CANCELABLE BIOMETRICS FOR BIMODAL CRYPTOSYSTEMS

V. ALARCON-AQUINO†, P. GOMEZ-GIL‡, J. M. RAMIREZ-CORTES‡, O. STAROSTENKO† and H.A. GARCIA-BALEON§

† *Department of Computing, Electronics and Mechatronics, Universidad de las Americas Puebla, Cholula, Puebla 72810, MEXICO. vicente.alarcon@udlap.mx*

‡ *Department of Electronics and Computer Science, National Institute for Astrophysics, Optics, and Electronics, Puebla, MEXICO*

§*Department of Electrical and Electronic Engineering, Imperial College London, London SW7 2AZ, UK*

***Abstract*— Biometric-based techniques have recently emerged as a trustworthy and effective approach of user authentication; however, unlike conventional authentication methods such as passwords and tokens, if an enrolled biometric template is compromised, usually it cannot be revoked or re-issued. In this paper, four naive cancelable techniques, namely, shifting, password-dependent shifting, XOR and adding, for a bimodal biometric cryptosystem are presented. The proposed cancelable techniques are designed to be embedded into any bimodal biometric cryptosystem. The bimodal biometric cryptosystem uses speech and electrocardiogram signals as biometric information. The biometric cryptosystem implements an error-correction layer using the Hadamard code. The performance of the four cancelable techniques is assessed using ECG signals from MIT-BIH database and speech signals from a speech database created for testing purposes. The results show that the best performance in terms of FAR and FRR metrics is achieved with XOR and adding techniques.**

***Keywords*— Biometric Cryptosystem, Cancelable Technique, Hadamard Code.**

I. INTRODUCTION

Biometrics guarantees the identification of individuals based on measuring their personal unique features with a high degree of assurance (see e.g. Clancy *et al.,* 2003; Goh and Ngo, 2003; Hao *et al.,* 2005; Hao and Chan, 2002; Daugman, 2009). However, the advantages of biometrics can be minimized if the true biometric privacy is exposed. It is well-known that unlike conventional authentication methods such as passwords or tokens, if an enrolled biometric template is compromised, usually it cannot be revoked or re-issued. Cancelable biometrics is thus a way in which to incorporate protection and the replacement features into biometrics (Ratha *et al.,* 2001; Rathgeb and Uhl, 2011). Protecting the true biometric using a cancelable technique enables to the biometric cryptosystems revoking easily the *fake* biometric when somehow the security of the biometric cryptosystem is compromised. Cancelable techniques for biometrics were proposed in Ratha *et al.* (2001) and it was successfully adapted to fingerprint biometrics (Ratha *et al.,* 2007; Ouda *et al.,* 2011). Later, other works have presented alternative cancelable techniques to protect the true biometric using hash functions (Davida *et al.,* 1998; Chakravarty *et al*., 2011; Gaddam and Lal, 2010), signature recognition systems (Maiorana *et al.,* 2010), and fuzzy schemes (Juels and Wattenberg, 1999; Rathgeb and Uhl, 2011). These works have shown the importance of protecting the true biometrics as well as an improvement in the performance and overall security of their biometric cryptosystems however their cancelable techniques are complex and oriented to a specific type of biometric.

Some biometric cryptosystems offer sophisticated techniques to extract templates or even to derive cryptographic keys from biometric data; however, these biometric cryptosystems expose the privacy of the true biometric through the processing stages (see e.g. Clancy *et al.,* 2003; Goh and Ngo, 2003; Hao *et al.,* 2005; Hao and Chan, 2002; Garcia-Baleon *et al*., 2009a; Garcia-Baleon and Alarcon-Aquino, 2009; Garcia-Baleon *et al*., 2009b)). This fact has a serious impact in the social acceptance of biometric cryptosystems. The design of the bimodal biometric cryptosystem reported in this paper exploits the advantages of biometrics and cancelable techniques to keep secret the true biometrics through the processing stages and to guarantee revocability of the fake biometrics when it is needed.

The use of the ECG (electrocardiogram) signals is widely spread. However, most of the research is focused on developing methods to diagnose heart diseases and methods to compress and to denoise the ECG signals (Yarman *et al*., 2004; Ktata *et al.*, 2009; Chouakri *et al.,* 2005). In recent years, the use of ECG signals has turned to the biometric field due to the fact that this biometric signal has the same potential compared with other well-known biometrics. In fact, ECG signals present advantages over fingerprint or faceprint such as liveness and circumvention (Wubbeler *et al.,* 2007; Ya-Ting *et al.*, 2007). Several works have reported systems to identify individuals with a high degree of trust (Garcia-Baleon *et al.,* 2009a; Garcia-Baleon and Alarcon-Aquino, 2009; Wubbeler *et al.,* 2007; Ya-Ting *et al.,* 2007). However, all these works have omitted to protect the true biometric in the process.

On the other hand, the use of speech as biometric has been proposed in several papers (Covell and Baluja, 2007a; Covell and Baluja, 2007b). The techniques and algorithms used for extracting and generating signatures using the speech can vary widely in power and sophistication, and range from statistical techniques or neural networks to artificial intelligence. The extraction of a spectrogram fingerprinting using wavelet hashing is re-

ported in Covell and Baluja (2007a). Also, the idea of audio fingerprinting combining computer vision and data stream processing has been proposed in Covell and Baluja (2007b).

