A Biometric Encryption System for the Self-Exclusion Scenario of Face Recognition

Karl Martin, Haiping Lu*, Francis Bui, K. N. Plataniotis, Dimitris Hatzinakos
The Edward S. Rogers Sr. Department of Electrical and Computer Engineering
University of Toronto, M5S 3G4, Canada
{kmartin, *haiping, bui, kostas, dimitris}@comm.toronto.edu

Abstract

This paper presents a biometric encryption system that addresses the privacy concern in the deployment of the face recognition technology in real-world systems. In particular, we focus on a self-exclusion scenario (a special application of watch-list) of face recognition and propose a novel design of a biometric encryption system deployed with a face recognition system under constrained conditions. From a system perspective, we investigate issues ranging from image preprocessing, feature extraction, to cryptography, error-correcting coding/decoding, key binding, and bit allocation. In simulation studies, the proposed biometric encryption system is tested on the CMU PIE face database. An important observation from the simulation results is that in the proposed system, the biometric encryption module tends to significantly reduce the false acceptance rate with a marginal increase in the false rejection rate.

Index Terms

Biometric encryption, face recognition, self exclusion, watch list, security, privacy.

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.

I. INTRODUCTION

Biometrics refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics, such as faces [1], iris, and gait [2]. In this paper, we focus on the application of the face recognition technology. Face recognition is one of the three identification methods used in e-passports and it has an important advantage over other popular biometric technologies: it is non-intrusive and easy to use. Among the six biometric attributes considered in [3], facial features scored the highest compatibility in a machine readable travel documents (MRTD) system based on a number of evaluation factors, such as enrollment, renewal, machine requirements, and public perception [3].

Despite the various benefits, the use of biometrics can create significant security risks, especially when there are large centralized databases of biometric passwords. Therefore, there is a need for biometrics to be deployed in a privacy-enhanced way that minimizes the possibility of abuse, maximizes individual control, and ensures full functionality of the systems in which biometrics are used [4]. A new technology called biometric encryption emerged recently to address this concern. For the case of face recognition, with biometric encryption, instead of storing a sample of one's facial image in a database, we can use the facial image to encrypt or code some other information, like a PIN or account number, or cryptographic key, and only store the biometrically-encrypted code, rather than the facial image itself. This removes the need for public or private sector organizations to store actual biometric images in their database. Thus, most privacy and security concerns associated with the creation of centralized databases are eliminated. Biometric encryption allows an individual's biometric data to be transformed into multiple and varied identifiers for different purposes, so that these identifiers cannot be correlated with one another. Moreover, if a biometric identifier is somehow compromised, a completely new one may be easily generated from the same biometric data of an individual.

Among the earliest proposals to utilize biometrics as privacy enhancing solutions was the work by G. Tomko in 1994, which highlighted the concept of biometrics encryption [5]. An important component of biometric encryption is key binding, which is the process of securely combining a key using a biometric derived from some physiological features [6]. One challenge to this approach is the unreliability of the individual bits in the biometrics-based cryptographic key, due to the variance of the input and other distortion sources. Solutions for such biometrics-driven cryptographic systems have first been introduced more than a decade ago, with the biometrics-driven crypto proposal by Bodo [7]. Addressing the same challenge when using fingerprints, the Bioscrypt solution of Soutar *et al.* [8] utilizes the Fourier transform, and a phase-to-phase correlation to lock the biometric sample with a pre-defined random key. The

biometrics locking approach of [9] prevents recovery of the original fingerprints, but with the random keys externally specified. By extracting fingerprints' minutiae locations, Clancy *et al.* [10] applied the fuzzy vault approach of Juels *et al.* [9], which is a polynomial reconstruction method that guarantees obscuration of the key.

While the earlier solutions focused on fingerprints, other biometrics were subsequently utilized in constructing privacy enhancing systems. With face biometrics, a fuzzy vault based cryptographic key generation method was introduced by Wang *et al.* [11]. With iris biometrics, a cryptographic signature verification method without stored reference data was proposed by Davida *et al.* [12]. Other notable biometric encryption proposals and variants include the helper data system (HDS) proposed in 2005 [13], the multi-bit quantization using likelihood ratio method proposed in 2007 [14], and the quantization index modulation (QIM) approach, which is first introduced in 2003 [15] and further developed in 2007 [16].

In this work, we consider a self-exclusion scenario of face recognition, which is a special application of watch-list, in contrast with the more commonly studied verification or identification problems. The goal is to enhance privacy protection compared to traditional system designs. The operating scenario is to match a few enrolled subjects from a large number of customers, followed by manual intervention, e.g., by security guard. In this case, subjects have limited motivation to spoof enrolled subjects since the enrolled subjects will be denied access once identified, and positive matches are followed up by personnel rather than automatic action. Nonetheless, there could be incentives for an enrolled subject to spoof subjects not on the watch-list to avoid the "exclusion". Possible solutions to this kind of spoofing include liveness detection [17] and abnormal behavior screening by security personnel. There is a realistic design constraint that is often imposed in practical biometric systems: using an existing (traditional/commercial) face recognition system which cannot be directly altered. We propose a biometric encryption system that draws from a number of key technologies including biometrics, cryptography, pattern recognition, and communications theory. There is no previous work/system that can satisfy all the constraints and fit the specific operating scenario of self-exclusion. Therefore, although built upon existing literatures, this work has made improvement over the previous work mainly at the system-level, where the specific requirements of self-exclusion are considered and respective solutions are proposed based on existing works.

This paper is organized as follows. Section II describes the self-exclusion scenario of face recognition in detail and proposes a biometric encryption system for it that combines commercial face recognition system and biometric encryption technology. In Section III, the proposed system is presented in detail, component

by component including preprocessing, feature extraction, cryptographic key module, cryptographic hash function, error-correcting code module, key binding module, and bit allocation strategy. Section IV discusses the performance indicators. In Section V, simulation studies are presented and finally, Section VI concludes this work.

