IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 20, 2017, accepted March 20, 2017, date of publication April 27, 2017, date of current version June 7, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2691578

Privacy-Preserving Comparison of Variable-Length Data With Application to Biometric Template Protection

MARTA GOMEZ-BARRERO[1], JAVIER GALBALLY[2], AYTHAMI MORALES[3], AND JULIAN FIERREZ[3]

[1]da/sec-Biometrics and Internet Security Research Group, Hochschule Darmstadt, Darmstadt 64295, Germany
[2]European Commission Directorate-General Joint Research Center, Ispra 21027, Italy
[3]Area del Tratamiento de la Voz y la Señal-Biometric Recognition Group, Universidad Autonoma de Madrid, Madrid 28049, Spain

Corresponding author: Marta Gomez-Barrero (marta.gomez-barrero@h-da.de)

This work was supported in part by the German Federal Ministry of Education and Research (BMBF); in part by the Hessen State Ministry for Higher Education, Research, and the Arts (HMWK) within the Center for Research in Security and Privacy (CRISP); in part by the Spanish Ministerio de Economia y Competitividad / Fondo Europeo de Desarrollo Regional through the CogniMetrics Project under Grant TEC2015-70627-R; and in part by Cecabank.

ABSTRACT The establishment of cloud computing and big data in a wide variety of daily applications has raised some privacy concerns due to the sensitive nature of some of the processed data. This has promoted the need to develop data protection techniques, where the storage and all operations are carried out without disclosing any information. Following this trend, this paper presents a new approach to efficiently compare variable-length data in the encrypted domain using homomorphic encryption where only encrypted data is stored or exchanged. The new variable-length-based algorithm is fused with existing fixed-length techniques in order to obtain increased comparison accuracy. To assess the soundness of the proposed approach, we evaluate its performance on a particular application: a multi-algorithm biometric template protection system based on dynamic signatures that complies with the requirements described in the ISO/IEC 24745 standard on biometric information protection. Experiments have been carried out on a publicly available database and a free implementation of the Paillier cryptosystem to ensure reproducibility and comparability to other schemes.

INDEX TERMS Privacy, security, homomorphic encryption, template protection, biometrics, signature.

I. INTRODUCTION

In the last few years, the volume of data captured and processed within cloud platforms has seen a huge increase. In spite of the numerous advantages offered by cloud computing, several unresolved security and privacy threats have been raised. These threats, which include privacy, confidentiality, integrity, and availability of data, are magnified by the volume, velocity, and variety of Big Data [1]. Therefore, while one of the fundamental challenges for Big Data is to extract useful information from large volumes of data, a real-world concern is that such applications are in many cases related to sensitive information, such as banking transactions or medical records [2]. As a consequence, it is of the utmost importance to protect the privacy of such data and its owner, developing privacy preserving data services approaches [3], [4]. In fact, numerous efforts are being directed towards this end within very diverse areas, including genomics [5] or drones [6].

One promising approach to achieve privacy preserving technologies is the use of Fully Homomorphic Encryption (FHE), which allows for computations to be performed on ciphertexts, generating encrypted results which decrypt to plaintexts that match the result of the operations carried out on the original plaintexts. However, practical implementations of FHE schemes, which allow for real-time computations, still remain a big challenge [7]. Therefore, somewhat Homomorphic Encryption (HE) schemes, which only allow a limited subset of operations in the encrypted domain, are nowadays being introduced into many signal processing based applications, such as electronic voting, private information retrieval and private searches [8].

More specifically, HE schemes are used in applications where it is required to compare data in a privacy enhancing manner [7], [9]. Such comparison can be established for fixed-length data, using common distance functions, or using variable-length data, via more complex algorithms such as

Dynamic Time Warping (DTW) [10]. Whereas systems using fixed-length data are computationally efficient even considering the overhead introduced by HE, in many cases they present lower accuracy than systems working with variable-length representations. To palliate the lower accuracy achieved, algorithms such as DTW have been proposed and implemented in the encrypted domain [11] at the cost of a big computational overhead, which is not affordable in real-time applications.

In the present work, we try to tackle those issues by applying different sub-sampling techniques to the input signals in order to reduce the computational complexity of the DTW-based algorithm. Then, in order to compensate for the reduced comparison accuracy derived from this sub-sampling process, the results are fused at score level with a time-efficient approach based on a global fixed-length representation of the data.

One example of the aforementioned applications is biometric recognition, which has emerged over the last decades as a reliable alternative to traditional authentication systems based on something that we know (i.e., PINs or passwords) or something that we have (i.e., IDs or tokens) [12]. This is partly due to the fact that biometric characteristics (e.g., signature, face or iris) cannot be lost or forgotten. On the down side, biometric information is very sensitive and some concerns have been raised regarding the privacy of the subjects and the security of the systems - it has already been proved that samples can be recovered from unprotected templates [13]–[16] and be subsequently used to impersonate genuine subjects [17]. As a consequence, any information leakage resulting from an inappropriate storage of the derived templates can lead to severe privacy and security issues. In fact, biometric data is considered sensitive data in European Union (EU) General Data Protection Regulation 2016/679 [18], which means that the use of these data is subjected to the right of privacy preservation. Biometric templates must be hence protected in order to prevent any potential leakage of the underlying information. Among other approaches to biometric template protection, HE allows to meet the privacy requirements established within the ISO/IEC 24745 international standard on biometric information protection [19] while preserving verification accuracy [20]–[22].

In order to confirm the validity of the proposed privacy-preserving comparison scheme, we carry out a thorough security and privacy evaluation of a biometric template protection scheme based on the proposed comparison technique. In particular, we have chosen online handwritten signatures as biometric modality, which is one of the most widely spread characteristics due to its traditional legal and social acceptance. For the evaluation, we follow the framework established in [23], which assesses all requirements established by the ISO/IEC 24745 standard on biometric information protection [19] for biometric template protection (BTP) schemes:

- *Irreversibility*: given a protected template, it should leak no biometric information (i.e., it should not be possible to go back from the template to the biometric sample that originated it).
- *Unlinkability*: given two templates protected with different keys (i.e., enrolled in different systems), it should not be feasible to decide whether they conceal the same biometric instance.
- *Renewability*: if one template is lost or stolen, it should be possible to issue a new one, not matching the old template.

In addition, and to make the experiments reproducible, a free implementation of the Paillier cryptosystem[1] and the signature corpus of the publicly available multimodal BiosecurID database [24] are used.

The main contributions of the article can therefore be summarised in the following:

- First multi-algorithm approach in the encrypted domain for fixed- and variable-length data representations, and its application to the particular case of biometric recognition based on online handwritten signature.
- Improvement of *i*) the computational complexity of the approach proposed in [25] and of *ii*) the verification accuracy achieved by the system proposed in [26].
- Full evaluation of the proposed multi-algorithm biometric template protection system according to the ISO/IEC IS 24745 requirements, following a reproducible experimental protocol.
- First unlinkability analysis of biometric template protection schemes based on Homomorphic Encryption.

The rest of the article is structured as follows. Related works on biometric template protection are summarised in Sect. II. Sect. III describes the Paillier cryptosystem. Sect. IV presents the unprotected comparison scheme. The protected comparison approach is described in Sect. V, and the complete biometric verification process to be evaluated is summarised in Sect. VI. The accuracy, irreversibility, unlinkability and complexity overhead of the biometric template protection scheme are analysed in Sect. VII, and final conclusions are drawn in Sect. VIII.

II. RELATED WORKS

As mentioned in Sect. I, the ISO/IEC 24745 standard on biometric information protection [19] establishes three main requirements for biometric template protection (BTP) systems (i.e., irreversibility, unlinkability and renewability). At the same time, verification accuracy of encrypted templates, verification time and storage requirments should be maintained with respect to the unprotected data [27].

Fulfilling the aforementioned requirements while minimising the accuracy degradation is not an easy task. Different approaches, mostly based on *cancelable biometrics* (i.e., irreversible transformations of the unprotected template which allow a comparison in the protected domain) or *cryptobiometrics* (i.e., a cryptographic key is either bound or extracted

[1]Publicly available at http://www.csee.umbc.edu/~kunliu1/research/Paillier.html

from the biometric data) have been proposed in the literature [28], [29]. More recent approaches based on Homomorphic Encryption and Garbled circuits can be classified within a new class, known as *biometrics in the encrypted domain*. Unlike cancelable biometrics, protected templates can be in this case decrypted with the secret key and re-encrypted with a different key, thereby granting renewability with no re-acquisition of the biometric data. On the other hand, there is no relationship between the biometric data and the cryptographic key as in biometric cryptosystems, thereby allowing for a higher level of security.

In the present section, we review the existing BTP schemes based on signature. For an exhaustive review of works dealing with with *cancelable biometrics* and *cryptobiometrics* template protection for biometric characteristics other than signature, the reader is referred to [30], [31].

A pioneering research line on BTPs for on-line signature relies on irreversible transformations that obscure the extracted features (i.e., *cancelable biometrics*). Although these techniques grant in most cases irreversibility, they usually result in some accuracy degradation. For instance, in the BioConvolving scheme [32], the original Hidden Markov Model (HMM) is trained with irreversibly transformed time sequences. On the other hand, in [33], a function-based on-line signature template protection system is proposed, where the time sequences are transformed in an irreversible manner. Performances degrade over 10% for all scenarios tested.

Another research line that has been studied for the development of template protection approaches in on-line signature is the use of fuzzy-based schemes, which account for the vast mayority of *cryprobiometric systems*. For instance, [34] proposes a fuzzy vault system based on minutiae extracted from on-line signatures. The fuzzy commitment paradigm was applied in [35] to a dynamic signature recognition system based on UBM-HMM (Universal Background Model-HMM), achieving a remarkable verification accuracy. Similarly, [36] presents a biometric cryptosystem based on hashes, while a BCH error correcting code and helper data were used in the scheme described in [37].

