, Secure sketch for biometric templates, in: X. Lai, K. Chen (Eds.), ASIACRYPT, in: LNCS, vol. 4284, Springer, 2006.

[21] J.-P.M.G. Linnartz, P. Tuyls, New shielding functions to enhance privacy and prevent misuse of biometric templates, in: J. Kittler, M.S. Nixon (Eds.), AVBPA, in: LNCS, vol. 2688, Springer, 2003.

[22] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-correcting Codes, North-Holland, 1988.

[23] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, A.K. Jain, FVC2000: Fingerprint verification competition, IEEE Transactions on Pattern Analysis and Machine Intelligence 24 (3) (2002) 402–412.

[24] D. Muller, Application of boolean algebra to switching circuit design and to error detection, IEEE Trans. Electron. Comput. 3 (1954) 6–12.

[25] S. Prabakhar, A.K. Jain, D. Maio, D. Maltoni, Handbook of Fingerprint Recognition, Springer-Verlag New York, Inc., 2003.

[26] N.K. Ratha, S. Chikkerur, J.H. Connell, R.M. Bolle, Generating cancelable fingerprint templates, IEEE Trans. Pattern Anal. Mach. Intell. 29 (4) (2007) 561–572.

[27] N.K. Ratha, J. Connell, R.M. Bolle, S. Chikkerur, Cancelable biometrics: A case study in fingerprints, in: ICPR (4), IEEE Computer Society, 2006.

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

[29] I. Reed, A class of multiple-error-correcting codes and their decoding scheme, IEEE Trans. Inf. Theory 4 (1954) 38–42.

[30] A. Sahai, B. Waters, Fuzzy identity-based encryption, in: Cramer [11], pp. 457–473.

[31] Y. Sutcu, Q. Li, N. Memon, Protecting biometric templates with sketch: Theory and practice, IEEE Transactions on Information Forensics and Security 2 (3) (2007) 503–512.

[32] P. Tuyls, A.H.M. Akkermans, T.A.M. Kevenaar, G.J. Schrijen, A.M. Bazen, R.N.J. Veldhuis, Practical biometric authentication with template protection, in: T. Kanade, A.K. Jain, N.K. Ratha (Eds.), AVBPA, in: LNCS, vol. 3546, Springer, 2005.

[33] P. Tuyls, J. Goseling, Capacity and examples of template-protecting biometric authentication systems, in: D. Maltoni, A.K. Jain (Eds.), ECCV Workshop BioAW, in: LNCS, vol. 3087, Springer, 2004.