A Dual-Factor Access Control System Based on Device and User Intrinsic Identifiers

R. Arjona, and I. Baturone
Instituto de Microelectrónica de Sevilla, IMSE, CNM (CSIC, Universidad de Sevilla)
Seville, Spain

Abstract—**This paper proposes an access control system based on the simultaneous authentication of what the user has and who the user is. At enrollment phase, the wearable access device (a smart card, key fob, etc.) stores a template that results from the fusion of the intrinsic device identifier and the user biometric identifier. At verification phase, both the device and user identifiers are extracted and matched with the stored template. The device identifier is generated from the start-up values of the SRAM in the device hardware, which are exploited as a Physically Unclonable Function (PUF). Hence, if the device hardware is cloned, the authentic identifier is not generated. The user identifier is obtained from level-1 fingerprint features (directional image and singular points), which are extracted from the fingerprint images captured by the sensor in the access device. Hence, only genuine users with genuine devices are authorized to access and no sensitive information is stored or travels outside the access device. The proposal has been validated by using 560 fingerprints acquired in live by an optical sensor and 560 SRAM-based identifiers.**

Keywords—Fingerprint recognition; Physical unclonable functions, PUFs; Electronic systems on chip.

I. INTRODUCTION

Traditionally, passwords have been employed for access control. However, since passwords must be remembered by the users, they are selected according to familiar words and dates, which are weak and vulnerable to attacks. A solution is to use wearable devices such as smart cards, key fobs, security tokens, or smart phones. Basically, a password stored in the device provides access to the system. In this way, "what the user knows" (the password which has to be remember) is converted to "what the user has" (the device which provides a password) and the user does not have to remember it. The security is higher if the password is not stored but generated by the hardware in the device. A device with Physical Unclonable Functions (PUFs) in its hardware cannot be cloned physically because the variability of the hardware manufacturing process creates a device with unique properties (like hardware fingerprints) that are exploited to regenerate unique, unclonable and unpredictable identifiers [1]-[2].

However, if the access device is stolen, an attacker can employ it to access. A solution to avoid this is to include biometric authentication in the access device. In this way, the attacker cannot access to the system because the genuine biometric data stored in the device do not match with the impostor data extracted and processed in the device. Currently, fingerprint recognition is widely used in smart phones. However, in the context of wearable devices with higher constraints of size, power consumption and real-time operation (i.e. smart cards, key fobs, wristbands, etc.), fingerprint recognition algorithms should be selected carefully to be implemented in the electronic system on chip of the access device [3]-[4]. A possibility is to employ simple algorithms to extract coarse fingerprint information from several fingers (instances) and several samples per finger, so that combination of information increases distinctiveness [5].

This paper proposes the fusion of hardware and user fingerprints in order to combine "what the user has" and "who the user is" in the same device. From a security point of view, this combination has a high potential since both types of information are required, so that the possibilities of incorrectly verifying unauthorized users are reduced significantly. Another advantage is that the fusion (performed in an obfuscated way) generates a protected template which can be stored in the access device without security problems [5]-[6]. In addition, the identifiers resulting from the fusion can be employed to generate secret keys to establish a secure communication link with the verifier of the access control system, so that no sensitive information travels outside the access device [7].

This paper focuses on the design of an access device that can combine biometric and PUF information. The hardware of the device has to include an acquisition module to capture biometric samples and processing modules to extract biometric and PUF information. Since both the selected user and device identifiers are binary, they are fused by using XOR operations. The objective is to implement all the required operations for the enrollment and verification in an electronic system on chip included in the access device. To the best of authors' knowledge no similar access device has been proposed in the literature.

The paper is structured as follows. Firstly, Section II describes the generation of binary biometric identifiers based on the selection of a simple fingerprint recognition algorithm. The use of the PUF identifier based on the start-up values of SRAMs is described in Section III. Section IV presents results of the fusion of biometric identifiers (which in turn combine several fingers and samples from each finger to obtain high

This work has been partially supported by TEC2014-57971-R and RTC-2014-2932-8 projects from Ministerio de Economía y Competitividad of the Spanish Government (with support from the PO FEDER-FSE).

distinctiveness) and device identifiers as well as a possible authentication scheme suitable for a system-on-chip realization. Finally, conclusions are given in Section V.