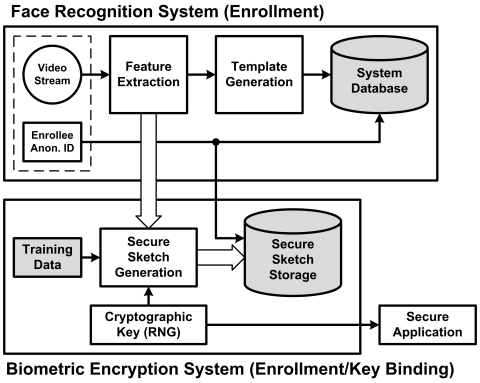
II. BIOMETRIC ENCRYPTION FOR THE SELF-EXCLUSION SCENARIO OF FACE RECOGNITION

This work was motivated by an Ontario Lottery and Gaming Corporation (OLG) initiative to evaluate facial recognition for its self-exclusion gaming initiative. The work is part of a system that attempts to solve the problem of identifying subjects in a self-exclusion program using facial recognition, while protecting the privacy of stored personal information. In this case, the personal information is considered to be the facial image itself, as well as application-specific meta-data related to the subject's identity.

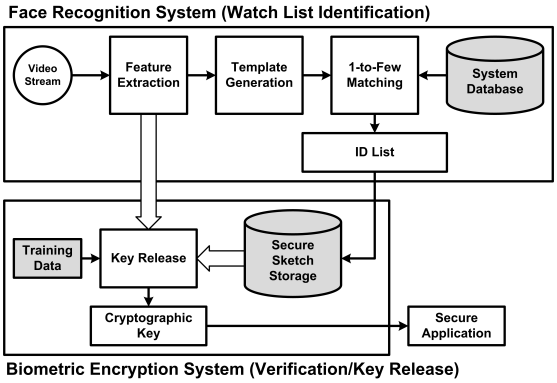
The self-exclusion initiative involves identifying voluntarily enrolled subjects who have entered a gaming facility, and contravened the terms of the program. In this case, the subjects entering the facilities do not provide claimed identities. In biometric recognition systems, this is termed the "watch list" scenario [18], which involves one-to-few matches that compare a query sample against a list of suspects. In this task, the size of database is usually very small compared to the possible queries, and the identity of the probe may not be in the database. Therefore, the recognition system should first detect whether the query is on the list or not and if yes, correctly identify it. In the self-exclusion scenario, the performance requirements (minimization) are placed on the false rejection rate (FRR), rather than the false acceptance rate (FAR). This is due to the OLG requirement that the system should identify as many enrolled subjects as possible.

There are two other common recognition tasks in biometric applications: verification and identification. Verification involves a one-to-one match that compares a query sample against the sample(s) of the claimed identity in the database. The claim is either accepted or rejected. Identification involves one-to-many matches that compare a query sample of an unknown person against the samples of all the persons in the database to output the identity or the possible identity list of the query sample. In this scenario, it is often assumed that the unknown (query) person belongs to the persons who are in the database. Currently known biometric encryption approaches only provide the equivalence of the verification task.

To offer the privacy protection properties of biometric encryption to the self-exclusion application scenario, the combined face recognition and biometric encryption approach shown in Fig. 1 is taken [19]. Figures 1(a) and 1(b) depict the proposed general enrollment and watch list identification systems, respectively. Subject identification is performed using a vendor-supplied face recognition system. A



(a) Enrollment and key binding



(b) Watch list identification and key release

Fig. 1. Combined face recognition system and biometric encryption.

biometric encryption module is then incorporated in order to offer privacy protection of the personal information by way of a bound cryptographic key which can be used with conventional cryptographic techniques to encrypt the subject's personal data for secure application.

As shown, the input during enrollment is the subject's facial image as well as a unique identifier (ID). This unique identifier should be anonymous and it must not directly relay private information about the subject (e.g., the subject's name should not be used). This identifier is simply used to connect the extracted facial feature record stored in the vendor-supplied identification database to a particular secure sketch in the biometric encryption system. The terminology "secure sketch" is introduced in [20] as a technique that can be used to reliably reproduce error-prone biometric inputs without incurring the security risk inherent in storing them. In enrollment, a secure sketch is generated as a result of binding the cryptographic key with the facial features. During watch list identification, the vendor-supplied system will attempt to match input subjects to those in the system database. If a match is made, the system will

output a claimed identity (ID) which is input into the face recognition based encryption system in order to release the key and subsequently access the protected private information.

In particular, it should be noted that this combined system is designed under two basic constraints: 1) The face recognition system will be a commercial system that cannot be modified at a low-level; 2) The biometric encryption module is used only for verification/key release. Therefore, the watch list identification is performed by the face recognition system alone and the verification/key release is then performed by the biometric encryption system. The face recognition system and the biometric encryption system work in cascade. In the next section, the proposed system will be described in detail.

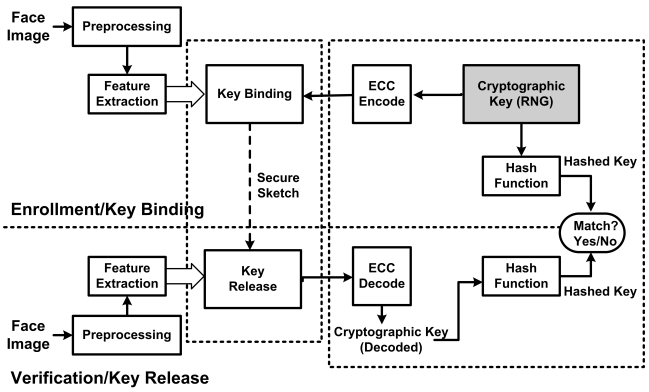


Fig. 2. Proposed biometric encryption system for enrollment (key binding) and verification (key release).

III. THE PROPOSED BIOMETRIC ENCRYPTION SYSTEM

The configuration of the proposed biometric encryption system is depicted in Figure 2, which is a generalization of the system diagram in [13]. As indicated in the figure, biometric 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 then be used for other security purposes. In order to support secure applications, other modules are constructed around the cryptographic key starting point. Graphically, this corresponds to a data signal flow from right to left in Fig. 2, starting with the cryptographic key module. After the starting point, 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 signals 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 secure sketch, to be used during verification. In the following, various modules are examined, with a focus on system-level

issues. Those modules that employ conventional techniques are described in brief while emphasis is put on the key binding module.