The main drawback of these cryptobiometric methods is that they use *Auxiliary Data* (AD), which can be exploited in order to obtain information about the hidden biometric data. This way, the privacy of the subject is violated, which entails that the irreversibility requirement is not fully met [38]–[40]. Additionally, as in the case of cancelable biometrics, cryptobiometric systems usually present a performance degradation with respect to the original systems relying on unprotected data.

As an alternative to the aforementioned approaches, secure multiparty computation and homomorphic cryptosystems can be used in order to carry out biometric recognition in the encrypted domain while obtaining results fully comparable to those yielded by plain data [7], [41]. In particular, current approaches to *biometrics in the encrypted domain* [22] are based on Garbled Circuits (GC) [42] and Homomorphic Encryption (HE) [7], [43].

Since efficient implementations of HE schemes are very recent [44], only a few *unimodal* biometric systems based on this protection technology have been proposed so far. In [21], the authors present a new fingerprint verification system based on the FingerCode fixed-length representation of fingerprints and HE. An improved version of that approach is suggested in [45]. In [46], Eigenface based templates are protected with HE. Then, a more efficient approach is presented in [47] using GCs for the threshold comparison. Furthermore, the SCiFI project [48] proposes a biometric identification algorithm specifically designed for a more efficient usage in secure computation, based on fixed-length templates with a constant Hamming weight. In [49], a secure iris BTP based on a combination of HE and GCs is proposed, handling encrypted iriscodes.

More recently, a general framework for fast and privacy-preserving distance computation, known as GSHADE and based on oblivius transfers, is proposed in [50]. In this work, the authors present particular implementations based on Garbled Circuits for several distance metrics and apply them to face, iris and fingerprint samples.

Regarding signature-based schemes, in [25] an on-line signature verification scheme is proposed, based on HE and a direct comparison of variable length functions extracted from the input signature. Even if a state-of-the-art verification accuracy is achieved, each comparison takes approximately one minute, thereby preventing its use in real time applications or where restrictions on the amount of exchanged data are low. On the other hand, a more efficient scheme based on a fixed-length global representation of the signature is described in [26]. The main drawback of this last system is the accuracy degradation with respect to that of more sophisticated comparison algorithms such as [25].

III. PAILLIER CRYPTOSYSTEM

We will use the following notation in the subsequent sections:

- $\mathbf{GX}_{F_g} = \{gx_1, \ldots, gx_f, \ldots, gx_{F_g}\}$: unprotected fixed-length representation, comprising F_g features gx_f.
- $\mathbf{SX}_{U\times F_s}$: unprotected variable-length representation, comprising F_s sequences of U time samples. The u-th point of the sample is an F_s-dimensional vector $\mathbf{SX}[u] = \mathbf{sx}^u = \{sx_1^u, \ldots, sx_{F_s}^u\}$. To simplify notation, to refer to *any* generic point we will use $\mathbf{sx} = \{sx_1, \ldots, sx_{F_s}\}$
- The set of both fixed- and variable-length representations belonging to a single data item (in our experiments one handwritten signature) will be denoted as $\mathbf{FX} = \left\{\mathbf{GX}_{F_g}, \mathbf{SX}_{U\times F_s}\right\}$ (where **FX** stands for full representation).
- m and m^*: plain message and its corresponding ciphertext.
- $m^* = E_{pk}(m, s)$, where E denotes the encryption function, s a random number and pk the public key.
- $m = D_{sk}(m^*)$, where D denotes the decryption function and sk the private key.

The multi-algorithm comparison strategy proposed in the present work (described in Sect. V) is based on the

specific implementation of the HE paradigm proposed by Paillier in [44]. In particular, all the operations involved in the similarity score computation are carried out in the encrypted domain. Therefore, for completeness, some important concepts related to the Paillier homomorphic probabilistic encryption scheme are introduced here, as they are key to the understanding of the proposed privacy-preserving comparison scheme.

The Paillier cryptosystem is based on the decisional composite residuosity assumption: given a composite n and an integer z, it is hard to decide whether z is an n-residue modulo n^2. As any other public key encryption scheme, it requires two separate keys: *i*) a public key $pk = (n, g)$, where $n = pq$ with p and q two large prime numbers such that $\gcd(pq, (p-1)(q-1)) = 1$, and $g \in \mathbb{Z}^*_{n^2}$; and *ii*) a secret key $sk = (\lambda, \mu)$, where $\lambda = \text{lcm}(p-1, q-1)$ and $\mu = \left(g^\lambda \mod n^2\right)^{-1} \mod n$.

Given a message $m \in \mathbb{Z}_n$, its encryption is denoted as $m^* = E_{pk}(m, s) \in \mathbb{Z}^*_{n^2}$, and computed as follows:

$$m^* = E_{pk}(m, s) = g^m \cdot s^n \mod n^2 \tag{1}$$

where $s \in \mathbb{Z}^*_n$ is a random number, generated a each encryption process, and hence providing the probabilistic nature of the cryptosystem. It should be noted that s is not needed for decryption, and a single value for s should not be used multiple times, dince it would decrease the security level of the system.

Then, in order to decrypt the ciphertext m^*, we have

$$m = D_{sk}(m^*) = L\left(m^{*\lambda} \mod n^2\right) \cdot \mu \mod n \tag{2}$$

where $L(t) = (t-1)/n$.

Two properties of Paillier cryptosystem will be used in the present scheme. First, the product of two ciphertexts, m_1^* and m_2^*, will decrypt to the sum of their corresponding plaintexts:

$$D_{sk}\left(m_1^* \cdot m_2^* \mod n^2\right) = m_1 + m_2 \mod n \tag{3}$$

Second, an encrypted plaintext, m_1^*, raised to a constant l, will decrypt to the product of the plaintext and the constant:

$$D_{sk}\left(\left(m_1^*\right)^l \mod n^2\right) = m_1 \cdot l \mod n \tag{4}$$

In order to avoid overcomplicated notation, in the description of the algorithm the keys pk and sk, as well as the random number s, will be omitted. Therefore, a generic cyphertext m^* will be simply denoted as $E(m)$.

IV. UNPROTECTED MULTI-ALGORITHM COMPARISON

In order to compare variable-length time sequences, the Dynamic Time Warping (DTW) algorithm has been widely used in the literature [10]. More specifically, within the biometric community, high accuracy rates within the state-of-the-art have been obtained for different characteristics, including EEGs [51] or handwritten signatures [25]. However, as mentioned in Sect. I, implementations of DTW in the encrypted domain show two major drawbacks [25]: *i*) the high computational complexity and *ii*) the increased storage requirements. Since both aspects are directly linked to the length of the input signals, these will be sub-sampled in order to achieve a more efficient system. However, such an approach may lead to degradation on comparison accuracy [52]. In order to minimise that degradation, the proposed system is based on the combination of two comparison schemes:

- A variable-length based algorithm, which compares sub-sampled sequences with the DTW algorithm. In order to obtain a similarity score between the probe ($\mathbf{SX}_{U\times F_s}$) and the reference data items ($\mathbf{SY}_{V\times F_s}$), a cost matrix ($\mathbf{Path}_{U\times V}$), minimizing the Euclidean distance between sequence points is computed. The final dissimilarity score is the last cell of the matrix: $S_{DTW} = \mathbf{Path}[U, V]$.
- An efficient but less accurate comparison algorithm based on a global fixed-length descriptor, **GX**, which compares the data items in terms of their Euclidean distance d_{euc}. Therefore, it outputs $S_{GF} = d^2_{euc}(\mathbf{GX}, \mathbf{GY})$. Since this representation will comprise information complementary to that of the sub-sampled sequences compared with the DTW algorithm, it is expected to palliate the accuracy degradation due to the sub-sampling of the original signals.

In order to output a single similarity score S, after obtaining both partial scores S_{GF} and S_{DTW}, they need to be *i*) normalised to a common range, and *ii*) fused. For the normalisation of the individual scores, several approaches are proposed in [53]. However, it is not possible to implement most of them in the encrypted domain without increasing the computational overhead. We therefore implement a different and simpler approach, which achieves the same accuracy as the min-max rule proposed for unprotected data in [53].

Without loss of generality, we can assume that $S_{DTW} > S_{GF}$. If the opposite is true, both scores need to be exchanged in the following computations in order to obtain integer parameters α and β, necessary for the Paillier cryptosystem. We can then perform the following normalisation, which in turn can be easily computed in the encrypted domain (see Sect. V-C):

$$S'_{GF} = \beta S_{GF} \Rightarrow E\left(S'_{GF}\right) = E\left(S_{GF}\right)^\beta \tag{5}$$

where β, the normalising parameter, is estimated as the average ratio between S_{DTW} and S_{GF} for genuine comparison scores.

Lastly, the final score is computed as the weighted sum of the two partial scores:

$$S = \alpha \cdot \beta \cdot S_{GF} + (10 - \alpha) \cdot S_{DTW} \tag{6}$$

where $\alpha \in [0, 10]$ is the integer weight applied to the fixed-length score, S_{GF}, and β is the aforementioned normalising parameter.

