

A Real Helper Data Scheme

Xiaoying Shao
EEMCS Falcuty
University of Twente
Enschede, The Netherlands
x.shao@utwente.nl

Raymond N.J. Veldhuis
EEMCS Falcuty
University of Twente
Enschede, The Netherlands
r.n.j.veldhuis@utwente.nl

Abstract—The helper data scheme utilizes a secret key to protect biometric templates. The current helper data scheme requires binary feature representations that introduce quantization error and thus reduce the capacity of biometric channels. For spectral-minutiae based fingerprint recognition systems, Shannon theory proves that the current helper data scheme cannot have more than 6 bits. A 6-bit secret key is too short to secure the storage of biometric templates. Therefore, we propose a new helper data scheme without quantization. A basic realization is to convert the real-valued feature vector into a phase vector. By applying the spectral minutiae method in the FVC2000-DB2 fingerprint database, our new helper data scheme together with repetition codes and BCH codes allows at least 76 secret bits.

Keywords—helper data scheme; biometric template protection; secret key.

I. INTRODUCTION

Wide-spread use of biometrics raises security and privacy concerns about biometric technologies. Unique biometric characteristics may contain sensitive personal information and cannot be changed easily. Once compromised, biometric templates are compromised forever [1]. Therefore, template protection techniques are proposed to solve these issues. One of the popular approaches is called the helper data scheme [2] that makes use of cryptographic primitives (e.g. Hash functions) and Error Correcting Codes (ECC). With the helper data scheme, a secret key is used to encrypt biometric templates. To avoid the brute-force attack, the secret key should be long enough (at least 75 bits¹) to secure the storage of biometric templates.

The biometric recognition system based on the current helper data scheme [2] 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 $\vec{b} \oplus \vec{b}'$, where \vec{b} and \vec{b}' are the binary feature vector during the enrollment and the verification phase, respectively. For memoryless biometric sources, biometric channel is a Binary Symmetric Channel (BSC) as depicted in Fig.2 [4]. The error rate of biometric channels is caused by the un-reproducible

biometric samples and determined by Feature Extraction (FE) algorithms that are used to authenticate individuals (see Fig.1), which directly affect the design of ECC. An effective FE algorithm enables biometric recognition system to be a good classifier, but it can give a low-quality biometric channel (i.e. high Bit Error Rate (BER)² or high crossover probability).

Spectral Minutiae (SM) [5] is one of the examples. With SM, an Equal Error Rate (EER) of 3.7% is achieved by setting BER = 48.6% to classify the matching channel and the non-matching channel³ [6]. Correspondingly, we need to design an ECC for a BSC with a crossover probability (p) of 48.6%. According to Shannon Theory [7], the channel capacity (\mathcal{C}) of BSC is defined as:

$$\mathcal{C} = 1 + p \log_2 p + (1 - p) \log_2 (1 - p) \quad (1)$$

In this case where $p = 0.486$, $\mathcal{C} \approx 5.7 \times 10^{-4}$. The number of secret bits (\mathcal{K}) is equal to:

$$\mathcal{K} = N_c \cdot \mathcal{C} \quad (2)$$

where N_c is the length of codeword (i.e. the length of \vec{u} or \vec{b} in Fig.1). Thus, $\mathcal{K} \approx 6$ by using the spectral minutiae method where $N_c = 10240$. It means that we can maximum have around 6 secret bits to achieve an EER of 3.7% in this system. A 6-bit secret key is so short that the system can be easily compromised by a brute-force attack.

A solution to increase the number of secret bits is to decrease the BER of matching channels. The current helper data scheme requires a binary representation of biometric feature vectors, which introduces quantization errors into biometric channels. Therefore, we propose a new helper data scheme in this paper that does not require a binary feature vector. The main difference between the proposed scheme and the current one is the definition of biometric

²The Bit Error Rate (BER) or the crossover probability of the biometric channel refers to the fractional Hamming distance between \vec{b} and \vec{b}' , which is used to quantify the difference between two biometric template bit streams.

