FACE RECOGNITION WITH BIOMETRIC ENCRYPTION FOR PRIVACY-ENHANCING SELF-EXCLUSION

Haiping Lu, Karl Martin, Francis Bui, K. N. Plataniotis, Dimitris Hatzinakos

The Edward S. Rogers Sr. Department of Electrical and Computer Engineering
University of Toronto, M5S 3G4, Canada
{haiping, kmartin, bui, kostas, dimitris}@comm.toronto.edu

ABSTRACT

Face recognition has been employed in various security-related applications such as surveillance, mugshot identification, e-passport, and access control. Despite its recent advancements, privacy concern is one of several issues preventing its wider deployment. In this paper, we address the privacy concern for a self-exclusion scenario of face recognition, through combining face recognition with a simple biometric encryption scheme called helper data system. The combined system is described in detail with focus on the key binding procedure. Experiments are carried out on the CMU PIE face database. The experimental results demonstrate that in the proposed system, the biometric encryption module tends to significantly reduce the false acceptance rate while increasing the false rejection rate.

Index Terms— Face recognition, biometric encryption, security, privacy, watch list.

1. INTRODUCTION

Face recognition has a wide range of applications, such as surveillance, access control, e-passport, and human-computer interaction [1]. In particular, face recognition is one of the three identification methods used in e-passports. Furthermore, facial features scored the highest compatibility among the six biometric attributes in a machine readable travel documents (MRTD) system based on several evaluation factors including enrollment, renewal, machine requirements, and public perception [2]. This is largely due to the fact that compared to other popular biometric technologies: face recognition is non-intrusive and easy to use [3].

The work presented in this paper has been partially supported by the Ontario Lottery and Gaming Corporation (OLG). The views, opinions, and findings contained in this paper are those of the authors and should not be construed as official positions, policies, or decisions of the OLG, unless so designated by other official documentation.

The authors would like to thank Mr. Klaus Peltsch from the Ontario Lottery and Gaming Corporation, and Dr. Ann Cavoukian and Dr. Alex Stoianov from the Information and Privacy Commissioner of Ontario for many useful discussions.

Although face recognition has made tremendous progress in the past two decades, there have been several concerns preventing its wider deployment, such as the effectiveness in field test, the performance under uncontrolled conditions, and privacy concern. Privacy concern arises when there are large centralized databases of biometric passwords and there are risks of identity theft and privacy leaks [4]. Consequently, biometric encryption has emerged to address this concern. The objective is to deploy biometrics in a privacy-enhancing way that minimizes the possibility of abuse, maximizes individual control, and ensures full functionality of the systems in which biometrics are used [5]. For face recognition with biometric encryption, rather than storing one's facial image in a database, the facial image is used to encrypt (code) some other information such as a cryptographic key and only the biometrically-encrypted data is stored. This removes the need to collect and store actual biometric data in database and most privacy concerns associated with centralized databases are eliminated.

There has been several works proposed to construct privacy-enhancing systems using biometric encryption for face biometrics. A fuzzy vault based cryptographic key generation method was introduced by Wang *et al.* [6]. The helper data system (HDS) is applied to face recognition in 2005 [4], and the multi-bit quantization using likelihood ratio method is proposed for privacy-enhancing face recognition in 2007 [7]. In [8], we have investigated a biometric encryption system based on the quantization index modulation (QIM) approach [9, 10] for a self-exclusion scenario of face recognition. In this paper, we investigate a biometric encryption system based on the helper data system in [4] for the same self-exclusion scenario.

In the HDS approach for face recognition presented in [4], the fiducial points are extracted from face images. Then, binarized features are constructed based on estimates of the reliability statistics. In a general HDS construction, during enrollment, these features are used to bind a cryptographic key, creating one of the helper data. The operation involved is the binary XOR. Here, the goal of the system is to reject, during the verification process, an unauthorized subject who does not

possess the original face features used during enrollment. In contrast, a genuine subject with the correct face features will be accepted. More importantly, the verification process needs to be based solely on the helper data, without requiring direct access to the original face features.

This paper is organized as follows. Section 2 describes the proposed HDS-based biometric encryption system for the self-exclusion scenario of face recognition, with emphasis on the key binding module and bit allocation strategy. Section 3 presents the experimental results and Section 4 draws the conclusions.

