Unlinkable Zero-Leakage Biometric Cryptosystem: Theoretical Evaluation and Experimental Validation

Gabriel Emile Hine, *Member, IEEE*, Ridvan Salih Kuzu, Emanuele Maiorana, *Senior Member, IEEE*, and Patrizio Campisi, *Fellow, IEEE*

***Abstract*— Template protection is an issue of paramount importance for the design of secure and privacy-compliant biometric recognition systems. Template unlinkability, together with template irreversibility, is an essential requirement to properly guarantee template protection. In fact, it ensures that templates generated from the same trait, but used in different applications, cannot be linked to the same identity. This paper deals with the design of a system satisfying the unlinkability requirement. The robustness of the proposed solution is evaluated by exploiting methods stemming from the theory of stochastic optimization, as well as by using quantitative measures specifically proposed to characterize the unlinkability of biometric protection schemes. A case study using finger-vein biometrics is considered to test the proposed cryptosystem on non-ideal data. The proposed scheme guarantees 128 bits of security with acceptable false recognition rates in real-life conditions. Moreover, we provide guidelines to determine the parameters of the transformations to be applied to real biometric traits so as to ensure proper recognition, security, and unlinkability performance.**

***Index Terms*— Biometrics, template protection, privacy, vein patterns.**

I. Introduction

THE use of biometric traits in automatic recognition systems offers several advantages over traditional approaches relying on passwords or tokens since biometric characteristics cannot be lost or forgotten, and, in general, they allow a much easier and more natural human-machine interaction. Nonetheless, the usage and storage of biometric data also pose several threats [1], [2]. For instance, if a biometric identifier is compromised, an attacker could exploit the collected information to impersonate its owner, and fraudulently gain access to specific resources. Therefore, the need to revoke biometric credentials could arise, posing an issue given the limited number of available traits. Furthermore, biometric data, when used as universal identifiers, could be used to track the users' activities across different domains, thus posing privacy concerns. Biometric data can also reveal sensitive information about their owners, that might be exploited for discriminatory purposes [3]. Not surprisingly, biometric information is retained as strictly confidential by the EU General Data Protection Regulation (GDPR), which recommends its management with adequate levels of security. Therefore, the aforementioned concerns have to be carefully taken into account and properly addressed when designing a biometric recognition system. In more details, the templates generated from the raw biometric data should be protected as effectively as the traits themselves, since it is often possible to adequately reconstruct the original data from their representations [4]. However, even if a template is not reversible, it must be considered sensitive data.[1]

Unfortunately, standard cryptographic algorithms cannot be effectively used to protect a biometric template, since comparison in the encrypted domain is not feasible due to the noisy nature of biometric data [1]. Homomorphic encryption has been exploited to tackle the aforementioned disadvantage, designing pipelines where the recognition step is performed in the encrypted domain [5]. However, the related computational complexity is relatively high, and trusted servers are needed to manage the exchange of the involved data, making this solution impractical for many applications.

Several biometric template protection (BTP) schemes have been proposed to design a secure and privacy-compliant biometric system. BTP methods generally modify the available biometric representations to generate alternative templates not leaking information about the original data. According to the ISO/IEC 24745 standard [6], a proper BTP method should satisfy the following properties:

- *irreversibility*: given a protected template, it should not be possible to reconstruct its unprotected version;
- *renewability*: from a given biometric sample, it should be possible to issue multiple protected templates;
- *unlinkability*: given two protected templates, generated from the same biometric sample and stored in different datasets, it should not be possible to determine that they belong to the same subject;
- *performance*: the use of a BTP scheme should not significantly affect the system recognition performance.

BTP schemes are typically implemented by means of two distinct methodologies, namely *cancelable biometrics* [7]

Manuscript received 5 December 2022; revised 31 March 2023 and 11 May 2023; accepted 12 May 2023. Date of publication 24 May 2023; date of current version 15 June 2023. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Andrew Beng Jin Teoh. *(Corresponding author: Emanuele Maiorana.)*

Gabriel Emile Hine, Emanuele Maiorana, and Patrizio Campisi are with the Section of Applied Electronics, Department of Industrial, Electronics and Mechanical Engineering, Roma Tre University, 00146 Rome, Italy (e-mail: gabriel.hine@uniroma3.it; emanuele.maiorana@uniroma3.it; patrizio.campisi@uniroma3.it).

Ridvan Salih Kuzu is with the German Aerospace Center (DLR), 82234 Weßling, Germany (e-mail: ridvan.kuzu@dlr.de).

Digital Object Identifier 10.1109/TIFS.2023.3279617

[1] See reasoning in the Decision of the Hellenic Data Protection Authority N°31/2010.

and *biometric cryptosystems* [8]. Cancelable biometrics refers to methods applying either invertible or non-invertible transformations to the biometric data. While non-invertible tranformation-based approaches have been proposed for several of the most used biometric traits [9], [10], their irreversibility has been rarely evaluated through rigorous proofs, due to the intrinsic difficulties in proving the non-invertibility of a function against any possible kind of attack.

On the other hand, biometric cryptosystems [11] can be classified into *key-generation* and *key-binding* approaches. The first extracts cryptographic keys from the considered biometric data. The latter aims at securing a cryptographic key by means of biometric data and vice versa: the key and the biometric data are combined into a template that can be split into a *pseudonymous identifier* (PI) and *auxiliary data* (AD) [6]. The *key-generation* approaches commonly lack in renewability and unlinkability since, by definition, the key is generated by exploiting the biometric trait only. On the other hand, detailed evaluations have been performed on the information about the original secrets leaked from templates protected with key-binding approaches [12]. Fundamental trade-offs among recognition performance, irreversibility, and security have been, for instance, discussed in [13] and [14]. In this regard, it has been demonstrated that both *security*, measured as the mutual information between the employed secret key and the stored AD, and *irreversibility*, intended as the difficulty of retrieving the original biometric information from the AD, could be improved only at the cost of worsening the achievable recognition performance.

This paper stems from our previous work [15], where we have proposed a zero-leakage key binding approach based on the use of quantization index modulation (QIM), with the goal to embed a secret key within a biometric representation. The approach in [15] guarantees that the generated AD does not reveal any information regarding either the employed secret binary key or the associated PI, thus achieving perfect security. Nonetheless, as it will be detailed in the following, the scheme proposed in [15] is vulnerable to linkability attacks. In this paper we overcome this issue, by designing a novel approach that enforces the desired template unlinkability, thus obtaining a zero-leakage biometric cryptosystems satisfying all the properties required by the ISO/IEC 24745 standard.

The effectiveness of the proposed approach is evaluated by testing its robustness against different linkage attacks, considering both methods stemming from the theory of stochastic optimization, as well as quantitative measures specifically designed to characterize the unlinkability of biometric protection schemes. The influence of the parameters employed in the proposed approach on the security and unlinkability of the templates created from non-ideal biometric data is also investigated. Furthermore, in order to apply the proposed BTP scheme to real-life biometric data, finger vein patterns are considered as case study.

The paper is organized as follows. Section II briefly outlines the zero-leakage cryptosystem introduced in [15], here analyzed with respect to the unlinkability requirement, and then further developed. In Section III, the approach proposed to generate unlinkable templates is described. Its effectiveness against different attacks is tested in Section IV. Specifically, attacks aimed at linking templates generated from the same original biometrics, and protected using different keys, are taken into account, considering biometric data with ideal distributions. In Section V, the issues to be faced when dealing with non-ideal data are discussed, and guidelines to define the parameters employed in the proposed approach are provided. The experimental tests conducted to verify the effectiveness of the proposed method in practical scenarios are described in Section VI, while conclusions are given in Section VII.

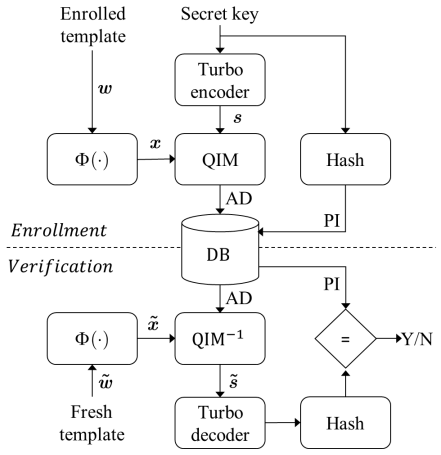

Fig. 1. Zero-leakage biometric cryptosystem [15].

II. A Zero-Leakage Cryptosystem

In this Section, the zero-leakage biometric cryptosystem presented in [15], and sketched in Figure 1, is briefly summarized. More in detail, in the enrolment stage, a fixed-length biometric representation $\boldsymbol{w} \in \mathbb{R}^L$ and a secret key with K bits are used to generate the couple (PI, AD), where the PI is a hashed version of the employed key, whereas a transformed version of $\boldsymbol{w}$ and an encoded version of the key are used to generate the AD using QIM.

Specifically, the K bits of the key are encoded into a string of N bits through an error correcting code (ECC), to handle the intra-class variability of the considered biometric data. The use of highly efficient ECC such as turbo codes, and the representation of the employed biometric templates with continuous variables, instead of binary ones as in the fuzzy commitment [16], is recommended for biometric cryptosystems in order to approach the Shannon limit during the decoding process, thus allowing to achieve the best possible recognition performance in terms of false rejection rate (FRR) [17]. The N encoded bits are divided into L symbols, each corresponding to a, potentially different, number B of bits. Each symbol is embedded into a coefficient w of the representation $\boldsymbol{w}$ as:

$$z = [\Phi(w) - s]_{2\pi} \tag{1}$$

which represents the AD, where

- $s \in \left\{\frac{2\pi m}{M} : m \in \mathbb{Z}_M\right\}$, with $M = 2^B$, is a symbol belonging to an alphabet with M elements and associated to the B bits to embed[2];

[2]In the actual implementation, M varies for each coefficient, but, for the sake of notation simplicity, we here represent M as coefficient-independent.

- $\Phi(\cdot)$ is a point-wise function defined as follows:

$$x = \Phi(w) = CDF_X^{-1}\left[CDF_W(w)\right], \tag{2}$$

where $CDF_W(w)$ and $CDF_X(x)$ are, respectively, the cumulative density functions of the original biometric coefficient W and of the target variable X.

As mentioned in [18], a zero-leakage biometric cryptosystem should guarantee that an auxiliary data Z leaks only a negligible amount of information about the associated secret key S and the biometric trait X. Information-theoretic analysis [14] has proved that the mutual information between the employed biometric representation and the stored AD cannot be null. In fact, the assumption that $I(X, Z) = 0$ implies that Z would not retain any information about the employed biometric trait X, with the consequence that the only achievable operating condition would be the one with FRR $= 100\%$ [14]. It is therefore possible to design cryptosystems with only close-to-zero leakage about the biometric data [19].