A. Facial image preprocessing

Facial image preprocessing is a necessary step for each facial image before feature extraction. The input is a raw facial image from the camera and the output is a facial image in a standardized format. The input facial images need to be normalized against variations which commonly occur, such as rotation, scaling, and dynamic range of pixel values. The stages in the facial image preprocessing pipeline include RGB to YCbCr colour transform, luminance component extraction, rotation, scaling, histogram equalization, masking and vectorization [1], [21].

B. Feature extraction

Feature extraction takes the standardized facial image as the input and output a set of features that are of much lower dimension than the facial image. There are a large number of feature extraction algorithms for face recognition proposed in the literature [1], [22], [23]. Since the focus of this work is biometric encryption, the simulation studies choose a baseline feature extraction algorithm, the PCA algorithm [24].

C. Cryptographic key module

The cryptographic key module is a random number generator producing a binary key. As a critical point in designing the system, the cryptographic key is essentially a binary string to be protected, i.e., securely stored and retrieved using other supporting modules in the pipeline. The key is to be used for a secure application, such as encrypting other subject-related data. A widely employed encryption method is the Advanced Encryption Standard (AES) [25], which is a symmetric scheme that has been adopted by various organizations as an encryption standard.

For practical usage, the AES key with the following three bit lengths are desirable: 128, 192 and 256, which are referred to as AES-128, AES-192 and AES-256, respectively. For AES key selection in the self-exclusion context, in general, the more stringent the security requirements, the longer the key should be. However, in a biometric encryption context, it should be noted that this security advantage can only be reaped if the underlying modules can support the specified key in the first place. If the associated biometric errors are unacceptably high, it would not be meaningful to specify an unachievable key requirement.

D. Cryptographic hash function

In the proposed system, instead of storing the actual key, its hashed version is stored. The cryptographic hash function takes the cryptographic key as the input and generates its hashed value as the output. The hash function has two related goals: (a) to conceal (making it computationally infeasible to recover) the cryptographic key in a secure sketch form suitable for storage; (b) to provide a secure comparison method for key verification. These two goals are the focus of the enrollment and the verification stages of the biometric encryption system, respectively. The hash function accepts a variable-length input, and produces a fixed-length output [26]. For the proposed system, SHA-256 is used as per NIST recommendation.

E. Error-correcting code module

The error-correcting code module takes the cryptographic key as the input and output an error-correcting coded version of it. This key will ultimately be utilized in an encryption algorithm, such as AES. It should be noted that the encryption-decryption procedure is an all-or-none process. In other words, if the keys, used during encryption and decryption, do not match exactly, the recovered data will be incorrect. Therefore, all bits in the two corresponding binary strings delivered by the underlying biometric system must be identical for successful decryption.

The feature vectors obtained during enrollment and verification differ due to various factors, e.g., inherent variability in pose, illumination, facial expressions, or environmental noise. This fuzzy variability results in errors when comparing the feature vectors. In the proposed system, error-correcting code (ECC) is adopted to take this into account.

In this work, the Bose, Chaudhuri, Hocquenghem (BCH) codes are used [27]. They 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. Relating these parameters to the requirements in the cryptographic key length (denoted by L) and the size of the feature vector to be generated from the feature extraction module, then n determines the number of bits to be bound with a feature vector, k determines the maximum number of bits in a cryptographic key (i.e., $L \leq k$), and t determines the number of bit errors allowed.

In addition, 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. For example, to support an AES key of L bits, BCH codes with $k \geq L$ are needed. In cases where multiple ECC options are available for a given key, the underlying feature extraction properties should be taken into account. For a particular BCH code, n bits

need to be bound with the feature vectors. Thus, it will affect the computational complexity and the feasibility of certain types of key binding strategies (e.g., the key binding strategy could fail if there is not enough useful components for binding all the n bits successfully).

F. Key binding module

The objective of the key binding module is to utilize a feature vector to securely bind the encoded cryptographic key, i.e., to generate a secure sketch for storage. Thus, the key binding module takes the feature vector from the feature extraction module and the encoded key from the ECC module as the input and output a secure sketch. For the chosen feature extraction algorithm (PCA), the number of components that can be kept depends on the reliability of the components. It should be noted that each specific choice of a key binding scheme and an ECC coding results in a specific system performance. In general, to support longer key sizes requires higher system complexity. These constraints are design issues that need to be taken into account for a practical system.

1) QIM-based biometric encryption: Here, we adopt the key binding method based on quantization index modulation (QIM) proposed in [15], [16]. In [15], a theoretical framework based on QIM was proposed for a one-bit-per-component key binding strategy. However, neither a complete system description nor practical simulation results were presented. This approach was subsequently extended in [16], which allowed for more practical biometric encryption design criteria to be considered.

In the self-exclusion context, the following implications when utilizing a QIM-based biometric encryption system can be noted. The secure sketch consists of continuous values, in contrast with the binary secure sketch in HDS [13]. QIM-based biometric encryption binds keys with feature vector through index modulation using a quantizer ensemble. In other words, the processes of feature binarization and key binding in many other biometric encryption systems [13], [14] are fused in QIM-based systems. No explicit feature binarization is performed as a distinct step. This makes system performance tuning more flexible.

The QIM design is applied after the feature extraction module. In utilizing a feature vector to securely bind the encoded cryptographic key (through ECC), i.e., to generate a secure template or sketch suitable for storage, QIM delivers several unique and advantageous properties [15], [16]. In particular, the QIM framework provides more flexibility in balancing the trade-off between FAR and FRR requirements. By varying the quantizer step size, it is possible to balance the security and reliability trade-off. This property is useful in designing practical biometric encryption systems, which are potentially subject to a wide range of operating conditions.

2) QIM encoding and decoding: Originally proposed for watermarking applications [28], the QIM construction can be viewed as binding or embedding a secret message (e.g., the encoded cryptographic key) using an ensemble of quantizers. The information to be embedded determines which quantizer needs to be used, as specified by an associated codebook. The QIM implementation using dither modulation [23] is chosen in this work. In this implementation, the quantization partitions and reconstruction points of the quantizer ensemble can be defined as shifted versions of a basis quantizer. The advantage is that the encoding and decoding procedures are simplified, due to the well-defined structure offered by the dither quantizers. In the following, the general mechanisms of QIM for key binding will be described.