2. HDS-BASED BIOMETRIC ENCRYPTION FOR THE SELF-EXCLUSION SCENARIO OF FACE RECOGNITION

This work was motivated by an Ontario Lottery and Gaming Corporation (OLG) initiative to evaluate facial recognition for its self-exclusion gaming program [8]. In a self-exclusion program, the system uses facial recognition to automatically identify voluntarily enrolled subjects who have entered a gaming facility and contravened the terms of the program, while protecting the privacy of stored personal information at the same time. This belongs to the "watch list" scenario [11], involving one-to-few matches that compare a query sample against a list of suspects. The size of database is usually very small compared to the possible queries in this task, and the identity of the probe subject may not be in the database. Therefore, the system needs to first detect whether the query is on the list and if yes, correctly identify it. Due to the OLG requirement that the system should identify as many enrolled subjects as possible, the performance requirements (minimization) in the self-exclusion scenario are placed on the false rejection rate (FRR), rather than the false acceptance rate (FAR) [8].

2.1. System overview

The combined face recognition and biometric encryption approach in [8] is modified for the HDS-based biometric encryption in this paper, as shown in Fig. 1. Figures 1(a) and 1(b) illustrate the general enrollment and watch list identification systems, respectively. Subject identification is performed using a commercial face recognition system and a biometric encryption module is incorporated to offer privacy protection of the personal information through a bound cryptographic key which can be used with conventional cryptographic techniques to encrypt the subject's personal data for secure application.

As shown in the figure, the input during enrollment is the subject's facial image as well as a unique identifier (ID). In enrollment, a helper data is generated as a result of binding the cryptographic key with the facial features. During watch list identification, the commercial system attempts to match

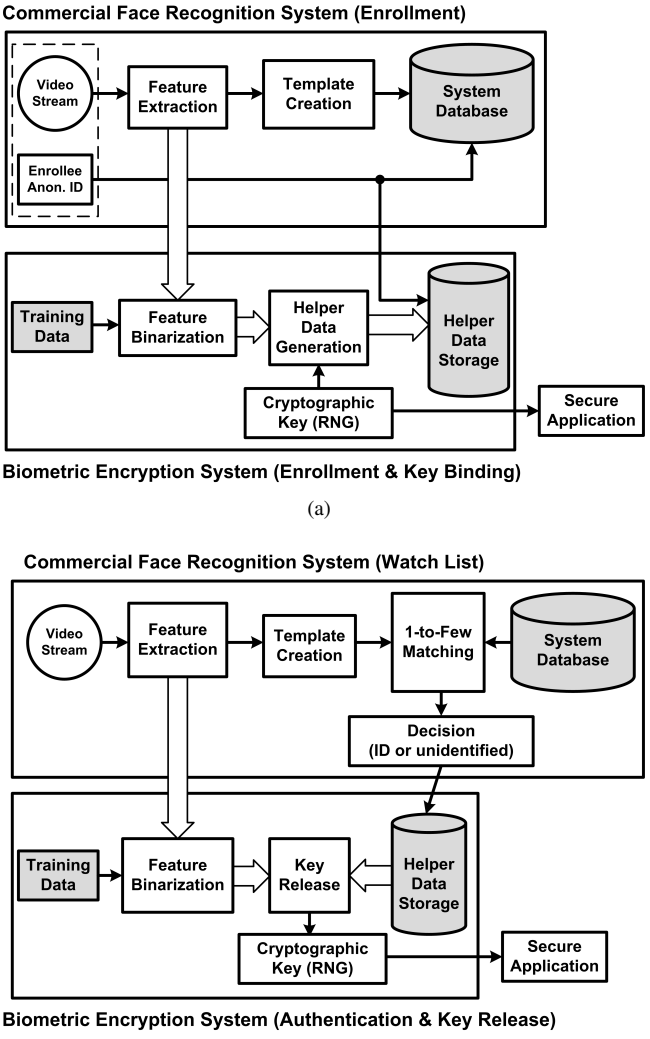

Fig. 1. Combined face recognition system and HDS-based biometric encryption for (a) enrollment and key binding, (b) watch list identification and key release.

input subjects to those in the system database. If a match is made, the system will output a claimed identity which is input into the biometric encryption system to release the key. As in [8], it should be noted that this system is designed under two constraints: the biometric encryption system is only for key verification, and the commercial face recognition system employed for watch list identification cannot be manipulated internally.

