Fuzzy Key Binding Strategies Based on Quantization Index Modulation (QIM) for Biometric Encryption (BE) Applications

Francis Minhthang Bui, *Member, IEEE*, Karl Martin, *Member, IEEE*, Haiping Lu, *Member, IEEE*, Konstantinos N. Plataniotis, *Senior Member, IEEE*, and Dimitrios Hatzinakos, *Senior Member, IEEE*

***Abstract*—Biometric encryption (BE) has recently been identified as a promising paradigm to deliver security and privacy, with unique technical merits and encouraging social implications. An integral component in BE is a key binding method, which is the process of securely combining a signal, containing sensitive information to be protected (i.e., the key), with another signal derived from physiological features (i.e., the biometric). A challenge to this approach is the high degree of noise and variability present in physiological signals. As such, fuzzy methods are needed to enable proper operations, with adequate performance results in terms of false acceptance rate and false rejection rate. In this work, the focus will be on a class of fuzzy key binding methods based on dirty paper coding known as quantization index modulation. While the methods presented are applicable to a wide range of biometric modalities, the face biometric is selected for illustrative purposes, in evaluating the QIM-based solutions for BE systems. Performance evaluation of the investigated methods is reported using data from the CMU PIE face database.**

***Index Terms*—Biometric encryption (BE), biometric security and privacy, facial recognition, fuzzy key binding, quantization index modulation (QIM).**

I. Introduction

IN MANY engineering designs it is increasingly desirable, if not indispensable, to ensure provisions for security and privacy. However, many conventional methods, including various cryptographic protocols, are traditionally not designed with both security and privacy requirements. This implies that conflicting design constraints may arise by employing such methods. Recently, it has been established that the biometric encryption (BE) framework is a useful design approach for systems that support security as well as privacy [1]–[3]. A practical application of this framework is currently being investigated for the Ontario Lottery and Gaming Corporation (OLG) in order to implement its self-exclusion gaming initiative [4].

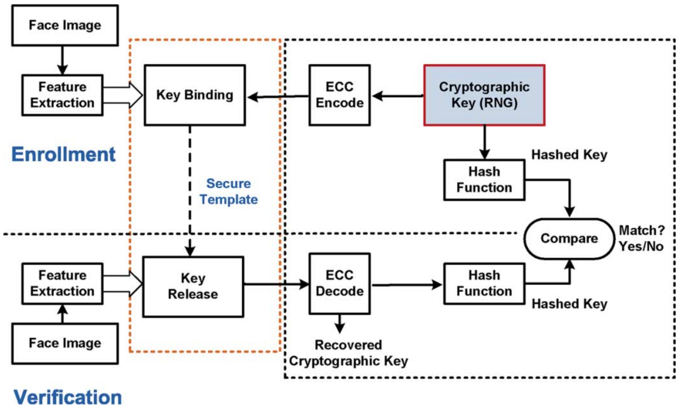


Fig. 1. BE system for key binding and key release.

As described in [4], and illustrated in Fig. 1, a complete system implementation requires a number of components to carry out various tasks, including operational blocks for image processing, feature extraction, random number generation, hash function, error-correction coding (ECC), etc. [5]–[7]. A system-level overview of these issues is presented in [4], with the expected conclusion that achieving good performance requires applying judicious design choices for all modules. In particular, both the biometric tasks of identification and verification are applicable in the considered framework. Identification is needed to perform one-to-many searches, while verification is required to perform one-to-one matches. It is important to note that the function of the key binding block is to implement verification, comparing a query sample against the sample(s) of the claimed identity in the database. Clearly, the key binding module depends on other preceding blocks for achieving good performance. Moreover, within the class of key binding methods, several alternatives are feasible. Fig. 1 situates the specific role of the key binding and corresponding key release blocks in an overall BE scheme. Essentially, the role of the key binding method is to securely combine a signal of interest (with sensitive information to be protected, e.g., a cryptographic key) with another signal (i.e., biometric signal)

Manuscript received May 21, 2009; accepted October 25, 2009. First published December 01, 2009; current version published February 12, 2010. The work presented in this paper was supported in part 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 associate editor coordinating the review of this manuscript and approving it for publication was Dr. Arun Abraham Ross.

F. M. Bui, K. Martin, K. N. Plataniotis, and D. Hatzinakos are with the Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, ON, M5S 3G4, Canada (e-mail: bui@comm.utoronto.ca; kmartin@comm.utoronto.ca; kostas@comm.utoronto.ca; dimitris@comm.utoronto.ca).

H. Lu was with the Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, ON, M5S 3G4, Canada. He is now with the Institute for Infocomm Research, Agency for Science, Technology and Research (A*STAR), Singapore 138632, Singapore (e-mail: hlu@i2r.a-star.edu.sg).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2009.2037662

derived from physiological features, such as facial images. The resulting combined signal is referred to as a secure template or sketch. The generated template is suitable for storage or archival, and should divulge neither the protected key (i.e., security criterion), nor the user information as exhibited by the physiological signal (i.e., privacy criterion).

It behooves us to remark that, while in the context of key binding [8]–[11], the term *sketch* has also been used when referring to the output of the key binding module; this usage should be distinguished from the class of secure sketch described in [12]–[14]. The secure sketch in the latter category takes as input the biometric signal itself to generate a key envisioned for cryptographic applications. By contrast, the binary cryptographic key is already present at the start of the key binding process (see Fig. 1). The secure template output is, therefore, destined for storage only, and not necessarily suitable as a cryptographic key.

The focus of this paper is on the key binding and release strategies, as well as the associated implementation issues for BE applications. Within the considered context, several relevant methods exist to implement key binding [4], [10], [15]. Based on the fuzzy commitment (FC) approach to realize the one-time pad principle [7], [16], the so-called Helper Data System (HDS) is a strategy that carries out key binding on a one-bit-per-feature-component basis [17]–[20]. In this case, binarization of the feature vector is explicitly needed, since an XOR operation is at the heart of this system. While the HDS system has the advantage of simplicity, it is limited in design flexibility due to the explicit binarization required. Indeed, given a set of binarized features, the system performance is essentially regulated by the selection of a suitable ECC scheme. This can be problematic, as ECC schemes typically admit rather restrictive structures (e.g., for a t-bit error-correcting code, not all values of t would be attainable [6]). As reported in [4], preliminary experimental trials with practical images when using the HDS approach do not lead to acceptable performance results, in terms of the false acceptance rate (FAR) and false rejection rate (FRR), with conventional ECC schemes. What is more, besides the limited ECC selection, other possibilities for tuning the achievable performance given a set of binarized features are not available with the HDS approach.

Another approach is based on Neyman–Pearson detection to implement a multibit likelihood ratio construction [21], [22]. In this case, a multibit nonuniform quantizer is applied for each component. The design of the quantizer is performed on a per-component and per-subject basis, and is based on formulating the biometric verification problem as a detection problem using Neyman–Pearson statistics [21]. Specifically, each component or a given subject is modeled as an independent Gaussian random variable both within the subject class, and the entire training population. Using this model and an estimation of the model parameters, a likelihood ratio is formed for each component. The quantizer is subsequently designed so that one of the quantizer regions is centered about the maximum likelihood, thus defining that quantizer region as the "acceptance region" for that subject-component. The remaining quantizer regions are defined such that they have equal mass across the population distribution. While this approach exhibits theoretical elegance, its performance results in practice are less optimistic due to various unsatisfied assumptions. Practical comparison results related to this scheme will be discussed later in Section VII.

Therefore, an alternative class of key binding methods addressing some of the described restrictions can be constructed using quantization index modulation (QIM), which is a particular realization of the dirty-paper coding principle for watermarking applications [23]–[25], and subsequently introduced for biometric systems in [8], [26]. The QIM construction can be viewed as binding or embedding of 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. It should be noted that the contributions of the previous works related to QIM applications in biometric systems have been mainly of a high-level systematic nature, with performance results limited to those of synthetic data [8], [10], [26]. Therefore, in this paper, the contributions involve adapting and extending the QIM approach to the BE framework of interest. Specific details regarding various relevant supporting modules, such as the quantizer design and bit allocation, will be presented. Furthermore, performance evaluation is practically investigated using face images from existing databases. The results obtained demonstrate that the QIM approach offers design flexibility in balancing the trade-offs in system performance (i.e., FAR and FRR), depending on the applications envisioned.

The remainder of the paper is organized as follows. In Section II, the general mechanism of QIM is presented, followed by its application for biometric key binding in Section III. Then, implementation issues related to the quantizer design, the bit allocation approaches and the performance characteristics of QIM are respectively described in Sections IV, V and VI. The performance evaluation results with facial images are presented in Section VII, followed by concluding remarks in Section VIII.

II. QIM Mechanism

As previously mentioned, the QIM method is originally targeted for watermarking applications, based on an ensemble of quantizers [24], [25]. In this work, the focus is on scalar one-dimensional quantizers. To this end, consider the following quantizer ensemble formulation.

Definition 1 (Quantizer Ensemble): A set of N quantizers $\{Q_1, Q_2, \ldots, Q_N\}$, where the nth quantizer Q_n has the code book C_n (of reconstruction points $q_{n,m}$) defined as

$$C_n = \{q_{n,m} | m \in \mathcal{M}\} \tag{1}$$

with $q_{n_1,m_1} \neq q_{n_2,m_2}$, $\forall n_1 \neq n_2$, $m_1 \neq m_2$, as well as, $q_{n,m_1} < q_{n,m_2}$, $\forall m_1 < m_2$, and $\mathcal{M} \subseteq \mathcal{Z}$. ■

In other words, the quantizer ensemble is defined to have quantizers with codebooks that are disjoint, and ordered in a monotonically increasing fashion. Also, the number of reconstruction points is countable (with countably infinite being a possibility). Then, the following QIM operation can be considered.

Definition 2 (QIM): The QIM function takes an input $u \in \mathcal{R}$ and a message $k \in \mathcal{K}$ to produce a reconstruction point q

$$q_k = \mathrm{QIM}(u, k) = Q_{b(k)}(u) = Q_n(u) = \arg\min_{q_{n,m_j}} \left| u - q_{n,m_j} \right| \tag{2}$$

which is the output of the quantizer indexed by k, being the reconstruction point of quantizer $Q_{b(k)} = Q_n$ that is closest to the input u. ■

The following assumptions are in effect:

1) u: A continuous signal (a real number).
2) k: A discrete message signal (a binary input vector), corresponding to a set of labels to index the N quantizers. The input signal sets are such that there exists a bijective mapping $b(\cdot)$ between the binary input set, and the index set of quantizer labels, i.e., $n = b(k)$, $n \in 1, 2, \ldots, N$, $k \in \mathcal{K}$. As discussed later, a Gray map can be effective.
3) q_k: A real number output, from the associated quantizer codebook C_n; the reconstruction points constitute a finite set of points selected from the space of input u.

Clearly, the cardinality of the discrete message signal set should be equal to N. Then, the discrete signal k serves as an indexed label to choose a particular quantizer Q_k to be applied to the given input u. In fact, given a QIM output $\tilde{q_k}$, which is possibly corrupted with noise (i.e., $\tilde{q_k} = q_k + \nu$, with ν being the additive noise), the identity of the quantizer used can be determined when ν is sufficiently small as follows.

