Multi-instance Based Cryptographic Key Regeneration System

Danielle P. B. de A. Camara, José Sampaio de Lemos-Neto and Valdemar C. da Rocha Jr.

***Abstract*—This paper introduces a new multi-instance *key regeneration* system used to regenerate cryptographic keys from biometric data. The serial concatenation of Reed-Solomon and Hadamard codes together with the use of a single extra mechanism and biometrics improve the biometric performance and security of the system, also making it possible the regeneration of longer and higher entropy cryptographic keys. The system was evaluated on two public databases: Casia-Biosecure and NIST-ICE 2005 and it provided a complete separation between the Hamming distance distributions for genuine users and impostors, respectively, being able to achieve both false acceptance rate (FAR) and false rejection rate (FRR) of 0%. Furthermore, on NIST-ICE 2005 it is possible to regenerate a 287 binary digit cryptographic key with estimated entropy of 160 bits at 0% FAR and 0.34% FRR.**

***Index Terms*—Biometrics, multibiometrics, cryptography, error-correcting codes, security.**

I. Introduction

BIOMETRICS verification techniques have been used for many decades providing authentication/identification of an individual based on his unique characteristics, e.g., fingerprint, iris, voice, hand geometry, etc. [1, pp.1-3]. In particular, the use of biometrics has grown significantly these last decades raising important concerns about the individual privacy and data confidentiality, since conventional biometric solutions require direct storing of user personal data [1, pp. 19-20]. On the other hand, secret-key cryptography is able to assure high data privacy as long as the cryptographic key is kept secret, and is as long and as random as possible to provide the required security level. For example, the Advanced Encryption Standard (AES) was designed to support encryption key lengths of 128, 192 or 256 bits [2]. However, classical cryptographic keys can not assure that the person using it is actually the genuine user (non-repudiation). The complementary nature of these two important and widely used security tools, namely cryptography and biometrics, stimulated many researchers to investigate new techniques capable of combining them in order to provide privacy to biometric data and obtain cryptographic keys truly linked to the user. The main drawback of this combination is the inherent variability in biometric data because so far cryptographic systems require exactitude to work properly. One of the approaches used to obtain cryptographic keys from biometrics, known as *key regeneration*, deals with this drawback using error-correcting coding (ECC) techniques.

Danielle P. B. de A. Camara, José Sampaio de Lemos-Neto and Valdemar C. da Rocha Jr, Communications Research Group - CODEC, Department of Electronics and Systems, Federal University of Pernambuco, 50740-550, Recife, PE, BRAZIL. e-mail: dpbac@ieee.org, {jose.lemosnt, vcr}@ufpe.br.

There are in the literature many unibiometric systems that combine biometrics and cryptography, e.g., [3] - [6], but most of them face problems with low entropy keys and high rejection rate. On the other hand, multibiometric systems [1, Chapter 14] can consolidate multiple sources of biometric information and are used to address some of the limitations of unibiometric systems, being able to improve matching accuracy, increase the population coverage and deter spoof attacks. Therefore, using multibiometrics seems to be a promising option to enhance systems that combine biometrics and cryptography. In addition, as shown in [7], the irises of a person are not correlated and so can be seen as two independent binary information sources, i.e., as a multi-instance crypto-biometric system.

In this paper we propose a multi-instance key regeneration (KR) system which makes use of serially concatenated Reed Solomon (RS) and Hadamard codes that are shown to suit very well the mixed error structure, containing both random and burst errors, presented by the iris. The proposed KR system combines the iris codes obtained from images of both eyes, forming a multibiometric feature binary vector, and makes use of a simple mechanism able to provide better biometric performance and offer a higher level of security. Our proposed system also makes it possible the regeneration of longer and higher entropy cryptographic keys, in comparison to the ones obtained by other systems [8] - [11].

Experiments were performed on Casia-Biosecure (CBS) [12] and NIST-ICE 2005 [13] databases. 287 binary digit keys with 160 bit estimated entropy were regenerated on the NIST-ICE 2005 database, at 0% false acceptance rate (FAR) and 0.34% false rejection rate (FRR)[1]. Furthermore, for the NIST-ICE 2005 database the proposed system was able to provide a complete separation between the Hamming distance distributions for genuine users and impostors, respectively, being able to achieve both false acceptance rate (FAR) and false rejection rate (FRR) of 0%.

The remaining parts of this paper are organized as follows. Section II provides the necessary background for understanding this paper. We introduce our KR system in Section III and in Section IV we give details on how the use of the new simple mechanism introduced here, together with the use of multiple biometric information sources, provides better biometric performance and higher level of security to the KR system. In Section V we describe the experiments performed

[1]FAR and FRR are parameters used to measure the performance of biometric systems, where FAR is the measure of the likelihood that false users will be accepted by the system and FRR is the measure of the likelihood that genuine users will be rejected by the system.

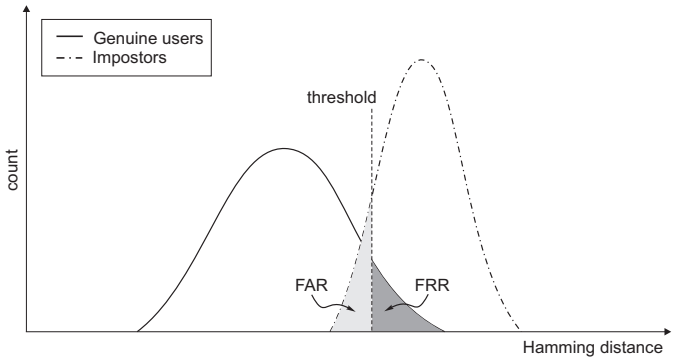

Fig. 1. Hamming distance distribution for genuine users and impostors for a given biometric system. As we can see, the threshold determines the values for FAR and FRR. It is worthy of note that because the intersection of the distributions, the adjusting of the threshold can not decrease simultaneously the values of FAR and FRR.

and present the results obtained. In Section VI we present a security analysis of the proposed KR system. Summing up, in Section VII we present some conclusions as well as suggestions for future research.

II. Background

Basically three approaches are used to combine cryptography and biometrics, namely *cancelable biometrics*, *key generation* and *key regeneration* (KR). The KR approach has been considered the most effective way to combine biometrics and cryptography in order to obtain cryptographic keys strongly linked to the user (non-repudiation), allowing key revocability, key diversity[2] and also privacy to the biometric data. ECC techniques are used in order to deal with biometrics inherent variability. However, the use of ECC schemes in KR systems is very peculiar. In order to choose the appropriate ECC technique the behaviour of biometrics variability of certain biometric characteristic must be observed, e.g., the iris data presents mixed random and burst errors. Moreover, the error-correcting capability of the code must be designed to correct *intra-user variations*, i.e., bit differences caused by biometrics variability for the same eye, but unable to correct *inter-user variations*, i.e., bit differences between eyes of different persons.

Cryptographic keys obtained by the KR approach are subject to some constraints because of the performance required of the biometric system. Every biometric recognition system has a built-in acceptance threshold, which when raised both increases FAR and decreases FRR, as is illustrated in Fig. 1. The choice of this threshold is usually done based on the specific application, e.g., low FAR for high security applications and low FRR for commercial applications.