The configuration of the HDS-based biometric encryption system is shown in Figure 2, which resembles that in [8] and is a generalization of the system diagram in [4]. As seen from the figure, facial features are used to verify whether the key associated with a user should be released or not. If released (i.e., the user identity is verified), the key can be used for other secure applications. To support secure applications, other

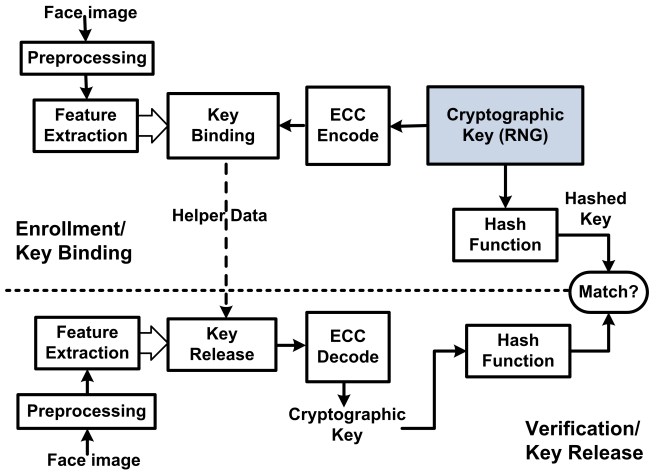

Fig. 2. The configuration of the HDS-based biometric encryption system for enrollment (key binding) and verification (key release).

modules need to be constructed around the cryptographic key. From the cryptographic key module, two diverging paths are implemented: one is cryptographic hash to generate a hashed key and the other is error-correcting code (ECC) to protect against fuzzy variability and other distortions. The data obtained after ECC are then used as input to a key binding module. The key binding module utilizes feature vectors to securely embed the encoded key and produce another helper data to be used during verification. In the following, various modules are examined. The focus is on the key binding module and bit allocation. More detailed discussions on other modules are available in [8].

2.2. Facial image preprocessing and feature extraction

Facial image preprocessing is a necessary step for each facial image before feature extraction. The input facial images need to be normalized against variations which commonly occur, such as rotation, scaling, and dynamic range of pixel values. For feature extraction, we choose the principal component analysis (PCA) algorithm [12, 13] in experiments for baseline comparisons, although there are many other more advanced feature extraction algorithms for face recognition [1, 14, 15, 16]. PCA computes a projection matrix and retains the top β bases, where β is usually chosen based on an energy criterion.

2.3. Cryptographic key module, cryptographic hash function, and error-correcting code module

The cryptographic key is a binary string to be protected and it is to be used for a secure application, such as encrypting other information data. In practice, the usage of AES-128, AES-192 and AES-256 are prefered[17]. In the self-exclusion context, AES key selection should consider not only the cryptographic security but also the biometric verification performances since if the associated biometric errors are too high, it would not be meaningful to specify an unachievable key requirement.

As shown in Fig. 1, instead of storing the actual key, its hashed version is stored in order to conceal the cryptographic key in a helper data form suitable for storage and to provide a secure comparison method for key verification. A hash function accepts a variable-length input and produces a fixed-length output [18]. In practice, the NIST recommends to employ at least SHA-256 [18].

In addition, to take into account of the fuzzy variability in the extracted feature vectors, error-correcting code (ECC) is needed and we choose the BCH family of codes [19, 20]. These codes are parameterized as (n, k, t): where n denotes the number of bits in a codeword, k denotes the number of bits in a message symbol, and t denotes the number of random bit errors correctable. It should be noted that the characteristics of the cryptographic keys impose constraints on the subsequent schemes to be applied, including the ECC parameters and the number of feature components to be extracted during enrollment [8]. For instance, to support an AES key of L bits, BCH codes with $k \geq L$ are needed.

2.4. HDS-based key binding module

The objective of the key binding module is to utilize a feature vector to securely bind the encoded cryptographic key, which generates a helper data for storage. In this work, each component of the PCA feature vector is used to bind one bit of the cryptographic key (after error-correcting encoding), and we adopt the HDS-based key binding scheme [4]. In considering this scheme, which is essentially based on the fuzzy commitment framework, it is useful to separate the process into two sub-modules: key binding and key release, corresponding to the enrollment and verification stages, respectively. The first module performs the biometric binding process, while the second is responsible for verifying the biometric and unbinding the cryptographic key.

