A COMPARATIVE ANALYSIS OF BIOMETRIC SECRET-KEY BINDING SCHEMES BASED ON QIM AND WYNER-ZIV CODING

Aniketh Talwai

Dept. of Electronics & Communication Engineering
Indian Institute of Technology Guwahati - 781039, India
Email: aniketh@iitg.ernet.in

Francis M. Bui, Ashish Khisti, Dimitrios Hatzinakos *

Dept. of Elec. and Comp. Engineering, University of Toronto
10 King's College Road, Toronto, Ontario, Canada M5S 3G4
E-mail: {bui,akhisti,dimitris}@comm.utoronto.ca

ABSTRACT

Biometric secret-key binding inherently requires signal processing and error correction schemes due to noisy measurement readings. Two previously proposed strategies, Quantization Index Modulation (QIM) and Wyner-Ziv (WZ) coding, are studied in the context of biometric key binding. We characterize the tradeoff between key rate-leakage and key rate-reconstruction distortion, showing that while WZ coding has a better rate-leakage tradeoff than QIM, the latter has a better rate-reconstruction tradeoff. A new strategy is proposed to combine the merits of these schemes. Known as distortion-enhanced Wyner-Ziv coding (DE-WZ), this scheme is demonstrated to exhibit improved flexibility based on numerical results for a uniform source model and scalar quantization.

***Index Terms*—** Biometrics, information security, secret key binding, quantization index modulation, Wyner-Ziv coding

1. INTRODUCTION

Security and privacy issues are of paramount importance in many engineering designs today. This paper focuses on a particularly auspicious approach to delivering security and privacy based on biometric encryption (BE) (also known as helper data) methods [1], which promise not only robustness but also flexibility. Essentially, the helper data method allows secure binding of a signal (containing sensitive information to be protected, such as a cryptographic key) with another signal derived from physiological features (i.e., the biometric). A significant number of security applications can be formulated in this context [1–3].

Our objectives involve investigating the theoretical performances of key binding strategies, for biometric enrollment and verification, based on the Wyner-Ziv (WZ) coding [4] and the quantization index modulation (QIM) method [2]. While the former WZ approach exhibits attractive features in terms of key rate, its associated distortion performance is surpassed by the latter QIM approach. As such, the feasibility combining the advantageous features of each method is explored, resulting in the distortion-enhanced Wyner-Ziv (DE-WZ) scheme, with particular characteristics described in the remainder of the paper.

2. SYSTEM MODEL AND NOTATIONS

Denote the biometric signal at enrollment by X, assumed to be a uniformly distributed random variable: $X \in (-\Delta, \Delta)$. Let U be the output of a uniform quantization encoder through which X is passed, then

$$U = X - E \tag{1}$$

where $E \in \left(-\frac{\delta}{2}, \frac{\delta}{2}\right)$, with δ being the distance between two consecutive quantizer output points. E represents the distortion between the biometric X and its quantized output U. With a uniform quantizer and uniformly distributed input X, E is also uniformly distributed.

Upon verification, the biometric signal Y is measured,

$$Y = X + W = U + E + W, \tag{2}$$

where W is a uniformly distributed random variable, representing the physiological noise or variation (which should be sufficiently small for the genuine user). Without loss of generality, $W \in (-0.5, 0.5)$, since other parameters can be scaled accordingly. Furthermore, for practical biometric applications, W is substantially less than X, to the extent that the distribution of Y (obtained as a convolution of distributions) can be assumed to be approximately uniform. Thus, this observation on the distribution of Y will be assumed for brevity of analysis.