In this paper we report four cancelable techniques, namely, shifting, password-dependent shifting, XOR and adding, to be embedded into any bimodal biometric cryptosystem. The approach uses speech and electrocardiogram (ECG) signals as biometric information. The remainder of this paper is organized as follows. In Section 2, the relevant characteristics of the biometric signals, the error metrics, and the Hadamard Code as well as the performed wavelet analysis is described. In Section 3, the proposed cancelable techniques are presented. In Section 4, simulation results of the different cancelable techniques are reported. Finally, conclusions are discussed in Section 5.

II. BIOMETRIC SIGNALS: ECG AND SPEECH

The proposed bimodal biometric cryptosystem works using forced-choice range ECG samples extracted from an ECG signal and forced-choice range speech samples extracted from simple utterances of predetermined single words. The forced-choice range of an ECG sample is defined as the range between the two maximum points (values) of two QRS complex neighbors. Figure 1 shows two QRS complex of an ECG signal.

The QRS complex represents ventricular depolarization. The duration of the QRS complex is normally between 0.06 to 0.1 seconds. The shape of the QRS complex changes depending on which recording electrods are being used. The forced-choice range ECG sample is delimited by the two maximum values of each QRS complex that occurs in R for both. Henceforth a forced-choice range ECG sample extracted from the ECG signal is referred to as $R-R$ signal. However, the quasi-periodicity of ECG signals leads to obtain $R-R$ signals with 75-120 samples instead of $R-R$ signals with constant samples. Then, it is necessary to establish a limit applicable to all $R-R$ signals to generate $R-R$ signals with constant samples. Several experiments lead to determine that 60 samples per $R-R$ signal are enough to identify different individuals with a high degree of trusting. If the magnitude of each sample of the $R-R$ signal is represented using a byte, a 60-byte string is then obtained.

Regarding the speech signal, the use of a predetermined single word as the biometric speech data reduces the complexity of processing multiple words and also avoids the consideration of algorithms for detecting endpoints, removing silent parts from the raw audio signal, among others. Figure 2 shows the speech sample of a predetermined single word from an individual. The proposed selection process of the forced-choice range is quite simple. As can bee seen, the speech signal begins around the 1000 sample. In other words, the signal before the 1000 sample can be considered as noise. The amplitude of the noise depends on the environment where the biometric system works. In this work, selecting the forced-choice range speech sample requires to

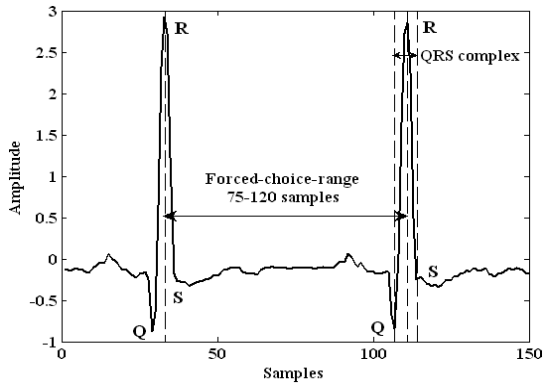

Figure 1: R −R signal, forced-choice-range ECG sample, of an ECG signal.

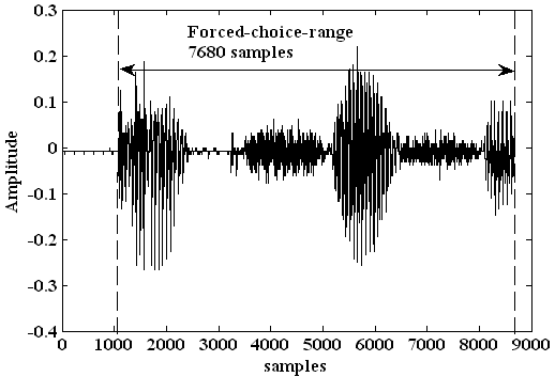

Figure 2: S signal, forced-choice-range speech sample, of an speech signal.

set a threshold. When the amplitude of the speech signal reaches the threshold, the acquisition process begins. The acquisition process takes the first 7680 samples beginning with the sample that launched the acquisition process. The acquisition characteristics of the process are as follows: sampling rate of 11025 samples/sec, bit resolution of 8 bits/sample, and one channel. In this experiment the selected value for the threshold was 0.035. However, there is no rule to establish the threshold value since it depends on the noise characteristics of the environment where the biomal biometric system works. The forced-choice range speech sample extracted from the speech signal is referred to as S signal. Thus after performing the acquisition process, a vector of 7680 values is obtained. If the magnitude of each sample of the S signal is represented using a byte, a 7680-byte string is then obtained.

A. Performance Errors Metrics

The design of the bimodal biometric cryptosystem is fully based on the error characteristics of the biometric signals. Two error metrics must be considered to design a robust architecture, namely, intra-error and inter-error (Garcia-Baleon and Alarcon-Aquino, 2009b). The intra-error is defined as the maximum permissible number of errors between two biometric signals, R-R signal or S signal, that belong to the same individual. The inter-error is defined as the minimum required number of errors between two biometric signals that let us to conclude that these biometric signals do not belong to the same individual.