Definition 3 (QIM Inverse): Since the codebooks are disjoint, an associated decoder can find the quantizer used. This is achieved by locating the quantizer index associated with the quantizer which yields the smallest difference between its reconstruction point and the given QIM output

$$n = \arg\min_{n_i} \left|\tilde{q_k} - q_{n_i,m_j}\right| \tag{3}$$

from which the embedded message $k = b^{-1}(n)$. ■

Note that for this current QIM formulation, the continuous signal u is not needed in the decoder. As such, while the message k is certainly contained in the output q_k, it is not embedded in a secret manner, i.e., q_k is not a qualified secure template. Indeed, in the absence of noise, $\tilde{q_k}$ is deterministically and exactly linked to a reconstruction point of the quantizer used. In fact, an alternative feasible decoder that needs neither the original feature component u nor the template q_k can be achieved, with different performance behavior compared to that in (3), as follows.

Definition 4 (Alternative QIM Inverse): Given an arbitrary QIM output, possibly corrupted with noise $\tilde{q_k}$ the index label can be located as

$$n = \arg\min_{n_i} \left|Q_{n_i}(\tilde{q_k}) - \tilde{q_k}\right| \tag{4}$$

from which the embedded message $k = b^{-1}(n)$. ■

In addition, there are privacy concerns to be considered. Since q_k is basically a quantized version of u (which, in application, corresponds to the original physiological signal from a user), the difference between u and q_k may not be significant. And depending on how u is encoded from the physiological features, it may preserve sufficient original data, to the extent that private information contained in u regarding the user would then also be revealed in q_k. This also implies that retaining q_k would not be acceptable from a privacy-protection perspective [1], [10]. Therefore, in its unmodified form, this construction of storing the quantized output value does not seem directly amenable to key binding. In Section III, it is shown that the existing QIM function can be modified as a building block to generate a secure template for key binding.

III. QIM-Based Key Binding

In this section, the application of QIM for key binding [8], [26] is described. The secure template produced by the key binding encoder should preserve the original cryptographic key, i.e., the key should be recoverable from the template. However, the recovery must only be feasible if certain controlled criteria are satisfied. In biometric parlance, the enrollment stage consists of: 1) collecting the physiological signal u from the user, 2) generating a binary input vector k (representing a cryptographic key), and 3) combining the signal collected from the user with the key k. Correspondingly, the verification stage consists of: 1) collecting the physiological signal u' from a test subject, and 2) attempting to perform key release of k, based on the collected signal u' and the stored secure template. The verification should only be successful if the test subject is in fact the original user during enrollment.

A. QIM Encoder for Key Binding

For the purpose of simplicity and clarity, it should be noted that this section focuses on the encoding and decoding of a particular feature component of a feature vector. When applying to a general feature vector, the number of key bits bound by each feature component needs to be allocated. Such bit allocation strategies will be addressed in Section V. Consider the following notational definitions (analogous to the variables in Section II).

1) u: A real-valued biometric feature component (used for key binding during enrollment).
2) u': A real-valued biometric feature component (obtained during verification for key release).
3) k: A binary input key to be bound; in the context considered, k consists of a segment of the ECC encoded cryptographic key (see Fig. 1), as given by the bit allocation strategy (e.g., in Section V). Also, $\mathcal{K}$: the set of all possible inputs k with the given bit segment length.
4) $\{Q_i\}_{i=1}^{N}$: An ensemble of N quantizers.

As before, the number of quantizers is designed to be $N = |\mathcal{K}|$, i.e., the cardinality of the set of all possible keys (so that a bijective mapping $b(\cdot)$ exists).

Definition 5 (QIM Encoder for Key Binding): The encoder produces a secure template, from an input key segment k and a biometric component u

$$w_{k,u} = \mathrm{Enc}(u,k) = \mathrm{QIM}(u,k) - u = q_k - u. \tag{5}$$

Thus, the encoded template $w_{k,u}$ is the offset between the input u and the closest reconstruction point q_k of the quantizer Q_k. ■

Fig. 2 summarizes the high-level structure of the encoder for QIM key binding. Clearly, with perfect knowledge of u, the situation is similar to that in (3) after offset compensation, from which the output $w_{k,u}$ can be used to recover k. On the other hand, knowledge of $w_{k,u}$ alone (i.e., without u) does not always imply knowledge of either k or u. In other words, $w_{k,u}$ is a feasible candidate for a secure template, suitable for storage purposes while protecting the privacy of the enrolled subject.

B. QIM Decoder for Key Release

At the decoder, the biometric signal u' extracted from a test subject is used to execute the following operations on the secure template $w_{k,u}$.

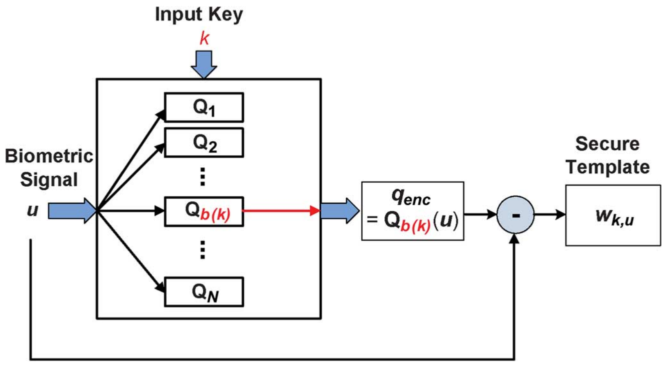


Fig. 2. QIM encoder for key binding.

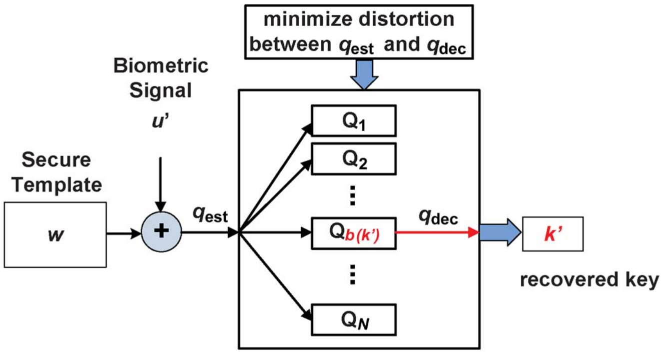


Fig. 3. QIM decoder for key release.

Definition 6 (QIM Decoder for Key Release): The quantizer label, associated with the quantizer used for embedding, is first identified as

$$n' = \arg\min_{n_i} d\left(u' + w_{k,q}, q_{n_i,m_j}\right) \tag{6}$$

(note that the above optimization is performed over all quantizers, and all reconstruction points for each quantizer) from which the message embedded is recovered as

$$k' = \mathrm{Dec}(u', w_{k,u}) = b^{-1}(n') \tag{7}$$

where $d(\cdot,\cdot)$ is an appropriate distance metric (e.g., Euclidean distance), and $b^{-1}(\cdot)$ is the inverse label mapping operation. ■

Fig. 3 summarizes the corresponding decoder structure. In other words, the decoder performs the following actions: 1) compensates for the offset; 2) searches for the closest reconstruction point from all quantizers in the ensemble; 3) returns the message k' associated with the label of the quantizer with the closest reconstruction.

When the similarity between u and u' is sufficiently high, these steps successfully extract the originally bound key k from the secure template $w_{k,u}$. In Sections IV and VI, the conditions and implications under which the key release can be achieved will be examined in more detail.

IV. Quantizer Design

The QIM framework in the literature, as described in Section III, establishes the approach in a general manner. In other words, it leaves open the flexibility of designing the actual quantizers to be used. Generally, for the QIM approach, the size of the partitions chosen determines the trade-off between the FAR and FRR. The class of uniform lattice quantizers [8], [25] is particularly advantageous, since the associated construction of the quantizer partitions is simplified.

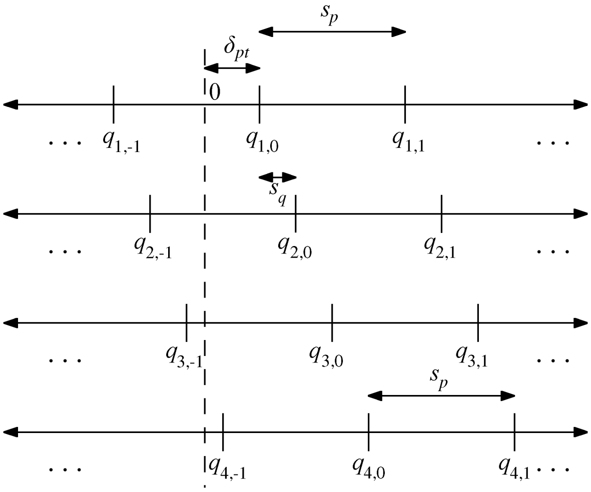


Fig. 4. Uniform quantizer ensemble with $n_b = 2$.

Definition 7 (Uniform Quantizer Ensemble): Let the number of quantizers in the ensemble be $N = 2^{n_b}$, where n_b represents the number of information bits to be bound. The codebooks of all the quantizers are shifted versions of a base quantizer codebook C_1. Define a shift parameter $s_q > 0$ (corresponding to the shift step-size between consecutive quantizers), and let base quantizer codebook be

$$C_1 = \{q_{1,m}|m \in \mathcal{M}\} = \{mNs_q + \delta_{pt}|m \in \mathcal{M}\} \tag{8}$$

where m is the reconstruction point index, and δ_{pt} (with $|\delta_{pt}| < s_q$) represents the offset from the point 0. Then the remaining codebooks are shifted by s_q

$$C_n = C_1 + ns_q = \{(n + mN)s_q + \delta_{pt}|m \in \mathcal{M}\}. \tag{9}$$

■

The above definition implicitly assumes that the point 0 is located within a finite (nonboundary) quantizer partition. This is so that a zero-point reference exists for brevity of proof. For a quantizer ensemble without this property, the relevant discussions can be readily modified to focus instead on a reference point within a particular finite quantizer partition (e.g., in Example 1, the reference point corresponds to the mean value). Fig. 4 illustrates an example quantizer ensemble for the case of $n_b = 2$.

By design, for the first quantizer Q_1, the positive reconstruction point closest to 0 is $\delta_{pt,1} = \delta_{pt} = q_{1,0}$, from which the negative reconstruction point closest to 0 is

$$\delta_{nt,1} = q_{1,-1} = \delta_{pt} - Ns_q = \delta_{pt} - 2^{n_b}s_q. \tag{10}$$

When $\mathcal{M} = \mathcal{Z}$, the set of integers, the quantizer consists of infinitely many reconstruction points and partitions, where the size of a partition is $s_p = Ns_q = \delta_{pt,n} - \delta_{nt,n}$ (i.e., the partition size is the same for all quantizers in the uniform ensemble). It is easy to see that, for each quantizer Q_n, the corresponding quantizer partitions are also shifted versions of the base partitions

$\{q_{n,-1}, q_{n,0}\}$. When $\mathcal{M} \subset \mathcal{Z}$, the scenario is similar except for the two boundary partitions: the two left-most and right-most partitions range respectively as $\{-\infty, q_{\text{left-most}} + s_q/2\}$ and $\{q_{\text{right-most}} - s_q/2, \infty\}$.

