A Zero-Leakage Fuzzy Embedder From the Theoretical Formulation to Real Data

Gabriel Emile Hine, *Student Member, IEEE,* Emanuele Maiorana, *Member, IEEE,* and, Patrizio Campisi *Senior Member, IEEE*

***Abstract*—In this paper we present a novel biometric cryptosystem obtaining perfect security, that is not leaking any information about the employed secret key from the knowledge of the stored helper data. While similar purposes have already been sought in literature, the approaches proposed so far have been evaluated in terms of recognition performance under the unrealistic assumption of ideal statistical distributions for the considered biometric data. Conversely, in this paper we investigate the applicability of the proposed framework to practical scenarios, while managing a trade-off between privacy and recognition performance. This goal has been achieved by introducing a class of transformation functions enforcing zero-leakage secrecy, by designing an adaptive strategy for embedding the secret key bits into the selected features, and by developing a system parameters optimization strategy with respect to security, recognition performance and privacy. Experimental tests conducted on real fingerprint data prove the effectiveness of the proposed scheme.**

I. Introduction

BIOMETRIC template protection has recently triggered the attention of both the research and the industrial community, due to the widespread social perception of the potential damages which could derive from the loss of secrecy and control over biometric traits [1].

As well know, the use of biometric data raises many security issues which are peculiar of biometrics-based recognition systems, not affecting other approaches employed for automatic people authentication. In fact, some biometrics such as voice, face, fingerprints and many others are exposed traits, they are not secret and therefore they can be covertly acquired or stolen by an attacker and misused. This can lead for example to identity theft. Moreover, raw biometrics cannot be revoked, canceled, or reissued if compromised, since they are user's intrinsic characteristics and they are in limited number. Therefore, if a biometrics is compromised, all the applications making use of that biometrics are compromised, and since biometric identifiers are permanent an issue is raised when it is needed to change them. The use of biometrics poses also many privacy concerns. In fact, when an individual gives out his biometrics, either willingly or unwillingly, he discloses unique information about himself. It has also been demonstrated that biometric data can contain relevant information regarding people health. This information can be used, for instance, to discriminate people for hiring or to deny insurance to those with latent health problems. The use of biometrics can also raise cultural-, religious- as well as ethnicity-related concerns. To some extent, the loss of anonymity can be directly perceived by users as a loss of autonomy.

Several schemes have been therefore proposed in recent years with the aim of protecting the templates stored in biometric databases, guaranteeing the properties of renewability, security and performance [2], [3]. Such approaches have been typically categorized into two major classes: cancelable biometrics and biometric cryptosystems [4].

The former kind of approach is based on the adoption of non-invertible transformation functions, whose defining parameters may be made publicly available or not [5]. Typically, in these cases the robustness analysis, that is the possibility of reverting the employed transformations, are not dealt with much details, due to both the difficulty in quantitatively evaluating the actual non-invertibility, and to the heterogeneity of the proposed approaches, which makes it arduous to define general metrics upon which evaluating the provided security.

Conversely, biometric cryptosystems [6], where cryptographic protocols encounter biometrics, have been object of extensive study, and metrics for assessing security and privacy have been proposed in literature. Specifically, several peculiar attacks against such template protection approaches have been described in [7] and [8]. Among them, one of the most threatening consists in the non-randomness attack, where the knowledge about the global statistics of the employed biometric data is exploited to obtain information about the secrets protected by the system. In more details, different information theoretic studies have deeply analyzed key-binding approaches, based on the combination of biometric information with secret cryptographic keys, trying to evaluate which amount of information is leaked by the resulting helper data regarding the original secret sources.

A fundamental trade-off between privacy, intended as the hardness of retrieving the original biometric information from the stored helper data, and security, measured by the uncertainty about the adopted cryptographic key, has been given in [9] and [10]. Further insights about the trade-off existing among security, privacy, and achievable recognition rates have been also discussed in [11], where it has been demonstrated that a system can obtain better recognition performance at the expenses of an increased leakage about the employed secret key and the adopted biometric data. The aforementioned theoretical investigations have also proven that, although privacy leakage is unavoidable, perfect security may be possible from an information-theoretical point of view. Nonetheless, this

G. E. Hine, E. Maiorana, P. Campisi, are with the Section of Applied Electronics, Department of Engineering, Roma Tre University, Via Vito Volterra 62, 00146, Rome, Italy
e-mail: {gabriel.hine, emanuele.maiorana, patrizio.campisi}@uniroma3.it

Please cite this work as:
G. E. Hine, E. Maiorana and P. Campisi, "A Zero-Leakage Fuzzy Embedder From the Theoretical Formulation to Real Data," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 7, pp. 1724-1734, July 2017.
doi: 10.1109/TIFS.2017.2686005

can be achieved only assuming some unrealistic requirements for practical biometric representations, such as the use of uncorrelated features with uniform distributions, as in [12] for fingerprint data.

The few attempts that have tried to empirically evaluate the protection provided by key-binding approaches applied to real biometric data, such as signature in [13], face in [14] and [15], iris in [16] and [17], and electroencephalography in [18], have shown that a very significant reduction of security, and a notable increase of privacy leakage, occur when biometric features with a non-ideal distribution are taken into account in practical scenarios.

Indeed, as further discussed in Section II, in [19], [20] and [21] some procedures to map biometrics data distributions into ideal ones have been proposed. Nonetheless, also in the aforementioned scenarios, the analysis has been carried out employing only synthetic data modeled as independent features, thus preventing to draw general conclusions when dealing with real-world biometrics. To the best of our knowledge, a template protection scheme able to provide perfect security against non-randomness attacks, also indicated as zero-leakage, and proved to be applicable to practical scenarios, is therefore still missing in literature.

Within this scenario, the goal of this paper is the proposition of a novel approach which allows the construction of a zero-leakage template protection system, applicable to real-world biometric data, still able to guarantee satisfactory privacy and recognition performance. As detailed in Section III-C, the proposed framework is also designed in order to endure attacks based on the exploitation of false acceptance rate (FAR) [22], [23], where a malicious user tries to get access to the system, by performing several recognition trails authentication.

The paper is organized as follows. A summary of the fundamental concepts regarding zero-leakage template protection schemes is given in Section II, where the approach proposed for achieving the desired perfect security, generalizing the method employed in [20], is also introduced. The proposed secure framework is presented in Section III, where the elements designed in order to allow the system achieving proper privacy and recognition performance are discussed in details. The performed experimental tests, carried out on a large real world fingerprint database, are then described in Section IV, while conclusions regarding the proposed method are eventually given in Section V.

II. Zero-Leakage Template Protection: Preliminaries

In this section we first introduce the conditions under which a zero-leakage biometric cryptosystem can be designed and then we sketch the rational behind the proposed template protection scheme, detailed in Section III. Specifically, the proposed secure system relies on quantization index modulation (QIM) [24], often employed to describe how to bind a generic biometric feature-based representation with a randomly generated secret key [25], and briefly summarized in Section II-A. The information leakage analysis is discussed in Section II-B, where it is also outlined how the proposed solution generalizes the state-of-the-art zero-leakage protection schemes.

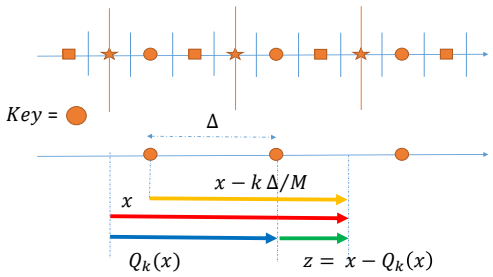


Fig. 1: QIM Principle.