After comparing randomly 6750 raw R-R signals, forced-choice range ECG samples, extracted from the MIT-BIH Normal Sinus Rhythm Database (Goldberger *et al.,* 2000), the mean square error (MSE) intra-error is 28.5% while the MSE inter-error is 43%. There is a band between 28.5% and 43% where the R −R signals falling within this band can not be classified. Note that if the band is thin, the false acceptance rate (FAR) and the false rejection rate (FRR) metrics of the approach improve because the degree of uncertainty at the classification decreases. One way to make the band thinner is to filter the random-background noise of the R-R signal before performing the comparison. The same experiment is performed for the S signals comparing randomly the 400 raw S signal, forced-choice range speech sample, from our speech database. This database contains 20 raw S signals from 20 different individuals. The MSE intra-error is 40.3% while the MSE inter-error is 68%. Comparing the MSE intra and inter-error of both, R −R and S, signals show that if the bimodal biometric cryptosystem had to work under these conditions the overall performance will be very poor.

B. Removing Background-Random Noise

The use of wavelets as signal analysis tool has increased in recent years due to its flexibility and analysis capacity. Wavelet analysis has been used in discontinuity and breakpoints detection algorithms, de-noising, pattern recognition and compression algorithms for signal and images, and object detection (Walker, 2008). This paper focuses on the idea of using wavelets as a tool for analyzing and then denosing the R-R signals. Removing the noise in the biometric signals improves the error metrics and reduces the degree of uncertainty. The selection of the wavelet function to analyze the $R-R$ signal is based on the reduced value of the MSE from the several denoising experiments performed over the signal of interest. Several experiments (Chouakri *et al*., 2005), including those performed in this work, have shown that the symlet8 wavelet is the best choice to analyze the ECG signals. Other wavelets like Daubechies family may also be considered. Table 1 summarizes the values for the MSE intra and inter error for each decomposition level using the maximal overlap discrete wavelet transform (MODWT) (Garcia-Baleon *et al*., 2009a; Garcia-Baleon and Alarcon-Aquino, 2009; Alarcon-Aquino and Barria, 2009). The MODWT is usually preferred over a discrete wavelet transform (DWT) due to the translation-invariant property of the MODWT. This property allows preserving the integrity of transient events. Also the MODWT can be applied to any sample size (Alarcon-Aquino and Barria, 2009). The proposed algorithm is based on the fact that the trend coefficients hold most of the energy of the original signal while the wavelet coefficients do not (Walker, 2008).

The 4-level symlet8 wavelet decomposition is good enough to remove some background random noise but also the resulting trend at this level is sufficient to reject those $R-R$ signals that are different. After performing the 4-level symlet8 wavelet decomposition, the MSE intra-error is reduced from 28.5% to 23.55% and the MSE inter-error is also reduced from 43% to 30.82%. The absolute value of the band is reduced from 14.5% to 7.27% then the uncertainty also decreases.

Table 1: Symlet8 Wavelet Decomposition

Decomposition level	ECG intra-error	ECG inter-error
1	28.50%	43.00%
2	26.00%	39.18%
3	24.72%	35.95%
4	23.55%	30.82%
5	23.45%	26.75%
6	23.20%	22.90%

Since we have a 7680-bytes of S signals and in order to have a 60-byte string similar to the ECG signal we use the discrete wavelet transform (DWT). That is, here we are more interested in preserving the bimodal biometric system balanced. When the S signal is decomposed a similar behavior to the $R-R$ signal is obtained, the intra-error diminishes slowly as the decomposition level increases and the inter-error diminishes more rapidly as the levels of decomposition increases. The 7-level wavelet decomposition is enough to remove some background-random noise but also the resulting trend at this level is sufficient to reject those *S* signals that are from different individuals.

After running iteratively the comparison process between *S* signals of same individual and S signals from different individuals the MSE intra-error improved from 40.3% to 25.6% while the MSE inter-error improved from 68% to 49.2%. Then the absolute value of band in the case of the S signalsdecreasedfrom27.7% to 23.6% thus the band of uncertainty also decreased. However, the MSE errors in the $R-R$ signals after the 4-level wavelet decomposition and in the *S* signal after the 7-level wavelet decomposition are still high to be ignored. To deal with these remained background-random noise errors, we use the Hadamard code to correct them.

C. Hadamard Code

Hadamard codes are obtained from a Hadamard matrix generated by Sylvester method (Massoud, 2010). Hadamard matrix is a square orthogonal matrix with elements '1'or '-1'. A Hadamard matrix of any dimension can be obtained recursively by (Massoud, 2010)

$$H_k = \begin{bmatrix} H_{k-1} & H_{k-1} \\ H_{k-1} & -H_{k-1} \end{bmatrix} \quad (1)$$

To obtain the Hadamard code once the Hadamard matrix H_k has been derived is necessary to cascade H and $-H$ as follows (Kabatiansky *et al*., 2005; Moon-Todd, 2005):

$$H_c = \begin{bmatrix} H \\ -H \end{bmatrix} \quad (2)$$

Each codeword can be derived by replacing from H_c each H_{k-1} by 1 and each $-H_{k-1}$ by 0. A Hadamard matrix of size n has $2n$ codewords. The code has a minimum distance 2^{k-1} and hence can correct upto $2^{k-2}-1$ errors (Morelos-Zaragoza, 2006; Moon-Todd, 2005). According to the MSE reported in the previous section, it was determined that the best suitable value for k was 7 for

both, $R-R$ and S, signals. In this way, the chosen code is able to correct 31 bit out of 128 bit or 24.22% which is good enough to correct the inter-errors but not the intra-errors. This analysis lets us to determine where the errors take place and the percentage of error per sample. $R-R$ signals from the same individual usually differs 23.55% of the total bits. However, the $R-R$ signals from different individuals differ 30.82% of the total bits. We chose a Hadamard code which is able to correct around 24.22% of the errors. Then the errors of $R-R$ signals from the same individual will be corrected. However, the error-correction layer is unable to correct the errors when an $R-R$ signal from a different individual is presented before the bimodal biometric system.

