Template Protection for HMM-based On-line Signature Authentication

E. Maiorana*, M. Martinez-Diaz**, P. Campisi*, J. Ortega-Garcia**, A. Neri*

*Dip. Elettronica Applicata
Universitá degli Studi “Roma Tre”
Via Della Vasca Navale 84, I-00146 Roma, Italy
http://www.comlab.uniroma3.it/people.htm

**ATVS, Escuela Politecnica Superior,
Universidad Autonoma de Madrid,
C/ Francisco Tomas y Valente 11, 28049 Madrid, Spain
http://atvs.ii.uam.es/listpeople.do

Abstract

The security of biometric data is a very important issue in the deployment of biometric-based recognition systems. In this paper, we propose a signature-based biometric authentication system, where signal processing techniques are applied to the acquired on-line signature in order to generate protected templates, from which retrieving the original data is computationally as hard as randomly guessing them. A Hidden Markov Model (HMM)-based matching strategy is employed to compare the transformed signatures. The proposed protected authentication system generates a score as the result of the matching process, thus allowing to implement protected multibiometric recognition systems, through the application of score-fusion techniques. The experimental results show that, at the cost of only a slight performance reduction, the desired protection for the employed biometric templates can be properly achieved.

1. Introduction

The most emerging technology for automatic people recognition is biometrics. In contrast with traditional approaches, based on what a person knows (password) or what a person has (ID card, tokens), biometric-based authentication relies on who a person is or what a person does. Unfortunately, the use of biometric data in an automatic recognition system involves various risks, not affecting other traditional methods: if biometric data are somehow stolen or copied, they can be hardly replaced. Moreover, biometric data can contain sensitive information (health, genetic background, age), that can be used in an unauthorized manner for malicious or undesired intents [1]. Users' privacy can also be compromised if a cross-matching between different biometric database is performed, in order to track the enrolled subjects. Therefore, when designing a biometric-based recognition system, the issues deriving from the exposed security and privacy concerns have to be carefully considered. The adopted measures should be able to enhance biometric data resilience against attacks, while allowing the matching to be performed efficiently, thus guaranteeing acceptable recognition performance.

In this contribution, a non-invertible transform-based approach is proposed for the implementation of an on-line signature-based biometric authentication system, where the stored templates cannot reveal any information about the originally acquired biometric characteristics.

2. Biometric Template Security

In a typical biometric-based authentication system, eight possible vulnerable points can be individuated [2]. The unauthorized acquisition of the employed biometric data, which represents one of the possible consequences of the attacks to a biometric recognition system, is probably the most dangerous treat regarding the privacy and the security of the users. Different solutions have been investigated, in the recent past, to secure the biometric templates generated from the feature extractor module. Among them, the most promising approaches consist in the implementation of what have been called *cancelable biometrics*. The concept of cancelable biometrics has been introduced in [2], and can be roughly described as the application of an intentional and repeatable modification to the original biometric template. Through the application of these distortions to the biometric data, the properties of *renewability* and *non-invertibility* [2] should be guaranteed. Moreover, the recognition performance achievable using cancelable templates, in terms of False Rejection Rate (FRR) and False Acceptance Rate (FAR), should not degrade significantly, when compared to an unprotected system.

A classification of the already proposed solutions for the generation of secure and renewable biometric templates has been presented in [3], consisting of two macro-categories referred to as *biometric cryptosystem* and *feature transformation* approaches. Biometric cryptosystems typically employ binary keys in order to secure the biometric templates, and during the process some public information, usually referred to as *helper data*, is used. This category can be furthered divided in *key binding* systems, where the helper data are obtained by binding a key with the biometric template, as it happens for the *fuzzy commitment* [4] and the *fuzzy vault* [5], and *key generation* systems, where both the helper data and the cryptographic key are directly generated from

IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). IEEE, 2008. 1-6

DOI: http://dx.doi.org/ 10.1109/CVPRW.2008.4563114

the biometric template, as in [6].