A. Quantization Index Modulation

In its general exploitation, QIM allows to embed a secret key into a noisy signal. This is achieved by exploiting a set of A quantizers, being A the number of alphabet symbols, each employing different quantization levels. Assuming that the host signal x is scalar, the A quantizers can be defined by means of one uniform quantizer. Specifically, a uniform scalar quantizer $Q(x)$ with step Δ is defined as $Q(x) = \Delta \left\lfloor \frac{x}{\Delta} \right\rfloor$, with the $\lfloor \cdot \rfloor$ operator mapping its argument to the largest previous integer. The function $Q(x)$ can be used to generate A different quantizers as:

$$Q_m(x) = Q\left(x - m\frac{\Delta}{A}\right) + m\frac{\Delta}{A}, \tag{1}$$

where $m = 0, 1, 2, \ldots, A-1$. Storing $Q_m(x)$ instead of x for a given application allows to carry information on both the original signal as well as on the considered secret key m. An example of the reproduction levels of the quantizers set $\{Q_0, Q_1, ..., Q_{A-1}\}$ when $A = 3$ is given in Figure 1.

When applied for the purpose of protecting a biometric information x extracted during the user enrolment, the QIM approach can be exploited to generate an helper data z as the difference between the original signal x and its quantized version $Q_m(x)$ obtained through the $m-th$ quantizer, often also indicated as code-offset, that is,

$$z = x - Q_m(x). \tag{2}$$

For our purposes (2) can be written as:

$$z = \left[x - m\frac{\Delta}{A}\right]_\Delta = \left[[x]_\Delta - m\frac{\Delta}{A}\right]_\Delta, \tag{3}$$

being $[\cdot]_\Delta$ the modulo Δ operation. Ideally, the storage of z should not reveal any information regarding either x or m, while allowing to perform recognition when a fresh template $\tilde{x}$ is made available, by retrieving the embedded key as:

$$\hat{m} = \arg\min_{\tilde{m}} \left| \tilde{m}\frac{\Delta}{A} - [\tilde{x} - z]_\Delta \right|. \tag{4}$$

If $\tilde{x}$ and x were identical, then $[\tilde{x} - z]_\Delta$ will be equal to $m\frac{\Delta}{A}$, and the extracted key $\hat{m}$ will be equal to m. More likely, $\tilde{x}$ is a noisy version of x, and the quantization step Δ has to be chosen accordingly to allow the retrieval of the original key.

B. Information Leakage

The main issue of a QIM-based biometric template protection scheme is the possible information leakage of the

helper data z about both the adopted key m and the biometric template x in a non-randomness attack, which exploits the knowledge of the global statistics of the signal x and of the employed quantization step Δ [26]. Specifically, in this scenario, if we consider mutually independent template coefficients, the amount of information revealed by the helper data z about the secret key m can be quantified by the mutual information between the two variables:

$$\begin{aligned} I(M,Z) &= h(Z) - h(Z|M) = \\ &= h(Z) - h\left([X - M\tfrac{\Delta}{A}]_\Delta | M\right) = \\ &= h(Z) - h([X]_\Delta | M) = \\ &= h(Z) - h([X]_\Delta), \end{aligned} \tag{5}$$

where $h(\cdot)$ denotes the differential entropy operator. It can be observed that, in case $[X]_\Delta$ has a uniform distribution in $[0;\Delta]$, the mutual information between Z and M would be zero:

$$I(M,Z) = \log\Delta - \log\Delta = 0. \tag{6}$$

The above condition would therefore guarantee a zero-leakage template protection system, in which the stored helper data z would not reveal any information about the employed secret m. In this regard, it has been demonstrated [27] that the necessary and sufficient condition to have $[X]_\Delta$ uniformly distributed is that the characteristic function (CF) of X, defined as the Fourier transform of its probability density function (PDF), satisfies the condition:

$$\varphi_X\left(\frac{2\pi l}{\Delta}\right) = 0, \;\; \forall l \neq 0. \tag{7}$$

Unfortunately, as already commented in Section I, it is unlikely to deal with real-world biometric data characterized by such property. It is therefore hard to implement practical zero-leakage biometric protected systems. Nonetheless, it is possible to apply some preprocessing to the extracted features in order to generate variables X having the desired characteristic as in (7).

Specifically, the addition of noise, with a uniform distribution in $[-\frac{\Delta}{2};\frac{\Delta}{2}]$, to the original values in x, before applying quantization, has been suggested in [19]. According to this approach, being the PDF of the sum of two independent random variables given by the convolution of the two PDFs, the CF of the resulting variable is given by the product of the respective CFs. In general, any random variable satisfying the condition (7) can be therefore employed as additive noise. However, this approach suffers from a severe drawback since it requires the presence of another key that must be kept secret. The key is in fact required during the verification phase to let the system generate the same noisy signal. Therefore, the need to store this additional information is not of practical use in many contexts.

A preferable solution has been proposed in [20] and in its extension [21], where a fuzzy extractor framework [28] is defined on the basis of a punctual transformation, applied to the originally extracted features W in order to make their distribution uniform. This goal is achieved by applying to the data w a monotonic increasing function given by the cumulative distribution function (CDF) of W itself, that is:

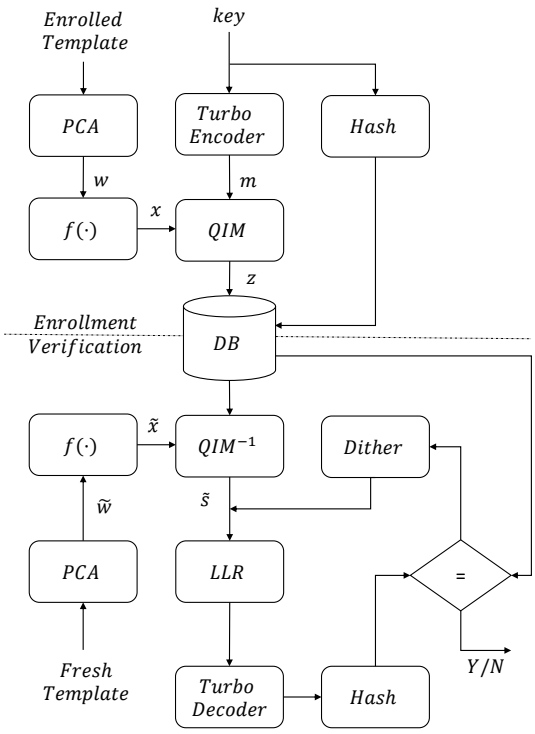


Fig. 2: Proposed biometric template protection scheme.

$$x = f(w) = CDF_W(w), \tag{8}$$

thus generating a uniformly distributed variable X. It is worth pointing out that although this approach satisfies (7), it is not the only possible solution to the above mentioned goal.

In fact, in this paper we propose a generalization of (8) as follows:

$$x = f(w) = {CDF_X}^{-1}\left[CDF_W(w)\right], \tag{9}$$

where CDF_X can be selected as any function representing the cumulative distribution function of a variable whose CF satisfies (7). The here proposed generalization (9) introduces a higher degree of freedom which we will exploit for selecting a transformation function that, still guaranteeing the needed zero-leakage requirements, could allow us optimizing other performance metrics of the proposed system, such as achievable recognition rate, security, or template irreversibility.

The proposed zero-leakage biometric cryptosystem, based on the use of the approach described in (9), is presented in Section III, where a family of transformation functions able to satisfy the property in (7) is introduced, and the practical implementation strategies designed to achieve the desired performance when using real biometric data are presented. It is worth specifying that, given the above considerations, the biometric cryptosystem here presented is able to provide zero-leakage security against non-randomness attacks, which assume potential attackers possess the knowledge regarding global statistics of the employed biometrics. More treacherous attacks, such as those where the attacker already knows specific information regarding the biometrics of the interested user [29], are not taken into account in the following discussion.