In this work, we consider only the QIM on scalar values so we are binding the encoded key with the feature vector in a component-by-component fashion. For notational simplicity, the feature component to be bound is denoted by X and the encoded key segment to be bound is denoted by M. X is of real value and M is a binary number. A quantizer is a function Q that maps each point in the input space $\mathcal{X}$ into one of the reconstruction points in a set $\mathcal{C}$, where $\mathcal{C} \in \mathcal{X}$.

In an N-point QIM, there are an ensemble of N quantizers $\{Q_1, Q_2, ..., Q_N\}$ that can map a $X \in \mathcal{X}$ into one of the reconstruction points of the quantizer ensemble. $\mathcal{M}$ is a set of labels to index the quantizers with $|\mathcal{M}| = N$. $\mathcal{C}_M$ is the set of reconstruction points of quantizer Q_M. For $X \in \mathcal{X}$ and $M \in \mathcal{M}$, the QIM function becomes $QIM(X, M) = Q_M X$, i.e., the quantizer indexed by M is chosen. In the following, the QIM encoder and decoder are defined.

Definition 1: **Encoder**: from an enrollment feature component X and an encoded key segment M, a secure sketch W is obtained using the quantizer indexed by M as

$$W = Enc(X, M) = Q_M(X) - X. \tag{1}$$

Thus, the secure sketch W generated is the offset between the input and the closest reconstruction point of the quantizer Q_M.

Definition 2: **Decoder**: from a test feature component Y (obtained during verification) and a given sketch W, the decoder extracts the bound encoded key segment using a minimum distance scheme as follows

$$\hat{M} = Dec(Y, W) = \arg\min_{M} d(Y + W, \mathcal{C}_M), \tag{2}$$

where $d(\cdot)$ is an appropriate distance metric.

In other words, the decoder performs the following steps: (1) Compensates for the offset; (2) Searches for the closest reconstruction point from all the N quantizers; (3) The label M of the quantizer with the closest reconstruction point corresponds to the embedded message is the decoded key segment $\hat{M}$.

The described decoding scheme can be understood by observing that

$$Y + W = Y + Q_M(X) - X = Q_M(X) + (Y - X) = Q_M(X) + E, \tag{3}$$

where E can be interpreted as an equivalent additive noise. This noise represents the difference between the enrollment feature component X and the test feature component Y. If E is additive white Gaussian noise (AWGN), the appropriate distance metric to be used is simply the absolute value of E, $|E|$. The allowed difference between X and Y for successful verification (i.e., the tolerance) is:

$$|E| = |Y - X| < \delta/2 \tag{4}$$

where δ is the distance between two closest reconstruction points in the quantizer used. In that case, by searching for the reconstruction point that is closest (i.e., with the minimal distance) to $Y + W$, the secret quantizer label M (i.e., the encoded key segment) can be recovered.

3) Quantizer construction: The QIM framework described above establishes the approach in a general manner while it leaves open a lot of flexibility in the actual design of the quantizers. Generally, for the QIM approach, the size of the partitions chosen determines the trade-off between the FAR and FRR. As mentioned previously, the class of dither quantizers [28] is particularly advantageous, since the associated construction of the quantizer partitions is simplified. In this case, the number of quantizers in the ensemble is equal to $L = 2^{\kappa}$, where κ represents the number of information bits to be embedded.

When using dither lattice quantizers, the reconstruction points of the quantizers are all constructed as shifts of a base quantizer $Q_1 = [R_1, S_1]$, where R_1 and S_1 represent the quantization partition and reconstruction points, respectively. Then, the subsequent quantizers are computed with shifted codebooks. The minimum and maximum reconstruction points are respectively P_0 and P_1. The following construction is made:

$$R_1 = (P_0 + P_1)/2, \qquad S_1 = [P_0, P_1] \tag{5}$$

where

$$P_0 = \mu - (\rho \times \sigma), P_1 = \mu + (\rho \times \sigma) \tag{6}$$

and μ is the mean, σ is the standard deviation of the feature component, and ρ is a scaling factor.

The following observations can be made from the above design. With the assumption of a symmetric distribution of the feature components, the definition of P_0 and P_1 specifies an operating dynamic range of values. The value of ρ provides the tolerance for the quantizer ensemble as follows.

First, the remaining quantizers Q_2, Q_3, ..., Q_N are constructed as dither quantizers [28], with shift step-size $\delta = (P_0 - P_1)/N$.

In other words, these partitions and reconstruction points are all shifted by δ from the basis quantizer Q_1 for the remaining quantizers.

With the given design, we have the range of output secure sketch to be $|W| \leq (P_0 - P_1)/2$ for all inputs within the quantizer dynamic range (P_0, P_1), and the tolerance of the QIM decoder to be $|E| = |Y - X| < \delta/2$.

From the above, the quantizer range [P_0,P_1] should correspond to the dynamic range of the input features to be effective. This means, when the distribution is Gaussian, a range covering several standard deviations should contain a significant portion of the input range (specified by ρ). However, when this is not the case (depending on the type of data inputs as well as the feature extraction algorithm used), the values of ρ may need to be larger to deliver acceptable tolerance.

Furthermore, a Gray coding scheme [29] is adopted for mapping the quantizers to its label (or index) M so that for M as a binary encoded key segment, incremental changes in the feature vectors result in incremental changes in the recovered key.

4) Bit allocation: In addition, depending on how the feature components are used to bind a secret message, we can have different implementations of the key binding framework. There are two general strategies. In the "one-bit per component strategy", each component is used to embed one bit of the encoded key sequence. For example, when using a BCH code (255,131,18), in order to embed a 128-bit key, a codeword of 255 bits is generated by the ECC module. Then, at least 255 components are required for the one-bit per component procedure. In the "multi-bit per component strategy", each feature component is used to embed a variable number of bits from the encoded key sequence. For example, each component can be used to embed 3 bits of the encoded key. Then, to embed 128-bit cryptographic key (which is ECC-encoded to 255 bits), 85 feature components would be required. In all cases, the number of feature components that should be kept depends on the reliability of the components.