In a feature transformation approach, a transformation function (typically dependent on some random parameters which are employed as transformation keys) is applied to the biometric templates, and the desired cancelable biometrics are given by the transformed versions of the original data. It is possible to distinguish between *salting* approaches, where the employed transformation functions are invertible, and where therefore the security of the templates relies in the secure storage of the function parameters [7], and *non-invertible transform* approaches, where a one-way function is applied to the considered biometrics, producing templates from which it is computationally hard to retrieve the original data, even if the transformation's defining parameters are known. Implementing recognition system according to this last category, the transformed templates can remain in the same (feature) space of the original ones, being then possible to employ, during the authentication, the matchers originally designed for the considered biometric templates, and thus allowing to guarantee performances that are similar to those of an unprotected approach. Moreover, having the possibility of employing dedicated matchers, a score can be obtained as the output of a recognition process, even if it has been performed in a transformed and secure domain: secure multibiometric systems can therefore be implemented through score-level fusion techniques [8].

The method presented in this paper falls in the category of the non-invertible transform approaches, being then possible to use it to protect the considered biometric data, while performing user authentication with performances very similar to those of an unprotected system, and giving the opportunity of designing multibiometric system. The first practical non-invertible transform-based approach for the protection of biometric data was presented in [9], where the minutiae pattern extracted from a fingerprint undergoes a key-dependent geometric transform. Generalizing this approach, three different non-invertible transforms, namely a cartesian, a polar and a functional transform, were proposed in [10] for generating cancelable fingerprint templates.

As far as signature template protection is concerned, it was first considered in [11] with a key generation approach. In [12] an adaptation of the fuzzy vault to signature protection is proposed, while also the fuzzy commitment (more specifically, its practical translation known as Helper Data System [13]) has been employed to provide security to the features extracted from an on-line signature, as proposed in [14]. A comprehensive survey on signature template protection can be found in [15]. Each of the referenced approaches relies on the extraction of some parametric features from the considered on-line signatures. On the other hand, the approach proposed in this paper directly works with the signature time sequences acquired by touch screens or digitizing tablets, trying to modify them in such a way that is computationally hard to recover the original information. Dealing with time sequences instead of parametric features will allow to manage a greater amount of information, thus enabling us to obtain significant authentication performances, as outlined in Section 5.

3. Proposed Approach for Cancelable On-line Signature Biometrics

As already pointed out, in this paper a non-invertible transform approach is proposed for the protection of on-line signature templates. Specifically, the template that has to be protected consists of a set of signature discrete time sequences (e.g., position trajectories, pressure, etc.). The desired protection is accomplished by properly modifying the considered time sequences, in such a way that it is not possible to retrieve the original data from the transformed one. A *function-based* authentication approach is then implemented in order to perform the matching, directly applying Hidden Markov Models (HMMs) for the modelization of the transformed templates. In Section 3.1, the employed feature extraction process, together with the implemented matching strategy, is presented.

3.1. HMM-based Signature Modeling

The proposed authentication system with protected templates is based on the on-line signature verification system presented in [16], where a function-based approach is employed to perform signature-based authentication, using HMMs to represent and match the signature discrete time sequences. Specifically, in the proposed approach three time sequences, the horizontal $x[n]$ and vertical $y[n]$ position trajectories, together with the pressure signal $p[n]$ (where $n = 1, \dots, N$ is the discrete time index, and N is the time duration of the signature in sampling units), are acquired from each on-line signature through a digitizing tablet. A geometric normalization, consisting of positions normalization followed by rotation alignment, is applied to the considered pen-position functions. Then, other four discrete time sequences are derived from the basic set, and used as an additional extended set of functions, namely the path-tangent angle $\theta[n]$, the path velocity magnitude $v[n]$, the log curvature radius $\rho[n]$ and the total acceleration magnitude $a[n]$, with $n = 1, \dots, N$. The considered original signature representation is then derived using both the basic and extended sets, and consists of a matrix $\mathbf{U} = [\mathbf{u}[1], \dots, \mathbf{u}[N]]$ whose columns $\mathbf{u}[n]$ are obtained as $\mathbf{u}[n] = [x[n], y[n], p[n], \theta[n], v[n], \rho[n], a[n]]^T, n = 1, \dots, N$. Each row of matrix $\mathbf{U}$ is therefore given from one of the $F = 7$ considered signature time sequences.