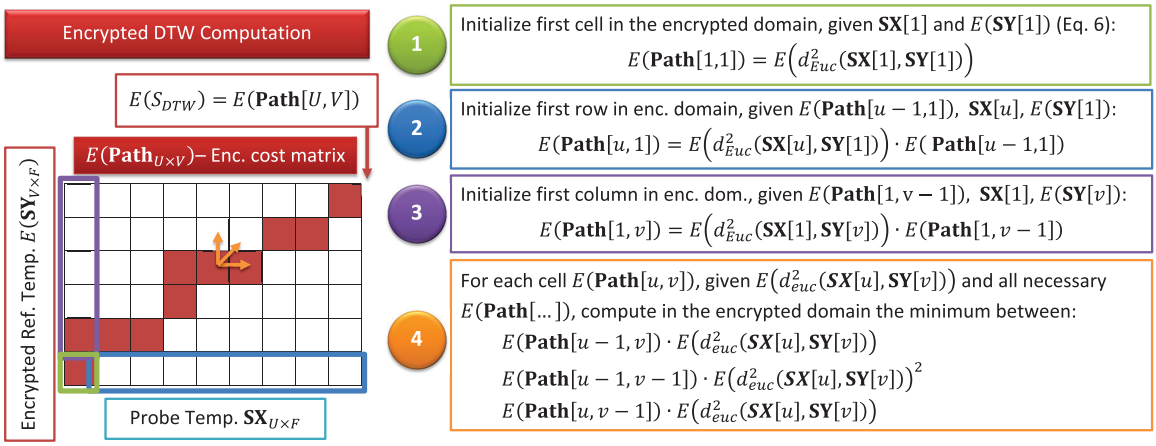


FIGURE 1. Encrypted DTW. In order to compare the probe $\mathbf{SX}_{U\times F_S}$ and the reference $\mathbf{SY}_{V\times F_S}$ data items, the optimal path, depicted in red, minimizing the Euclidean distance between points, is computed following the DTW algorithm. An encrypted cost matrix, Path is built in four steps. The last entry of the matrix contains the final encrypted score $E(S_{DTW})$.

V. PROTECTED MULTI-ALGORITHM COMPARISON

As mentioned in Sect. IV, the proposed multi-algorithm comparison approach is based on the score level fusion of two different comparison schemes: *i*) one based on fixed length global descriptors and the Euclidean distance; *ii*) a second one based on variable-length local descriptors and the DTW algorithm. Their corresponding implementations in the encrypted domain and the score level fusion are described in the following sections.

A. ENCRYPTED EUCLIDEAN DISTANCE

Both unencrypted comparison algorithms (see Sect. IV) ultimately rely on the Euclidean distance. Given two F-dimensional points $\mathbf{x}$ and $\mathbf{y}$, in the unprotected domain the Euclidean distance $d^2_{euc}(\mathbf{x}, \mathbf{y})$, can be computed as

$$d^2_{euc}(\mathbf{x}, \mathbf{y}) = \sum_{f=1}^{F} \left(x_f^2 + y_f^2 - 2x_f y_f\right) \tag{7}$$

Then, using Eqs. 3 and 4, the encrypted distance can be directly computed in the encrypted domain without performing any encryptions in the client (see Sect. VI and Fig. 2 for more details on the client-server model) as

$$\begin{aligned} E\left(d^2_{euc}(\mathbf{x}, \mathbf{y})\right) &= \prod_{f=1}^{F} E(1)^{x_f^2} \cdot E\left(y_f^2\right) \cdot E(y_f)^{-2x_f} \\ &= \prod_{f=1}^{F} (1^*)^{x_f^2} \cdot euc2_f^* \cdot \left(euc1_f^*\right)^{-2x_f} \end{aligned} \tag{8}$$

The reference data item (i.e., in biometrics the subject's reference template) stored in the encrypted database is thus defined by the following ciphertexts:

$$E(\mathbf{Y})_{euc} = \{1^*\} \cup \left\{euc1_f^*, euc2_f^*\right\}_{f=1}^{F} \tag{9}$$

where $euc1_f^* = E(y_f)$ and $euc2_f^* = E\left(y_f^2\right)$.

B. ENCRYPTED VARIABLE-LENGTH DATA COMPARISON BASED ON DTW

The particular implementation of the encrypted DTW proposed in the present article is shown in Fig. 1. In contrast to the unencrypted algorithm, all computations are now carried out directly in the encrypted domain. The algorithm computes an encrypted cost matrix $E(\mathbf{Path}_{U\times V})$, obtained from a plain probe item $\mathbf{SX}_{U\times F_s}$ and an encrypted reference item $E\left(\mathbf{SY}_{V\times F_s}\right)$, minimising the distance between item data points in terms of their Euclidean distance. The final encrypted comparison score is the last cell of a matrix, namely $E(S_{DTW}) = E(\mathbf{Path}[U, V])$. For the computations, Eqs. 3 and 4 are applied to convert the unprotected scheme to the encrypted domain: summations of plaintexts are substituted by products, and products of plaintexts by exponentiations.

As it may observed in Fig. 1, in order to compute the encrypted cost matrix, the encrypted Euclidean distance between data points will be calculated using Eq. 8. After initialising the first row and column of the cost matrix (steps 1 to 3), only three different directions are considered to the compute the best path at each new cell of the matrix (step 4). As a consequence, in order to grant the required privacy to the subject, an additional issue needs to be solved in the encrypted domain: compute the minimum between three encrypted values in the $E(\mathbf{Path})$ matrix.

Encrypted Minimum Computation: In order to compute the minimum between three values, without revealing any information about the plain values involved to the server, a two-phase protocol is established:

- The client generates a set of K random values $R = \{r_{min}, r_2, \ldots, r_K\}$, where $r_k > r_{min}$ for $k = 2, \ldots, K$. Then, the values to be minimized (m_1, m_2, m_3) are obscured by adding r_{min} to each of them:

$$E(m_i) \rightarrow E(m_i + r_{min}) = E(m_i) \cdot E(r_{min}) \quad \text{for } i = 1, 2, 3$$

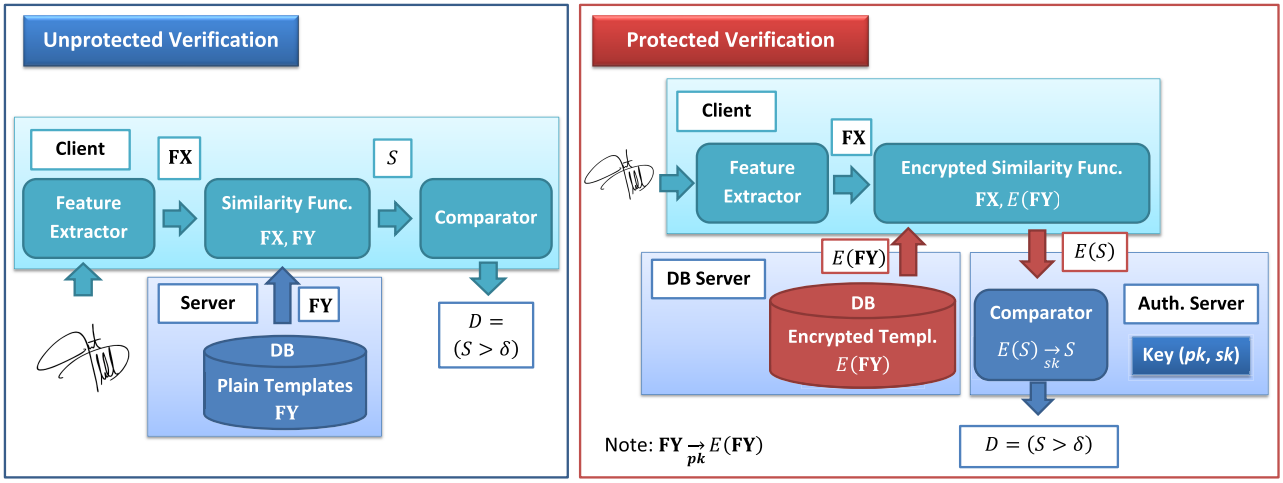


FIGURE 2. Unprotected vs Protected Biometric Verification. In the unprotected scenario (left), a probe biometric sample is acquired and its features extracted (FX). The final output is the binary decision $D = (S > \delta)$, where S is computed as the similarity distance with respect to the stored unprotected reference (FY). In the protected scenario (right), all the encrypted data or information flow is depicted in red: E (FY) and E (S).

To further hide those values, $K - 1$ additional numbers are generated by *i*) randomly choosing one of those original three values ($E(m_k)$) and *ii*) obscuring it with the corresponding value in R, r_k:

$$E(m_k) \rightarrow E(m_k) \cdot E(r_k) \quad \text{for } k = 2, \ldots, K$$

Therefore, the complete list $E(minList)$ comprises the aforementioned $K + 2$ encrypted and obscured values.

- The client then sends the complete list $E(minList)$ to the authentication server, who decrypts all the values using its secret key sk, computes the obscured minimum, encrypts it again, and sends it back to the client: $E(minCost + r_{min})$.

Finally, the client can compute the encrypted minimum value as

$$E(minCost) = E(minCost + r_{min}) \cdot E(r_{min})^{-1}$$

For a more detailed description of the algorithm, the interested reader is referred to [25].

C. ENCRYPTED SCORE LEVEL FUSION

As described in Sect. IV, the two, now protected, individual scores $E(S_{GF})$ and $E(S_{DTW})$ need to be fused into a single final encrypted score $E(S)$. From Eq. 6, and applying Eqs. 3 and 4, it follows that the final encrypted score $E(S)$ can be directly computed from the partial encrypted scores, $E(S_{GF})$ and $E(S_{DTW})$:

$$E(S) = E(S_{GF})^{\alpha \cdot \beta} \cdot E(S_{DTW})^{10-\alpha} \tag{10}$$

VI. BIOMETRIC TEMPLATE PROTECTION SCHEME

Taking into account the encrypted multi-algorithm comparison scheme described in Sect. V, we can define a complete encrypted verification process applicable to biometric template protection. To that end, we first need to define a security model and then the steps needed to carry out biometric verification in a privacy-preserving manner under the constraints of that security model.

A. SECURITY MODEL

In the present section we describe the general security model considered in this work, including all the assumptions made regarding the expected behaviour (honest or malicious) of each of the entities involved in the biometric recognition process. This way the reader can have a more general perspective of how different threats have been taken into account and how the proposed scheme deals with several privacy and/or security risks.

First, a general diagram of the unencrypted biometric verification system is depicted in Fig. 2 (left), where two entities are involved:

- A client, which will acquire the probe biometric sample, extract the features and encode them in the template **FX**, generate the similarity score between **FX** and the reference template **FY**, and compute the final genuine/impostor verification decision $D = (S > \delta)$, where δ is the pre-defined verification threshold.
- A server, which will hold the database with the reference templates **FY** and send them to the client during verification.

