Implementation of Fixed-Length Template Protection Based on Homomorphic Encryption with Application to Signature Biometrics

Marta Gomez-Barrero, Julian Fierrez
ATVS - Biometrics Recognition Group
Universidad Autonoma de Madrid
{marta.barrero,julian.fierrez}@uam.es

Javier Galbally
European Commission - Joint Research Centre
Inst. for the Protection and Security of the Citizen
javier.galbally@jrc.ec.europa.eu

Emanuele Maiorana, Patrizio Campisi
Dipartimento di Elettronica Applicata
Universita degli Studi Roma Tre
{emanuele.maiorana,patrizio.campisi}@uniroma3.it

Abstract

Given the high sensitivity of biometric data, any information leakage poses severe security and privacy risks. This fact raises the need to protect biometric templates so that no information can be learned from them, preserving at the same time the unprotected system's performance and speed. We propose a new efficient biometric template protection scheme based on homomorphic probabilistic encryption for fixed-length templates, where only encrypted data is handled. Under a fully reproducible experimental framework, we analyse different distance measures for the particular case of on-line signature, showing that all requirements described in the ISO/IEC 24745 standard on biometric information protection are met with no performance degradation and at a low computational cost. Furthermore, the proposed approach is robust to hill-climbing and inverse-biometrics attacks.

1. Introduction

With the wide deployment of biometric verification systems in the last few years, some concerns regarding users' privacy have been raised: any leakage of biometric information can lead to the disclosure of very sensitive information, like medical conditions, or identity theft. As a consequence, biometric templates need to be protected, fulfilling three main requirements in accordance with the ISO/IEC IS 24745 standard on biometric information protection [21]: *i*) irreversibility (i.e., no biometric information should be leaked by the template), *ii*) unlinkability (i.e., given two templates protected with different keys, it should not be feasible to decide whether they belong to the same subject) and *iii*) renewability (i.e., if one template is lost or stolen, a new one, not matching the old template, should be issued). At the same time, verification performance of encrypted templates should be maintained with respect to the case of unprotected data [31].

Among the different biometric characteristics used in automatic verification systems, handwritten signature is one of the most widely legally and socially accepted [10]. A research line for on-line signature template protection has been developed based on obscuring the extracted features with some irreversible transformation, which results in some performance degradation. This is the case, for instance, of BioConvolving [8], where HMMs (Hidden Markov Models) are trained with irreversibly transformed time sequences.

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. For instance, [24] proposes a fuzzy vault system based on minutiae extracted from on-line signatures. For fixed-length templates, the fuzzy commitment paradigm was applied in [1] to a dynamic signature recognition system based on UBM-HMM (Universal Background Model-HMM), achieving a remarkable verification accuracy. Similarly, [12] presents a biometric cryptosystem based on hashes, and a BCH error correcting code and helper data were used in the scheme described in [13]. The main drawback of these methods is that they use *Auxiliary Data* (AD) [27], which can be exploited in order to obtain information about the hidden biometric data, thus violating the privacy of the subject [19, 20].

Unlike the previous approaches, Homomorphic Encryption schemes require no AD and allow for computations to be performed on ciphertexts, which generate encrypted results whose corresponding plaintexts match the results of the operations carried out on the original plaintext [3, 11, 23]. Semi Homomorphic Encryption (HE) schemes, which only allow a limited subset of operations on the encrypted domain, are nowadays being introduced into many applications based on signal processing, and, particularly, biometrics [2, 5, 6, 7, 29, 33].

In particular, a novel biometric identification scheme based on HE and k-Anonymous Quantization is presented in [33] and tested on an iris database. In [2], the authors propose a new scheme based on a fixed-length representation of fingerprints and HE. An improved version of that approach is suggested in [4], where a more compact implementation using quantization is proposed at a small cost in terms of verification accuracy. More recently, [6] proposes an efficient implementation, known as GSHADE, of several metrics, including the scalar product, the Hamming, Euclidean and Mahalanobis distances. Using oblivious transfers, both the computation time and the bandwidth requirements are improved by a least one order of magnitude with respect to the algorithms proposed in previous works [5, 29]. Finally, a different approach, in which all computations are carried out on the server side, with no interaction with the client, is proposed in [32].

