A Privacy-compliant Fingerprint Recognition System Based on Homomorphic Encryption and Fingercode Templates

Mauro Barni[1], Tiziano Bianchi[2], Dario Catalano[3], Mario Di Raimondo[3], Ruggero Donida Labati[4], Pierluigi Failla[1], Dario Fiore[5], Riccardo Lazzeretti[1], Vincenzo Piuri[4], Alessandro Piva[2], Fabio Scotti[4]

***Abstract*— The privacy protection of the biometric data is an important research topic, especially in the case of distributed biometric systems. In this scenario, it is very important to guarantee that biometric data cannot be steeled by anyone, and that the biometric clients are unable to gather any information different from the single user verification/identification. In a biometric system with high level of privacy compliance, also the server that processes the biometric matching should not learn anything on the database and it should be impossible for the server to exploit the resulting matching values in order to extract any knowledge about the user presence or behavior.**

Within this conceptual framework, in this paper we propose a novel complete demonstrator based on a distributed biometric system that is capable to protect the privacy of the individuals by exploiting cryptosystems. The implemented system computes the matching task in the encrypted domain by exploiting homomorphic encryption and using Fingercode templates. The paper describes the design methodology of the demonstrator and the obtained results. The demonstrator has been fully implemented and tested in real applicative conditions. Experimental results show that this method is feasible in the cases where the privacy of the data is more important than the accuracy of the system and the obtained computational time is satisfactory.

I. INTRODUCTION

Biometric traits are more and more exploited for authentication and identification tasks in a multitude of applications ranging from institutional, governance, police and commercial systems. The use of biometric technologies within such applications requires the protection of the biometrics templates and the protection of the user privacy, as well [1]. In order to guarantee the user privacy, it is of paramount importance that the collected biometric information should not be used for any other activities than the ones expressly declared, and, at the same time, that the biometric system is capable to protect and avoid any misuse of the biometric information in [2].

The privacy protection of the biometric data is even much more critical in the case of distributed biometric systems since the biometric data are transmitted through a network infrastructure and hence it is greatly reduced the direct user control about her/his biometric information. In a distributed biometric system with an high level of privacy compliance, also the server that processes the biometric matching should not learn anything on the database and it should be impossible for the server to exploit the resulting matching values in order to extract any knowledge about the user presence or behavior.

In this paper, we refer to the general application where a biometric client checks if the "fresh" captured fingerprint belongs to the database of authorized entities managed by a biometric server. In order to preserve the users privacy, we require that the biometric client trusts the server to correctly perform the matching algorithm for the fingerprint recognition and it also should not learn anything about the fingerprint templates stored in the server with the exception of the resulting matching process. On the biometric server side, we want to guarantee that it is not possible to get any information about the requested biometry and even also the resulting matching value. This working hypothesis is very important since it allows to avoid any tracking and logging activity of the user presence and behavior on the server side.

Within this conceptual framework, in this paper we propose a novel complete demonstrator and the related design methodology. This demonstrator is capable to deal with distributed biometric systems protecting the privacy of the individuals by exploiting cryptosystems. The implemented system computes the matching task in the encrypted domain by exploiting homomorphic encryption and using the fingerprint templates proposed by A. K. Jain called Fingercode [3]. In particular, in this paper we propose the design of all the step required to implement the demonstrator while a complete discussion about the cryptographic aspects of the adopted protocol is available in [4].

In the proposed demonstrator, the biometric client captures the user fingerprint trait and it processes the obtained sample in order to produce the related Fingercode template (Fig. 1).

This work was supported in part by the MIUR (Ministero dell'Università e della Ricerca) under Grant 2007JXH7ET. The research at the University of Milan was also supported in part by the EU within the 7FP project "PrimeLife" under grant agreement 216483.

