A 3-Layer Coding Scheme for Biometry Template Protection based on Spectral Minutiae

Xiaoying Shao, Haiyun Xu, Raymond N.J. Veldhuis and Cornelis H. Slump
University of Twente, Enschede, The Netherlands
E-mail: {x.shao, h.xu, r.n.j.veldhuis and c.h.slump}@ewi.utwente.nl

***Abstract*—Spectral Minutiae (SM) representation enables the combination of minutiae-based fingerprint recognition systems with template protection schemes based on fuzzy commitment, but it requires error-correcting codes that can handle high bit error rates (i.e. above 40%). In this paper, we propose a 3-Layer coding scheme based on erasure codes for the SM-based biometric recognition system. Our approach is inspired by the fact that the Packet Error Rate (PER) is proportional to the Bit Error Rate (BER). Each packet is encoded by an Error Detection Code (EDC) and an Error Correction Code (ECC). The packet can only survive if it successfully passes the ECC and EDC decoder. With the erasure code, the system can reconstruct the secret key by only using the survived packets. By applying SM to the FVC2000-DB2 fingerprint database, the unprotected system achieves an EER of around 6% while our proposed coding scheme reaches an EER of approximately 6.5% with a 1032-bit secret key.**

I. Introduction

Biometrics is about measuring unique personal features, such as a person's voice, fingerprint, face or iris. Unlike passwords, biometric characteristics cannot be changed easily and may contain sensitive personal information about people. Once compromised, biometric templates are compromised forever and cannot be replaced [1]. In order to deal with these issues, cryptography technology is applied in many biometric recognition systems [2]. The basic idea is to use a secret key to encrypt biometric templates. To identify whether a person has his/her biometric templates in the central database, this secret key has to be recovered without any error. However, the cryptography approach lacks error-tolerance, and unfortunately it is not possible to exactly reproduce biometric samples due to the variability in the user interaction. Therefore, Error Correction Codes (ECCs) have to be adopted together with cryptography to achieve a secure and robust biometric recognition system [3], [4].

The performance of biometric template protection systems depends on the Feature Extraction (FE) and ECCs, as shown in Fig. 1. From this figure, we can see that FE determines the biometric channel, which directly affects the design of ECCs. The biometric channel is often characterized by the fractional Hamming distance that is used to quantify the difference between two fingerprint patterns. Here, we define the fractional Hamming distance between $\mathbf{b}$ and $\mathbf{b}'$ as the Bit Error Rate (BER) of the biometric channel. A low BER enables the use of a high-rate ECC and thus the use of a long secret key in biometric template protection systems.

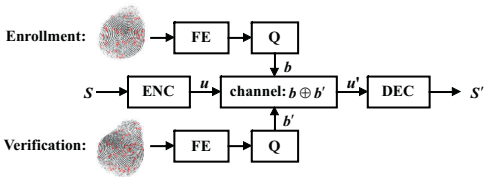

Fig. 1. The equivalent communication system model for biometric recognition systems. (S - the secret key, FE - Feature Extraction, Q - Quantization, ENC - Encoder, DEC - Decoder). The encoded key $\mathbf{u}$ is transmitted over the biometric channel defined as $\mathbf{b} \oplus \mathbf{b}'$, where $\mathbf{b}$ is the biometric template bits stream during the enrollment phase and $\mathbf{b}'$ is the biometric template bits stream during the verification phase.

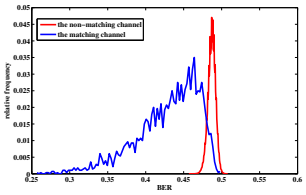

Fig. 2. Histogram of BER of the matching channel and the non-matching channel by applying spectral minutiae in the FVC2000-DB2 fingerprint database. This histogram is based on 100 different finger identities and each identity has 8 samples. Biometric channels consist of the matching channel and the non-matching channel. 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.

The reliable component scheme proposed in [4] aims at combining fingerprint recognition with template protection. For the FE part, this system uses the fingerprint's directional field and the Gabor filter responses as features. For the ECC part, the system uses the (511,40,95) BCH code that can handle a BER of around 18.6%, which means that this system realizes most of the biometric channels with a BER $\leq 18.6\%$. The recognition performance of an unprotected biometric system depends on the False Match Rate (FMR) and the False Non-Match Rate (FNMR), which are functions of the system threshold t. For a traditional biometric system, the threshold t can be set at a value depending on the system performance requirement. However, when combining a biometric system with template protection schemes based on fuzzy commitment schemes, the system performance depends on the error correcting capability of ECCs.