Furthermore, we also consider the case where a uniformly distributed noise, $N \in (-N_L, N_L)$, is *intentionally* added to the biometric X (to potentially enhance privacy, as described later). For this construction, upon verification at the receiver,

$$Y = X + W + N. \tag{3}$$

The various key binding schemes will be compared based on the following criteria: key rate, mean square error (MSE) distortion, and mutual information (between the biometric and the knowledge of attacker) [5,6]. Note that the leakage and distortion are computed assuming that the attacker is revealed the secret-key, in addition to the helper data message. This corresponds to the conditional leakage cases in [6]. Clearly, the higher the MSE distortion, the higher the privacy, as it would be more difficult for an attacker to reconstruct the original biometric from the shared message. Also, the higher the key rate, the higher the security, as a longer and hence safer key could be used. Last but not least, the lower the mutual information, the higher is the privacy from an information-theoretic perspective.

3. WYNER-ZIV SCHEME

Previously proposed for video coding in [4], the WZ scheme by scalar quantization can be adapted for secret key binding as follows. Consider a quantizer with the set of reconstruction points $\mathcal{Q} = \{q_1, q_2, \ldots, q_B, q_{B+1}, q_{B+2}, \ldots\}$, spaced δ apart, i.e., $q_{i+1} - q_i = \delta$. Then, each point q_i is labeled with a bin index $l(q_i)$,

*This work was supported by the MITACS Globalink Program, and the Natural Sciences and Engineering Research Council of Canada (NSERC).

sequentially and cyclically up to B. In other words, the labeling pattern is: $\{l(q_1), l(q_2), \ldots, l(q_B), l(q_{B+1}), l(q_{B+2}), \ldots\} = \{1, 2, \ldots, B, 1, 2, \ldots\}$. For proper operations, B is chosen such that the distance between two points bearing the same index, i.e., $q_{i+B} - q_i = B\delta$, should be minimal, but still greater than the range of the noise W, i.e., $B\delta \geq 1$.

Given a biometric signal X, with quantizer output U corresponding to some point q_U. Then the bin index $l(q_U)$ is the helper data message M that is transmitted to the receiver. With the above operating conditions, it is easy to see that knowledge of both Y and $l(q_U)$ enables proper recovery of the original $q_U = U$ [4]. Since both the transmitter and receiver of the genuine user has knowledge of q_U, the set of reconstruction points $\mathcal{Q}$ can be mapped to a set of binary messages/keys. In other words, q_U can be used to securely construct a binary key K for cryptographic applications. However, in the following analysis, we will not explicitly consider such a binary map; instead, an information-theoretic approach will be pursued.

3.1. Key Rate

From the operations of the WZ scheme, with the relative bin index $l(q_U)$ being the helper data message M, the achievable key rate R is a function of the quantizer spacing δ. Specifically, R is limited by the mutual information

$$R = I(U;Y) = h(Y) - h(Y|U) \tag{4}$$

with the differential entropy

$$h(Y) = -\int_Y p_Y(y) \log(p_Y(y))\, dy \tag{5}$$

and conditional differential entropy,

$$h(Y|U) = -\int_U p_U(u) \int_Y p_{Y|U}(y) \log(p_{Y|U}(y))\, dy\, du. \tag{6}$$

As discussed in Sec. 2, for a uniform distribution assumption, the probability distribution function (PDF) of Y is

$$p_Y(y) = \frac{1}{2\Delta} \quad \text{for} \quad -\Delta \leq y \leq \Delta. \tag{7}$$

Also, since U is the quantized output of uniformly distributed X,

$$p_U(u) = \sum_{m=-\Delta/\delta}^{\Delta/\delta} \frac{\delta}{2\Delta} \times \text{Impulse}(u - m\delta). \tag{8}$$

Next, let $V = E + W$, so that $p_V(v) = p_E(e) \otimes p_W(w)$. Then,

$$p_{Y|U}(y|u = u_i) = \frac{\delta}{2\Delta} \times \text{Impulse}(u - m_i\delta) \otimes p_V(v) \tag{9}$$

where we have chosen the impulse corresponding to the given value of $u = u_i$. After substitution and simplification, we obtain

$$R = \begin{cases} \log_2(2\Delta) \; - \; \dfrac{\delta}{2\log_e 2}, & \delta < 1 \\ \log_2(2\Delta) \; - \; \dfrac{\delta - 1}{\delta}\log_2(\delta) + \\ \qquad \dfrac{2\delta}{\log_e(2)}\left(\dfrac{-\log_e(\delta)}{2\delta^2} - \dfrac{1}{4\delta^2}\right), & \delta > 1. \end{cases} \tag{10}$$