Instead of training a HMM with the original signature template $\mathbf{U}$, we represent each signature using a transformed version of $\mathbf{U}$, indicated as $\mathbf{T} = [\mathbf{t}[1], \dots, \mathbf{t}[K]]$. Each column $\mathbf{t}[n]$, $n = 1, \dots, K$ represents a vector of

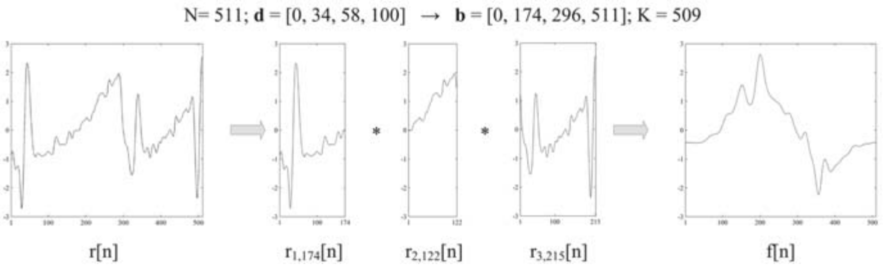

Figure 1. Example of a signature function transformation, where $W = 3$.

length F, whose elements $\mathbf{t}[n] = [f_{(1)}[n], \ldots, f_{(F)}[n]]^T$, $n = 1, \ldots, K$, are derived from the elements of the original template in such a way that it is not possible to recover $\mathbf{U}$ from the knowledge of $\mathbf{T}$.

HMMs are employed to model the obtained transformed signature representations $\mathbf{T}$. Specifically, the employed models are defined by the number of hidden states H, and by the number M of Gaussian densities which are used to describe the probability $p_h(\mathbf{t})$ of the emission of symbol $\mathbf{t}$ from the state h, $h = 1, \ldots, H$.

During enrollment, E signatures are acquired from each user, and a client model λ (composed by an initial distribution π, a state transition matrix $\mathbf{A}$ and an observation density functions B [16]) is estimated from the transformed signature representations $\left\{\mathbf{T}^{(1)}, \ldots, \mathbf{T}^{(E)}\right\}$, by following the iterative strategy presented in [16]. When the user claims his identity providing a new signature, its representation $\mathbf{T}$ is evaluated, and a similarity score is calculated as $(1/K) \log P(\mathbf{T}|\lambda)$ using the Viterbi algorithm [17].

3.2. Time Sequences Transformation

In the proposed approach, the number of transformed discrete functions $f_{(i)}[n]$, $i = 1, \ldots, F$ and $n = 1, \ldots, K$, which define the transformed template $\mathbf{T}$, equals the number F of the original functions. The transformed functions are generated through *linear combinations* of the time sequences belonging to the original signature template $\mathbf{U}$.

Specifically, in the proposed approach each transformed function $f_{(i)}[n]$ is derived from a single corresponding original function $r_{(i)}[n]$, which represents a generic original discrete time sequence selected among the F rows of $\mathbf{U}$ (*i.e.* among the signature functions $x[n], y[n], p[n], \theta[n], v[n], \rho[n]$, and $a[n]$). A number $(W - 1)$ of values d_j, are randomly selected between 1 and 99 in an ordered fashion, in such a way that $d_j > d_{j-1}$, $j = 1, \ldots, W$, and arranged in a vector $\mathbf{d} = [d_0, \ldots, d_W]$, having kept $d_0 = 0$ and $d_W = 100$. The vector $\mathbf{d}$ represents the key of the employed transformation. Then, the values d_j are converted according to the relations $b_j = \text{round}(\frac{d_j}{100} \cdot N)$, $j = 0, \ldots, W$, where round$(\cdot)$represents the nearest integer, and the original sequence $r_{(i)}[n]$ is divided into W segments $r_{(i)j,N_j}[n]$ of length $N_j = b_j - b_{j-1}$, each defined as