³The matching channel is generated by errors $\vec{b} \oplus \vec{b}'$, where \vec{b} and \vec{b}' are biometric template bit streams and come from the same person. The non-matching channel is generated by errors $\vec{b} \oplus \vec{b}'$, where \vec{b} and \vec{b}' come from different persons.

¹Breaking a 75-bit key by brute force requires 2^{75} times computation power. The Dutch national supercomputer (called Cartesius [3]) that could check 2.71×10^{14} keys per second would, in theory, require 4.42 years to exhaust the 75-bit key space.

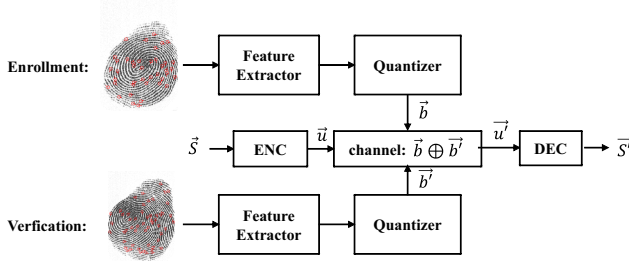


Figure 1. The equivalent communication system model for biometric recognition systems based on the helper data scheme [8]. (\vec{S} - the secret key, ENC - Encoder, DEC - Decoder).

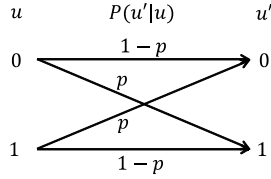


Figure 2. Binary Symmetric Channel (BSC) [7]. p is the crossover probability which is the error rate of the channel. u is the channel input and u' is the channel output.

channels. Instead of quantization, we convert a real-valued feature vector \vec{v} into a phase vector $\vec{\phi}$. In such a case, the channel in the new scheme is defined as $e^{j(\vec{\phi}-\vec{\phi}')}$, where $\vec{\phi}$ and $\vec{\phi}'$ are the phase vector during the enrollment and the verification phases, respectively. To transmit the secret key over such a channel, we need to introduce one of digital modulation schemes to the system.

The proposed real helper data scheme aims to assist any feature extractor to achieve a longer secret key without sacrificing its classification performance, in comparison with the current scheme. Finding out the best feature extractor for template protection systems is out of this paper's scope. Our paper is organized as follows. In Section II, we present the new helper data scheme in details whose performance is analyzed theoretically in Section III. Then, we compare the proposed helper data scheme with the current one in the SM-based fingerprint recognition system, and investigate their performance in the FVC2000-DB2 fingerprint database in Section IV. This paper ends with a discussion of the results.

II. A REAL HELPER DATA SCHEME

The proposed helper data scheme is depicted in Fig.3. It can be applied in any biometric recognition system such as fingerprint, face, et al. In this section, we take fingerprint as an example to explain how the proposed system works.

During the enrolment phase, the fingerprint of User X is sampled and processed by a feature extractor. We refer a real-valued feature vector to $\vec{v} = [v^1, \dots, v^{n_v}]$, where n_v is the number of features. \vec{v} is divided into two sub-sets \vec{v}_r

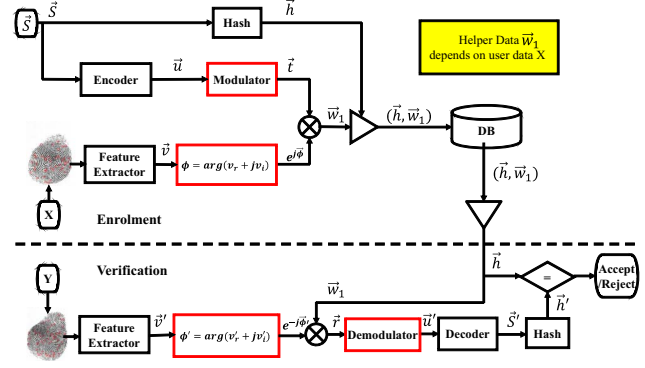


Figure 3. A real helper data system.