Figure 3(a) shows the key binding process. First, the cryptographic key is encoded for error tolerance. It is then bound to the binarized feature vector. The binding is performed using an XOR operation. This process is analogous to storing and locking the cryptographic key in a "secure box", where the "key" to this box is the biometric feature vector itself. Without access to the correct physiological features, the cryptographic key cannot be recovered. Thus, an intruder cannot feasibly produce the feature vector necessary to unlock this secure box. The theoretical basis of this form of information concealment is known as a one-time pad (OTP) [18]. Basically, as long as the mask used for XOR (i.e., the binarized feature vector) is of random nature, then the "locking" mechanism is information-theoretically secure.

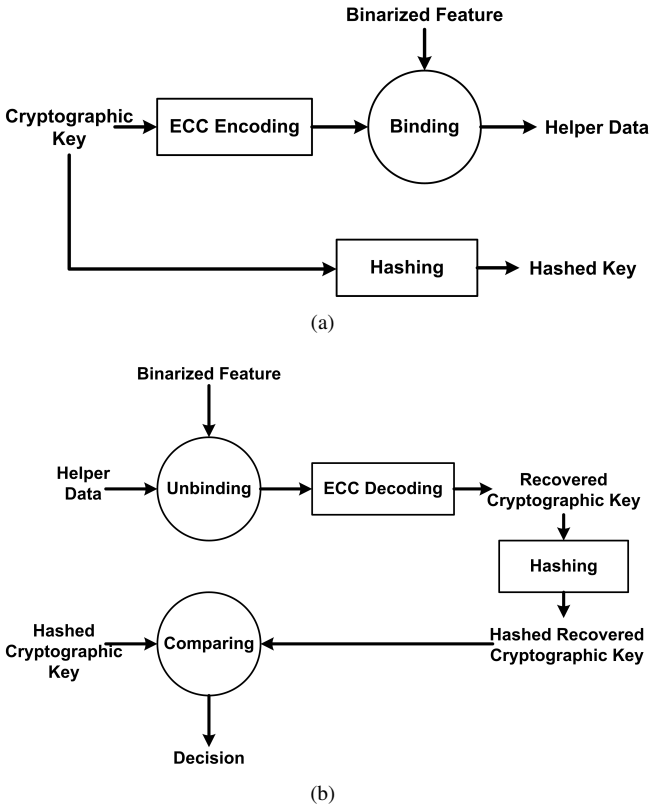

Fig. 3. Illustration of (a) the key binding process, (b) the key release process.

Figure 3(b) shows the steps for unbinding the key. In this case, a user claiming some identity submits his or her facial features for verification, from which a binarized feature vector is extracted. The unbinding operation is also an XOR operation. If the two feature vectors, during enrollment and during verification, match exactly, then the original cryptographic key is unbound successfully. However, in a practical scenario, there are typically differences in the two vectors. Due to the XOR operation, the bit differences take the form of an aggregate "error vector". This error vector has the equivalent effect of an additive (binary) noise on the received codeword. It is characterized using the Hamming distance, which is defined as the number of bit differences between two binary sequences. The ECC decoding block is responsible for eliminating these bit differences, up to some allowed Hamming distance.

The result of the ECC decoder, the recovered cryptographic key, needs to be tested for authenticity. It should be noted that the original key is not stored (in plain text) anywhere; instead only its hashed value is available. Therefore, the hashed value of the recovered key is generated for comparison against the stored value. If the two hashed values match exactly, then the system declares a positive match. Otherwise, the system rejects this user.

2.5. Bit allocation

Bit allocation refers to the process of assigning an integer quantity of bits to be embedded into each of the biometric feature components. In this work, we embed one bit to each retained PCA feature components. For PCA feature components selection, there are two choices to embed L bits: 1) the first L PCA components (which capture the most variations) are selected; 2) the most reliable L PCA components are selected. The following describes how to select the PCA components that are most reliable for binding, following [4].

Our reliability-based feature component selection scheme adopts a per-user bit allocation policy, with each user having a different set of components used for key binding. For a particular user i, the reliability of the component γ is denoted as $R_{i,\gamma}$, and is defined as

$$R_{i,\gamma} = \frac{1}{2}\left(1 + \mathrm{erf}\left(\frac{|\mu_{i,\gamma} - \mu_{\gamma}|}{\sqrt{2\sigma_{i,\gamma}^2}}\right)\right), \qquad (1)$$

where $\mu_{i,\gamma}$ is the subject mean of component γ, μ_{γ} is the population mean of component γ, and $\sigma_{i,\gamma}^2$ is the subject variance. The rationale for the preceding definition is that, assuming a Gaussian distribution for the feature component, this reliability measure is the probability that a new measurement (e.g., during verification) from the same subject results in the same bit which was assigned previously (e.g., during enrollment). Higher reliability implies higher discriminative power of the corresponding component. To bind with a secret key of L bits, the L components with the highest reliability are selected.