$$r_{(i)j,N_j}[n] = r_{(i)}[n + b_{j-1}], \qquad (1)$$

for $n = 1, \ldots, N_j$ and $j = 1, \ldots, W$. Basically, the function $r_{(i)}[n]$ is split into W separated parts according to the randomly generated vector $\mathbf{d}$, as illustrated in Figure 1 for the case with $W = 3$. A transformed function $f_{(i)}[n]$, $n = 1, \ldots, K$, is then obtained through the linear convolution of the functions $r_{(i)j,N_j}[n]$, that is,

$$f_{(i)}[n] = r_{(i)1,N_1}[n] * \ldots * r_{(i)W,N_W}[n]. \qquad (2)$$

Each transformed function $f_{(i)}[n]$ is therefore obtained through the linear convolutions of parts of the corresponding original functions $r_{(i)}[n]$, $i = 1, \ldots, F$. Moreover, each original function undergoes the same decomposition before applying the convolutions. As it can be seen, due to the convolution operation in (2), the length of the transformed functions is equal to $K = N - W + 1$, being therefore almost the same of the original functions one. A final signal normalization, oriented to obtain zero mean and unit standard deviation transformed functions, is then applied. Different realizations can be obtained from the same original functions, simply varying the size or the values of the parameter key $\mathbf{d}$. The security analysis of the proposed online signature template protection scheme is conducted in Section 4.

4. Security Analysis

Having defined the function transformation as in eq. (2), if an attacker gains access to the stored information, he has to resolve a *blind deconvolution* problem [18] to retrieve any information regarding the signature biometrics. Typically, the goal of blind deconvolution is to recover a source signal given only the output of an unknown filter, or to separate different source signals from their convolutive mixtures. However, some statistical properties of the filter, or of the considered sources, have to be assumed. Otherwise, some further constraints have to be established, in order to perform the process. In our case, the transformed template $\mathbf{T}$ contains only convolutions between segments extracted from the original functions, about which no *a priori* information can be assumed. Then, employing the proposed transformation, recovering in a deterministic way the original data from the transformed ones, employed to train the HMMs, is as much hard as randomly guessing the segments extracted from the signature functions.

