A CONCATENATED CODING SCHEME FOR BIOMETRIC TEMPLATE PROTECTION

Xiaoying Shao, Haiyun Xu, Raymond N.J. Veldhuis and Cornelis H. Slump

University of Twente, Enschede, The Netherlands

ABSTRACT

Cryptography may mitigate the privacy problem in biometric recognition systems. However, cryptography technologies lack error-tolerance and biometric samples cannot be reproduced exactly, rising the robustness problem. The biometric template protection system needs a good feature extraction algorithm to be a good classifier. But, an even effective feature extractor can give a very low-quality biometric channel (i.e. high Bit Error Rate (BER)). Using the Spectral Minutiae method to identify fingerprints is one of the examples, which gives a BER of $40 \sim 50\%$ to most of the matching channels. Therefore, we propose a concatenated coding scheme based on erasure codes to achieve a robust and secure biometric recognition system. The key idea is to transmit more packets than needed for decoding and allow the erasure-encoded packet suffering high BER to be discarded. The erasure decoder can reconstruct the secret key by collecting enough surviving packets. By applying the spectral minutiae method in the FVC2000-DB2 fingerprint database, the unprotected system achieves an EER of 3.7% and our proposed coding scheme reaches an EER of 4.6% with a 798-bit secret key.

1. INTRODUCTION

Biometrics refers to technologies that measure and analyze personal features (e.g. fingerprints, voice, iris) for authenticating individuals. Because of the uniqueness, biometric characteristics may contain sensitive personal information which cannot be changed like a password. Once compromised, biometric templates are compromised forever[1]. Hence, cryptography technologies are often adopted in many biometric recognition systems [2]. The basic idea is to use a secret key to protect biometric templates. To identify whether a person has his/her biometric data in the central database, this secret key has to be recovered without any error. In other words, the cryptography approach lacks error-tolerance. However, biometric features can not be exactly reproducible. Therefore, Error Correction Codes (ECCs) have to be employed together with cryptography to achieve a secure and robust biometric recognition system [2].

The biometric recognition system based on the helper data scheme is equivalent to a communication system, as shown in Fig.1. The secret key is first encoded by an ECC then transmitted over the biometric channel defined as $\mathbf{b} \bigoplus \mathbf{b}'$, where

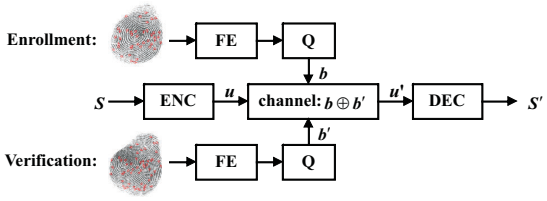

Fig. 1. The equivalent communication system model for biometric recognition systems based on the helper data scheme [3]. (*S* - the secret key, FE - Feature Extraction, Q - Quantization, ENC - Encoder, DEC - Decoder).

$\mathbf{b}$ and $\mathbf{b}'$ are the biometric template bits stream during the enrollment phase and the verification phase, respectively. As seen in Fig.1, the biometric channel is determined by the Feature Extraction (FE) algorithm that is used to authenticate individuals, which directly affects the design of ECC. An effective FE algorithm enables the biometric recognition system to be a good classifier, but it can give a low-quality biometric channel (i.e. high Bit Error Rate (BER) [1]). Spectral Minutiae (SM) [4] is one of the examples. With SM, most of the matching channels[2] have a BER of 40$\sim$50% [3]. However, the error correcting capability of any binary ECC is upper-bounded to $\frac{2^L}{4(2^L-1)}$, where L is the number of source bits (i.e. the length of secret key in this paper) [5]. When $L \geq 8$, ECC can maximum reduce a BER of around 25% to 0. A 8-bit secret key is so short that it can be figured out easily by an attacker.

In [3], we propose a 3-layer coding scheme based on erasure codes for the SM-based biometric recognition system. With this coding scheme, the secret key is first divided into K packets. Each packet is considered as a unit and they are encoded by an erasure code. The erasure decoder can reconstruct the original secret key once it has *enough error-free* erasure-encoded packets. It does not matter which packet is received. However, the biometric channel is not an erasure channel but a noisy channel. By applying an ECC in each

[1]The Bit Error Rate (BER) of the biometric channel refers to the fractional Hamming distance between $\mathbf{b}$ and $\mathbf{b}'$, which is used to quantify the difference between two biometric template bits streams.