In order to deal with biometrics inherent variability by using ECC techniques, two constructions are popular: the *Fuzzy commitment scheme* [14] and the *Fuzzy vault scheme* [15]. In 1999 Juels and Wattenberg [14] proposed the use of ECC to deal with this variability in order to regenerate cryptographic keys. However, no practical ECC technique was proposed in [14]. Only in 2006 Hao et al. [3] proposed a practical KR system based on iris using as ECC technique serially concatenated Reed-Solomon (RS) and Hadamard codes. As explained in [3], the Hadamard code is used to deal with background errors (random errors) caused for example by camera noise, iris distortion, image-capture effects that cannot be effectively corrected by the pre-processing phase, while the RS code deals with burst errors caused for example by eyelashes, eyelids and reflections. This system is able to regenerate 140 binary digit keys with estimated entropy of 44 bits at 0.47% FRR and 0% FAR over a 700-image proprietary database. However over a public database, NIST-ICE 2005 [13], it showed very high FRR, e.g., 19.41% for a 42 bit key.

Other unibiometric KR systems based on the Hao et al. [3] scheme were proposed. Kanade et al. [4] inserted two new mechanisms maintaining the ECC technique. As a result, 198 binary digit cryptographic keys with estimated entropy of 83 bits, at 0.06% FAR and 1.04% FRR on NIST-ICE 2005 database [13] are regenerated. In 2009, another scheme also based on the same ECC technique was introduced in [5] providing 94 bit entropy cryptographic keys with variable key length. Bringer et al. [6] proposed a KR system, also based on the iris, that uses a Reed-Muller code in a product code, obtaining 42 bit keys at 10^{-5} FAR and 5.62% FRR.

In Section IV, using the NIST-ICE database, we show that the proposed system is able to separate the genuine and impostor distributions, and thus it is possible to set the threshold in such way to achieve both FAR and FRR of 0%. We have no knowledge of any previously published work based on the ECC technique which separates the genuine and impostor distributions and achieve both FAR and FRR of 0%.

In this paper we consider the use of multibiometrics, more specifically, the use of two eyes of the same individual (multi-instance). As stated in [1, p. 272] a multibiometric system relies on the evidence presented by multiple sources of biometric information in order to enhance classification performance.

The multibiometric system is classified taking into account the nature of the following multiple sources [1, pp.272-275]:

(i) **multi-instance systems**: capturing a sample of multiple instances, e.g., right and left irises, with the same sensor;
(ii) **multi-sensor systems**: using different sensors to acquire a single biometric trait of an individual, e.g., infrared and visible-light images of a person's face;
(iii) **multi-algorithm systems**: applying multiple feature extraction and/or matching algorithms on the same biometric data;
(iv) **multi-sample systems**: capturing multiple samples using the same sensor and instance;
(v) **multi-modal systems**: fusing sources of biometric information from multiple modalities, e.g., fingerprint, face, iris, to establish identity;
(vi) **hybrid systems**: a combination of a subset of the types just described.

The biometric information can be combined at different levels, depending on the level of information fusion: sensor-level, feature-level, score-level, rank-level, or decision-level fusion [1, Chapter 14].

[2]Different keys are associated with different applications using the same biometric data.

So far, there is not much work published regarding the use of multibiometrics in crypto-biometric systems. In 2008 Nandakumar and Jain [8] proposed a multibiometric system that combines fingerprint with iris based on a fuzzy vault scheme proposed originally by Juels and Sudan [15] with the main goal of providing security to multibiometric templates. Recently, A. Nagar et al. [11] published a paper proposing another feature-level fusion framework for the design of multibiometric cryptosystems based on iris, face and fingerprint that simultaneously protects the multiple templates of a user using a single secure sketch. The feasibility of such a framework has been demonstrated using both fuzzy vault [15] and fuzzy commitment [14]. In the scope of fuzzy commitment schemes [14], designed with the aim of protecting multibiometric templates as well as providing cryptographic keys strongly linked to the user, we can name, for example, the KR systems introduced in [9] and [10]. In 2009 Kanade et al. [9] proposed a multi-instance KR system based on iris, using a weighted error correction technique plus the mechanisms of iris code shuffling and zero insertion, introduced earlier in [4]. Later on, in 2010 Kanade et al. [10] proposed a multibiometric weighted feature level system based on iris and face. This system also makes use of the mechanisms of iris code shuffling and zero insertion, introduced in [4]. The results obtained by these systems are presented in Table II at Section VI.

III. New Proposal

In this section, we introduce a new multi-instance KR system able to regenerate longer and higher entropy cryptographic keys. The proposed KR system uses the serial concatenation of an RS code and a Hadamard code. However, there are two important differences between the scheme presented here and previous ones that use a similar ECC technique:

(i) the use of a single mechanism that consists of inserting, as uniformly as possible among the binary digits of the iris code, a sequence of randomly generated binary digits (**Rand_num**);

(ii) the use of multiple biometric information sources, more specifically, right and left irises.

Hereafter we make a description of the proposed system and then we justify our choice for the ECC technique. The use of **Rand_num** and a multi-instance system are justified in Section IV.

A. Description of the New Proposal

The KR system introduced is illustrated by means of a block diagram in Fig. 2. During the *enrolment phase (key generation)* a random cryptographic key $\mathbf{K}$ is generated and encoded by the serial concatenation of an RS code and a Hadamard code, resulting in the binary vector $\boldsymbol{\theta}_{\rm ps}$ of blocklength n, denominated *pseudo-iris code*. The hash value of $\mathbf{K}$, denoted as $h(\mathbf{K})$, is stored in a smart card while $\mathbf{K}$ is discarded.

The user presents both eyes to the system and the reference iris codes of his right and left eyes, $\boldsymbol{\theta}_{\rm ref_1}$ and $\boldsymbol{\theta}_{\rm ref_2}$ respectively, are extracted[3]. The iris codes $\boldsymbol{\theta}_{\rm ref_1}$ and $\boldsymbol{\theta}_{\rm ref_2}$ are concatenated forming the vector $\boldsymbol{\theta}_{\rm ref} = (\boldsymbol{\theta}_{\rm ref_1}|\boldsymbol{\theta}_{\rm ref_2})$ of blocklength p. For reasons that will soon be clear, we assume $n \geq p$. For each user a different sequence of $n-p$ binary digits, represented by the vector **Rand_num**, is randomly generated and kept secret in a smart card. These binary digits are inserted as uniformly as possible and in exactly the same way during enrolment phase and verification phase into the iris code. The *modified reference iris code*, $\boldsymbol{\theta}'_{\rm ref}$, of this new system is obtained by simply inserting uniformly the $n-p$ binary digits of **Rand_num** into $\boldsymbol{\theta}_{\rm ref}$, i.e., a quantity of bits sufficient to make $\boldsymbol{\theta}'_{\rm ref}$ to have the same blocklength as $\boldsymbol{\theta}_{\rm ps}$. The modified iris code $\boldsymbol{\theta}'_{\rm ref}$ is then combined with $\boldsymbol{\theta}_{\rm ps}$ by bitwise exclusive-or (XOR) operation, resulting in

$$\boldsymbol{\theta}_{\rm lock} = \boldsymbol{\theta}_{\rm ps} \oplus \boldsymbol{\theta}'_{\rm ref}.$$

Rand_num, $\boldsymbol{\theta}_{\rm lock}$ and $h(\mathbf{K})$ are stored in a smart card protected by a password.