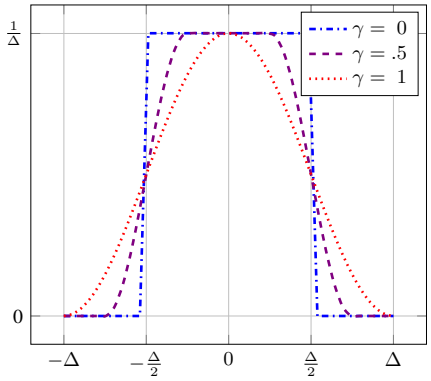


Fig. 3: Raised Cosine Probability Density Function.

III. The Proposed Biometric Cryptosystem

The proposed template protection scheme, described in Figure 2, besides not leaking any information about the employed secret through the stored helper data, (see [19], [20]), leverages on the generalization presented in (9) to guarantee proper performance in terms of recognition rate, security, and template irreversibility, when applied to actual biometric scenarios.

In details, the preprocessing performed on the features extracted from a given biometrics is described in Section III-A. The class of transformation functions proposed for the generation of templates satisfying (7) is introduced in Section III-B. The effects resulting from the selection of a specific transformation family on the achievable recognition rates, as well as on the level of security of the proposed system, are discussed in Section III-C through the analysis of the embedding capacity per template coefficient. An evaluation of guaranteed template irreversibility, handled in terms of system privacy leakage, is provided in Section III-D. In Section III-E a procedure to determine the system configuration to trade-off between security and privacy is then described. Eventually, in Section III-F we introduce a method to improve the recognition capability of the proposed protected system in terms of false recognition rate (FRR), while keeping unaltered the other performance metrics. It is worth pointing out the proposed method, differently from zero-leakage state of the art approaches, is validated through an analysis conducted on real biometric data.

A. Template Preprocessing

The description of QIM in Section II-A, as well as the discussion about its information leakage when used for data protection in Section II-B, has been conducted considering biometric information represented through mutually independent coefficients. Conversely, commonly employed feature-based template representations comprise a large number of strongly correlated coefficients. Nonetheless, the approaches described in Section II are still applicable to real biometric scenarios by performing a decorrelation process over the available data as preliminary step of both the enrolment and verification stages. This goal can be achieved resorting to techniques such as principal component analysis (PCA) or linear discriminant analysis (LDA), given that the statistics of the target population's biometrics can be considered known. The following discussions are therefore carried out by describing the proposed operations as being applied in a coefficient-wise manner, having assumed that the treated biometric templates w are composed by a collection of practically independent scalar components.

It is however worth remarking that, even if the application of PCA or analogous transformations to the considered biometric data is needed in the proposed approach to achieve the desired zero-leakage property, such operation usually produces features with an increased intra-class variability with respect to the original ones, which makes often difficult to keep low the FRR in a protected system. In more detail, due to the PCA energy compaction property, the generated components are typically characterized by significantly different statistical properties. Therefore, in order to exploit such property we propose an adaptive modulation technique described in Section III-C, and a dithering-based performance improvement method in Section III-F, meant to guarantee proper recognition rates when the aforementioned preprocessing is adopted.

B. Proposed Class of Transformations

After the decorrelation process described in Section III-A (see Figure 2) each generated component is transformed so that the distribution of the obtained coefficient satisfies the condition in (7). To this aim, the CDF_X function in (9) is here defined through the cumulative distribution function of the raised cosine class of functions as:

$$rc_\gamma^\Delta(x) = \begin{cases} \frac{1}{\Delta} & |x| < \frac{\Delta}{2}(1-\gamma) \\ \frac{1}{2\Delta}\left(1-\sin\frac{\pi(x-\frac{\Delta}{2})}{\Delta\gamma}\right) & \frac{\Delta}{2}(1-\gamma) < x < \frac{\Delta}{2}(1+\gamma) \\ \frac{1}{2\Delta}\left(1+\sin\frac{\pi(x+\frac{\Delta}{2})}{\Delta\gamma}\right) & -\frac{\Delta}{2}(1+\gamma) < x < -\frac{\Delta}{2}(1-\gamma) \\ 0 & \text{otherwise} \end{cases} \tag{10}$$

where $0 \leq \gamma \leq 1$. Figure 3 shows the PDFs associated to different values of γ. It can be observed that the approach employed in [20] and [21] can be considered as a particular case of the proposed method for $\gamma = 0$. On the contrary, in our approach, by varying γ in (9), we are able to trade-off between recognition, security and privacy performance, as detailed in the next sections.

C. Embedding Capacity Estimation: Adaptive Modulation

With reference to Figure 2, after the template w has been processed according to (7) in order guarantee zero-leakage, the QIM technique described in Section II-A is employed to embed $B = \log_2(A)$ secret bits into each template coefficient x, thus generating the stored helper data z. Specifically, the embedding can be performed by resorting to the digital modulation paradigm described in [13], where an original secret key of length k is fed to an n/k turbo encoder, in order to generate symbols s belonging to a phase-shift keying (PSK) constellation of size A. Once a fresh biometric is acquired during the verification stage, a possibly corrupted codeword

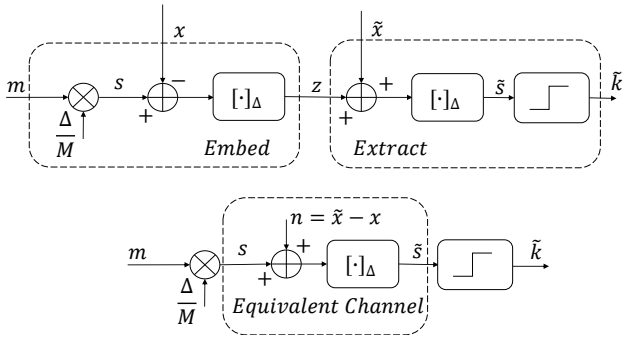


Fig. 4: Channel seen by the encoded secret key.

is retrieved by combining the available information with the stored helper data, and turbo codes are employed as in [13] to perform soft demodulation. This allows to fully exploiting the error correction capacity of the adopted codes.

It has to be remarked that the size of the employed constellations can be chosen adaptively with respect to each symbol. In fact, according to the proposed approach, the number of bits embedded into each coefficient x depends on its discriminative power, as well as on the parameter γ employed in the associated raised cosine transformation function.

In order to gain more insights about the proposed approach, let us consider the equivalent channel, depicted in Figure 4, seen by the encoded secret m from its embedding (during enrolment) to its extraction (during verification) [30]. It can be in fact modeled through the introduction of an additive independent phase noise, given by the difference between the enrolled template x and the one presented during the verification phase $\tilde{x}$. Having indicated with s the PSK transmitted symbol, $s = m\frac{\Delta}{A}$ with $\Delta = 2\pi$, and with r the equivalent noise given by the difference between the enrolled template x and the fresh one $\tilde{x}$, the received noisy PSK symbol $\tilde{s}$ is obtained as:

$$\begin{aligned}\tilde{s} &= [\tilde{x} - z]_\Delta = [\tilde{x} - [x - s]_\Delta]_\Delta = \\ &= [s + (\tilde{x} - x)]_\Delta = [s + r]_\Delta.\end{aligned} \tag{11}$$

In the genuine hypothesis (H_0) case, the characteristics of the phase noise r depend on the intra-class variability of the considered biometric representation, while in the impostor hypothesis (H_1) case, its statistics depend on the inter-class variability. We can therefore define two distinct channel capacities, giving the theoretical upper bounds on the rate at which information can be reliably transmitted over the equivalent channels under the two hypotheses, according to Shannon's definition: the genuine capacity C_{H_0} and the impostor capacity C_{H_1}, depending on the user typology at the verification stage. In the considered scenario, such capacities give us respectively the upper and lower boundaries for the information on the secret key which can be reliably transmitted over the equivalent channel:

$$C_{H_1} < \frac{k}{n}B < C_{H_0}, \tag{12}$$

being $\frac{k}{n}B$ the portion of the secret key entropy conveyed through the B bits embedded into the considered coefficient. Such percentage cannot exceed the genuine capacity C_{H_0}, since otherwise genuine users would not have any chance to correctly decode the secret. On the other hand, if such percentage is considerably lower than the non-genuine capacity C_{H_1}, the FAR would become unacceptable in practical applications. It has also to be remarked that, since the number of coefficients x in the available templates is usually limited, the employed error correcting codes won't be able to reach their best possible decoding performance, theoretically close to the Shannon's limit [31]. Therefore, it is recommended to have an adequate margin from the upper bound, while this is not required for the lower bound. Being possible for the considered coefficients x to significantly vary statistically-wise, and therefore in the associated capacity as a consequence, the number of bits to be allocated to each component should be chosen in an adaptive manner.