[2]The matching channel is generated by errors $\mathbf{b} \oplus \mathbf{b}'$, where $\mathbf{b}$ and $\mathbf{b}'$ are biometric template bit streams and come from the same person. The non-matching channel is generated by errors $\mathbf{b} \oplus \mathbf{b}'$, where $\mathbf{b}$ and $\mathbf{b}'$ come from different persons.

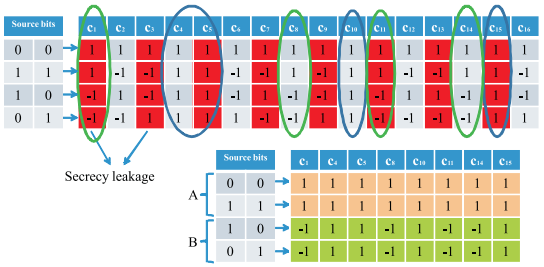

Fig. 2. The risk of zero insertion. In [3], the EDC encoder together with the ECC encoder change the length of a packet from 2 bits to 16 bits. If zeros are inserted in the red positions like [3], the packet can be figured out easily. Still with 50% zero insertion, if we insert zeros in $[c_1, c_4, c_5, c_8, c_{10}, c_{11}, c_{14}, c_{15}]$, the attacker can only guess whether the packet belongs to *Type A* or *Type B*.

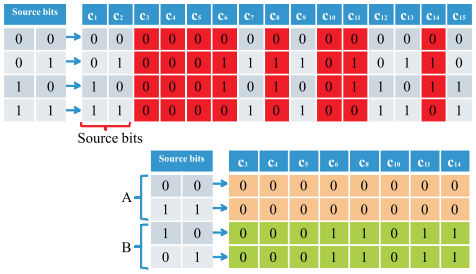

Fig. 3. The zero insertion scheme for the (5,15) BCH code.

packet (after the erasure encoder), the noisy biometric channel can behave like an erasure channel. To make sure that the erasure decoder receives the *error-free* packets, Error Detection Code (EDC) is used to detect the un-detected errors from the ECC decoding. In [3], the (5,16) Hadamard Code is used as ECC, which can correct 18.75% errors [6]. However, the SM-based biometric channel has a BER of $40 \sim 50\%$. To compensate for the limited error correcting ability of the Hadamard code, zero insertion is necessary. In [3], we insert a '0' between two adjacent bits in $\mathbf{b}$ and $\mathbf{b}'$ which is not secure. As you can see in Fig.2, $[c_1, c_3]$ already can help the attacker to distinguish each erasure-encoded packet. In such a case, the secret key can be compromised easily.

In this paper, we propose another concatenated coding scheme for biometric template protection systems, which is the improved version of the coding scheme in [3]. The main differences between these two coding schemes are the zero insertion and the error detection. Zero insertion contains a risk but it does not imply insecurity. Fig. 2 shows the secrecy leakage in [3] due to the zero insertion scheme. Here, we define an encoded packet (i.e. codeword) in [3] as $[c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8, c_9, c_{10}, c_{11}, c_{12}, c_{13}, c_{14}, c_{15}, c_{16}]$. As seen in Fig.2, all codewords have the same information in $[c_4, c_5, c_{10}, c_{15}]$ (i.e. [1,1,1,1]). Equivalently, inserting zeros in those positions will not cause any information leakage. Besides, columns of $[c_1, c_8, c_{11}, c_{14}]$ are the same (i.e. [1,1,-1,-1]). If we insert zeros in those columns, we only will leak 1-bit information of each packet. Thus, if zeros are inserted in $[c_1, c_4, c_5, c_8, c_{10}, c_{11}, c_{14}, c_{15}]$, the attacker can only classify all the packets into two types: *Type A* and *Type B*. Each type contains two elements. To figure out the secret key, the attacker needs to guess 2^N times, where N is the number of packets required in the erasure decoder. However, the EDC scheme in [3] can not work together with this zero insertion scheme. Because if 4 bits or more in $[c_2, c_3, c_6, c_7, c_9, c_{12}, c_{13}, c_{16}]$ are in error (i.e. BER $\geq 50\%$ that often happens in the SM-based biometric channel), those errors will change the transmitted codeword into another codeword which can never be found out by any EDC scheme. Therefore, a robust detection scheme is proposed in this paper which will be explained in the coming section.