Proposition 1 (QIM Encoder): Corresponding to (5), the output of the QIM encoder has the following form for the uniform quantizer ensemble:

$$w_{k,u} = \begin{cases} -\Delta, & |\Delta| < \frac{s_p}{2} \\ s_p - \Delta, & |\Delta| > \frac{s_p}{2} \end{cases} \tag{11}$$

where Δ is an appropriately defined quantity with $|\Delta| < s_p$

Proof: In the following, we consider the case of $\mathcal{M} = \mathcal{Z}$ specifically, from which the $\mathcal{M} \subset \mathcal{Z}$ case follows in a straight-forward manner by tackling the left-most and right-most partitions as needed. For a particular quantizer $Q_n = Q_{b(k)}$, let us focus on the partition that includes the origin 0, namely $\{\delta_{nt,n}, \delta_{pt,n}\}$. Consider the quantity

$$\hat{q_k} = \left\lfloor \frac{u - \delta_{nt,n}}{s_p} \right\rfloor \tag{12}$$

which represents the number of quantizer steps away from base. Then the QIM function (2) can be explicitly represented as (recall the label mapping operation $n = b(k)$ is applied)

$$q_k = \text{QIM}(u, k) = \begin{cases} \hat{q_k} s_p + \delta_{nt,n}, & |\Delta| < \frac{s_p}{2} \\ (\hat{q_k} + 1) s_p + \delta_{nt,n}, & |\Delta| \geq \frac{s_p}{2} \end{cases} \tag{13}$$

where

$$\Delta = u - (\hat{q_k} s_p + \delta_{nt,n}). \tag{14}$$

Due to the definition of $\hat{q_k}$ in (12), Δ is bounded, with $|\Delta| < s_p$, which is the size of a partition. In addition, from (5), the output of the QIM encoder is $w_{k,u} = q_k - u$, so that

$$w_{k,u} = \begin{cases} \hat{q_k} s_p + \delta_{nt,n} - u, & |\Delta| < \frac{s_p}{2} \\ (\hat{q_k} + 1) s_p + \delta_{nt,n} - u, & |\Delta| > \frac{s_p}{2} \end{cases} \tag{15}$$

from which the required result follows immediately. ■

Before deriving the decoder operations, let us reconsider the objectives of the key binding and corresponding key release schemes. First, the key release should be successful for feature components sufficiently close to the original value u used, while rejecting components farther away from u. As will be seen shortly, when the original u is not available (i.e., not stored in the database to preserve user privacy, since u represents the physiological features of a user), additional constraints need to be placed on the quantizer encoder in order to realize this goal. Furthermore, it is also clear that the secure template $w_{k,u}$ should not leak information regarding the original key k embedded. Addressing this criterion requires design constraint on the quantizer step-sizes. Therefore, the described two issues of bounded constraint and secrecy preservation will be examined respectively in the following.

Proposition 2 (QIM Decoder): Corresponding to Definition 6, the QIM decoder for a uniform quantizer ensemble admits a *modulo*-operation formulation.

Proof: Focusing once again on the case of $\mathcal{M} = \mathcal{Z}$ for illustrative purposes, the decoder used to realize (6) is

$$n' = \arg\min_{n_i} |u' + w_{k,q} - [(n_i + mN)s_q + \delta_{pt,1}]| \tag{16}$$

with $m \in \mathcal{M}$, which searches through all quantizers and reconstruction points to locate the most probable quantizer label. The above function can also be equivalently achieved with a *modulo*-type operation, when a uniform quantizer ensemble is used

$$n' = \text{round}\left(\frac{w_{k,u} + u' - \delta_{nt,1}}{s_q}\right) \bmod N + 1 \tag{17}$$

from which $k' = b^{-1}(n')$. ■

However, the inherent *modulo* operation in the decoder means that if a particular signal component u' produces successful key release with $n' = n$, and $k' = k$, then a subject presenting a signal component

$$\hat{u} = u' + l s_q N, \quad l \in \mathcal{Z} \setminus \{0\} \tag{18}$$

also successfully releases the key $k' = k$. On the other hand, a subject presenting a signal component $\breve{u} = u' + \zeta s_q$, with $0.5 < \zeta < 1$, will release a different key $k' = b^{-1}(n+1) \neq k$. And since $N \geq 2$ ($N = 2$ for embedding one bit of information)

$$|\hat{u} - u| - |\breve{u} - u| = |(u + \eta) + l s_q N| - |(u + \eta) + \zeta s_q| > 0 \tag{19}$$

where $u' = u + \eta$, with $|\eta| < s_q/2$ being the (same) noise value for u' to successfully release k (actually, it may also be *modulo* N). As such, a signal component that is further away from the original signal, viz., $\hat{u}$, may be accepted, while one that is closer, viz., $\breve{u}$, may be rejected (as it should be).

In biometric parlance, this means that a false acceptance occurs in the case of $\hat{u}$. To take this issue into account more formally, let us consider the following notion of an unambiguous decoder system.

Definition 8 (Decoder Ambiguity): A decoder is said to be *unambiguous* if it has an acceptable region, i.e., the set of verification signals successfully releasing the bound key, that is singularly connected (consisting of only a single interval in the one-dimensional case). In other words, no *modulo*-type ambiguity can exist. More precisely, suppose the signal component used during enrollment is u, then there exists a finite $\epsilon > 0$ such that the acceptable region is defined as $\{u' : |u' - u| < \epsilon\}$. By contrast, any u' such that $|u' - u| > \epsilon$ belongs to the rejection region.

On the other hand, a decoder is ambiguous if the acceptable region consists of multiple (disconnected) intervals. The number of intervals present in the acceptable region is referred to as its *multiplicity*. In this sense, an unambiguous decoder can be said to have an acceptable region with multiplicity of 1. ■

Clearly, the decoder in Proposition 2 for $\mathcal{M} = \mathcal{Z}$ is not unambiguous (in fact, it has infinite multiplicity). Reverting to the unsimplified form in (16), a solution to rectify this undesirable scenario may entail restricting the decoder to consider only reconstruction points in the partition enclosing the signal component under verification. In other words, m should be a single value corresponding to the relevant partition. But, when considering two different signal components $\hat{u}$ and $\breve{u}$, this is only appropriate if the two components are both in the same partition, ideally in the same partition containing u (otherwise both should be rejected). However, this naive solution does reveal the necessary constraint: to prevent false acceptance due to the inherent *modulo*-ambiguity, the quantizer ensemble should all be limited to the same partition range. In other words, the source of ambiguity stems from the fact that the quantizer has an excess of reconstruction points. To this end, the following notion is useful.

Definition 9 (Truncated Quantizer Ensemble): A quantizer ensemble in which the constituent quantizers consist of a finite number of reconstruction points. Moreover, the number of reconstruction points for each of the quantizer may differ.

In other words, corresponding to Definition 1, $\mathcal{M} \subset \mathcal{Z}$ (i.e., a strict subset). The possibly varying number of reconstruction points can be stated as

$$C_n = \{q_{n,m} | m \in \mathcal{M}\} = \{mNs_q + \delta_{pt} | m \in \mathcal{M}_n\} \quad (20)$$

where $\mathcal{M}_n \subset \mathcal{Z}$. ■

In effect, the truncated ensemble limits the number of reconstruction points in each of the quantizers. We will consider the problem of finding the required cardinalities of the sets $\mathcal{M}_n$ later, in Proposition 7. But at this point, we have the following result.

Proposition 3 (Ambiguity Characterization): Consider a truncated uniform quantizer ensemble. Let the maximum number of reconstruction points in the quantizer be l (i.e., there exists at least one quantizer in the ensemble with l reconstruction points). Then l determines the multiplicity of the decoder ambiguity (from Definition 8). In other words,

1) $l = 1$: an unambiguous decoder exists;
2) $l \geq 1$: an ambiguity of up to ls_p in the signal amplitude for the acceptable set is present, with multiplicity of l.

Proof: The proof follows readily from *modulo* characterization in Proposition 2. If $l = 1$, there is only one reconstruction point for each quantizer, so that no *modulo* ambiguity exists.

On the other hand, when $l > 1$, then in the quantizer with the maximum number of points, the boundary reconstruction points lead to an ambiguity. That is, if a signal u' is accepted, then a signal of $u' + ts_p$, with $t = 1, \ldots, l-1$ is also accepted in this quantizer. As a result, an acceptable point occurs with multiplicity l, creating l different intervals in the (disconnected) acceptable region. ■

Minimizing the ambiguity multiplicity is evidently desirable. However, limiting the number of reconstruction points for this purpose also introduces new issues. In particular, the size of the partition s_p, and the location of the reconstruction points on the number line need to be properly selected. For these issues, the notion of secrecy preservation previously alluded to is relevant. It will be seen that there is a trade-off between resolving the ambiguity and controlling the amount of secret information leakage. To this end, the following definition of functional secrecy is useful.

Definition 10 (Functionally Secret System): A key binding system in which the output template does not deterministically reveal the quantizer, or correspondingly the input message, used. That is, there is no value of $w_{k,u}$ that deterministically identifies the quantizer used. ■

In other words, an attacker should never be able to use only the output $w_{k,u}$ to extract k. However, it should be noted that this definition is rather relaxed in that it imposes no qualification regarding the possible bias between various quantizers in the ensemble. In Section VI, a stronger notion of unbiased secrecy will be explored. It is worthwhile to emphasize that functional secrecy should be the minimal requirement for a key binding scheme.

Corollary 1 (Functional Secrecy Characterization): To be functionally secret, the observed ranges of the encoder output, conditioned upon the quantizer used, must be identical.

Proof: Clearly, if there are output values that can only be uniquely found due to a particular quantizer, then whenever those values occur, that quantizer identity is deterministically leaked or revealed. Therefore, functional secrecy is violated in such cases.

However, in order to further motivate the relevance and utility of this corollary, a constructive counterexample will be actually given in the following. We will show, for a specific counterexample, that when the quantizer ensemble leads to the observed output ranges depending on the quantizer used, then functional secrecy is invalidated.

First, denote the maximum and minimum input values to the key binding system, respectively, as $u_{\max}$ and $u_{\min}$. Without loss of generality, assume that the point 0 is within this range (otherwise, perform a linear shift with respect to the mean). Then, consider the following construction of a quantizer ensemble with $N = 2$. Let the quantizer shift be $s_q = u_{\max} - u_{\min}$, and the offset be $\delta_{pt} = \bar{u} + s_q$, where $\bar{u} = (u_{\max} + u_{\min})/2$. In other words, the base partitions for the two quantizers in the ensemble are designed with reconstruction points

$$\bar{C_1} = \{q_{1,-1}, q_{1,0}\} = \{\bar{u} - s_q, \bar{u} + s_q\} \quad (21)$$
$$\bar{C_2} = \{q_{2,-1}, q_{2,0}\} = \{\bar{u}, \bar{u} + 2s_q\}. \quad (22)$$

In fact, due to construction, only the base partitions will be used for the given input range $[u_{\min}, u_{\max}]$. Also, the observed output values $w_{k,u}$ of the key binding system take on the ranges for the first and second quantizer, respectively, as

$$\begin{aligned} QR_1 &= [q_{1,-1} - \bar{u}, q_{1,-1} - u_{\min}] \cup [q_{1,0} - u_{\max}, q_{1,0} - \bar{u}] \\ &= [-s_q, -s_q/2] \cup [s_q/2, s_q] \end{aligned} \quad (23)$$

and

$$QR_2 = [q_{2,-1} - u_{\max}, q_{2,-1} - u_{\min}] = [-s_q/2, s_q/2]. \quad (24)$$

Therefore, the two output ranges due to two different quantizers are not identical: $QR_1 \neq QR_2$. As a result, output values that are unique to a specific quantizer will deterministically identify the quantizer.