II. Identifiers Based on Biometrics

One of the most distinctive biometric traits is fingerprints. Fingerprints are captured by means of sensors (the most extended types are optical or capacitive) and are converted to images. Fingerprint images are composed of ridges (depicted in dark in the left of Fig. 1) and valleys (depicted in white in Fig. 1). Generally, fingerprint images are not compared directly at the verification step because there are variations between different captures. In contrast, fingerprint images are processed to obtain distinctive features.

There are three different fingerprint features, depending on the information level considered to process the fingerprint image. Level-1 features offer global information, which describes the fingerprint as a whole. The most extended approaches employ textures (basically, ridge orientations or frequencies) or geometric information. For example, directional image (also known as orientation image, field or map, or directional field or map) contains local ridge orientations for each pixel, or singular points which are central points where ridges converge (cores) or diverge (deltas). Level-2 features require a detailed analysis of the fingerprint image to obtain local information. The traditional level-2 features are minutiae: endings (ridges which end) and bifurcations (ridges which are divided into two ridges). Level-3 features are finer details of ridges such as width, shape, edge contour, pores, incipient ridges, breaks or scars.

The algorithms to extract and process the fingerprint features are more complex as the detail of the feature increases. For example, if the recognition is based on level-2 features, a complex preprocessing to enhance fingerprint images is required to locate minutiae correctly. In this work, level-1 features are selected to offer the sufficient recognition information with low processing complexity to implement the algorithm in a wearable device with high constraints in terms of size, power consumption and real-time operation. The fingerprint feature considered is based on a distinctive window of the directional image centered at the core point of the fingerprint image.

For the feature selected, one of the most relevant steps is the directional image extraction. There are two main approaches for the computation of the directional image: gradients and slits (also known as masks). The computation of the directional image using gradients is based on applying convolution of windows centered at each image pixel with horizontal and vertical operator matrices (Sobel, Gaussian, or Prewitt). The computation of the directional image based on slits associates a discrete direction from a set of predefined directions to each pixel depending on the neighbor luminance values for the current ridge within a window. The objective is to find the dominant ridge direction at each pixel [8]. Both approaches are similar in terms of computational complexity. Their performance in terms of accuracy in directional image extraction can be seen in the study reported in [9]. That study shows that the method based on slits performs better than gradients.

Our analysis carried out over several fingerprint databases also shows that fingerprint features based on slits offer a better trade-off between implementation cost and recognition than level-1 features based on gradient computations. Hence, although in previous works we used level-1 features based on gradients [5], the features used in this paper are based on slits. The multiscale directional operator proposed in [8] has been employed to estimate the direction of the ridges at every pixel. The basic idea is to calculate the standard deviation of the luminance of the pixels which determine each predefined direction (or slit). Then, the direction at each image pixel is selected as the slit with the maximum difference of the standard deviations between the luminance of the pixels at that slit and the pixels at the orthogonal direction.

The parameters selected to calculate the slits are based on the results obtained in [9]: 16 directions, 9 pixels for each direction, and a smoothing window size of 27 x 27 pixels.

The correct extraction of the core point is crucial for the level-1 feature selected. The approaches proposed for the extraction of the singular points are based on detecting discontinuities in the directional image. The traditional way to compute the singular points is based on the Poincaré Index. However, this method alone cannot detect correctly the singular points if the fingerprint images are captured with bad quality and no enhancement is applied as considered here to reduce processing steps. Hence, a method based on complex filtering has been considered. The convolution of the directional image with complex filters allows detecting prominent symmetries even in images of low quality [10]. The implementation reported in [11] has been employed. It finds