The same happens with the S signals. S signals from the same individual usually differs 25.6% of the total bits. However, the S signals from different individuals differ 49.2% of the total bits. We chose a Hadamard code with k=7 which is able to correct around 24.22% of the errors. Then the errors of S signals from the same individual will be corrected but not those from different individuals.

III. PROPOSED CANCELABLE TECHNIQUES

Since the cancelable biometric concept was proposed in (Ratha 2001) several cancelable techniques have been reported (see e.g. Ratha *et al.,* 2001; Ratha *et al.,* 2007; Davida *et al.*, 1998; Juels and Wattenberg, 1999). However, most of these techniques are designed for a specific type of biometric or even for a specific system. In this section, four naive cancelable techniques are presented. These techniques are flexible and can be adapted to work with different biometric signals (e.g. speech, ECG (Garcia-Baleon *et al.,* 2009a; Garcia-Baleon and Alarcon-Aquino, 2009)) or even biometric images (e.g. faceprint, fingerprint (Rathgeb and Uhl, 2011).

As stated in Israel *et al*. (2005) and Singh and Gupta (2008) the identification of individuals using ECG or speech signals is possible. Also, a cancelable technique only makes sense if both biometric signals are acquired at exactly the same time. The proposed biometric cancelable techniques are designed to be implemented on hardware. This is due to the fact that a software implementation may use reverse software engineering. The use of databases to test the performance of the biometric cancelable techniques is allowed to emulate the devices used to acquire the biometric signals.

Figure 3 summarizes the proposed cancelable techniques. Due to the fact that the proposed biometric cancelable techniques can be used or adapted to work with any biometric signal, a general explanation of the biometric cancelable techniques is given. A particular realization using electrocardiogram and speech signals is then shown. All the proposed biometric cancelable techniques, Figure3(a-d), are non-invertible and revocable. The first criterion is essential to guarantee the security whereas the second assures the generation of new fake biometrics when there are security concerns.

Consider that two biometric signals of size n are acquired at exactly the same, these biometric signals may be represented using the vector a, $\{a_1, a_2, a_3, ..., a_n\}$ and the vector b, $\{b_1, b_2, b_3, ..., b_n\}$. Once the biometric signals are acquired, the magnitude of each element of the vector is represented using a byte. This process also can be performed in real time. The resultant signal after performing a biometric cancelable technique is referred to as vector c.

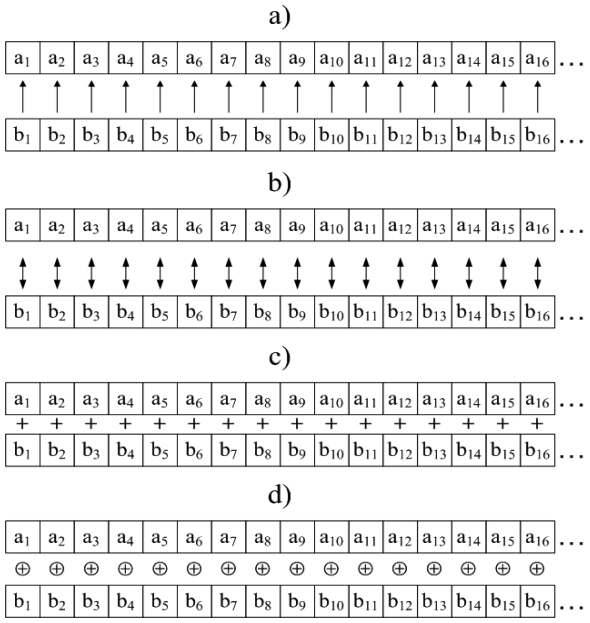

Figure 3: Proposed Cancelable techniques. a)Shifting; b)Password-dependent shifting; c)Adding; d)XOR

Figure 3(a) shows the first method, henceforth referred to as shifting technique, which is an adaptation of the GRAY-COMBO method reported in Ratha (2008). Taking one biometric vector as a base, the magnitude of the elements of the other biometric vector indicates how many shifts are applied to the element in turn. The shifts are done circularly, to avoid losing data, in the right direction. For example, if vector a has been selected as the vector base, an example of the shifting process for the first element position is as follows: before the shifting process (a_1= 00101011 and b_1= 00000011), after the shifting process (c_1 = 01100101, the bits of vector a1 are moved circularly to the right three positions because of the magnitude of b_1). This method can be expressed as follows:

$$c_i\big|_{i=1}^{n} = a_i >> |b_i| \tag{3}$$

Figure 3(b) shows the second method, referred to as *password-dependent shifting technique*. This method works similar to the first method however the direction of the shifts can be either left or right. The shift direction can be defined by a password associated to the individual. For example, given a vector password p, $\{p_1, p_2, p_3, ..., p_n\}$, in binary form. If p_1 is equal to '0', the shift must be done to the right. If it is equal to '1', the shift must be done to the left. The direction of the shifting does not affect the error characteristics of the biometric signals; moreover, the password represents another layer of security to the bimodal biometric cryptosystem. This technique is given by

$$c_i\big|_{i=1}^{n} = \begin{cases} si & p_i = 0; \quad a_i >> |b_i| \\ si & p_i = 1; \quad a_i << |b_i| \end{cases} \tag{4}$$