In order to increase the privacy of the subject, the server must process the client's biometric data without disclosing at any point any unprotected sensitive information, and at the same time, the server must protect the information stored in the database [54]. To that end, a different security model is used in the *protected* system (see Fig. 2, right) where all the data, either stored or shared between client and server in the

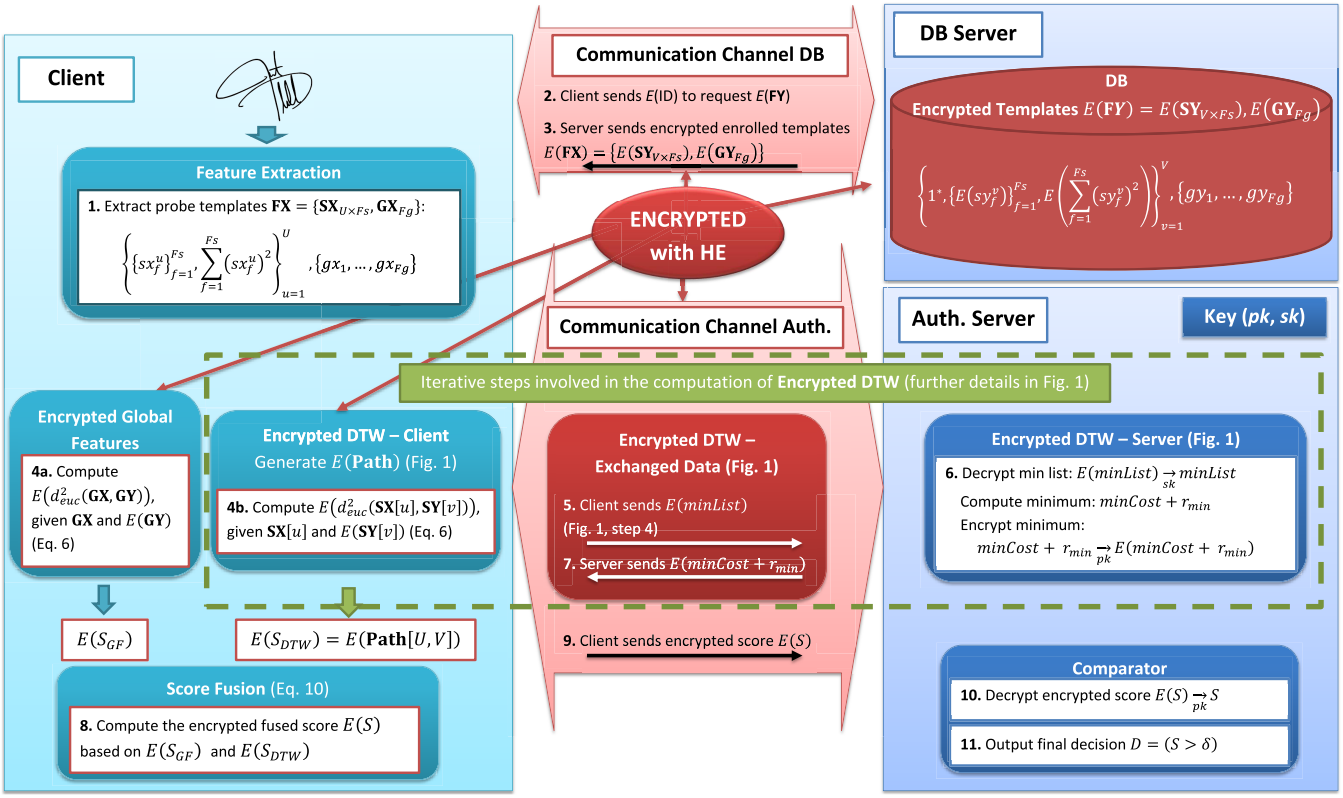


FIGURE 3. General diagram of the proposed encrypted verification process. A local client acquires and extracts the features of the probe signature ($\mathbf{SX}_{U\times Fs}$ and $\mathbf{GX}_{Fg}$) and computes the encrypted dissimilarity scores ($E(S_{GF})$ and $E(S_{DTW})$) between the probe and the reference signatures ($\mathbf{SY}_{V\times Fs}$ and $\mathbf{GY}_{Fg}$), in collaboration with the authentication server, which holds the key pair (pk, sk) and outputs the final decision. The DB server holds the encrypted database. All the encrypted values, either stored or transmitted on the communication channel, are depicted in red.

verification process, should be encrypted. Therefore, the new entities and roles are the following:

- The client acquires the probe biometric sample, extracts the template **FX** and generates the encrypted score $E(S)$ (see Sect. V), sending it to the authentication server.
- The DB server holds the database comprising only encrypted templates, and sends the encrypted reference template $E(\mathbf{FY})$ to the client during verification.
- The authentication server holds the key pair (sk, pk) and computes the final genuine/impostor decision D. It should be noted that a single key pair will be used for all subjects enrolled in the system.

With respect to the security model proposed in other biometric template protection approaches [55], in the present scheme the sensor and comparator have been integrated into a single entity: the client. Therefore, the requirements on the data flow described in [55] to fulfil the aforementioned irreversibility and unlinkability criteria have been adapted to the present model as:

- The authentication server should not learn **FY** or **FX**.
- The DB server should not learn **FY** or **FX**, or trace subjects.
- The client should not learn **FY**.

To fulfil those requirements we assume that:

- According to the honest-but-curious adversary model [56], all parts involved follow the protocols honestly. As a consequence, we may assume that the scores computed by the client are correct.
- An adversary may have access to one of the servers, but the authentication and DB servers will not collude.

More details on the full protected verification process are described in Sect. VI-B. In addition, a detailed unlinkability and irreversibility analysis based on this security model is provided in Sects. VII-E and VII-F, respectively.

B. ENCRYPTED MULTI-ALGORITHM VERIFICATION PROCESS

Building upon the security model described in Sect. VI-A, the final encrypted verification process comprises ten steps (see Fig. 3):

0) During enrolment, the reference templates **SY** and **GY** are acquired, encrypted using the server public key pk to generate $E(\mathbf{SY})$ and $E(\mathbf{GY})$ (Eq. 1) and finally stored in the database.
1) The client captures the probe sample and extracts the templates **GX** and **SX**.
2) The client sends to the DB server the encrypted ID, $E(\text{ID})$, of the client to request the appropriate reference template $E(\mathbf{FY})$.
3) The DB server sends the encrypted reference templates $E(\mathbf{SY})$ and $E(\mathbf{GY})$ to the client.

4) a. The client computes the global features similarity score, according to Eq. 8, $E(S_{GF})$.
Steps 4b to 7 are related to the iterative encrypted DTW verification algorithm, depicted inside a green box in Fig. 3. In order to obtain the encrypted score, $E(S_{DTW})$, between de probe template, $\mathbf{SX}_{U\times F_s}$, and the encrypted reference, $E\left(\mathbf{SY}_{V\times F_s}\right)$, each value of the encrypted cost matrix $E(\mathbf{Path}[u,v])$ is computed as follows (see Fig. 1 and Sect. V-B):
4) b. The client calculates the encrypted Euclidean distance $E\left(d^2_{euc}(\mathbf{SX}[u],\mathbf{SY}[v])\right)$ according to Eq. 8.
5) If $u, v \neq 1$ (Fig. 1 step 4), the minimum between three values is computed following the two step protocol established above. In this first step, the client generates an encrypted list of values $E(minList)$ and sends it to the server.
6) The server decrypts the list using sk, finds the obscured minimum $minCost + r_{min}$ and re-encrypts it with pk.
7) The server sends the re-encrypted minimum value to the client, setting $E(\mathbf{Path}[u,v]) = E(minCost) = E(minCost + r_{min}) \cdot E(r_{min})^{-1}$.
8) When the iterative process is finished, the client computes the fused score $E(S)$ from $E(S_{DTW}) = E(\mathbf{Path}[U,V])$ and $E(S_{GF})$ (Eq. 10).
9) The client then sends $E(S)$ to the authentication server.
10) The authentication server decrypts the score with sk, obtaining S.
11) In the last step, the authentication server generates and outputs the final binary verification decision: $D = (S > \delta)$.

VII. EXPERIMENTAL EVALUATION

In this section, we analyse whether the proposed protection scheme fulfils the requirements established within the ISO/IEC IS 24745 [19]. To that end, all experiments are carried out on the BiosecurID multimodal database [24], described in Sect. VII-A, and an implementation of an on-line signature based verification system, described in Sect. VII-B. We have analysed the impact of signal sub-sampling on its accuracy in Sect. VII-C1. Then, for the encrypted system we additionally analyse: *i*) accuracy preservation (Sect. VII-C2), *ii*) time and storage complexity preservation (Sect. VII-D), *iii*) irreversibility of the templates (Sect. VII-E), and *iv*) unlinkability of the templates (Sect. VII-F).

A. EXPERIMENTAL ON-LINE SIGNATURE DATABASE

Experiments have been run on the on-line signature subcorpus of the BiosecurID database [24], which comprises data belonging to 400 subjects. Signatures were captured in four sessions over a four month period with a Wacom Intuos3 A4/Inking pen tablet, including four genuine signatures and three skilled forgeries per session and subject. In order to allow comparisons with future studies, the unprotected templates will be made public through the http://atvs.ii.uam.es/databases.jsp website.

In addition, two different scenarios are considered:

- Random forgeries: impostor scores are computed comparing the subject's signature to genuine signatures belonging to other subjects (different from the owner). In other words, an eventual impostor tries to fool the system using his own signature.
- Skilled forgeries: impostor scores are computed comparing the subject's signature to imitations of his own signature made by other subjects, with different skill levels. See the database description for more details [24].