Bit allocation refers to the process of assigning an integer quantity of bits to be embedded into each of the biometric feature components. This usually applies to the multi-bit strategy. In general, there are two bit allocation approaches: uniform bit allocation and variable bit allocation based on component reliability. In the simulations here, we adopt the simple uniform allocation strategy only. Specifically, based on the total number of bits required to be bound (depending on the cryptographic constraint and the choice of ECC), equal number of bits are allocated to each retained feature component. This will often result in a number of bits remaining, which are then simply allocated to a few most reliable feature components. For example, if 500 feature components are used and an ECC codeword length of 1023 bits is used (i.e., 1023 bits need to be bound), then the first 23 components will be allocated 3 bits, and the

remaining will be allocated 2 bits.

G. Training requirements

In general, two main components in the biometric encryption system require training: feature extraction and key binding/release. The training requirements of the feature extractor vary depend on which algorithm is used. Usually, the feature extractor should be trained on images that match the general nature of the images to be used when the system is deployed (i.e., lighting, pose, and resolution). For the biometric encryption key binding/release, the training requirements generally involve calculating 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.

IV. Performance indicator

Biometric recognition system performance can be generally measured using two quantities: false acceptance rate (FAR) and false rejection rate (FRR). These values can commonly be varied by way of system parameter choices. The plot of FAR vs. FRR using different parameters generates what is known as the receiver operating characteristic (ROC) curve. However, these values have different definitions depending on whether identification, verification, or watch list is being performed. Following [18], we give their definitions for the two scenarios considered in the simulation studies presented in the next section: watch list and verification.

A. Performance indicator in the watch list scenario

In a watch list operation, enrolled subjects (the watch list) represent only a small subset of subjects which will be processed by the system. In this scenario, the system must attempt to detect whether a given subject entering the premises (termed a probe subject) is enrolled in the system and, if he or she is enrolled, identify that subject. When a positive detection and identification is achieved, this is considered acceptance in the system. Conversely, if detection fails, despite the subject being in the watch-list, then rejection has occurred.

Biometric templates are usually compared using a similarity measure. The detection performance is affected by the similarity threshold (t_s). Specifically, if a similarity measure s_{ij} is used to compare two biometric templates, X_i and X_j, then a positive detection is registered when $s_{ij} \geq t_s$.

Following detection, identification performance is affected by means of a ranking threshold, r, which determines how many of the enrolled subjects (which achieved positive detection when compared to the probe subject) may achieve positive identification.

A correct detection and identification is achieved when $s_{ij} \geq t_s$, $rank(p_j) \leq r$, and $id(p_j) = id(g_i)$, where p_j is a given probe subject, and g_i is a gallery subject enrolled in the system. In contrast, a false detection and identification is achieved when $s_{ij} \geq t_s$, $rank(p_j) \leq r$, and $id(p_j) \neq id(g_i)$. The probability of correct detection and identification is

$$P_{DI}(t_s, r) = |\{p_j : s_{ij} \geq t_s, rank(p_j) \leq r, \text{and} \\ id(p_j) = id(g_i)\}|/|\mathcal{P}_G|, \ \forall p_j \in \mathcal{P}_G, \tag{7}$$

where $\mathcal{P}_G$ represents the set of all gallery subjects and $|\mathcal{P}_G|$ is the number of gallery subjects. The probability of false rejection or FRR is: $P_{FR}(t_s, r) = 1 - P_{DI}(t_s, r)$. The other measure of performance is the FAR, which is measured as:

$$P_{FA}(t_s, r) = \frac{|\{p_j : \max_i s_{ij} \geq t_s|}{|\mathcal{P}_N|}, \forall p_j \in \mathcal{P}_N, \forall g_i \in \mathcal{P}_G, \tag{8}$$

where $\mathcal{P}_N$ is a set of imposter subjects. In other words, measuring across a set of imposter subjects, the FAR is determined by the fraction of those subjects exhibiting a similarity with a gallery subject greater than the threshold t_s.

In the context of the self-exclusion program, the performance requirements (i.e., minimization) are generally to be placed on the FRR, rather than the FAR. This may result in a large FAR, meaning that a potentially significant number of patrons who are not enrolled in the system will be falsely identified as being enrolled. In this case, the identified subjects would undergo a manual verification process by security personnel as long as this is manageable.

B. Verification performance

In 1-to-1 verification operation, the system must verify whether a probe subject matches a certain claimed identity (i.e., the identity output through face identification). When a positive verification is achieved, this is considered acceptance in the system. Conversely, if verification fails, then rejection has occurred.

As in the watch list scenario, the verification performance is affected by the similarity threshold (t_s). If a similarity measure s_{ij} is used to compare two biometric templates, X_i and X_j, then a positive verification is registered when $s_{ij} \geq t_s$.

Thus, a correct verification is achieved when $s_{ij} \geq t_s$ and $id(p_j) = id(g_i)$. A false verification is achieved when $s_{ij} \geq t_s$ and $id(p_j) \neq id(g_i)$. The measure of probability of correct verification is then

TABLE I

PROPERTIES OF THE SELECTED SUBSET FROM THE CMU PIE DATABASE.

Number of subjects	68
Number of images per subject	Minimum = 17; Maximum = 21
Resolution	70 pixels between eyes
Pixel representation	8 bits gray levels per pixel

defined as:

$$P_V(t_s) = \frac{|\{p_j : s_{ij} \geq t_s, id(p_j) = id(g_i)\}|}{|\mathcal{P}_G|}, \forall p_j \in \mathcal{P}_G. \quad (9)$$

The probability of false rejection or FRR is: $P_{FR}(t_s) = 1 - P_V(t_s)$. As in the watch list scenario, the other measure of performance is the FAR, which is measured as follows:

$$P_{FA}(t_s) = \frac{|\{p_j : s_{ij} \geq t_s|}{|\mathcal{P}_N|}, \forall p_j \in \mathcal{P}_N, \forall g_i \in \mathcal{P}_G. \quad (10)$$

V. SIMULATION STUDIES

This section presents simulation results of the proposed biometric encryption system. First, the simulation setup will be described, followed by the resulting baseline recognition performance without the application of biometric encryption, and finally the recognition performance of the system with the proposed biometric encryption modules.