In order to evaluate the channel capacities C_{H_0} and C_{H_1}, given (11) the former can be expressed as:

$$\begin{aligned}C_{H_0} &= \max_{p_Z(z)} I(S, \tilde{S}) \\ I(S, \tilde{S}) &= h(\tilde{S}) - h(\tilde{S}|S) \\ &= h(\tilde{S}) - h([S + R]_\Delta|S) \\ &= h(\tilde{S}) - h([R]_\Delta) \\ \max\ h(\tilde{S}) &= -\int_0^\Delta \frac{1}{\Delta} log \frac{1}{\Delta} d\tilde{s} = log\Delta \\ \rightarrow C_{H_0} &= log\Delta - h([R]_\Delta),\end{aligned} \tag{13}$$

being the domain of $\tilde{S}$ bounded in $[0; \Delta]$, and being the differential entropy of limited domain random variable maximum when uniformly distributed.

The capacity C_{H_1} turns out to be equal to zero since, under the hypothesis of a non-genuine user during verification, the equivalent noise $[R]_\Delta$ is uniform in [0,Δ] due to the adoption of the proposed feature transformation in (9)[1]. This implies that the system operating point is implicitly set such that the FAR is next to zero, making the proposed protected system intrinsically robust against FAR-based attacks. The aforementioned property is a direct consequence of the design of the proposed system as a zero-leakage scheme, having a null mutual information between the key and the helper data.

Only the genuine capacity C_{H_0} has to be therefore evaluated in order to determine the number of bits B to be embedded into a given coefficient. Specifically, the assignable number of bits can be computed as:

$$B = \lfloor \frac{n}{k} \alpha C_{H_0} \rceil, \tag{14}$$

where the $\lfloor \cdot \rceil$ operator maps a real number to the closest integer value, while the parameter α is chosen within the interval $[0; 1]$ in order to let the sum of all the bits assigned to each coefficient being equal to the size n of the encoded secret key. Such bit allocation procedure implicitly selects the coefficients to be used in the system, since those with a very low capacity will have no associated bits, and will be automatically discarded from the embedding process.

It has to be pointed out that, in case the proposed class of transformations in (10) is employed to implement (9), C_{H_0}

[1]The difference between two realization of a random variable uniform distributed in $[0; \Delta]$ has a triangular distribution in $[-\Delta; \Delta]$

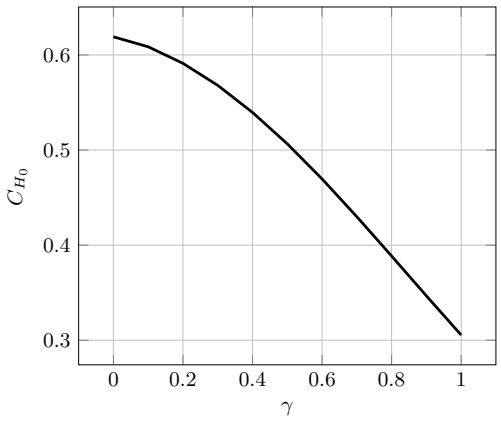


Fig. 5: Channel capacity C_{H_0} vs γ, for theoretic biometric distribution.

has a monotonically decreasing behavior with respect to the selection of the employed raised cosine parameter γ. As an example, Figure 5 shows the values obtained when considering the application of the proposed scheme to synthetic data generated with an equivalent channel having a signal-to-noise ratio (SNR) equal to $4.7dB$, suggested as characteristic of fingerprint templates in [32]. Therefore, given a coefficient and its associated statistics, the number of bits that can be embedded into it also depends on the chosen parameter γ. Specifically, since using a lower γ would ensure higher capacity values, more bits can be embedded into the employed biometric representation, with a resulting improved security $H(M|Z) = H(M) = k$, for a given encoding ratio n/k and maintaining the condition in (12) for guaranteeing a proper FRR. Likewise, for specific encoding ratio n/k and security k, achieving larger capacities C_{H_0} using lower γ parameters would result in improved FRR, being the employed error correcting codes able to better deal with the considered intra-class variability. Although such observations would lead to choose low γ values for implementing the proposed zero-leakage cryptosystem, other performance metrics worsen because of this choice. Therefore, a proper trade-off strategy is described in Section III-E.

D. Template Irreversibility: Privacy Evaluation

Together with the evaluation of the information leakage regarding the employed secret key $I(M, Z)$, a performance metric, commonly used for helper data based biometric cryptosystems, is the privacy leakage $I(X, Z)$ between the template X and the helper data Z. In this regard, this measure is not helpful when applied to a QIM approach since it diverges:

$$\begin{aligned} I(X,Z) &= h(X) - h(X|Z) = \\ &= h(X) - (-\infty) = +\infty. \end{aligned} \tag{15}$$

This happens because the random variable $X|Z$ is a discrete variable, while X is continuous. This fact does not imply that the knowledge of Z gives certain understanding of X. It is in fact due to the fact that the cardinality of X is reduced to be numerable.

Alternatively, since $X|Z$ is a discrete variable, we could measure the privacy of our scheme by means of the equivocation $H(X|Z)$ that describes the uncertainty about the template X given the knowledge of the helper data Z, commonly indicated as irreversibility:

$$\begin{aligned} H(X|Z) &= H(X|[X]_\Delta) + H([X]_\Delta|Z) = \\ &= H(X|[X]_\Delta) + H(K|Z) \end{aligned} \tag{16}$$

where $H(X|[X]_\Delta)$ represents the information loss about the template X after the modulo operation and $H(M|Z)$ relates to system security, expressing the uncertainty of the key once Z is known. It is worth pointing out that, in order to be authenticated by the system, the only required information is $[X]_\Delta$, whose equivocation related to Z is $H(M|Z)$. In fact, once m is known, $[x]_\Delta$ is univocally determined and vice versa. Nevertheless, the above mentioned irreversibility measure only provides an indication about the possibility of retrieving the template X extracted during enrolment from the stored helped data Z. More practically, due to the noisy nature of the considered biometric data, an eventual attacker could be interested in getting just an estimate of X, rather than its exact value, since it would suffice in obtaining enough information about the biometrics of the targeted user. In order to evaluate the privacy leakage associated to the proposed system in a broader sense, a more suitable index for the considered scenario can be defined as the mean root square error between the enrolled template x and its best estimation $\hat{x}(z)$ obtained from the helper data z, that is,

$$P = \frac{E_{X,M}\{(\hat{x}(z) - x)^2\}}{E_X\{x^2\}}. \tag{17}$$

Values of P range in $[0; 1]$, with larger values associated to a better privacy. The value $P = 1$ corresponds to a variance of the estimation error equal to the one of the original signal, with a consequent negligible privacy leakage. From the estimation theory the minimum square error estimator is given by:

$$\hat{x}(z) = E_X(x|z) = \int x\, p_{X|Z}(x|z)\, dx, \tag{18}$$

which can be used for estimating the privacy metrics P in (17) for the proposed zero-leakage biometric cryptosystem.