In fact, for the considered example, except the boundary points, the two ranges are disjoint. As such, there exist output values $w_{k,u}$ for which the quantizer identification is deterministically revealed or leaked. For example, values of $w_{k,u} \in (s_q/2, s_q)$ deterministically identify the quantizer as Q_1, whereas $w_{k,u} \in (-s_q/2, s_q/2)$ imply the quantizer Q_2. Clearly, the key binding system based on this quantizer ensemble is not functionally secret. ■

The preceding constructive proof is actually a specific case of the following result.

Proposition 4 (Partition Size and Functional Secrecy): If the quantizer partition size $s_p = Ns_q$ is sufficiently large so as to completely contain within a single partition the input dynamic range, i.e., $|u_{\max} - u_{\min}| < s_p$, then the resulting key binding system is not functionally secret.

Proof: With an ensemble of N quantizers, it suffices to show that the quantizer identity is revealed for any pair of quantizers. It will be shown that the output ranges are not identical for this pair of quantizers, whence functional secrecy is violated (by Corollary 1).

The proof is partially similar to the one presented in Corollary 1. Therefore, for clarity and notational brevity, it is assumed that the base partition of the base quantizer Q_1 and the input value range are aligned together with the same center point so that

$$\bar{u} = \frac{u_{\max} + u_{\min}}{2} = \frac{q_{1,-1} + q_{1,0}}{2}. \tag{25}$$

This corresponds in fact to a symmetric alignment of the dynamic range and the quantizer partition, and is evidently most effective for symmetric input distributions. However, when this condition is not true, a straightforward modification to the proof presented below can be made to account for the offset from the center.

Proceeding with the case of the same center, we have the range of the first quantizer Q_1 as

$$QR_1 = [q_{1,-1} - \bar{u}, q_{1,-1} - u_{\min}] \cup [q_{1,0} - u_{\max}, q_{1,0} - \bar{u}]. \tag{26}$$

Due to the given condition of complete containment, i.e., $q_{1,-1} < u_{\min}$ and $q_{1,0} > u_{,\max}$, QR_1 is nondegenerate with two distinct proper intervals, i.e., $q_{1,-1} - \bar{u} < q_{1,-1} - u_{\min}$ and $q_{1,0} - u_{\max} > q_{1,0} - \bar{u}$.

Next, consider the second quantizer Q_2, which has base partition $[q_{2,-1}, q_{2,0}] = [q_{1,-1} + s_p/N, q_{2,0} + s_p/N]$. As such, the center of this partition is $\bar{u} + s_p/N = \bar{u} + s_q$. Then, depending on the number of quantizers present in the ensemble (e.g., embedding n_b bits requires $N = 2^{n_b}$), the size of $s_q = s_p/N$ can be such that either

1) $\bar{u} + s_q > u_{\max}$
2) $\bar{u} + s_q \leq u_{\max}$.

In fact, the first case is the one considered already in the proof of Corollary 1, where functional secrecy is shown to be violated. Now, for the second case

$$\begin{aligned} QR_2 = {} & [q_{2,-1} - (\bar{u} + s_q), q_{2,-1} - u_{\min}] \\ & \cup [q_{2,0} - u_{\max}, q_{2,0} - (\bar{u} + s_q)] \\ = {} & [q_{1,-1} - \bar{u}, q_{2,-1} - u_{\min}] \\ & \cup [q_{2,0} - u_{\max}, q_{1,0} - \bar{u}]. \end{aligned} \tag{27}$$

Compared to (26), $QR_1 \neq QR_2$. Therefore, by Corollary 1, functional secrecy is also violated in the second case. ■

Thus far, various results regarding decoder ambiguity and functional secrecy have been established. The connections between these two notions will now be explored.

Proposition 5 (Unambiguous Decoder and Secrecy Leakage): An unambiguous quantizer ensemble (with $l = 1$) is not functionally secret.

Proof: As in Proposition 4, in an ensemble of N quantizers, it suffices to demonstrate functional secrecy violation for any pair of quantizers. Consider the first two quantizers Q_1 and Q_2. The key criterion enabling our proof in this case is that $q_{1,0} \neq q_{2,0}$ (otherwise, no information bit can be embedded in the ensemble; also see Definition 1). Then, in all cases, the output ranges of $w_{k,u}$ will be different. The following explicitly demonstrates this fact for the case where the reconstruction points are completely contained in the dynamic range, i.e., $u_{\min} < q_{1,0} < u_{\max}$ and $u_{\min} < q_{2,0} < u_{\max}$ (other scenarios are analogous):

$$\begin{aligned} [q_{1,0} - u_{\max}, q_{1,0} - u_{\min}] &= QR_1 \neq QR_2 \\ &= [q_{2,0} - u_{\max}, q_{2,0} - u_{\min}]. \end{aligned} \tag{28}$$

■

Indeed, it turns out that to be conducive to a key binding system design, the minimum number of quantizer reconstruction points in the ensemble is two. By Proposition 3, this implies that a minimal ambiguity multiplicity of 2 is imposed. For this case of $l = 2$, the following result is established.

Proposition 6 (Functionally Secret Design With Ambiguity Multiplicity $l = 2$): Given knowledge of the input dynamic range (i.e., maximum and minimal values of the input), there exists a functionally secret design with an ambiguity multiplicity $l = 2$ for all $N = 2^{n_b}$, where n_b is the number of bits to be bound.

Proof: In fact, the required design is the truncated uniform quantizer ensemble with the following parameters. The base quantizer has the reconstruction points exactly coinciding with the boundary points

$$[q_{1,-1}, q_{1,0}] = [u_{\min}, u_{\max}]. \tag{29}$$

Also, since there are only two reconstruction points in each quantizer, the notations introduced in the discussions following Definition 7 can be used as follows for improved brevity. The two reconstruction points for a quantizer Q_n are $\delta_{nt,n}$ and $\delta_{pt,n}$ (with $\delta_{pt,n} > \delta_{nt,n}$). Previously, these points refer, respectively, to the closest points to the left and the right of the zero-point reference. In this case, the reference is instead the center of the partition.

Then for $n = 1, 2, \ldots, N/2$

$$[\delta_{nt,n}, \delta_{pt,n}] = [q_{n,-1}, q_{n,0}] \tag{30}$$

and for $n = N/2 + 1, \ldots, N$

$$[\delta_{nt,n}, \delta_{pt,n}] = [q_{n,-2}, q_{n,-1}]. \tag{31}$$

(Actually, for $n = N/2 + 1$, it is also valid to use the first assignment.) Then it is straightforward to verify that all quantizers have an identical output range for $w_{k,u}$ of

$$QR_n = \left[-\frac{s_p}{2}, \frac{s_p}{2}\right] = \left[-\frac{s_q}{2N}, \frac{s_q}{2N}\right]. \tag{32}$$

Also, refer to Example 1 and the corresponding Table I for an illustrative construction. ■

As will be discussed in Section VI, the tolerance of the key binding system determines its robustness in the presence of distortions. This tolerance is proportional to the partition size. Therefore, since the system in Proposition 6 achieves the largest possible partition size while still maintaining functional secrecy (see Proposition 4), it can be referred to in some sense as the "optimal" key binding system in terms of robustness. It should be noted, however, that knowledge of the absolute max and min values is required in this construction. In practice, when the absolute max and min values are not known, a strategy based on the mean and variance can be employed as follows.

TABLE I
CODEBOOKS FOR ENSEMBLE WITH $n_b = 3$, AND BASE QUANTIZER $[\delta_{nt,1}, \delta_{pt,1}] = [-2, 4]$

n	$\delta_{nt,n}$	$\delta_{pt,n}$
1	-2.00	4.00
2	-1.25	4.75
3	-0.50	5.50
4	0.25	6.25
5	-5.00	1.00
6	-4.25	1.75
7	-3.50	2.50
8	-2.75	3.25

Example 1 (Truncated Quantizer Ensemble Application): Let the mean and standard deviation of the input distribution be denoted, respectively, as μ and σ. Then, the scheme from Proposition 6 can be applied by setting the reconstruction points for Q_1 as

$$[\delta_{nt,1}, \delta_{pt,1}] = [q_{1,-1}, q_{1,0}] = [\mu - \rho\sigma, \mu + \rho\sigma] \qquad (33)$$

where ρ represents a scaling factor. The remaining quantizers can then be constructed according to (30) and (31). In effect, by varying the scaling factor, the partition size is changed proportionally. Evidently, for functional secrecy, the scaling factor should be limited such that the maximum partition size $s_p < u_{\max} - u_{\min}$. Of course, without exact knowledge of the dynamic range, statistical knowledge of the distribution may need to be used in constraining ρ.

More importantly, the quantizer design parameter ρ can be used to tune or modify the system performance, with respect to the FAR and FAR, as will be subsequently described in Section VI. In addition, a Gray coding scheme [6] is utilized for labeling the quantizers according to the input binary key bits to be encoded (i.e., $b^{-1}(\cdot)$ is a Gray mapper), so that incremental changes in the feature vectors result in incremental changes in the recovered key.

As an illustrative example, the partitions and codebooks are shown in Table I for the following setting: $[\delta_{nt,1}, \delta_{pt,1}] = [-2, 4]$, and $n_b = 3$. ■

At this point, it is worthwhile to remark that the previous example may in fact violate functional secrecy. Recall that while the requirement of having a partition size less than or equal to the dynamic range is a *necessary* condition, it not a *sufficient* condition. In Proposition 6, the reconstruction points in the base quantizer are selected to be *exactly* the same as the max and min input values. By Proposition 4, when the reconstruction points exceed these boundary values, functional secrecy is never achieved. However, when they are smaller than these boundary values, functional secrecy is not necessarily guaranteed either. Instead of formalizing this fact as a proposition, a simple numerical example is offered in the following.

Example 2 (Partition Size and Functional Secrecy Violation): Suppose the dynamic range is known to be $[-1, 5]$. Consider a quantizer ensemble with two quantizers (i.e., capable binding 1 bit of information) defined with code books: $C_1 = \{0, 4\}$ and $C_2 = \{0+2, 4+2\} = \{2, 6\}$. Then the output ranges are, respectively,

$$QR_1 = [0-2, 0-(-1)] \cup [4-5, 4-2] = [-2, 2] \qquad (34)$$

and

$$QR_2 = [2-4, 2-(-1)] \cup [6-5, 6-4] = [-2, 3] \qquad (35)$$

which, by Corollary 1, violate functional secrecy, since $QR_1 \neq QR_2$. ■

The source of the information leakage in the previous example is due to the second quantizer, with a minimal reconstruction point of 2 that is "too far" from the minimum value of -2. As such, whenever an input value between $[-1, 0)$ occurs and quantizer 2 is used, the identity is immediately revealed (with output $w_{k,u}$ between (2,3]). The next example shows how this issue can be fixed via insertion of additional reconstruction points.