In this paper, we propose, implement and evaluate a new biometric template protection scheme based on Homomorphic Encryption and fixed-length templates, providing fast verification and fulfilling the requirements established in the ISO/IEC IS 24745. We present the implementation in the encrypted domain of two different distance measures, namely: *i*) Euclidean distance, and *ii*) Cosine similarity, defining which information should be stored in the database in each case. For the particular application to on-line signature, we have considered a global features based approach. We then analyse and compare the protected and unprotected systems in terms of verification performance and computational complexity. The irreversibility and unlinkability of the proposed scheme are also analysed. Experiments are carried out on a reproducible research framework: the publicly available BioSecure Multimodal database [28] and an open-source implementation of the Paillier cryptosystem[1].

The rest of the article is organized as follows: the baseline unprotected on-line signature verification system is described in Sect. 2, and the new system is presented in Sect. 3. Verification performance is evaluated in Sect. 4, while irreversibility and unlinkability are analysed in Sect. 5. Then computational complexity is studied in Sect. 6 and final conclusions drawn in Sect. 7.

2. Unencrypted On-Line Signature Verification System

For the identity verification based on dynamic signatures, a state-of-the-art approach based on global features has been chosen [26]. 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 [22]. The best 40 normalized features according to [14] are selected to form the final template $\mathbf{X} = \{x_1, \ldots, x_{40}\}$.

Although in the original system similarity scores between the probe template $\mathbf{X}$ and the claimed identity $\mathbf{Y}$ were computed using the Mahalanobis distance, it showed a poor performance when compared to other distances. As a consequence, in this article we consider two measures (i.e., Euclidean and Cosine), which achieved an optimum performance and whose particular implementations in the encrypted domain are described in Sect. 3.2.

3. Encrypted On-Line Signature Verification System Based on HE

In the rest of the paper, we will use the following notation:

- $\mathbf{X} = \{x_1, \ldots, x_f, \ldots, x_F\}$ denotes the template, comprising F features.

- $S_{dist} = d_{dist}(\mathbf{X}, \mathbf{Y})$ denotes the similarity score of two templates $\mathbf{X}$ and $\mathbf{Y}$, where d_{dist} is the distance measure and the suffix $dist = \{euc, cos\}$ indicates the particular measure (see Sect. 3.2).

- m denotes a plain message and m^* its corresponding ciphertext, with $m^* = E_{pk}(m, s)$, where E denotes the Encryption function, s a random number

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

and pk the public key. Similarly, $m = D_{sk}(m^*)$, where sk is the private or secret key and D the Decryption function.

The proposed system is based on the combination of the on-line signature verification scheme based on global features described in Sect. 2, and Homomorphic Encryption.

3.1. Homomorphic Encryption

In an honest-but-curious adversary model [15], where both parties, client and server, follow the established protocols but may try to learn additional information about the other side template, the server must process the client's biometric data without extracting any information from it, and at the same time, the server must protect the information stored in the database [3]. To achieve this, the Paillier homomorphic probabilistic encryption scheme [30] is used, which 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, two separate keys are required: *i*) a public key pk for encryption, and *ii*) a secret key sk for decryption. In the Paillier cryptosystem, the public key is defined as $pk = (n, g)$, where $n = p \cdot q$ with p and q two large prime numbers such that $\gcd(pq, (p-1)(q-1)) = 1$, and $g \in \mathbb{Z}^*_{n^2}$. On the other hand, the secret key is defined as $sk = (\lambda, \mu)$, 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:

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

where $s \in \mathbb{Z}^*_n$ is a random number providing the probabilistic nature of the cryptosystem, necessary to grant semantic security against chosen-plaintext attacks [16]. In particular, different ciphertexts are obtained when the same plaintext is encrypted several times using the same public key: $E_{pk}(m, s_1) \neq E_{pk}(m, s_2)$. This randomness provides the required unlinkability to the protected templates: even if the exact same unprotected features are extracted from a particular biometric sample, the encrypted templates would be different.