Specifically, as demonstrated in Appendix, the minimum square estimator of a variable X obtained through the application of raised cosine transforms, given the helper data Z, is:

$$\begin{aligned} \hat{x}(z) &= \int_X x p_{X|Z}(x|z) dx = \\ &= \frac{\Delta}{A} \sum_{m=0}^{A-1} \left[m\frac{\Delta}{A} + z \right]_\Delta rc_\gamma^\Delta \left(\left[m\frac{\Delta}{A} + z \right]_\Delta \right) + \\ &+ \left(\left[m\frac{\Delta}{A} + z \right]_\Delta - \Delta \right) rc_\gamma^\Delta \left(\left[m\frac{\Delta}{A} + z \right]_\Delta - \Delta \right) \end{aligned} \tag{19}$$

where $A = 2^B$ represents the number of possible symbols that can embedded in the considered coefficient using B bits. Given the aforementioned minimum square estimator, the behavior of the considered privacy metrics P with respect to the parameter γ employed in the adopted raised cosine transform is shown in Figure 6. As can be seen, the privacy of the proposed scheme

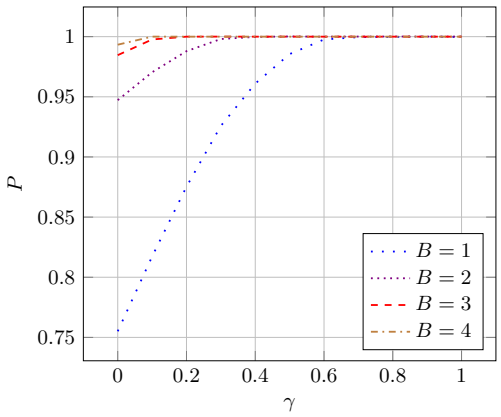


Fig. 6: Privacy leakage P vs γ, for different values of embedded bits B.

increases with the use of larger values of γ, and embedding more bits in the considered coefficients. Comparing the plots in Figure 5 and 6, it can be seen that privacy and capacity are conflicting requirements for coefficients obtained through the employed raised cosine transform. A trade-off strategy is described in the next section.

E. Transform Parameters (γ and B) Selection

As observed in the previous sections, the selection of the parameter γ of the raised cosine transform, here employed to satisfy (7), has hindering effects on the capacity and irreversibility of the associated coefficient. A proper strategy has to be therefore defined for selecting the γ parameter for each coefficient keeping both aspects into account. Specifically, we propose to choose γ as the minimum value guaranteeing a desired level of privacy $\bar{P}$. This can be achieved by applying the following iterative procedure for each available coefficient:

1) $\gamma = 0$ is assigned at an initial stage;
2) the embedding capacity C_{H_0} in estimated through (13) and the number of bits to be embedded in the coefficient is set though (14);
3) the considered privacy level is estimated by means of (17);
4) if the evaluated privacy exceeds the target threshold level $\bar{P}$, the algorithm stops, otherwise, γ is increased and the procedure restarts from step 2.

The proposed γ-selection iterative procedure has to be performed for different values of α, till reaching the one for which the sum of the numbers of bits associated to each component is equal to n, once both the system security k and the desired encoding ratio n/k have been determined. It can be observed that the proposed strategy dynamically determines both the transformation to be applied, as well as the number of bits to be embedded into the coefficient, thus implementing the adaptive modulation approach presented in Section III-C. As already remarked, and shown with the experimental results reported in Section IV, such adaptive modulation is especially relevant in case of coefficients decorrelated through techniques as PCA, which confine as much energy as possible in few components, while leaving mostly noise in the remaining ones. Typically, a high γ value is assigned to these latter coefficients, whose statistics result in a low capacity which may imply the possibility of embedding a single bit, with the consequent requirement of a high γ value for guaranteeing high privacy levels, as shown in Figure 6. Low γ values are instead associated with coefficients characterized by a high capacity, having the possibility of embedding a large number of bits into them.

It is worth pointing out that, although the proposed γ and B adaptive selection strategy requires the storage of additional information in the system, this does not affect the privacy and security of the enrolled users, since the same parameters are employed for all of them.

F. Performance Improvement through Dithering

As already pointed out, the proposed system is characterized by construction by a very low FAR, that could lead to a high FRR. In order to compromise between the two, an iterative process based on dithering is performed during the verification phase, as shown in Figure 2. Specifically, the proposed approach takes inspiration from real life when people are unable to open a door with the correct key: shaking a bit the key till all the gears of the lock are aligned often allows opening the door. Such operation typically increases the success rate of the genuine user, while having a negligible influence on the success rate of an impostor using a wrong key.

In case a match between the stored hash and the one retrieved during verification is not obtained, trying to slightly alter the template $\tilde{x}$ with an additive zero-mean uniformly distributed noise, and then attempting again to decode the resulting message, could be beneficial for improving the system recognition rate in terms of FRR, without affecting notably the associated FAR. For each treated coefficient the width of the noise distribution can be defined as a fraction of the decision interval for a PSK symbol. In the practical implementation of the proposed approach, employed to obtain the results described in Section IV-B, such noise is defined in order to be kept in the range $[-0.3\frac{\Delta}{A}; 0.3\frac{\Delta}{A}]$. The number of iterations T the system can perform while trying to correctly decoding the original secret key is obviously limited by computational time constrains. An analysis on the effects of the proposed dithering approach on the achievable performance is reported in Section IV-B.

IV. Experimental Analysis

The proposed system described in Section III is here analyzed when applied for a practical application involving fingerprint data. Section IV-A introduces the adopted template representation, as well as the database providing the employed biometric data. The performance achieved by the proposed system when applied to the considered practical scenario are then reported in Section IV-B.

A. Employed Template Representation

Without any loss of generality, we employ fingerprints to test the performance of the proposed system when applied to

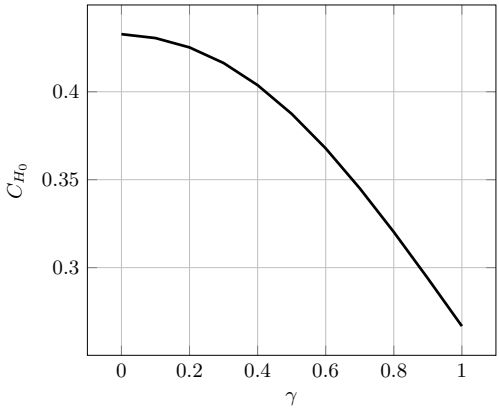


Fig. 7: Channel capacity C_{H_0} vs γ, for the considered fingerprints.

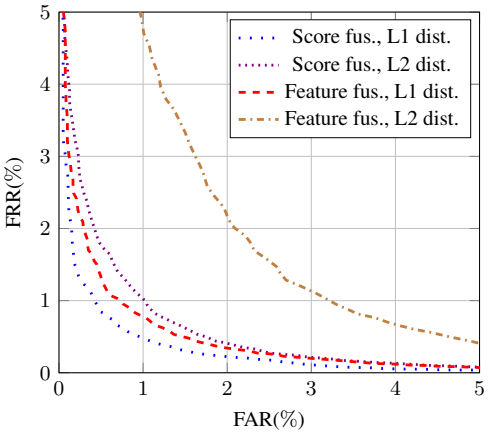


Fig. 8: Recognition performance of unprotected systems.

real data. More specifically, traditional fingerprint recognition approaches rely on the extraction of minutiae information from the analyzed traits, localizing ridge anomalies such as bifurcations or endings. Nevertheless, such technique produces templates composed by unordered sets of characteristics with variable sizes, while the proposed cryptosystem is designed to be applied to fixed-dimension ordered collections of parametric features. In order to obtain such template, the FingerCode representation proposed in [33] is here taken into account. According to this processing, a reference fingerprint point, characterized by the maximum curvature of the concave ridges, is first determined. The fingerprint region around this point is then divided into different sectors, each processed through a bank of Gabor filters used to capture both local and global fingerprint details. According to the processing described in [33], 640 features can be generated for each fingerprint.