Example 3 (Reconstruction Point Insertion for Functional Secrecy): With the same initial setup as in Example 2, the following observations can be made. Ideally, the nominal range of all the quantizers should be $[-s_p/2, s_p/2] = [-2, 2]$, so that functional secrecy is attained. However, the second quantizer cannot satisfy this condition since it does not have a reconstruction point in a sufficiently close neighborhood of the minimum input value. Instead, let the codebook of the second quantizer be enlarged as $C_2 = \{-2, 2, 4\}$, then it can be readily verified that the output range $QR_2 = [-2, 2]$ as required. ■

Essentially, in the previous example, an additional reconstruction point has been inserted, so that the codebook has the form $\{q_{2,-2}, q_{2,-1}, q_{2,0}\}$. Of course, the ambiguity multiplicity has been increased by 1, by Proposition 3. However, note that this is the minimum number of reconstruction points needed in the codebook to support functional secrecy. This notion is formalized as follows.

Definition 11 (Minimal Ambiguity Quantizer Ensemble): A quantizer ensemble with the least number of reconstruction points in each of its quantizer, that is capable of supporting functional secrecy. ■

Clearly, the goal is to design a QIM-based key binding system that possesses functional secrecy, but has the minimal ambiguity in the associated quantizer ensemble. The following construction is presented precisely for this objective.

Proposition 7 (Functionally Secret System With Minimal Ambiguity): Given an input dynamic range of $[u_{\min}, u_{\max}]$. Then a quantizer ensemble with a nominal partition size $s_p \leq u_{\max} - u_{\min}$ can be designed to support functional secrecy as follows.

Let the base partition of the base quantizer Q_1 be $[\delta_{nt,1}, \delta_{pt,1}]$, where $\delta_{nt,1} \geq u_{\min}$ and $\delta_{pt,1} \leq u_{\max}$ (by assumption). Then the following two major steps are performed.

1) Following the same procedure as in Proposition 6:
   - for $n = 1, 2, \ldots, N/2$,

$$[\delta_{nt,n}, \delta_{pt,n}] = [q_{n,-1}, q_{n,0}] \qquad (36)$$

   - for $n = N/2 + 1, \ldots, N$,

$$[\delta_{nt,n}, \delta_{pt,n}] = [q_{n,-2}, q_{n,-1}]. \qquad (37)$$

2) Following the idea of Example 3, for each quantizer insert reconstruction points to control the leakage, limiting the output range to $[-s_p/2, s_p/2]$.
   - For quantizer n, compute the distances between the boundary points: $\epsilon_{ntq} = |\delta_{nt,n} - u_{\min}|$ and $\epsilon_{pt} = |\delta_{pt,n} - u_{\max}|$

- If $\epsilon_{nt} > s_p/2$, insert to the left of $\delta_{nt,n}$ a total of $\iota_{nt} = \lfloor \epsilon_{nt}/s_p \rfloor$ points of the form

$$\delta_{nt,n} - is_p, \quad i = 1, 2, \ldots, \iota_{nt}. \tag{38}$$

- Similarly, if $\epsilon_{pt} > s_p/2$, insert to the right of $\delta_{pt,n}$ a total of $\iota_{pt} = \lfloor \epsilon_{pt}/s_p \rfloor$ points of the form

$$\delta_{pt,n} + is_p, \quad i = 1, 2, \ldots, \iota_{pt}. \tag{39}$$

Proof: The proof is mostly straightforward in this case, due to the constructive nature of the described scheme. The first step starts with the minimum number of two quantization points needed for functional secrecy (see Proposition 5). Since any potential functional secrecy violations would occur with respect to the boundary points, the second step inserts the minimum of reconstruction points needed to rectify these cases (similar to Example 3). Therefore, the overall scheme achieves functional secrecy, with all quantizers achieving an output range of $[-s_p/2, s_p/2]$. ■

The approach presented in the preceding proposition represents a compromise between decoder ambiguity and functional secrecy, that is biased towards the latter. This criterion is arguably more important, since any leakage of the secret information from the supposedly secure template would not be acceptable.

V. Bit Allocation Approaches

Another important design issue in QIM implementation for the considered BE system is bit allocation, or the process of assigning an integer quantity of bits to be embedded into each of the biometric feature components [27]. This requirement has been alluded to in the previous sections, and handled temporarily by an assumption that the encoder and decoder have been already given a preselected feature component. Moreover, all the encoding and decoding schemes presented are capable of operating on n-bit keys.

In practice, given an overall number of key bits to be bound, a sensible scheme must be used to assign the appropriate number of bits to be bound by each available component. Essentially, the more reliable a component, the more information it can contain. Given sufficient side information and statistical knowledge, it is possible to optimize the bit allocation [27]. However, more simplified approaches are also feasible depending on the feature extraction methods utilized. Consider the scenario described in [4], where the Principal Component Analysis (PCA) is utilized for feature extraction, resulting in feature vectors that consist of PCA feature components. Then the bit allocation block is responsible for assigning in some manner these components as inputs to the QIM encoder (during enrollment), and to the QIM decoder (during verification). Two approaches can be taken: 1) greedy bit allocation; 2) component-reliability-based bit allocation.

A. Greedy Bit Allocation

The greedy approach is essentially a two-pass uniform bit allocation strategy.

1) The number n_c of feature components to be retained needs to be determined, e.g., based on the PCA energy criterion. Then, given a total number of bits n_b required to be bound, an equal number of bits is greedily allocated to each component, i.e., each component receives $\lfloor n_b/n_c \rfloor$ bits uniformly in the first pass.
2) In the second pass, any remaining bits $n_r = n_b - n_c \times \lfloor n_b/n_c \rfloor$ are allocated to the first n_r feature components.

B. Component-Reliability-Based Bit Allocation

More generally, when the feature components are not guaranteed to be in a decreasing order of reliability, an alternative bit allocation is described in this section. First, it is noted that for the one-bit per component HDS scheme [17], the selection of bits for key binding is based on utilizing bits that have the greatest reliability. This leads to a per-user bit allocation policy, with each user having a different set of bits used for key binding.

Definition 12 (Component Reliability): For a particular user i, the reliability of the Gaussian component t (indexed t) is denoted as $R_{i,t}$, and is defined as [17]

$$R_{i,t} = \frac{1}{2}\left(1 + \operatorname{erf}\left(\frac{|\mu_{i,t} - \mu_t|}{\sqrt{2\sigma_{i,t}^2}}\right)\right) \tag{40}$$

where $\mu_{i,t}$ is the subject mean of component t, μ_t the population mean of component t, and $\sigma_{i,t}^2$ 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).

The reliability computation requires knowledge of the subject mean and variance. This implies that, in order to estimate these statistics, multiple enrollment images are required. Moreover, as in existing key binding strategies with the notion of reliability [10], [17], [18] as well as when using a feature extractor such as the PCA, since the computed statistics may be exposed to an external observer, some degree of leakage should be anticipated. In particular, global statistical information regarding a set of users may be revealed if the system storage mechanism is not carefully implemented.

The following steps describe the procedure for bit allocation with QIM. The general idea is to assign the bits in a manner that best preserves the reliability profile of the feature components.

1) Compute the reliability of each component (establishing a continuous-valued reliability profile).
2) Apply a threshold for acceptable reliability to obtain the candidate set (CS). This step is analogous to the decision in the simple bit allocation case of how many components to retain (i.e., determining the cut-off point based on the PCA energy). In more detail,
    a) Set a threshold parameter t_d between 0 and 1.
    b) Set $r_{\max}$ = the highest reliability value.
    c) Discard all components with reliability less than $t_d \times r_{\max}$ (zero bit allocated).
3) Perform linear rescaling, so that the sum of all the scaled components in the CS is equal to the number of total bits required. The scaling factor is computed as

$$\rho_l = \frac{n_b}{\sum_{t \in CS} R_t} \tag{41}$$

where n_b is the number of bits to be allocated, R_t the reliability of component t, and CS the candidate set. Clearly, for linear scaling, the relative importance of components (according to the original reliability profile) is still maintained.

4) Convert the scaled reliability profile to integers as follows:
   a) Round the scaled reliability profile.
   b) Compute $RS =$ sum of the integer components in the rounded and scaled reliability profile.
   c) Compare RS to n_b
      i) $RS = n_b$: the allocation is complete.
      ii) $RS < n_b$: the allocation is underestimated. To compensate, the $(n_b - RS)$ components with the highest reliability are each incremented by 1.
      iii) $RS > n_b$: the allocation is overestimated. To compensate, the $(RS - n_b)$ nonzero components with the lowest reliability are each decremented by 1.

In addition, it should be noted that the analytical results related to the quantizer design in Section IV are contingent upon the underlying components being orthogonal to each other, which is true if they are generated via a PCA-type extractor. Therefore, when the feature extraction does not have this property, appropriate measures should be taken to ensure that this is the case, e.g., orthogonalization can be explicitly enforced in conjunction with the bit allocation scheme.

VI. Performance Characteristics

With the objectives of providing security while preserving privacy, two main design criteria have been identified: resolving decoder ambiguity to reduce false acceptances, and controlling the information leakage to secure sensitive information bound to the template generated. The following characteristics highlight the interactive aspects of these criteria.

1) The more reconstruction points present, the higher the ambiguity, thus affecting the FAR. However, without sufficient reconstruction points, potential leakage of the key bits may occur, whenever the output ranges of the template exceed the nominal $[-s_p/2, s_p/2]$. This makes it possible for an unauthorized user to maliciously extract the associated key bits stored in the template.
2) The larger the partition size, the more likely leakage may occur. In fact, once the input dynamic range is completely contained within a partition, functional secrecy is provably violated.
3) An ambiguity error implies that, instead of submitting a signal that is within some neighborhood of the original signal to attack the system, an unauthorized user can also submit a signal that is within several other neighborhoods, which are all related to the original neighborhood. Of course, without knowledge of the original neighborhood, the attacker does not have a deterministic method to routinely "guess" these other neighborhoods to compromise the system. As such, unintentional system malfunctions due to false acceptances are the main issues with ambiguity. In other words, ambiguity would prove to be more of a nuisance to authorized users, rather than facilitating unauthorized users significantly.
4) A leakage error due to functional secrecy violation, on the other hand, is arguably more serious. This is because, once leakage is detected by a malicious attacker, the attacker can immediately obtain the identification of the quantizer used.

Based on the apparent degree of severity associated with these criteria, the approach taken in this work has been to strictly guarantee functional secrecy first, without which the system cannot be suitably used. Then, ambiguity is optimized as much as can be allowed while preserving functional secrecy. Proposition 7 is the manifestation of this design approach.