B. UNPROTECTED ON-LINE SIGNATURE VERIFICATION SYSTEM

For fixed-length verification, as proposed in [57], a set of 100 global features x_f is extracted from the x and y coordinates, and the pressure signal, and then normalized to the range $[0, 1]$ using tanh estimators. The best $F_g = 40$ normalized features according to [58] are selected to form the final template $\mathbf{GX}_{40} = \{x_1, \ldots, x_{40}\}$. Then, the Euclidean distance will be used to compute the similarity scores, as it performs better than the Mahalanobis distance proposed in [57].

For the identity verification based on variable-length templates, a subset of $F_s = 9$ time sequences selected using the Sequential Forward Floating Selection (SFFS) algorithm from the total set of functions defined in [57], is directly compared using DTW [10]. Those time sequences include, for instance, the horizontal x and vertical y coordinates, the speed or the pressure.

C. ACCURACY ANALYSIS: UNPROTECTED vs PROTECTED SYSTEM

As pointed out in a [25], the complexity of the DTW scheme depends on the square of the number of samples of the considered signature. Therefore, sub-sampling the signatures will considerably reduce the time needed for verification as well as the storage requirements.

As a consequence, the accuracy analysis has a twofold objective: *i*) assess the impact of sub-sampling (Sect. VII-C1) on the verification accuracy of the DTW based scheme, and *ii*) select the adequate configuration for the final system, which will be implemented in the encrypted domain (Sect. VII-C2. In order to evaluate the accuracy, the first 350 subjects are enrolled and modelled with the four signatures captured in the first session, being the samples of the remaining 50 subjects used for the random forgeries comparisons in order to avoid biased results. More specifically, the first four samples of each subject are used at enrolment. Then, the remaining 12 samples are used to compute the genuine scores ($350 \times 12 = 4,200$ scores). The fifth sample of each of the 50 impostors is compared to the enrolled models for the random impostor score computation ($350 \times 50 = 17,500$ scores). Finally, all 12 skilled forgeries are used for the skilled impostor scores ($350 \times 12 = 4,200$ scores).

TABLE 1. Accuracy analysis of the two sub-sampling approaches, for different sampling rates, in terms of *nSamples* and the EER (in %) for the unimodal unprotected DTW-based scheme and the multi-algorithm approach.

	nSamples	DTW Unprotected		Muti-Algorithm Unprotected	
		EER Rand	EER Skilled	EER Rand	EER Skilled
Baseline	752	**0.86**	**5.38**	0.86	5.36
MaxMin	72	3.99	14.86	2.56	7.50
Rate 1:2	376	1.12	6.90	**1.10**	**6.88**
Rate 1:5	150	1.66	8.96	**1.50**	**6.54**
Rate 1:10	75	3.26	12.31	2.17	6.92
Rate 1:15	50	5.86	15.17	2.53	7.33
Rate 1:20	37	8.47	17.93	3.06	7.45

1) SUB-SAMPLING TECHNIQUES

We will consider in the present article two different approaches for sub-sampling signature sequences:

- Fixed rate: for a given sub-sampling rate *sRate*, one out of each *sRate* samples will be selected (denoted as 1:*sRate*).
- MaxMin: in this case, first the local maxima and minima of each x and y signals will be computed. Then, the corresponding samples in all three input signals (x, y and p) will be retained. Since those are the points in which the signer changes the direction, they should contain the most discriminative information of the signature, thereby providing a minimal loss on verification accuracy.

2) ACCURACY RESULTS

We now evaluate the performance of the aforementioned approaches in terms of the average number of samples of the sub-sampled signatures (*nSamples*) and the verification accuracy of the multi-algorithm based scheme. Details are given in Table 1, where the Equal Error Rate (ERR) of the DTW based system (second and third columns), and for the multi-algorithm system (fourth and fifth columns) are shown for sub-sampling configuration, as well as for the baseline (first row), together with the corresponding average number of samples (*nSamples*, first column).

As it may be observed, the MaxMin sampling strategy offers no clear advantages: whereas *nSamples* is similar to a fixed rate of $sRate = 10$, in both the skilled and random forgeries scenarios MaxMin yields a higher EER (3.99% vs 3.25% and 14.86% vs 12.31%). Consequently, given its higher complexity due to the maxima and minima computation, in the rest of the article we will focus on the fixed rate sampling strategy.

In this latter case, we may observe that, when only the DTW scheme is taken into account, accuracy drops quickly (i.e., the EER increases), specially in the random forgeries scenario for $sRate \geq 10$. Nevertheless, it may observed on the last two columns of Table 1, where the performance of the multi-algorithm scheme is analysed, that the higher *sRate*, the more effective the fusion with the fixed-length scheme is. This is due to the fact that the accuracy of the DTW decreases with *sRate*, but the fixed-length scheme remains the same, since those templates are computed on the original signature, where no sub-sampling has been applied.

In order to grant a low accuracy degradation, in the following subsections we will consider the schemes with $sRate = \{2, 5\}$, which achieve the lowest EERs as highlighted in Table 1.

Taking those remarks into account, we evaluate the accuracy degradation at all operating points. To that end, the Detection Error Trade-off (DET) curves for $sRate = 2$ (left) and $sRate = 5$ (right) are depicted in Fig. 4, both for the random forgeries (solid lines) and the skilled forgeries (dashed lines) scenarios. In both cases, the multi-algorithm based approach (in black) is compared to the original DTW approach (in grey) where no sub-sampling is applied. Since verification accuracy is fully preserved at all operating points, the DET curves of the protected and unprotected systems overlap completely. Therefore, to make the figures easier to read, we have only depicted the protected system DETs.

As it may be observed, accuracy is almost preserved for $sRate = 2$, especially in the random forgeries scenario. In the case of $sRate = 5$, accuracy is more severely degraded. More specifically, the EER raises raises 75% and 22% with respect to the original DTW algorithm for the random and skilled forgeries, respectively. However, the time and storage requirements and verification time are considerable reduced (see Sect. VII-D).

D. COMPLEXITY ANALYSIS: UNPROTECTED vs PROTECTED SYSTEM

The complexity of the proposed approach is analysed and compared to the method presented in [25], in terms of the most costly operations (encryptions, decryptions, exponentiations and products), the storage requirements, the amount of data exchanged between server and client, and the time needed for verification. Results are summarised in Table 2, where experiments have been run on a machine with an Intel Core i7 with four 2.67 GHz cores on Java. Since the complexity of the fixed-length system is negligible with respect to DTW, only the latter will be analysed.

As indicated in [25], the number of encryptions and decryptions carried out depends on the square of *nSamples*.

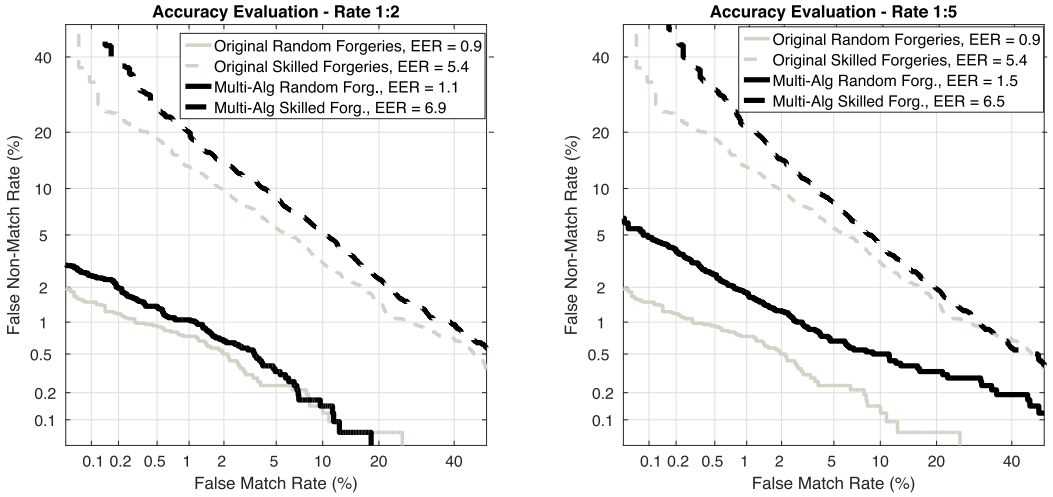


FIGURE 4. Accuracy analysis: DET curves of the original unimodal DTW scheme, with no sub-sampling (grey), and for the proposed multi-algorithm scheme for the corresponding values of *sRate* (black), considering random forgeries (solid) or skilled forgeries (dashed).

TABLE 2. Complexity analysis for the proposed scheme, compared to the unimodal DTW-based schemes presented in [25]. The number of operations is showed for the client/server.

	Protected Multi-Algorithm	Protected DTW [25]	Unprotected DTW
Encryptions	2.3×10^5 / 2.3×10^4	5.6×10^6 / 5.6×10^5	-
Decryptions	0 / 2.7×10^5	0 / 6.8×10^6	-
Exponentiations	4.1×10^5 / 0	1.0×10^7 / 0	-
Products	8.7×10^5 / 0	2.2×10^7 / 0	-
Template size	0.66 MB	3.30 MB	0.01 MB
Exchanged data	36 MB	864 MB	0.01 MB
Verif. Time	0.04 minutes	1 minute	$<$ 0.01 minute

Therefore, for $sRate = 5$, complexity is reduced by 25 times, thereby enabling a much faster comparison of signatures. Additionally, it should be noted that the single comparison of the fixed-length templates can be computed in parallel with the much more costly DTW-based algorithm, hence requiring no additional time. These facts lead to a reduction in the time needed for verification from one minute to approximately three seconds (0.04 minutes).

In a similar manner, the amount of data either exchanged or stored in the reference template are reduced from 864 MB and 3.30 MB in [25], to 36 MB and 0.66 MB, respectively. Compared to the unprotected verification, where only 0.01 MB are stored or exchanged, there is still a big gap. However, current technologies allow a real-time verification for the proposed multi-algorithm approach, at a small cost in terms of verification accuracy (see Fig. 4).