Nowadays, most fingerprint recognition systems are based

on minutiae comparison. Minutiae are the endpoints and bifurcations of fingerprint ridges. They are known to remain unchanged over an individual's lifetime and allow a very discriminative classification of fingerprints [5]. However, minutiae sets are unordered collections of points, suffering from various deformations such as translation, rotation and scaling. The binarization of SM leads to a good binary classifier, but is characterized by a higher BER. This differs from other template protection systems, such as [4]. With SM, most of matching channels have a BER of 40%∼50% as shown in Fig. 2. Thus, the practical SM-based biometric recognition system does need an ECC scheme that can cope with a BER $> 40\%$. Besides, the designed ECC should allow for a secret key with enough length (e.g. around 100 bits) to guarantee a sufficient level of template protection. Till now, no practical coding scheme has been proposed to match the requirements of SM. In this paper, we propose a novel 3-Layer coding scheme based on erasure codes for SM-based recognition systems which allows a long enough secret key.

The idea of the 3-Layer coding scheme 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 and we divide $\mathbf{u}$ into N_t packets and each packet has n bits. We define that a packet is received correctly if less than σ bits are in error. In a practical biometric system, the BER in the matching channel is, on average, lower than in the non-matching channel as shown in Fig. 2. That also applies to the PER, meaning that using the PER to classify the matching channel and the non-matching channel should achieve a similar value of FMR and FNMR as the best case of using BER (i.e. the Hamming distance between biometric template bit streams). Therefore, we propose to apply an ECC and an Error Detection Code (EDC) on each packet. If the received packet has fewer than σ error bits, 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 survive. With the assistance of erasure codes, the system can reconstruct the secret key by only using the surviving packets.

The paper is organized as follows. In Section II, we present the proposed 3-Layer coding scheme in details and explain how to adapt it to cope with a $\mathrm{BER} > 40\%$. By applying the 3-layer coding scheme in the SM-based fingerprint recognition system, we describe its corresponding system model in Section III. We investigate its performance in the FVC2000-DB2 fingerprint database. Finally, the experiment results are analyzed. The paper ends with a discussion of the results.

II. The 3-Layer Coding Scheme

The 3-Layer coding scheme can be applied in any biometric recognition system with a high BER (i.e. >25%) channel. It is based on erasure codes and any erasure code can be applied in it. Fountain codes are erasure codes that we choose to apply in our scheme [6]. Just like a metaphorical fountain, the encoder of a fountain coder produces a stream of 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 [6]. 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 suffering from high BER.

Assume that a secret key has $\mathcal{K}$ bits and is divided into K packets with a length of k bits (i.e. $\mathcal{K} = K \cdot k$). By treating each packet as a unit, they are encoded by a fountain code. The transmitter generates N_t fountain-encoded packets with a length of k bits. Then, each packet is encoded by an EDC and an ECC to transform the noisy biometric channel into an erasure channel. After the EDC and ECC encoding, each packet has n bits. So, the encoded key $\mathbf{u}$ has a length of $\mathcal{N} = N_t \cdot n$.

In the 3-Layer coding scheme, we require an ECC with a high error correction ability but a short codeword length. BCH and Hadamard [7] codes are two suitable options. In this paper, we choose the Hadamard code due to its relatively low encoding and decoding complexity. However, Hadamard codes can only handle a channel with $\mathrm{BER} < 25\%$ [7]. That limits the performance of the 3-Layer coding scheme in a channel with $\mathrm{BER} \geq 25\%$. To combat this limitation, we improve the biometric channel condition artificially by inserting zeros in $\mathbf{b}$ and $\mathbf{b}'$. In this paper, we halve the BER by inserting a '0' between two adjacent bits in $\mathbf{b}$ and $\mathbf{b}'$. Although the performance of Hadamard codes increases with the codeword length n, the code rate decreases with n. Lower code rate leads to a shorter secret key and thus a lower-secure biometric recognition system. To achieve a good balance between the error correction ability and the code rate of Hadamard codes, we choose the (5,16) Hadamard code (i.e. $n = 16$) in this paper. The minimum distance in the (5,16) Hadamard code is 8. Because the zero insertion ensures that half of a packet is correctly received, the effective minimum distance of the Hadamard code in our case is 4. In such case, some remaining errors might never be found if more than 4 bits in a packet are flipped. To avoid this, we discard the packet if the minimum Hamming distance $\mathcal{D}_{min}$ between the received packet and the 16 Hadamard codewords is larger than 4. However, the undetected errors may still exist in the Hadamard decoded packet. Therefore, we need the EDC to identify any undetected error bits. In this paper, we use the repetition code and 1-bit Cyclic Redundancy Check (CRC) for error detection. In this way, each packet contains 2 source bits (i.e. $k = 2$). A packet survives only if it passes the ECC and EDC decoding. With the help of fountain codes, the secret key can be recovered reliably by only using surviving packets.