During the *verification phase (key regeneration)* the user presents his irises and his smart card containing **Rand_num**, $\boldsymbol{\theta}_{\rm lock}$ and $h(\mathbf{K})$ to the system. The *sample iris codes* for right and left eyes are extracted, $\boldsymbol{\theta}_{\rm sam_1}$ and $\boldsymbol{\theta}_{\rm sam_2}$, respectively. Similar to what happened during the enrolment phase the iris codes are concatenated producing the vector $\boldsymbol{\theta}_{\rm sam} = (\boldsymbol{\theta}_{\rm sam_1}|\boldsymbol{\theta}_{\rm sam_2})$ and the binary digits of **Rand_num** are uniformly inserted into $\boldsymbol{\theta}_{\rm sam}$. The *modified sample iris code*, $\boldsymbol{\theta}'_{\rm sam}$, obtained by this procedure is combined with $\boldsymbol{\theta}_{\rm lock}$ by a bitwise XOR operation, resulting in:

$$\boldsymbol{\theta}^*_{\rm ps} = \boldsymbol{\theta}'_{\rm sam} \oplus \boldsymbol{\theta}_{\rm lock} = (\boldsymbol{\theta}'_{\rm sam} \oplus \boldsymbol{\theta}'_{\rm ref}) \oplus \boldsymbol{\theta}_{\rm ps} = \mathbf{e} \oplus \boldsymbol{\theta}_{\rm ps},$$

where $\mathbf{e}$ denotes the vector of errors between the two iris codes, $\boldsymbol{\theta}_{\rm ref}$ and $\boldsymbol{\theta}_{\rm sam}$. The vector $\boldsymbol{\theta}^*_{\rm ps}$ is decoded by the serially concatenated Hadamard and RS codes resulting in $\mathbf{K}'$ that is hashed and compared with $h(\mathbf{K})$. If $h(\mathbf{K}')$=$h(\mathbf{K})$ it means that $\mathbf{K}$=$\mathbf{K}'$ with high probability, as a consequence the cryptographic key is considered valid and can be used successfully by the cryptosystem. Notice that the user identity is also verified assuring non-repudiation of the key.

B. The ECC scheme: concatenated RS and Hadamard codes

As mentioned in Section II, applying serially concatenated RS and Hadamard codes suits well the characteristics presented by the iris (mixed errors). Other ECC techniques are capable of dealing with this mixed error structure [16, Chapter 20]. Nevertheless, the results obtained so far by the use of other ECC techniques are inferior to the ones obtained by the use of concatenated RS and Hadamard codes, especially in relation to the regenerated cryptographic key length. For example, Bringer et al. proposed in [6] the use of a Reed-Muller based product code obtaining a 42 bit key at 10^{-5} FAR and 5.62% FRR.

The serially concatenated code used in the proposed system is formed by a t_s-error-correcting (n_s, k_s) RS code with symbols from $GF(2^m)$ and a binary t_{HC}-error-correcting $(2^k, k+1)$ Hadamard code, denoted respectively, by $RS(n_s, k_s, t_s)$ and $HC(2^k, k+1, t_{HC})$ where n_s is the number of m bit blocks after encoding and k_s is the number of m bit blocks before encoding, k is the order of the Hadamard

[3]OSIRIS (Open Source Iris System) developed under the Biosecure project [18, pp. 34-40] is used to extract a 1,188 bit iris code per iris.

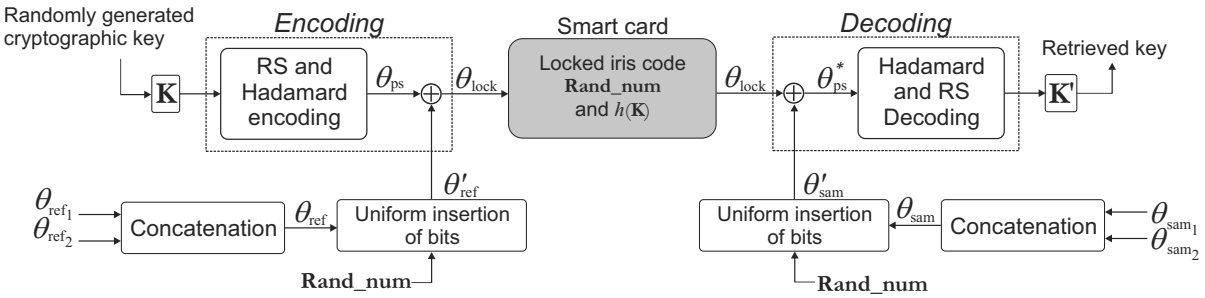

Fig. 2. Multi-instance key regeneration system using smart card, iris and password.

matrix that is obtained by the Sylvester method. Observe that in order to make the two codes work properly in serially concatenated form, it is required to set $m = k + 1$. RS codes are MDS (*Maximum Distance Separable*)[16, pp.238], i.e., $d_{RS} = 2t_s + 1 = n_s - k_s + 1$ and thus, $n_s - k_s = 2t_s$. More details about these codes can be obtained in [16, pp. 1119-1121], [17, pp. 307; 589-590].

IV. Novel Ingredients

In this section we emphasize the key role played by the novel ingredients used in the proposed system, they are: **Rand_num** and multiple biometric information sources.

A. The use of randomly generated bits ($\mathbf{Rand\_num}$)

The use of serial concatenation of RS and Hadamard codes in KR systems based on iris was first introduced by Hao et al [3]. It was observed that applying serially concatenated RS and Hadamard codes suits well the characteristics presented by the iris (mixed errors). However under less controlled circumstances, where variations present in more realistic databases is an issue, extra mechanisms are necessary in order to artificially adapt errors to the error-correcting capability of the ECC scheme. This scenario was considered, for example, in [4] and [5], where in addition to the ECC technique two mechanisms were used: the *iris code shuffling*, to improve the biometric performance of the system as well as provide revocability to the system, and the *zero insertion* to adjust the number of errors to match the error-correcting capability of the concatenated code to a desirable level.

Fig. 3 shows the normalized Hamming distance distribution for genuine users and impostors for the Biosecure database. Fig. 4 in turn shows the normalized Hamming distance distribution for genuine users and impostors for the Biosecure database for the system proposed in [4], that is a unibiometric system and uses *zero insertion* and *iris code shuffling* as extra mechanisms. As we can observe, the histograms in Fig. 3 and in Fig. 4 present each an overlap between genuine and impostor Hamming distributions. However, the overlap in Fig. 3, without using any extra mechanism, is greater than the overlap in Fig. 4, as we can check by observing the minimum and maximum values for the distributions in both figures.