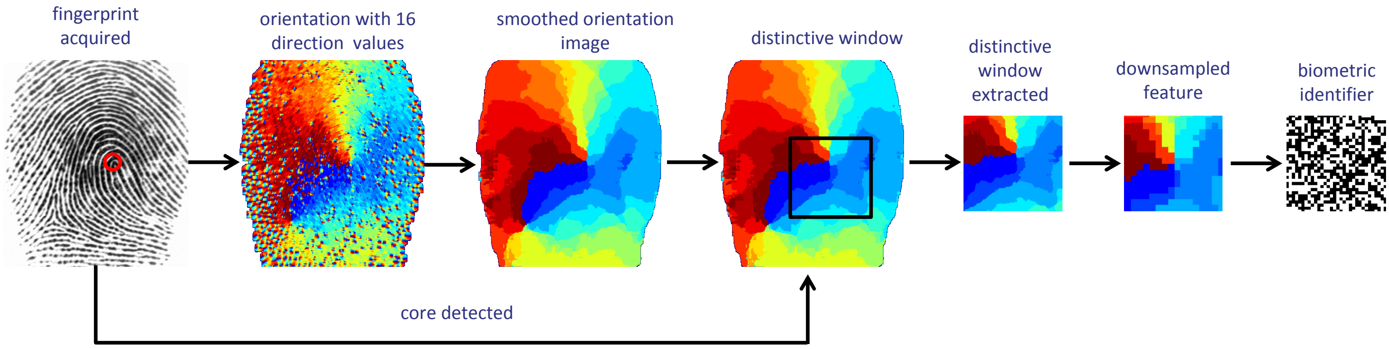
fingerprint acquired
orientation with 16 direction values
smoothed orientation image
distinctive window
distinctive window extracted
downsampled feature
biometric identifier
core detected

Fig. 1. Extraction of the fingerprint feature.

several core point candidates (up to 19) for each fingerprint image.

A window is centered at each core point candidate of the fingerprint image to obtain the most of the distinctive information. The selection of the distinctive window size is relevant for the recognition process. An adequate size value depends on the fingerprint image size acquired by the sensor. For most fingerprint sensors, which capture a fingerprint size of, approximately, 300 x 300, a small window size (for example, 32 x 32) does not give enough information and a medium size (such as a 64 x 64 window) offers limited information. The most suitable option is a large window size (for instance, 128 x 128). Enlarging the window size from 128 x 128 to 256 x 256 implies increasing the number of fingerprint images with uncompleted windows. It has to be considered that the core point is not usually located in the central part of the image because the fingerprint capture is not centered with respect to the sensor.

In order to reduce the size of the feature vector, redundant information is removed by down-sampling the distinctive window. We have proven experimentally that the most suitable down-sampling factor for maintaining the distinctive information is 8. Therefore, the down-sampled distinctive window size is 16 x 16. Since 16 direction values are possible at each pixel, each direction value can be represented by 4 bits and the biometric identifier contains 16 x 16 x 4 = 1024 bits (per core point candidate). The complete process for the extraction of the biometric identifier is illustrated in Fig. 1.

Since the proposed level-1 features are sequences of ordered bits, matching two identifiers is done by computing their Hamming Distance (HD) to obtain a score value which indicates the number of different bits.

III. Identifiers based on PUFs

PUFs allow generating unique and distinctive identifiers because they exploit intrinsic features of the hardware that are consequence of the manufacturing process variability. Since process variability is usually random, PUF responses are random and cannot be predicted, which is very interesting to avoid attacks.

Different types of electronic circuits have been employed as PUFs: SRAMs, latches, D Flip-Flops, arbiters, ring oscillators, etc. [1]. In this paper, the memory cells of SRAMs have been selected since SRAMs are required by the processing carried out in the access device, so that no additional circuitry has to be included to perform as PUF. The start-up values of the SRAM memory cells in an access device are almost the same for each powered up. In the other side, the start-up values in another access device are quite different. Hence, the device can be identified by the SRAM start-up values. The start-up values generated are random and difficult to predict. In addition, since they are lost when the memory is powered down, the identifier is generated on the fly and does not need to be stored, which is more secure.

The identification process with SRAM start-up values is composed of two stages (as the identification process with biometrics): (1) registration or enrollment of the memory (*n* start-up values from *n* memory cells are stored as template) and (2) verification (the *n* start-up values are obtained again from the memory and compared with the template).