While the discussions have so far focused on the FAR, as it is related to the security, the FRR is also important in certain applications, since this latter quantity determines the system robustness or resilience in the presence of distortions. As will be seen, the FRR is related also to the partition size used in the quantizer ensemble.

Let us recast the QIM decoding scheme in the following manner. After the first offset-compensation step between the secure template and the biometric component under verification

$$u' + w = u' + (q_k - u) = q_k + (u' - u) = q_k + e. \tag{42}$$

As such, e can be interpreted as an equivalent additive error, which represents the difference between the original signal u and the noisy (fuzzy) verification signal u'. Therefore, for one-dimensional quantizers with e being additive white Gaussian noise (AWGN), the tolerance of the system, i.e., the tolerable difference between u and u' for successful verification, is found as

$$|u' - u| = |e| < \frac{s_q}{2} = \frac{s_p}{2^{n_b+1}} \tag{43}$$

where we recall that s_q represents the quantizer step-size, or the distance between any two closest reconstruction points (from all quantizers) in the ensemble used. By construction, for a uniform quantizer ensemble (Definition 7), $s_q = s_p/N$. When the tolerance is satisfied, then the original key can be successfully extracted upon verification. In other words, if the verification error is within tolerance, the estimate k' is the result of successful extraction or release of the original k from the secure template $w_{k,u}$.

Actually, from Proposition 2 and the *modulo* action, depending on how many reconstruction points are in the quantizer, the acceptable set may also consist of other regions. However, these regions are spaced apart from the genuine set by multiple of s_p (the partition size). Evidently, such a large difference would not represent an error caused by typical random distortions. In particular, an authorized user who has his or her verification signal deviating from the original enrollment signal by such a significant amount should not be accepted by the system.

These characteristics imply that the system performance measures can be modified by designing the quantizer ensemble appropriately. For instance, in utilizing the approach of statistical design (when the absolute max and min values are unknown) in Example 1, the quantizer step-size can be tuned, by selecting ρ appropriately, to achieve particular system performance specifications in terms of the FAR (security), or the FRR (robustness).

In addition, as shown in Fig. 1, when ECC is preapplied to the input to the QIM encoder, the overall system performance is also enhanced by the ECC specifications. Moreover, as previously discussed, while the ECC can be used to modify the system performance, it may not be sufficiently flexible. Indeed, while the quantizer parameter ρ accepts a range of (continuous) values, the error-correcting capability offered by ECC is typically limited to a number of (discrete) values [6]. Therefore, the QIM approach arguably represents a more flexible design for key binding.

However, the QIM methodology does impose higher complexity, either in computational cost or in storage overhead, when compared to HDS using an XOR primitive. In particular, with a large number of quantizers in the ensemble, the cost of either constructing or storing the codebook may be significant. Therefore, there is a trade-off to be balanced between performance flexibility and resource complexity with the introduction of a QIM module.

Last but not least, while emphasis has been placed on functional secrecy, this criterion is actually a rather relaxed constraint, which represents a minimal requirement. As previously alluded to in the discussions following Definition 10, functional secrecy makes no restriction regarding possible bias present in the quantizer ensemble. The following example illustrates this issue.

Example 4 (Quantizer Bias and Functional Secrecy): Consider an ensemble of two quantizers. Suppose the configuration is such that the output $w_{k,u}$ values have the following conditional probability density functions (pdfs):

$$P(w_{k,u}|Q_1) = \begin{cases} x + \frac{1}{2}, & 0 \leq x \leq 1 \\ 0, & \text{otherwise} \end{cases} \tag{44}$$

under quantizer Q_1, and

$$P(w_{k,u}|Q_2) = \begin{cases} -x + \frac{3}{2}, & 0 \leq x \leq 1 \\ 0, & \text{otherwise} \end{cases} \tag{45}$$

under quantizer Q_2. Then the system satisfies functional secrecy, since the output range is identically [0,1]. However, it is clear that quantizer Q_1 has a higher probability for values of $w_{k,u}$ closer to 1, while Q_2 has a higher probability for values closer to 0. Therefore, any values other than $w_{k,u} = 1/2$, at which the probability is identical, would reveal more bias towards the quantizer used, e.g, an observed value closer to 1 is more likely to indicate that Q_1 has been used. ■

A more refined definition for secrecy preservation may be formulated as follows.

Definition 13 (Unbiasedly Secret System): A key binding system in which the output template does not reveal any statistical bias towards any of the quantizer used. That is, given a particular value of $w_{k,u}$, no statistical information regarding the quantizer used can be obtained. ■

Recall that functional secrecy entails identical range in the output $w_{k,u}$. A similar result can be readily obtained for unbiased secret system, which should need no detailed proof.

Corollary 2: To be unbiasedly secret, the pdfs of the output template under different quantizers must be independent and identically distributed. ■

While achieving unbiased secrecy is clearly more desirable compared to functional secrecy, this stricter constraint appears to limit flexibility, by imposing further constraints on the system design, and the types of admissible input distributions. The following example explores some implications of unbiased secrecy requirements.

Example 5 (Unbiased Secrecy and Symmetry Conditions): Let the input dynamic range be $[u_{\min}, u_{\max}]$. Consider a simple quantizer ensemble containing two quantizers, with codebooks $C_1 = \{u_{\min}, u_{\max}\}$, $C_2 = \{u_{\min} - s_q, u_{\max} - s_q\}$. Then the output range is identically $[-s_p/2, s_p/2]$.

If the underlying input distribution is $P_U(u), u \in [u_{\min}, u_{\max}]$, then the output pdfs are

$$P(w_{k,u}|Q_1) = \begin{cases} P_U(u_{\min} - w_{k,u}), & -\frac{s_p}{2} < w_{k,u} < 0 \\ P_U(u_{\max} - w_{k,u}), & 0 < w_{k,u} < \frac{s_p}{2} \\ 0, & \text{otherwise} \end{cases} \tag{46}$$

and

$$P(w_{k,u}|Q_1) = \begin{cases} P_U\left(\frac{u_{\min}+u_{\max}}{2} - w_{k,u}\right), & -\frac{s_p}{2} < w_{k,u} < \frac{s_p}{2} \\ 0, & \text{otherwise.} \end{cases} \tag{47}$$

As such, for unbiased secrecy, the input distribution $P_U(u)$ is required to be such that

$$P_U(u_{\min} - w_{k,u}) = P_U\left(\frac{u_{\min}+u_{\max}}{2} - w_{k,u}\right), -\frac{s_p}{2} < w_{k,u} < 0 \tag{48}$$

and

$$P_U(u_{\max} - w_{k,u}) = P_U\left(\frac{u_{\min}+u_{\max}}{2} - w_{k,u}\right), \quad 0 < w_{k,u} < \frac{s_p}{2}. \tag{49}$$

These two equations imply that a symmetry where the input distribution consists of two identical half shapes, placed side-by-side, from $[u_{\min}, (u_{\min} + u_{\max})/2]$ and $[(u_{\min} + u_{\max})/2, u_{\max}]$, would be needed. Therefore, while a uniform distribution would satisfy this condition, a Gaussian bell-shaped (with mirror symmetry) input distribution would not generate unbiased secrecy for this quantizer ensemble. ■

Similar considerations can be made for the case of $n_b > 1$, with more quantizers in the ensemble. A preliminary investigation seems to indicate that, besides the trivial case of a uniform input distribution, the types of symmetry (if any permissible at all) required may not occur naturally in practical applications. Therefore, further significant modifications may be needed to realize unbiased secrecy on a large scale. On the other hand, functional secrecy represents not only a minimal requirement, but also is conducive to practical applications.

In closing this section, we remark that while the present work has explored issues related to the security and privacy of the generated template, there remains a notable caveat. The protection of the cryptographic key and biometric signal in the template is clearly dependent on the secrecy of both of these inputs. If the key is somehow compromised, then it can be potentially regenerated to create a new template. However, what is perhaps problematic is that whatever signal used to originally bind this key in the template would also be potentially revealed (up to an ambiguity factor, see Proposition 3). If this signal happens to be the original biometric signal, itself being a permanent feature of an individual, this leakage is definitely undesirable. While a complete exploration of the various implications is beyond the scope of this paper, potential directions for future work addressing this serious issue can be outlined in the following.

It turns out that the class of secure sketch and related fuzzy extractor systems previously mentioned in Section I seems to provide a potential solution. The main idea is that, instead of using the biometric signal directly to bind the key, the signal can be first conditioned by a preceding secure sketch/fuzzy extractor block. The rationale for this approach is that, should a cryptographic key compromise occur, only the secure sketch object would be revealed by the template. Such a secure sketch object benefits from a wealth of literature regarding the system analysis as well as issues of key strength and cancelability [14], [28]–[30]. Of course, this implies that the design of the quantizer ensemble would also have to take into account the statistical nature of the secure sketch for efficiency, the results of which should form the subject of a future work.

VII. Performance Evaluation With Facial Biometric Modality

A. Experimental Setup

Images from the CMU PIE database are utilized to assess the performance of the proposed QIM methods. The feature extraction is selected to be PCA for baseline evaluation. The experimental setup is similar to that in [4], in which various implications related to the system-level aspects are also discussed. Since this paper is focused on the key binding module, only a selective set of simulation scenarios will be pursued. The reader is referred to [4] for a more comprehensive treatment. To this end, the salient parameters are summarized. The simulation database contains 68 individuals with face images captured under three frontal poses under seven illumination conditions, giving a total of about 21 samples per subject (with some faces missing). From the database, a gallery set was created (containing all but one of the images for each of the subjects), as well as a probe set (containing the single remaining image for each subject). The gallery set is used for training the feature extractor and the BE modules as well as enrollment of the subjects. The probe set is used for testing the recognition performance, while the PCA is trained on the gallery set. In order to retain 95% of the signal energy, the first 154 PCA components are selected for bit allocation. In other words, depending on the target key length, each component may be used to bind a different number of key bits, as described in Section V.

B. Performance With Various Key Lengths

Fig. 5 shows the receiver-operating characteristic (ROC) for various scenarios, each characterized by a certain key length in the input key to be bound.

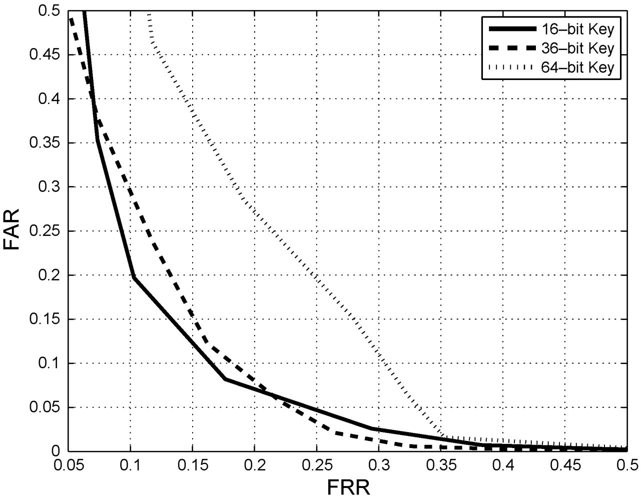


Fig. 5. ROC with various key lengths.