Now, consider a unibiometric version of the proposed KR system. In this case, the block 'Concatenation' in Fig. 2 is not necessary and $\boldsymbol{\theta}_{\mathrm{ref}}$ corresponds an iris code from a unique eye. In this case, 764 randomly generated bits are inserted into the iris code. The normalized Hamming distance distribution for genuine users and impostors for the Biosecure database is exhibited in Fig. 5. As we mentioned earlier, the histograms in Fig. 3 and in Fig. 4 present an overlap between genuine and impostor Hamming distributions. On the other hand, the

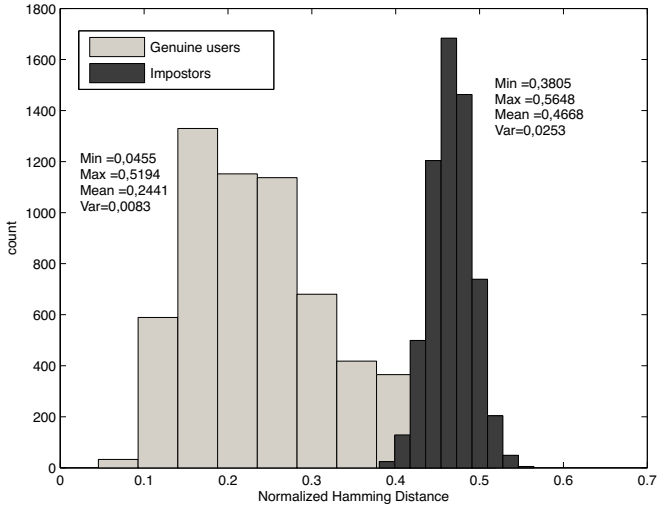

Fig. 3. Normalized Hamming distance distribution for genuine users and impostors for Biosecure database. No extra mechanism is used in order to provide a separation between the Hamming distance distributions for genuine users and impostors.

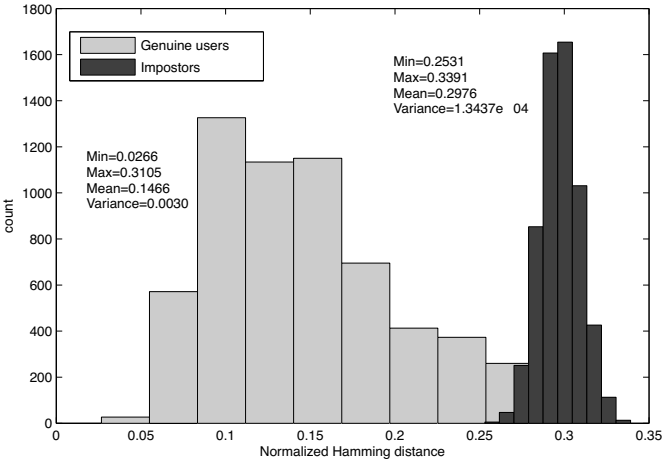

Fig. 4. Normalized Hamming distance distribution for genuine users and impostors for Biosecure database for the unibiometric KR system introduced in [4] that uses zero insertion and iris code shuffling.

histograms in Fig. 5 do not overlap and the distributions are completely separated allowing to set the threshold in a manner that we can decrease the FAR without necessarily increasing the FRR, i.e., we reach FAR=FRR=0%.

It is observed that the multibiometric system introduced in this paper presents even better biometric performance than its unibiometric version in addition to other advantages that will be shown later in this section.

The improvement of the biometric performance is possible because **Rand_num** is user specific, when a genuine user uses his **Rand_num** at pre-defined positions no errors are introduced; however, if an impostor uses his **Rand_num**, the modified iris code has different bits at the pre-defined positions, and errors are introduced. In this manner the separation between genuine and impostor Hamming distance distribution is increased, thus improving the biometric performance of the system (Fig. 5 and Fig. 6).

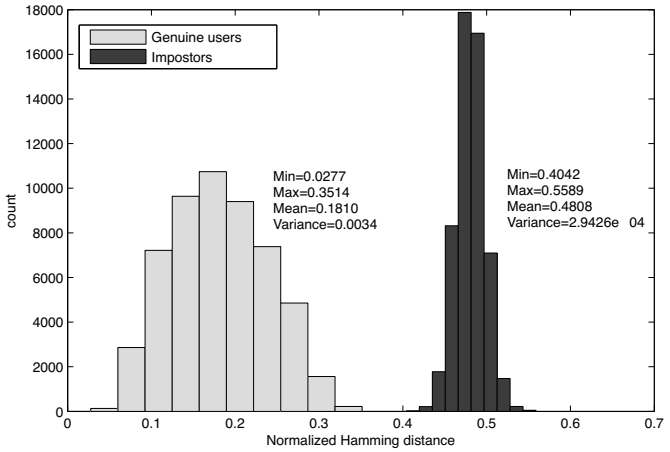

Fig. 5. Normalized Hamming distance distribution for genuine users and impostors for Biosecure database for a unibiometric version of the KR system proposed. 764 randomly generated bits are inserted among the iris codes bits

In addition of providing better separation between the normalized Hamming distance distribution for genuine users and impostors, which is translated in an improvement of the biometric performance of the system, the insertion of **Rand_num** allows to adapt the error-correcting capability of the ECC scheme in a way that will be explained in the sequel.

The Hadamard code with blocklength 2^k corrects up to $2^{k-2}-1$ errors in 2^k bits which means that its error-correcting capability is limited to $(2^{k-2}-1)/2^k \approx 1/4$, i.e., roughly 25%. Experiments showed that this error-correcting capability is not enough to deal with variabilities present in the iris [19]. This fact can be illustrated by observing the distribution for genuine users in Figs. 4, 5 and 6. As we can see, the bits of the iris code from the same user can differ by more than 30%, so the error-correcting capability of the Hadamard code is insufficient. By using **Rand_num**, genuine users introduce the same randomly generated binary digits at the same locations during enrolment and verification phases so at these locations the random bits contribute with no errors. This insertion is able to adjust the number of errors to match the error-correcting capability of the ECC to the desirable level. By random bits insertion at genuine user iris codes the total number of errors remains the same, but the number of errors per block of the Hadamard code decreases. Suppose there are t errors in the binary vector $\mathbf{e} = \boldsymbol{\theta}_{\text{sam}} \oplus \boldsymbol{\theta}_{\text{ref}}$ of blocklength p. Recall that n denotes the blocklength of $\boldsymbol{\theta}_{\text{ps}}$. If $n = p$ then the Hadamard code will need to cope with the fraction t/p of the errors. However, if $n > p$ and we make $n - p = q$, then the same t errors will be spread and will appear to the Hadamard code now as a fraction $t/n = t/(p+q) < t/p$ on average. It turns out that if at most 25% of the bits in each codeword of the Hadamard code are in error, they can be corrected, and all the t errors can thus be corrected.