It is shown in [30] that E is a one-way function (i.e., irreversible) if and only if the decisional composite residuosity assumption holds. Therefore, a computationally-bound attacker in possession of an encrypted message m^* (a protected biometric template) and the public key pk would not be able to extract any information about the plaintext m (biometric information). He could only do so if he obtained the secret key sk and decrypted the ciphertext m^* as follows

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

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

Finally, two properties of the Paillier cryptosystem will be used in the present scheme. On the one hand, the product of two ciphertexts, m_1^* and m_2^*, decrypts to the sum of their corresponding plaintexts:

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

On the other hand, an encrypted plaintext, m^*, raised to a constant l, decrypts to the product of the plaintext and the constant:

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

As a consequence, while an unlimited number of summations can be carried out in the encrypted domain, not all products can be computed - as it is shown in Eq. 4, one of the factors must be known to the party computing the product. As a consequence, it is not possible to perform a product between two encrypted values. This fact poses a severe challenge for the implementation of many similarity measures.

In the remainder of the article, to avoid overcomplicated notation, the keys pk and sk, as well as the random number s, will not be specified even if they are necessary to encrypt and decrypt messages. This way, an encrypted message will be denoted simply by $E(m)$.

3.2. Distances in the Encrypted Domain

Since HE works on integers, we should transform the real-valued features x_f in the range $[0, 1]$ to integer values in a bigger range, in our experiments $[0, 10^3]$: $X \rightarrow round\left(10^3\ X\right)$. Furthermore, since computing square roots in the encrypted domain is not straightforward, the square Euclidean measure will be used.

It should finally be noted that, in order to minimize the number of encryptions at verification time, a different encrypted reference template $E(\mathbf{Y})_{dist}$ will be defined for each distance measure, comprising all the necessary encrypted information.

3.2.1 Euclidean Distance

Given two templates $\mathbf{X}$ and $\mathbf{Y}$, the square Euclidean distance between them $d^2_{euc}(\mathbf{X}, \mathbf{Y})$ is defined as:

$$d^2_{euc}(\mathbf{X}, \mathbf{Y}) = \sum_{f=1}^{F} x_f^2 + \sum_{f=1}^{F} y_f^2 - 2\sum_{f=1}^{F} x_f y_f \qquad (5)$$