E. IRREVERSIBILITY ANALYSIS: PROTECTED SYSTEM

Unlike the analysis of the accuracy and the complexity, in this case the irreversibility of the *unprotected* system is not studied because, by default, unprotected systems have been proven to be reversible [14]–[16]. That is, in fact, one of the main purposes of developing a protected system: adding irreversibility to the original unprotected system, as requested by the ISO/IEC International Standard 24745 [19].

To grant such irreversibility, and following the security model described in Sect. VI-A, three different pieces of information should be hidden: *i*) only the client can have access to the plain probe biometric data $\mathbf{FX}$, *ii*) the plain reference templates $\mathbf{FY}$ should not be seen by any entity, being only their encrypted version E ($\mathbf{FY}$) stored, and *iii*) the plain score S should not be transmitted as it can potentially be used to perform hill-climbing [59] or inverse-biometrics attacks [15], [16].

For each distance measure considered, the information exchanged from the DB server to the client is the encrypted reference template E ($\mathbf{FY}$). Given that the decisional composite residuosity is an NP-hard problem, decoding the templates without sk could be considered computationally infeasible. Therefore, since only the authentication server knows the decryption key, sk, but he has never access to any protected or unprotected templates, there is no way for the client or any of the servers to learn any information from it. Conversely, the client sends no information about the acquired probe samples $\mathbf{FX}$ to any server. We may thus conclude that the first requirement established by the ISO/IEC 24745 standard, irreversibility, is met.

F. UNLINKABILITY AND RENEWABILITY ANALYSIS: PROTECTED SYSTEM

As in the case of irreversibility, unprotected systems are, by definition, fully linkable and not renewable, which leads to a severe information leakage from the subject's privacy protection perspective. As a consequence, in this section we will only analyse if the protected system is able to add unlinkability and renewability to the original system, as required by the ISO/IEC International Standard 24745 [19].

On the one hand, it should be noted that a different key pair (sk, pk) will be used for each application, and utilised to encrypt all the information within that particular application. Therefore, it will provide the desired *renewability* property: different protected templates can be generated from a single sample using different keys. In addition, should a key pair be compromised, the database can be regenerated by decrypting and re-encrypting all templates with a new key pair $\left(sk', pk'\right)$.

Regarding *unlinkability*, from a theoretic perspective, since unencrypted distances (i.e., similarity scores) between plaintexts are not preserved in the encrypted domain, given two samples $\mathbf{M}_1$ and $\mathbf{M}_2$ belonging to a given subject, their corresponding protected templates $E\left(\mathbf{FX}^1\right)$ and $E\left(\mathbf{FX}^2\right)$, encrypted with the same key at different times (due to the probabilistic nature of Paillier cryptosystem) or different keys, are not related. On the other hand, since the Paillier cryptosystem provides semantic security against chosen-plaintext attacks [60], given a protected template $E\left(\mathbf{FX}^1\right)$, no information can be feasibly derived about the original unprotected features $\mathbf{FX}^1$. That way, no comparison can be established in the unprotected domain between some kind of information retrieved from the protected templates.

In addition, only the encrypted ID, $E\left(\mathrm{ID}\right)$, is shared between the client and DB server. Such encrypted ID will have a different value at each attempt due to the probabilistic nature of the Paillier cryptosystem (see Eq. 1). As a consequence, an eventual eavesdropper will not be able to track the verification attempts of a single client.

In addition to that theoretical analysis, an experimental evaluation of the unlinkability of the templates is carried out, following the unlinkability analysis framework proposed in [23]. In the following we summarise this evaluation protocol, and we referer the reader to [23] for more details on the computations.

Two templates, $E\left(\mathbf{FX}\right)$ and $E\left(\mathbf{FY}\right)$, enrolled in different applications (and eventually protected with different keys), are defined as linkable if an eventual attacker can determine whether they were extracted from mated instances, and hence conceal a unique identity. Therefore, an eventual attacker launching a cross-matching attack to take advantage of this particular vulnerability of the BTP scheme can be assumed to:

- be in possession of two protected templates, $E\left(\mathbf{FX}\right)$ and $E\left(\mathbf{FY}\right)$, enrolled in different applications,
- following Kerckhoffs's principle [61], know how the system works and, in particular, the *Mated instances* and *Non-mated instances* score distributions.

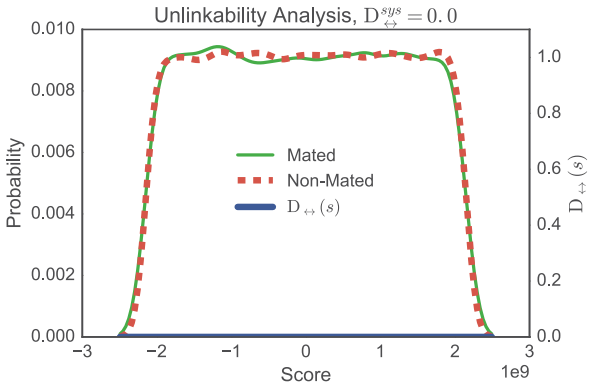


FIGURE 5. Unlinkability analysis: scores distributions for comparisons belonging to *Mated instances* (green) or to *Non-mated instances* (red). $D_{\leftrightarrow}(s)$ (blue) represents the local linkability measure.

To reach his goal of determining whether both protected templates, $E\left(\mathbf{FX}\right)$ and $E\left(\mathbf{FY}\right)$, conceal the same biometric instance (i.e., they represent different samples of biometric data extracted from the same biometric instance - e.g., the same left index finger), he computes a dissimilarity score between them, $s = DS\left(E\left(\mathbf{FX}\right), E\left(\mathbf{FY}\right)\right)$. This function will be defined by the attacker ad-hoc in order to compromise the unlinkability of the system (i.e., it can be the dissimilarity score of the system or any other more sophisticated function to compare the templates and link them). Then, given s, he will decided whether or not it stems from a mated instances comparison: if it does, the attack will have succeeded. On the other hand, if such a positive decision (i.e., both templates come from the same instance) cannot be made based on the computed s, the attacker will have failed in his goal.

As a consequence, in order to evaluate the unlinkabiliy of the templates, the corresponding *Mated instances* (in green, and stemming from similarity scores between samples of the same instance protected with different keys) and *Non-mated instances* (in red, and stemming from similarity scores between samples of different instances protected with different keys) score distributions are depicted in Fig. 5. Those distributions are quantitatively compared in terms of two different measures:

- Local measure $D_{\leftrightarrow}(s)$: it evaluates the linkability of the templates in a score-wise basis. If for a specific score s_1, a system yields $D_{\leftrightarrow}(s_1) = 1$, it means that, *in case* a cross-matching attack produced s_1, the attacker would be able to link both templates $E\left(\mathbf{FX}\right)$ and $E\left(\mathbf{FY}\right)$ to the same instance with almost all certainty. On the other hand, $D_{\leftrightarrow}(s_0) = 0$ should be interpreted as full unlinkability for that particular score s_0. All intermediate values of $D_{\leftrightarrow}(s)$ between 0 and 1 report an increasing degree of linkability.
- Global measure $D_{\leftrightarrow}^{sys}$: it gives an overall measure of the linkability of the whole system, independent of the score domain of the system at hand, thereby allowing a comparison among different systems. This way, if a system has $D_{\leftrightarrow}^{sys} = 1$ (i.e., case in which both the *Mated*

samples and *Non-mated samples* distributions have no overlap), it means that it is fully linkable for all the scores of the *Mated samples* distribution domain (i.e., where $D_{\leftrightarrow}(s) = 1$). Similarly, $\mathrm{D}_{\leftrightarrow}^{sys} = 0$ means that the system is fully unlinkable for the whole score domain, since both distributions overlap for the whole domain of scores. All intermediate values of $\mathrm{D}_{\leftrightarrow}^{sys}$ between 0 and 1 report a decreasing degree of unlinkability (i.e., increasing degree of linkability).

In order to compute such metrics, we need to take into account the key on the success of a cross-matching attack: determining whether, given a score s, it is more likely that two templates stem from mated samples, $p(H_m|s)$, than from non-mated samples, $p(H_{nm}|s)$. Therefore, such linkability can be accounted for in terms of the difference of conditional probabilities of each hypothesis H_m and H_{nm} for a given score s:

$$D_{\leftrightarrow}(s) = p(H_m|s) - p(H_{nm}|s) \tag{11}$$

However, these two conditional probabilities are unknown. What can be computed a priori, and is known for each system, are the *Mated* and *Non-mated samples* distributions (i.e., $p(s|H_m)$ and $p(s|H_{mn})$), that is, the probability of observing s knowing that two templates belong to mated samples or to non-mated samples. We can therefore compute Eq. 11 in terms of the likelihood ratio between these probabilities.

For the global linkability measure, $\mathrm{D}_{\leftrightarrow}^{sys}$, we are interested in measuring how likely it is to get a score stemming from the *Mated samples* distribution. This can be achieved computing the difference $p(H_m \cap s) - p(H_{nm} \cap s)$ and integrating it over the whole score domain. However, regarding the success of cross-matching attacks, we are only interested in the probabilities stemming from the *Mated samples* distribution. In addition, as in the definition of the local linkability measure $\mathrm{D}_{\leftrightarrow}(s)$, a cross-matching attack will only be successful if $p(H_m|s) > p(H_{nm}|s)$. We can hence define $\mathrm{D}_{\leftrightarrow}^{sys}$ as:

$$\mathrm{D}_{\leftrightarrow}^{sys} = \int_{s_{min}}^{s_{max}} p(s|H_m) \cdot \mathrm{D}_{\leftrightarrow}(s)\, \mathrm{d}s \tag{12}$$

We have depicted in Fig. 5 the local linkability measure $D_{\leftrightarrow}(s)$ in blue. As it may be observed, both *mated* (green) and *non-mated* (red) score distributions overlap completely, thereby preventing the success of a cross-matching attack: given a particular score s, the eventual attacker cannot determine whether the corresponding templates conceal the same identity. As a consequence, the local linkability measure $\mathrm{D}_{\leftrightarrow}(s) = 0$ for all s, which in turn this leads to a global linkability value of $\mathrm{D}_{\leftrightarrow}^{sys} = 0$. We may therefore conclude that the encrypted templates are fully unlinkable.