3.2. MSE Distortion

For privacy preservation in biometric systems, it is desirable that the original biometric X is not divulged, even with the accidental loss of the secret key K (mapped from the reconstruction point q_U) [1, 6]. Therefore, in considering the distortion, knowledge of not only the helper data but also the key is assumed. Then, for the WZ scheme, the distortion is: $E = U - X$, resulting in the MSE distortion,

$$D = \text{Power of } E = \int_{-\frac{\delta}{2}}^{\frac{\delta}{2}} \frac{e^2}{\delta}\, de = \frac{\delta^2}{12}. \tag{11}$$

3.3. Mutual Information

The privacy leakage can also be quantified by the mutual information, $I(X; M, K)$, between the biometric X and the attacker knowledge of helper data M and the key K. In the WZ case, the attacker can recover $q_U = U$, given M and K. Thus, the conditional probability distribution $p_{X|M,K}$ reduces to a window of size δ around a known quantization point, viz., it reduces to E, so that

$$\begin{aligned} I(X; M, K) &= h(X) - h(X|M, K) = h(X) - h(E) \\ &= \log_2(2\Delta) - \log_2(\delta). \end{aligned} \tag{12}$$

4. QIM SCHEME

In the QIM key binding scheme, an ensemble of shifted quantizers is utilized. The complete encoder/decoder operations of the QIM system are described in [2, 3]. For the purpose of this paper, the following salient points are recapitulated. In QIM, the identity or label m of each quantizer corresponds to a secret key K. Then, for a given key K to be bound, the corresponding quantizer Q_m is used to quantize the biometric signal X, producing the output $Q_m(X)$. The helper data message M is the difference between the quantized version and the original biometric. With the appropriate parameters, the genuine user can successfully recover the original label m upon verification, given knowledge of M and Y [2].

4.1. Key Rate

As mentioned in Sec. 2, the possibility of intentional noise addition for enhanced privacy is of interest. Thus, consider the general form of the helper data $M = Q_m(X + N) - (X + N)$, so that the case without noise added corresponds to $N = 0$. Upon verification, decoding is performed by first adding the helper data to the measured biometric: $M + Y = Q_m(X + N) - (X + N) + Y = Q_m + W - N$ [2]. Furthermore, the same decoding behavior is achieved with the quantity $Q_m + W + N$, i.e., due to the symmetry of the random variable N. Therefore, the preceding quantity is henceforth considered as the information available at the decoder.

For the QIM ensemble, the set of reconstruction points from all quantizers creates an equivalent fine quantizer. It is easy to see that successful operations require the fine quantizer spacing δ to be greater than $N_L + 1$. From an information-theoretic perspective, the key rate is the difference between the rate where the inter quantizer spacing is minimum and the rate for a single quantizer,

$$\begin{aligned} R &= I(Q_m + W + N; Q_m) - I(U; X) \\ &= h(Q_m + W + N) - h(Q_m + W + N|Q_m) \\ &\quad - (h(X) - h(X|Q_m)). \end{aligned} \tag{13}$$

Each term in the preceding expression can be evaluated for the QIM scheme as follows. First, we have

$$h(X) = \log_2(2\Delta) \tag{14}$$

and

$$\begin{aligned} h(X|Q_m) = h(E+N) &= \frac{\delta - N_L}{\delta}\log_2(\delta) \\ &- \frac{2\delta \times N_L}{\log_e(2)}\left(\frac{1}{2\delta^2}\times\log_e(\frac{1}{\delta}) - \frac{1}{4\delta^2}\right). \end{aligned} \tag{15}$$

The remaining quantities have different expressions depending on the two conditions, $N_L \leq 1$ and $N_L > 1$, arising because of the different forms of the PDFs for $W+N$ as the range of N is greater than, or less than, that of W respectively.