and \vec{v}_i :

$$\vec{v}_r \cup \vec{v}_i \subseteq \vec{v} \quad (3)$$

$$\vec{v}_r \cap \vec{v}_i = \emptyset \quad (4)$$

where \emptyset denotes empty set. \vec{v}_r and \vec{v}_i have the same number of elements (i.e. $\lfloor \frac{n_v}{2} \rfloor$). Based on \vec{v}_r and \vec{v}_i , we compose a complex vector $\vec{v}_c = \vec{v}_r + j\vec{v}_i$ where we derive our phase vector $\vec{\phi}$. For $\phi^k \in \vec{\phi}$, it is defined as:

$$\phi^k = \arg\{v_c^k\} \quad (5)$$

where \arg denotes the phase of a complex number, $k = 1, \dots, \lfloor \frac{n_v}{2} \rfloor$ and $\phi^k \in [-\pi, \pi]$. The number of elements in $\vec{\phi}$ (n_ϕ) is:

$$n_\phi = \lfloor \frac{n_v}{2} \rfloor \quad (6)$$

Given \vec{v} , there are many ways to define \vec{v}_r and \vec{v}_i , leading to variable definitions of $\vec{\phi}$ vector. However, we can not concatenate these $\vec{\phi}$ vectors into a long vector because of the information leakage. Let us take a simple example to explain this. Assume that $\vec{v} = [v^1, v^2, v^3, v^4, v^5, v^6]$, we define \vec{v}_r and \vec{v}_i into two ways:

$$\text{I: } \left. \begin{array}{l} \vec{v}_{r,\text{I}} = [v^1, v^2, v^3] \\ \vec{v}_{i,\text{I}} = [v^4, v^5, v^6] \end{array} \right\} \Rightarrow \tan(\vec{\phi}_{\text{I}}) = [\frac{v^4}{v^1}, \frac{v^5}{v^2}, \frac{v^6}{v^3}] \quad (7)$$

$$\text{II: } \left. \begin{array}{l} \vec{v}_{r,\text{II}} = [v^1, v^3, v^5] \\ \vec{v}_{i,\text{II}} = [v^2, v^4, v^6] \end{array} \right\} \Rightarrow \tan(\vec{\phi}_{\text{II}}) = [\frac{v^2}{v^1}, \frac{v^4}{v^3}, \frac{v^6}{v^5}] \quad (8)$$

With the information in Eq.7 and Eq.8, we can easily get this vector $[\frac{v^2}{v^1}, \frac{v^3}{v^1}, \frac{v^4}{v^1}, \frac{v^5}{v^1}, \frac{v^6}{v^1}]$. If we guess v^1 correctly, we will know the rest feature values. Equivalently, combining both phase vectors reduces the uncertainty of this six-element vector \vec{v} into the uncertainty of one element v^1 . By using $\vec{\phi}_{\text{I}}$ or $\vec{\phi}_{\text{II}}$, we only reduce the uncertainty of this six-element vector \vec{v} into the uncertainty of a three-element vector e.g. $\vec{v}_{r,\text{I}}$. For a long \vec{v} , we still keep enough uncertainty of feature vectors that cannot be compromised easily by the brute-force attack.

To protect biometric templates, a secret key \vec{S} is generated and its hashed version \vec{h} is stored in the central database.

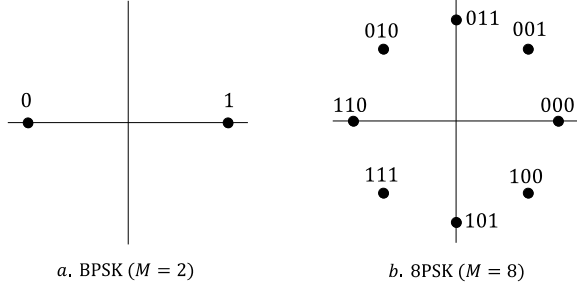


Figure 4. Signal space diagrams for PSK signals [9].