Two sets of start-up values (PUF responses) are compared by computing their Hamming Distance (HD). Ideally, several PUF responses from the same memory should have zero Hamming distance. However, some bit flipping is unavoidable among different start-ups of the same memory [2]. Anyway, bit flipping does not affect the identification process because the Hamming distances between PUF responses of genuine memories are clearly smaller than the distances between PUF responses of genuine and impostor memories.

If all the bits of the set of start-up values are assumed to be independent (as should be ideally), the probability of finding *t* different bits in *n* bits is given by a binomial distribution, as follows:

$$P(t) = \binom{n}{t} \cdot p^{t} \cdot (1-p)^{n-t} \qquad (1)$$

where *p* is the bit flipping probability.

According to the Moivre-Laplace theorem, if the number of Hamming distances measured for PUF responses is large, the binomial distribution can be approximated by a normal distribution whose mean value (μ) is $n \cdot p$ and the standard deviation value (σ) is $\sqrt{n \cdot p(l-p)}$. If the distribution is calculated for the genuine population of PUF responses, the bit flipping probability is ideally zero. In the other side, if the distribution is calculated for the impostor population, the bit flipping probability is 0.5 ideally (as the probability when tossing a coin).

The biggest distance between PUF responses of genuine memories can be estimated by considering the maximum intra HD, which is defined as follows:

$$\max_{IntraHD} = \max_{\substack{x=1,\dots,k \\ i=1,\dots,m-1 \\ j=i+1,\dots,m}} \left[\frac{HD(R_{ix}, R_{jx})}{n} \right] \cdot 100 \qquad (2)$$

where *m* is the number of PUF responses evaluated from *k* devices and *R* are the PUF responses to compare.

For the comparison between genuine and impostor memories, the smallest distance can be estimated by the minimum inter HD, which is defined as follows:

$$\min_{InterHD} = \min_{\substack{x=1,\dots,k-1 \\ y=x+1,\dots,k \\ i,j=1,\dots,m}} \left[\frac{HD(R_{ix}, R_{jy})}{n} \right] \cdot 100 \qquad (3)$$

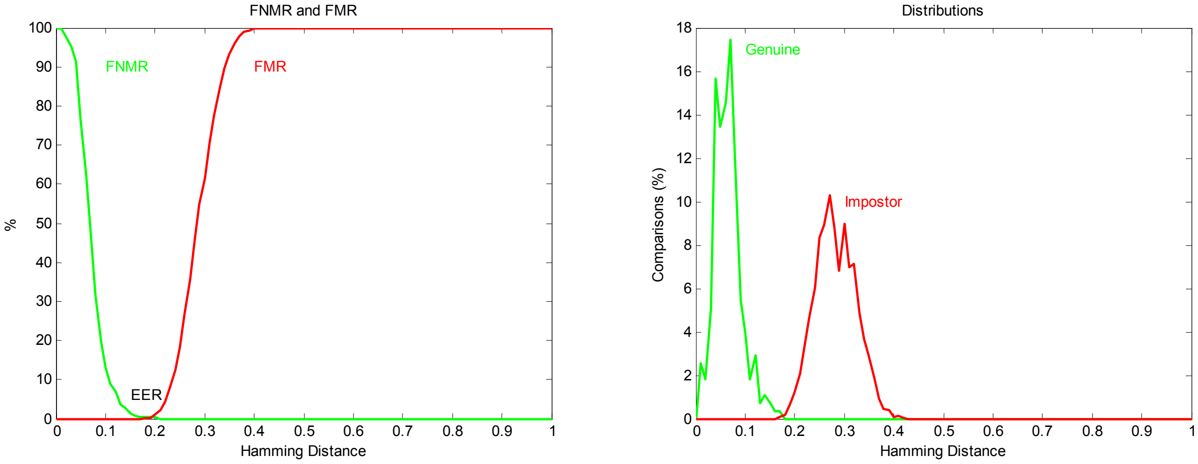

Fig. 2. FNMR and FMR curves and genuine and impostor distributions for recognition based on fingerprint identifiers.

