CIHSPS 2006 - IEEE International Conference on
Computational Intelligence for Homeland Security and Personal Safety
Alexandria, VA, USA, 16-17 October 2006

Personal identification and verification using multimodal biometric data

Stelvio Cimato, Marco Gamassi, Vincenzo Piuri, Daniele Sana, Roberto Sassi, and Fabio Scotti

Dipartimento di Tecnologie dell'Informazione,
Università di Milano,
via Bramante, 65 – 26013 Crema, Italy
E–mail: {cimato, gamassi, piuri, sana, sassi, fscotti}@dti.unimi.it.

Abstract – *Several proposals have been formulated to combine cryptography and biometrics in order to secure data and to strengthen the personal authentication process, making the falsification of personal ID, like passports, more challenging.*

In this work we describe a system for personal identification and verification, based on the combination of multiple biometric readings and other user inputs. In such way authentication control can be performed and only allowed persons can access the resources which must be protected.

The method consists of two main phases: enrollment and verification. In the first phase the data extracted from user inputs are processed by the proposed system and stored the in a innovative non-reversible form. In the second phase, the stored data are combined with the biometric readings and other user inputs in order to identify and verify the identity of the person. The system does not rely on network access or databases to perform the verification/authentication phase.

Keywords – *Biometric identification, Privacy, biometric documents, e-passports.*

I. INTRODUCTION

Recently, many research efforts have tackled the problem of devising practical systems for personal identification and verification relying on biometrical data. Several commercial systems have been proposed by companies, such as Bioscrypt Inc. (formerly Mytec Technologies Inc.), etc. Such commercial implementations usually do not provide security guarantees in explicit form and rely on proprietary procedures which are generally not disclosed to the general public. On the other hand, researchers have devised systems which do not fit the challenge of real world applications very well. In fact, such systems rely on low error tolerance thresholds or on infrastructures which are not already available or worldwide accepted.

Biometrics such as fingerprints, voice and face are permanently associated with the user and can therefore obviate the need to carry tokens or remember passwords and keys. Unfortunately, the higher variability within different readings of biometric data makes them unsuitable to be directly used to secure data. In fact, cryptographic keys have zero uncertainty and a single-bit difference (in the key or in the message) spoils the possibility of accessing the encrypted data. On the other side, the strict association between each user and his biometrics templates raises concerns on possible uses and abuses of such kind of sensible information. For all of these traits privacy is a critical issue since, in the case their digital representation is loss or stolen, they cannot be replaced or modified in any way. In literature a wide range of techniques have been presented, based on the combination of biometrics and cryptography, in order to cope with both problems: variability of biometric templates and protection of personal data.

The process of generating cryptographic keys from biometrics generally relies on an error tolerant binary representation of the biometrics features. In Davida et al. [1], [2], hash functions are used to protect the sensitive user template. Furthermore, error correction codes are employed in order to extract an unique associated feature from each different biometric reading: the different readings are treated as corrupted codewords and are accordingly decoded. During the verification phase, the feature retrieved by a biometric reading is given as input to an hash function, and compared with the hash value stored during the enrollment phase.

Juels and Wattenberg [3] proposed the "fuzzy commitment" scheme where a secret message is protected using a biometric template. Also in this case, an error correcting code is used in order to associate a codeword c with a person and compute an offset ($\delta = c \oplus x$) for the biometric template x. The encrypted message (the *fuzzy commitment*) is then represented by the pair $(\delta, h(c))$, where $h(c)$ is a one way hash function. It is worth to notice that neither the biometric feature, nor the associated codeword are publicly stored. The authentication process is correctly performed if a fresh biometric reading y allows the computation of a binary string $c' = \delta \oplus y$ sufficiently close to c so that the code decodes it to c and the comparison between their hash values succeeds. Moving in the same direction, Hao et al proposed a biometric key generation procedure, which is based on an iris code feature extraction algorithm and on the combined use of Hadamard and Reed-Solomon codes [4]. Juels and Sudan also proposed a "fuzzy vault scheme" in [5] relying on the polinomial interpolation technique in order to cope with variability of the biometrics template stored.

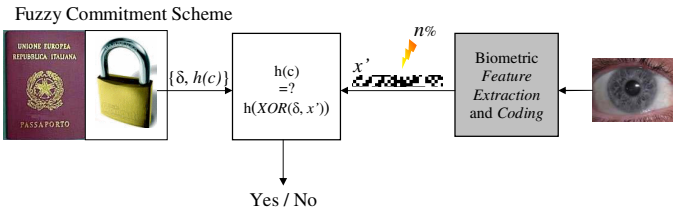

Fig. 1. Application of a Fuzzy Commitment Scheme for identification (Verification phase). The method does not allow the adoption of traditional biometric matching systems.