Figure 3(c) shows the third method, referred to as *adding technique*, where the magnitude of both biometrics, a and b, are added, which can be expressed as $c = a + b$. Note that this method adds the error characteristics of both biometric signals. The performance of the bimodal biometric cryptosystem will not be affected while the error in vector c is kept below the correctable error rate explained in previous sections.

Figure 3(d) shows the fourth method, referred to as *XOR technique*, which takes both biometric signals and XORs the vector elements, position by position. For example, given two biometric signals in vector form such as: a_1 = 00101011 and b_1 = 00000011. The resultant vector will be c_1 = 00101000. This can be expressed as $c = a \oplus b$.

Methods (a, c, d) have the advantage that they can be embedded in the current biometric cryptosystems because the biometric signals conserve their own characteristics. Also, these methods do not need extra information besides the biometric signals then these methods are independent of the architecture (Zuo *et al.,* 2008). Method (b) could require a slight modification in the architectures because of the password. However, the password represents another layer of security to biometric cryptosystems.

A. Design and Security Analysis of Proposed System.

In this section, we present the design of the proposed bimodal biometric cryptosystem. The proposed architecture is based on simple concepts. The proposed design does not require a speech recognition technique in the case of the speech signal or fiducial points (landmarks on the ECG complex) detection in the case of the ECG signal. The concept is focused on protecting keys using biometric information and a XOR function. The concept is explained using a theoretical example; however, the idea is the same and can be expanded to the case presented in this paper.

Consider a randomly generated key of any length. For this example, suppose k = 1010. Also, suppose two biometric signals, a = 32 and b = 21. Then, assume that after performing an error analysis was concluded that biometric signals from the same individual differ at most in 1 bit. If both differ in more than 1 bit, it may be concluded that those biometric signals do not belong to the same individual thus the key will not be derived correctly. According to this assumptions, a suitable value for designing the Hadamard code is k = 3. In this example, the XOR technique will be tested. A complete example of how the bimodal biometric cryptosystem works is presented as follows:

1. Encode the randomly generated key using Hadamard code. If the key is k = 1010, the encoded key will be: $H(k)$=1010101001010101.
2. Change the magnitude of the biometric signals to a binary representation as follows: a = 0000001100000010 and b = 0000001000000001.
3. Apply the proposed cancelable technique. Given that the XOR technique is tested, the cancelable biometric signal is computed using $a \oplus b$ thus the result will be: c =0000000100000011.
4. Protect the encoded key $H(k)$ with the cancelable biometric signal c obtained in the previous step. This is done by XORing $H(k)$ and c. It is important to state that this XOR operation is part of the proposed architecture and its purpose is to protect the encoded key. The XOR operation in this step is not related to any XOR operation of the proposed cancelable techniques. Then, the protected key will be: $H(k)_{protected} = H(k) \oplus c$ =1010101101010110.

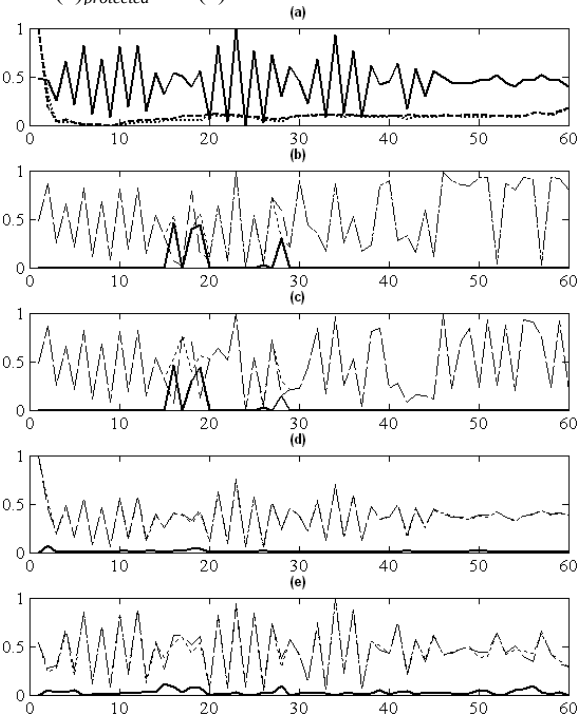

Figure 4: Cancelable techniques in practice. (a) S signal (solid line), $R-R_1$ signal (dashed line), $R-R_2$ signal (dotted line); (b) Shifting technique; (c) Password-dependent shifting technique; (d) XOR technique; (e) Adding technique.