2.6. Gray coding

In a number of the underlying modules, there is a common operation involved, which requires representing a numerical quantity as a binary string. This binarization process can potentially have a notable impact on the overall system performance, if certain design factors are not considered. For example, for binarized feature vectors, even minor environmental noise may lead to significant changes in the encoded binary (i.e., large Hamming distance). This is particularly true for a natural binary mapping, e.g., using a pulse code modulation (PCM) scheme [20, 21]. Therefore, in this work, a special type of mapping known as the Gray coding can be applied, after PCM, to minimize this behavior. While there is an increased cost in system complexity, the encoded binary strings are less susceptible to dramatic changes in response to noise variations. For example, in the enrollment stage, incremental changes in the input features should result in incremental changes in Hamming distances for the binarized feature vectors. This implies that performance loss due to the binarization procedure can be reduced.

2.7. Training requirements

Generally, two main components in the biometric encryption system need training: feature extraction and key binding/release. The training requirements of the feature extractor vary depending on the feature extraction algorithm. Nevertheless, the feature extractor should be trained on images that match the general capturing conditions of the images to be used in practice. For the key binding and release, the training generally involves calculation of the statistics for each feature component across the population and for individual subjects. Specifically, the mean and variance must be calculated for each component across the entire enrolled population. In addition, per subject statistics (again, mean and variance) are also required. Thus, we need several enrollment images per subject to allow the accurate estimation of these statistical parameters.

3. EXPERIMENTAL RESULTS

The experiments were carried out on a subset of the Pose, Illumination, and Expression (PIE) database provided by the Carnegie Mellon University (CMU) [22]. This database contains 68 subjects with face images captured under varying pose, illumination and expression. The subset includes three frontal poses (C07, C09, and C27) under seven illumination conditions (06, 07, 08, 11, 12, 19, and 20) so there are approximately 21 (3×7) images per subject (with some faces missing). The images are resized so that there are 70 pixels between eyes, with 8-bit gray levels per pixel. The experiments are performed using MATLAB v.7.5.0.

The PIE subset is partitioned into a gallery set containing all except one of the images for each subject, and a probe set with the single remaining image for each subject. The gallery set is for training the system and enrollment of the subjects. The probe set is for testing the recognition performance. For the chosen feature extraction algorithm PCA, the first 154 PCA components are retained for each image.

In experiments, the biometric encryption module is tested in isolation first to get the verification performance, and then as part of the whole system to get the performance in the watch list scenario. In the watch list scenario, the identification process generates a ranked list of candidate subjects for each probe subject tested. This list is then passed to the biometric encryption module where 1-to-1 verification is performed individually. The length of the list may vary between 0 (i.e., unidentified - no matching subject found in the gallery) and r (the maximum rank for identification), where r is to be chosen based on the application requirements.

3.1. Baseline performance without biometric encryption

Since the watch list recognition operation is to be performed, a baseline level of recognition performance needs to be established to evaluate the system with biometric encryption. Therefore, the baseline performance under the watch list scenario is simulated first.

Using the definitions in [8, 11], each probe subject p_j is compared against each gallery subject g_i using a similarity metric s_{ij}. Subject p_j is unidentified and rejected if s_{ij} is less than a given threshold t_s for all gallery subjects. When there are gallery subjects for which $s_{ij} \geq t_s$, these subjects are ranked according to the value s_{ij} and the first r are returned. The similarity metric used is the normalized inner product defined below:

$$s_{ij} = \frac{\langle X_i, X_j \rangle}{\| X_i \| \cdot \| X_j \|} = \frac{\sum_{k=1}^{N} X_i(k) \cdot X_j(k)}{\sqrt{\sum_{k=1}^{N} X_i(k)^2} \cdot \sqrt{\sum_{k=1}^{N} X_j(k)^2}} \tag{2}$$