VIII. CONCLUSIONS

We have proposed a time-efficient, secure and privacy-preserving comparison scheme based on Homomorphic Encryption through combination of fixed-length and sub-sampled variable-length descriptors. As a case study, we have applied the proposed general approach to an on-line signature based biometric system, achieving a high accuracy, almost comparable to that of state-of-the-art unprotected schemes, at the cost of a reasonably low computational overhead.

A theoretical and empirical analysis of the irreversibility and unlinkability of the protected templates has been carried out. The results show that all requirements established within the ISO/IEC IS 24745 [19] are met. Furthermore, protected templates are compressed to 20% of the original size and the amount of exchanged data is reduced to less than 5% with respect to the original approach [25]. Consequently, verification in real-time applications is allowed, solving most of the practical implementation issues detected in the original approach described in [25].

It should be also noted that, even if only a subsampling value of 1:5 has been analysed in the case of the protected system, higher rates can be considered to further reduce verification time, at the cost of some accuracy degradation (as it has been seen in the case of the unprotected system). In future works, we will study how to further improve verification accuracy using subject-specific thresholds [63] or quality measures [64].

Finally, regarding the overall security and privacy protection offered by biometric systems, the reader should bear in mind that these systems are vulnerable to external attacks carried out by malicious adversaries, as first stated by Ratha *et al.*. Biometric template protection technologies such as the one proposed in this article are not enough to tackle all vulnerabilities: additional countermeasures need to be applied. For instance, Presentation Attacks (PA) refer to the use of synthetic artifacts or the alteration of someone's real biometric charateristics with the goal of either impersonating another subject or avoid being recognised, according to the ISO/IEC IS 30107 on Presentation Attack Detection (PAD). These attacks can be prevented by the addition of PAD techniques. Furthermore, internal modules of the system (e.g., feature extractor or comparator) can be overriden with Trojan horses such that they always output the values desired by the adversary. These attacks can be counterfeited with secure code execution practices. Similarly, an adversary can intercept and modify the data being transferred between such internal modules. A countermeasure for this attack is to use time-stamps or a challenge/response mechanism.

In this context, note that we defined an informal security model in Sect. VI-A to analyse some of the benefits of the proposed methods (e.g., eavesdroppers will obtain no information about the original biometric data and subject's activities cannot be tracked). As future work we foresee the application of more comprehensive security models [56] to the proposed approach for privacy-preserving comparison of variable-length data.

REFERENCES

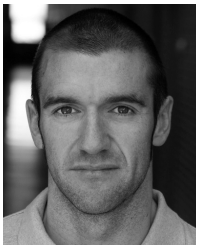
[1] I. A. T. Hashem, I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. U. Khan, "The rise of 'big data' on cloud computing: Review and open research issues," *Inf. Syst.*, vol. 47, pp. 98–115, Jan. 2015.

[2] X. Wu, X. Zhu, G.-Q. Wu, and W. Ding, "Data mining with big data," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 1, pp. 97–107, Jan. 2014.

[3] R. Agrawal and R. Srikant, "Privacy-preserving data mining," in *Proc. ACM SIGMOD Rec.*, vol. 29. 2000, pp. 439–450.
[4] Y. Lindell and B. Pinkas, "Privacy preserving data mining," *J. Cryptol.*, vol. 15, no. 3, pp. 177–206, Jun. 2002.
[5] M. Naveed *et al.*, "Privacy in the genomic era," *ACM Comput. Surv.*, vol. 48, no. 1, pp. 1–44, 2015.
[6] R. Finn and A. Donovan, *The Future Drone Use*. New York, NY, USA: Springer, 2016, pp. 47–67.
[7] C. Aguilar-Melchor, S. Fau, C. Fontaine, G. Gogniat, and R. Sirdey, "Recent advances in homomorphic encryption: A possible future for signal processing in the encrypted domain," *IEEE Signal Process. Mag.*, vol. 30, no. 2, pp. 108–117, Mar. 2013.
[8] X. Yi, R. Paulet, and E. Bertino, *Homomorphic Encryption and Applications*. New York, NY, USA: Springer, 2014.
[9] J. R. Troncoso-Pastoriza and F. Perez-Gonzalez, "Secure signal processing in the cloud: Enabling technologies for privacy-preserving multimedia cloud processing," *IEEE Signal Process. Mag.*, vol. 30, no. 2, pp. 29–41, Mar. 2013.
[10] A. Kholmatov and B. Yanikoglu, "Identity authentication using improved online signature verification method," *Pattern Recognit. Lett.*, vol. 26, no. 15, pp. 2400–2408, 2005.
[11] H. Zhu, X. Meng, and G. Kollios, "Privacy preserving similarity evaluation of time series data," in *Proc. Int. Conf. Extending Database Technol. (EDBT)*, 2014, pp. 499–510.
[12] A. K. Jain, "Biometric recognition," *Nature*, vol. 449, no. 7158 pp. 38–40, 2007.
[13] J. Galbally *et al.*, "An evaluation of direct attacks using fake fingers generated from ISO templates," *Pattern Recognit. Lett.*, vol. 31, pp. 725–732, Jun. 2010.
[14] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 9, pp. 1489–1503, Sep. 2007.
[15] J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez, and J. Ortega-Garcia, "Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms," *Comput. Vis. Image Understand.*, vol. 117, no. 10, pp. 1512–1525, 2013.
[16] M. Gomez-Barrero, J. Galbally, A. Morales, M. A. Ferrer, J. Fierrez, and J. Ortega-Garcia, "A novel hand reconstruction approach and its application to vulnerability assessment," *Inf. Sci.*, vol. 268, pp. 103–121, Jun. 2014.
[17] A. Hadid, N. Evans, S. Marcel, and J. Fierrez, "Biometrics systems under spoofing attack: An evaluation methodology and lessons learned," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 20–30, Sep. 2015.
[18] *EU Regulation 2016/679 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, Eur. Parliament, Brussels, Belgium, 2016.
[19] *ISO/IEC JTC1 SC27 Security Techniques, ISO/IEC 24745:2011. Information Technology—Security Techniques—Biometric Information Protection*, Int. Org. Standardization, Geneva, Switzerland, 2011.
[20] S. Ye, Y. Luo, J. Zhao, S.-Ching, and S. Cheung, "Anonymous biometric access control," *EURASIP J. Inf. Sec.*, vol. 2009, no. 1, pp. 1–17, Nov. 2009.
[21] M. Barni *et al.*, "A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates," in *Proc. Int. Conf. Biometrics, Theory Appl. Syst. (BTAS)*, 2010, pp. 1–7.
[22] J. Bringer, H. Chabanne, and A. Patey, "Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends," *IEEE Signal Process. Mag.*, vol. 30, no. 2, pp. 42–52, Mar. 2013.
[23] M. Gomez-Barrero, C. Rathgeb, J. Galbally, C. Busch, and J. Fierrez, "Unlinkable and irreversible biometric template protection based on bloom filters," *Inf. Sci.*, vols. 370–371, pp. 18–32, Nov. 2016.
[24] J. Fierrez *et al.*, "BiosecurID: A multimodal biometric database," *Pattern Anal. Appl.*, vol. 13, pp. 235–246, May 2010.
[25] M. Gomez-Barrero, J. Galbally, and J. Fierrez, "Variable-length template protection based on homomorphic encryption with application to signature biometrics," in *Proc. Int. Workshop Biometrics Forensics (IWBF)*, Mar. 2016, pp. 1–6.
[26] M. Gomez-Barrero, J. Galbally, E. Maiorana, P. Campisi, and J. Fierrez, "Implementation of fixed-length template protection based on homomorphic encryption with application to signature biometrics," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2016, pp. 259–266.
[27] K. Simoens *et al.*, "Criteria towards metrics for benchmarking template protection algorithms," in *Proc. Int. Conf. Biometrics*, 2012, pp. 498–505.
[28] P. Tuyls, B. Skoric, and T. Kevenaar, Eds., "Security with noisy data," in *On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*. New York, NY, USA: Springer, 2007.
[29] P. Campisi, Ed., *Security Privacy Biometrics*. Springer, 2013.
[30] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP J. Inf. Sec.*, vol. 3, pp. 1–25, Dec. 2011.
[31] 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.
[32] P. Campisi, E. Maiorana, J. Fierrez, J. Ortega-Garcia, and A. Neri, "Cancelable templates for sequence-based biometrics with application to on-line signature recognition," *IEEE Trans. Syst., Man Cybern., A, Syst. Humans*, vol. 40, no. 3, pp. 525–538, May 2010.
[33] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia, and A. Neri, "Template protection for HMM-based on-line signature authentication," in *Proc. IEEE Comput. Soc. Workshop Biometrics*, Jun. 2008, pp. 1–6.
[34] A. Kholmatov and B. Yanikoglu, "Biometric cryptosystem using online signatures," in *Proc. Int. Symp. Comput. Inf. Sci.*, 2006, pp. 981–990.
[35] E. A. Rua, E. Maiorana, J. L. A. Castro, and P. Campisi, "Biometric template protection using universal background models: An application to online signature," *IEEE Trans. Inf. Forensics Sec.*, vol. 7, no. 1, pp. 269–282, Feb. 2012.
[36] M. R. Freire, J. Fierrez, J. Galbally, and J. Ortega-Garcia, "Biometric hashing based on genetic selection and its application to on-line signatures," in *Proc. Int. Conf. Biometrics*, 2007, pp. 1134–1143.
[37] M. R. Freire, J. Fierrez, and J. Ortega-Garcia, "Dynamic signature verification with template protection using helper data," in *Proc. Int. Conf. Acoust., Speech Signal Process., ICASSP*, 2008, pp. 1713–1716.
[38] T. Ignatenko and F. M. J. Willems, "Biometric systems: Privacy and secrecy aspects," *IEEE Trans. Inf. Forensics Sec.*, vol. 4, no. 4, pp. 956–973, Dec. 2009.
[39] T. Ignatenko and F. M. J. Willems, "Information leakage in fuzzy commitment schemes," *IEEE Trans. Inf. Forensics Sec.*, vol. 2, no. 5, pp. 337–348, Jun. 2010.
[40] C. Rathgeb and A. Uhl, "Statistical attack against fuzzy commitment scheme," *IET Biometrics*, vol. 1, no. 2, pp. 94–104, Jun. 2012.
[41] R. L. Lagendijk, Z. Erkin, 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.
[42] A. C.-C. Yao, "How to generate and exchange secrets," in *Proc. Annu. Symp. Found. Comput. Sci.*, 1986, pp. 162–167.
[43] C. Fontaine and F. Galand, "A survey of homomorphic encryption for nonspecialists," *EURASIP J. Inf. Sec.*, vol. 2007, no. 1, pp. 1–15, Dec. 2007.
[44] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. EUROCRYPT*, 1999, pp. 223–238.
[45] T. Bianchi, S. Turchi, A. Piva, R. D. Labati, V. Piuri, and F. Scotti, "Implementing fingercode-based identity matching in the encrypted domain," in *Proc. Workshop Biometric Meas. Syst. Sec. Med. Appl.*, 2010, pp. 15–21.
[46] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, "Privacy-preserving face recognition," in *Proc. Int. Symp. Privacy Enhancing Technol. Symp.*, 2009, pp. 235–253.
[47] A.-R. Sadeghi, T. Schneider, and I. Wehrenberg, "Efficient privacy-preserving face recognition," in *Proc. Int. Conf. Inf., Sec. Cryptol.*, 2010, pp. 229–244.
[48] M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich, "SCiFI—A system for secure face identification," in *Proc. IEEE Symp. Sec. Privacy*, May 2010, pp. 239–254.
[49] M. Blanton and P. Gasti, "Secure and efficient protocols for iris and fingerprint identification," in *Proc. Eur. Symp. Res. Comp. Sec.*, 2011, pp. 190–209.
[50] J. Bringer, H. Chabanne, M. Favre, A. Patey, T. Schneider, and M. Zohner, "GSHADE: Faster privacy-preserving distance computation and biometric identification," in *Proc. ACM Workshop Inf. Hiding Multimedia Sec.*, 2014, pp. 187–198.
[51] E. Maiorana, D. L. Rocca, and P. Campisi, "Cognitive biometric cryptosystems a case study on eeg," in *Proc. Int. Conf. Syst., Signals Image Process.*, Sep. 2015, pp. 125–128.
[52] M. Martinez-Diaz, J. Fierrez, M. R. Freire, and J. Ortega-Garcia, "On the effects of sampling rate and interpolation in hmm-based dynamic signature verification," in *Proc. Int. Conf. Doc. Anal. Recognit.*, vol. 2. Sep. 2007, pp. 1113–1117.

