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 is used with a single mechanism that improves the biometric performance and security of the system, also making possible the regeneration of longer and higher entropy cryptographic keys. The system was evaluated on two public databases: CBS and NIST-ICE 2005. On NIST-ICE 2005 it is possible to regenerate a 287 binary digit cryptographic key with estimated entropy of 160 bits at 0% False Acceptance Rate (FAR) and 0.3371% False Rejection Rate (FRR).**

***Keywords*— 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]. 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]. On the other hand, secret-key cryptography is able to assure high data privacy as long as the cryptographic key is secret, long and as random as possible to provide the required security level (e.g., the Advanced Encryption Standard (AES) was designed to support encryption keys of length 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.

There are in the literature many unibiometric systems that combine biometrics and cryptography (e.g. [3], [4], [5], [6]) but most of them face problems regarding low entropy keys and high rejection rate. On the other hand, multibiometric systems [1] 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[1] 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 multi-biometric 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], [9].

Experiments were performed on CBS (Casia-Biosecure) [10] and NIST-ICE 2005 [11] databases. 287 binary digit keys with 160 bit estimated entropy were regenerated on the ICE-NIST2005 database, at 0% false acceptance rate (FAR) and 0.3371% false rejection rate (FRR)[2].

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. In Section IV we describe the experiments performed and present the results obtained. In Section V we present a security analysis of the proposed KR system. Summing up, in Section VI 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

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, Recife, PE, BRAZIL.e-mail: dpbac@ieee.org, {jose.lemosnt, vcr}@ufpe.br.

[1] A multibiometric system that captures a sample of multiple instances (e.g. right and left iris) with the same sensor.

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

strongly linked to the user (non-repudiation), allowing key revocability, key diversity[3] and also privacy to the biometric data. ECC techniques are used in order to deal with biometrics inherent variability. Two constructions are popular in this approach: the *Fuzzy commitment scheme* [12] and the *Fuzzy vault scheme* [13]. In 1999 Juels and Wattenberg [12] proposed the use of ECC to deal with this variability in order to regenerate cryptographic keys. However, no practical ECC technique was proposed. 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 [11], showed very high FRR, e.g., 19.41% for a 42 bit key.

Other unibiometric KR systems based on 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 0.055% FAR and 1.04% FRR on NIST-ICE 2005 database [11] 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.

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

The use of ECC 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 enough to correct *intra-user variations*, e.g., differences between error bits for the same eye, but unable to correct *inter-user variations*, e.g., differences between different eyes.

In this paper we have considered the use of multibiometrics, more specifically the use of two eyes of the same individual (multi-instance). As stated in [1] a multibiometric system relies on the evidence presented by multiple sources of biometric information in order to enhance classification performance. Multibiometric systems are classified as multi-instance, multi-sensor, multi-algorithm, multi-sample, multi-modal and hybrid systems. 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].

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 [13] to regenerate cryptographic keys. Recently, 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].

In the next section, we introduce a new multi-instance KR system able to regenerate longer and higher entropy cryptographic keys.

III. New Proposal

As observed in [3], applying serially concatenated RS and Hadamard codes suits well the characteristics presented by the iris. However under less controlled circumstances, where variations present in more realistic databases is an issue, other mechanisms are necessary in order to 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. The proposed KR system also uses a serial concatenation of an RS code and a Hadamard code. An important difference between the scheme presented here and previous ones, that use a similar ECC technique, is the use of a single mechanism to provide revocability to the system, to adapt the errors in a way that the ECC technique can deal with them and to improve even more the biometric performance, achieving not only 0% FAR but also reducing to very low levels the FRR.

A. Description of the New Proposal

The KR system introduced is illustrated in Fig. 1. During the *enrolment phase (key generation)* a random cryptographic key $\mathbf{K}$ is generated and encoded by the serial concatenation of RS and Hadamard codes resulting in the vector $\boldsymbol{\theta}_{\text{ps}}$, denominated *pseudo-iris code*. The hash value of $\mathbf{K}$, $h(\mathbf{K})$, is stored in a smart card while $\mathbf{K}$ is discarded.

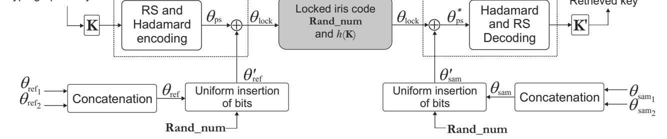

Fig. 1. Multi-instance key regeneration system using smart card, iris and password.