where X_i and X_j are the N-component feature vectors for g_i and p_j, respectively. This metric s_{ij} represents the cosine of the angle between the two vectors. A greater value of s_{ij} indicates higher similarity between the two compared feature vectors. The FRR and FAR for the watch list scenario are calculated respectively as [8, 11]

$$P_{FR}(t_s, r) = 1 - \frac{|\{p_j : s_{ij} \geq t_s, rank(p_j) \leq r, id(p_j) = id(g_i)\}|}{|\mathcal{P}_G|}, \quad \forall p_j \in \mathcal{P}_G, \tag{3}$$

where $|\mathcal{P}_G|$ is the number of gallery subjects, and

$$P_{FA}(t_s, r) = \frac{|\{p_j : \max_i s_{ij} \geq t_s|}{|\mathcal{P}_N|}, \forall p_j \in \mathcal{P}_N, \forall g_i \in \mathcal{P}_G, \tag{4}$$

where $\mathcal{P}_N$ denotes a set of imposter subjects. For a particular r, 1000 (FAR,FRR) value pairs are generated by varying the threshold t_s linearly in the range $[-1, 1]$. The recognition performance for $r = 5$, 10, and 20 are shown in Fig. 4.

It should be pointed out that in this work, the actual performance values (FAR and FRR) are not significant since they depend on the database, the feature extractor, and the classifier. The significance of these results is to demonstrate the effect of r on recognition performance as well as the relative recognition performance compared against the system with biometric encryption.

In addition, it should be noted that the self-exclusion scenario requires minimal FRR since FRR represents the rate at which the enrolled self-exclusion subjects would go undetected and allowed to enter the gaming premises. Thus, for each scenario, an operating point is chosen where FRR is minimized. These operating points need to be chosen to test the system with the biometric encryption module since the operating points determine the identification results (the list) to be passed to the biometric encryption module. Three operating points are labeled in Fig. 4, as listed in the left half of Table 1.

Table 1. Full watch list recognition performance for system with and without HDS-based biometric encryption.

Operating point label	Rank list length r	Baseline performance (without biometric encryption)		Key length (bits)	Code length (bits)	Full system performance (with HDS-based biometric encryption)	
		FAR	FRR			FAR	FRR
OP5	5	0.1159	0.3088	16	63	0	0.4706
				36	63	0	0.8676
OP10	10	0.1591	0.2794	16	63	0	0.4706
				36	63	0	0.8676
OP20	20	0.2801	0.2353	16	63	0	0.4412
				36	63	0	0.8529

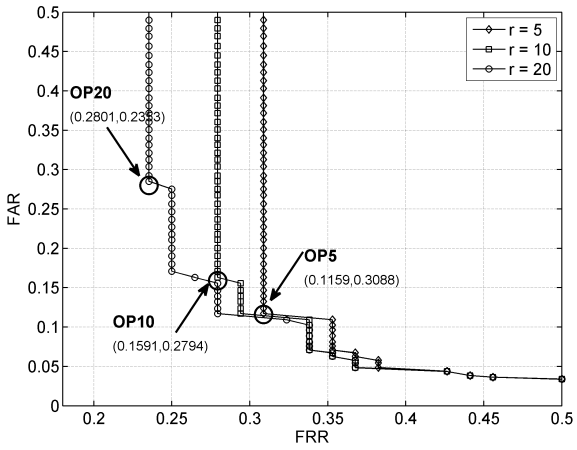

Fig. 4. Baseline performance using maximum rank $r = 5, 10$, and 20. The three chosen operating points for each scenario are labeled OP5, OP10, and OP20, respectively.

3.2. The performance of the HDS-based biometric encryption system

The recognition performance of the HDS-based biometric encryption system is first tested in isolation as a verification operation. As discussed in Sec. 2.5, the biometric encryption module has two different modes of operation, based on which feature components are selected for binding. One is based the energy (or variance) captured and the other is based on the reliability computed through (1). The FRR and FAR for the verification scenario are calculated respectively as [8, 11]

$$P_{FR}(t_s) = 1 - \frac{|\{p_j : s_{ij} \geq t_s, id(p_j) = id(g_i)\}|}{|\mathcal{P}_G|}, \forall p_j \in \mathcal{P}_G, \quad (5)$$

and

$$P_{FA}(t_s) = \frac{|\{p_j : s_{ij} \geq t_s|}{|\mathcal{P}_N|}, \forall p_j \in \mathcal{P}_N, \forall g_i \in \mathcal{P}_G. \quad (6)$$