Moreover, also considering different transformed templates employed in different systems (record multiplicity attack), it is not possible to retrieve the original signature sequences. In order to properly illustrate this, some assumptions have to be stated. First, it is supposed that the different transformed versions are derived from exactly the same original data (although this is almost impossible, being on-line signatures characterized by a significant intra-user variability). Moreover, it is worth pointing out that, in the proposed approach, for each user the HMM λ, estimated from the signature representations $\mathbf{T}$, is the stored template. Then, if someone wants to retrieve the original signature time sequences, he has to generate realizations from the available HMMs. In order to analyze the security of the proposed approach in the worst considerable case, it is assumed that, from a stored HMM λ, it is possible to synthesize exactly the same functions from which the model has been estimated. Under these assumptions, which define a very restrictive scenario, we then consider a case where an attacker has acquired, from two different systems, two different transformed signature representations $\mathbf{T}^{(1)}$ and $\mathbf{T}^{(2)}$, generated from the same original template $\mathbf{U}$. Considering the simplest case with $W = 2$, it is supposed that an attacker possess two transformed instances $f^{(1)}[n]$ and $f^{(2)}[n]$, $n = 1, \ldots, K = N - 1$, of the same original time sequence $r[n]$, $n = 1, \ldots, N$, obtained using respectively the transformation parameters $d_1^{(1)}$ and $d_1^{(2)}$. In order to retrieve the function $r[n]$, the attacker should be able to obtain the segments $r^{(1)}_{1,N_1^{(1)}}[n]$ and $r^{(1)}_{2,N_2^{(1)}}[n]$, where $N_1^{(1)} = b_1^{(1)}$ and $N_2^{(1)} = N - b_1^{(1)}$, or the segments $r^{(2)}_{1,N_1^{(2)}}[n]$ and $r^{(2)}_{2,N_2^{(2)}}[n]$, with$N_1^{(2)} = b_1^{(2)}$ and $N_2^{(2)} = N - b_1^{(2)}$, from the available transformed functions $f^{(1)}[n] = r^{(1)}_{1,N_1^{(1)}}[n] * r^{(1)}_{2,N_2^{(1)}}[n]$ and $f^{(2)}[n] = r^{(2)}_{1,N_1^{(2)}}[n] * r^{(2)}_{2,N_2^{(2)}}[n]$. Deconvolution problems are typically coped with in the frequency domain, being the convolutions transformed into simple multiplications. In order to properly define the Discrete Fourier Transforms (DFTs) of the considered sub-functions of $r[n]$, the extended versions $\hat{r}^{(j)}_{i,K}[n]$, $i, j = 1, 2$, are generated applying a zero padding to the respective original functions, until reaching the length $K = N - 1$ (that is the length of the convolutions $f^{(1)}[n]$ and $f^{(2)}[n]$). Then, a sequence $\Delta[n]$, $n = 1, \ldots, K$, is defined as the difference between $\hat{r}^{(1)}_{1,K}[n]$ and $\hat{r}^{(2)}_{1,K}[n]$, which share a common part that is exactly $r^{(2)}_{1,K}[n]$, having assumed that $b_1^{(1)} > b_1^{(2)}$:

$$\Delta[n] = \hat{r}^{(1)}_{1,K}[n] - \hat{r}^{(2)}_{1,K}[n], \quad n = 1, \ldots, K. \tag{3}$$

It can then be demonstrated that the following relations can be derived for the considered finite sequences:

$$\begin{cases} \hat{r}^{(1)}_{1,K}[n] = \hat{r}^{(2)}_{1,K}[n] + \Delta[n] \\ \hat{r}^{(1)}_{2,K}[n - b_1^{(1)}] = \hat{r}^{(2)}_{2,K}[n - b_1^{(2)}] - \Delta[n] \end{cases} \tag{4}$$

where all the considered shifts are circular shifts. Then, applying the DFT to the *a priori* known functions $f^{(1)}[n]$ and $f^{(2)}[n]$, and considering the relations between the DFT and the linear convolution of two discrete sequences, it results:

$$\begin{cases} DFT\{f^{(1)}[n]\} = DFT\{\hat{r}^{(1)}_{1,K}[n]\} \cdot DFT\{\hat{r}^{(1)}_{2,K}[n]\} = \\ \quad DFT\{\hat{r}^{(1)}_{1,K}[n]\} \cdot DFT\{\hat{r}^{(2)}_{1,K}[n - b_1^{(1)}]\} \cdot e^{j2\pi(k/K)b_1^{(1)}} \\ DFT\{f^{(2)}[n]\} = DFT\{\hat{r}^{(2)}_{1,K}[n]\} \cdot DFT\{\hat{r}^{(2)}_{2,K}[n]\} \end{cases} \tag{5}$$

and using the relations in (4), the first equation of (5) can be written as:

$$\begin{aligned} DFT\{f^{(1)}[n]\} = {} & \left[DFT\{\hat{r}^{(2)}_{1,K}[n]\} + DFT\{\Delta[n]\}\right] \cdot \\ & \left[DFT\{\hat{r}^{(2)}_{2,K}[n - b_1^{(2)}]\} - DFT\{\Delta[n]\}\right] \cdot \\ & e^{j2\pi(k/K)b_1^{(1)}} \end{aligned} \tag{6}$$