Besides providing better biometric performance and adjusting the number of errors in a manner that the ECC scheme can deal with them, the insertion of **Rand_num** also provides revocability to the system. Only the binary sequence built from the combination of the iris code and **Rand_num**, i.e., the modified iris code, is able to release the cryptographic key. In case of template compromise it can be revoked by changing **Rand_num**, $\mathbf{K}$ and the smart card password.

Finally, the use of **Rand_num** makes the proposed system less vulnerable to information leakage if compared to the previous systems which use a zero insertion mechanism ([4], [5], [9] and [10]). The details about this security aspect are given in Section VI where we make a security analysis of the proposed system.

B. The use of multiple biometric information sources

We justify our choice for a multi-instance biometric system by all known advantageous features of multibiometric systems while maintaining things simple and being able to regenerate longer and higher entropy keys. Multibiometric systems [1, p. 272] can consolidate multiple sources of biometric information and are used to address some of the limitations of unibiometric systems, being able to improve matching accuracy, increase the population coverage and deter spoof attacks.

The use of a multi-instance biometric system was a choice not only because it enhances classification performance of the biometric system, but also because it allows maintaining the level of the cryptographic key entropy in a baseline that fulfil the security requirements of current security systems, which is very important for our application. We know that some factors during the use of biometric key regeneration systems, as for example the redundancy inserted by the error correction procedure, make the entropy level decrease.

In what concerns to biometric characteristics, iris is the biometric characteristic that presents the highest entropy [21, pp. 51], without counting that it is currently considered to be the best practical modality in terms of recognition performance, in terms of large database accuracy and search speed [1, p.74], [21, pp.6]. In addition, as shown in [7], the irises of a person are not correlated and so can be seen as two independent binary information sources.

Previously, we showed that by using **Rand_num** it is possible to separate the genuine and impostors Hamming distance distributions and we have compared a unibiometric version of our system with a previously proposed unibiometric system [4] (Figs. 4 and 5).

Although, the unibiometric version of our system already showed better biometric performance than other previous unibiometric systems, the multibiometric system introduced here presents even better performance allied with other advantages that will be explained in details soon.

For our proposed multibiometric system (Fig. 2), the normalized Hamming distance distribution for genuine users and impostors for Biosecure database is exhibited in Fig. 6. By comparing the histogram in Fig. 6 with the histogram in Fig. 5, we can observe that the histogram in the Fig. 6 presents greater separation between genuine and impostor Hamming distributions. Thus, the use of multibiometrics allows further enlargement in the separation between the two distributions. So, in terms of biometric performance, we conclude that the use of **Rand_num** in addition to the use of multibiometrics leads to a greater separation between the distributions, i.e. an improvement in the biometric performance of the system.

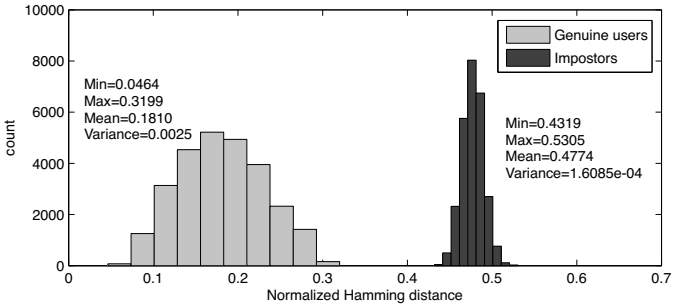

Fig. 6. Hamming distance distribution for genuine users and impostors for Biosecure database for a multi-instance system and inserting 1,528 randomly generated bits among the iris code bits.

Another advantage in using a multibiometric system is the possibility of (re)generating longer cryptographic keys. The cryptographic key length $\|\mathbf{K}\| = m \cdot k_s$ is a function of the parameters of the code and the length of the modified iris code and is expressed as

$$\|\mathbf{K}\| \quad = \quad m \cdot (n_s - 2t_s) = m \cdot \left(\frac{\| \boldsymbol{\theta}'_{\mathrm{ref}} \|}{2^k} - 2t_s \right). \quad (1)$$

The output of the serially concatenated code, $\boldsymbol{\theta}_{\mathrm{ps}}$, has its length limited by the length of the modified iris code and must be equal to $\|\boldsymbol{\theta}'_{\mathrm{ref}}\|$, consequently limiting $\|\mathbf{K}\|$ (Fig. 2). Therefore, by the use of multi-instance biometrics and **Rand_num** insertion we increase the length of the modified iris code, $\|\boldsymbol{\theta}'_{\mathrm{ref}}\|$, consequently increasing the cryptographic key length (Eq. 1).

V. Experiments and Results

In order to evaluate the proposed system computer simulations were performed. The main goal was to be able to regenerate long and strong cryptographic keys (considering current security applications) obtaining at the same time a good biometric system performance, i.e., low values of FAR and FRR. We recall that, for a security application, achieving FAR=0% or as close as possible is most important, however it is also important to keep the FRR as low as possible in order to avoid user annoyance.

For the proposed system, the acceptance threshold described in Section II is equivalent to the total error correction rate of the system, which depends on the error-correcting capability of the serial concatenation of the RS and Hadamard codes plus the effect of inserting **Rand_num**, as we discussed in the Section IV-A. Another important aspect considered during the experiment was that the choice of code parameters and the insertion of **Rand_num** also affects security aspects of the system, more precisely the key length according to (1).

As a first step, computer simulations were performed in order to find the parameters of RS and Hadamard codes able to keep the biometric performance and the security of the system at desirable levels. In order to achieve this goal different values of code parameters (n_s, m) and **Rand_num** were chosen taking into account factors as cryptographic key length and estimated error-correcting capability. These parameters were kept fixed while the system was tested for different values of t_s. We observe that, according to (1), lower values of t_s result in longer keys but decrease the total error correction rate of the system, which implies moving to the left the threshold in Fig. 1. As a result, lower values of t_s result in longer keys but with higher values of FRR and vice-versa (Table I). Thus, t_s acts as a second level threshold, the adjustment of which allows to fine tune system performance.

CBS and NIST-ICE 2005 databases were used to evaluate the system. The initial test used the CBS database [12] in order to tune the system parameters (ECC parameters and length of **Rand_num**) and then the selected parameters were used to evaluate the system under the NIST-ICE 2005 database [13]. Since iris rotations during image acquisition are possible, we move the normalized iris image horizontally in both directions to eliminate rotation effects [18].

CBS-Biosecure V1 and CBS-Casia V2 databases contain 20 images from each eye from 30 persons, i.e., 1200 images. A total of 27,000 genuine comparisons and 27,000 impostor comparisons were performed, considering the mechanism used to eliminate the rotation effects on each database. The NIST-ICE 2005 database consists of 2,953 images from 244 different eyes consisting of 1,425 images of right irises from 124 users and 1,528 images of left irises from 120 users. The right irises are coupled with the left irises for the multi-instance experiments that consisted of 56,061 genuine comparisons and 3,699,108 impostor comparisons also considering the procedure used to avoid rotation effects.