The employed biometric data are taken from the BiosecurID DB [34], comprising 16 optical impressions for each of index and middle fingers from both right and left hands of 400 subjects. Such fingers have been acquired in the considered DB taking into account that they could be easily simultaneously captured at once, in a very fast and comfortable way, in practical recognition systems. Acquisition devices able to collect four fingerprints at one time are commercially available (e.g. [35]) and widely used in real-life critical scenarios, like the border crossing US-Visit. Such acquisition modality could be therefore easily employed to replace knowledge-based authentication procedures relying on PINs or passwords with a biometric-based approach (e.g. cash withdrawal).

The impressions from all the four available fingers of a given person are considered altogether in generating a single template, making thus available for testing a set of 16 templates composed by $4 \cdot 640 = 2560$ coefficients for each of employed 400 users.

The available dataset is split into two disjoint subsets, comprising acquisitions coming from 100 and 300 subjects. The first subset is employed to test the performance of the proposed system, as reported in the following section. The remaining 300 users are exploited to train the considered protected cryptosystem, providing the data for estimating the needed PCA projection matrix, as well for evaluating the capacity associated with each transformed component. In this regard, Figure 7 reports the actual behavior of the capacity C_{H_0} with respect to the adopted parameter γ, evaluated as mean curve over all the coefficients of the employed whitened template. It can be seen that the mean capacity estimated for the proposed fingerprint representation is significantly lower than the one reported in Figure 5, evaluated on the basis of the assumptions taken in [32], testifying the difficulty of implementing a zero-leakage cryptosystem usable with real biometric data.

It has to be remarked that, since the dimension of PCA projections is limited by the minimum between the number of classes employed for the training phase and the size of the original representation, template representations with only 299 coefficients are generated by the proposed approach, and used as templates for the method described in Section III. Larger representations with more components could be processed in case larger training databases would be available in practical applications.

B. Results Discussion

The recognition rates achievable with unprotected systems exploiting the features extracted from the considered fingerprint data are reported in Figure 8. Specifically, we have evaluated the performance reachable when fusing the information from the four available fingers of each subject at feature and score levels, using the inverse of both L1 and L2 distance metrics as matching scores. The best of the four classifiers gives an equal error rate (EER) of 0.67%.

Table I summarizes the results obtained when evaluating the performance of the considered protected biometric cryptosystems. Specifically, the required minimum level of privacy which has been employed in the iterative procedure described in Section III-E is $\bar{P} = 0.99$. We have investigated the behaviors achievable when using secret keys of length $k = \{40, 48, 56, 64\}$, and compared the capabilities of systems based on either static or dynamic bit allocation. In case of dynamic bit allocation, the rate of the employed error correcting turbo code has always been set to $\frac{n}{k} = 7$. When considering static bit allocation, the adopted rate has been chosen in the set $\frac{n}{k} = \{3, 5, 7\}$ as the one minimizing the FRR, that is, selecting the largest ratio $\frac{n}{k}$ admissible once the length of the secret key k and the number of available coefficients

TABLE I: Performance of the proposed zero-leakage cryptosystem, with either static or dynamic bit allocation for QIM embedding.

k	FRR(%)		
	Static allocation	Dynamic allocation	Dynamic allocation + dither
40	9.99	7.05	4.21
48	12.15	10.18	6.56
56	15.79	13.99	9.82
64	21.34	19.79	14.28

have been fixed. In more detail, in case of static bit allocation, the n bits are embedded into the n most stable coefficients, *i.e.* the n coefficients with highest embedding capacity. Only the FRR recognition rate is reported in Table I since, as already remarked, the proposed zero-leakage system is by construction set to an operating point with approximately null FAR, condition which has been confirmed in the experimental tests. From the reported results it is evident that, for all the considered key lengths, the dynamic bit allocation strategy ensures better performance in comparison with static bit allocation.

It has to be remarked that the static bit allocation here considered guarantees recognition performance practically undistinguishable from those obtained when applying the approach in [20] and [21]. However, only transformations with $\gamma = 0$ are there considered, whereas in the proposed approach, larger γ values can be employed even when considering a static bit allocation method, thus resulting in a far lower privacy leakage. In fact, as shown in Figure 6, the required condition of minimum privacy equal to $\bar{P} = 0.99$ cannot be satisfied with a γ parameter equal to zero, regardless of the number of bits embedded in a given coefficient. It is also worth pointing out that, in case a less strict requirement would have been taken into account for the minimum privacy level $\bar{P}$, the iterative procedure described in Section III-E would have led to the selection of lower γ values, with higher capacities therefore associated with each coefficient, and the consequent possibility of either embedding more bits increasing the security k of the system, or improving the achievable recognition performance in terms of FRR.

The experimental results reported in Table I also show that a significant improvement in terms of FRR can be achieved when the proposed dithering technique is exploited. Figure 9 shows the trend of the obtained FRR with respect to the number of attempts performed in the proposed dithering technique. However,we would like to point out that the proposed dithering method, besides improving the achievable FRR, also affects the security of the proposed cryptosystem with respect to FAR-based attacks. In fact, performing several recognition attempts for each presented biometrics may increase the probability of accepting a malicious user. Specifically, a loss of up to $log_2(T)$ bits against a FAR-based attack, being T the number of performed iterations, can be assumed when the dithering process is carried out. In the performed experimental tests, a FAR greater than 0, and specifically equal to 0.0051%, has been registered only when considering secret keys with $k = 40$, reasonably due to the limited training resources that have been exploited to properly estimate the PCA projection matrix and the coefficients' capacities. Nevertheless, the behavior of the achievable FRR with respect to the theoretic security against FAR-based attacks, when considering secret keys having length $k = \{40, 48, 56, 64\}$ bits, is depicted in Figure 10. This figure, as well as Figure 9, also illustrates that implementing a dithering approach allows tuning with improved degrees of freedom the recognition performance of the proposed cryptosystem. In fact, since standard implementations of error correcting codes, such as the turbo-codes we have employed, leave the possibility of choosing only a finite pre-defined set of key lengths to be encoded, the resulting number of feasible operational points may be significantly limited. Such limitation can be overcome by exploiting the proposed dithering technique, thus guaranteeing the capability of selecting the operating point providing the desired FRR, even if the security associated to a FAR-based attack may be affected by the process. It is worth remarking that the security against brute-force and non-randomness attacks remains unaffected by the proposed dithering approach.

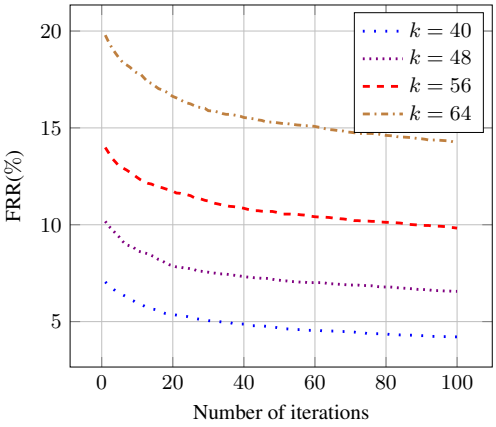


Fig. 9: FRR improvement with respect to the number of iterations performed in the proposed dithering approach.