Meanwhile, \vec{S} is protected by error correcting codes then modulated into PSK (Phase-Shift Keying [9]) symbols (see Fig.4). With PSK, m bits are mapped into one of $M (= 2^m)$ uniform angular spaced points in a unit circle [9]. Rotating the PSK-modulated symbol $t^k (\in \vec{t})$ by a certain angle $\phi^k (\in \vec{\phi})$ defines the helper data $w_1^k (\in \vec{w}_1)$,

$$w_1^k = t^k \cdot e^{j\phi^k} \quad (9)$$

which is made publicly available and is needed in the verification phase.

When a user Y claiming to be X later authenticate herself/himself, her/his fingerprint needs to be measured. $\vec{\phi}'$ is obtained and $\vec{r} = \vec{w}_1 \cdot e^{-j\vec{\phi}'}$ is calculated, where \cdot denotes element-by-element multiplication between two vectors. Only if the secret key \vec{S} is correctly recovered from \vec{r} , X and Y are identified to be the same person.

Like the current helper data system, the proposed system is equivalent to a communication system. As mentioned earlier, their main difference is the channel model. Whether the new system prevails the current one is dependent on the answers to the following questions which will be found in the next section.

- 1) Is the new system secure?
- 2) Given a feature extractor, can we have a better channel quality from the new system?

III. THEORETICAL ANALYSIS

In this section, we analyze the performance of the proposed system under Gaussian assumption. Principle component analysis (PCA) or linear discriminant analysis (LDA) are often used to reduce the dimensionality of the transformed data in order to simplify the classifier [10]. PCA or LDA is, in fact, a linear combination of many components. Due to the Central Limit Theorem, we can assume that the real-valued feature vector will tend to be an independent and identically distributed (i.i.d.) multi-variate Gaussian distribution [11].

The non-reproducible biometric samples lead to the variability of feature components. For person X , the noisy feature component v_x^j is modeled as a Gaussian random variable

with mean of μ_x^j and variance of $\sigma_x^{j^2}$, where μ_x^j and $\sigma_x^{j^2}$ are random variables. We assume that $\mu_x^j \sim \mathcal{N}(0, 1 - \sigma_x^{j^2})$ and $\sigma_x^{j^2}$ is uniformly distributed in the range of $[0, 1]$. For any person, $v^j \sim \mathcal{N}(0, 1)$ where $v^j \in \vec{v}$ and v^j is the real-valued feature across the whole population.

We divide \vec{v} into two subsets: \vec{v}_r and \vec{v}_i . For any pair (v_r^j, v_i^j) where $v_r^j, v_i^j \sim \mathcal{N}(0, 1)$, its ratio $\frac{v_i^j}{v_r^j}$ follows the standard Cauchy distribution [12]. If ψ is a uniform random variable on the interval $I = (-\frac{\pi}{2}, \frac{\pi}{2})$, it is well known that $\mathcal{Y} = \tan(\psi)$ follows the standard Cauchy distribution [13]. Also $\mathcal{Z} = \tan(n\psi)$, where n is any positive integer, has this distribution [13]. Therefore, $\vec{\phi}$ is uniformly distributed over a unit circle. The probability density function (pdf) of $\phi^k (\in \vec{\phi})$ is:

$$f(\phi^k) = \frac{1}{2\pi} \quad \text{where } -\pi \leq \phi^k \leq \pi \quad (10)$$

Since t^k is one of M uniform angular spaced points in a unit circle (see Fig.4), the helper data w_1^k is uniformly distributed over a unit circle with the same pdf as ϕ^k . Given the information of $\vec{w}_1 = \vec{t} \cdot e^{j\vec{\phi}}$ where $t^k \in \vec{t}$ is uniformly distributed over a unit circle with a probability of $\frac{1}{M}$ (see Fig. 4), it is not possible to learn about \vec{t} or $\vec{\phi}$ from \vec{w}_1 . Thus, we conclude that the proposed scheme is secure.