In the sequel we present results better than the best results published so far by considering: 1) FAR as close to zero as possible, since we are considering a security application, 2) low FRR, to avoid user annoyance, 3) cryptographic key lengths and 4) entropy values equal to or higher than the ones required by actual cryptosystems. More details about the entropy values are given in Section VI.

Table I shows results in terms of FAR, FRR and cryptographic key length, $\|\mathbf{K}\|$, obtained by an experiment performed on CBS and NIST-ICE 2005 databases, respectively. In these experiments the parameters for the ECC are $n_s = 61, m = 7$, varying t_s. $\|\mathbf{Rand\_num}\| = 1,528$, two binary digits of **Rand_num** are inserted after every three bits at the first 2,208 bits of $\boldsymbol{\theta}_{\mathrm{ref}}$ and one binary digit of **Rand_num** is inserted

after every three bits at the next 168 bits of $\boldsymbol{\theta}_{\text{ref}}$ resulting in a 3,904-bit modified iris code. We notice that, according to (1), lower values of t_s result in longer key lengths but higher values of FRR (Table I). Although we have not displayed the Hamming distance distributions for genuine users and impostors for the Casia V2 and NIST-ICE 2005 databases, the results presented in Table I assure the separation between these two distributions, especially for the NIST-ICE database where, for $t_s = 14$, we have obtained both FAR and FRR at 0%.

TABLE I
RESULTS IN TERMS OF FAR, FRR AND CRYPTOGRAPHIC KEY LENGTH, $\|\mathbf{K}\|$, ON CBS AND NIST-ICE 2005 DATABASES. FAR IS ALWAYS ZERO FOR ALL THESE TESTS.

Database	t_s	FRR(%)	$\|\mathbf{K}\|$
Biosecure V1	**10**	1.03	287
	11	0.60	273
	12	0.17	259
	13	0.13	245
	14	0.10	231
Casia V2	**10**	0.67	287
	11	0.23	273
	12	0.13	259
	13	0.10	245
	14	0.07	231
NIST-ICE	**10**	0.34	287
	11	0.16	273
	12	0.11	259
	13	0.05	245
	14	0.00	231

The Hamming distance distribution for genuine users and impostors for the NIST-ICE 2005 database, as explained in Section VI, shows that for these parameters the modified iris code has $z = 1,595$ degrees-of-freedom. Furthermore, it is possible to obtain 287-bit keys at 0% FAR and 0.34% FRR, i.e., only 21 ($0.34 \times 6,229 \simeq 21$) among 6,229 authentic samples were falsely rejected. These 21 false rejections occurred because of bit-error rates above 31.93%. The estimated entropy (4) is 160 bits.

VI. SECURITY ANALYSIS

Our proposed multi-instance KR system employs all three factors used for authentication: (a) what the user knows (e.g., password), (b) what the user possesses (e.g., smart card) and (c) what the user is (e.g., biometrics), in order to provide a higher level of security [20]. Since our KR system is used to regenerate cryptographic keys it is important to analyse its security in terms of key entropy. The estimation of the entropy, H, is done using the same criterion used by Hao et al. [3], based on the sphere-packing bound [17, p.19] and using the concept of degree-of-freedom as introduced by Daugman [7, p.283].

The statistical variability that is the basis of iris recognition was analysed in [7] using 9.1 million comparisons between different pairings of 4,258 different irises. The histogram obtained from the distribution of the normalized Hamming distances for distinct irises for this database showed a binomial distribution with mean $\mu = 0.499$, standard deviation $\sigma = 0.0317$ and $z = 249$ degrees-of-freedom [7, p.283] that is calculated by

$$z = \frac{\mu \cdot (1-\mu)}{\sigma^2}. \tag{2}$$

Therefore, using the same analysis for the distribution of the normalized Hamming distances for distinct irises for Biosecure database, which is illustrated in Fig. 6, we observe that it corresponds to a binomial distribution with mean $\mu = 0.4774$ and standard deviation $\sigma = 0.0127$ with $z = 1,551$ degrees-of-freedom. Thus, this statistical analysis of the iris shows that not all bits of the iris code are statistically independent. For example, our experiments on the Biosecure database showed that from 3,904 bits of the modified iris code $\boldsymbol{\theta}'_{\text{ref}}$ only 1,551 bits are independent ($z = 1,551$ degrees-of-freedom), i.e., the modified iris code has 1,551 bits of entropy. From the same experiments running on the NIST-ICE 2005 database we observed that the modified iris code has $z = 1,595$ degrees-of-freedom. For a biometric recognition system based on iris it means that if the correlations within the iris code are known it is enough for the enemy to know z of these bits to obtain the complete iris code. In the specific case of a KR system based on iris, similar to our system, it must also be considered that the codeword $\boldsymbol{\theta}_{\text{ps}}$ is combined with the modified iris code $\boldsymbol{\theta}'_{\text{ref}}$. Therefore, the redundancy inserted by the error correction procedure must also be considered as a factor that reduces the entropy of the iris. Thereby, the sphere-packing bound is a useful tool in order to estimate how many bits of information the enemy actually needs to obtain the cryptographic key, **K**.

Considering that an attacker can obtain the smart card, the system security will rely on the iris and the user **Rand_num**. Supposing that the enemy was able to guess the correct **Rand_num**, the enemy must also provide the correct iris codes extracted from both eyes of the user. In order to set a lower bound on the number M of trials, necessary for the enemy to find the correct iris codes, we consider a worst case by assuming that the enemy knows all the correlations within the user's irises. It has been proved that these correlations exist but it is not clear yet how they can be exploited [7]. Therefore, by considering the sphere-packing bound it follows that

$$M \geq \frac{2^z}{\sum_{i=0}^{w} \binom{z}{i}} \simeq \frac{2^z}{\binom{z}{w}}, \tag{3}$$

where $z = 1,595$ is the uncertainty provided by the modified iris code and $w = \frac{t}{n} \times z$. Since the estimated error correction rate of the system is 31.93%, $w = 0.3193 \times 1,595 \simeq 509$. It follows from (3) that $M \simeq 2^{160}$ which means that the enemy must try to find a 1,595 bit string within 160 bits Hamming distance from the key. In other words, the entropy provided by the system is $\log_2 M = 160$ bits, i.e,

$$H \simeq \log_2 M. \tag{4}$$

Table II compares published unibiometric and multibiometric cryptographic key regeneration algorithms with the

proposed algorithm. It is observed that our proposal (in bold in Table II) achieves better results, e.g., it is possible to regenerate 287 binary digit cryptographic keys with estimated entropy of 160 bits at 0% FAR and 0.34% FRR. All the multibiometric cryptographic algorithms presented in Table II have in common the fact that all perform information fusion at feature level. The main difference in relation to our system is that all the others, besides the system introduced in [9], fuse the information from multiple modalities while in our system we use one single modality, and thus we are able to achieve the advantages usually obtained by the use of multibiometrics keeping things simpler.