[53] N. Poh and J. Kittler, "A unified framework for biometric expert fusion incorporating quality measures," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 34, no. 1, pp. 3–18, Jan. 2012.
[54] M. Barni, G. Droandi, and R. Lazzeretti, "Privacy protection in biometric-based recognition systems: A marriage between cryptography and signal processing," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 66–76, Sep. 2015.
[55] K. Simoens, J. Bringer, H. Chabanne, and S. Seys, "A framework for analyzing template security and privacy in biometric authentication systems," *IEEE Trans. Inf. Forensics Sec.*, vol. 7, no. 2, pp. 833–841, Apr. 2012.
[56] O. Goldreich, *The Foundations of Cryptography*, vol. 2. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[57] M. Martinez-Diaz, J. Fierrez, R. P. Krish, and J. Galbally, "Mobile signature verification: Feature robustness and performance comparison," *IET Biometrics*, vol. 3, no. 4, pp. 267–277, 2014.
[58] J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Performance and robustness: A trade-off in dynamic signature verification," in *Proc. Int. Conf. Acoust., Speech Signal Process., ICCASP*, 2008, pp. 1697–1700.
[59] M. Gomez-Barrero, J. Galbally, and J. Fierrez, "Efficient software attack to multimodal biometric systems and its application to face and iris fusion," *Pattern Recognit. Lett.*, vol. 36, pp. 243–253, Jan. 2014.
[60] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Hoboken, NJ, USA: Wiley, 2001.
[61] A. Kerckhoffs, "La cryptographie militaire," *J. Des Sci. Militaires*, vol. 9, pp. 5–83, Jun. 1883, available on-line at. [Online]. Available: http://www.petitcolas.net/fabien/kerckhoffs/#english
[62] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch, "General framework to evaluate unlinkability in biometric template protection systems," *IEEE Trans. Inf. Forensics Sec.*, to be published.
[63] J. Fierrez, D. Garcia-Romero, J. Ortega-Garcia, and J. Gonzalez-Rodriguez, "Adapted user-dependent multimodal biometric authentication exploiting general information," *Pattern Recognit. Lett.*, vol. 26, no. 16, pp. 2628–2639, 2005.
[64] F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "Quality measures in biometric systems," *IEEE Sec. Privacy*, vol. 10, no. 9, pp. 52–62, Dec. 2012.

MARTA GOMEZ-BARRERO received the M.Sc. degrees in computer science and mathematics, and the Ph.D. degree in electrical engineering from the Universidad Autonoma de Madrid, in 2011 and 2016, respectively. Since 2016, she has been a Post-Doctoral Researcher with the Center for Research in Security and Privacy, Germany. She has carried out research internships with several worldwide leading groups in biometric recognition, such as the Norwegian Biometrics Laboratory, part of the NISlab-Norwegian Information Security Laboratory; NTNU i Gjøvik; and the COMLAB, Università degli Studi Roma Tre, Italy. Her current research focuses on the development of privacy-enhancing biometric technologies and presentation attack detection methods within the wider fields of pattern recognition and machine learning. She has been actively involved in European projects focused on vulnerability assessment of biometrics including EU FP7 Tabula Rasa and EU FP7 BEAT. She was a recipient of a number of distinctions, including the 2015 EAB European Biometric Industry Award, the Siew-Sngiem Best Paper Award from ICB 2015, the Archimedes Award for Young Researches from the Spanish Ministry of Education in 2013, and the Best Poster Award from ICB 2013.



JAVIER GALBALLY received the M.Sc. degree in electrical engineering from the Universidad de Cantabria, Santander, Spain, in 2005, and the Ph.D. degree in electrical engineering from the Universidad Autónoma de Madrid, Madrid, Spain, in 2009. He was an Assistant Professor at the Universidad Autónoma de Madrid until 2012. In 2013, he joined the European Commission DG Joint Research Center, where he is currently a Post-Doctoral Researcher. He has carried out different research internships with worldwide leading groups in biometric recognition, such as BioLab, Universitá di Bologna, Italy; the IDIAP Research Institute, Switzerland; the Scribens Laboratory, École Polytechnique de Montréal, Canada; and the Integrated Pattern Recognition and Biometrics Laboratory, West Virginia University, USA. His research interests are mainly focused on the security evaluation of biometric systems, pattern and biometric recognition, synthetic generation of biometric traits, and inverse biometrics. He is actively involved in European projects focused on biometrics. He was a recipient of a number of distinctions, including the IBM Best Student Paper Award from ICPR 2008, was a finalist for the 2009 EBF European Biometric Research Award, the Best Ph.D. Thesis Award from the Universidad Autónoma de Madrid in 010, the Best Poster Award from ICB 2013, and the Best Paper Award from ICB 2015.

AYTHAMI MORALES received the M.Sc. degree in telecommunication engineering and the Ph.D. degree from the Universidad de Las Palmas de Gran Canaria, in 2006 and 2011, respectively. He was involved in research stays with the Biometric Research Laboratory, Michigan State University; the Biometric Research Center, Hong Kong Polytechnic University; and the Biometric System Laboratory, University of Bologna. He is currently involved in research with the ATVS-Biometric Recognition Group, Universidad Autonoma de Madrid. He has authored over 60 scientific articles published in international journals and conferences. He has participated in seven National and European projects in collaboration with other universities and private entities; such as UAM, UPM, EUPMt, Indra, Union Fenosa, and Soluziona. His research interests are focused on pattern recognition, computer vision, machine learning, and biometrics signal processing. He has received awards from ULPGC, La Caja de Canarias, SPEGC, and COIT.

JULIAN FIERREZ received the M.Sc. and Ph.D. degrees in telecommunications engineering from the Universidad Politecnica de Madrid, Spain, in 2001 and 2006, respectively. From 2007 to 2009, he was a Visiting Researcher at Michigan State University, USA, under a Marie Curie Fellowship. Since 2002, he has been with the ATVS-Biometric Recognition Group, Universidad Politecnica de Madrid, and since 2004, with the ATVS-Biometric Recognition Group, Universidad Autonoma de Madrid, where he is currently an Associate Professor. His research interests include general signal and image processing, pattern recognition, and biometrics with emphasis on signature and fingerprint verification, multi-biometrics, biometric databases, system security, and forensic applications of biometrics. He has been actively involved in multiple EU projects focused on biometrics, such as TABULA, RASA, and BEAT, and has attracted notable impact for his research. He was a recipient of a number of distinctions, including the 2006 EBF European Biometric Industry Award, the 2012 EURASIP Best Ph.D. Award, the Medal in the Young Researcher Awards in 2015 from the Spanish Royal Academy of Engineering, and the Miguel Catalan Award to the Best Researcher under 40 in the Community of Madrid in the general area of science and technology.