To answer the second question, we generate feature vectors based on the above assumptions. In the simulation, we assume there are 100 persons in the database. Each person has 10 samples and each real-valued vector has 2048 features. For the current helper data scheme, we choose 1-bit quantization. The 1-bit quantization method may not optimize the classification performance, but it gives us the lowest BER of biometric channels (i.e. the maximum channel capacity). For the new scheme, we choose BPSK (i.e. $M = 2$) as the modulation scheme that gives the shortest codeword.

Simulation results show that the average BER of matching channels is about 32% in the current scheme and 25% in our approach, meaning that the channel capacity (i.e. $I(\vec{u}, \vec{u}')$) of the proposed helper data system is about twice as much as the current system. Hence, we conclude that the new system gives better channel quality. Whether this occurs to real biometric data will be investigated in the next section.

IV. EXPERIMENT RESULTS

In this section, we analyze the performance of our proposed helper data scheme by testing it in the FVC2000-DB2 fingerprint database [14]. 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 [5] to get a string of 10240 real-valued features (i.e. \vec{v}).

We compare two systems. The first system, *System A*, is a SM-based fingerprint recognition system using the current helper data scheme as shown in Fig.1. In this system,

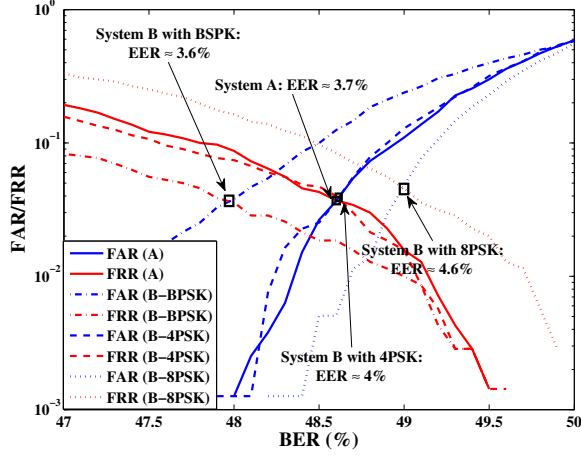


Figure 5. FAR/FRR curves. In the experiment, the user gives one sample during the enrolment and one sample during the verification. A - System A; B - System B.

we choose 1-bit quantization to convert real-valued feature vectors into binary vectors. In this case, the length of ECC codeword of System A ($N_{c,A}$) is:

$$N_{c,A} = n_v \quad (11)$$

The second system, *System B*, is a SM-based fingerprint recognition system using the real helper data scheme, see Fig.3. For System B, we analyze its performance for three different modulation schemes (i.e. BPSK, 4PSK and 8PSK), respectively. The phase vector is defined by Eq.5, where \vec{v}_r and \vec{v}_i are the vector with all the odd-indexed elements and the even-indexed elements in \vec{v} , respectively. System B with different modulation type has different length of codeword. For System B, the length of ECC codewords ($N_{c,B}$) is defined as:

$$N_{c,B} = m \cdot \lfloor \frac{n_v}{2} \rfloor \quad (12)$$

where m is the number of bits per PSK symbol. Higher order of PSK (i.e. larger m) means longer codeword (i.e. larger $N_{c,B}$). BPSK has the smallest m (i.e. $m = 1$) and thus has the shortest codeword. As mentioned earlier, the design of ECC is dependent on the channel quality that will be firstly investigated in our experiments.