We eventually further outline in Figure 11 the existing trade-off between the achievable recognition rates, in terms of FRR, and the possible privacy leakage P. Specifically, a comparison between the results which could be obtained when $\gamma = 0$ is adopted for each considered coefficient, and those achieved by our proposed system with adaptive γ selection is shown. Each plotted point represents the performance, in terms of FRR, obtained when considering keys having length $k = \{40, 48, 56, 64\}$ bits, by applying up to 100 dithering iterations. As it can be seen, a system using $\gamma = 0$ always performs better in terms of recognition rates, even if at the cost of a reduced privacy P, reported as the average evaluated over all the employed coefficients for each considered key length. Conversely, the proposed γ selection strategy always guarantee a minimum desired privacy level $P > 0.99$, at the cost of a slight reduction in FRR.

V. Conclusions

In this paper we have introduced a novel zero-leakage biometric cryptosystem. The proposed system guarantees no information leakage about the employed secret key from the stored helper data in case of non-randomness attacks, and it allows achieving a trade-off between privacy and recognition

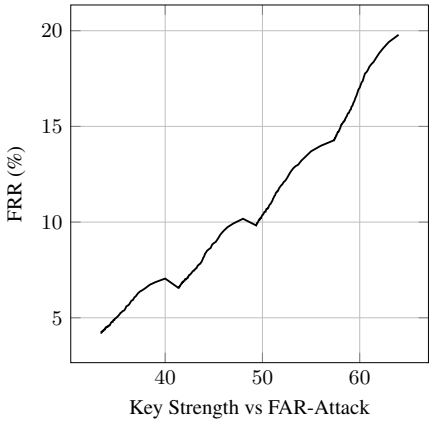


Fig. 10: FRR behavior with respect to the associated security, expressed in terms of robustness against FAR-based attacks, when adopting the proposed dithering technique.

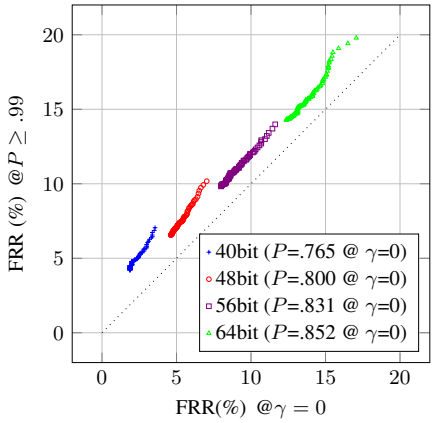


Fig. 11: comparison between systems using γ = 0, and systems adopting the proposed adaptive γ selection procedure for guaranteeing a privacy level $P > 0.99$.

rates. Specifically, in our approach we have introduced a class of transformation functions enforcing zero-leakage. In addition, we have proposed a strategy for adaptively embedding the bits of the secret key into the extracted template. Moreover, a system parameters optimization strategy with respect to security, recognition performance, and privacy has been proposed. As a proof-of-concept, and differently from state-of-the-art approaches, the proposed method has been tested on real fingerprint data. Experimental results show the effectiveness and the flexibility of the proposed system.

APPENDIX

In this section the biometric template minimum square estimator given in (23), when using a raised cosine distribution, is demonstrated. Let us indicate:

- x the biometric template transformed by means of (9) so that its probability density function is characterized by (10);
- y the error of the quantized version of x, that is $y = [x]_\Delta$; $m = 0, 1, \ldots, A-1$ the symbol to embed in the coefficient;
- the helper data coefficient $z = [x - m\frac{\Delta}{A}]_\Delta = [y - m\frac{\Delta}{A}]_\Delta$.

Using the chain rule, it is straightforward to show that:

$$p_{X|Z}(x|z) = p_{Y|Z}(y|z)\frac{p_{X|Y}(x|y)}{p_{Y|Z}(y|z)} = p_{Y|Z}(y|z)\frac{p_X(x)}{p_Y(y)}. \tag{20}$$

Ones z is set, y can be equal only to m equally likely values, depending on the embedded symbol:

$$p_{Y|Z}(y|z) = \frac{1}{A}\sum_{m=0}^{A-1}\delta_0\left(y - \left[m\frac{\Delta}{A} + z\right]_\Delta\right). \tag{21}$$

Replacing (21) into (20) and taking into account X and Y distributions, we have:

$$\begin{aligned} p_{X|Z}(x|z) &= \frac{\Delta}{A}\sum_{m=0}^{A-1}\delta_0\left([x]_\Delta - \left[m\frac{\Delta}{A} + z\right]_\Delta\right) rc_\gamma^\Delta(x) \\ &= \frac{\Delta}{A}\sum_{m=0}^{A-1}\left\{\delta_0\left(x - \left[m\frac{\Delta}{A} + z\right]_\Delta\right) + \right. \\ &\quad \left. + \delta_0\left(x - \left[m\frac{\Delta}{A} + z\right]_\Delta + \Delta\right)\right\} rc_\gamma^\Delta(x) \end{aligned} \tag{22}$$

The minimum mean square estimator of x, known z, is thus given as follows:

$$\begin{aligned} \hat{x}(z) &= \int_X x p_{X|Z}(x|z)dx = \\ &= \frac{\Delta}{A}\sum_{m=0}^{A-1}\left[m\frac{\Delta}{A} + z\right]_\Delta rc_\gamma^\Delta\left(\left[m\frac{\Delta}{A} + z\right]_\Delta\right) + \\ &+ \left(\left[m\frac{\Delta}{A} + z\right]_\Delta - \Delta\right) rc_\gamma^\Delta\left(\left[m\frac{\Delta}{A} + z\right]_\Delta - \Delta\right) \end{aligned} \tag{23}$$

ACKNOWLEDGMENT

We acknowledge the support of NVIDIA® with the donation of the Titan X™ GPU used for this research.

REFERENCES

[1] K. Nandakumar and A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 88–100, 2015.
[2] T. I. D. S. P. Tuyls, E. Verbitskiy and A. Akkermans, "Privacy-protected biometric templates: Acoustic ear identification," in *Proceedings of SPIE, Vol. 5404*, 2004, pp. 176–182.
[3] P. Campisi, *Security and Privacy in Biometrics*. Springer Publishing Company, Incorporated, 2013.
[4] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 3, pp. 1–25, 2011.
[5] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Processing Magazine: Special Issue on Biometric Security and Privacy*, vol. 32, no. 5, pp. 54–65, 2015.
[6] U. Uludag, S. Pankanti, and A. K. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of IEEE*, vol. 92, no. 6, pp. 948–960, 2004.

[7] K. Simoens, P. Tuyls, and B. Preneel, "Privacy weaknesses in biometric sketches," in *IEEE Symp. on Security and Privacy*, 2009, pp. 188–203.

[8] A. Stoianov, "Security issues of biometric encryption," in *IEEE Toronto International Conference on Science and Technology for Hunanity (TIC-STH)*, 2009, pp. 34–39.

[9] T. Ignatenko and F. M. J. Willems, "Biometric systems: Privacy and secrecy aspects," *IEEE Trans. on Information Forensics and Security*, vol. 4, no. 4, pp. 956–973, 2009.

[10] L. Lai, S.-W. Ho, and H. V. Poor, "Privacysecurity trade-offs in biometric security systemspart i: Single use case," *IEEE Trans. on Information Forensics and Security*, vol. 6, no. 1, pp. 122–139, 2015.

[11] T. Ignatenko and F. Willems, "Fundamental limits for privacy-preserving biometric identification systems that support authentication," *IEEE Trans. on Information Theory*, vol. 61, no. 10, pp. 5583–5594, 2015.