Identification can be carried out without error if the maximum intra HD is smaller than the minimum inter HD. In addition, in order to generate ideal identifiers, the maximum intra HD should tend to 0% and the minimum inter HD should tend to 50%. These conditions should also apply for biometric identifiers. However, the level-1 fingerprint features described in Section II do not offer so much distinctiveness as PUF identifiers. This is illustrated in the following section.

IV. Design of the Access Device

A. User identifiers

The fusion of multiple sources of fingerprint information is employed to achieve higher performance in individual recognition as well as to increase the security because if more information is required, an attack is more difficult. The fusion scenarios considered here are several fingers and several captures of each finger. This can be done if the access device contains a fingerprint sensor and a way to communicate with the user so as to control which finger and sample is being placed in the sensor. The fusion of biometric information can be applied at all stages of the recognition process: fingerprint acquisition, features, matching scores, and recognition decision. The most extended alternative is at the score level, which is simpler than the fusion of data or features and maintains a higher amount of recognition information than the decision level. Hence, score level is considered for the design of the access device.

Recognition systems apply multi-sample fusion by default. At enrollment, which is performed once to register the user, several samples (typically, three) of the same finger are acquired to obtain the best representation of the captures. At matching, which is performed as many times as the recognition is needed, the user is required to introduce fewer samples (typically, one).

The access device considers the acquisition of 3 samples of each finger at enrollment and 1 or 2 samples at matching. Hence $3 \cdot s$ sequences of bits are stored as templates for each finger, assuming that s core point candidates are found for each finger sample. At verification, if s sequences of bits are extracted from 1 sample of a finger or $2 \cdot s$ sequences are extracted from 2 samples, all possible combinations are considered ($3 \cdot s^2$ or $6 \cdot s^2$ Hamming distances are computed) and the matching score for each finger is evaluated as the minimum value of all of them. In addition, the access device considers the acquisition of 2 fingers. The final matching score for both fingers is evaluated as the average of the matching scores for each finger. Hamming distances, minimum and average are very simple operations to implement.

The fingerprint database employed to obtain recognition results has been created by using an optical sensor (the FS90 sensor from Futronic) and fingerprints captured in live. The fingerprint database is composed of 56 individuals and each person introduces 2 fingers and 5 samples for each finger (560 fingerprints in total). The recognition results in terms of EER (Equal Error Rate), ZeroFMR (Zero False Match Rate) and ZeroFNMR (Zero False Non-Match Rate) are shown in Table I. Recognition results are obtained considering all the possible combinations according to the FVC (Fingerprint Verification Competition) recommendations and removing symmetric comparisons.

For the multi-sample and multi-instance fusion (two fingers and three samples at enrollment and two fingers and two samples at matching) the FMR and FNMR curves are illustrated on the left of Fig. 2 and the genuine and impostor distributions are shown on the right of Fig 2.

B. Device identifiers

The PUF response database employed to obtain device

Table I: Recognition Indicators for Different Approaches of Biometric Fusion

Biometric approach	***EER***	***ZeroFMR***	***ZeroFNMR***
3 samples at enrollment and 1 sample at matching	1.91	21.81	72.40
3 samples at enrollment and 2 samples at matching	0.67	10.54	30.55
2 fingers and 3 samples at enrollment and 2 fingers and 2 samples at matching	0.36	0.55	2.12