The protected key can be saved in any server or portable device. The protected key will be derived correctly if and only if both biometric signals are legitimate. Then, there are two possible cases: biometric signals are legitimate and biometric signals are not from the same individual who originally protected the key. Assume that a legitimate user provides the two biometric signals, a = 0000001100000010 and b =1000001000000001. Note that the most significant bit of b is different to the expected bit. The change of bits originally expected is due mainly to noise or artifacts. However, Hadamard code is able to correct 1 bit out of 16 in this example, the architecture should be able to recover from this error. To deduce the original key, the inverse process takes place as follows:

1. Apply the proposed cancelable technique. Given we are using the XOR technique, the cancelable biometric signal is computed using $a \oplus b$ thus the result will be: c' =1000000100000011.

2. Unprotect the $H(k)_{protected}$. This is done as follows: $H(k)' = H(k)_{protected} \oplus c'$. The result of this operation will be: $H(k)' = 0010101001010101$. If the unprotected key $H(k)'$ is compared with the original encoded key $H(k)$, it is possible to determine that both vector only differs in the most significant bit.
3. Decode the encoded key using Hadamard code to obtain the original k. The result will be $k = 1010$. The deduced key is equal to the original key, and then it can be released to the user.

If the biometric signals are not from the same user who originally protected the key, there will be more errors that expected, the Hadamard code will not be able to recover from these errors thus the key will not be deduced correctly. This example showed how the proposed architecture works but it also shows how important is to analyze the error characteristics of the biometric signals to design correctly the Hadamard code. A correct design will be able to correct the errors and derive correctly the key for a legitimate user but the code will be unable to correct error if the individual presents not legitimate biometric signals. The use of an error correction technique in this proposed bimodal biometric cryptosystem helps to break the fuzziness of the biometrics and the exactitude required by cryptographic. Also, the complexity of the biometric cryptosystem remains low. This is particularly useful for hardware implementations.

IV. SIMULATION RESULTS

The results reported in this section are divided in three parts, namely, graphical demonstration of the biometric cancelable techniques, performance of the bimodal biometric cryptosystem using the false acceptance rate (FAR) and the false rejection rate (FRR) and distinctness of the proposed biometric cancelable techniques. Note that the simulation results in this section use speech and ECG signals extracted from speech and MIT-BIH Normal Sinus Rhythm Database respectively (Goldberger *et al*., 2000). The selection of the samples is as described in Section 2. Also, note that the key is randomly generated and its length is 480bits.

Figure 4 shows the simulations results of the biometric cancelable techniques. Figure 4(a) shows a S signal (solid line) and two samples of $R-R$ signals ($R-R_1$ dashed and $R-R_2$ dotted lines) that belongs to the same individual. These three biometric signals are used to assess the effectiveness of the proposed biometric cancelable techniques. Figure 4(b) shows the shifting technique. The dashed line is obtained using the $R-R_1$ signal as basis signal while the dotted line is obtained when $R-R_2$ signal is used as basis signal. The solid line represents the error between these two cancelable biometric signals which is clear under the error correction rate that the proposed architecture is able to work under these conditions. This can be seen under samples 15 to 20 and around 30. Figure 4(c) shows the password-dependent shifting technique. Also, two different cancelable biometric signals are obtained using $R-R_1$ and $R-R_2$ signal. The solid line shows the error between these two cancelable biometric signals which is also under the error correction capabilities of the architecture.

Figure 4(d) shows the XOR technique. The error represented by the solid line is very low however the cancelable biometric signals obtained applying this technique are quite similar to the original speech signal. Figure 4(e) shows the adding technique. The solid line shows the error between two cancelable biometric signals of the same individual. The error is higher than the XOR technique but the cancelable biometric signal compared with the previous technique is less similar to the speech signal.

The second part of the results reported in this section is related to the FAR and the FRR metrics. To illustrate the performance of the proposed architecture we have used the MIT-BIH Normal Sinus Rhythm Database (Goldberger *et al*., 2000). The complete test made include all the available records in this database (18 records in total). Each record offers around 60,000 $R-R$ signals of that ECG signal. Our system architecture only uses 60 samples out of 75-120 samples that offer each $R-R$ signal. Then, we have around 780 $R-R$ signals to be possible verified per ECG signal. One $R-R$ signal is randomly selected between the780 possible $R-R$ signals and used to generate the cancelable biometric signal. The rest of the $R-R$ signals are used as the universe to determine the FAR and FRR metrics. Regarding the S signals, a speech database was created for testing purpose. This database contains 20 raw different speech signals from 20 different individuals. Also, one S signal is randomly selected between the 400 possible S signals. The rest of the S signals from the speech database is used to compute the FAR and FRR.

Table 2 summarizes the FAR and FRR metrics obtained for all the four cancelable techniques. The XOR and adding techniques show the best performance regarding the FAR and FRR metrics; however, Figure 4 shows that these cancelable techniques produce cancelable biometric signals quite similar to speech signal. In contrast, the shifting and password-dependent shifting techniques perform poor regarding the metrics compared with the adding and XOR techniques; however, the resultant cancelable biometric signals do not look similar to the speech signal (see Fig. 4).

The third part of the experiments is related to the distinctness of the generated cancelable biometric signals using different cancelable techniques. The distinct ness is tested for each cancelable technique as follows: 30 cancelable biometric signals are generated using information from the same individual and 150 cancelable biometric signals are generated selecting randomly information from different individuals of the available databases; then, 1 out of 30 signals is selected. Using the selected cancelable biometric signal as a base is computed the Hamming distance with the rest of the 149 cancelable biometric signals. It is expected that the 29 cancelable biometric signals from the same individual have a small Hamming distance. On the other hand, the other 150 cancelable biometric signals should show a greater Hamming distance compared with the base.