[1]M. Barni, P. Failla, R. Lazzeretti, are with the Department of Information Technologies, Università degli Studi di Siena, Siena, SI, 53100, Italy. barni@dii.unisi.it, (pierluigi.failla, riccardo.lazzeretti)@gmail.com

[2]T. Bianchi and A. Piva are with the Department of Electronics and Telecommunications, Università degli Studi di Firenze, Firenze, FI, 50139, Italy. (tiziano.bianchi, alessandro.piva)@unifi.it

[2]D. Catalano and M. Di Raimondo are with the Department of Mathematics and Computer Science, Università degli Studi di Catania, Catania, CT, 9515, Italy. (catalano, diraimondo)@dmi.unict.it

[4]R. Donida Labati, V. Piuri, and F. Scotti, are with the Department of Information Technologies, Università degli Studi di Milano, Milano, MI, 20122, Italy. (ruggero.donida, vincenzo.piuri, fabio.scotti) @unimi.it

[5]D. Fiore is with the Ecole Normale Supèrieure, France. dario.fiore@ens.fr

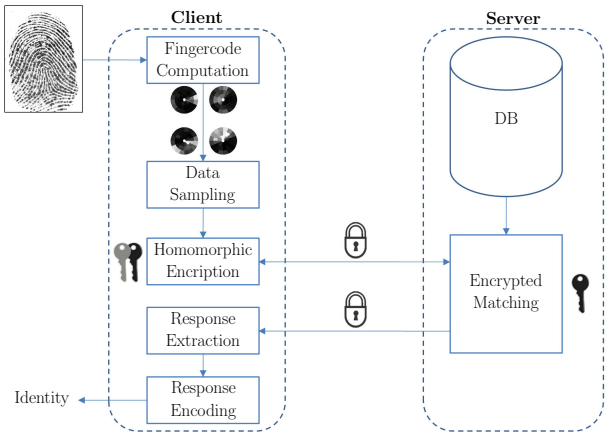

Fig. 1. Scheme of the proposed demonstrator.

The underling cryptographic protocol accepts in input only integer values, hence a data sampling operation is needed in order to suitably convert the floating point elements of the Fingercode template in integer values. The quantization step of the Fingercode template is critical since it effects the final accuracy of the overall system and the final requested bandwidth. A discussion of the design of the quantization step is given in the following sections.

In the proposed demonstrator, the fresh biometric template is sent to the biometric server in the encrypted format and the server returns the identity information in the encrypted format as well (or just a boolean outcome for the authentication request). Hence, on the server side (the right subplot in Figure 1), it is not possible to extract or determine any personal information on the biometric data of the users during all the phases of the verification / identification procedures. Further details on the encryption methods used in the demonstrator will be given in the related section of the paper.

The contribute of the paper is twofold. At the best of our knowledge, no such complete demonstrator has been proposed yet in the literature. Moreover, the paper presents a complete discussion of the design methodology dealing with all theoretical and implementation aspects of demonstrator with specific reference to the effects of Fingercode quantization on the template size, final accuracy and bandwidth of the system. Experimental results show that the proposed method is feasible in the cases where the privacy of the data is more important than the accuracy of the system. Obtained performance in terms of accuracy, efficiency and used bandwidth are satisfactory.

The paper is structured as follows. In the next section, the state of the art of the privacy protection of the biometric data is resumed. Section III presents the proposed demonstrator and the related design methodology, then in Section IV we discuss the implementation and the demonstrator, its accuracy and performance evaluation in different applicative conditions, and the obtained results.

II. Previous work

The objective of the most of the systems for the privacy protection of the biometric data in the literature is to modify the stored biometric templates for denying the access to these data to unauthorized persons. These methods can be divided in four different categories.

- **Biohashing**: the biometric features are transformed using a function defined by a user-specific key or password. Usually this transformation is invertible. The system proposed in [5] is based on the face, but similar techniques can be applied to different biometric traits (e.g. iris and fingerprint [6]).
- **Noninvertible transform**: the biometric template is secured by applying a noninvertible transformation function to it. There are methods based on different biometric traits. For example, in [7] it is used the fingerprint, and in [8] the iris. The main problem is that it is necessary to study the tradeoff between discriminability and noninvertibility of the transformation function. In [9] is presented a study on the measurement of the noninvertibility of methods based on the fingerprint.
- **Key-binding biometric cryptosystem**: the template is secured by applying cryptographic algorithms. Usually, the system must compute a transformation of the encrypted templates in the plain domain. This task is usually time expansive. Examples of methods used by this approach are the fuzzy commitment scheme [10] and the fuzzy vault [11].
- **Key generating biometric cryptosystem**: these methods compute the cryptographic key directly from the biometric data (e.g. [12]). The main problem is that it is difficult to generate keys with high stability and entropy. This approach can also be useful in other applications (e.g. in [13]).