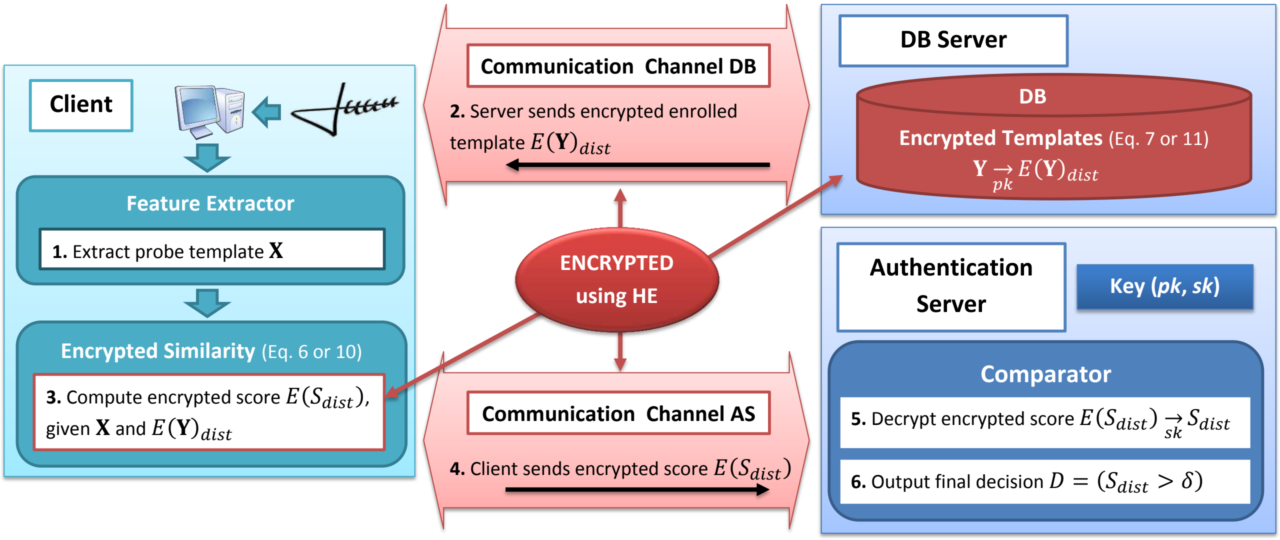
Client
Feature Extractor
1. Extract probe template $\mathbf{X}$
Encrypted Similarity (Eq. 6 or 10)
3. Compute encrypted score $E(S_{dist})$, given $\mathbf{X}$ and $E(\mathbf{Y})_{dist}$
Communication Channel DB
2. Server sends encrypted enrolled template $E(\mathbf{Y})_{dist}$
ENCRYPTED using HE
Communication Channel AS
4. Client sends encrypted score $E(S_{dist})$
DB Server
DB
Encrypted Templates (Eq. 7 or 11)
$\mathbf{Y} \underset{pk}{\rightarrow} E(\mathbf{Y})_{dist}$
Authentication Server
Key (pk, sk)
Comparator
5. Decrypt encrypted score $E(S_{dist}) \underset{sk}{\rightarrow} S_{dist}$
6. Output final decision $D = (S_{dist} > \delta)$

Figure 1: **General diagram of the proposed scheme**. A local client acquires and extracts the template of the probe template ($\mathbf{X}$) and computes the encrypted dissimilarity score ($E(S_{dist})$) between the probe and the encrypted reference templates ($E(\mathbf{Y})_{dist}$), in collaboration with a centralized server. This server holds the key pair (pk, sk) and the encrypted references, and outputs the final decision D. All the values, either stored or transmitted on the communication channel, are encrypted (depicted in red).

Based on the Paillier cryptosystem properties described in Eqs. 3 and 4, the score $E(S_{euc})$ can be computed in the encrypted domain as

$$E(S_{euc}) = E\left(\sum_{f=1}^{F} x_f^2\right) \cdot E\left(\sum_{f=1}^{F} y_f^2\right) \cdot \prod_{f=1}^{F} E(y_f)^{-2x_f} \tag{6}$$

The first factor of the product can be locally computed on the client side - $\mathbf{X}$ is the extracted probe template. The second factor can be computed on the server side at enrolment and its encryption stored in the database. Finally, in order to compute the third factor, the server sends $E(y_f)$, for $f = 1, \ldots, F$ to the client, and then the client computes $E(y_f)^{-2x_f}$ applying Eq. 4. Therefore, we define the encrypted reference template as

$$E(\mathbf{Y})_{euc} = \left\{ E(y_1), \ldots, E(y_F), E\left(\sum_{f=1}^{F} y_f^2\right) \right\} \tag{7}$$

3.2.2 Cosine Similarity

The cosine similarity between two templates $\mathbf{X}$ and $\mathbf{Y}$ is defined as

$$d_{cos}(\mathbf{X}, \mathbf{Y}) = \frac{\mathbf{X} \cdot \mathbf{Y}}{\|\mathbf{X}\| \cdot \|\mathbf{Y}\|} = \sum_{f=1}^{F} \frac{x_f \cdot y_f}{\|\mathbf{X}\| \cdot \|\mathbf{Y}\|} \tag{8}$$