2. THE PROPOSED CODING SCHEME

The proposed coding scheme has the same principle as the one in [3], which is inspired by the fact that the Packet Error Rate (PER) is proportional to the BER. Assume that the encoded key $\mathbf{u}$ in Fig.1 has $\mathcal{N}$ bits which consists of N_t packets. Each packet has n bits. We define that a packet is received correctly if t bits or less are in error. Each packet is encoded by an ECC and an EDC. If the received packet has t bits in error or less, the ECC can recover it. EDC is used to detect any undetected error from the ECC decoding and identify whether the packet is error free. Only error-free packets survives. With the assistance of erasure codes, the system can reconstruct the secret key by only using the surviving packets.

It is a concatenated coding scheme based on erasure codes, ECC and EDC. In this paper, we choose *fountain codes* [7] as erasure codes. Just like a metaphorical fountain, the fountain encoder produces a stream of fountain-encoded packets. Anyone who wishes to receive the encoded file holds a bucket under the fountain and collects enough packets to recover the original data [7]. It does not matter which packet is received, only a minimum amount of packets have to be received correctly. With the help of fountain codes, each transmitted packet becomes independent with respect to each other. In such a case, we are allowed to discard some packets with more than t errors.

ECC can help us to correct some error packets if they have $\leq t$ errors. In this paper, we choose *the (5,15) BCH code* [8] which corrects a maximum of 3 error bits (i.e. a BER of 20%). However, the SM-based biometric channel often has a BER of 40% or more. Thus, zero insertion is required. To insert 50% zeros without leaking all the information, each codeword can only have 2 source bits instead of 5 bits. Before the BCH encoding, we attach 3 '0's after 2 source bits. In such a case, we can insert around 53% zeros in each codeword (i.e. packet) as shown in Fig.3. From this figure, we can see that

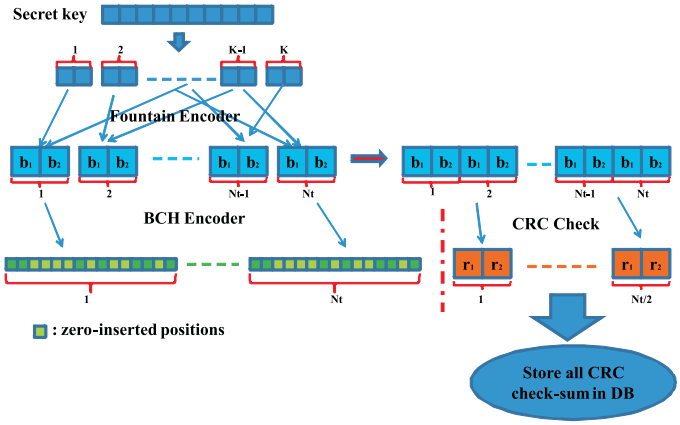

Fig. 4. The proposed encoder.

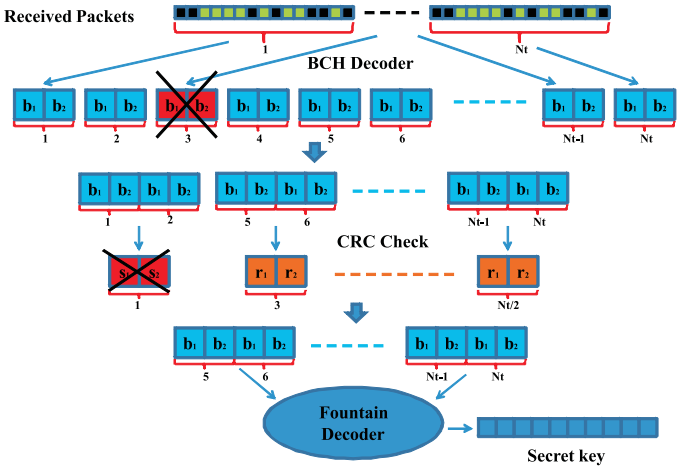

Fig. 5. The proposed decoder.