Furthermore, there are methods applicable to multi-biometric system (e.g. in [14]). Unfortunately, in the most of the cases, the obtained accuracy is decreased by the transformation method.

In the literature, there are other methods for the protection of the privacy of the template Fingercode. For example, in [15] a method based on fuzzy vault is used and in [16] a biohashing transformation is applied. Our method encrypts the data with robust algorithms and the encryption does not impact to the accuracy because we use an homomorphic cryptosystem.

A similar approach to the privacy preserving authentication through biometric measures but applied to the face recognition is used in [17], [18]: the former makes use of homomorphic encryption, as in the present work, but presents a rounds complexity that is logarithmic in the number of the verified features and a huge bandwidth requirement; the latter is more efficient and bandwidth saving (with constant round complexity) and exploits the use of both homomorphic encryption and Garbled Circuits [19].

There are also systems that can compute the Hamming distance between biometric templates (e.g. Iriscode [20]) that

are use homomorphic encryption methods. For example, the system in [21] is based on the Blum-Goldwasser cryptosystem, the system in [22] on the Goldwasser-Micali scheme, the system in [23] on the method on homomorphic properties of Goldwasser-Micali and Paillier cryptosystems, the system in [24] on the ElGamal scheme and Garbled Circuits.

There are also systems that secure the data by distributing the tasks of classifiers based on computational intelligence techniques in the server and client side. In [25], [26] a method based on Support Vector Machines (SVM) is used. The main drawback of this system is that requires a preliminary training phase.

III. The Design of the Demonstrator

The proposed approach can be applied in distributed biometric systems in verification/identification tasks. Without any lack of generality, in the following we present the implementation of the method for the identification procedure. On the client side (left subplot, Figure 1), the biometric sample is captured and then computed in order to obtain the related Fingercode template [3] (*Template Creation* step). Then, the floating point elements of the Fingercode template are sampled and converted to integers in order to allow the adoption of the following encryption method (*Template Quantization* step). The important effects on the final accuracy and bandwidth of this step will be further discussed in the following subsections. The reduced template is now encrypted using the public-key of the client and the biometric matching is processed on the server side (right subplot, Figure 1) by an homomorphic cryptosystems (*Encrypted Matching* step). The matching algorithms do not transform the data in the plain domain. All computation steps of the matching method (evaluation of the matching value, thresholding and extraction of the best candidates) are processed directly in the encrypted domain. Let us now detail all the design steps of the proposed demonstrator.

A. Template Creation

The computation of the biometric template in the plain domain is based on a method that uses the Fingercode template. This method starts with the estimation of the reference point that we implemented with the following steps:

- Definition of the ROI as a ring with fixed size (height H).
- The ROI is partitioned in N_R rings and N_A arcs, obtaining $N_S = N_R \times N_A$ sectors S_i.
- A bank of N_F Gabor filters with different directions is applied to the image obtaining N_F filtered images $F_{i\theta}(x, y)$. A symmetric Gabor filter has the following general form in the spatial domain:

$$G(x, y; f, \theta) = \exp\left\{-\frac{1}{2}\left[\frac{x'^2}{\sigma_{x'}^2} + \frac{y'^2}{\sigma_{y'}^2}\right]\right\}\cos(2\pi f x'), \quad (1)$$

$$x' = x\sin\theta + y\cos\theta, \quad (2)$$

$$y' = x\cos\theta - y\sin\theta, \quad (3)$$

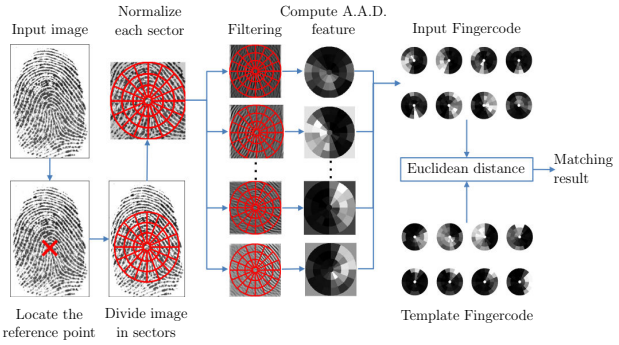

Fig. 2. Scheme of the biometric recognition method based on the template Fingercode.

where f is the frequency of the sinusoidal plane wave along the direction θ from the x-axis, and $\sigma_{x'}$ and $\sigma_{y'}$ are the space constants of the Gaussian envelope along x' and y' axes, respectively.