Specifically, for $N_L \leq 1$,

$$\begin{aligned} h(Q_m + W + N) &= 2\times\log_2\left(\frac{2\Delta}{N_L+1}\right)\times\frac{1-N_L}{2} \\ &- 2\times\frac{N_L}{\log_e(2)}\times\left(\frac{2\Delta}{N_L+1}\right)^2 \\ &\times\left[\frac{(\frac{N_L+1}{2\Delta})^2\times\log_e(\frac{N_L+1}{2\Delta})}{2} - \frac{(\frac{N_L+1}{2\Delta})^2}{4}\right] \end{aligned} \tag{16}$$

and,

$$h(Q_m + W + N|Q_m) = \frac{N_L}{2\log_e(2)}. \tag{17}$$

Similarly, for $N_L > 1$,

$$\begin{aligned} h(Q_m + W + N) &= \frac{2}{N_L}\times\log_2\left(\frac{2\Delta\times N_L}{N_L+1}\right)\times\frac{N_L-1}{2} \\ &- 2\times\frac{N_L}{\log_e(2)}\times\left(\frac{2\Delta}{N_L+1}\right)^2 \\ &\times\left[\frac{(\frac{N_L+1}{2\Delta\times N_L})^2\times\log_e(\frac{N_L+1}{2\Delta\times N_L})}{2} - \frac{(\frac{N_L+1}{2\Delta\times N_L})^2}{4}\right] \end{aligned} \tag{18}$$

and,

$$\begin{aligned} h(Q_m + W + N|Q_m) &= \frac{N_L-1}{N_L}\log_2(N_L) \\ &- \frac{2N_L}{\log_e(2)}\left(\frac{-\log_e(N_L)}{2N_L^2} - \frac{1}{4N_L^2}\right). \end{aligned} \tag{19}$$

Then, it is straightforward to substitute (14)-(19) into (13) to obtain an explicit expression for the key rate. It should be noted, for these computations, that $\delta < \Delta$, and that it must be ensured the error distribution E remains uniform, possibly by wraparound.

4.2. MSE Distortion

As in the WZ case, the distortion is evaluated assuming knowledge of both M and K. Given K, the $n = \frac{2\Delta}{\delta}$ possible reconstruction points in the corresponding quantizer Q_m are also known. Then, an attacker can narrow down the original biometric to be one of the n equally likely points, spaced δ apart. The minimum distortion occurs when the original biometric is in the center of the range. This lower bound in distortion can be computed as follows. First, for $N = 0$

$$\begin{aligned} D &= \begin{cases} \sum_{i=1}^{\frac{n}{2}} \frac{2\times(i\delta)^2}{n} - \frac{1}{n}\times(\frac{n\delta}{2})^2, & n \text{ even} \\ \sum_{i=1}^{\frac{n-1}{2}} \frac{2\times(i\delta)^2}{n}, & n \text{ odd} \end{cases} \\ &= \begin{cases} \dfrac{2\,\Delta^2 + \delta^2}{6}, & n \text{ even} \\ \dfrac{4\,\Delta^2 - \delta^2}{12}, & n \text{ odd.} \end{cases} \end{aligned} \tag{20}$$

Next, since the intentional noise is independently added, its noise power $\frac{N_L^2}{12}$ can be simply added to (20) to obtain the distortion for the general case.