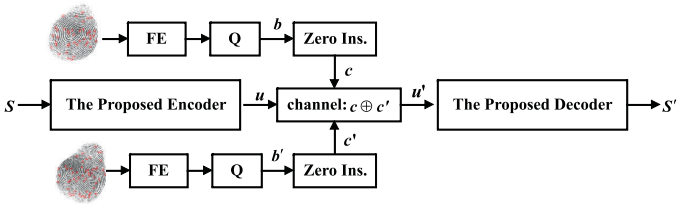

Fig. 6. The proposed fingerprint recognition system.

this zero insertion scheme divides all the packets into 2 types:

$$A = \{[0\,0], [1\,1]\}$$
$$B = \{[0\,1], [1\,0]\}$$

Each type contains two elements. With the knowledge of this zero insertion scheme, the attacker can figure out the secret key by guessing 2^N times, where N is the number of packets required by the fountain decoder. Only if N is large enough, the biometric recognition system can not be compromised easily.

Unfortunately, the chosen BCH code and the proposed zero insertion scheme can not completely make the noisy biometric channel behave like an erasure channel. In other words, there are un-detected errors from the BCH decoding. To solve this problem, we connect two adjacent packets (before the BCH encoding) together and encode them by the Cyclic Redundancy Check (CRC) [8]. CRC is a type of error detection codes. Here, we refer these two packets to brother packets and use 2-bit CRC to check whether these brother packets are error-free. If the CRC decoding fails, both packets will be discarded. We store all CRC checksums in the central database. Because of the multiple-to-one characteristics of CRC, the attacker can not distinguish the packet uniquely with the knowledge of the CRC checksum.

The encoding process of our coding scheme is performed in the following order as shown in Fig.4. Assume that the secret key has $\mathcal{K}$ bits and is divided into K packets. Each packet has 2 bits, so $\mathcal{K} = 2K$. First, a fountain-encoded packet is created. Then, it is attached by three '0's then encoded by the (5,15) BCH code. In total, N_t packets are transmitted over the biometric channel. Meanwhile, two adjacent fountain-encoded packets are connected together then is encoded by 2-bit CRC. The CRC generator used in this paper is $x^2 + x + 1$. All CRC checksums are stored in the central database.

The decoding process is depicted in Fig.5. Each received packet first passes the BCH decoder. Only if both brother packets succeed in the BCH decoding, they can go to the next stage, namely, the CRC decoding. Otherwise, they will be discarded. The CRC is used to identify any errors undetected by the BCH code. If the CRC decoder detects an error, both brother packets will be discarded as well. Once the fountain decoder gets N surviving packets, it starts to recover the original secret key. The secret key can only be recovered successfully, if $N_r \geq N$ where N_r is the total number of surviving packets. Therefore, we can use N as a threshold to classify the matching channel and the non-matching channel.

3. EXPERIMENTAL RESULTS

In this section, we analyze the performance of our proposed coding scheme by testing it in the FVC2000-DB2 fingerprint database [9]. Here, we compare two systems. The first system, *system A*, is a SM-based fingerprint recognition system without using any ECC. Although this system can be compromised easily, the fractional Hamming distance between $\mathbf{b}$ and $\mathbf{b}'$ (i.e. BER) offers the best performance in terms of Force Match Rate (FMR) and Force Non-Match Rate (FNMR). The second system, *System B*, is a SM-based fingerprint recognition system based on the proposed coding scheme as shown in Fig. 6. Unlike System A, the robustness and the security of System B are enabled by the proposed coding scheme depicted in Section 2. Our coding scheme makes use of the

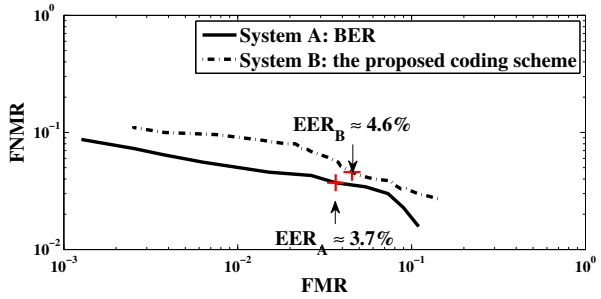

Fig. 7. Experiment results: ROC comparison between System A without ECC and System B based on the proposed coding scheme.