Table 2: Performance of Proposed Cancelable Techniques

Cancelable Technique	FAR	FRR	Clock cycles
Shifting	0.84%	14.12%	480
Password-dependent	0.18%	13.70%	1080
XOR	0.14%	9.56%	360
Adding	0.30%	11.60%	360

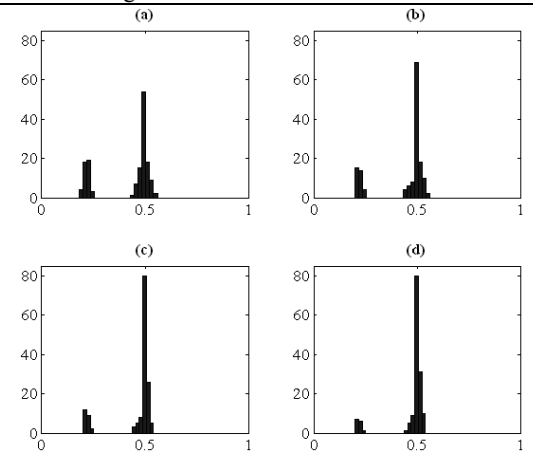

Figure 5: Distinctness Histograms. (a) XOR technique; (b) Adding technique; (c) Password-dependent shifting technique; (d) Shifting technique.

Figure 5 shows the histograms for all the cancelable techniques. The Hamming distance has been normalized. The best performance regarding the distinctness is given by the shifting and the password-dependent shifting techniques because approximately 80 cancelable biometric signals have about half the bits different (see Fig.5(c),(d)). Also, the 30 cancelable biometric signals from the same individual are concentrated around the 0.25. This also shows that these two cancelable techniques have repeatability for the same individual but distinctiveness for different individuals. This data also matches with the error characteristics presented before. Adding and XOR techniques have a poor performance as expected after analyzing the data from Fig. 4 where it was concluded that the two techniques generate quite similar cancelable biometrics signals compared to the original speech signal.

V. CONCLUSION

In this paper four naive cancelable techniques have been reported. The complexity of the proposed techniques is quite low compared with other more sophisticated techniques (see e.g. Garcia-Baleon *et al*., 2009a; Garcia-Baleon and Alarcon-Aquino, 2009; Zho *et al*., 2008). However, the proposed techniques also offer a notable distinctiveness between the generated cancelable biometric signals. Moreover, a simple bimodal biometric cryptosystem is presented to show the application of the cancelable techniques. The cancelable techniques are general and can be used with any type of biometrics signals, not only ECG and speech.

Adding and XOR techniques perform very well regarding the FAR and the FRR metrics however the distinctiveness is poor. In contrast, shifting and password-dependent shifting techniques perform poorly regarding the performance metrics however the generated cancelable biometric signals show a high degree of distinctiveness. Also, the computational cost is important due to the fact that cancelable techniques are usually implemented in hardware. Then, adding and XOR techniques are easily implemented compared with shifting and password-dependent shifting. Note that the four cancelable techniques do not require a high computational capacity. Thus, if there is a cryptosystem with low hardware resources and the metrics are quite important, it is recommended the adding or XOR technique. But if a extra layer of security is required and the metrics are not so determinant, a password-dependent shifting implementation is suggested.

The shifting technique is recommended when the biometrics signals are in more danger of being stolen due to the fact that this technique performs very well regarding the distinctiveness. However, the metric will affect the overall performance of the bimodal biometric cryptosystem.

The biometrically protected random-key is 480-bits length. This key length is good enough to work with most of the well-known cryptographic algorithms. A successful recovering of the key depends on the legitimacy of the biometrics signals provided by the individual who requires the verification. The error correction layer and the wavelet analysis performed over the biometric signals helped to improve the performance metrics.

REFERENCES

Alarcon-Aquino, V. and J.A. Barria, "Change Detection in Time Series Using the Maximal Overlap Discrete Wavelet Transform," *Latin American Applied Research*, **39**, 145-152 (2009)

Chakravarty, I., B.E. Reddy and V. Balaram, "Cancelable Biometrics -A Survey," *International Journal of Computer Science and Information Security,* **19**, 186-195 (2011).

Chouakri, S.A., F. Bereksi-Reguig, S. Ahmaidi and O. Fokapu, "Wavelet denoising of the electrocardiogram signal based on the corrupted noise estimation," *Computers in Cardiology*, **32**, 1021-1024 (2005).

Clancy, T.C., N. Kiyavash and D.J. Lin, "Secure smart card-based fingerprint authentication," *ACM SIGMM Workshop of Biometrics Methods and Application* (2003).

Covell, M. and S. Baluja, "Known-Audio Detection using Waveprint: Spectrogram Fingerprinting byWavelet Hashing," IEEE International Conference on Acoustics, Speech and Signal Processing, **1**, I237-I240 (2007a).

Covell, M. and S. Baluja, "Audio Fingerprinting: Combining Computer Vision and Data Stream Processing," IEEE International Conference on Acoustics, Speech and Signal Processing, **2**, II213-II216 (2007b).

Daugman, J., *Combining Multiple Biometrics*, TheComputer Laboratory, Cambridge University (2009).