On the other hand, the zero-leakage property is achievable for the employed secret key, assuring a null mutual information between the secret key and the AD [20], [21], i.e., $I(S, Z) = 0$. Within the considered framework, this latter requirement can be obtained by choosing the function $\Phi(\cdot)$ is such a way that the characteristic function CF of the target variable X, i.e., the Fourier transform of its probability density function (PDF), satisfies [15]:

$$CF_X(l) = 0, \quad \forall l \in \mathbb{Z} - \{0\}. \tag{3}$$

A family of random variables X, fulfilling the requirement in Eq. (3), is the one whose PDF has a raised cosine shape [15], that is:

$$\mathrm{rc}_\gamma^{2\pi}(x) = \begin{cases} \dfrac{1}{2\pi}, & |x| \leq \pi(1-\gamma) \\ \dfrac{1}{4\pi}\left(1-\sin\dfrac{|x|-\pi}{2\gamma}\right), & \pi(1-\gamma) < |x| \leq \pi(1+\gamma) \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

with $\gamma \in [0, 1]$. As shown in Eq. (15), the choice of the parameter γ is responsible for both the irreversibility and the capacity of the resulting coefficient x. Specifically, in the considered framework, the irreversibility can be evaluated by measuring, for each coefficient of the employed biometric representation, the mean root square error between the actual value x and its best estimate $\hat{x}(z)$ obtained by exploiting the knowledge of the associated AD z, that is:

$$P = \frac{E_{X,Z}\{[x - \hat{x}(z)]^2\}}{E_X\{x^2\}} \in [0, 1). \tag{5}$$

The irreversibility P, evaluated according to Eq. (5) as a function of the parameter γ, parameterized *wrt* an increasing number of bits B embedded into x, is shown in Figure 2. Higher values of irreversibility, corresponding to a negligible leakage about the original biometric information, are achieved for increasing values of γ. As suggested in [15], in the proposed scheme the γ value used in the employed transformation is determined with the goal of minimizing the information leakage about the used biometric data, thus achieving close-to-zero leakage about X, by guaranteeing that $P \approx 1$.

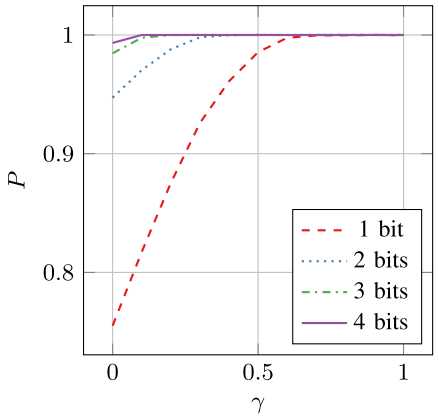

Fig. 2. Irreversibility measure P vs γ.

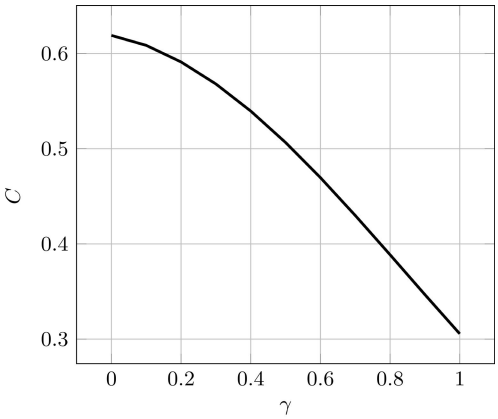

Fig. 3. Capacity C vs γ, adapted from [15].

On the other hand, in [15] it has also been shown that the capacity of each coefficient x, i.e., the upper bound of the number of bits B that can be embedded in the enrolment stage and reliably retrieved during verification using an ECC, decreases when increasing the value of γ. In Figure 3, the capacity C *vs* γ, for a synthetic biometric coefficient x characterized by a signal-to-noise (SNR) ratio equal to $4.7dB$, as in [22], is depicted. It is evident that the use of larger values of γ improves the irreversibility of the created templates and yet affects the capacity of the obtained representations. This behavior makes the coefficient capable of hosting a smaller number of bits, and results in a greater vulnerability to brute force attacks since the usable secret keys must be shorter. This confirms a trade-off between security and irreversibility [14].

As shown in the following sections, the parameter γ also influences the unlinkability of the proposed enhanced system to properly generate multiple protected templates from the same biometric representation.

III. Proposed Approach: Generation of Unlinkable Templates

In this Section, we show the limits of the system we have proposed in [15] (see Section II) in terms of unlinkability, and we propose a possible solution for their mitigation.

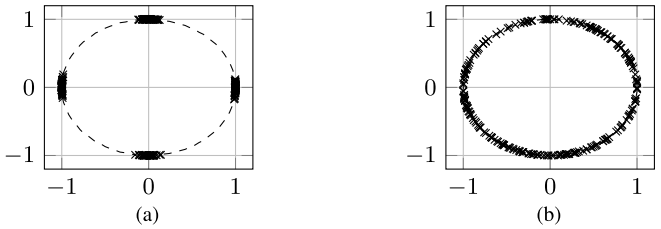

Fig. 4. Distributions of $[z_1 - z_2]_{2\pi}$ for linkability attacks targeting (a): mated AD; (b): non-mated AD.

Algorithm 1 Key Embedding Process

input : $\boldsymbol{w} \in \mathbb{R}^L$; $\boldsymbol{k} \in \{0,1\}^K$;
$\boldsymbol{A} \in \mathbb{R}^{L\times L} : \boldsymbol{A}^\intercal \boldsymbol{A} = \boldsymbol{I}$
output: $z \in [0, 2\pi)^L$
$\boldsymbol{c} \leftarrow \text{Encode}(\boldsymbol{k}, \frac{N}{K})$; // $\boldsymbol{c} \in \{0,1\}^N$
$\boldsymbol{s} \leftarrow \text{Map}(\boldsymbol{c}, M)$; // $\boldsymbol{s} \in \left\{\frac{2\pi m}{M} : m \in \mathbb{Z}_M\right\}^L$
$\boldsymbol{x} \leftarrow g\left[\boldsymbol{A} \cdot f(\boldsymbol{w})\right]$;
$\boldsymbol{z} \leftarrow [\boldsymbol{x} - \boldsymbol{s}]_{2\pi}$;

The method we have proposed in [15] appears not to be robust *wrt* the unlinkability of protected templates generated from the same biometric data. In fact, as shown in [23], given a biometric trait $\boldsymbol{x}$ and a pair of keys $\boldsymbol{k}_1$ and $\boldsymbol{k}_2$ encoded into $\boldsymbol{s}_1$ and $\boldsymbol{s}_2$, the corresponding AD are obtained as $\boldsymbol{z}_i = [\boldsymbol{x} - \boldsymbol{s}_i]_{2\pi}$, $i = 1, 2$. We observe that:

$$[\boldsymbol{z}_1 - \boldsymbol{z}_2]_{2\pi} = [\boldsymbol{x} - \boldsymbol{s}_1]_{2\pi} - [\boldsymbol{x} - \boldsymbol{s}_2]_{2\pi} = \\ = [\boldsymbol{s}_2 - \boldsymbol{s}_1]_{2\pi} \in \left\{\frac{2\pi m}{M} : m \in \mathbb{Z}_M\right\}^L, \quad (6)$$

meaning that the difference between two AD generated from the same biometric data $\boldsymbol{x}$ is bound to a discrete set of values. On the other hand, when the AD are created from different biometric representations $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$, $[\boldsymbol{z}_1 - \boldsymbol{z}_2]_{2\pi}$ is uniformly distributed in $[0, 2\pi)^L$. It is worth observing that even when the two biometric representations are not identical, but they differ because of the intra-class variability of the considered trait, $[\boldsymbol{z}_1 - \boldsymbol{z}_2]_{2\pi}$ would be still close to $[\boldsymbol{s}_2 - \boldsymbol{s}_1]_{2\pi}$, as shown in Figure 4. Therefore, a linkability attack would be able to relate the two identifiers, thus posing privacy concerns.

In order to overcome the limitations of the method in [15], we propose the following approach. With reference to Figure 5 and to the pseudo-code in Algorithm 1, the generic coefficient x_i of the template $\boldsymbol{x}$ is obtained as follows[3]:

$$u_i = f(w_i),$$
$$v_i = \sum_{j=1}^{L} A_{i,j} u_j,$$
$$x_i = g(v_i), \quad i = 1, \ldots, L. \quad (7)$$

[3]For the sake of simplicity, we will denote with the same symbols $f(\cdot)$ both scalar ($f(w) : \mathbb{R} \to \mathbb{R}$) and vector ($f : \mathbb{R}^L \to \mathbb{R}^L$) functions, depending on the argument. Hence, $f(\boldsymbol{w}) = (f(w_1), f(w_2), \ldots, f(w_L))^\intercal$. The same convention applies to $g(\cdot)$.

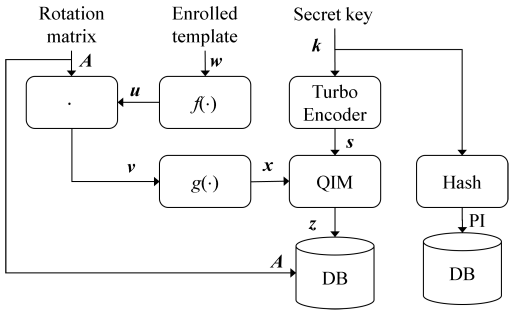

Fig. 5. Enrolment phase of the proposed unlinkable zero-leakage biometric cryptosystem.

In details, $f(\cdot)$ is a point-wise function:

$$f(\cdot) = \text{erf}^{-1}\left[CDF_W(\cdot)\right], \quad (8)$$

designed such that the coefficients $u_i = f(w_i)$ have a normal distribution $\mathcal{N}(0, 1)$. Assuming that the template coefficients w_i are statistically independent, as commonly assumed in the analysis of biometric cryptosystems [14], $\boldsymbol{u} = (u_1, u_2, \ldots, u_L)^\intercal$ will be normally distributed with an identity covariance matrix, namely $\boldsymbol{u} \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{I})$. Therefore, $\boldsymbol{u}$ is a realization of a rotational-symmetric distribution. The vector $\boldsymbol{v} = \boldsymbol{A}\boldsymbol{u}$, being $\boldsymbol{A}$ a record-specific $L \times L$ orthonormal matrix, is therefore a realization of the same process $\mathcal{N}(\boldsymbol{0}, \boldsymbol{I})$. Roughly speaking, given a properly designed $\mathbf{A}$ matrix, it is not possible to distinguish two independent realizations $(\boldsymbol{u}, \boldsymbol{u}^\star) \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{I}) \times \mathcal{N}(\boldsymbol{0}, \boldsymbol{I})$ from the couple $(\boldsymbol{u}, \boldsymbol{A}\boldsymbol{u})$. This is a key factor for the unlinkability of AD instances.

The template $\boldsymbol{x}$, with coefficients distributed as in Eq. (4), is finally obtained by applying a proper point-wise transformation $g(\cdot)$:

$$g(\cdot) = CDF_X^{-1}\left[\text{erf}(\cdot)\right] \quad (9)$$

to $\boldsymbol{v}$. Then, the couple (PI, AD) is obtained as summarized in Section II, with the AD given by $(\boldsymbol{z}, \boldsymbol{A})$.