The results are shown in Table 2, where each row indicates a different choice of key length and codeword/feature length. As can be seen, the FAR is 0 in all cases, i.e., no non-matching subjects are incorrectly verified. This is because the Hamming distance between the binarized features of non-matching subjects is greater than what can be corrected by the corresponding BCH code for each scenario, which is the desired result. However, in most cases, the FRR is 1, indicating that the Hamming distance for matching subjects is also too great to be corrected. This is not desired since it means that no correct matching subjects can be correctly verified in those scenarios. Thus, the HDS-based biometric encryption system is not able to produce binary features similar enough (based on Hamming distance) except for very short keys.

Table 2. The isolated 1-to-1 verification performance of the HDS-based biometric encryption system.

Achievable key length (bits)	# of feature components (code length)	Feature components selection			
		By PCA energy		By reliability	
		FAR	FRR	FAR	FRR
16	**63**	0	0.8529	**0**	**0.3088**
22	127	0	0.9412	0	0.8824
21	255	0	1	0	1
19	511	0	1	0	1
36	**63**	0	1	**0**	**0.7941**
36	127	0	1	0	0.9853
37	255	0	1	0	1
40	511	0	1	0	1
64	127	0	1	0	1
71	255	0	1	0	1
67	511	0	1	0	1
131	255	0	1	0	1
130	511	0	1	0	1

Based on the results above, two scenarios are chosen for

simulation of the full watch list system. One is the 16-bit key with 63-bit codeword length using reliability based feature selection, which achieves (FAR,FRR) of (0,0.3088). The other is 36-bit key with 63-bit codeword length using reliability based feature selection, which gives (FAR,FRR) of (0,0.7941). The two choices are shown in bold fonts in Table 2. Nonetheless, it should be noted that in practice, 16-bit and 36-bit keys are considered too short to be used alone in cryptographic systems.

The full watch list recognition performance is shown in Table 1. Three operating points are simulated with rank list length $r = 5$, 10, and 20. For each operating point, two key lengths (16 and 36 bits) are tested. As shown in the table, due to the zero-FAR performance of the HDS-based biometric encryption module, the system is able to subsequently reduce the entire system FAR to zero, which is highly desirable. On the other hand, in all cases, the FRR is increased due to the biometric encryption module erroneously rejecting some correct matching subjects. This increase in FRR is more significant with longer keys.

Furthermore, it is observed that the overall performance at operating points OP5 and OP10 is the same. This indicates that the increase in length of the candidate identity list from 5 to 10 does not add correct matching subjects to the list that would be subsequently erroneously rejected by the biometric encryption module. However, when r is increased to 20, the FRR is modestly reduced, showing that correct matching subjects may rank low, but will be correctly verified by the biometric encryption module. Hence, as long as the biometric encryption module is able to maintain zero-FAR, increasing the length of the rank list r may prove to be a viable approach to reducing FRR. Nonetheless, the FRR can not be reduced to be below what the biometric encryption module is able to achieve in isolation (see Table 2), and a larger r increases the computational overhead of the biometric encryption system since up to r separate biometric encryption verification operations will have to be performed for each test subject.

4. CONCLUSIONS

This paper presents a combination of face recognition and simple biometric encryption using helper data system (HDS). The objective is to address the privacy concern in a self-exclusion scenario of face recognition. The HDS-based biometric encryption system is described in detail, with emphasis on the key binding module and bit allocation strategy. The experimental studies employ a subset of the CMU PIE face database. The HDS-based biometric encryption system has been simulated both in isolation (1-to-1 verification operation) and as part of the full watch list system. In isolation, the HDS-based system exhibited performance allowing the reliable binding of short keys. For the full watch list scenario, the HDS-based biometric encryption system has given improved FAR results compared to the system without biometric encryption, but with poorer FRR results.

Nonetheless, the HDS-based biometric encryption offers little flexibility and produces only one operating point ((FAR,FRR) pair) with no parameters to tune. In contrast, the biometric encryption system based on quantization index modulation (QIM) in [8] offers great flexibility and can generate a curve of operating points to give system implementers the freedom to control the operating point.