- The Average Absolute Deviation (AAD) from the mean of gray values in individual sectors in filtered images is computed to define the feature vector that represent the biometric template. The value $V_{i\theta}$ of the template related to each sector of each filtered image is computed as:

$$V_{i\theta} = (1/n_i)\left(\sum_{1}^{n_i} |F_{i\theta}(x, y) - F_{i\theta}|\right) \quad (4)$$

where n_i is the number of pixels in S_i and $P_{i\theta}$ is the mean of pixel values $P_{i\theta}$ of $F_{i\theta}(x, y)$ in sector S_i.

The obtained feature vector is composed by $N_V = N_S \times N_F$ values (for example in [3], N_V ranges from 640 to 896 according to the used fingerprint dataset). This method is not rotational invariant. For this reason, during the enroll phase, N_θ templates related to different rotations of the original image are computed. The match-score from two templates consists in the minimum Euclidean distance between the N_θ enrolled templates and the live template. We used $N_\theta = 9$, rotating the sample in a range from -45° to 45° with a constant step equal to 11.25°. This step reduces the problem related to the bad placement of the finger on the sensor. Fig. 2 shows the schema of the Fingercode method.

It is well known in the literature that the estimation of the reference point for the Fingercode template is a critical task with respect to the final accuracy of the system (an incorrect estimation of this point implies a different ROI evaluation, causing an increasing of the identification errors). We manually selected the reference point for each image in order to create a supervised points dataset as reference, then we applied different methods present in the literature in order to study this effect and to reduce its impact. First of all, we tested the identification of the reference point by selecting the candidate points in the image with the highest Poincare index [27], then we tested the a different method creating a single Fingercode template for each candidate point. In any case, if a fingerprint image does not present any singular point, we consider the point with the maximum Poincare

index as the reference point. Since a complete discussion of the effect of the reference point on the accuracy is outside the scope of the paper, in the following we refer to the first presented method.

B. Template Quantization

In order to limit the complexity of Fingercode matching in the encrypted domain, we investigated the possibility of reducing the number of features of the fingercode templates and the number of bits used for the physical representation of each value of the template. The effects of the reduction of the number of features have been studied by appropriately decimating the tesselation of the region of interest. We tested different configurations of the algorithm: H, N_R, N_A, N_F. We preferred to use a fixed reduction strategy, instead of methods that minimize the correlation among different features, like principal component analysis, since the latter should be optimized for each database and their application in the encrypted domain would not be convenient. The effects of quantization have been studied by converting each value of the template into an integer number representable with b bits, according to a uniform quantization criterion. The performances of the different configurations have been compared by evaluating the empirical distribution of the distances of genuines and impostors after feature reduction and quantization, from which we can compute receiver operating characteristic (ROC) curves and equal error rate (EER).

C. The Encryption Method

Our cryptographic protocol strongly relies on the notion of (additively) homomorphic encryption. A public-key encryption scheme is said to be additively homomorphic if, given the encryptions of two message a and b, the ciphertext of $a+b$ can be easily computed (for example, by multiplication) from the two original cyphertexts without the knowledge of the secret key.

Our solution makes use of two specific encryption schemes: the Paillier's encryption scheme [28] and a known-variant of the ElGamal encryption scheme [29] but ported on Elliptic Curves. The latter scheme is wisely used in order to save further bandwidth.