[12] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G.-J. Schrijen, A. M. Bazen, and R. N. J. Veldhuis, "Practical biometric authentication with template protection," in *AVBPA*, 2005, pp. 436–446.

[13] E. Maiorana, D. Blasi, and P. Campisi, "Biometric template protection using turbo codes and modulation constellations," in *IEEE WIFS*, 2012.

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

[15] X. Zhou, A. Kuijper, R. Veldhuis, and C. Busch, "Quantifying privacy and security of biometric fuzzy commitment," in *International Joint Conference on Biometrics (IJCB)*, 2011, pp. 1–8.

[16] X. Zhou and C. Busch, "Measuring privacy and security of iris fuzzy commitment," in *IEEE International Carnahan Conference on Security Technology (ICCST)*, 2012, pp. 168–173.

[17] E. Maiorana, P. Campisi, and A. Neri, "Iris template protection using a digital modulation paradigm," in *IEEE International Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, 2014, pp. 3759–3763.

[18] E. Maiorana, D. L. Rocca, and P. Campisi, "Cognitive biometric cryptosystems a case study on eeg," in *International Conference on Systems, Signals and Image Processing (IWSSIP)*, 2015, pp. 125–128.

[19] I. Buhan, J. Doumen, and P. Hartel, "Controlling leakage of biometric information using dithering," in *16th European Signal Processing Conference*, 2008, pp. 1–5.

[20] J. A. de Groot and J.-P. Linnartz, "Zero leakage quantization scheme for biometric verification," in *IEEE International Conference onAcoustics, Speech and Signal Processing (ICASSP)*, 2011, pp. 1920–1923.

[21] N. d. J.A. de Groot, B. Škorić and J.-P. Linnartz, "Quantization in zero leakage helper data schemes," *EURASIP Journal on Advances in Signal Processing*, vol. 54, pp. 1–13, 2016.

[22] U. Korte and R. Plaga, "Cryptographic protection of biometric templates: Chance, challenges and applications," in *BIOSIG*, 2007, pp. 33–46.

[23] J. Bringer, H. Chabanne, and Q. D. Do, "A fuzzy sketch with trapdoor," *IEEE Trans. on Information Theory*, vol. 52, no. 5, pp. 2266–2269, 2006.

[24] B. Chen and G. W. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," *IEEE Trans. on Information Theory*, vol. 47, no. 4, pp. 1423–1443, 2001.

[25] 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 Trans. on Information Forensics and Security*, vol. 5, no. 1, pp. 118–132, 2010.

[26] J. Linnartz and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates," in *AVBPA*, 2003, pp. 393–402.

[27] A. B. Sripad and D. Snyder, "A necessary and sufficient condition for quantization errors to be uniform and white," *IEEE Trans. on Acoustics, Speech, and Signal Processing*, vol. 25, no. 5, pp. 442–448, 1977.

[28] L. R. Y. Dodis, R. Ostrovsky and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Lecture Notes in Computer Science, Vol. 3027*, 2004, pp. 523–540.

[29] N. d. J. A. de Groot, B. Škorić and J.-P. Linnartz, "Diagnostic category leakage in helper data schemes for biometric authentication," in *IEEE SECRYPT*, 2013, pp. 1–6.

[30] J.-P. Linnartz, P. Tuyls, and B. Škorić, "A communication-theoretical view on secret extraction," in *Security with Noisy Data*. Springer, 2007, pp. 57–77.

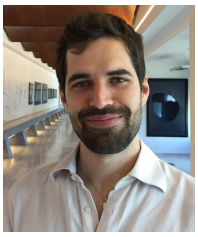
[31] C. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding: Turbo-codes," *IEEE Trans. on Communications*, vol. 44, no. 10, pp. 1261–1271, Oct. 1996.

[32] T. Ignatenko and F. M. J. Willems, "Privacy leakage in binary biometric systems: From Gaussian to binary data," in *Security and Privacy in Biometrics*, P. Campisi, Ed. Springer London, 2013, pp. 105–122.

[33] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching," *IEEE Trans. on Image Processing*, vol. 9, no. 5, pp. 846–859, 2000.

[34] J. e. a. Fierrez, "BiosecurID: a multimodal biometric database," *Pattern Analysis and Applications*, vol. 13, pp. 235–246, 2009.

[35] "Greenbit dactyscan84c," http://www.greenbit.com/livescans-3/ten-prints/dactyscan84c-with-standard-top-cover/, accessed: 2017-01-26.



Gabriel Emile Hine (S'16) was born in Braintree (UK) in May 1990. Since November 2015, he has been a PhD student in Applied Electronics at Roma Tre University. His main research areas are in Signal Processing, Information Security and Biometrics. He received his Bachelor's Degree in Electronic Engineering (cum laude) at Roma Tre University in February 2013 with the thesis "Biometric Systems Security: Attacks and Countermeasures". In October 2015, he got his Master's Degree in Information and Communication Technology Engineering (cum laude) at Roma Tre University with the thesis "Biometric Cryptosystems Development". During summer 2016, he worked at Telefonica(I+D), Barcelona, Spain, as a visiting researcher, as part of the European H2020 project ENCASE (ENhancing seCurity and privAcy in the Social wEb: a user-centered approach for the protection of minors).

Emanuele Maiorana (S'06-M'08) received the Ph.D. degree in biomedical, electromagnetism and telecommunication engineering with European Doctorate Label from Roma Tre University, Rome, Italy, in 2009. He was a visiting researcher at the Universidad Autonoma de Madrid, Madrid, Spain, in 2007 and 2008, at the Universidad de Vigo, Vigo, Spain, in 2010, at the University of Warwick, Coventry, UK, in 2012, at the Ecole Polytechnique de Nantes, Nantes, France, in 2013, at the University of Twente, Twente, The Netherlands, in 2013, and at the University of Salzburg, Salzburg, Austria, in 2015. He is currently a research engineer at the Section of Applied Electronics, Department of Engineering, of Roma Tre University, Rome, Italy. He is the recipient of the Lockheed Martin Best Paper Award for the Poster Track at the IEEE Biometric Symposium 2007, and of the Honeywell Student Best Paper Award at the IEEE Biometrics: Theory, Applications and Systems conference 2008. His research interests are in the area of digital signal and image processing with applications to biometrics, multimedia communications and security of telecommunication systems.

Patrizio Campisi (IEEE SM) received the Ph.D. degree in Electrical Engineering from Roma Tre University, Rome, Italy, where he is now Full Professor at the Section of Applied Electronics, Dept. of Engineering. His research interests are in the area of secure multimedia communications and biometrics. He has been the General Chair of the seventh IEEE Workshop on Information Forensics and Security, WIFS 2015, November 2015, Rome, Italy and of the 12th ACM Workshop on Multimedia and Security, September 2010 Rome, Italy. He is the editor of the book "Security and Privacy in Biometrics", SPRINGER, July 2013 and co-editor of the book "High Dynamic Range Video, Concepts, Technologies and Applications", Academic Press, Nov. 2016 and of "Blind Image Deconvolution: theory and applications", CRC press, May 2007. He is co-recipient of an IEEE ICIP06 and IEEE BTAS 2008 best student paper award and of an IEEE Biometric Symposium 2007 best paper award. He has been Associate editor of IEEE Signal Processing Letters and of IEEE Transactions on Information Forensics and Security. He has been Senior Associate editor of IEEE Signal Processing Letters. He is IEEE SPS Director Student Services and elected Chair of the IEEE Information Forensics and Security Technical committe. He is a member of the IEEE Technical Committee on Information Assurance & Intelligent Multimedia-Mobile Communications, System, Man, and Cybernetics Society and was a member of the IEEE Certified Biometric Program (CBP) Learning System Committee.