5. REFERENCES

[1] H. Lu, J. Wang, and K. N. Plataniotis, "A review on face and gait recognition: System, data and algorithms," in *Advanced Signal Processing: Theory and Implementation for Sonar, Radar, and Non-Invasive Medical Diagnostic Systems*, S. Stergiopoulos, Ed., pp. 303–330. CRC Press, Boca Raton, Florida, second edition, 2009, ISBN: 978-1-4200-6238-0.

[2] R. Hietmeyer, "Biometric identification promises fast and secure processing of airline passengers," *The International Civil Aviation Organization Journal*, vol. 55, no. 9, pp. 10–11, 2000.

[3] Stan Z. Li and Anil K. Jain, "Introduction," in *Handbook of Face Recognition*, Stan Z. Li and Anil K. Jain, Eds. 2004, pp. 1–11, Springer-Verlag.

[4] T. A. M. Kevenaar, G. J. Schrijen, M. v. d. Veen, A. H. M. Akkermans, and F. Zuo, "Face recognition with renewable and privacy preserving binary templates," in *Proc. IEEE Workshop on Automatic Identification Advanced Technologies*, October 2005, pp. 21–26.

[5] A. Cavoukian and A. Stoianov, "Biometric encryption," *Biometric Technology Today*, vol. 15, no. 3, pp. 11, Mar. 2007.

[6] Y. Wang and K. N. Plataniotis, "Fuzzy vault for face based cryptographic key generation," in *Proc. Biometrics Symposium 2007*, September 2007.

[7] C. Chen, R. N. J. Veldhuis, T. A. M. Kevenaar, and A. H. M. Akkermans, "Multi-bits biometric string generation based on the likelihood ratio," in *Proc. IEEE Int. COnf. on Biometrics: Theory, Applications, and Systems*, September 2007, pp. 1–6.

[8] Karl Martin, Haiping Lu, F. Bui, K. N. Plataniotis, and Dimitris Hatzinakos, "A biometric encryption system for the self-exclusion scenario of face recognition," *IEEE Systems Journal*, 2009, under review.

[9] J. P. Linnartz and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates," in *Proc. Int. COnf. on Audio and Video Based Biometric Person Authentication*, June 2003.

[10] I. Buhan, J. Doumen, P. Hartel, and R. Veldhuis, "Constructing practical fuzzy extractors using qim," Tech. Rep. TR-CTIT-07-52, Centre for Telematics and Information Technology, University of Twente, Enschede, 2007.

[11] P. Grother, R. J. Micheals, and P. J. Phillips, "Face recognition vendor test 2002 performance metrics," in *Proc. Int. COnf. on Audio and Video Based Biometric Person Authentication*, June 2003.

[12] M. Turk and A. Pentland, "Eigenfaces for recognition," *Journal of Cognitive Neurosicence*, vol. 3, no. 1, pp. 71–86, 1991.

[13] I. T. Jolliffe, *Principal Component Analysis*, Springer Serires in Statistics, second edition, 2002.

[14] H. Lu, K. N. Plataniotis, and A. N. Venetsanopoulos, "Uncorrelated multilinear discriminant analysis with regularization and aggregation for tensor object recognition," *IEEE Transactions on Neural Networks*, vol. 20, no. 1, pp. 103–123, Jan. 2009.

[15] J. Lu, K. N. Plataniotis, A. N. Venetsanopoulos, and S. Z. Li, "Ensemble-based discriminant learning with boosting for face recognition," *IEEE Transactions on Neural Networks*, vol. 17, no. 1, pp. 166–178, Jan. 2006.

[16] H. Lu, K. N. Plataniotis, and A. N. Venetsanopoulos, "A taxonomy of emerging multilinear discriminant analysis solutions for biometric signal recognition," in *Biometrics: Theory, Methods, and Applications*, N. V. Boulgouris, K.N. Plataniotis, and E. Micheli-Tzanakou, Eds. Wiley/IEEE, 2009, to appear.

[17] J. Daemen and V. Rijmen, "Aes proposal: Rijndael," 1999.

[18] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[19] R. Morelos-Zaragoza, *The Art of Error Correcting Coding*, Wiley, 2006.

[20] S. Lin and D. Costello, *Error Control Coding*, Prentice-Hall, second edition, 2004.

[21] William Press and Saul Teukolsky, *Numerical Recipes in C*, Cambridge University Press, second edition, 1992.

[22] T. Sim, S. Baker, and M. Bsat, "The CMU pose, illumination, and expression database," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 12, pp. 1615–1618, Dec. 2003.