D. The Matching Method in the Encrypted Domain

The protocol may be subdivided in three main steps to be accomplished by the two parties (the client with the biometric measure to authenticate and the server with an in-clear database with all the features of the enrolled persons):

- **vector extraction**: on a first stage the target biometry (i.e. the information acquired by the biometric device) is "converted" by the client, using the methodologies shown in this work, in a quantized characteristic feature vector; this preliminary work is performed in clear and only the resulting feature vector is encrypted and sent to the server;
- **distances computation**: the distances (more specifically the square of the Euclidean distance) between the target vector and the vectors in the database are computed in the ciphertext domain: this is done by the server exploiting the homomorphic properties of the adopted cryptosystems. The outcome of this phase consists of the encryption of the required distances that still remain unknown to the server. Differently from the original Fingercode matching method, we decided to compute the squared distance from two templates for reducing the computational complexity.
- **selection of the matching identities**: in this final step the server interacts with the client in order to select, in the ciphertext domain, the enrolled identities with the related distances that are below a known threshold. This is accomplished through several internal sub-protocols nevertheless keeping a constant round complexity. The final outcome is kept secret to the server and is only revealed to the client: it can consist of more than one identity (if this is the case) where the previous works [17], [18] just report the identity with the minimum distance. A simple variant allows the use of a boolean outcome: authenticated/rejected.

Such solution has been formally proven to be secure against an *honest-but-curious* adversary, where we assume that he follows the protocol but may try to learn additional information from the protocol trace beyond what can be derived from the inputs and outputs of the algorithm when used as a black-box. The final protocol has a constant round complexity and a bandwidth usage that is better than the works [17], [18] (when applied to the fingercode template). More details on the protocol and on the performance comparison are available in [4]).

E. Individual Threshold

In many biometric systems, the use of individual threshold values can produce a better final accuracy than a single threshold value used for all enrolled individuals. This is related to the fact that different training levels of the users and skin conditions can be present in the dataset. Considering a dataset D composed by N samples of M individuals, for each individual i is assigned a different threshold value t_i that is used in the identity verification step of the biometric recognition process. For each individual i, the distributions of False Match (FM_i) and False Non Match (FNM_i) are computed (with the corresponding individual EER_i) considering only the set of user templates X_i as the genuine template set. All other samples of the dataset are considered as the set of the impostor $I_i = D \supset X_i$. In our experiment, we set the value t_i as the threshold corresponding to the individual Equal Error Rate (EER_i). Differently, it is possible to set the individual threshold value as the threshold that corresponds to the Zero FMR or Zero FNMR. This important method can be applied to the proposed demonstrator. The results of the described methods are reported in Section IV.

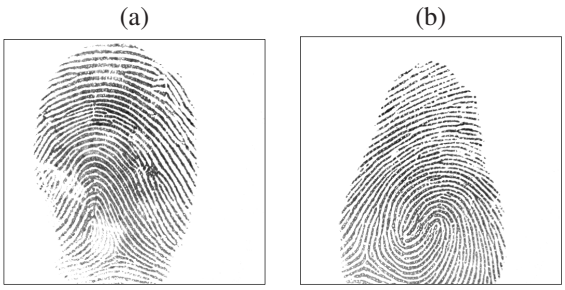

Fig. 3. Examples of test images.

IV. Implementation of the Demonstrator and Experimental Results

We tested the proposed demonstrator by using a well known public fingerprint dataset composed by 408 grayscale fingerprint images acquired by a CrossMatch Verifier 300 sensor [30] [31]. The dataset contains 8 images for each individual with a resolution equal to 500 dpi and the dimension of 512×480 pixel. Figure 3 shows two examples of images of the test database.

The application of the Individual Threshold method cited in Section III-E is shown in Fig. 4 where different figures of merits are reported with $N_V = 640$. The overall accuracy has been enhanced by reducing the initial EER (equals to 0.065) of a factor close to 0.5. In particular, we obtained a ZeroFM rate with FMR=0.1653 and a ZeroFNM rate with FMR=0.0512. This method can typically produce relevant enhancement in overall accuracy when the samples belonging to Dataset have not the same quality level. This is the case of the proposed test dataset.