Since $x_f, y_f > 0$, d_{cos} will also be a positive number in the range $[0, 1]$. In order to have a bigger range that will allow a comparison among integers, $d_{cos}(\mathbf{X}, \mathbf{Y})$ is multiplied by 10^{12}:

$$S_{cos} = 10^{12} d_{cos}(\mathbf{X}, \mathbf{Y}) = \sum_{f=1}^{F} \frac{10^6 x_f}{\|\mathbf{X}\|} \cdot \frac{10^6 y_f}{\|\mathbf{Y}\|} \tag{9}$$

so that, using Eq. 4, we can encrypt it as:

$$E(S_{cos}) = \prod_{f=1}^{F} E\left(\frac{10^6 y_f}{\|\mathbf{Y}\|}\right)^{10^6 x_f / \|\mathbf{X}\|} \tag{10}$$

For each factor, the base of the exponentiation is sent encrypted by the server and the exponent's plaintext is known by the client - it is the acquired probe template. Therefore, we define the encrypted reference template as

$$E(\mathbf{Y})_{cos} = \left\{ E\left(\frac{10^6 y_f}{\|\mathbf{Y}\|}\right) \right\}_{f=1}^{F} \tag{11}$$

It should be finally noted that, since $y_f \in [0, 10^3]$, we have $\|\mathbf{Y}\| = \sqrt{\sum_{f=1}^{F} y_f^2} \leq \sqrt{\sum_{f=1}^{F} 10^6} = 10^3\sqrt{F}$. Therefore, $10^6 y_f / \|\mathbf{Y}\| \geq 10^6 y_f / 10^3\sqrt{F} = 10^3 y_f / \sqrt{F}$. Assuming $10^3 > \sqrt{F}$, $10^6 y_f / \|\mathbf{Y}\| \geq y_f$, which yields large enough integers to encrypt.

3.3. The Final Complete System

Finally, as shown in Fig. 1, three entities are involved in the encrypted identity verification process:

- The client, which acquires the probe biometric sample, extracts the corresponding template $\mathbf{X}$, computes the encrypted similarity score $E(S_{dist})$ and sends it to the authentication server.

- The DB server, which holds the database comprising only encrypted templates, and sends the encrypted reference template $E(\mathbf{Y})_{dist}$ to the client during verification.

- The authentication server, which holds the key pair (pk, sk) and computes the final verification decision D.

The database and authentication server should be separate entities in order to avoid information leakage. If encrypted templates were stored with the decryption key, sk, a malicious server or an eventual external attacker could use the secret key to decrypt the templates. As a consequence, we define two different entities and assume that both servers do not collude.

Finally, identity verification is carried out in six successive steps:

0. During enrolment, the reference biometric templates are encrypted using the server public key pk. The encrypted templates $E\left(\mathbf{Y}\right)_{dist}$ are stored in the database (see Sect. 3.2 for a definition of the encrypted templates for each of the distances considered).

1. The client captures the probe sample and extracts the features, generating the probe template $\mathbf{X}$ (see Sect. 2).

2. The DB server sends the reference template $E\left(\mathbf{Y}\right)_{dist}$, encrypted using an HE scheme, to the client (see Sect. 3.1).

3. The client computes the encrypted distance between the reference and the probe templates $E\left(S_{dist}\right)$, given only $\mathbf{X}$ and $E\left(\mathbf{Y}\right)_{dist}$ (the implementation of the different distances in the encrypted domain is explained in Sect. 3.2). It should be noted that one encrypted distance per reference template is computed: $E\left(S^m_{dist}\right)$, with $m = 1, \ldots, M$. Then, the product of those scores is considered as the final encrypted similarity score: $E\left(S_{dist}\right) = \prod_{m=1}^{M} E\left(S^m_{dist}\right)$, which corresponds to the sum of the scores in the unencrypted domain (see Eq. 3).