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

The user presents both eyes to the system and the reference iris codes of his right and left eyes, $\boldsymbol{\theta}_{\text{ref}_1}$ and $\boldsymbol{\theta}_{\text{ref}_2}$, are extracted[4]. The iris codes $\boldsymbol{\theta}_{\text{ref}_1}$ and $\boldsymbol{\theta}_{\text{ref}_2}$ are concatenated forming the vector $\boldsymbol{\theta}_{\text{ref}} = (\boldsymbol{\theta}_{\text{ref}_1}|\boldsymbol{\theta}_{\text{ref}_2})$. For each user a different sequence of binary digits, represented by the vector **Rand_num**, is randomly generated and kept secret, encrypted in a smart card. The *modified reference iris code*, $\boldsymbol{\theta}'_{\text{ref}}$, of this new system is obtained by simply inserting uniformly the binary digits of **Rand_num** into $\boldsymbol{\theta}_{\text{ref}}$. The modified iris code $\boldsymbol{\theta}'_{\text{ref}}$ is then combined with $\boldsymbol{\theta}_{\text{ps}}$ by bitwise exclusive-or (XOR) operation, resulting in $\boldsymbol{\theta}_{\text{lock}} = \boldsymbol{\theta}_{\text{ps}} \oplus \boldsymbol{\theta}'_{\text{ref}}$. **Rand_num**, $\boldsymbol{\theta}_{\text{lock}}$ 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**, $\boldsymbol{\theta}_{\text{lock}}$ and $h(\mathbf{K})$ to the system. The *sample iris codes* for right and left eyes are extracted, $\boldsymbol{\theta}_{\text{sam}_1}$ and $\boldsymbol{\theta}_{\text{sam}_2}$. Similar to what happened during the enrolment phase the iris codes are concatenated resulting in the vector $\boldsymbol{\theta}_{\text{sam}} = (\boldsymbol{\theta}_{\text{sam}_1}|\boldsymbol{\theta}_{\text{sam}_2})$ and the binary digits of **Rand_num** are uniformly inserted into $\boldsymbol{\theta}_{\text{sam}}$. The *modified sample iris code*, $\boldsymbol{\theta}'_{\text{sam}}$, obtained by this procedure is so combined with $\boldsymbol{\theta}_{\text{lock}}$ by a bitwise XOR operation, resulting in:

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

where $\mathbf{e}$ indicates the errors between the two iris codes, $\boldsymbol{\theta}_{\text{ref}}$ and $\boldsymbol{\theta}_{\text{sam}}$.

$\boldsymbol{\theta}^*_{\text{ps}}$ 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.

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 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 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*)[14, 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 [14], [15].

For each user a different sequence of binary digits, **Rand_num**, is randomly generated. 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 insertion of **Rand_num** provides to the system:

(a) ***Improvement of Biometric Performance***: 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. 2).

(b) ***System Revocability***: 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.

(c) ***Adjusting the number of errors***: The Hadamard code corrects up to $2^{k-2} - 1$ errors in 2^k bits which means that its error-correcting capability is limited to 25%. Experiments showed that this error-correcting capability is not enough to deal with variabilities present in the iris [17]. 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 decreases.

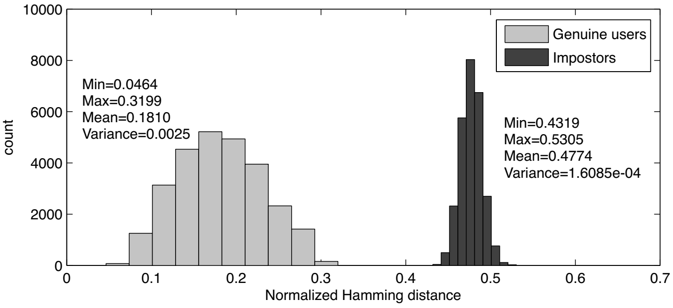

Fig. 2. Hamming distance distribution for genuine users and impostors for Biosecure database for a multi-instance system and inserting 1,528 randomly generated bits among the iris code bits.

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

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

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

IV. Experiments and Results

For the computer simulations different values of code parameters (n_s, m) were chosen taking into account factors as cryptographic key length and estimated error-correction capability. These parameters were kept fixed while the system

[4] OSIRIS (Open Source Iris System) developed under the Biosecure project [16, pp. 34-40] is used to extract a 1,188 bit iris code per iris.

was tested for different values of t_s. As illustrated in Table I lower values of t_s result in longer keys but with higher FRR and vice-versa. 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 system was initially tested on CBS database [10] 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 ICE-NIST 2005 database [11]. Since iris rotations during image acquisition are possible, we move the normalized iris image horizontally in both directions to eliminate the rotation effects [16].