It can be noted that, when $\boldsymbol{A} = \boldsymbol{I}$, the proposed scheme is equivalent to the one in [15]:

$$CDF_X^{-1}\left[\text{erf}\left[\text{erf}^{-1}\left[CDF_W(\boldsymbol{w})\right]\right]\right] = CDF_X^{-1}\left[CDF_W(\boldsymbol{w})\right]. \quad (10)$$

This suggests that not all orthonormal matrices $\boldsymbol{A} \in \mathbb{R}^{L\times L}$ are eligible for the proposed system. This aspect will be further explained in Section V.

In summary, the key embedding process can be expressed by the pseudo-code given in Algorithm 1. The inverse procedure, i.e., the key retrieval, is summarized by the pseudo-code given in Algorithm 2. Further implementation details are provided in Section VI-D.

It is worth mentioning that a similar approach, yet relying on permutation matrices, has been proposed in [24] to improve the unlinkability of the fuzzy commitment BTP scheme [16]. A permutation matrix $\boldsymbol{\Pi} \in \{0,1\}^L$ is a special kind of orthonormal matrix, with all zeros but only a 1 for each row and column. However, the use of a permutation matrix would be ineffective to obtain the desired unlinkability property for

Algorithm 2 Key Retrieval Process

input : $\tilde{\boldsymbol{w}} \in \mathbb{R}^L$; $\boldsymbol{z} \in [0, 2\pi)^L$;
$\boldsymbol{A} \in \mathbb{R}^{L\times L} : \boldsymbol{A}^\intercal \boldsymbol{A} = \boldsymbol{I}$
output: $\hat{\boldsymbol{k}} \in \{0,1\}^K$
$\tilde{\boldsymbol{x}} \leftarrow g\left[\boldsymbol{A} \cdot f(\tilde{\boldsymbol{w}})\right]$;
$\tilde{\boldsymbol{s}} \leftarrow \left[\tilde{\boldsymbol{x}} - \boldsymbol{z}\right]_{2\pi}$; // $\tilde{\boldsymbol{s}} \in [0, 2\pi)^L$
$\hat{\boldsymbol{c}} \leftarrow$ LogLikelihoodDemod($\tilde{\boldsymbol{s}}$, M); // $\hat{\boldsymbol{c}} \in \mathbb{R}^N$
$\hat{\boldsymbol{k}} \leftarrow$ Decode($\hat{\boldsymbol{c}}$, $\frac{N}{K}$);

the considered zero-leakage biometric cryptosystem. In fact, if a permutation matrix $\boldsymbol{\Pi}$ is used instead of a generic orthonormal matrix $\boldsymbol{A}$, we obtain that $g(\boldsymbol{\Pi u}) = \boldsymbol{\Pi} g(\boldsymbol{u})$. Hence, given a pair of AD $\boldsymbol{z}_1$ and $\boldsymbol{z}_2$, derived from the same biometric trait $\boldsymbol{w}$, we have:

$$\boldsymbol{z}_i = \left[g\left(\boldsymbol{\Pi}_i \boldsymbol{u}\right) - \boldsymbol{s}_i\right]_{2\pi} = \left[\boldsymbol{\Pi}_i g(\boldsymbol{u}) - \boldsymbol{s}_i\right]_{2\pi}, \quad i = 1, 2, \tag{11}$$

and

$$\boldsymbol{\Pi}_i^\intercal \boldsymbol{z}_i = \left[g(\boldsymbol{u}) - \boldsymbol{\Pi}_i^\intercal \boldsymbol{s}_i\right]_{2\pi}, \tag{12}$$

from which

$$\left[\boldsymbol{\Pi}_1^\intercal \boldsymbol{z}_1 - \boldsymbol{\Pi}_2^\intercal \boldsymbol{z}_2\right]_{2\pi} = \left[\boldsymbol{\Pi}_2^\intercal \boldsymbol{s}_2 - \boldsymbol{\Pi}_1^\intercal \boldsymbol{s}_1\right]_{2\pi} = \left[\boldsymbol{s}_2' - \boldsymbol{s}_1'\right]_{2\pi} \tag{13}$$

where the last step exploits the fact that the permutation of a string comprising a set of discrete symbols produces another string with coefficients belonging to the same alphabet. Therefore, this approach leads to the same scenario in Eq. (6) and Fig. 4(a), thus failing to provide unlinkability.

IV. Unlinkability Analysis

As it has been shown in [14], no helper data scheme can guarantee, from an information-theoretic perspective, a null mutual information between the original biometric data and the stored AD, and consequently a perfect unlinkability. In fact, a certain amount of template information should be retained in the AD to absorb the intra-class variability of the biometric trait and guarantee reliable recognition performance. Nevertheless, the linkability attack can be made computationally unfeasible. In this regard, the unlinkability property of the proposed approach is here investigated.

Specifically, we analyze the system robustness against two different attacks. The attack described in Section IV-A relies on the assumption that the space discretization carried out by the QIM module should match in case of mated biometric traits. We show that the verification of such hypothesis reduces to a Boolean Satisfiability (SAT) problem, hence it can be only solved with brute force. The attack described in Section IV-B attempts to link distinct AD by matching the best estimates of the biometric templates the attacker can achieve from the AD themselves. We show that the system can be set in a way that the mated estimates are indistinguishable from non-mated ones, thus making the attack ineffective.

A. Space Discretization Attack

The first attack we consider is an extension of the one proposed in [23], described by Eq. (6) and Figure 4. The direct application of such attack is not effective against the proposed system since each coefficient of $\boldsymbol{z}$ is not dependent on a single element of $\boldsymbol{w}$, as in [15], being instead obtained as a non-linear function of the entire original template. The domain of $\boldsymbol{z}$ is still quantized as a function of $\boldsymbol{u}$, but in a convoluted manner.

We try to retrieve $\boldsymbol{u}$ from $\boldsymbol{z} = [g(\boldsymbol{Au}) - \boldsymbol{s}]_{2\pi}$ as follows:

$$[\boldsymbol{z} + \boldsymbol{s}]_{2\pi} = [g(\boldsymbol{Au})]_{2\pi}. \tag{14}$$

Given that the co-domain of $g(\cdot)$ is limited to $[-2\pi, +2\pi)$, we can write:

$$[g(\boldsymbol{Au})]_{2\pi} = g(\boldsymbol{Au}) - 2\pi\boldsymbol{\xi} \tag{15}$$

where $\boldsymbol{\xi} \in \{0,1\}^L$ represents the information lost by the modulo operation. We can now express $\boldsymbol{u}$ as:

$$\boldsymbol{u} = \boldsymbol{A}^\intercal g^{-1}([\boldsymbol{z} + \boldsymbol{s}]_{2\pi} - 2\pi\boldsymbol{\xi}). \tag{16}$$

Considering now two AD sets $\{\boldsymbol{z}_1, \boldsymbol{A}_1\}$ and $\{\boldsymbol{z}_2, \boldsymbol{A}_2\}$, generated respectively by the inputs $\{\boldsymbol{w}_1, \boldsymbol{k}_1\}$ and $\{\boldsymbol{w}_2, \boldsymbol{k}_2\}$, and assuming the same biometric trait $\boldsymbol{w}_1 = \boldsymbol{w}_2 = \boldsymbol{w}$, we have:

$$\boldsymbol{u_1} = \boldsymbol{u_2}$$
$$\boldsymbol{A}_1^\intercal g^{-1}([\boldsymbol{z}_1 + \boldsymbol{s}_1]_{2\pi} - 2\pi\boldsymbol{\xi}_1) = \boldsymbol{A}_2^\intercal g^{-1}([\boldsymbol{z}_2 + \boldsymbol{s}_2]_{2\pi} - 2\pi\boldsymbol{\xi}_2),$$

from which:

$$g\left\{\boldsymbol{A}_2\boldsymbol{A}_1^\intercal g^{-1}\left([\boldsymbol{z}_1 + \boldsymbol{s}_1]_{2\pi} - 2\pi\boldsymbol{\xi}_1\right)\right\} = [\boldsymbol{z}_2 + \boldsymbol{s}_2]_{2\pi} - 2\pi\boldsymbol{\xi}_2$$
$$\left[g\left\{\boldsymbol{A}_2\boldsymbol{A}_1^\intercal g^{-1}\left([\boldsymbol{z}_1 + \boldsymbol{s}_1]_{2\pi} - 2\pi\boldsymbol{\xi}_1\right)\right\}\right]_{2\pi} = [\boldsymbol{z}_2 + \boldsymbol{s}_2]_{2\pi}$$
$$\left[g\left\{\boldsymbol{A}_2\boldsymbol{A}_1^\intercal g^{-1}([\boldsymbol{z}_1 + \boldsymbol{s}_1]_{2\pi} - 2\pi\boldsymbol{\xi}_1)\right\} - \boldsymbol{z}_2\right]_{2\pi} = [\boldsymbol{s}_2]_{2\pi} = \boldsymbol{s}_2,$$

thus obtaining:

$$\left[g\left\{\boldsymbol{A}_2\boldsymbol{A}_1^\intercal g^{-1}([\boldsymbol{z}_1 + \boldsymbol{s}_1]_{2\pi} - 2\pi\boldsymbol{\xi}_1)\right\} - \boldsymbol{z}_2\right]_{\frac{2\pi}{M}} = 0. \tag{17}$$

Eq. (17) represents a system of non-linear equations whose unknowns are the coefficients of $\boldsymbol{s}_1$ and $\boldsymbol{\xi}_1$, and whose solution would allow demonstrating that $\boldsymbol{z}_1$ and $\boldsymbol{z}_2$ are linked to the same identity.

We claim that there is no algorithm that can solve this problem in polynomial time. Let's redefine the problem as a minimization problem. We rely on a stochastic optimization algorithm, e.g., a genetic algorithm (GA), whose objective is to find:

$$\min_{(\boldsymbol{s},\boldsymbol{\xi})} t(\boldsymbol{s}, \boldsymbol{\xi}), \tag{18}$$

with the fitness function $t(\boldsymbol{s}, \boldsymbol{\xi})$ defined as:

$$t(\boldsymbol{s}, \boldsymbol{\xi}) = \min\left(t'(\boldsymbol{s}, \boldsymbol{\xi}),\ \frac{2\pi}{M} - t'(\boldsymbol{s}, \boldsymbol{\xi})\right), \text{ where}$$
$$t'(\boldsymbol{s}, \boldsymbol{\xi}) = \left[g\left(\boldsymbol{A}_2\boldsymbol{A}_1^\intercal g^{-1}([\boldsymbol{z}_1 + \boldsymbol{s}]_{2\pi} - 2\pi\boldsymbol{\xi})\right) - \boldsymbol{z}_2\right]_{\frac{2\pi}{M}}. \tag{19}$$

The mixture of modulo, rotation/reflection, and non-linear operators makes the system of equations strongly non-smooth

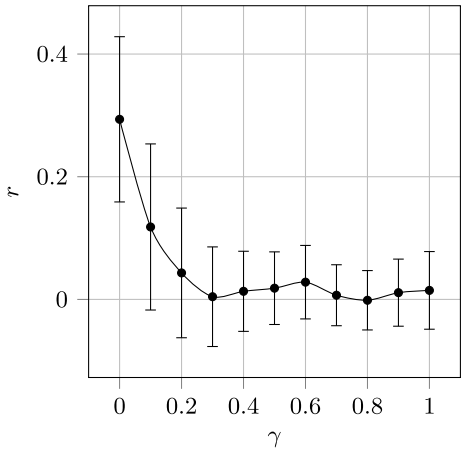

Fig. 6. Average fitness-distance correlation r vs γ.