In interpreting the results, it should be noted that the specific values of the operating points on the ROC curves depend on many factors, including the coding scheme, the feature extraction utilized, etc. And improving the overall performances requires modifying these constituent methods. In [4], performance results with varying system conditions related to the preceding modules are presented. Here, it is important to focus on the overall trend for a particular system setting. Indeed, it is seen that a range of operating points can be achieved, by modifying the corresponding quantizer step-size. For scenarios requiring higher security (lower FAR), the operating points should be steered towards the right side of the plot, by selecting a smaller step-size. Conversely, a larger step-size can be selected to achieve higher tolerance, steering the operating points to the left side of the plot (lower FRR). Therefore, in applications requiring particular performance requirements, the QIM approach represents an attractive asset.

Also, when more key bits are to be bound, the overall performance degrades, e.g., in increasing the key length from 36-bit to 64-bit, the ROC plot moves upward with a substantial margin. This is the same behavior found in other key binding strategies. However, what is different here is the ability to generate the continuous ROC plot from a given set of binarized features. By contrast, when using other key binding strategies, such as the HDS and multibit likelihood ratio approaches, the behavior of the operating points can only be changed by selecting a different coding scheme. In other words, for a selected ECC code, a single operating point in performance is obtained.

And more importantly, a barrier that prevents these systems from being practically used is the inability to achieve sufficiently low FRR. In other words, while low FAR is a positive characteristic of these systems, reducing the FRR to a sufficiently low value has appeared elusive with the currently available ECC codes. For example, using HDS with 16-bit key, and code length 63, the $(\mathrm{FAR}, \mathrm{FRR}) = (0, 0.8529)$ for the given data set and preprocessing methods. Clearly, this represents a system with poor verification performance (besides that fact that a key length of 16 bits may be deemed insecure). The main reason is that ECC codes generally cannot achieve an arbitrary error-correction rate, e.g., the BCH family is limited to bit errors of approximately 25% or less, even with the most robust selections. The situation is essentially similar using the multibit likelihood ratio approach. With the same configuration, $(\mathrm{FAR}, \mathrm{FRR}) = (0, 0.5294)$. While this represents improved performance compared to the HDS case, it is questionable whether it can be practically used.

C. Performance With Bit Allocation Approaches

Fig. 6 shows first the reliability profile of a typical subject. It can be seen that the components with the highest reliability are concentrated at the beginning of the feature vector. Therefore, as long as the cut-off point is sufficiently accurate, the simple greedy bit allocation strategy should yield results similar to those based on reliability. In this case, the cut-off point (how

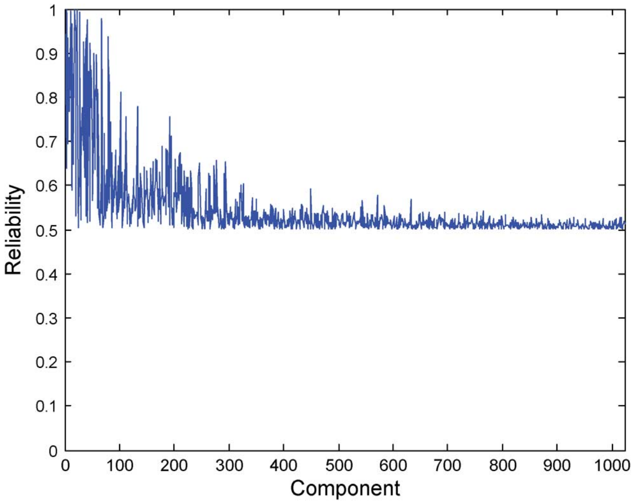


Fig. 6. Reliability profile of a typical subject.

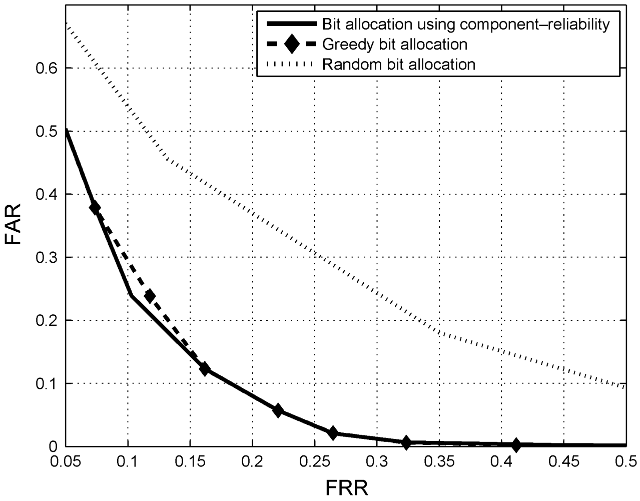


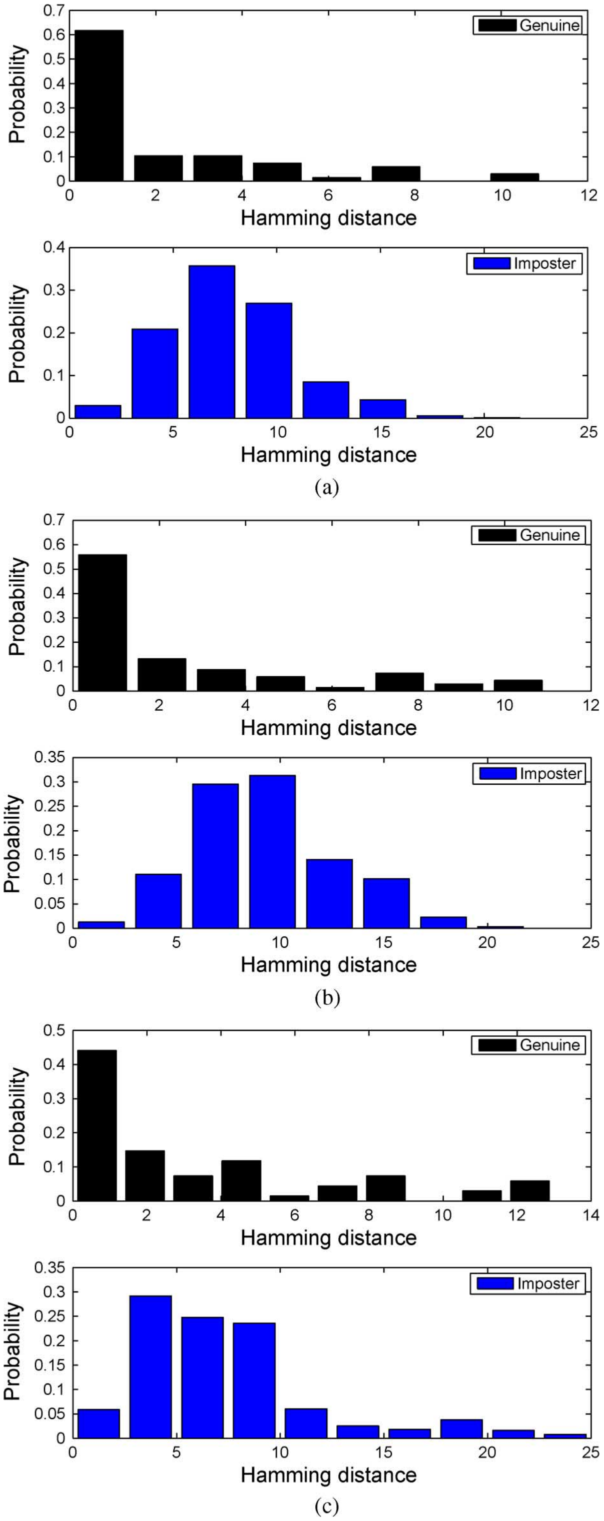
Fig. 7. ROC with 36-bit keys, using various bit allocation approaches.

many components to retain) for the simple allocation scheme is less than 300-component mark (based on the energy of the PCA), which from the above figure is the approximate point beyond which most components can be categorized as unreliable.

However, in general cases, where the PCA is not necessarily employed, such a straight-forward demarcation for greedy allocation may not be possible. In those cases, the more flexible method based on reliability should be more beneficial.

The above observations are clarified by examining the ROCs corresponding to three different bit allocation strategies, as shown in Fig. 7. The three cases use the same key length, with bit allocation methods: 1) random bit allocation (an arbitrary number of bits assigned to each component); 2) greedy bit allocation; 3) bit allocation using component-reliability.

The obtained results demonstrate two main points. First, without a sensible bit allocation scheme, such as when using a random selection, the results obtained would be substantially inferior. This is because components that are more reliable may not be assigned more bits compared to the less reliable ones. Second, for the scenario presented, the two proposed bit allocation approaches yield similar performance. This is due to the fact that the PCA feature extraction produce feature vectors with ordered components. Then a greedy approach which exploits this underlying characteristic essentially produces the same bit allocation as the one based on actual reliability computations.



(a)

(b)

(c)

Fig. 8. Example distributions of Hamming distances for the genuine and imposter users for various bit allocation approaches. (a) Bit allocation using component-reliability; (b) greedy bit allocation; (c) random bit allocation.

Last but not least, to reveal in more specific detail the local behavior of the examined system, the distributions of the key bits, as exhibited by the Hamming distance, for the genuine and imposter users are shown in Fig. 8.

The illustrated results reinforce the similarities in performance between the greedy bit allocation and that using component reliability for the given scenario (which is also true on a more global scale, as supported by Fig. 7). In this case, the distributions illustrate a more local performance corresponding to a specific operating point. The applicable BCH code is (63,36,5), which implies that a Hamming distance greater than 5 (equivalently, a difference of more 5 bits in the recovered key) is rejected by the system. Therefore, considering Fig. 8(a) specifically for the genuine plot, the total probability due to bin 5 and higher contributes to the FRR. Similarly, for the imposter plot, the total probability due to the first two bins represents the FAR. The operating point illustrated by these two plots is thus $(\mathrm{FAR}, \mathrm{FRR}) = (0.2386, 0.1029)$. A similar interpretation can be readily made for the remaining two bit allocation approaches in Fig. 8(b) and (c) in analyzing the local behavior. By contrast, these details are not evident in the higher-level ROC plots shown in Fig. 7), which is more useful in studying the global behavior.

VIII. Conclusion

In this paper, various strategies related to key binding with QIM in a BE context are examined. Besides the algorithmic basis and assumptions necessary for QIM, practical implementation issues, including quantizer design and bit allocation, are presented. The obtained results demonstrate that the QIM method facilitates tuning of the system performance. This is made possible by designing the quantizer ensemble in a structured manner, which allows for parametric modification of the quantizer distance. Consequently the system tolerance can be varied to accommodate requirements in terms of FAR and FRR for specific conditions. Therefore, the QIM approach represents a flexible key binding approach that can accommodate a wider range of envisioned applications.

Acknowledgment

The authors would like to thank K. Peltsch from the OLG, and Dr. A. Cavoukian and Dr. A. Stoianov from the Information and Privacy Commissioner of Ontario for many useful discussions.

References

[1] A. Cavoukian and A. Stoianov, Biometric Encryption: A Positive-Sum Technology That Achieves Strong Authentication, Security and Privacy Information and Privacy Commissioner/Ontario, Mar. 2007.

[2] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. V. K. Vijaya Kumar, "Biometric encryption," in *ICSA Guide to Cryptography*, R. K. Nichols, Ed. New York: McGraw-Hill, 1999, pp. 649–675.