III. System Model

In this paper, we apply the 3-Layer coding scheme in the SM-based fingerprint recognition system, whose BER is mainly in the range of $40\% \sim 50\%$. The proposed system model is depicted in Fig. 3. In this system, the fingerprints of users are sampled during an enrollment phase, and the

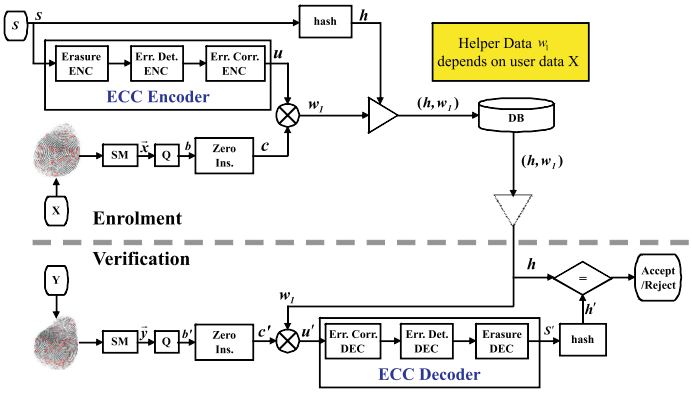

Fig. 3. The proposed SM-based fingerprint recognition system. (SM - Spectral Minutiae.) The secret key S is first divided into K packets with a length of k bits. In the 3-Layer encoder, first source packets are encoded by erasure codes then an EDC and an ECC are applied to each erasure-encoded packet. Equivalent to a communication system, each encoded packet is transmitted over the biometric channel (i.e. $\mathbf{c} \oplus \mathbf{c}'$). In the 3-Layer decoder, each received packet is decoded by the ECC and EDC decoder. The packet will be discarded if it does not pass either the ECC decoding or the EDC decoding. When the erasure decoder collects N packets, it can reconstruct the secret key.

feature bits are stored in a central database. Later, when the user wants to authenticate himself/herself to the system, a fresh measurement of the fingerprint is taken and the same biometric signal processing is done. The 3-Layer decoder can help us to recover the secret key which is matched against the corresponding key. The whole system is equivalent to a communication system involving three parts: the 3-Layer encoder, the biometric channel and the 3-Layer decoder.

A. The 3-Layer Encoder

We have assumed that the secret key has $\mathcal{K}$ bits. The $\mathcal{K}$-bit key is divided into K packets with a length of 2 bits, so $\mathcal{K} = 2K$. At this moment, we do not know K as it depends on the number of packets survived in the biometric channel (i.e. N_r). The Luby Transform (LT[1]) code generates N_t LT-encoded packets. Each LT-encoded packet is the bit-wise sum of a set of randomly selected source packets. The number of selected packets is also random. We define the LT-encoded packet as $\mathbf{s} = [\mathrm{s}_1\ \mathrm{s}_2]$, which is first encoded by the repetition code plus 1-bit CRC. The resulting packet has a format of $[\mathrm{s}_1\ \mathrm{s}_2\ \mathrm{s}_1\ \mathrm{s}_2\ \mathrm{s}_1 \oplus \mathrm{s}_2]$ and is encoded by the (5,16) Hadamard code. Thus, we have $\mathcal{N} = 16N_t$, which is determined by the length of $\mathbf{c}$ in Fig. 3.