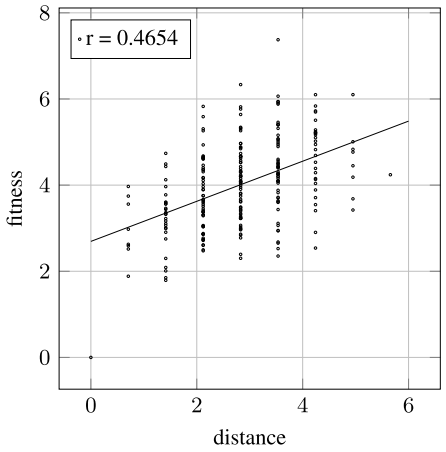

Fig. 7. Fitness t vs distance d @ $\gamma = 0$.

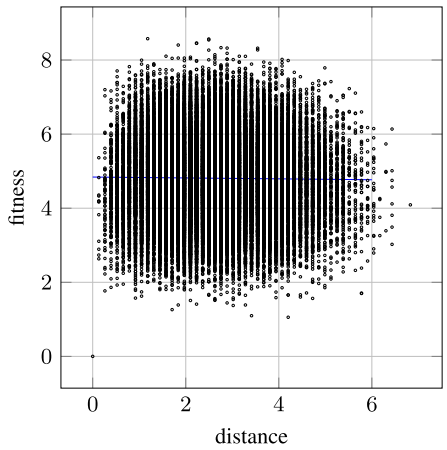

Fig. 8. Fitness t vs distance d @ $\gamma = 1$.

and therefore hard to solve by iterative algorithms. The difficulty of finding the minimum in Eq. (18) can be assessed using the so-called *fitness-distance correlation* [25], a simple method employed to evaluate the complexity of a genetic algorithm. In more detail, assuming the solution of the optimization problem in Eq. (18) is known, the distance d between such global optimum and values computed for the fitness function t can be evaluated. Given a set of T values $\mathcal{T} = \{t_i : i = 1, 2, \ldots, T\}$ computed during an iterative process, and the corresponding set of distances $\mathcal{D} = \{d_i : i = 1, 2, \ldots T\}$, a fitness-distance correlation can be obtained as:

$$r = \frac{1}{T}\frac{1}{\sigma_t \sigma_d}\sum_{i}^{T}(t_i - \overline{t})(d_i - \overline{d}), \tag{20}$$

where $\overline{t}$, $\overline{d}$, σ_t, and σ_d are respectively the means and standard deviations of the fitness function t and the distance to the optimum d. Such correlation reaches the value $r = 1$ in case the global optimum is found during the optimization process [25]. Since

$$g(\boldsymbol{A}\,\boldsymbol{u}) = [\boldsymbol{z} + \boldsymbol{s}]_{2\pi} - 2\pi\boldsymbol{\xi}, \tag{21}$$

the following expression can be used for the distance d:

$$d(\boldsymbol{s}^{\star}, \boldsymbol{\xi}^{\star}) = ||g(\boldsymbol{A}\boldsymbol{u}) - \left[\boldsymbol{z} + \boldsymbol{s}^{\star}\right]_{2\pi} - 2\pi\boldsymbol{\xi}^{\star}||, \tag{22}$$

being $||\cdot||$ the norm operator. Figure 6 shows an estimation of the average fitness-distance correlation r, obtained with a Monte-Carlo simulation for different γ values, with $B = 1$, $L = 24$,[4] and orthonormal matrices randomly generated as described in [26]. It is evident that r rapidly decreases for increasing γ, and approximately reaches $r = 0$ when $\gamma \geq 0.3$, suggesting that querying the fitness function in Eq. (18) would not give any useful feedback to find the solution of Eq. (17).

To get more insights into the complexity of the optimization problem, we can inspect the scatter plots of the fitness as a function of the considered distance. Examples of such plots are reported in Figures 7 and 8, for systems using $\gamma = 0$ and $\gamma = 1$, respectively. For illustrative purposes, these figures are referred to a simple scenario with a simulated biometric template with $L = 8$ coefficients and $B = 1$ bit embedded into each element of $\boldsymbol{x}$. For $\gamma = 0$, the significant correlation between distance and fitness suggests that a hill-climbing-based algorithm can solve the optimization problem. If $\gamma = 1$, there is instead no correlation between the two values.

The analysis based on the fitness-distance correlation suggests that solving the problem in Eq. (18) is unfeasible for high values of γ. Under such conditions, the solution of Eq. (17) can be only guessed. Formally, the existence of such a solution is a Boolean Satisfiability (SAT) problem, which is an NP-complete problem. Guessing the optimum pair $(\boldsymbol{s}, \boldsymbol{\xi})$ would have a computational cost that is exponentially proportional to the entropy of the two strings:

$$H(\boldsymbol{S}, \boldsymbol{\Xi}|AD) = H(\boldsymbol{S}) + H(\boldsymbol{\Xi}|\boldsymbol{S}, AD). \tag{23}$$

The entropy of $\boldsymbol{S}$ is the key-length K, while the equivocation of $\boldsymbol{\Xi}$ given $\boldsymbol{S}$ and AD is given by the uncertainty of $g(\boldsymbol{Au})$ given $[g(\boldsymbol{Au})]_{2\pi} = [\boldsymbol{z} + \boldsymbol{s}]_{2\pi}$, hence, $H(\boldsymbol{\Xi}|\boldsymbol{S}, AD) = H(\boldsymbol{X}|\boldsymbol{X}_{2\pi})$.

The equivocation of each coefficient X is given by:

$$H(X|X_{2\pi} = x) = -\mathcal{P}(x)\log_2\mathcal{P}(x) - (1 - \mathcal{P}(x))\log_2(1 - \mathcal{P}(x)), \tag{24}$$

[4]Simulations with larger templates were computationally unfeasible with the available computing node: 2 Xeon 16-Core 2.3Ghz processors, 8 × 16 GB RAM, 4 NVIDIA Tesla V100 32GB.

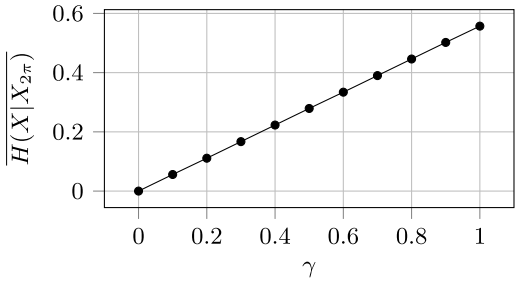

Fig. 9. Average information lost by the modulo-2π operation.

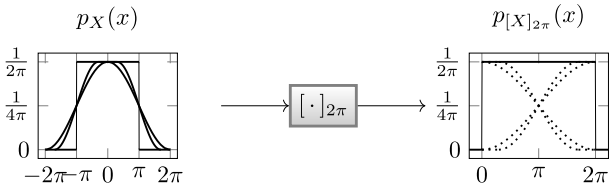

Fig. 10. Modulo-2π applied to the raised cosine distributions.

with $\mathcal{P}(x) = 2\pi\,\mathrm{rc}_{\gamma}^{2\pi}(x)$. On average, the equivocation expected value is then:

$$\begin{aligned}\overline{H(X|X_{2\pi})} &= E_x\{H(X|X_{2\pi}=x)\}\\ &= \int_0^{2\pi} H(X|X_{2\pi}=x)p_{X_{2\pi}}(x)dx\\ &= \int_0^{2\pi} H(X|X_{2\pi}=x)\frac{1}{2\pi}dx. \end{aligned} \tag{25}$$

Interestingly, by solving the integral numerically, it turns out that the average equivocation grows roughly linearly with γ, as shown in Fig. 9. It is worth mentioning that such equivocation is zero with $\gamma = 0$. In fact, with reference to Figure 10, when $\gamma = 0$ no information is lost after the modulo operator, since $x \in [-\pi, \pi)$, and, in this case, the modulo operator is a bijective function. Summarizing, solving the linkability problem in Eq. (17) is equivalent to randomly guessing approximately $K + L \times \overline{H(X|X_{2\pi})}$ bits.

B. Template Estimation-Based Attack

Other linkability attacks can be attempted by performing the best estimates of the biometric representations that generate different AD. From Eq. (16), given the AD, namely $\{z, \boldsymbol{A}\}$, the original template $\boldsymbol{u}$ can be estimated as:

$$\hat{\boldsymbol{u}} = E\left[\boldsymbol{A}^{\intercal} g^{-1}\left([z + \boldsymbol{s}]_{2\pi} - 2\pi\boldsymbol{\xi}\right)\right], \tag{26}$$

being $E[\cdot]$ the expected value over all $(\boldsymbol{s}, \boldsymbol{\xi})$ couples. Therefore, given two sets $AD_1 = \{z_1, \boldsymbol{A}_1\}$ and $AD_2 = \{z_2, \boldsymbol{A}_2\}$, an attacker can first estimate the corresponding representations $\hat{\boldsymbol{u}}_1$ and $\hat{\boldsymbol{u}}_2$ and then compute their similarity through a *linkage function* $l = \mathcal{L}(\hat{\boldsymbol{u}}_1, \hat{\boldsymbol{u}}_2)$. The effectiveness of such linkage function can be assessed using metrics specifically designed to evaluate template unlinkability, such as those proposed in [27] or [28]. In more detail, we here consider the linkability measure $D_{\leftrightarrow}^{sys}$ defined in [27] as:

$$D_{\leftrightarrow}^{sys} = \int p(l|\mathcal{H}_m) D_{\leftrightarrow}(l)\mathrm{d}l \tag{27}$$

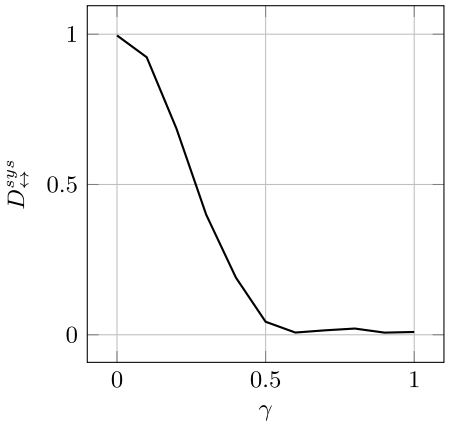

Fig. 11. Linkability measure $D_{\leftrightarrow}^{sys}$ vs γ.

where

$$D_{\leftrightarrow}(l) = \begin{cases} 0 & \text{, if } \mathcal{R}(l)\cdot\omega \le 1,\\ 2\dfrac{\mathcal{R}(l)\cdot\omega}{1+\mathcal{R}(l)\cdot\omega} - 1 & \text{, if } \mathcal{R}(l)\cdot\omega > 1 \end{cases} \tag{28}$$

is the score-specific linkability, and

$$\mathcal{R}(l) = \frac{p(l|\mathcal{H}_m)}{p(l|\mathcal{H}_{nm})} \tag{29}$$

is the likelihood ratio between *mated* ($\mathcal{H}_m$) and *non-mated* ($\mathcal{H}_{nm}$) distributions, and $\omega = p(\mathcal{H}_m)/p(\mathcal{H}_{nm})$ denotes the ratio between the unknown prior probabilities of the mated and non-mated score distributions. The measure $D_{\leftrightarrow}^{sys}$ is bound within [0, 1], with $D_{\leftrightarrow}^{sys} = 1$ obtained for fully distinguishable mated and non-mated distributions, therefore corresponding to fully linkable AD. On the other hand, $D_{\leftrightarrow}^{sys} = 0$ is achieved for fully overlapped distributions, meaning that two AD derived from the same biometric trait cannot be linked using the considered linkage function.