[3] L. Lai, S.-W. Ho, and H. Vincent Poor, "Privacy-security tradeoffs in biometric security systems," in *Annual Allerton Conf. Communication, Control, and Computing (Allerton)*, Monticello, IL, Sept. 2008.

[4] K. Martin, H. Lu, F. M. Bui, K. N. Plataniotis, and D. Hatzinakos, "A biometric encryption system for the self-exclusion scenario of face recognition," *Special Issue on Biometrics Systems, IEEE Syst. J.*, to be published.

[5] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 4th ed. Englewood Cliffs, NJ: Prentice-Hall, 2006.

[6] G. Kabatiansky, E. Krouk, and S. Semenov, *Error Correcting Coding and Security for Data Networks: Analysis of the Superchannel Concept*. Hoboken, NJ: Wiley, 2005.

[7] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 1996.

[8] 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, 1381-3625.

[9] I. R. Buhan, J. M. Doumen, and P. H. Hartel, "Controlling leakage of biometric information using dithering," in *16th Eur. Signal Processing Conf., EUSIPCO. EURASIP, European Association for Signal, Speech and Image Processing, Lausanne, Switzerland*, Lausanne, Switzerland, Aug. 2008 [Online]. Available: http://www.eurasip.org/Proceedings/Eusipco/Eusipco2008/papers/1569105382.pdf, Article 1569105382

[10] , P. Tuyls, B. Skoric, and T. Keveenaar, Eds., *Security With Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*. New York: Springer Verlag, 2007.

[11] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *Special Issue on Pattern Recognition Methods for Biometrics, EURASIP J. Advances Signal Process.*, vol. 2008, pp. 1–17, 2008, Article 579416.

[12] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Computing*, vol. 8, no. 1, pp. 97–139, 2008.

[13] Q. Li, Y. Sutcu, and N. Memon, "Secure sketch for biometric templates," in *Proc. Asiacrypt*, Shanghai, China, Dec. 2006.

[14] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric templates with sketch: Theory and practice," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 503–512, Sep. 2007.

[15] F. M. Bui and D. Hatzinakos, "Secure methods for fuzzy key binding in biometric authentication applications," in *Proc. Asilomar Conf. on Signals, Systems and Computers*, Pacific Grove, CA, Oct. 2008, pp. 1363–1367.

[16] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. 6th ACM Conf. Comp. and Commun. Sec.*, 1999, pp. 28–36.

[17] T. A. M. Kevenaar, G. J. Schrijen, M. van der Veen, and A. H. M Akkermans, "Face recognition with renewable and privacy preserving binary templates," in *Proc. Automatic Identification and Advanced Technologies, 4th IEEE Workshop*, 2005, pp. 21–26.

[18] M. van der Veen, T. Kevenaar, G.-J. Schrijen, T. H. Akkermans, and F. Zuo, "Face biometrics with renewable templates," in *Proc. SPIE, Security, Steganography and Watermarking of Multimedia Contents*, San Jose, CA, 2006, vol. 6072, pp. 205–216.

[19] C. Busch and A. Nouak, "3D face recognition for unattended border control," in *Proc. 2008 Int. Conf. Security and Management (SAM'08)*, Las Vegas, NV, 2008, pp. 350–356.

[20] E. J. C. Kelkboom, B. Gökberk, T. A. M. Kevenaar, A. H. M. Akkermans, and M. van der Veen, "3D face: Biometric template protection for 3D face recognition," in *Proc. ICB 2007*, 2007, pp. 566–573.

[21] H. L. Van Trees, *Detection, Estimation, and Modulation Theory, Part I*. Hoboken, NJ: Wiley-Interscience, 2001.

[22] 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 *IEEE Conf. Biometrics: Theory, Applications and Systems*, Sep. 2007, pp. 1–6.

[23] M. Costa, "Writing on dirty paper (corresp.)," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 439–441, May 1983.

[24] B. Chen and G. W. Wornell, "Quantization index modulation methods for digital watermarking and information embedding of multimedia," *J. VLSI Signal Process.*, vol. 27, no. 1, pp. 7–33, 2001.

[25] B. Chen and G. W. Wornell, "Dither modulation: A new approach to digital watermarking and information embedding," in *Proc. SPIE: Security and Watermarking of Multimedia Contents*, P. W. Wong and E. J. Delp, III, Eds., Apr. 1999, vol. 3657, pp. 342–353.

[26] J. P. Linnartz and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates," in *4th Int. Conf. Audio and Video Based Biometric Person Authentication*, Guildford, U.K., Jun. 2003, pp. 393–402.

[27] C. Chen, R. N. J. Veldhuis, T. A. M. Kevenaar, and A. H. M. Akkermans, "Biometric binary string generation with detection rate optimized bit allocation," in *Proc. Computer Vision and Pattern Recognition Workshops, 2008. (CVPRW 08)*, Jun. 2008, pp. 23–28.

[28] Q. Li, M. Guo, and E.-C. Chang, "Fuzzy extractors for asymmetric biometric representations," in *Proc. IEEE Computer Society Workshop on Biometrics*, Anchorage, AK, Jun. 2008, pp. 1–6.

[29] Y. Sutcu, Q. Li, and N. Memon, "Design and analysis of fuzzy extractors for faces," in *Biometric Technology for Human Identification, Part of the SPIE Int. Defense and Security Symp.*, Orlando, FL, Apr. 2009.

[30] J. D. Golic and M. Baltatu, “Entropy analysis and new constructions of biometric key generation systems,” *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 2026–2040, May 2008.

Francis Minhthang Bui (S’99–M’08) received the B.A. degree in French language, and the B.Sc. degree in electrical engineering from the University of Calgary, Alberta, Canada, in 2001. He then received the M.A.Sc. and Ph.D. degrees, all in electrical engineering, in 2003 and 2009, respectively, from the University of Toronto, ON, Canada, where he is now a postdoctoral fellow.

He is also currently the technical manager for the Ontario Research Fund Research Excellence (ORF-RE) project focusing on Self-Powered Sensor Networks (SPSN), with a multidisciplinary team of researchers at the University of Toronto and various industrial partners. His research interests include signal processing methodologies for resource allocation and security in wireless communication networks.

Karl Martin (S’00–M’08) received the B.A.Sc. degree in engineering science and the M.A.Sc. degree in electrical engineering, from the University of Toronto, Canada in 2001 and 2003, respectively. He is currently pursuing the Ph.D. degree at the Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto.

His research interests include multimedia security and privacy, biometrics, multimedia processing, wavelet-based image coding, and object-based coding. He is a member of the IEEE Signal Processing Society, Communications Society, and Circuits and Systems Society. He has been a technical reviewer for numerous journals and conferences.

Haiping Lu (S’02–M’08) received the B.Eng. and M.Eng degrees in electrical and electronic engineering from Nanyang Technological University, Singapore, in 2001 and 2004, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Toronto, Toronto, ON, Canada, in 2008.

Currently, he is a research fellow with the Institute for Infocomm Research, Agency for Science, Technology and Research (A*STAR), Singapore. Before joining A*STAR, he was a postdoctoral fellow at the Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto. His current research interests include statistical pattern recognition, machine learning, multilinear algebra, tensor object processing, biometric encryption, and data mining.

Konstantinos N. (Kostas) Plataniotis (S’90–M’92–SM’03) is a Professor with The Edward S. Rogers Sr. Department of Electrical and Computer Engineering at the University of Toronto in Toronto, ON, Canada, and an Adjunct Professor with the School of Computer Science at Ryerson University, Canada. He is the Chair of the Communications Group at the ECE Department, Deputy Director of The University of Toronto’s Knowledge Media Design Institute (www.kmdi.utoronto.ca), and the Director of Research for the Identity, Privacy and Security Institute at the University of Toronto (www.ipsi.utoronto.c). His research interests include biometrics, communications systems, multimedia systems, and signal and image processing.

Prof. Plataniotis is the Editor in Chief (2009–2011) for the IEEE Signal Processing Letters and chairs the Examination Committee for the IEEE Certified Biometrics Professional (CBP) Program (www.ieeebiometricscertification.org). He is a member of the Nominations Committee for the IEEE Council on Biometrics, a member of Publications and Awards Boards, IEEE Signal Processing Society, and a Member of the Steering Committee, IEEE Transactions on Mobile Computing. He served on the IEEE Educational Activities Board (EAB) and he was the Chair (2008–09) of the IEEE EAB Continuing Professional Education Committee. He has served as Chair (2000–2002) IEEE Toronto Signal Processing Chapter, Chair (2004–2005) IEEE Toronto Section, and he was a member of the 2006 and 2007 IEEE Admissions and Advancement Committees. He is the 2005 recipient of IEEE Canada’s Outstanding Engineering Educator Award “for contributions to engineering education and inspirational guidance of graduate students” and the corecipient of the 2006 IEEE Transactions on Neural Networks Outstaning Paper Award for the paper, published in 2003, titled “Face Recognition Using Kernel Direct Discriminant Analysis Algorithms”. He is a registered professional engineer in the province of Ontario, and a member of the Technical Chamber of Greece.

Dimitrios Hatzinakos (S’87–M’90–SM’98) received the Diploma degree from the University of Thessaloniki, Greece, in 1983, the M.A.Sc degree from the University of Ottawa, Canada, in 1986, and the Ph.D. degree from Northeastern University, Boston, MA, in 1990, all in electrical engineering.

In September 1990, he joined the Department of Electrical and Computer Engineering, University of Toronto, where now he holds the rank of Professor with tenure. He served as Chair of the Communications Group of the Department during the period July 1999 to June 2004. Since November 2004, he is the holder of the Bell Canada Chair in Multimedia, at the University of Toronto. He is cofounder and Director of the Identity, Privacy and Security Initiative (IPSI) at the University of Toronto. His research interests are in the areas of multimedia signal processing, multimedia security, multimedia communications, and biometric systems. He is author/coauthor of more than 200 papers in technical journals and conference proceedings and he has contributed to 12 books in his areas of interest. He is the coauthor of *Multimedia Encoding for Access Control with Traitor Tracing: Balancing Secrecy, Privacy and Traceability* (VDM Verlag Dr. Muller, 2008) (ISBN: 978-3-8364-3638-0). His experience includes consulting through Electrical Engineering Consociates Ltd. and contracts with United Signals and Systems Inc., Burns and Fry Ltd., Pipetronix Ltd., Defense R&D Canada (DRDC), Nortel Networks, Vivosonic Inc., and CANAMET Inc.

He is currently an Associate Editor for the IEEE Transactions on Mobile Computing. He has served as an Associate Editor for the IEEE Transactions on Signal Processing from 1998 to 2002 and Guest Editor for the *Special Issue on Signal Processing Technologies for Short Burst Wireless Communications, Signal Processing,* Elsevier, which appeared in October 2000. He was a member of the IEEE Statistical Signal and Array Processing Technical Committee (SSAP) from 1992 to 1995 and Technical Program co-chairof the 5th Workshop on Higher-Order Statistics in July 1997. He is a member of EURASIP, the Professional Engineers of Ontario (PEO), and the Technical Chamber of Greece.