4. The client sends $E\left(S_{dist}\right)$ to the authentication server.

5. The authentication server decrypts the score, using the secret key sk, thus obtaining S_{dist}.

6. Finally, the authentication server generates and outputs the final genuine/impostor verification decision $D = (S_{dist} > \delta)$, where δ is a predefined threshold.

4. Performance Evaluation

According to the ISO/IEC 24745 standard on biometric information protection, the first requirement for biometric template protection schemes is that verification performance is preserved with respect to the equivalent unprotected system. In this section we address this feature of the proposed method, comparing the performance of the unprotected and encrypted systems over the signature subcorpus of the DS2 BioSecure Multimodal database [28]. This subset comprises 30 genuine signatures and 20 skilled forgeries of 210 subjects, acquired in two separate sessions with the Wacom Intuos 3 pen tablet. The first 160 subjects are enrolled to the system with $M = 5$ signatures. The remaining genuine signatures are used for computing the genuine scores ($160 \times 25 = 4,000$ genuine scores), and all the skilled forgeries of those subjects will be used for the skilled forgeries comparisons ($160 \times 20 = 3,200$ skilled impostor scores). Finally, for the random forgeries scenario, the first sample of the last 50 subjects (i.e., those that were not enrolled to the system) will be compared to each user model ($160 \times 50 = 8,000$ random impostor scores).

Verification performance is analysed in Fig. 2: the Detection Error Trade-Off (DET) curves for the unprotected (solid) and the protected (dashed) systems are depicted for the two distances considered, under the random forgeries (thick blue) and the skilled forgeries (thin purple) scenarios. As it may be observed, both distances show the same performance at all operating points, as desired.

5. Irreversibility and Unlinkability

As described in Sect. 1, the ISO/IEC 24745 standard requires for biometric template protection systems to ensure both irreversibility and unlinkability. To that end, three different pieces of information should be hidden: *i*) only the client can have access to the plain probe template, *ii*) the plain reference template should not be seen by the client, and only its encryption should be stored or handled during verification, and *iii*) the score should also be protected in order to prevent hill-climbing and inverse-biometrics attacks.

In the first place, given the semantic security against chosen plaintext attacks provided by Paillier's cryptosystem, no information can be feasibly derived from encrypted data without knowledge of the secret key sk.

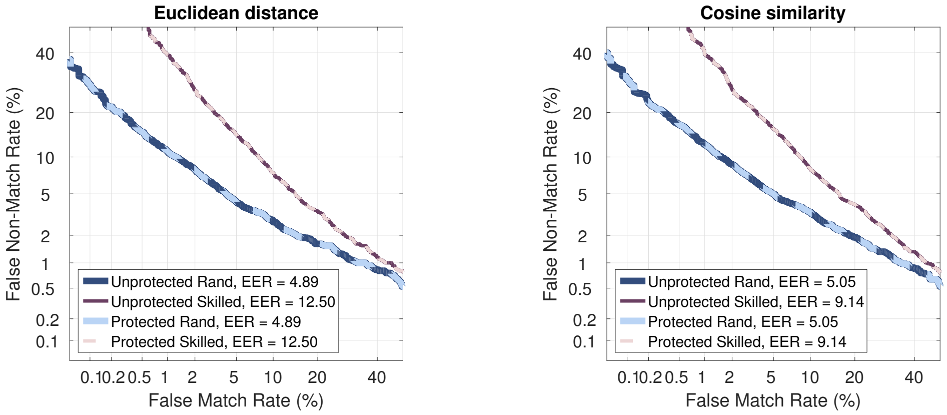

Figure 2: **Performance analysis**. DET curves for the two distances considered, under random (thick blue) and skilled (thin purple) forgeries scenarios, for the original unprotected scheme (solid) and the proposed BTP scheme (dashed).