As shown in [15] and mentioned in Section II, high values of γ in Eq. (4) make the estimate $\hat{\boldsymbol{u}}$, in Eq. (26), arbitrarily unreliable, and therefore the described linkability attack ineffective. The behavior of the linkability measure $D_{\leftrightarrow}^{sys}$ as a function of γ, obtained using the Euclidean distance as linkage function, is shown in Figure 11. As it can be seen, $D_{\leftrightarrow}^{sys}$ is roughly equal to 1 for $\gamma = 0$, i.e., two AD generated from the same trait are fully linkable. As γ grows, two AD related to the same identity get as unlinkable as templates obtained from distinct users. Examples of mated and non-mated distributions, together with the corresponding linkability measures, are shown in Figures 12 and 13, for $\gamma = 0$ and $\gamma = 1$ respectively.

V. Dealing With Non-Ideal Data

The system described in Section III and the analysis of its effectiveness reported in Section IV refer to the ideal assumption of biometric templates with *i.i.d.* coefficients. The *i.i.d.* hypothesis is commonly assumed for security evaluation assessment of most biometric cryptosystems [19], [21], as well as in the analysis of the requirements ensuring the zero-leakage conditions [14], [20]. However, biometric representations with *i.i.d.* coefficients are hardly encountered in real life. In more

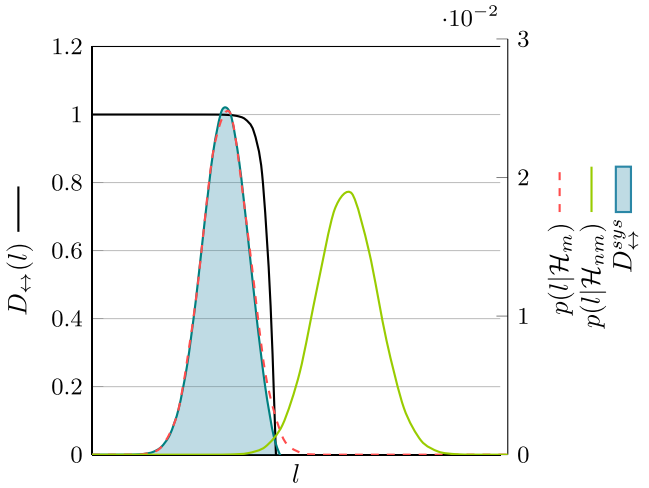

Fig. 12. Linkability measures for $\gamma = 0$.

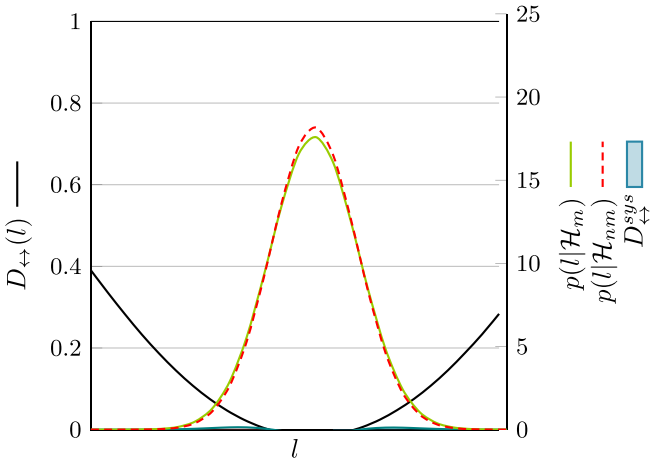

Fig. 13. Linkability measures for $\gamma = 1$.

detail, templates usually employed in biometric recognition systems include strongly correlated elements. Moreover, coefficients' distributions can be significantly different, with some features characterized by much greater discriminative capabilities than others. Therefore, the design of a protection mechanism applicable to real biometric data needs to take into account many issues not addressed when considering ideal conditions in order to avoid significant security losses, which become increasingly severe the more the biometric data deviate from ideal assumptions [29].

In order to approximate the *i.i.d.* condition, whitening methods, such as principal component analysis (PCA) or independent component analysis (ICA), could be employed. These methods have the side effect of generating representations with coefficients having uneven SNRs, i.e., most of the meaningful information is concentrated in a few components [15]. Dealing with data having the aforementioned characteristics has a major impact on the selection of the orthonormal matrices employed in the proposed cryptosystem.

In order to gain a deeper understanding, we consider a toy model where the template $\boldsymbol{u}$ is made of two coefficients, i.e., u_1 and u_2, with Gaussian distributions and unitary covariance matrix. Let us assume that both coefficients are affected by additive Gaussian noise, having respectively variance σ_1^2 and

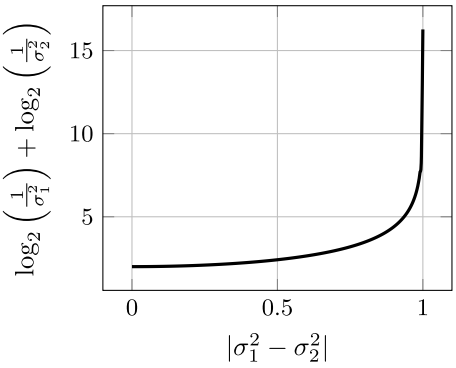

Fig. 14. Overall capacity of a two-coefficient template vs SNR balance.

σ_2^2, with $\sigma_1^2 + \sigma_2^2 = 1$. The Shannon's capacity of the system is given by:

$$C = \log_2\left(\frac{1}{\sigma_1^2}\right) + \log_2\left(\frac{1}{\sigma_2^2}\right). \tag{30}$$

Such capacity tends to infinity as $|\sigma_1^2 - \sigma_2^2| \to 1$, that is, when one of the two coefficients is noiseless. On the other hand, the overall capacity is minimum when the noise is evenly distributed between the two coefficients, as depicted in Figure 14. Therefore, in order to guarantee high capacity, it is desirable to describe the coefficients in a vector basis that concentrates the noise in few coefficients, leaving the remaining ones noiseless, which is what the PCA tries to achieve. Unfortunately, the application of a random orthonormal matrix to a given representation tends to distribute the noise more evenly across the coefficients. In fact, considering a generic transformation:

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \leftarrow \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}, \tag{31}$$

we have $\sigma_{V_1}^2 - \sigma_{V_2}^2 \leftarrow (\sigma_{U_1}^2 - \sigma_{U_2}^2)(2\cos^2\phi - 1)$, where $|2\cos^2\phi - 1| < 1$, meaning that the operating point on Figure 14 moves left and the overall capacity decreases. The capacity loss becomes more prominent the more the original coefficients have uneven SNRs. In the extreme case, even a noiseless element would be mapped into a noisy term, leading to an infinite capacity loss. On the other hand, no capacity is lost when combining features having the same SNR.

Given these observations, specific care needs to be taken when dealing with real biometric traits, in order to generate templates with features having high SNR, and thus preserve the original capacity. Specifically, each template coefficient should be combined only with features having similar SNRs. This goal can be achieved by rearranging the vector $\boldsymbol{u}$ so as to be sorted with respect to the SNR, and designing the matrix $\boldsymbol{A}$ as a banded matrix. The matrix $\boldsymbol{A}$ bandwidth $Q \in \{1, 2, \ldots, L\}$ controls the capacity-unlinkability trade-off. Note that in the extreme case of $Q = 1$, the orthonormal matrix is diagonal and the proposed approach collapses to the original one described in [15], providing no unlinkability at all. Clearly, Q controls the trade-off existing between capacity and unlinkability. This approach can be implemented by initializing $\boldsymbol{A}$ as a diagonal matrix $\boldsymbol{R}$ whose elements

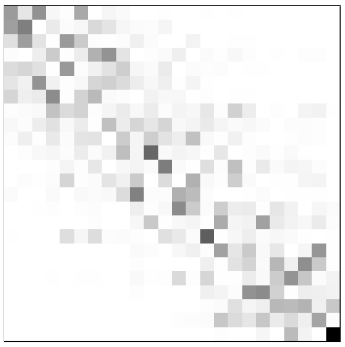

Fig. 15. Example of a matrix $\boldsymbol{A}$ created as in Eq. (33) with $L = 24$ and $Q = 6$ (absolute values; white = 0, black = 1).

are randomly chosen as $\{-1, +1\}$, i.e., a random reflection matrix. Then we iteratively rotate randomly chosen coefficients (i, j), such that $|i - j| \leq Q$, by a random angle $0 \leq \theta_{ij} \leq \pi/20$. This can be formalized by the use of Givens rotation matrices [30]. Specifically, from a set of $\boldsymbol{G}_{ij}$ matrix operators, each performing a rotation on the (i, j) plane:

$$\boldsymbol{G}_{ij} = \begin{array}{c} \\ i \\ \\ j \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccccccc} & & i & & j & & & & \end{array} \\ \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & \cdots & 0 \\ \vdots & 1 & \vdots & & \vdots & & & \vdots \\ 0 & \cdots & \boxed{c} & \cdots & \boxed{-s} & \cdots & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & & \vdots \\ 0 & \cdots & \boxed{s} & \cdots & \boxed{c} & \cdots & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \ddots & & \vdots \\ \vdots & & \vdots & & \vdots & & 1 & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & & 1 \end{pmatrix} \end{array}, \tag{32}$$

with $\boldsymbol{G}_{ij}(k, k) = 1$ for $k \neq i, j$, $\boldsymbol{G}_{ij}(i, i) = \boldsymbol{G}_{ij}(j, j) = c = \cos\theta_{ij}$, and $\boldsymbol{G}_{ij}(j, i) = -\boldsymbol{G}_{ij}(i, j) = s = \sin\theta_{ij}$, with θ_{ij} randomly sampled in $(0, \pi/20)$, we design the orthonormal matrix $\boldsymbol{A}$ as:

$$\boldsymbol{A} = \left[\prod_{(i,j)\in\mathcal{S}} \boldsymbol{G}_{ij} \right] \boldsymbol{R} \tag{33}$$

with $\mathcal{S} \in \{(i, j) : |i - j| < Q)\}$. A visual example of a matrix $\boldsymbol{A}$ obtained as in Eq. (33) is shown in Figure 15. It can be noticed that such matrix is not banded in a strict sense, because the many consecutive rotations may produce combinations of coefficients for which $|i - j| \geq Q$. Nevertheless, since the weights of the combinations decrease with $|i-j|$, the resulting matrix can be assumed to be banded in a fuzzy meaning.