A. Data and simulation setup

The simulations were performed on a subset of the Pose, Illumination, and Expression (PIE) database from Carnegie Mellon University (CMU) [30]. The CMU PIE database contains 68 individuals with face images captured under varying pose, illumination and expression. We choose three frontal poses (C07, C09, C27), under seven illumination conditions (06, 07, 08, 11, 12, 19, 20). Thus, there are about 21 (3×7) samples per subject (with some faces missing), which is not difficult in practice with voluntary and cooperative subjects using video camera. The properties of this CMU PIE subset are listed in Table I. This database was chosen over other available databases due to its large number of images per subject. Biometric encryption schemes usually depend on reliable intra-class (i.e., within subject) statistics which cannot be calculated using databases with a small number of images per subject. The simulations were performed using the MATLAB v.7.5.0 computing environment.

The database was partitioned into a gallery set containing all but one of the images for each of the subjects, and a probe set containing the single remaining image for each subject. The gallery set was

used for training the feature extractor and the biometric encryption modules as well as enrollment of the subjects. The probe set was used for testing the recognition performance. As mentioned earlier, PCA is the chosen feature extraction algorithm and it is trained on the gallery set. The first 154 PCA components were retained for each image, constituting 95% of the signal energy.

For the proposed biometric encryption approach, the biometric encryption module is first tested in isolation to determine the verification performance, and then as part of the whole system to test the performance in the watch list scenario. In the watch list scenario, the face recognition module produces a ranked list of candidate gallery subject identities for each probe subject tested, as shown in Fig. 1(b). This list of claimed identities for each probe subject is passed to the biometric encryption module where verification is performed on each one individually. The length of the list of claimed identities may vary between 0 (i.e., unidentified - no matching subject found in the gallery) and r (the maximum rank allowed for identification). The system parameter r is to be chosen based on the application requirements. The final output of the system is the cryptographic key for subjects producing positive verification.

B. Baseline watch list recognition performance

Since in the self-exclusion scenario, the watch list face recognition operation is to be performed, it is important to first establish a baseline level of recognition performance to which the system with biometric encryption will be compared. Thus, the baseline recognition performance under the watch list scenario was simulated first.

Using the definitions found in Section IV, each probe subject p_j is compared with each enrolled gallery subject g_i via a similarity metric s_{ij}. If s_{ij} is less than a given threshold t_s for all gallery subjects, then subject p_j is unidentified and rejected. If there are gallery subjects for which s_{ij} is greater than t_s, then all those subjects are ranked according to the value s_{ij} (i.e., greater similarity achieves higher rank) and the first r are returned.

The similarity metric used for classification is the normalized inner product, defined as follows:

$$s_{ij} = \frac{\langle X_i, X_j \rangle}{\parallel X_i \parallel \cdot \parallel X_j \parallel} = \frac{\sum_{k=1}^{N} X_i(k) \cdot X_j(k)}{\sqrt{\sum_{k=1}^{N} X_i(k)^2} \cdot \sqrt{\sum_{k=1}^{N} X_j(k)^2}} \tag{11}$$

where X_i and X_j are the N-component feature vectors from gallery subject g_i and probe subject p_j, respectively. This represents the cosine of the angle between the two vectors, with possible values ranging $[-1, 1]$. The greater the value of s_{ij} achieved, the more similar the two compared feature vectors are.

For a given r, a set of (FAR,FRR) value pairs are generated by varying the similarity threshold t_s. For the provided simulation results, t_s was linearly varied in the range $[-1, 1]$, with a total of 1000 points.

As shown in Fig. 3, the recognition performance was simulated for $r = 5$, 10, and 20.

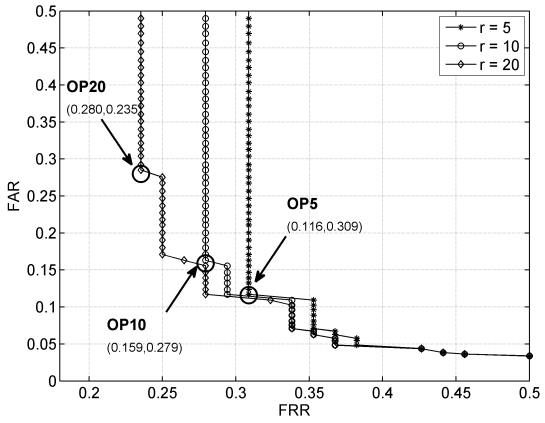


Fig. 3. Baseline watch list recognition performance using maximum rank $r = 5$, 10, and 20. The chosen operating points for each scenario are labeled OP5, OP10, and OP20, respectively.

It should be noted that the actual performance values (i.e., FAR and FRR) are not significant here, since they depend on the image database, the feature extractor, and the chosen classifier - some or all of which will be different in the practical operating scenario, depending on the choice of vendor. What is significant in these results is the demonstration of the effect that the choice of r has on recognition performance as well as the relative recognition performance compared to the system with biometric encryption.

It should be noted that the self-exclusion operating scenario requires minimal FRR since this represents the rate at which enrolled self-exclusion subjects would go undetected and allowed onto the gaming premises. This is in contrast to many other face recognition systems reported in the literature, which place an emphasis on minimizing FAR. As such, for each scenario, an operating point is chosen where FRR is minimized. These operating points must be fixed in order to simulate the entire system with the biometric encryption module in place. This is because the operating points determine the identification results to be passed on to the biometric encryption modules. The operating points are labeled in Fig. 3 and listed in Table II.