and therefore:

$$\begin{cases} DFT\{f^{(1)}[n]\} = e^{j2\pi(k/K)b_1^{(1)}} \cdot \Big[\\ \quad DFT\{\hat{r}^{(2)}_{1,K}[n]\} \cdot DFT\{\hat{r}^{(2)}_{2,K}[n]\} \cdot e^{-j2\pi(k/K)b_1^{(2)}} - \\ \quad DFT\{\Delta[n]\} \cdot DFT\{\hat{r}^{(2)}_{1,K}[n]\} + DFT\{\Delta[n]\} \cdot \\ \quad DFT\{\hat{r}^{(2)}_{2,K}[n]\} \cdot e^{-j2\pi(k/K)b_1^{(2)}} - DFT^2\{\Delta[n]\}\Big] \\ DFT\{f^{(2)}[n]\} = DFT\{\hat{r}^{(2)}_{1,K}[n]\} \cdot DFT\{\hat{r}^{(2)}_{2,K}[n]\} \end{cases} \tag{7}$$

As it can be seen, the obtained system cannot be resolved, due to the fact that the term $DFT\{\Delta[n]\}$ represents an additional unknown variable, added to the unknown functions $\hat{r}^{(2)}_{1,K}[n]$ and $\hat{r}^{(2)}_{2,K}[n]$. Then, also if an attacker is able to acquire more than two distinct transformed versions of the original signature functions, it is however impossible to recover the original information using the data coming from different sources.

5. Experimental Results

An extensive set of experimental results has been performed using the MCYT on-line signature corpus [19]. This database contains 330 users, for each of which 25 genuine signatures and 25 skilled forgeries have been captured during five different sessions.

In order to properly analyze the proposed non invertible transform-based signature template protection, the following aspects have been investigated:

- which is the variability of the matching performances when the transformation parameters are changed?

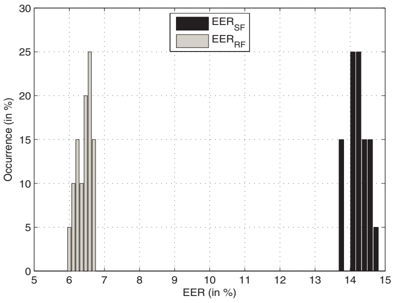

Figure 2. Normalized histograms for the EERs obtained repeating 20 times the authentication process. The employed system parameters are $W = 2$, $H = 16$ and $M = 2$.

- which is the loss in matching performances between an unprotected and a protected systems?
- which are the matching performances of protected systems employing different HMM parameters or a different number W of function decompositions?

First, we verified which is the variability of the authentication performance with respect on the selection of the system parameters, keeping fixed the number of segments W in which the signature time sequences are divided. The configuration initially considered for the experiments consists in the use of HMMs with $H = 16$ states and $M = 2$ Gaussian mixtures for each state. Each user is enrolled using the $E = 5$ signatures from the first session, while the other four sessions are employed to estimate the FRR. Systems' FAR for skilled forgeries (FAR$_{SF}$) was computed using the available 25 skilled forgeries for each user, while the FAR for random forgeries (FAR$_{RF}$) has been computed taking, for each user, one signature from each of the rest of the users. We considered the case where $W = 2$, and performed 20 times the authentication process over the entire MCYT database, varying at each iteration the transformation parameters $\mathbf{d}$ for each user. In Figure 2 the dependance of the matching performance from the employed transformation parameters is shown, through the normalized histograms of the Equal Error Rates (EERs) that are obtained considering both random (EER$_{RF}$) and skilled forgeries (EER$_{SF}$). As requested for a properly designed non-invertible transform method, varying the parameters of the employed transformation does not result in significant modifications for the matching performances. In our case, the mean EER value considering skilled forgeries is 14.2%, and the performances show a very low standard deviation of about 0.3%. The EER for random forgeries has a mean value of 6.4% and a standard variation of 0.2%.