The effects of the Q parameter on the properties of the resulting templates can be illustrated through an example relying on a synthetic template $\boldsymbol{w}$ made of $L = 24$ coefficients, whose capacities are not evenly distributed as shown in Figure 16, mimicking the behavior of biometric data whitened using, for example, a PCA or ICA method. The overall capacity of the template $\boldsymbol{x}$ generated through the proposed approach is shown in Figure 17. As it can be seen, the number of bits that can be embedded in $\boldsymbol{x}$ rapidly decreases for increasing values of Q, till a plateau is reached when the effective bandwidth of the rotation matrix $\boldsymbol{A}$ is saturated.

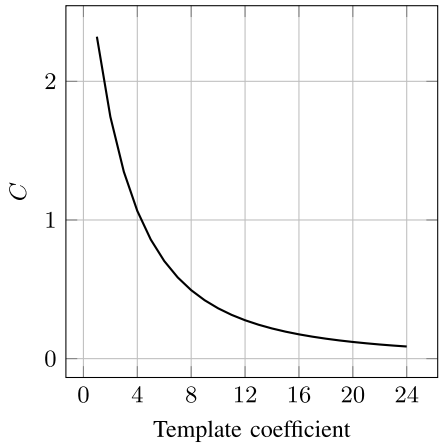

Fig. 16. Capacities of the L=24 coefficients of the synthetic template.

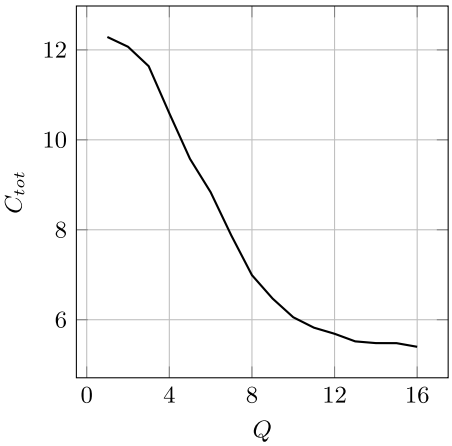

Fig. 17. Overall capacity C_{tot} vs Q, for a synthetic template with L=24 coefficients.

Template unlinkability with respect to the employed parameter Q is evaluated by considering the attacks described in Section IV. The fitness-to-distance correlation r is shown in Figure 18, considering synthetic templates made of $L = 24$ coefficients and one bit embedded into each coefficient. The behavior of the linkability measure $D^{sys}_{\leftrightarrow}$ is instead shown in Figure 19, for different values of γ. As expected, templates generated from the same original representations get less linkable as both parameters Q and γ increases.

VI. Experimental Validation on Real Biometric Data

The proposed zero-leakage unlinkable cryptosystem, depicted in Figure 20, is tested using real biometric data. Specifically, in Section VI-A we introduce the biometric database exploited in the tests. The feature extraction approach is described in Section VI-B. The preprocessing applied to the extracted features to generate a template $\boldsymbol{w}$ with independent coefficients, and the estimation of the point-wise function $f(\cdot)$, are given in Section VI-C. Details about both the employed ECC and the QIM are given in Section VI-D. The obtained results are finally discussed in Section VI-E.

A. Finger Vein Biometrics

Without any loss of generality, in our experiments we have considered finger-vein biometrics, and specifically the

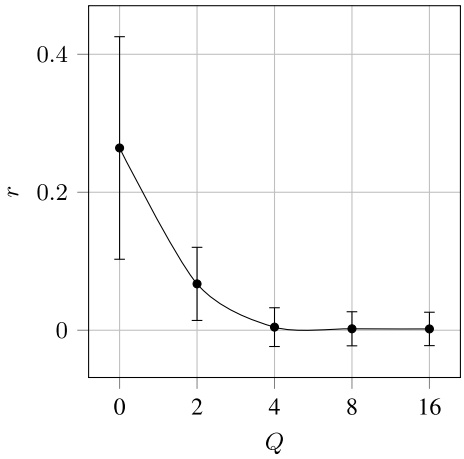

Fig. 18. Average and standard deviation of the fitness-distance correlation r vs Q.

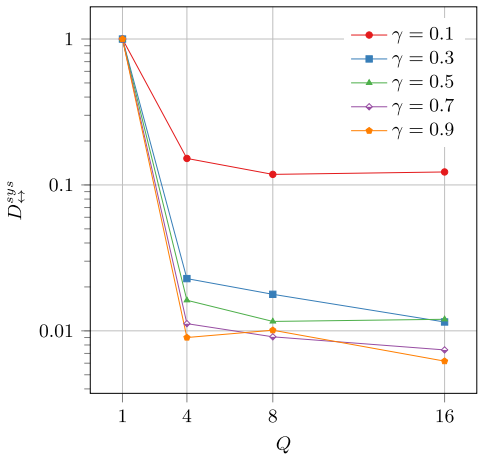

Fig. 19. Linkability measure $D^{sys}_{\leftrightarrow}$ vs Q.

SDUMLA database [31], containing images of the index-, middle- and ring-fingers captured from the left and right hands of 106 subjects. Six gray-scale samples of 320 × 240 pixels are available for each finger.

Assuming an open-set scenario, the employed database has been split into two equal-size subsets, with data from 53 subjects employed for training, and samples from the remaining ones for testing. The employed feature extractor has been trained using each available finger as an independent class. Then, the template used in the experimental tests is obtained by concatenating the features obtained from the three fingers of a user's hand, in order to handle identifiers with a larger number of coefficients. Therefore, the considered testing dataset comprises 6 samples for each of 53 × 2 classes.

B. Feature Extraction

A fixed-length feature vector, with the desirable discriminative capabilities described in Section II, is obtained by using the approach proposed in [32], where representations of vein patterns suitable for verification systems have been obtained using deep learning techniques.

In more detail, a Densenet-161 [33] convolutional neural network (CNN), modified with the addition of a custom embedder layer producing 2048 features in the final output layer, has been trained using an additive angular margin penalty (AAMP) [34] as loss function. Such approach allows training the employed network in a standard modality for classification purposes, while achieving the additional goal of generating representations having the largest possible inter-class variance, as well as the smallest possible intra-class variance.

The employed network has been trained by initializing Densenet-161 with weights pre-trained on the ImageNet dataset for object recognition purposes, while a Glorot uniform distribution has been used to initialize the fully-connected layers of the custom embedder. Stochastic gradient descent (SGD) with a batch size of 64, a learning rate of 0.01 divided by 10 after every 30 epochs, a momentum of 0.9, and a maximum number of 120 epochs have been considered during training. As for the hyper-parameters of the employed AAMP loss function, the penalty margin has been selected in the range $m \in [0.3, 0.7]$, with a step size of 0.05, as the one providing the best results, while the associated scale parameter has been selected in the range $s \in [16, 96]$, with a step size of 16.

In [32], an equal error rate (EER) at 0.02% on SDUMLA, using identifiers derived from a single finger, has been reported. The concatenation of the features associated to three fingers allows to further improve the performance of an unprotected system, with the FRR and the false acceptance rate (FAR) reported in Figure 21, when using the Euclidean distance to compare the considered identifiers. Given the size of the employed database, the obtained FRR and FAR curves do not Intersect each other, being therefore only possible to report that EER $< 0.06\%$, the lowest measured FRR, for an unprotected system.

C. Preprocessing

As remarked in Section V, in order to enforce the security requirement, the employed biometric representations should have independent features. Unfortunately, the features extracted through a CNN are not independent and therefore they should be further processed to generate an appropriate representation, namely $\boldsymbol{w}$ in our approach, as input of the proposed protection scheme.

To this goal, we have here exploited the Reconstruction Independent Component Analysis (RICA) [35], differently from [15] where the PCA has been employed. RICA is an unsupervised feature learning approach, which possesses some advantages *wrt* ICA. In fact, ICA requires a whitening stage, commonly performed through PCA, which makes its application difficult when dealing with high-dimensional input data and limited training sets. These conditions apply to the considered scenario, since the CNN described in Section VI-B extracts 2048-long templates, while the available training set only comprises 53 × 6 unique fingers, 6 instances each. Therefore, the total number of samples is slightly smaller than the size of the input space. Furthermore, since the samples of each user are strongly correlated, the number of reliable components that a PCA can learn is limited by the number of available classes. Therefore, while the use of classical PCA or ICA is inappropriate in the considered framework, RICA can

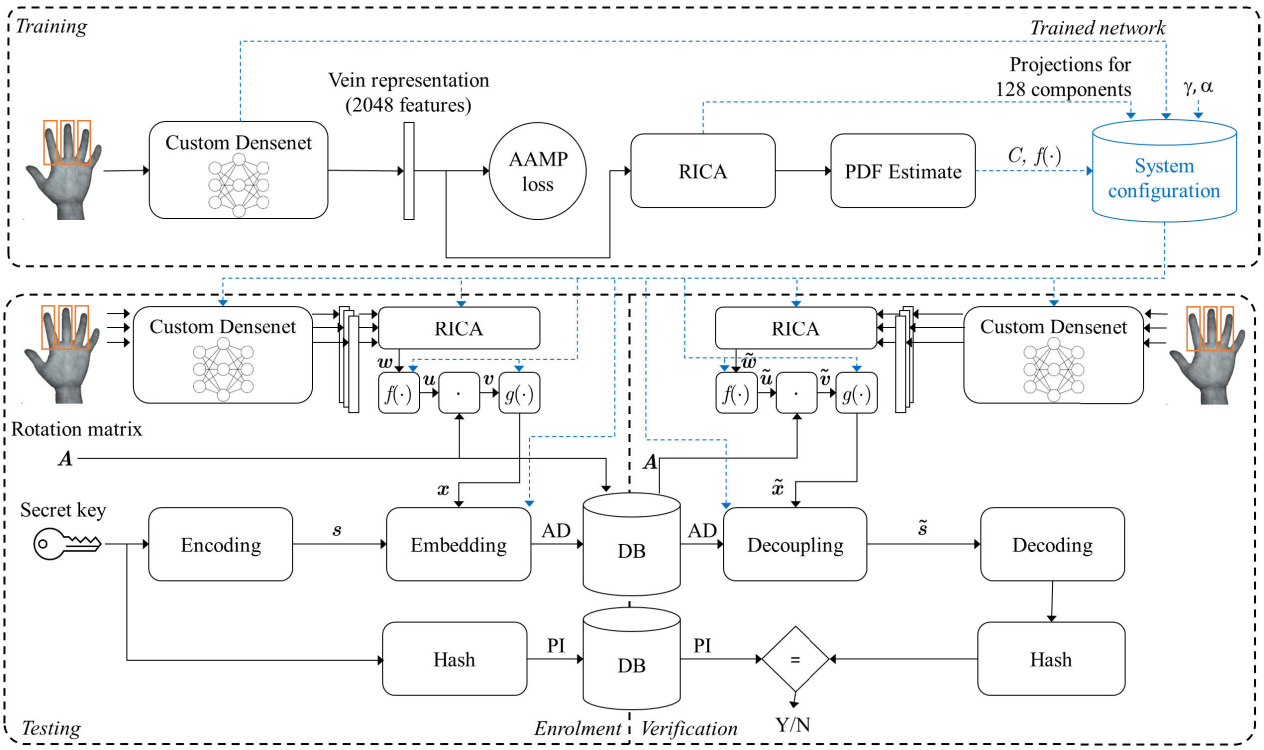

Fig. 20. High-level representation of training and testing phases for the proposed system.