Furthermore, as explained in Sects. 3.2.1 and 3.2.2, for each distance measure considered, the only biometric information exchanged from the database server to the client is the encrypted reference template. Therefore, assuming the authentication server is able to protect the key, neither the client nor the DB server will be able to learn any information from it. Conversely, the client sends no information about the acquired probe template to the any of the servers. In addition, since the client cannot decrypt the protected score $E\left(S_{dist}\right)$, and it is never shared in its plain form, attacks based on the evolution of the similarity score [17, 18, 25] are prevented. We may thus conclude that the first requirement established by the ISO/IEC 24745 standard, irreversibility, is met.

Similarly, should an encrypted template be stolen, a new key pair (sk, pk) could be generated. Then the entire database could be re-encrypted using the new key pair without having to re-acquire any biometric sample from the enrolled subjects. This way renewability is also achieved.

Finally, unlinkability is also granted. On the one hand, unencrypted distances between templates are not preserved in the encrypted domain, thereby preventing a direct comparison of protected templates. On the other hand, given the semantic security provided by the Paillier cryptosystem, any comparison or statistical analysis of plain data is prevented. Furthermore, since the Paillier cryptosystem is based on probabilistic encryption, the randomness incorporated in the encryption algorithm leads to different ciphertexts given a particular message. This means that if $\mathbf{X}$ is encrypted twice with the same key, the corresponding ciphertexts could not be matched: $E_{pk_1}\left(\mathbf{X}, s_1\right) \neq E_{pk_1}\left(\mathbf{X}, s_2\right)$.

6. Complexity Analysis

Finally, the computational cost is estimated in terms of the encryptions and decryptions carried out, as well as the number of products and exponentiations, since those are the most costly computations. On the other hand, for the estimation of the template size, the size of the modulo $n = p \cdot q$ on which the encryption and decryption functions rely, has to be taken into account: for a length of $|n|$ bits, ciphertexts will be $2|n|$ bits long. The complexity analysis for each distance is summarised in Table 1. In our experiments, we considered $|n| = 1,024$ (a key size which obtains the recommended level of security [9]), $F = 40$ features and $M = 5$ enrolment templates.

As it may be observed in Table 1, regarding the number of operations carried out, whereas no encryptions are required for the Cosine distance $E(S_{cos})$ (see Eq. 10), in order to compute the Euclidean distance $E(S_{euc})$, the client needs to encrypt the first term in Eq. 6 once. On the other hand, in both cases the authentication server needs to decrypt the score $E(S_{dist})$ to compute the final verification decision D. Regarding the number of products and exponentiations in the encrypted domain, a similar complexity is achieved for each distance. Using Kun Liu's implementation of the Paillier cryptosystem in Java [2], and running the experiments in a machine with an Intel Core i7 with four 2.67 GHz cores, one comparison takes about 10^{-4} seconds. Even if it should be noted that this is just an illustrative approximation (code should be optimized and a separate servers for the DB and authentication need to be incorporated), we may conclude that both distances can be implemented in real time applications,

[2] http://www.csee.umbc.edu/~kunliu1/research/Paillier.html

Table 1: **Complexity analysis** for $F = 40$ features and $M = 5$ enrolment templates.

	Euclidean	Cosine
Encryptions / Decryptions	1 / 1	0 / 1
Products	214	199
Exponentiations	200	200
Encrypted Template size	51.25 KB	50 KB
Plain Template size	0.39 KB	0.39 KB
Exchanged data	53.25 KB	52 KB

being the Cosine distance slightly more efficient.