B. The Biometric Channel

The objective is to represent a minutiae set as a fixed-length feature vector, that is invariant to translation, rotation and scaling. In this paper, we use the *Complex Spectral Minutiae Representation* (SMC) method proposed in [8]. In SMC, the minutiae location, orientation and quality information is coded into the spectral minutiae features. Further, we apply the *Column-PCA* feature reduction and the *Spectral Bits* method proposed in [8] to generate a binary representation of the spectral minutiae features. The Spectral Bits generates a binary string of 10240 bits. To reduce the BER, we artificially insert zeros in the binary representation, as explained in Section II, which leads to a binary string of 20480 bits (i.e. $\mathcal{N} = 20480$, $N_t = 1280$). It should be noted that in this paper, we do not incorporate the masks that are proposed in [8].

[1]LT codes are a kind of fountain codes [6]

C. The 3-Layer Decoder

At the 3-Layer decoder, each received packet is first decoded by the Hadamard decoder. As mentioned earlier, the packet is discarded if the minimum Hamming distance $\mathcal{D}_{min}$ between the received packet and the 16 Hadamard codewords is larger than 4. Here, we denote the Hadamard-decoded packet as $[\mathrm{s}'_1\ \mathrm{s}'_2\ \mathrm{s}'_3\ \mathrm{s}'_4\ \mathrm{s}'_5]$. The surviving Hadamard-decoded packet will be discarded if it does not satisfy the following constraints: $\mathrm{s}'_1 = \mathrm{s}'_3$, $\mathrm{s}'_2 = \mathrm{s}'_4$ and $\mathrm{s}'_1 \oplus \mathrm{s}'_2 = \mathrm{s}'_5$. Only the packets succeeded in the ECC and EDC decoding go to the LT decoder. We assume that N_r packets survives. The LT decoder can reconstruct the secret key by collecting enough surviving packets. The number of LT-encoded packets N required at the receiver is slightly larger than the number of source packets K [6]:

$$N = (1 + \varepsilon)K \tag{1}$$

where ε is the percentage of extra packets and is called the overhead. To achieve a low ε with small block size, we choose to decode the LT code by using the combination of the message-passing algorithm and Gaussian elimination [9]. In such case, we can have $\varepsilon = 0.03$ for $K \geq 500$. The mathematical principle behind the fountain or erasure decoding is to solve K unknown parameters from N linear equations. If $N_r \geq N$, the secret key can be reconstructed uniquely. However, if $N_r < N$, it is not possible to solve the N_r linear equations with K unknown parameters. Equivalently, the LT decoder fails and thus the 3-Layer coding scheme fails if $N_r < N$. Thus, N is the parameter to classify the matching channel and the non-matching channel. N can be obtained according to the request FMR and FNMR. Once N is obtained, K can be derived by Eq. 1. Correspondingly, the length of the secret key (i.e. $\mathcal{K}$) can be calculated.

IV. Performance Analysis

In this section, 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 FMR and FNMR. The second system, System B, is a SM-based fingerprint recognition system based on the 3-Layer coding scheme shown in Fig. 3. Unlike System A, the robustness and security of System B are enabled by the proposed 3-Layer coding scheme. In System B, the 3-Layer coding scheme is set up by using the parameters in Section III. Our coding approach makes use of the PER, which is proportional to the BER of the channel. Therefore, we expect it has a similar performance to System A. This will be investigated in this section.

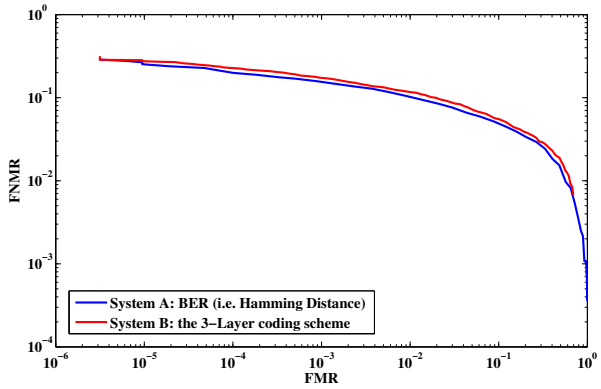

Fig. 4. Experiment results: ROC comparison between System A without ECC (i.e. using Hamming distance) and System B based on the 3-Layer coding scheme.

In our experiment, we use the FVC2000-DB2 fingerprint database [10] to evaluate our scheme. We use the samples from finger ID 1 to 100. Each identity contributes 8 samples. The minutiae sets including the minutiae quality data are extracted by a proprietary method [11]. For the spectral minutiae representation, we use the same parameter setting as in [11].