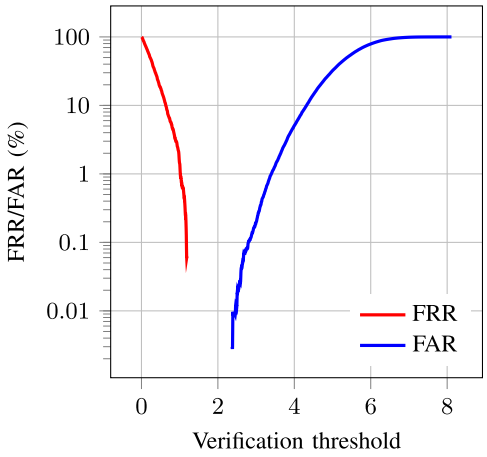

Fig. 21. Recognition rates for an unprotected system.

be instead effectively applied in such over-complete scenarios since it does not need an initial whitening stage.

We set the RICA algorithm to extract 128 features from the original 2048 coefficients. As mentioned in Section VI-A, the proposed cryptosystem is tested on biometric representations obtained by combining the features extracted from three fingers of a user's hand, thus obtaining a template $\boldsymbol{w}$ with $L = 384$ coefficients.

During the training stage, the templates obtained applying a RICA to the representations generated through the employed CNN are also examined in order to estimate the PDFs of each feature, required to define the functions $f(\cdot)$ introduced in Eq. (8). Since the treated coefficients can be assumed independent, the distribution estimates can be easily computed through the marginal variables. For each feature, the following seven different distributions are fit to the available data:

- Extreme Value Distribution;
- Generalized Extreme Value Distribution;
- Logistic Distribution;
- Normal Distribution;
- Rayleigh Distribution;
- Stable Distribution;
- t Location Scale Distribution.

The function $f(\cdot)$ associated with each coefficient is chosen by selecting the best fitting distribution by means of the Anderson-Darling test [36].

In summary, the proposed preprocessing allows creating representations $\mathbf{x}$, after having set γ, with *i.i.d.* coefficients. These templates are used as input of the proposed QIM-based protection scheme.

D. System Configuration

The implementation of the proposed biometric cryptosystem needs the design of the function $g(\cdot)$, the required ECC, and the allocation of the bits within the template coefficients.

As outlined in Sections II and III, the function $g(\cdot)$ can be specified by selecting the roll-off parameter γ of the employed raised-cosine distribution. As discussed in Sections IV and V, the unlinkability of the proposed system improves for increasing values of γ, just like the irreversibility shown in Figure 2, with no significant improvements for $\gamma > 0.7$. Since the overall capacity is instead negatively affected by high γ values, in the performed tests we have opted to select a $g(\cdot)$ function with $\gamma = 0.7$ for all the coefficients. The N encoded bits $\boldsymbol{c}$

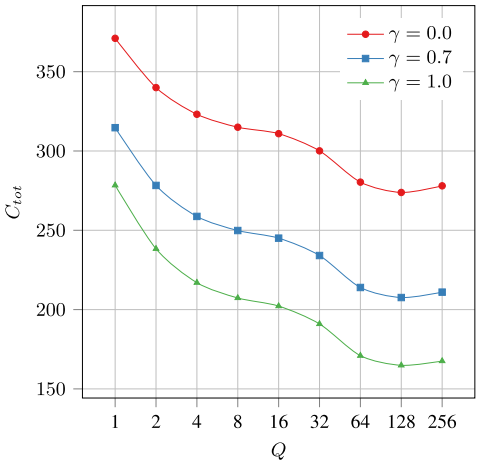

Fig. 22. Overall capacity vs rotation bandwidth Q, for different γ values.

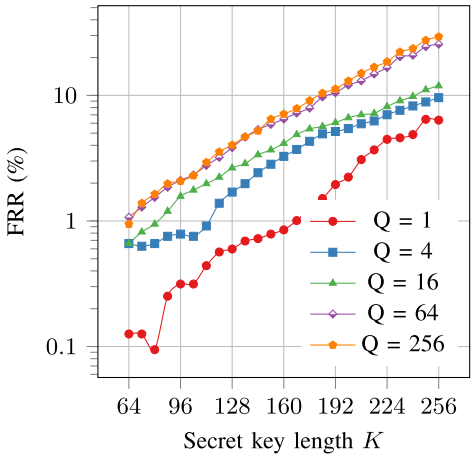

Fig. 23. FRR (in %) vs secret key length K and rotation bandwidth Q.

are distributed among the coefficients of $\boldsymbol{x}$ as a function of their capacity:

$$B = \lfloor \frac{N}{K} \alpha C \rfloor, \tag{34}$$

being $\lfloor \cdot \rfloor$ the floor function, K the size of the secret key, C the capacity of the considered coefficient, and α a parameter, same for all the L features, chosen in such a way that the sum of all the bits assigned to each coefficient equals the size N of the encoded secret key.

As for ECC, we have used Turbo Codes with a rate $N/K = 7$. Specifically, we have used codes specified in the Long Term Evolution (LTE) standard. Turbo codes are particularly powerful because they can rely on log-likelihood-based receivers to perform soft decoding, so to approach Shannon's capacity minimizing the FRR.

As mentioned in Section II, the possibility of using likelihood-based decoders is the main advantage of real-valued auxiliary-data schemes over binary ones. In fact, the hard quantization needed in classical schemes, such as in the fuzzy commitment, leads to huge information losses with a significant impact on the probability of correct recognition.

E. Obtained Results

The overall capacity C_{tot} of the representations obtained following the described approach is reported in Figure 22, where the influence of the bandwidth of the orthonormal matrix $\mathbf{A}$ on the system characteristics is shown. As already outlined in Section V, an increase in the values of Q and γ negatively affects the attainable capacity. Choosing a value $\gamma = 0.7$ for the employed raised cosine distribution allows achieving capacities around 250 bits for $Q \leq 16$, while secret keys with 128 bits can be obtained also for large values of Q.

The recognition performance achievable by applying the proposed protection method to finger-vein traits, as a case study and without any loss of generality, is reported in Figure 23. While the system is inherently designed to work at FAR $= 2^{-K}$, the achievable FRR depends both on the length of the employed secret key and on the value Q adopted for the orthonormal matrix $\mathbf{A}$. A system with $Q = 1$, as in [15], achieves the best possible recognition performance, with FRR $= 0.1\%$ for $K = 80$, yet it is not able to provide any unlinkability. On the other hand, the approach here proposed guarantees unlinkability with a FRR lower than 5% when using secret keys with $K = 128$ bits. This makes the considered system secure against any brute-force attacks carried out with the technology currently conceivable.[5] Embedding keys with 256 bits would imply a FRR at about 10% for $Q \leq 16$, while worse recognition performances are achieved when using orthonormal matrices with larger bandwidths due to associated reduction in the available capacity. To the best of our knowledge, no other biometric cryptosystems able to embed secret keys with lengths in the order of hundreds of bits, and able to properly meet, at a satisfactory recognition rate, both the required security and renewability constraints, has been proposed in the literature.

It is worth remarking that conditions at FAR $= 2^{-K}$ are achievable in the proposed system under the assumption of *i.i.d* representations $\mathbf{x}$. However, since both RICA projections and the PDFs of each feature in $\mathbf{w}$ are estimated over a training dataset, and then applied to a different one, realistic applications of the proposed method would result in non-ideal characteristics for the biometric templates $\mathbf{x}$ adopted in testing conditions. This is due to the inaccurate estimates of the involved coefficients distributions, and it is typically the more significant the smaller the size of the training dataset. The influence of such discrepancies on the achievable security has been analyzed by evaluating the security bound $K \frac{DoF}{N}$ described in [29], with DoF representing the degrees of freedom of the best binomial distribution fitting the inter-class Hamming distance distribution obtained when comparing the binarized templates $\mathbf{x}$ of a subject with those associated to possible impostors. In case of independent coefficients, the estimated DoF would correspond to N, with the achievable security therefore corresponding to the length of the secret keys employed in the proposed scheme, that is, $K \frac{DoF}{N} \approx K$.

Figure 24 shows the results obtained when considering $Q = 1$ in the employed rotation matrix ($\mathbf{A} = \mathbf{I}$), in order

[5] https://www.simms.co.uk/tech-talk/understanding-the-levels-of-encryption/

Fig. 24. Effective security as in [29].

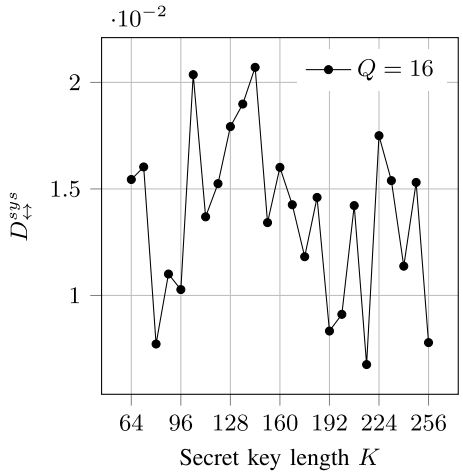

Fig. 25. Linkability measure $D^{sys}_{\leftrightarrow}$ vs K on real data.

to avoid any other source of fluctuation in addition to the inter-class variability. For the training dataset, a behavior close to the ideal one ($K\frac{DoF}{N} \approx K$) is achieved. However, the mismatch between the distributions characterizing the training and the testing datasets causes a performance worsening on the testing dataset. Nevertheless, the consequent amount of degradation is limited, thus allowing high values of $K\frac{DoF}{N}$ to be reached. Therefore, the carried out analysis confirms that the proposed protection scheme, which applies transformations to the original templates to make the coefficients of the representations $\mathbf{w}$ independent, is effective to guarantee high levels of security in practical scenarios.