It is also important to observe that the proposed system is less vulnerable to information leakage if compared to the systems introduced in [4], [9] and [10] which use a zero insertion mechanism. In the positions where zeroes are inserted $\boldsymbol{\theta}_{\rm lock} = \boldsymbol{\theta}_{\rm ps}$ which can leak useful information for the enemy while inserting a randomly generated binary sequence into $\boldsymbol{\theta}_{\rm ref}$ causes in some parts $\boldsymbol{\theta}_{\rm lock}$ equal to $\boldsymbol{\theta}_{\rm ps} \oplus$ **Rand_num**. Consequently, the only way for an enemy to obtain some potentially useful information about $\boldsymbol{\theta}_{\rm ps}$ is by finding the values of **Rand_num**.

In order to improve the smart card content security the maximum number of login attempts before lockout can be limited. We suggest the possibility of using another biometric feature of the same individual to unlock the smart card instead of a password.

Some systems in Table II as, for example, the systems introduced in [8] and [11] do not make use of other authentication methods as the mechanism we use to protect the data in the smart card (e.g., password). Since we offer the possibility of using authentication mechanisms other than password to protect the smart card content, we have decided to follow a more conservative approach considering the estimation of the entropy of the system itself in order to make the comparison with other systems. For this reason, the entropy values presented in Table II do not consider the addition of the entropy of the password or of any other mechanism used to protect the smart card content. Considering the addition of the entropy of a password generated randomly the systems introduced in [9] and [10] present effective entropy of 147 bits and 183 bits, respectively.

In order to illustrate the maximum effective entropy that our system can achieve consider the use of an 8 character randomly generated password chosen from the standard 94 keyboard characters (not including the space). The entropy for this randomly generated password is $8 \log 94 \simeq 52$ bits [20]. Following the same approach as in [9] and [10], the total entropy of the proposed system is calculated by adding the two entropies: the estimated entropy of the system for $\|\mathbf{K}\| = 287$ and the entropy of the password used to secure the smart card contents, i.e., the total entropy is approximately $160 + 52 = 212$ bits. Hence the effective entropy is $\min(212, \|\mathbf{K}\|) = \min(212, 287)$, i.e., the total estimated entropy considering that a password generated randomly was used to protect the data in the smart card is 212 bits. Other values of entropy can be achieved depending on the mechanism used to lock the smart card, going from 160 bits until 212 bits of entropy for a cryptographic key of 287 bits.

VII. Conclusions

This paper introduces a new multi-instance KR system to regenerate cryptographic keys from biometric data, specifically from the iris. Our proposed KR system uses as ECC technique serially concatenated RS and Hadamard codes together with a mechanism that inserts a randomly generated binary digit sequence, that is unique for each user. As a result, for example, cryptographic keys were regenerated with length 287 binary digits and an estimated entropy of 160 bits at 0% FAR and 0.34% FRR on the NIST-ICE 2005 database. Table II shows that our proposed multibiometric system is able to regenerate cryptographic keys longer and stronger than the ones obtained by previous multibiometric [8] - [11] as well as unibiometric [4] - [6] KR proposals. It is worthy of note that the key length and entropy obtained can be used by real cryptosystems. The FAR is zero, which is important for security applications as the one considered here, and FRR was reduced to very low levels making user acceptance of the system higher, since low FRR avoids user annoyance.

The results obtained so far showed good improvements, nevertheless we are still considering other possible scenarios. For example, by taking into account other codes, i.e., other values for m and n_s and also other ECC techniques. It is also our goal to investigate ways of not reducing so much the uncertainty, and consequently keeping the entropy as high as possible while keeping a good performance in terms of FAR and FRR.

We believe that is also important to go deeper in the security analysis and measure the security improvement which results when we insert randomly generated binary digits versus schemes inserting just zeroes. In principle our proposed system can be used by other biometric modalities as long as the feature vector is in binary form. Therefore it would be interesting to investigate the use of this system, for example, when using combined iris and face features.

Acknowledgements

Danielle P. B. de Arruda Camara and José Sampaio de Lemos Neto acknowledge partial support from the Pernambuco State Foundation to Support Science and Technology - FACEPE, Project APQ-0055-3.04/09 and Project IBPG-0288-0.34/10, respectively, and Valdemar C. da Rocha Jr. acknowledges partial support from the Brazilian National Council for Scientific and Technological Development - CNPq, Project No. 304696/2010-2.

The authors are grateful to the Editor and to reviewer C for useful comments which helped to improve this paper.

References

[1] A. K. Jain, P. Flynn and A. A. Ross, *Handbook of Biometrics*, Springer, 2008.

[2] "Advanced encryption standard (AES)", Federal Information Processing Standards Publication 197, National Institute of Standards and Technology, November 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

TABLE II
COMPARISON BETWEEN UNIBIOMETRIC (*) AND MULTIBIOMETRIC CRYPTOGRAPHIC KEY REGENERATION ALGORITHMS; ECC: ERROR-CORRECTING CODING, RSH: RS AND HADAMARD CODE, RMP: PRODUCT CODES BASED ON REED MULLER CODES AND BCH+: BCH CODES FOLLOWED BY POLYNOMIAL RECONSTRUCTION

Reference	ECC	Key length (in bits)	Entropy (in bits)	FRR (%)	FAR (%)	Database
Hao et al. [3]*	RSH	140	44	0.47	0	Proprietary
Kanade et al. [4]*	RSH	282	83	8.42	0	NIST-ICE (right eyes)
Kanade et al. [5]*	RSH	128/256	94	0.76	0.10	NIST-ICE (right eyes)
Bringer et al. [6]*	RMP	42	-	0.47	0	NIST-ICE (right eyes)
Nandakumar et al. [8]	BCH+	208	49	1.80	0.02	CasiaV1 + MSU-DBI
Nagar et al. [11]	BCH+	224	53	1.00	0	CasiaV1 + MSU-DBI
Kanade et al. [9]	RSH	147	140	0.18	0	NIST-ICE
Kanade et al. [10]	RSH + BCH	210	131	0.91	0	NIST-ICE+NIST-FRGCv2
Proposed	**RSH**	**231**	**154**	**0**	**0**	**NIST-ICE**
Proposed	**RSH**	**287**	**160**	**0.34**	**0**	**NIST-ICE**

[3] F. Hao, R. Anderson and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, No. 9, pp. 1081-1088, 2006.

[4] S. Kanade, D. Camara, E. Krichen, D. Petrovska-Delacrétaz and B. Dorizzi, "Three factor scheme for biometric-based cryptographic key regeneration using iris," *The 6th Biometrics Symposium 2008 (BSYM2008)*, pp. 59 - 64, Tampa, Florida, USA, 2008.

[5] S. Kanade, D. Camara, D. Petrovska-Delacrétaz and B. Dorizzi, "Application of biometrics to obtain high entropy cryptographic keys," *Proceedings of World Academy of Science, Engineering and Technology*, Vol. 27, pp. 251 - 255, Hong Kong, China, March 2009. http://www.waset.org/journals/waset/v27/v27-43.pdf

[6] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji and G. Zmor, "Theoretical and practical boundaries of binary secure sketches," *IEEE Transactions on Information Forensics and Security*, Vol. 3, No. 4, pp. 673-683, 2008.