PER, which is proportional to the BER of the channel. Therefore, we expect that it has a similar performance to System A. This will be investigated in this section.

In the FVC2000-DB2 fingerprint database [9], we use the samples from finger ID 1 to 100. Each identity contributes 8 samples. For each sample, we use the *Complex Spectral Minutiae Representation* method [4] to get a string of 10240 spectral bits (i.e. $\mathbf{b}$). Here, we do not incorporate the masks that are proposed in [4]. With the zero insertion, the number of channel bits (i.e. $\mathbf{c} \bigoplus \mathbf{c}'$ in Fig.6) is increased to 21930. As each packet has 15 bits after the BCH encoding, we have $N_t = 1462$ packets to be transmitted in the biometric channel.

Only both brother packets succeeding in the BCH and CRC decoding go to the fountain decoder. In this paper, we use *the Luby-Transform (LT) codes* [7] to reconstruct the secret key. LT codes are a kind of fountain codes. The LT decoder requires $N = (1 + \varepsilon)K$ packets to recover the source file, where ε is the percentage of extra packets [7]. If the LT codes are decoded by combining the message-passing algorithm and Gaussian elimination, we can have $\varepsilon = 0.05$ for $K \geq 400$ [10]. As mentioned earlier, N is the parameter to classify the matching channel and the non-matching channel. N can be obtained according to the required FMR and FNMR. Once N is obtained, K can be derived. Correspondingly, the length of the secret key (i.e. $\mathcal{K}$) can be calculated.

Fig.7 shows the Receiver Operating Characteristic (ROC) curves for both systems. System A achieves an EER of around 3.7% (i.e. FMR = 3.66%, FNMR = 3.71%) by setting $\mathrm{BER} = 48.6\%$ to classify the matching channel and the non-matching channel; while System B reaches an EER of around 4.6% (i.e. FMR = 4.55%, FNMR = 4.57%) by using $N = 418$ to do such classification. That means that the attacker has to guess 2^{418} times to compromise the secret key. With the EER of 4.6%, we have $K = 398$. Equivalently, the proposed coding scheme allows a 796-bit secret key in the FVC2000-DB2 database.

4. CONCLUSIONS

In this paper, we propose a concatenated coding scheme based on erasure codes for biometric template protection. Like the coding scheme in [3], it is inspired by the fact that the PER is proportional to the BER. Their main differences are the zero insertion and the error detection. The zero insertion scheme in [3] leaks all the information of each packet which makes the whole coding scheme unsecure. However, the new zero insertion scheme proposed in this paper only divides the packets into two types instead of distinguishing each packet clearly. To make sure that the packets going to the erasure decoder are error-free, we connect two adjacent packets together and encode them by 2-bit CRC. Due to the multiple-to-one nature of CRC, the attacker can not figure out the erasure-encoded packet uniquely with the knowledge of CRC checksums. By applying the spectral minutiae method in the FVC2000-DB2, the proposed coding scheme achieves an EER of 4.6% and allows a 798-bit secret key.

5. REFERENCES

[1] B. Schneier, "Inside risks: the uses and abuses of biometrics," *Commu. of the ACM*, vol. 42, p. 136, 1999.

[2] A. Juels, et al., "A fuzzy commitment scheme," in *the 6th ACM conference on Computer and Comm. security*, 1999, pp. 28–36.

[3] X. Shao, et al., "A 3-layer coding scheme for biometry template protection based on spectral minutiae," in *ICASSP*, 2011, pp. 1948 – 1951.

[4] H. Xu, et al., "Binary representations of fingerprint spectral minutiae features," in *ICPR*, 2010.

[5] R.G. Gallager, *Information theory and reliable communication*. Wiley, 1968.

[6] K. Horadam, *Hadamard Matrices and Their Applications*. Princeton Press, 2007.

[7] D. MacKay, "Fountain Codes," *IEE Communications*, vol. 152, no. 6, pp. 1062–1068, 2005.

[8] R. Blahut, *Theory and Practice of Error Control Codes*. Addison-Wesley, 1983.

[9] D. Maio, et al., "FVC2000: Fingerprint verification competition," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 24, no. 3, pp. 402–412, 2002.

[10] X. Shao, et al., "An Opportunistic Error Correction Layer for OFDM Systems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 1–10, 2009.