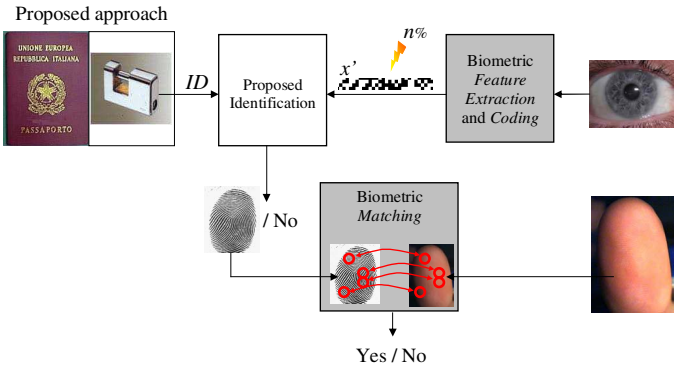

Fig. 2. Application of the proposed method for identification (Verification phase). The proposed method allows the adoption of any biometric matching system.

II. METHOD

The following section describes the proposed method (which was patented) and discusses the differences with respect to the approaches previously presented in the literature.

A. Comparison with other systems and methods in literature

The present technique uses an approach similar to the one described in Juels and Wattenberg [3], to achieve a system and method for personal identification and verification, but it differs with respect to inputs/outputs, techniques and usage.

Figure 1 shows the application of fuzzy commitment scheme in the verification phase. The biometric traits given by the individual are acquired and coded by a classical biometric system (encompassing acquisition, feature extraction and coding modules) into a string of bits x' (upper left). Different acquisitions of the same biometric trait of the same individual can produce differences in the bits of the coded string up to $n\%$ in order to be correctly identified (where n can vary tipically from 10% up to 25%). It is worth noting that the usage of the fuzzy commitment scheme as described can be considered as a biometric identification process since the input is indeed a biometric trait. On the other side, the fuzzy commitment scheme does not work as a traditional biometric system since it produces the identification answer just checking the condition $h(\delta \oplus x') = h(c)$. The condition can be thought as positive if the string of bits in input x' has enough bits in common with the string x required to give a positive authentication. Recently, Hao et al [4] proposed a practical application relying on the fuzzy commitment primitive of Juels et al to generate a biometric key up to 140 bits long. In their setting the key is a random string of bit which is double encoded using first an Hadamard code and then a Reed Solomon code. The resulting string (2048 bits long) is then xored to the iris code of the subject and the result is stored on a physical token (a smart-card) together with the hash of the key. In the decoding phase, the iris sample of the subject holding the token is used to unlock and recover the key previously stored.

Such approaches have two main drawbacks:

1. At the moment, to the best of our knowledge, most of the common biometric feature extraction algorithms find difficulties when deployed with fuzzy commitment primitive. In fact, one of the requirements is that the biometric matching scheme has an error rate (the rate of bits in the pattern which could be modified without affecting the biometric identification of the subject) compatible with the error rate of the correcting code. For example, the BCH code employed by Juels in [3] withstands an error rate up to 25%. The system proposed by Hao et al [4], which uses Hadamard and Reed-Solomon codes, achieves a 27% of bit error rate.
2. The proper "matching" phase" present in all biometric systems has been substituted with the bit comparison $h(\delta \oplus x') = h(c)$. In this sense the matching phase is not properly biometric since it does not compare biometric features.

The method we propose tries to offer a solution to the main drawbacks of fuzzy commitment schemes. We will delve into the details of the method in the next section. Figure 2 shows a sketch of the basic functioning of the proposed method during the verification phase. Our method is multimodal, in the sense that at least two biometric readings must be processed (but strictly speaking, only one "classical" biometric matching is performed). Firstly, a biometric reading (e.g., an iris scan) is processed in order to extract a binary string x' containing the relative biometric feature. After an error corcecting phase, such string is employed to retrieve from an ID a second set of biometric features previously extracted during the enrollment phase. A repeated failure of the retrieval process implies that the carrier of the document is an impostor. Otherwise, the retrieved biometric features are compared with a fresh biometric reading in a classical biometric matching phase.