[7] J. Daugman, "The importance of being random: statistical principles of iris recognition," *Pattern Recognition*, vol. 36, no. 2, pp. 279-291, 2003.

[8] K. Nandakumar and A. K. Jain,"Multibiometric template security using fuzzy vault," *IEEE 2nd International Conference on Biometrics: Theory, Applications and Systems*, Washington DC, USA, 2008.

[9] S. Kanade, D. Petrovska-Delacretaz, and B. Dorizzi,"Multi-biometrics based cryptographic key regeneration scheme," *IEEE 3rd International Conference on Biometrics: Theory, Applications and Systems*,Washington DC, USA, 2009.

[10] S. Kanade, D. Petrovska-Delacretaz, and B. Dorizzi,"Obtaining cryptographic keys using feature level fusion of iris and face biometrics for secure user authentication," *IEEE Computer Vision and Pattern Recognition Workshops (CVPRW)*,Washington DC, USA, pp. 138-145, San Francisco, USA, June 13-18, 2010.

[11] A. Nagar, K. Nandakumar, and A. K. Jain, "Multibiometric cryptosystems based on feature level fusion," *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 1, pp. 255-268, Feb. 2012.

[12] "BioSecure Network of Excellence," www.biosecure.info.

[13] National Institute of Science and Technology (NIST), "Iris Challenge Evaluation," 2005, http://iris.nist.gov/ice.

[14] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," *Proceedings of the Sixth ACM Conference on Computer and Communication Security (CCCS)*, pp. 28-36, Singapore, 1999.

[15] A. Juels and M. Sudan, "A fuzzy vault scheme," *Proc. IEEE Int. Symp. Information Theory*, p. 408, Lausanne, Switzerland, 2002.

[16] S. Lin and D. J. Costello Jr., *Error Control Coding*, 2nd Edition, Prentice Hall, 2004.

[17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, 1988.

[18] D. Petrovska-Dlacretaz, G. Cholet and B. Dorizzi; *Guide to Biometric Reference Systems and Performance Evaluation*, Springer, 2009.

[19] J. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148-1161, 1993.

[20] W. E. Burr, D. F. Dodson, and W. T. Polk, "Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology," April 2006. http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.

[21] P. Tuyls, B. Skoric and T. Kevenaar, *Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*, Springer, 2007.

Danielle Paes Barretto de Arruda Camara was born in Recife, Pernambuco, Brazil, on June 9, 1974. She received the B.Sc. (1998), M.Sc. (2001) and Ph.D. (2006) degrees, all in Electrical Engineering from the Federal University of Pernambuco, Recife, Brazil. She conducted her post-doctoral research in France (2007-2008) where she participated in the Biotyful project concerned with the combination of biometrics and cryptography with the Intermedia group of TELECOM SudParis. This multidisciplinary project that involved research areas such as cryptography, biometrics, error-correcting codes and information theory was funded by the French National Agency for Research - ANR.

She developed a three year project (2009-2012) entitled "Cryptographic Security based on Noisy Physical Elements" for regional scientific development in Brazil which was supported by the Pernambuco State Foundation to Support Science and Technology - FACEPE and by the Brazilian National Council for Scientific and Technological Development - CNPq.

She joined the IEEE Information Theory Society in 2007, the IEEE Computer Society and IEEE Biometrics Council in 2013. She is an IEEE Certified Biometrics Professional (CBP) since 2010. Dr. Camara's professional experience includes research, project coordination, teaching, undergraduate project advising. During her master and doctorate she was a teaching assistant for courses on number theory, cryptography and information theory. Also during her doctorate she worked as a part-time lecturer teaching courses on stochastic processes, scientific methodology and cryptography at University of Pernambuco, Recife, Brazil. She also worked as part-time lecturer teaching courses on linear algebra and analytical geometry, mathematical logic and optical telecommunications systems at Integrated Faculties of Recife (FIR), Recife, Brazil.

Dr. Camara's research interests includes cryptography, information theory, error-correcting codes and biometrics.

José Sampaio de Lemos Neto was born in Bezerros, Pernambuco, Brazil, on November 27, 1980. He received the B.Sc. (2004) and the M.Sc. (2011) degrees in Electrical/Electronics Engineering from the Federal University of Pernambuco, Recife, Brazil. He is currently a doctoral student with the Communications Research Group, Department of Electronics and Systems, Federal University of Pernambuco.

He was a research assistant in the project "Cryptographic Security based on Noisy Physical Elements" developed by Dr. D. P. B. A. Camara and supervised by Prof. V. C. da Rocha, Jr.. He joined in the Brazilian Telecommunications Society in 2010. His professional experience includes research and teaching. He has been a teaching assistant for the course on information theory.

Mr. Lemos-Neto's research interests are in applied digital information theory, error-correcting codes, digital communications, digital signal processing and applied mathematics.

Valdemar C. da Rocha Jr. (M'77, SM'04, LSM'13) was born in Jaboatão, Pernambuco, Brazil, on August 27, 1947. He received in 1970 the B.Sc. degree in Electrical/Electronics Engineering from the Escola Politécnica, Recife, Brazil, and in 1976 he received the Ph.D. degree in Electronics from the University of Kent at Canterbury, U.K. He joined the faculty of the Federal University of Pernambuco, Recife, Brazil, in 1976 as an Associate Professor and founded its Electrical Engineering Postgraduate Programme. He served as Department Chair (1992-1996), and in 1993 he became Professor of Telecommunications.

He was editor for Coding Theory and Techniques, Journal of Communication and Information Systems, co-sponsored by the Brazilian Telecommunications Society and the IEEE Communications Society, and has been a reviewer for a number of scientific journals including IET Electronics Letters, IET Communications and IEEE Transactions on Information Theory. He has also been involved in the organization of conferences in Brazil and abroad.

He is a founder (2002) and past President (2002-2004) of the IEEE Information Theory Society Chapter, Brazil Council. He is founder (2003) and Vice-President for three consecutive terms (2003-2015) of the Institute for Advanced Studies in Communications. He is a founding member (1983) of the Brazilian Telecommunications Society, served as Vice-President for two terms (2000-2004) and as President also for two terms (2004-2008). He joined the IEEE Communications Society in 1977 and the IEEE Information Theory Society in 1981. He is a Member (1982) of the Brazilian Society of Applied and Computational Mathematics, and a Fellow (1992) of the Institute of Mathematics and its Applications, UK.

During 1990-1992, he was a Visiting Professor at the Swiss Federal Institute of Technology-Zurich, Institute for Signal and Information Processing. In 2005-2006 he was a Visiting Professor at the Institute of Integrated Information Systems, University of Leeds, UK, and in 2007 he was a Visiting Professor at the Department of Communication Systems, Lancaster University, UK.

Prof. da Rocha research interests are in applied digital information theory, including error-correcting codes and cryptography. He has published over 100 engineering and scientific papers, including journal and conference papers, and the books Communication Systems, Springer, 2005, and Elements of Algebraic Coding Systems, Momentum Press, 2014.