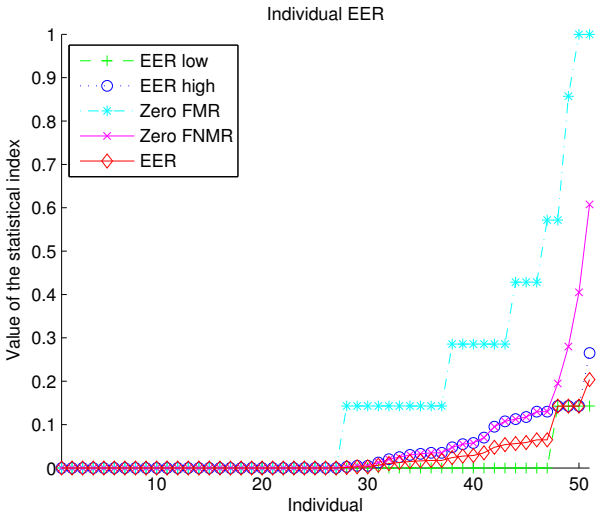

Fig. 4. Results obtained by computing method of Individual Threshold.

As a second step, in order to test the effect of the number of features in the Fingercode template we generated a total of eight different configurations, corresponding to eight sets of Fingercode vectors with length ranging from 640 features (the original configuration) to 8 features. The parameters of the reduced tesselations for each configuration are detailed in Table I.

TABLE I

Tested configurations for feature size reduction.

Configuration	N_V	N_F	N_R	H (pixel)	N_A
A	640	8	5	20	16
B	384	8	4	25	12
C	192	8	3	20	8
D	96	4	3	33	8
E	48	4	3	33	4
F	32	4	2	50	4
G	16	4	2	50	2
H	8	2	2	50	2

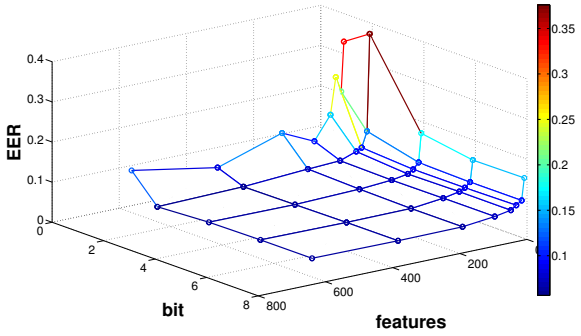

Fig. 5. Equal Error Rate of the different configurations.

For investigating the effects of the Template Quantization, each configuration has been normalized and quantized using a different number of bits, ranging from eight bits to a single bit, producing a total of $5 \times 8 = 40$ quantized configurations. The behavior of the EER for the testing dataset is shown in Fig.5. From the above figure, it is evident that the performance of the system is practically unaffected by feature size reduction when the number of features is above 96 and the number of bit is above 2. This suggested to consider for further testing only the configurations C and D, both quantized with 4 and 2 bits.

To evaluate the performances in bandwidth and computational complexity we implemented a client-server prototype version of our construction written in C++, using the GMP Library (version 5.0.1) and the PBC Library (version 0.5.8). The experimental results were run on 2.4 GHz with 4 GB of RAM PCs. The experimental results show that the proposed method based on Fingercode templates and homomorphic cryptosystem is feasible in the cases when the privacy of the data is more important than the accuracy of the system, and the obtained performances on accuracy measured as EER are comparable to the original method. Table II shows the obtained accuracy, the computational time and the bandwidth required by the configurations C and D described in Table I, each quantized with 2 and 4 bits.

We estimated the time required for the identification in the encrypted domain using a dataset composed by 100 enrolled individuals using a 80 bits security key. Table III reports the obtained results. The time complexity of the underling

TABLE II

PERFORMANCE OF THE PROPOSED METHOD WITH A DATABASE OF 408 ENTRIES (3672 FEATURE VECTORS).

Parameters				
Configuration	Quantization	Security	EER	Bandwidth (bit)
C	2	80	0.0758	6568792
		112		10824021
		128		14374232
C	4	80	0.0732	7802584
		112		12527832
		128		16313048
D	2	80	0.0715	6902008
		112		11299320
		128		14932856
D	4	80	0.0673	8135800
		112		13003128
		128		16871672

TABLE III

REQUIRED TIME FOR THE IDENTIFICATION IN THE ENCRYPTED DOMAIN USING A DATASET COMPOSED BY 100 ENROLLED ENTRIES USING A 80 BITS SECURITY KEY.

Configuration	Quantization	Time (s)
C	2	44.43
	4	53.66
D	2	37.43
	4	45.58

protocol is linear in the number of enrolled identities.