Figure 3 shows the overall structure of the method we propose. As depicted, more than two biometric traits can be simultaneously employed. In the following subsection we detail the functioning of the basic modules: The first one creates the non reversible ID starting from the biometric samples (*enrollment* module). The second (*verification module*) performs the identification process just described.

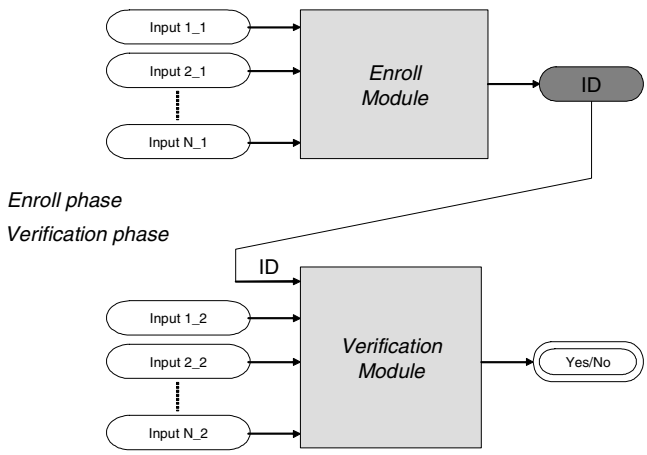

Fig. 3. The overall structure of modules required by the proposed approach.

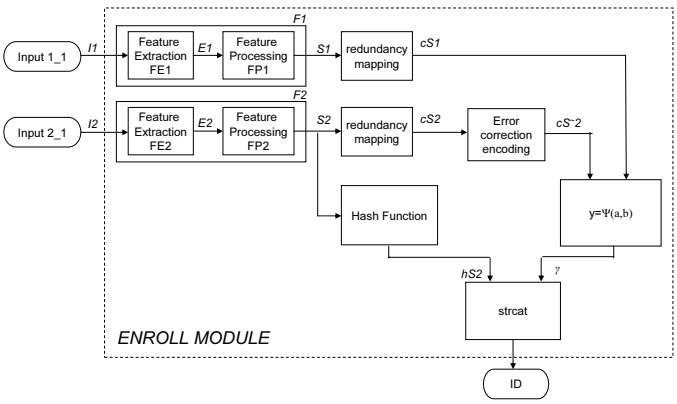

Fig. 4. The enroll module.

B. Creation of the ID (Enrollment module)

During the *enrollment* phase, the user is assigned a suitable ID. The ID might be then stored as desired by the issuing authority (passport, badge, ...) and must be provided during any verification phase. The general structure is depicted in Figure 4.

At least two different biometric features, I_1 and I_2, are collected at baseline (in the next Section some suggestions will be provided on how to use a number of biometrics samples larger than two). The two biometric readings are then separately processed to extract two sets of biometric features as usual. The proposed system relies on at least a couple of feature extraction algorithms $\mathcal{F}_1$ and $\mathcal{F}_2$ which can be selected among the already known feature extraction algorithms in literature. Each generic feature extraction algorithm $\mathcal{F}_i$ returns an output encodable in a n_i bit long key and has an error rate r_i (the rate of bits in the pattern which could be modified without affecting the biometric identification of the subject).

The two algorithms $\mathcal{F}_1$ and $\mathcal{F}_2$, whose bit string outputs are $S_1 = \mathcal{F}_1(I_1)$ and $S_2 = \mathcal{F}_2(I_2)$, respectively, may be used in pair only if $n_2 \leq (1-2r_1)n_1$.

Upon letting $\kappa = \lfloor (1-2r_1)n_1 \rfloor$, each n_i-bit key is then mapped to a longer codeword cS_i, replacing each bit with a corresponding pattern of $m = \lceil \log_2(n_1) \rceil$ bits. We will refer to this mapping with the term "redundancy mapping". For the sake of simplicity, let's assume here that each bit set to 0 in S_i is mapped to a pattern made of m-zeros, while each 1 to an all-ones pattern.

The shortest codeword cS_2 is padded with $\kappa - n_2$ m-bits words and it is subsequently encoded using a $(N = n_1, \kappa)$-Reed-Solomon (possibly shortened) code. This ensures that up to $\lceil (n_1 - \kappa)/2 \approx r_1 n_1 \rceil$ symbols might be corrupted without affecting the decoding process. Please note that the encoded message $c\tilde{S}_2$ is now $n_1 m$ bits long.