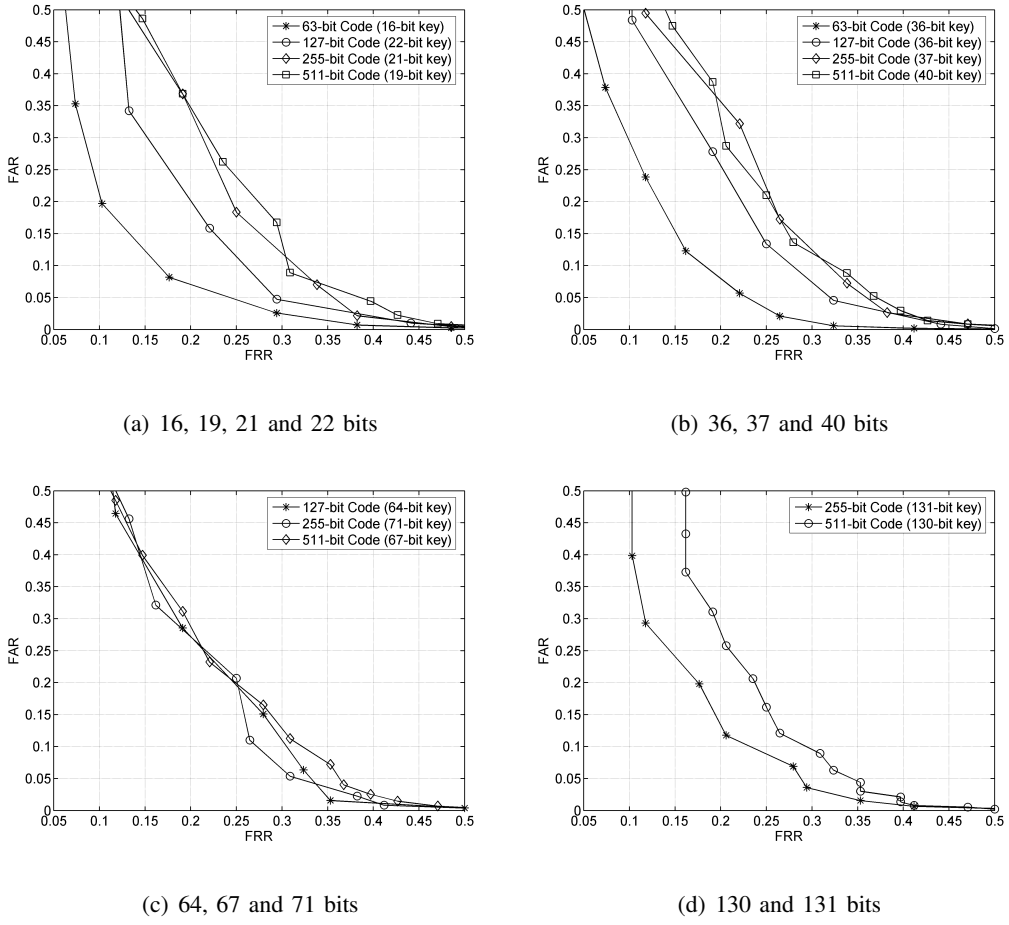
C. Performance of the proposed biometric encryption system

The recognition performance of the proposed QIM-based biometric encryption system is first simulated in isolation as a verification operation. The verification results are shown in Fig. 4, where the results are grouped according to the achieved key length. It should be noted that short keys are used here for

TABLE II

LIST OF WATCH LIST OPERATING POINTS

Operating point label	Rank list length r	Baseline performance	
		FAR	FRR
OP5	5	0.116	0.309
OP10	10	0.159	0279
OP20	20	0.280	0.235



(a) 16, 19, 21 and 22 bits

(b) 36, 37 and 40 bits

(c) 64, 67 and 71 bits

(d) 130 and 131 bits

Fig. 4. ROC curves for the isolated verification performance with various key lengths.

demonstrating the behavior of the system and some of the key lengths are not for practical use, such as a 16-bit key. The key length in this paper is constrained by the feature extraction method, PCA. This constraint could be alleviated through selecting an appropriate commercial face recognition product.

For keys with approximately the same length (as grouped in Fig. 4), it can be seen that shorter codeword

TABLE III

FOUR SELECTED CONFIGURATIONS FOR DIFFERENT KEY LENGTHS (BITS)

Achieved key length	Closest standard key length	Code length
16	16	63
36	32	63
64	64	127
131	128	255

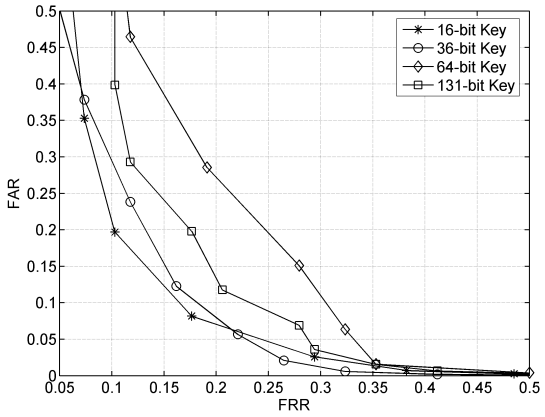


Fig. 5. ROC curves for the isolated verification performance with selected configurations for different key lengths.

length generally achieves better performance since using more low energy PCA components tend to make classification more difficult. Next, the configurations listed in Table III are selected for simulation of the full watch list system. The results from these four configurations are selected from Fig. 4 and shown in Fig. 5. It should be noted here that the verification performance in different cases are affected not only by the key length but also the respective ECC coding configuration and bit allocation scheme.

The full watch list system with the proposed QIM-based biometric encryption module was simulated using the selected operating points OP5, OP10, and OP20 and the four key length configurations described in Table III. The results are shown in Fig. 6. As can be seen, for all tested key lengths, the addition of the QIM biometric encryption module is able to provide improved recognition results, compared to the operating point without BE. Specifically, the use of the biometric encryption module is able to significantly reduce FAR while achieving approximately the same FRR.

D. Discussions

The proposed biometric encryption system is simulated both in isolation (1-to-1 verification operation) and as part of the full watch list scenario. In isolation, the proposed biometric encryption system exhibited performance allowing the reliable binding of short keys. While for the full watch list scenario, the proposed biometric encryption system has achieved improved FAR results compared to the system without biometric encryption. This could be understood by the fact that the biometric encryption module receives a candidate list of identities from the watch list module. Falsely accepted imposter subjects are placed on the list by the watch list module, while the biometric encryption module cannot add to this list. Thus, the biometric encryption module cannot increase the number of subjects falsely accepted. This is inherent in the system design that has the watch list module in series with the biometric encryption module. In all simulation cases, the biometric encryption module in fact rejected many imposter candidates, thus reducing the FAR. However, the equivalent implication of the system design is that the full system cannot achieve a lower FRR than the watch list module alone. This is because subjects falsely rejected by the watch list module cannot be placed back on the candidate list by the biometric encryption module. In fact, the biometric encryption module may falsely reject legitimate subjects placed on the candidate list, thus increasing the FRR.