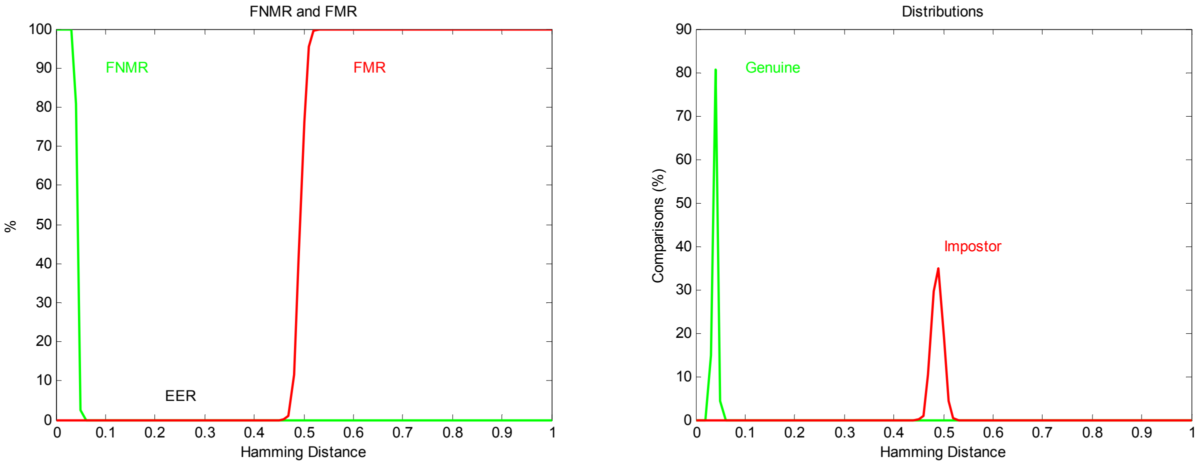

Fig. 3. FNMR and FMR curves and genuine and impostor distributions for recognition based on PUF identifiers.

recognition results has been created from SRAM modules included in 10 integrated circuits evaluated at 6 different operation conditions of temperature and power supply voltage, taking 20 start-up responses at each operation condition [2]. One of the results obtained was that the mean value of the maximum intra HD was 6.80%.

Since the 99.74% of a normal distribution, approximately, is in the interval [μ-3σ, μ+3σ], we have considered that the value μ+3σ is equal to the maximum intra HD value (6.80%). Since μ=$n \cdot p$ and σ=$\sqrt{n \cdot p(1-p)}$, we have considered a bit flipping probability p equal to 0.048 for n=1024 (ideally, p should be zero for the bit flipping of PUF responses generated by the same memory). 1024 bits are considered to identify a device because 1024 bits are also considered to identify a user. These parameters have been selected to carry out the simulation of 112 sets of 1024 memory cells and 5 start-ups for each set. Therefore, 112 different 1024-bit identifiers are generated following a binomial distribution based on the selected parameters. 112 device identifiers are considered because 112 fingerprint identifiers are also considered (if several core points are detected, the same device identifier is employed). 5 start-ups for each device identifier are considered because 5 samples are also considered for each fingerprint identifier. Simulations were performed with Matlab.

Similarly to the biometric recognition using 2 fingers and 3 samples at enrollment and 2 fingers and 2 samples at matching, 2 sets of 1024 memory cells and 3 start-ups are considered at enrollment and the same sets of 1024 memory cells and 2 start-ups at matching. The FMR and FNMR curves are illustrated on the left of Fig. 3 and the genuine and impostor distributions are shown on the right of Fig 3. The device identifiers are reliable and unique because the genuine distribution is near to 0% and the impostor distribution is around 50%. In addition, genuine and impostor distributions are well separated.

C. Fusion of user and device identifiers

Two approaches are possible for the fusion of both identifiers: concatenation-based or XOR-based fusions. At security level, XOR-based fusion offers more advantages since the resulting identifier is random. The properties of the PUF identifier, such as uniqueness, reliability and unpredictability are maintained for the resulting identifier. In addition, the template identifier is protected because the XOR operation obfuscates the PUF and biometric information and none of them can be recovered. The resulting identifiers do not contain sensitive information and, hence, can be stored as template in a non-volatile memory of the access device which does not need to be secure. In addition, the recognition operations are performed in the protected domain at a bit level (or feature level) without recover the PUF and biometric information separately at a Hamming distance level (or score level).