Afterwards, cS_1 is combined with $c\tilde{S}_2$ by means of a function $y = \Psi(a, b)$. Ψ must be such that it exists a function Ψ^* so that $b = \Psi^*(a, y)$. A possible choice for Ψ is $\oplus$, the XOR function, for which $\Psi^* = \Psi$.

Finally, the ID is constructed appending $\gamma = \Psi(cS_1, c\tilde{S}_2)$ to $\mathcal{H}(S_2)$ an hashed version of S_2 (for example using SHA-1).

For exemplificative purposes and without any loss of generality, let consider I_1 to be an iris scan and I_2 a fingerprint reading. Moreover, let assume $\mathcal{F}_1$ to be the IrisCode® technique suggested by Daugman [] for which $n_1 = 2048$ and $r_1 = 0.32$, and $\mathcal{F}_2$ a minutiae extraction procedure which has $n_2 = 640$ and r_2 is unknown. Let us compute $N = n_1 = 2048$ and $\kappa = \lceil 2048(1 - 2 \times 0.32) \rceil = 737$. The condition $n_2 \leq \kappa$ is fulfilled, thus the two biometric sets can be used together.

First, the 640-bits key S_2 is redundancy mapped such that each 0 is substituted with the $m = 12$ bits-long word "000"(hexadecimal) and each 1 with "FFF" (hexadecimal). Also, the new codeword is prepended with $\kappa - n_2 = 737 - 640 = 97$ null "000" patterns. Then, cS_2 is encoded using a $(N = 2048, \kappa = 737)$ Reed-Solomon shortened code and $\gamma = cS_1 \oplus c\tilde{S}_2$. Finally, S_2 is hashed, leading to $hS_2 = \mathcal{H}(S_2)$. The ID is built composing hS_2 and γ.

C. Verification module

When the subject has to prove his identity (*verification* phase), he furnishes the ID he received during the enrollment phase. Figure 5 shows the structure of the verification module.

Let us denote with J_1 and J_2 the biometric features freshly collected and with Σ_1 and Σ_2 the corresponding bit strings computed. The ID provided by the subject is split into γ and the hash hS_2.

Firstly, Σ_1 is redundancy mapped into $c\hat{S}_1$ which is next used to extract a corrupted version of $c\tilde{S}_2$, $c\tilde{S}'_2 = \Psi^*(c\hat{S}_1, \gamma)$. By definition of $\mathcal{F}_1$, two different biometric readings of the same subject produce two keys whose Hamming distance (HD) is smaller than r_1; on the other hand, HD$> r_1$ when the readings belong to different subjects. In the first case, i.e, if the subject who tries to validate is the same who also went through the enrollment phase, $c\tilde{S}'_2$ and $c\tilde{S}_2$ will differ for a number of words $< r_1 n_1$ only.

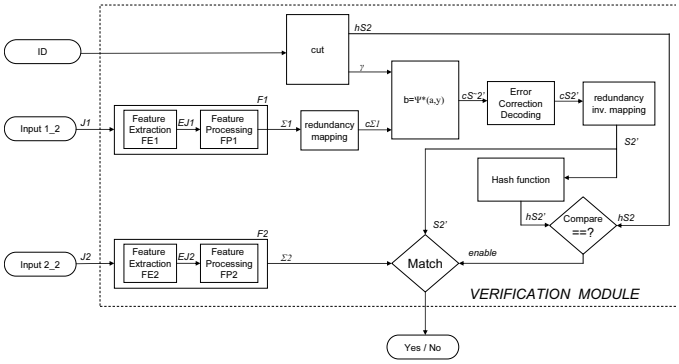

Fig. 5. The verification module.

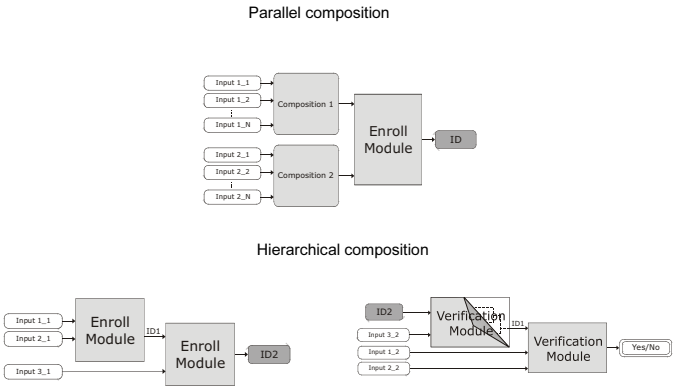

Fig. 6. Examples of possible compositions of the proposed basic modules during the enroll and verification phases.