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 the best results obtained 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 equal to or higher than the ones required by actual cryptosystems. More details about the entropy are given in Section V.

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. $||\textbf{Rand\_num}|| = 1,528$, 2 binary digits of **Rand_num** are inserted after every 3 bits at the first 2,208 bits of $\boldsymbol{\theta}_{\text{ref}}$ and 1 binary digit of **Rand_num** is inserted after every 3 bits at the next 168 bits of $\boldsymbol{\theta}_{\text{ref}}$ resulting in a 3,904-bit modified iris code. The Hamming distance distribution for genuine users and impostors for NIST-ICE 2005 database shows that for these parameters the modified iris code has $z = 1,595$ degrees-of-freedom [7, p.283] and that it is possible to obtain 287-bit keys at 0% FAR and 0.3371% FRR, i.e., only 21 ($0.3371 \times 6,229 \simeq 21$) among 6,229 authentic samples were falsely rejected. These 21 false rejections occurred because of bit-error rates above 31.93%. The estimated entropy is 160 bits (Eq.3).

V. Security Analysis

Our proposed multi-instance KR system employs of 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 [18]. 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 [15].

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*
Casia V2	**10**	*0.67*	*287*
	11	*0.23*	*273*
	12	*0.13*	*259*
	13	*0.10*	*245*
NIST-ICE	**10**	*0.34*	*287*
	11	*0.16*	*273*
	12	*0.11*	*259*
	13	*0.05*	*245*

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 irises codes extract 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 right irises 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 [15, p.19] it follows that

$$M \geq \frac{2^z}{\sum_{i=0}^{w} \begin{pmatrix} z \\ i \end{pmatrix}} \simeq \frac{2^z}{\begin{pmatrix} z \\ w \end{pmatrix}}, \qquad (2)$$

where $z = 1,595$ is the uncertainty provided by the iris code modified and $w = \frac{t}{n} \times z$.

Since the estimated error correction rate of the system is 31.93%, $w = 0.3193 \times 1,595 \simeq 509$. By Eq. (2) $M \simeq 2^{160}$ 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,

$$H \simeq \log_2 M. \qquad (3)$$

Table II compares actual unibiometric(*) and multibiometric cryptographic key regeneration algorithms with the proposed algorithm. It can be observed that our proposal (in bold) 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 0.3371 % FRR.

It is also important to observe that the proposed system is less vulnerable to information leakage than the system introduced in [4], which uses a zero insertion mechanism. In the positions where zeroes are inserted $\boldsymbol{\theta}_{\text{lock}} = \boldsymbol{\theta}_{\text{ps}}$ which

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

Ref.	ECC	Key bits	Entropy	FRR%	FAR%	Database
[3]*	RS	*140*	*44*	*0.47*	*0*	Proprietary
[4]*	RS	*282*	*83*	*8.42*	*0*	NIST-ICE (right eyes)
[5]*	RS	*128/256*	*94*	*0.76*	*0.096*	NIST-ICE (right eyes)
[6]*	RMP	*42*	-	*0.47*	*0*	NIST-ICE (right eyes)
[8]	BCH+	*208*	*49*	*1.80*	*0.02*	CasiaV1 + MSU-DBI
[9]	RSH	*147*	*147*	*0.18*	*0*	ICE-NIST
-	**RSH**	***231***	***154***	***0***	***0***	**NIST-ICE**
-	**RSH**	***287***	***160***	***0.3371***	***0***	**NIST-ICE**

can leak useful information for the enemy while inserting a randomly generated binary sequence into $\boldsymbol{\theta}_{\text{ref}}$ causes in some parts $\boldsymbol{\theta}_{\text{lock}}$ equal to $\boldsymbol{\theta}_{\text{ps}} \oplus$ **Rand_num**. Consequently, the only way for an enemy to obtain some potentially useful information about $\boldsymbol{\theta}_{\text{ps}}$ 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.

VI. 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 0.3371% FRR on the NIST-ICE 2005 database. Table II shows that our proposed multi-biometric system is able to regenerate cryptographic keys longer and stronger than the ones obtained by previous multi-biometric [8], [9] as well as unibiometric [4], [5], [6] KR proposals. It is worth noticing 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 show formally why inserting randomly generated binary digits is more secure than 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 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.

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.

[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. 39, pp. 264 - 268, Hong Kong, China, March 2009. http://www.waset.org/pwaset/v39/v39-45.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,"Multibiometric template security using fuzzy vault," *IEEE 3rd International Conference on Biometrics: Theory, Applications and Systems*,Washington DC, USA, 2009.

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

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

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

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

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

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

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

[17] 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.

[18] 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.