Let us consider that ($B_1,\ldots,B_I$) are the instances captured as templates at enrollment, ($B_1',\ldots,B_I'$) are the instances captured as inputs at matching, *S* and *S'* the template and the input samples, *P* and P' are the template and input PUF identifiers, *Sfusion* is a fusion operator that provides a normalized score from the fusion of the sample scores (*t* at enrollment and *q* at matching), and *Tfusion* is a fusion operator that results a normalized score from the fusion of the instance scores. The score computation is as follows:

$$\mathrm{score}\left[(\mathrm{B}_1',\ldots,\mathrm{B}_I'),(\mathrm{B}_1,\ldots,\mathrm{B}_I)\right]=\mathrm{Sfusion}_{k=1,\ldots,I}$$
$$\left\langle \mathrm{Tfusion}_{\substack{i=1,\ldots,t\\ j=1,\ldots,q}}\left\{\mathrm{HD}\left[\mathrm{S}_j'\left(\mathrm{B}_k'\right)\oplus \mathrm{P}_{jk}',\mathrm{S}_i(\mathrm{B}_k)\oplus \mathrm{P}_{ik}\right]\right\}\right\rangle \quad (6)$$

In the case of multi-sample fusion, the most suitable fusion operator is *min* because the best sample is selected. For multi-instance fusion, the most suitable fusion operator is *sum* (*average*) to take into account the different instances. Fig. 4 shows the recognition and distribution curves for the fusion of PUF identifiers with the biometric identifiers based on 2 fingers and 3 samples at enrollment and 2 fingers and 2 samples at matching. EER=0 because genuine and impostor distributions are separated.

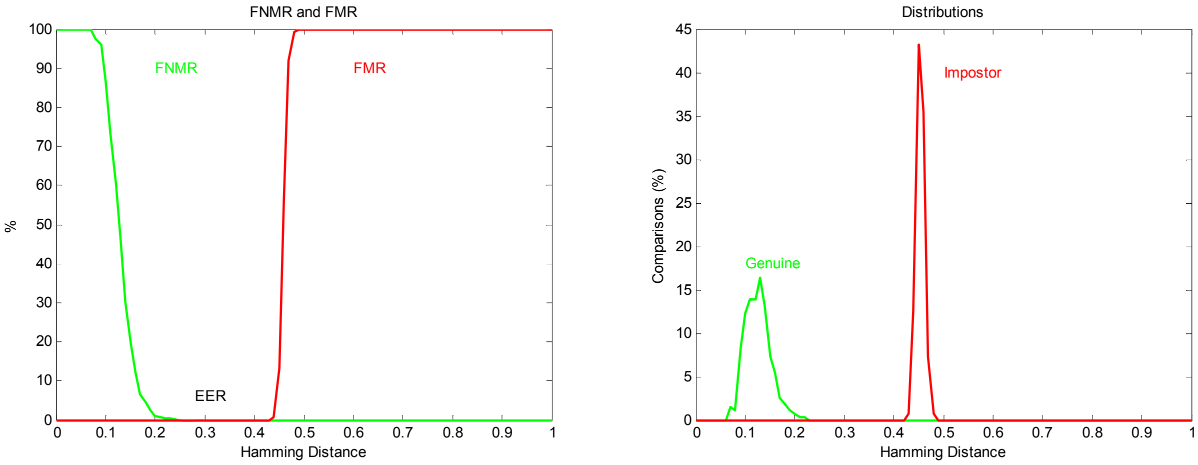

Fig. 4. FNMR and FMR curves and genuine and impostor distributions for recognition based on the fusion of PUF and fingerprint identifiers.

All the functionality described above can be implemented in a system-on-chip included in the access device. For an example of authentication with only one user registered in the access device, two fingers are considered and three samples of fingerprints are acquired for each finger at enrollment. At the same time, the corresponding start-up values from a SRAM in the device are collected for each sample. Then, the features are extracted for each sample and for each core point detected. Once each fingerprint identifier is XOR-ed with its associated PUF identifier, two sets of 3-fused identifiers are obtained and stored as template in a flash memory. At the matching stage, two sets of 2-fused identifiers are obtained and compared to the template. The identifiers from each set are compared by a Hamming distance, thus resulting six score values for each set. The scores from each set are fused by a *min* operator and the resulting two scores are fused by a *sum* (*average*) operator. A threshold is imposed for this score to make a recognition decision. This scheme is illustrated in Fig. 5. All the operations required are very suitable for a system-on-chip implementation.