Eventually, Figure 25 reports the linkability measure $D^{sys}_{\leftrightarrow}$ computed on real data, for different values of K, when considering $Q = 16$. The obtained results show that the evaluated $D^{sys}_{\leftrightarrow}$ is weakly correlated with the length K of the employed secret key, yet with a decreasing slope. In addition, as already shown in Figures. 11 and 19 for ideal and synthetic data, our analysis shows that very low linkability rates can be achieved also in real-world conditions.

VII. Conclusion

In this paper, the biometric cryptosystem system proposed by the authors in [15] has been improved in order to make it immune to linkability attacks. In contrast with other methods proposed in the literature, unlinkability is here achieved using parameters that can be considered as public, with no requirements for their secret storage.

The effectiveness of the proposed solution is tested against two different kinds of attacks. The first one, based on stochastic optimization, is shown to be unfeasible due to the computational complexity required to solve a system of non-linear equations. The second one relies on estimates of the employed biometric representations, and it is evaluated using quantitative measures, showing that templates stemming from the same identity cannot be linked if the parameters of the proposed scheme are properly selected.

In addition, real-world scenario data have been considered as a case study, and guidelines to properly design the components of the proposed scheme are given. The proposed cryptosystem has been applied to biometric templates derived from finger-vein patterns, using CNNs to generate the employed representations, and processing the obtained data to achieve feature independence, irreversibility, and unlinkability. The performed tests have shown that it is possible to perform protected biometric recognition while guaranteeing user-friendly recognition performance in terms of FRR at FAR ≈ 0, and a level of security comparable with the one achieved in current cryptographic protocols relying on keys with at least 128 bits.

References

[1] P. Tuyls, B. Škorić, and T. Kevenaar, *Security With Noisy Data*. London, U.K.: Springer, 2007.

[2] P. Campisi, *Security and Privacy in Biometrics*. London, U.K.: Springer, 2013.

[3] A. Dantcheva, P. Elia, and A. Ross, "What else does your biometric data reveal? A survey on soft biometrics," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 441–467, Mar. 2016.

[4] G. Mai, K. Cao, P. C. Yuen, and A. K. Jain, "On the reconstruction of face images from deep face templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 41, no. 5, pp. 1188–1202, May 2019.

[5] R. L. Lagendijk and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 82–105, Jan. 2013.

[6] *Information Technology—Security Techniques—Biometric Information Protection*, Standard ISO/IEC JTC1 SC27 Security Techniques, ISO/IEC 24745:2011, International Organization for Standardization, 2011.

[7] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 54–65, Sep. 2015.

[8] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP J. Inf. Secur.*, vol. 2011, no. 1, pp. 1–25, Dec. 2011.

[9] S. Wang and J. Hu, "Design of alignment-free cancelable fingerprint templates via curtailed circular convolution," *Pattern Recognit.*, vol. 47, no. 3, pp. 1321–1329, Mar. 2014.

[10] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Secure and robust iris recognition using random projections and sparse representations," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 9, pp. 1877–1893, Sep. 2011.

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

[12] K. Simoens, P. Tuyls, and B. Preneel, "Privacy weaknesses in biometric sketches," in *Proc. 30th IEEE Symp. Secur. Privacy*, May 2009, pp. 188–203.

[13] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy–security trade-offs in biometric security systems—Part I: Single use case," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 122–139, Mar. 2011.

[14] T. Ignatenko and F. M. J. Willems, "Fundamental limits for privacy-preserving biometric identification systems that support authentication," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5583–5594, Oct. 2015.
[15] G. E. Hine, E. Maiorana, and P. Campisi, "A zero-leakage fuzzy embedder from the theoretical formulation to real data," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 7, pp. 1724–1734, Jul. 2017.
[16] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. 6th ACM Conf. Comput. Commun. Secur.*, Nov. 1999, pp. 28–36.
[17] E. Maiorana, D. Blasi, and P. Campisi, "Biometric template protection using turbo codes and modulation constellations," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Dec. 2012, pp. 25–30.
[18] T. Ignatenko and F. M. J. Willems, "Biometric systems: Privacy and secrecy aspects," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 956–973, Dec. 2009.
[19] L. Zhou, T. J. Oechtering, and M. Skoglund, "Fundamental limits-achieving polar code designs for biometric identification and authentication," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 180–195, 2022.
[20] J. de Groot, B. Škorić, N. de Vreede, and J.-P. Linnartz, "Quantization in zero leakage helper data schemes," *EURASIP J. Adv. Signal Process.*, vol. 2016, no. 1, pp. 1–13, Dec. 2016.
[21] T. Stanko, F. Nur Andini, and B. Škorić, "Optimized quantization in zero leakage helper data systems," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 8, pp. 1957–1966, Aug. 2017.
[22] 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. London, U.K.: Springer, 2013, pp. 105–122.
[23] I. Buhan, J. Breebaart, J. Guajardo, K. de Groot, E. Kelkboom, and T. Akkermans, "A quantitative analysis of indistinguishability for a continuous domain biometric cryptosystem," in *Data Privacy Management and Autonomous Spontaneous Security*. Berlin, Germany: Springer, 2010.
[24] E. J. C. Kelkboom, J. Breebaart, T. A. M. Kevenaar, I. Buhan, and R. N. J. Veldhuis, "Preventing the decodability attack based cross-matching in a fuzzy commitment scheme," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 107–121, Mar. 2011.
[25] T. Jones and S. Forrest, "Fitness distance correlation as a measure of problem difficulty for genetic algorithms," in *Proc. Int. Conf. Genetic Algorithms*, 1995, pp. 184–192.
[26] F. Mezzadri, "How to generate random matrices from the classical compact groups," *Notices Amer. Math. Soc.*, vol. 54, no. 5, pp. 592–604, Oct. 2006.
[27] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch, "General framework to evaluate unlinkability in biometric template protection systems," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 6, pp. 1406–1420, Jun. 2018.
[28] H. O. Shahreza, Y. Y. Shkel, and S. Marcel, "Measuring linkability of protected biometric templates using maximal leakage," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 2262–2275, 2023.
[29] T. Van hamme, E. A. Rúa, D. Preuveneers, and W. Joosen, "On the security of biometrics and fuzzy commitment cryptosystems: A study on gait authentication," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 5211–5224, 2021.
[30] W. Press, S. Teukolsky, W. Vetterling, and B. Flannery, *Givens Method*. Cambridge, U.K.: Cambridge Univ. Press, 2007.
[31] Y. Yin, L. Liu, and X. Sun, "SDUMLA-HMT: A multimodal biometric database," in *Proc. Chin. Conf. Biometric Recognit.*, 2011, pp. 260–268.
[32] R. S. Kuzu, E. Maiorana, and P. Campisi, "Loss functions for CNN-based biometric vein recognition," in *Proc. EUSIPCO*, 2020, pp. 750-754.
[33] G. Huang, Z. Liu, L. Van Der Maaten, and K. Q. Weinberger, "Densely connected convolutional networks," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jul. 2017, pp. 2261–2269.
[34] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive angular margin loss for deep face recognition," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2019, pp. 4685–4694.
[35] Q. Le, A. Karpenko, J. Ngiam, and A. Ng, "ICA with reconstruction cost for efficient overcomplete feature learning," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 24, 2015, pp. 1017–1025.
[36] M. A. Stephens, "EDF statistics for goodness of fit and some comparisons," *J. Amer. Stat. Assoc.*, vol. 69, no. 347, pp. 730–737, Sep. 1974.

Gabriel Emile Hine (Member, IEEE) received the Ph.D. degree in applied electronics from Roma Tre University in 2019. Since 2020, he has been an Algorithms and Systems Engineer at Fingerprint Cards AB, filing several patents on iris-liveness detection. His main research interests include signal processing, information security, and biometrics. His Ph.D. thesis received the 13th European Biometrics Research Award by the European Association for Biometrics. He was a recipient of the Best Paper Award from the ICPRAM 2022.

Ridvan Salih Kuzu received the Ph.D. degree in applied electronics from Roma Tre University in 2021. Since 2021, he has been a Research Assistant with the Remote Sensing Technology Institute, German Aerospace Center (DLR), and a AI Consultant at the Helmholtz AI Cooperation Unit. His current research interests include signal processing, multi-spectral image processing, machine learning, and quantum computing. His Ph.D. thesis received the 15th European Biometrics Research Award by the European Association for Biometrics. He was a recipient of the Best Demo Award from the 9th GTTI Thematic Meeting on Multimedia Signal Processing in 2019 and the Best Paper Award from the ICPRAM 2022.

Emanuele Maiorana (Senior Member, IEEE) received the Ph.D. degree in telecommunication engineering, with European Doctorate Label, from Roma Tre University in 2009. He is currently an Assistant Professor with the Department of Industrial, Electronics and Mechanical Engineering, Roma Tre University. His research interests include digital signal and image processing, with specific emphasis on biometric recognition. He was a recipient of the Lockheed Martin Best Paper Award for the Poster Track from the IEEE Biometric Symposium in 2007, the Honeywell Student Best Paper Award from the IEEE BTAS Conference in 2008, and the Best Paper Award from the ICPRAM in 2022. He was the General Chair of the 9th IEEE International Workshop on Biometrics and Forensics (IWBF) in 2021. He is an Associate Editor of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.

Patrizio Campisi (Fellow, IEEE) received the Ph.D. degree in electrical engineering from Roma Tre University. He is currently a Full Professor with the Department of Industrial, Electronics and Mechanical Engineering, Roma Tre University. His research interests include biometrics and secure multimedia communications. He was a co-recipient of the Best Student Paper Award from IEEE ICIP06 and the IEEE BTAS in 2008 and the Best Paper Award from IEEE Biometric Symposium in 2007. He was the IEEE SPS Director–Student Services from 2015 to 2017 and the Chair of the IEEE Technical Committee on Information Forensics and Security from 2017 to 2018. He was the General Chair of the 26th European Signal Processing Conference (EUSIPCO) in 2018 and the 7th IEEE Workshop on Information Forensics and Security (WIFS) in 2015. He is an Editor of the book *Security and Privacy in Biometrics* (Springer, 2013) and a Co-Editor of the books *Blind Image Deconvolution: Theory and Applications* (CRC Press, 2007) and *High Dynamic Range Video, Concepts, Technologies and Applications* (Academic Press, 2017). He was an Associate Editor and a Senior Associate Editor of the IEEE SIGNAL PROCESSING LETTERS, an Associate Editor of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY (TIFS), and the Editor-in-Chief of the IEEE TIFS. He is the Vice-President of Publications for the IEEE Biometrics Council.

Open Access funding provided by 'Università degli Studi Roma Tre' within the CRUI CARE Agreement