As shown in Table II and Table III different performances can be obtained varying the number of features of the template and the number of bits used for representing each value. On the other hand, the best computational performances can be obtained with a small number of features and bits.

Fig. 6 plots the ROC curves of the configurations that we consider as a good trade off. The performance of the different configurations are very close each other, the effects of both feature reduction and quantization being very limited on the accuracy of the system. It is worth noting that the original configuration, i.e., 640 features with floating point implementation, reported an EER of 0.065333 on the testing dataset, which is comparable with the performance of the tested configurations.

The obtained final results of the system (in term of ERR and ROC curves) show the proposed method is only slightly worse than the results of the original Fingercode technique applied on the same dataset, and that the privacy protection implementation we proposed can be feasible in the cases when the privacy of the data is more important than the accuracy of the system. Unfortunately, the simplicity of the matching function used in the Fingercode is suitable for the processing in the encrypted domain, but it limits the final accuracy of the system. In fact, much more accurate methods capable to work with the same fingerprint dataset are available in the literature, but their complexity excludes the adoption in the proposed framework implemented in the demonstrator.

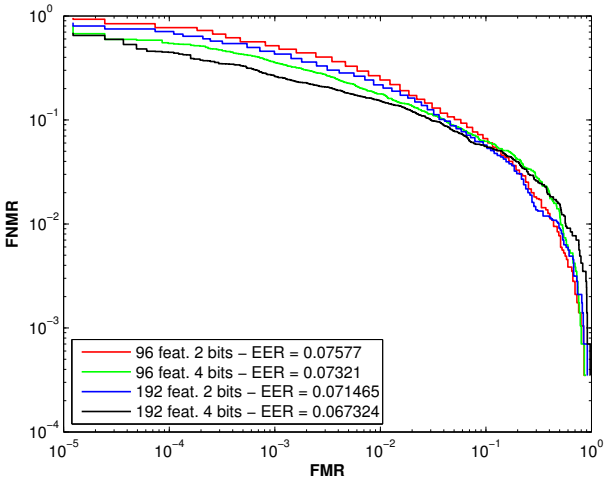

Fig. 6. ROC curves of the configurations of the proposed method that we consider as the best suitable in real applicative conditions.

V. CONCLUSION

The paper presented the design of a demonstrator of an approach to protect the privacy of the biometric data in distributed biometric systems based on fingerprints. In the proposed approach, on the client side, the biometric data are captured and then an encrypted representation of the template Fingercode is computed. We reduced the data contained in the template for obtaining a smaller representation of the encrypted template that should be shared with the server. The encryption matching algorithm is based on the homomorphic cryptosystems. The experimental results show that the proposed approach has an equivalent accuracy with respect the original Fingercode method. Improvements of the security model will be considered in the future work by applying encryption methods also on the biometric templates stored in the database. This new security model is stronger than the model proposed in this paper but it is also more difficult to realize. The obtained computational time permits the use of the proposed system in real applications. The main drawback of this approach consists in the low accuracy of

the recognition method based on the Fingercode template that permit the use of this system only in a limited subset of security applications with respect to the state-of-the-art methods based on minutiae.

REFERENCES

[1] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process*, vol. 2008, pp. 1–17, 2008.

[2] K. W. Webb, "Biometric security solutions," *IEEE Security and Privacy*, vol. 3, p. 7, 2005.

[3] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching," *IEEE Transactions on Image Processing*, vol. 9, pp. 846–859, 2000.

[4] M. Barni, T. Bianchi, D. Catalano, M. D. Raimondo, R. D. Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, F. Scotti, and A. Piva, "Privacy-preserving fingercode authentication," in *12th ACM Multimedia and Security Workshop*, 2010.

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

[6] L. Nanni and A. Lumini, "Empirical tests on biohashing," *Neurocomputing*, vol. 69, no. 16-18, pp. 2390 – 2395, 2006.

[7] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, 2007.

[8] S. Kanade, D. Petrovska-Delacretaz, and B. Dorizzi, "Cancelable iris biometrics and using error correcting codes to reduce variability in biometric data," *Computer Vision and Pattern Recognition, IEEE Computer Society Conference on*, pp. 120–127, 2009.