V. Conclusions

The fusion of fingerprint and PUF identifiers is employed in this work to increase the security of an access control system. Recognition results show that the identifiers generated provide a zero EER, that is, a well separation between genuine and impostor distributions. In addition, the XOR operation employed for the fusion of identifiers obfuscates the information and allows performing the recognition in a protected domain. Since the involved processing has low computational cost, it is suitable to be performed in a system on chip in a wearable access device.

References

[1] R. Maes, “PUF-Based Entity Identification and Authentication, Physically Unclonable Functions”, in Physically Unclonable Functions, Chapter 5, pp. 117-141. Springer 2013.

[2] I. Baturone, M. A. Prada-Delgado, and S. Eiroa, “Improved Generation of Identifiers, Secret Keys, and Random Numbers From SRAMs”, IEEE Trans. on Information Forensics and Security, Vol. 10, No. 12, pp. 2653-2668, 2015.

[3] M. Fons, F. Fons, and E. Cantó, “Design of a Embedded Fingerprint Matcher System”, IEEE Intern. Symp. on Consumer Electronics, ISCE, pp. 1-6, 2006.

[4] G. Vitello, V. Conti, A. Gentile, S. Vitabile, and F. Sorbello, “Design and Implementation of an Efficient Fingerprint Features Extractor”, Euromicro Conf. on Digital System Design, DSD, pp. 695-699, 2014.

[5] R. Arjona, and I. Baturone, “A Fingerprint Biometric Cryptosystem in FPGA”, IEEE Intern. Conf. on Industrial Technology, ICIT, pp. 1554-1559, 2015.

[6] T. Ahmad, and F. Han, “Cartesian and Polar Transformation-based Cancelable Fingerprint Template”, 37th Annual Conf. on IEEE Industrial Electronics Society, IECON, pp. 373 – 378, 2011.

[7] P. Schaumont, D. Hwang, S. Yang, and I. Verbauwhede, “Multilevel Design Validation in a Secure Embedded System”, IEEE Trans. on Computers, Vol. 55, No. 11, pp. 1380-1390, 2006.

[8] M. A. Oliveira, and N. J. Leite, “A Multiscale Directional Operator and Morphological Tools for Reconnecting Broken Ridges in Fingerprint Images”, Pattern Recognition, Vol. 41, pp. 367-377. Elsevier, 2008.

[9] F. Turroni, D. Maltoni, R. Cappelli, and D. Maio, “Improving Fingerprint Orientation Extraction”, IEEE Trans. on Information Forensics and Security, Vol. 6, No. 3, pp. 1002-1013, 2011.

[10] K. Nilsson, and J. Bigun, “Complex Filters Applied to Fingerprint Images Detecting Prominent Symmetry Points used for Alignment”, Biometric Authentication, Lecture Notes in Computer Science, 2359, pp. 39-47. Springer, 2002.

[11] Fingerprint Recognition Software based on FingerCodes (2006): http://www.advancedsourcecode.com/fingerprint.asp

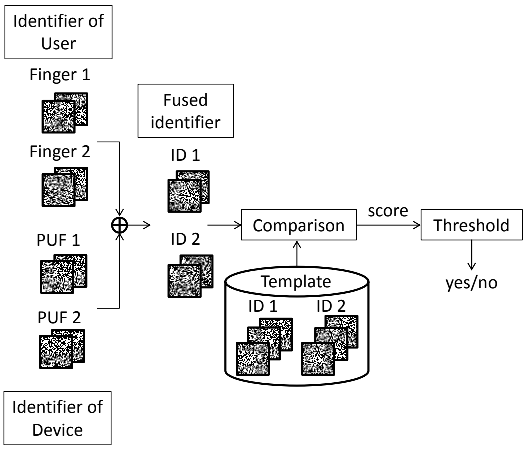

Fig. 5. Authentication scheme based on the fusion of fingerprint and PUF identifiers.