Next, we performed tests to compare the performances of an unprotected and a protected system where HMMs are used as matching algorithm. Specifically, we kept the HMM configuration with $H = 16$ states and $M = 2$ Gaussian mixtures for each state, and performed the authentication using an unprotected system (employing then the same method of [16]), and a protected system based on the approach presented in Section 3, varying the number of division W for $W = 2, 3, 4$. For the protected system, the key vector $\mathbf{d}$ is randomly selected for each considered user, taking the values $d_j, j = 1, \ldots, W-1$, in the range of integers $[5, 95]$. In Figure 3 the achieved authentication rates, where the FAR is referred to the situation with skilled forgeries (FAR$_{SF}$), are presented. As it can be seen from the reported Receiver Operating Characteristic (ROC) curves, the EER for skilled forgeries in an unprotected system is equal to 10.74%, and it increases only slightly to 14.03% when the protection of the templates is introduced, considering $W = 2$. Performing the transformations keeping $W = 3$ results in an EER of about 19.24%, while if each signature function is divided in $W = 4$ segments before performing the convolutions, the EER raises to 24.92%. The loss in performance can be explained as due to the fact that, in the proposed approach, the division in segments of the considered signature time sequences is accomplished using a set of fixed parameters d_j, $j = 1, \ldots, W-1$, which express, in terms of the percentage of the total sequence length, the point where the separations have to be done. However, due to the characteristics of the signature biometrics, sequences extracted from different signatures, also if from the same user, typically have different lengths, and in order to align two signature sequences a dynamic programming strategy is typically needed (as in the Dynamic Time Warping approaches for signature recognition [20]), whereas a simple linear correspondence strategy does not represent the best signatures alignment approach. As a consequence, the more separations are performed, the more variable the convolutions at the output will be.

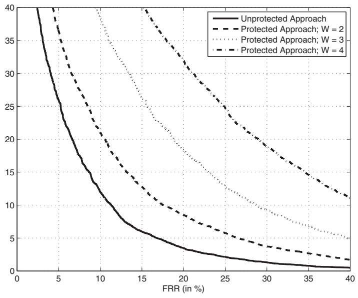

Figure 3. ROC curves for an unprotected system, and for protected systems with $W = 2, 3, 4$, considering skilled forgeries. The employed HMM parameters are $H = 16$, $M = 2$.

Moreover, the dependency of the authentication performances from the employed HMM has also been analyzed. Specifically, it has been found that the best recognition rates, both in the case of unprotected and protected systems, are achieved considering HMM with $H = 8$ or $H = 12$

H	M	Non-Protected Approach	Protected Approach		
			$W = 2$	$W = 3$	$W = 4$
8	1	13.45%	13.98%	17.11%	**21.24**%
	2	11.89%	**13.30**%	17.50%	22.83%
	4	11.14%	14.35%	19.41%	25.73%
	8	11.97%	14.65%	22.47%	29.50%
	16	15.00%	17.85%	31.18%	36.26%
12	1	11.85%	13.39%	**17.08**%	21.61%
	2	10.91%	13.44%	18.38%	23.92%
	4	11.20%	14.76%	21.14%	28.27%
	8	12.00%	16.52%	26.14%	34.08%
	16	**10.29**%	20.47%	34.30%	39.03%

Table 1. EERs for different HMM configurations considering skilled forgeries, in unprotected and protected systems.

states. In Table 1 the obtained EERs, considering skilled forgeries, are listed, indicating in bold the best authentication results. As it can be seen, the best performance achievable with an unprotected approach consists in an EER of 10.29%, and it occurs for $H = 12$ and $M = 16$. The best performances for the protected approach with $W = 2$ is about 13.30%, obtained for $H = 8$ and $M = 2$. Considering $W = 3$ or $W = 4$, the best achievable EERs are respectively 17.08% ($H = 12$ and $M = 1$) and 21.24% ($H = 8$ and $M = 1$).