Without taking ECC into account, both systems use the BER as the matching score to classify the matching channel and the non-matching channel. Assuming that the user gives one sample during the enrolment and one sample during the verification. Fig.5 shows the FAR (False Acceptance Rate) and FRR (False Rejection Rate) curves against the matching score (i.e. BER). As you can see, the performance of System B is affected by the modulation type. Compared to System A, only System B with BPSK has a lower EER ($\approx 3.6\%$) and requires a lower BER threshold ($\approx 48\%$) to do the

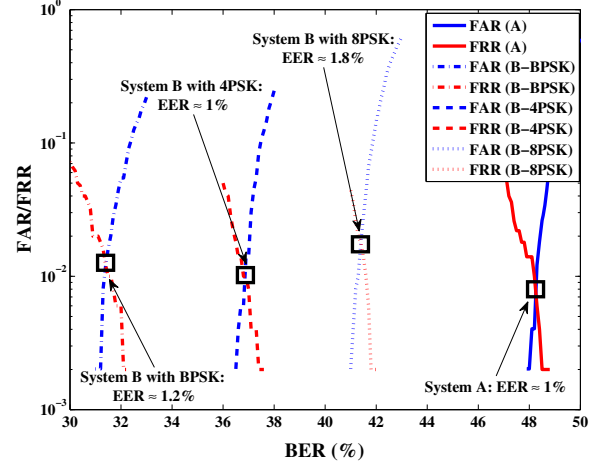


Figure 6. FAR/FRR curves. In this experiment, the user gives one sample during the enrolment and three samples during the verification. A - System A; B - System B.

classification. However, Shannon theory proves that this system can only have around 6 secret bits, which is derived from Eq.1 and Eq.2. As mentioned in Section I, System A achieves a 6-bit secret key as well. Correspondingly, compared to the current helper data scheme, our real helper data scheme improves the classification performance (an EER gain of 0.1%) but does not increase the length of secret key. A 6-bit secret key is too short to secure the system. Thus, using multiple samples during the verification is proposed to improve the channel quality for both systems. Not choosing multiple samples during the enrolment is due to the possible information leakage. As we defined in Section I, the channel of the proposed system is $e^{j(\phi - \phi')}$, where ϕ and ϕ' are the phase vectors from two samples. If we enrol multiple samples, the attacker may have the chance to decode the secret key successfully. The same principle applies to the current helper data scheme.

Now let us get three samples during the verification. In such a case, the channel of System A (\vec{c}_A) is defined as:

$$\vec{c}_A = \vec{b} \oplus \vec{b}_f \quad (13)$$

where \vec{b}_f is related to the binary feature vectors (i.e. \vec{b}' , \vec{b}'' and \vec{b}''') from the verification. Here, we define a binary matrix \vec{B} whose rows are \vec{b}' , \vec{b}'' and \vec{b}''' , respectively. The element of \vec{b}_f is defined as:

$$b_f^k = \begin{cases} 1, & \text{if the } k^{\text{th}} \text{ column of } \vec{B} \text{ has at least two 1's.} \\ 0, & \text{else.} \end{cases}$$

where $k = 1, \dots, 10240$.

For System B, the channel \vec{c}_B is defined as:

$$\vec{c}_B = [e^{j\Delta\vec{\phi}} \quad e^{j\Delta\vec{\phi}'}] \quad (14)$$

	$\mathcal{K} = 56$			$\mathcal{K} = 66$			$\mathcal{K} = 76$		
	BPSK	4PSK	8PSK	BPSK	4PSK	8PSK	BPSK	4PSK	8PSK
FAR	0.2%	0.0%	0.0%	0.2%	0.0%	0.0%	0.0%	0.0%	0.0%
FRR	2.4%	4.4%	20.2%	2.6%	5.6%	21.0%	3.4%	5.8%	21.8%
EER	1.3%	2.2%	10.1%	1.4%	2.8%	10.5%	1.7%	2.9%	10.9%

Table I

PERFORMANCE COMPARISON AMONG SYSTEM B'S FOR DIFFERENT \mathcal{K} , WHERE \mathcal{K} IS THE SECRET LENGTH. IN THE EXPERIMENTS, WE USE REPETITION CODES AND BCH CODES WITH A CODE RATE OF $\frac{\mathcal{K}}{1023}$ TO PROTECT THE SECRET KEY.