Davida, G.I., Y. Frankel and B.J. Matt, "On enabling secure applications through off-line biometric identification," *IEEE Symposium on Security and Privacy*, Los Alamitos, CA, USA, 148-157 (1998).

Gaddam, S.V.K. and M. Lal, "Efficient Cancellable Biometric Key Generation for Cryptography," International Journal of Network Security, **11**, 61-69 (2010).

Garcia-Baleon, H.A. and V. Alarcon-Aquino, "Cryptographic Key Generation from Biometric Data Using Wavelets," *IEEE Electronics, Robotics and Automotive Mechanics Conference*, Mexico (2009).

Garcia-Baleon, H.A., V. Alarcon-Aquino and O. Starostenko, "A Wavelet-Based 128 bit Key Generator Using Electrocardiogram Signals," *IEEE International Midwest Symposium on Circuits and Systems*, Mexico (2009a).

Garcia-Baleon, H.A., V. Alarcon-Aquino, O. Starostenko and J.F. Ramirez-Cruz, "Bimodal Biometric System for Cryptographic Key Generation Using Wavelet Transforms," *IEEE Mexican International Conference on Computer Science*, 185-196 (2009b).

Goh, A. and D.C.L. Ngo, "Computation of cryptographic keys from face biometrics," *Communications and Multimedia Security. Advanced Techniques for Network and Data Protection,* Lecture Notes in Computer Science, **2828**, 1-12 (2003).

Goldberger, A.L., L.A.N. Amaral and L. Glass, "PhysioBank, PhysioToolkit, and PhysioNet: Components of a New Research Resource for Complex Physiologic Signals, Circulation," **101**, e215-e220 (2002).

Hao, F. and C.W. Chan, "Private key generation from on-line handwritten signatures," *Information Management and Computer Society*, **10**, 159-164 (2002).

Hao, F., A. Ross and J. Daugman, *Combining Cryptography with Biometrics Effectively*, Computer Laboratory, University of Cambridge, Technical Report Number 640, UCAMCL-TR-640, July (2005).

Israel, S.A., J.M. Irvine, A. Cheng, M.D. Wiederhold and B.K. Wiederhold, "ECG to identify individuals," *Pattern Recognition,* **38**, 133-142 (2005).

Juels, A. and M. Wattenberg, "A fuzzy commitment scheme," *ACM Conference on Computer and Communications Security* (1999).

Kabatiansky, G., E. Krouk and S. Semenov, *Error Correcting Coding and Security for Data Networks: Analysis of the Superchannel Concept*, John Wiley and Sons Ltd. (2005).

Ktata, S., K. Ouni and N. Ellouze, "A Novel Compression Algorithm for Electrocardiogram Signals based on Wavelet Transform and SPIHT," *International Journal of Signal Processing*, **5,** 253-258 (2009).

Maiorana, E., P. Campisi, J. Fierrez, J. Ortega-Garcia and A. Neri, "Cancelable Templates for Sequence-Based Biometrics with Application to On-line Signature Recognition," *IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems andHumans*, **40**, 525-538 (2010)

Massoud, M., *Hadamard Codes, Coding Theory*, USA (2010).

Moon-Todd, K., *Error Correction Coding, Mathematical Methods and Algorithms*, John Wiley and Sons Ltd. (2005).

Morelos-Zaragoza, R.H., *The Art of Error Correcting Coding*, Second Edition, John Wiley and Sons Ltd. (2006).

Ouda, O., N. Tsumura and T. Nakaguchi, "On the Security of Bioencoding Based Cancelable Biometrics," *IEICE Transactions on Information and Systems*, **E94.D**, 1768-1777 (2011).

Ratha, N.K., J.H. Connell and R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, **40,** 614-634 (2001).

Ratha, N.K., S. Chikkerur, J.H. Connell and R.M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Analysis Mach. Intell*., **29**, 561-572 (2007).

Rathgeb, C and A. Uhl, "A Survey on Biometric Cryptosystems and Cancelable Biometrics," *Eurasip Journal on Information Security*, **3,** 1-25 (2011).

Singh, Y.N. and P. Gupta, "ECG to Individual Identification," *2nd IEEE International Conference on Biometrics: Theory, Applications and Systems*, 1-8 (2008).

Walker, J.S., *A Primer on Wavelets and their Scientific Applications*, Second Edition, Chapman and Hall/CRC Press (2008).

Wubbeler, G., M. Stavridis, D. Kreiseler, R. Bousseljot and C. Elster, "Verification of humans using the electrocardiogram," *Pattern Recognition Letters,* **28**, 1172-1175 (2007).

Ya-Ting, T., S. Tsu-Wang, K. Tung-Fu and L. Tsung-Hsing, "The Morphology of the Electrocardiogram for Evaluating ECG Biometrics," *9th International Conference on e-Health Networking, Application and Services*, 233-235 (2007).

Yarman, B.S., H. Gurkan, U. Guz and B. Ayun, "A Novel Method to represent ECG Signals via predefined Personalized Signature and Envelope Functions," *International Symposium on Circuits and Systems*, **4** (2004).

Zuo, J., N.K. Ratha and J.H. Connell, "Cancelable Iris Biometric," IEEE International Conference on Pattern Recognition, Florida, USA (2008).

Received: July 8, 2012
Accepted: February 8, 2013
Recommended by Subject Editor: José Guivant