4.3. Mutual Information

In this case, the conditional PDF $p_{X|M,K}$ reduces to a series of $\frac{2\Delta}{\delta}$ windows of width N_L (because of the error due to noise), value $\frac{\delta}{N_L\times 2\Delta}$, centered on points spaced δ apart (because these are possible values of X given the quantization error and set of quantization points). Then,

$$\begin{aligned} I(X;M,K) &= h(X) - h(X|M,K) \\ &= \log_2(2\Delta) + \frac{2\Delta}{\delta}\int_{N_L/2}^{N_L/2}\frac{\delta}{2\Delta\times N_L}\times\log_2\left(\frac{\delta}{2\Delta\times N_L}\right) \\ &= \log_2\left(\frac{\delta}{N_L}\right). \end{aligned} \tag{21}$$

The above analysis shows the necessity, in controlling leakage, of the intentional noise addition, without which the mutual information is infinite. However, this is at the expense of a reduced key rate.

5. DISTORTION-ENHANCED WYNER-ZIV SCHEME

As will be seen in Sec. 6, the WZ approach suffers from low distortion, but delivers high key rate. By contrast the QIM method exhibits superior distortion performance. This desirable characteristic is emulated in DE-WZ. Here, the WZ approach is modified so that the keys are assigned with a multiple mapping scheme, with β bins assigned to the same key. Hence, even if K is known, there will be β bins that might have produced the key. For maximum privacy, the bins that map to the same key are spaced $\frac{\Delta}{\beta-1}$ apart.

5.1. Key Rate

Let OR be the key rate from (10) of the original WZ scheme, so that there are $n = 2^{OR}$ possible keys. Then for a multiple mapping scheme with duplication factor β, there are effectively $\frac{n}{\beta}$ keys for coding. Thus, for DE-WZ, the rate $R = \log_2\left(\frac{n}{\beta}\right)$.

5.2. MSE Distortion

In this scheme, the distortion is due to the uncertainty regarding which of the β points actually produced the key. The lower bound of the distortion occurs for a point located in the center of the range. If d is the distance between adjacent bins mapping to the same key,

then $d = \frac{\Delta}{\beta-1}$, so that the lower bound distortion can be found as

$$D = \begin{cases} \sum_{i=1}^{\frac{\beta}{2}} \frac{2\times(id)^2}{\beta} - \frac{1}{\beta} \times (\frac{\beta d}{2})^2 + \frac{\delta^2}{12}, & \beta \text{ even} \\ \sum_{i=1}^{\frac{\beta-1}{2}} \frac{2\times(id)^2}{\beta} + \frac{\delta^2}{12}, & \beta \text{ odd} \end{cases}$$
$$= \begin{cases} \left(\frac{\Delta^2}{12\left(\beta-1\right)^2} \times \left(\beta^2+2\right) \right) + \frac{\delta^2}{12}, & \beta \text{ even} \\ \left(\frac{\Delta^2}{12\left(\beta-1\right)^2} \times \left(\beta^2-1\right) \right) + \frac{\delta^2}{12}, & \beta \text{ odd.} \end{cases} \quad (22)$$

5.3. Mutual Information

Here, the conditional PDF $p_{X|M,K}$ reduces to a series of β windows (because there are β duplicates) of width δ (because of the error due to quantization), value $\frac{1}{\beta\delta}$ (corresponding to the multiple mapped keys), centered on points spaced $\frac{\Delta}{\beta-1}$ apart. Then,

$$\begin{aligned} I(X;M,K) &= h(X) - h(X|M,K) \\ &= \log_2(2\Delta) + \beta \int_{-\delta/2}^{\delta/2} \frac{1}{\delta\times\beta} \times \log_2(\frac{1}{\delta\times\beta}) \quad (23) \\ &= \log_2(2\Delta) - \log_2(\delta\times\beta). \end{aligned}$$

6. RESULTS AND DISCUSSIONS

Fig. 1 and Fig. 2 show the achievable key rate performances as a function of the distortion and the mutual information, respectively, for the three key binding cases considered. It can be observed that the WZ scheme has a high key rate, but low distortion. Furthermore, any attempt to increase the distortion, or lower the mutual information, leads to a loss in the key rate, presenting an inherent tradeoff between rate and distortion, mutual information.