With the zero insertion, the channel bits doubles. So, we have $\mathcal{N} = 20480$ and $N_t = 1280$. The number of surviving packets N_r can be found out after sending the 1280 encoded packets over each biometric channel. As just explained, the number of packets required in the LT decoder (i.e. N) determines the value of FMR and FNMR by using the 3-Layer coding scheme. Fig. 4 shows the Receiver Operating Characteristic (ROC) curve for both systems. As we can see, the two curves almost overlap. System A achieves an EER of around 6% (i.e. FMR = 6.05% and FNMR = 5.96%) by setting BER = 47.9% to classify the matching channel and the non-matching channel; while System B reaches an EER of around 6.5% (i.e. FMR = 6.45% and FNMR = 6.61%) by choosing $N = 532$ to do such classification. Thus, we have $K = 516$ according to Eq. 1. Correspondingly, the 3-Layer coding scheme can give us a 1032-bit secret key in the FVC2000-DB2 database.

Risks exist in the zero insertion. The biometric template protection may not work by inserting too much zeros. Fig. 2 shows that the BER of the non-matching channels has a range of $46\% \sim 51\%$. Because the (5,16) Hadamard code can deal with a BER of 18.75%, we can not classify the matching channel and the non-matching channel by inserting around 63% zeros in $\mathbf{c}$. Besides, the zero insertion may decrease the security of the whole system, as it leaks half information of $\mathbf{u}$ to the attacker. We assume that the attacker has full knowledge of the 3-Layer coding scheme. If the attacker can recover N or more packets from the helper data $\mathbf{w_1}$, he/she is able to recover the secret key S. In our experiment, we have tested 800 samples. By setting $N = 532$ to achieve an EER of around 6.5%, 0.25% of those samples can be compromised and 99.75% of samples can be stored safely. However, if we set $N = 550$ to do the classification, the attacker can not recover the secret key. In such case, we have FMR = 0.67% and FNMR = 12.46%. There are two solutions to improve the security of the proposed SM-based biometric recognition systems. One is not to use the zero insertion by designing an ECC with much higher error correction ability. In this way, we do not leak any information of $\mathbf{u}$ to the attacker. The other solution is to reduce the BER in the biometric channel by improving the SM algorithm, e.g. applying the multi-sample fusion technique [11]. In this way, we are allowed to have a larger N. The feasibility of these approaches will be investigated in our future work.

V. Conclusions

In this paper, we propose a 3-Layer coding scheme based on erasure codes to show the feasibility of a secure and robust SM-based biometric recognition system. To prove the concept, we use fountain codes as erasure codes, the Hadamard code to protect each packet and the repetition code plus CRC to identify any undetected error from the ECC decoding. To compensate for the limited error correction ability of Hadamard codes, we improve the biometric channel condition artificially by inserting zeros in $\mathbf{b}$ and $\mathbf{b}'$. By testing it in FVC2000-DB2, the proposed system achieves an EER of around 6.5% with a 1032-bit secret key. The zero insertion can decrease the security of the whole system. To avoid this issue, the future research will be focused on designing an ECC which can correct around 40% errors. In such a case, the zero insertion is not necessary. The other solution is to reduce the BER in the biometric channel by improving the SM algorithm. In this way, it is possible to have a larger N to classify the matching channel and the non-matching channel.

References

[1] B. Schneier, "Inside risks: the uses and abuses of biometrics," *Communications of the ACM*, vol. 42, no. 8, p. 136, 1999.

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

[3] A. Juels, et al., "A fuzzy vault scheme," *Designs, Codes and Cryptography*, vol. 38, no. 2, pp. 237–257, 2006.

[4] P. Tuyls, et al., "Practical biometric authentication with template protection." in *AVBPA*, 2005, pp. 436–446.

[5] Maltoni, Davide, et al., *Handbook of Fingerprint Recognition*. Springer Publishing Company, Incorporated, 2009.

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

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

[8] H. Xu, et al., "Binary representations of fingerprint spectral minutiae features," in *20th International Conference on Pattern Recognition (ICPR 2010)*, Turkey, August 2010.

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

[10] D. Maio, et al., "FVC2000: Fingerprint verification competition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 402–412, 2002.

[11] H. Xu, et al., "Binary spectral minutiae representation with multi-sample fusion for fingerprint recognition," in *The 12th ACM Workshop on Multimedia and Security*, Rome, Italy, September 2010.