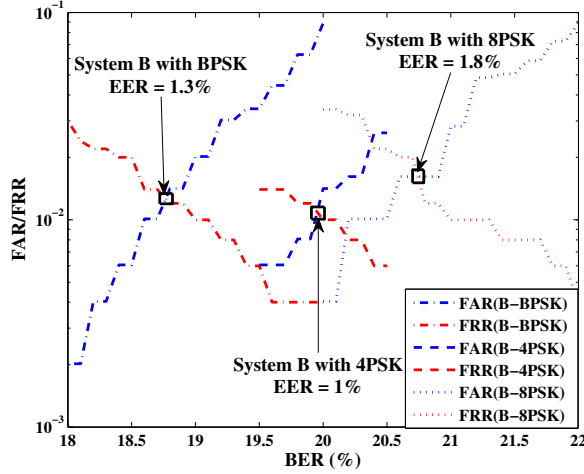


Figure 7. FAR/FRR curves after using repetition codes. In this experiment, the user gives one sample during the enrolment and three samples during the verification. The code rate of repetition codes for System B with BPSK, 4PSK and 8PSK is $\frac{1}{9}$, $\frac{1}{19}$ and $\frac{1}{29}$, respectively.

where $\Delta\vec{\phi}$ and $\Delta\vec{\varphi}$ are the average value of $\vec{\phi} - \vec{\phi}'$, $\vec{\phi} - \vec{\phi}''$ and $\vec{\phi} - \vec{\phi}'''$. $\vec{\phi}$ is from the enrolment; $\vec{\phi}'$, $\vec{\phi}''$ and $\vec{\phi}'''$ are the phase vectors from the verification. $\Delta\vec{\phi}$ and $\Delta\vec{\varphi}$ are calculated by two different methods, respectively.

$$\Delta\vec{\phi} = \frac{1}{3}[(\vec{\phi} - \vec{\phi}') + (\vec{\phi} - \vec{\phi}'') + (\vec{\phi} - \vec{\phi}''')] \quad (15)$$

$$\Delta\vec{\varphi} = \arg\{e^{j(\vec{\phi} - \vec{\phi}')} + e^{j(\vec{\phi} - \vec{\phi}'')} + e^{j(\vec{\phi} - \vec{\phi}''')}\} \quad (16)$$

where \arg denotes the phase of a complex number. The periodicity of phase allows us to use these two ways to get the average phase value, meaning that the codeword length is doubled in comparison with the case using one sample per verification.

Fig.6 shows the experiment results. An increase of the number of samples during the verification enhances the performance of both systems (i.e. lower EER and lower BER). Both System A and System B with 4PSK achieve the lowest EER (i.e. 1%), which are followed by System B with BPSK (i.e. 1.2%) and then System B with 8PSK (i.e. 1.8%). Meanwhile, using three samples per verification improves the channel quality in both systems. System B with BPSK requires the lowest BER (i.e. 31.4%) to do the

classification, followed by System B with 4PSK (i.e. 36.8%), System B with 8PSK (i.e. 41.4%) and System A (i.e. 48.2%). In comparison with one sample per verification, System B with BPSK has the most BER reduction (i.e. 17.2%) and System A has the least reduction (i.e. 0.4%). The BER reduction in System A is too little to increase the secret key length significantly (i.e. around 9 bits according to Eq.1 and Eq.2). For System B, the Shannon Theory shows that using BPSK gives us the most secret bits (1047 bits) followed by 4PSK (1041 bits) and 8PSK (658 bits).

A secret key of 9 bits is still too short to secure the whole system, so we only design codes for System B. In this paper, repetition codes are chosen to further reduce the BER of the channel, and then BCH codes are adopted to correct the rest errors. The code rate of repetition codes is determined by the codeword length of BCH codes. To prove concept, we only use BCH codes with a length of 1023. In this way, the rate of repetition code for BPSK, 4PSK and 8PSK is $\frac{1}{9}$, $\frac{1}{19}$ and $\frac{1}{29}$, respectively. As we can see in Fig.7, repetition codes significantly decrease the BER of biometric channels (a BER gain of 12.6%~20.8%). The BER of System B with BPSK is still the lowest after using repetition codes. The classification performance (i.e. EER) of these three systems are rarely affected by repetition codes. Only the EER of System B with BPSK is increased by 0.1%.