Up to $t = r_1 n_1$ "errors" are corrected using on $c\tilde{S}'_2$ a (N, κ)-Reed Solomon decoder and the decoded value S'_2 is identical to S_2 collected if the subject is not an impostor and the number of bits in Σ_1 which have a different value S_1 is smaller than $r_1 n_1$. For security reasons (the method was set up so that no biometric features were comprised into the ID), there is no S_2 to compare with, but we can still compare the hashed values.

If $\mathcal{H}(S'_2) = hS_2$, then $S'_2 = S_2$ and S'_2 is then used in a usual biometric comparison with Σ_2, the features collected during the verification phase.

D. Composition of basic modules

It is possible to compose the basic modules in order to create different levels of security, complexity and use a higher number of different biometric features in the identification/verification procedures. For example, the basic *enrollment* and *verification* modules could be combined in parallel or hierarchically. Figure 6 shows two examples of these basic compositions.

The *parallel composition* offers a simple method to exploit different biometric traits in order to create the ID. This way, the level of multi-modality implemented is higher than in the standard approach since more than two biometric traits are in use. However, the error rate r in the composed input needs particular scrutiny as each biometric method differently contributes to the overall error rate.

Basic modules can be composed also in hierarchical structures. Without loss of generality, figure 6 shows an example of a two levels hierarchical composition. Biometric inputs I_1 and I_2 are used to create $ID1$ by means of a basic enroll module. Then, $ID1$ is used in place of a biometric trait in a second basic enroll module together with a third biometric input I_3 leading to the creation of $ID2$.

The hierarchical composition enables *different levels of security*. In low-security applications only the biometric inputs J_2 and J_3 could be required to verify $ID1$. On the other hand, in high-security applications, a third biometric sample J_1 would be required to verify also $ID2$ (obviously given the fact that the verification of $ID1$ had been successful).

Figure 6 (bottom, right) shows the structure of the hierarchical verification module. The module is composed by two basic verification modules. The inputs $ID1$, J_2 and J_3 are verified by the *first* basic verification module. Then, the output of the first basic verification module is used to eventually *enable* the functioning of the *second* verification basic module. This output can be also used as a *first-level security authentication signal*. Additionally, the identity of the user could be verified also using the input $ID2$ and the third biometric input J_1. The output of the second basic verification module is the *second security-level authentication signal*.

It is worth noting, that it is possible to build more complex systems by using each method of composition (parallel and hierarchical) recursively or by combining the methods iteratively.

III. CONCLUSION

The method presented in this short paper permits to identify and verify the identity of persons using more than one biometric trait simultaneously. Building over Juel's Fuzzy Commitment scheme the features extracted from the biometrics are fuse together in a non reversible fashion. The system is multimodal since it works using at least two different biometric traits (for example the iris pattern and the fingerprint).

The method is particularly suitable for controlling the access of authorized persons into restricted areas like through borders or into high security zones. Given the fact that the ID carried by the persons seeking access contains only a code obtained from the biometrics and not the biometrics themselves, the method might help reducing the concerns often present when adopting biometrics ID. In fact, when lost or stolen the ID is of no use in obtaining the carrier biometrics traits.

The technique we suggest does not rely on network infrastructure or on the storage of information into database. Therefore, it might be used also in those situations in which such facilities are difficult or impossible to access. Secondarily, as

no biometric information is stored into a central database, the risk of having it tampered and sensible information exposed is avoided. For example, a bank could use such an identification system to let customers access their accounts through an ATM machine without the need of building a large database of biometrics features.

REFERENCES

1. G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric," in *Proceedings of the IEEE International Symposium on Security and Privacy, 1998*. 1998, pp. 148–157, IEEE Press.
2. G. I. Davida, Y. Frankel, B. J. Matt, and R. Peralta, "On the relation of error correction and cryptography to an off line biometrics based identification scheme," in *WCC99, Workshop on Coding and Cryptography*, 1999.
3. A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *CCS '99: Proceedings of the 6th ACM conference on Computer and communications security*, New York, NY, USA, 1999, pp. 28–36, ACM Press.
4. F. Hao, R. Anderson, and J. Daugman, "Combining cryptography with biometrics effectively," Tech. Rep. UCAM-CL-TR-640, University of Cambridge, Computer Laboratory, United Kingdom, July 2005.
5. A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proceedings of the IEEE International Symposium on Information Theory, 2002*, A. Lapidoth and E. Teletar, Eds. 2002, p. 408, IEEE Press.