[9] A. Nagar and A. Jain, "On the security of non-invertible fingerprint template transforms," in *Information Forensics and Security, 2009. WIFS 2009. First IEEE International Workshop on*, 6-9 2009, pp. 81 –85.

[10] A. Juels and M. Wattenberg, "A fuzzy commitment scheme." ACM Press, 1999, pp. 28–36.

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

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

[13] S. Cimato, M. Gamassi, V. Piuri, D. Sana, R. Sassi, and F. Scotti, "Metodo di generazione e di verifica di una informazione di sicurezza ottenuta mediante letture biometriche," March 2006.

[14] B. Fu, S. Yang, J. Li, and D. Hu, "Multibiometric cryptosystem: Model structure and performance analysis," *Information Forensics and Security, IEEE Transactions on*, vol. 4, no. 4, pp. 867 –882, dec. 2009.

[15] M. AlTarawneh, W. Woo, and S. Dlay, "Fuzzy vault crypto biometric key based on fingerprint vector features," in *Communication Systems, Networks and Digital Signal Processing, 2008. CNSDSP 2008. 6th International Symposium on*, 25-25 2008, pp. 452 –456.

[16] A. Teoh, W. Yip, and K.-A. Toh, "Cancellable biometrics and user-dependent multi-state discretization in biohash," *Pattern Analysis & Applications*.

[17] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, "Privacy-preserving face recognition," in *PETS '09: Proceedings of the 9th International Symposium on Privacy Enhancing Technologies*. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 235–253.

[18] A. Sadeghi, T. Schneider, and I. Wehrenberg, "Efficient privacy-preserving face recognition," in *ICISC '09: Proceedings of the 12th Annual International Conference on Information Security and Cryptology*, ser. LNCS, vol. 5984. Springer-Verlag, December 2-4, 2009, pp. 235–253, full version available at http://eprint.iacr.org/2009/507.

[19] V. Kolesnikov, A.-R. Sadeghi, and T. Schneider, "Modular design of efficient secure function evaluation protocols," Cryptology ePrint Archive, Report 2010/079, 2010, http://eprint.iacr.org/2010/079/. [Online]. Available: http://thomaschneider.de/papers/KSS10.pdf

[20] J. Daugman, "How iris recognition works," in *Image Processing. 2002. Proceedings. 2002 International Conference on*, vol. 1, 2002, pp. 33 –36.

[21] A. Stoianov, "Cryptographically secure biometrics," B. V. K. V. Kumar, S. Prabhakar, and A. A. Ross, Eds., vol. 7667, no. 1. SPIE, 2010, p. 76670C.

[22] J. Bringer, H. Chabanne, M. Izabachène, D. Pointcheval, Q. Tang, and S. Zimmer, "An application of the goldwasser-micali cryptosystem to biometric authentication," in *ACISP'07: Proceedings of the 12th Australasian conference on Information security and privacy*. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 96–106.

[23] J. Bringer and H. Chabanne, "An authentication protocol with encrypted biometric data," in *AFRICACRYPT'08: Proceedings of the Cryptology in Africa 1st international conference on Progress in cryptology*. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 109–124.

[24] B. Schoenmakers and P. Tuyls, *Computationally Secure Authentication with Noisy Data*. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 141–149.

[25] M. Upmanyu, A. M. Namboodiri, K. Srinathan, and C. V. Jawahar, "Efficient biometric verification in encrypted domain," in *ICB '09: Proceedings of the Third International Conference on Advances in Biometrics*. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 899–908.

[26] M. Upmanyu, A. Namboodiri, K. Srinathan, and C. Jawahar, "Blind authentication: A secure crypto-biometric verification protocol," *Information Forensics and Security, IEEE Transactions on*, vol. 5, no. 2, pp. 255 –268, june 2010.

[27] A. K. Jain and D. Maltoni, *Handbook of Fingerprint Recognition*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2003.

[28] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *EUROCRYPT*, 1999, pp. 223–238.

[29] T. El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Proceedings of CRYPTO 84 on Advances in cryptology*, 1985, pp. 10–18.

[30] CROSSMATCH Technologies, Verifier 300, http://www.neurotechnology.com.

[31] Neurotechnology, dataset Cross Match Verifier 300, http://www.neurotechnology.com.