After repetition codes, BCH codes further reduce the remaining error rates to zero. Table I shows the performance of System B's based on repetition codes and the $(1023, \mathcal{K})$ BCH codes where \mathcal{K} is the secret length. The help of both codes decreases the FAR but increases the FRR of System B (see Fig.6 and Table I). Besides, the performance loss increases with the order of PSK and \mathcal{K} . System B with BPSK and a 56-bit secret key has the best performance with an EER of around 1.3% (FAR = 0.2%, FRR = 2.4%), which followed by BPSK with a 66-bit key (FAR = 0.2%, FRR = 2.6%) and BPSK with a 76-bit key (FAR = 0.0%, FRR = 3.4%). Because the used BCH codes correct 18.3%~18.7% errors which is closer to the BER score at the EER value of BPSK than the other two systems (see Fig.7), System B with BPSK outperforms the one with 4PSK. Furthermore, the experiment results show that this system can have a larger \mathcal{K} (> 76) with slightly performance loss, but a 76-bit key is long enough to secure the system.

V. CONCLUSIONS

In this paper, we propose a real helper data scheme for biometric template protection systems. A basic realization is to convert the real-valued feature vector into a phase vector. In such a case, we avoid quantization error that exists in the current helper data system. By applying the spectral minutiae method in the FVC2000-DB2 fingerprint database, using three samples during the verification improves the channel quality in the proposed system significantly. Unfortunately, that does not occur to the current scheme that maximum can have 9 bits in this case. With the help of repetition codes and BCH codes, the proposed system allows at least 76 secret bit with an EER loss of about 0.5% compared to the case without error correcting codes.

REFERENCES

- [1] B. Schneier, "Inside risks: the uses and abuses of biometrics," *Comm. of the ACM*, vol. 42, p. 136, 1999.
- [2] P. Tuyls, et al., "Practical biometric authentication with template protection," in *AVBPA*, 2005, pp. 436–446.
- [3] Cartesius. [Online]. Available: <https://www.surfsara.nl/systems/cartesius>
- [4] T. Ignatenko, "Secret-key rates and privacy leakage in biometric systems," Ph.D. dissertation, PhD thesis, Technical University of Eindhoven, 2009.
- [5] H. Xu, et al., "Binary representations of fingerprint spectral minutiae features," in *ICPR*, 2010.
- [6] X. Shao, et al., "A concatenated coding scheme for biometric template protection," in *ICASSP*, 2012, pp. 1865–1868.
- [7] R.G. Gallager, *Information theory and reliable communication*. Wiley, 1968.
- [8] X. Shao, et al., "A 3-layer coding scheme for biometry template protection based on spectral minutiae," in *ICASSP*, 2011, pp. 1948 – 1951.
- [9] J. Proakis, *Digital communications*. McGraw-hill, 1987, vol. 1221.
- [10] A.K. Jain, et al., "Statistical pattern recognition: A review," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 1, pp. 4–37, 2000.
- [11] E.J.C. Kelkboom, et al., "Binary biometrics: An analytic framework to estimate the performance curves under gaussian assumption," *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, vol. 40, no. 3, pp. 555–571, 2010.
- [12] P. Athanasios, *Probability, random variables and stochastic processes*. McGraw-Hill, 1991.
- [13] C. M. C. Avellana, "Geometrical understanding of the cauchy distribution," *Questi  : Quaderns d'Estad  stica, Sistemes, Inform  tica i Investigaci   Operativa*, vol. 26, no. 1, pp. 283–287, 2002.
- [14] D. Maio, et al., "FVC2000: Fingerprint verification competition," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 24, no. 3, pp. 402–412, 2002.