Therefore, the simulation studies have shown the possibility of biometric encryption module to significantly reduce the FAR (from the watch list alone) with a marginal (or zero) increase in the FRR. In addition, the proposed biometric encryption system is able to produce a curve of operating points, offering system designers an important degree of freedom to choose the desirable operating point.

VI. CONCLUSIONS

This paper presents a biometric encryption system in an attempt to address the privacy concern in the deployment of the face recognition technology. A self-exclusion scenario of face recognition is the focus of this research, with a novel design of a biometric encryption system proposed, integrated with the face recognition technology. From a system perspective, various issues are studied, ranging from image preprocessing, feature extraction, to cryptography, error-correcting coding/decoding, key binding, and bit allocation. The proposed biometric encryption system is tested on the CMU PIE face database. Simulation results demonstrate that in the proposed system, the biometric encryption module tends to significantly reduce the false acceptance rate with a marginal increase in the false rejection rate.

ACKNOWLEDGMENTS

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.

REFERENCES

[1] J. Lu, K. N. Plataniotis, and A. N. Venetsanopoulos, "Face recognition using kernel direct discriminant analysis algorithms," *IEEE Trans. Neural Netw.*, vol. 14, no. 1, pp. 117–126, Jan. 2003.

[2] H. Lu, K. N. Plataniotis, and A. N. Venetsanopoulos, "MPCA: Multilinear principal component analysis of tensor objects," *IEEE Trans. Neural Netw.*, vol. 19, no. 1, pp. 18–39, Jan. 2008.

[3] 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.

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

[5] ——, "Biometric encryption: A positive sum technology that achieves strong authentication, security and privacy," *White Paper, Office of the Information and Privacy Commissioner of Ontario*, Mar. 2007.

[6] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," *Proc. IEEE*, vol. 92, no. 6, pp. 948–960, Jun. 2004.

[7] A. Bodo, "Method for producing a digital signature with aids of a biometric feature," German Patent DE 42 43 908 A1, 1994.

[8] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. V. K. V. Kumar, "Biometric encryption," *ICSA Guide to Cryptography*, pp. 649–6750, Mar. 1999.

[9] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proc. IEEE International Symposium on Information Theory*, 2002, p. 408.

[10] T. C. Clancy, N. Kiyavash, and D. J. Lin, "Secure smartcard-based fingerprint authentication," in *Proc. ACM Workshop on Biometrics: Methods and Applications*, 2003, pp. 42–52.

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

[12] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," in *Proc. IEEE Symposium on Security and Privacy*, May 1998, pp. 148–157.

[13] 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.

[14] 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.

[15] 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.

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

[17] K. Kollreider, H. Fronthalera, and J. Biguna, "Non-intrusive liveness detection by face images," *Image and Vision Computing Special Issue on Multimodal Biometrics*, vol. 27, no. 3, pp. 233–244, Feb. 2009.

[18] 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.

[19] A. Stoianov, private communication, Aug. 2007.

[20] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Advances in Cryptology - EUROCRYPT 2004*, ser. Lecture Notes in Computer Science, vol. 3027. Springer, 2004, pp. 523–540.

[21] H. Lu, "Multilinear subspace learning for face and gait recognition," Ph.D. dissertation, University of Toronto, 2008. [Online]. Available: https://tspace.library.utoronto.ca/handle/1807/16750

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

[23] G. Shakhnarovich and B. Moghaddam, "Face recognition in subspaces," in *Handbook of Face Recognition*, S. Z. Li and A. K. Jain, Eds. Springer-Verlag, 2004, pp. 141–168.

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

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

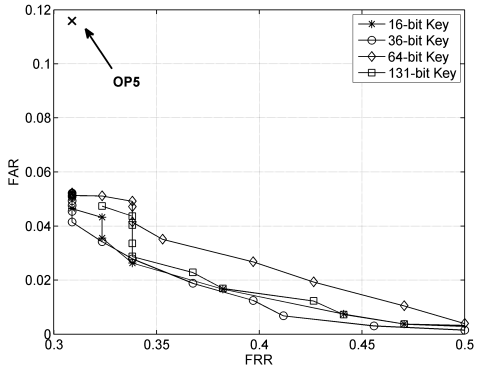
[26] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1997.

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

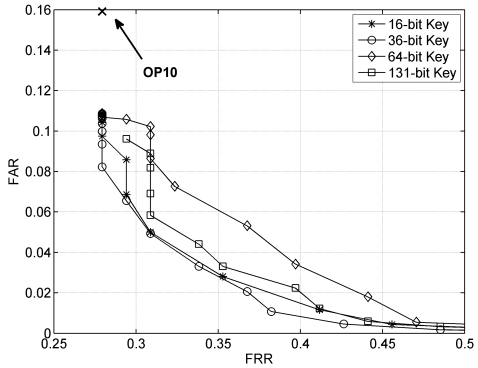
[28] B. Chen and G. W. Wornell, "Dither modulation: a new approach to digital watermarking and information embedding," in *Proceedings of SPIE Vol. 3657: Security and Watermarking of Multimedia Contents*, April 1999, pp. 342–353.

[29] W. Press and S. Teukolsky, *Numerical Recipes in C*, 2nd ed. Cambridge University Press, 1992.

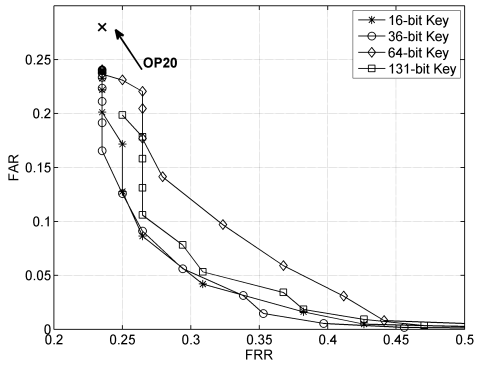
[30] T. Sim, S. Baker, and M. Bsat, "The CMU pose, illumination, and expression database," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 12, pp. 1615–1618, Dec. 2003.



(a) $r = 5$ operating point (OP5)



(b) $r = 10$ operating point (OP10)



(c) $r = 20$ operating point (OP20)

Fig. 6. ROC curves of the proposed biometric encryption system for the full watch list system with three operating points.