6. Conclusions and Future Works

In this paper a biometric template protection scheme for on-line signature verification, based on a non-invertible transform, has been proposed. The functions employed for the authentication are derived from the original discrete time sequences, through non-invertible transformations based on convolutions. From the transformed functions, retrieving the original ones is as much hard as randomly guessing them. The experimental results show a very slight loss of performance in terms of EER, with respect to an unprotected system. Moreover, being able to provide a score as output of the authentication process, the proposed method can be employed for the construction of protected multibiometrics-based recognition system. Further improvements can regard the definition of other transformation function, based on the proposed one, and the analysis of the renewability capacity of the proposed non-invertible function-based template protection scheme.

References

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

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

[3] A.K. Jain, K. Nandakumar, and A. Nagar. Biometric template security. *EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics*, 2008.

[4] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In *6th ACM Conf. Computer and Communication Security*, pages 28–36, Singapore, 1999.

[5] A. Juels and M. Sudan. A fuzzy vault scheme. In *Proc. IEEE on Int. Sympos. on Information Theory*, page 408, 2002.

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

[7] A.B.J. Teoh, D.C.L. Ngo, and A. Goh. Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. *IEEE Trans. on PAMI*, 28(12):1892–1901, 2006.

[8] A. Ross, K. Nandakumar, and A.K. Jain. *Handbook of Multibiometrics*. Springer, USA, 2006.

[9] R. Ang, R. Safavi-Naini, and L. McAven. Cancelable key-based fingerprint templates. In *Proc. 10th Australian Conf. Information Security and Privacy*, pages 242–252, 2005.

[10] N. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle. Generating cancelable fingerprint templates. *IEEE Trans. on PAMI*, 29(4):561–572, 2007.

[11] C. Vielhauer, R. Steinmetz, and A. Mayerhöfer. Biometric hash based on statistical features of online signatures. In *Int. Conf. Pattern Recognit.*, volume 1, pages 123–126, 2002.

[12] M. Freire-Santos, J. Fierrez-Aguilar, and J. Ortega-Garcia. Cryptographic key generation using handwritten signature. In *Defense and Security Symp., Biometric Technol. for Human Identification*, volume 6202, pages 225–231, 2006.

[13] M. van der Veen, T. Kevenaar, G.-J. Schrijen, T.H. Akkermans, and F. Zuo. Face biometrics with renewable templates. In *SPIE Proceedings on Security, Steganography, and Watermarking of Multimedia Contents*, volume 6072, 2006.

[14] E. Maiorana, P. Campisi, and A. Neri. User adaptive fuzzy commitment for signature templates protection and renewability. *SPIE Journal of Electronic Imaging, Special Section on Biometrics: Advances in Security, Usability and Interoperability*, March 2008.

[15] P. Campisi, E. Maiorana, and A. Neri. On-line signature based authentication: template security issues and countermeasures. *Biometrics: Theory, Methods, and Applications, N. V. Boulgouris, K.N. Plataniotis, and E.Micheli-Tzanakou, editors, Wiley/IEEE (in print)*, 2008.

[16] J. Fierrez, D. Ramos-Castro, J. Ortega-Garcia, and J. Gonzalez-Rodriguez. HMM-based on-line signature verification: feature extraction and signature modeling. *Pattern Recognition Letters*, 28(16):2325–2334, 2007.

[17] L.R. Rabiner. A tutorial on hidden markov models and selected applications in speech recognition. *Proceedings of the IEEE*, 7(2):257–286, 1989.

[18] S. Haykin. *Blind Deconvolution*. Prentice-Hall, 1994.

[19] J. Ortega-Garcia et al. MCYT baseline corpus: A bimodal biometric database. *IEE Proceedings Vision, Image and Signal Processing, Special Issue on Biometrics on the Internet*, 150(6):395–401, 2003.

[20] M. Faundez-Zanuy. On-line signature recognition based on VQ-DTW. *Pattern Recognition*, 40:981–992, 2007.