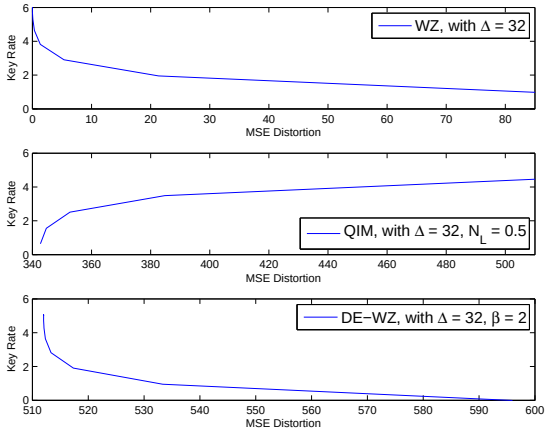

Fig. 1. Trade-off between Key Rate and MSE Distortion

For the QIM scheme, we can observe a high square error distortion, a lesser key rate than Wyner Ziv, but high mutual information, especially for low noise levels. Increasing the key rate can simultaneously increase the distortion, provided one remains within system limits, but leads to a rise in mutual information. Lowering mutual information by increasing noise also increases the distortion (though not significantly), but leads to a loss in the rate.

For the DE-WZ scheme, the key rate is sacrificed for an increase in distortion and loss in mutual information. Increasing the MSE distortion and lowering the mutual information by assigning more keys to the multiple mapping scheme, or by increasing the number of duplicates for each key, both lead to a loss in key rate. Therefore, the performance tradeoffs in this case can be controlled via the parameter β.

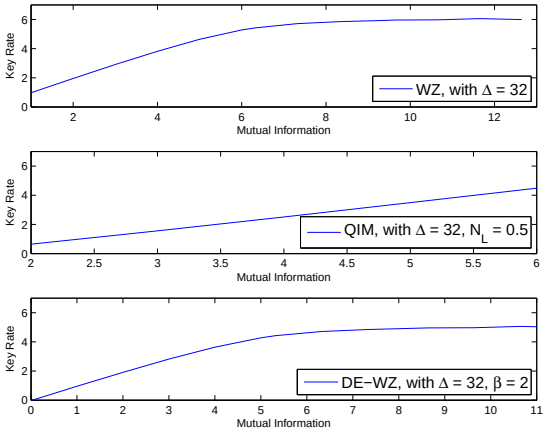

Fig. 2. Trade-off between Key Rate and Mutual Information

7. CONCLUSION

In this paper, a theoretical analysis of various key binding schemes is presented. The performance limits are evaluated with respect to the key rate, as a function of distortion and mutual information. These quantities establish the upper bounds, and operating points, that could be achieved by a practical system. The obtained results demonstrate the utility of combining desirable characteristics from the WZ and QIM approaches, in order to enhance flexibility in controlling the tradeoffs in privacy and security.

8. REFERENCES

[1] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing, Special Issue on Pattern Recognition Methods for Biometrics*, 2008.

[2] F. M. Bui, K. Martin, H. Lu, K. N. Plataniotis, and D. Hatzinakos, "Fuzzy key binding strategies based on quantization index modulation (QIM) for biometric encryption (BE) applications," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 118–132, Mar. 2010.

[3] 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," *IEEE Systems Journal, Special Issue on Biometrics Systems*, vol. 3, no. 4, Dec. 2009.

[4] Qian Xu and Zixiang Xiong, "Layered Wyner-Ziv video coding," *IEEE Trans. Image Processing*, vol. 15, no. 12, Dec. 2006.

[5] Lifeng Lai, Siu-Wai Ho, and H. Vincent Poor, "Privacy-security tradeoffs in biometric security systems," in *Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL*, Sept. 2008.

[6] Tanya Ignatenko and Frans Willems, "Biometric systems: Privacy and secrecy aspects," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 4, pp. 956–973, Dec. 2009.