As for storage and bandwidth requirements, a higher increase is observed. While only $M \times F = 5 \times 40$ real valued features are stored in the unprotected templates, requiring $5 \times 40 \times 16$ bits $= 3,200$ bits $=$ 0.39 KB, in the protected domain we need to store:

- For the Euclidean distance (see Eq. 7), $M \times (F + 1) = 5 \times 41$ cyphertexts, requiring $5 \times 41 \times 2,048$ bits $= 419,840$ bits $= 51.25$ KB.

- For the Cosine distance (see Eq. 11), $M \times F = 5 \times 40$ cyphertexts, requiring $5 \times 40 \times 2,048$ bits $=$ $409,600$ bits $= 50$ KB.

As a consequence, the storage requirements are multiplied by a factor of 128 in the protected domain. However, it should be noted that encrypted templates require only 50 KB, a size which can be handled by most systems.

Finally, regarding the require bandwidth, during verification one reference template is sent from the DB server to the client and the encrypted score $E(S_{dist})$ is sent from the client to the authentication server, increasing the aforementioned values by 2 KB, as shown in Table 1.

7. Conclusions

In this article we have proposed a new efficient biometric template protection scheme based on fixed-length templates and Homomorphic Encryption. Two different distance measures have been implemented and thoroughly analysed, showing that the verification performance is preserved in the encrypted domain for the Euclidean distance and Cosine similarity, while irreversibility, unlinkability and renewability are provided in all cases, thus meeting the requirements of the ISO/IEC IS 24745 on biometric technologies.

It should be noted that the stored templates and all the computations are carried out in the encrypted domain, so that no biometric information is revealed, and the plain dissimilarity score is never shared, thereby preventing hill-climbing based attacks. In contrast to other approaches regarding signal processing and HE, the computational cost is very low: none or only one encryptions are needed at verification time and only 50 KB are exchanged between server and client. We may hence conclude that the proposed scheme can be deployed in real-time applications.

As future work lines, we will study the feasibility of applying HE to multi-biometric systems at different fusion levels (i.e., feature, score or decision level).

Acknowledgements

This work has been partially supported by projects BEAT (FP7-SEC-284989) from EU, CogniMetrics (TEC2015-70627-R) from Spanish MINECO, and *CECABANK*. M. G.-B. is supported by a FPU Fellowship from Spanish MECD. This work was conducted during a research stay at the Biometrics and Multimedia Forensics Laboratory, Roma Tre University, Italy.

References

[1] E. Aragones-Rua, E. Maiorana, et al. Biometric template protection using universal background models: An application to online signature. *IEEE TIFS*, 7(1):269–282, 2012.

[2] M. Barni, T. Bianchi, et al. A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates. In *Proc. BTAS*, pages 1–7, 2010.

[3] M. Barni, G. Droandi, and R. Lazzeretti. Privacy protection in biometric-based recognition systems. *IEEE Sign. Proc. Magazine*, 32(5):66–76, 2015.

[4] T. Bianchi, S. Turchi, A. Piva, R. Labati, V. Piuri, and F. Scotti. Implementing fingercode-based identity matching in the encrypted domain. In *Proc. Int. Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS)*, pages 15–21, Sept 2010.

[5] M. Blanton and P. Gasti. Secure and efficient protocols for iris and fingerprint identification. In *Proc. European Symposium on Research in Computer Security (ESORICS)*, pages 190–209, 2011.

[6] 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 on Information Hiding and Multimedia Security*, pages 187–198, 2014.

[7] J. Bringer, H. Chabanne, and A. Patey. Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends. *IEEE Signal Processing Magazine*, 30(1):42–52, 2013.

[8] P. Campisi, E. Maiorana, et al. Cancelable templates for sequence based biometrics with application to on-line signature recognition. *IEEE Trans. on SMC-A*, 40(3):525–538, 2010.

[9] D. Catalano, R. Gennaro, and N. Howgrave-Graham. The bit security of paillier's encryption scheme and its applications. In *Proc. EUROCRYPT*, pages 229–243, 2001.

[10] J. Fierrez and J. Ortega-Garcia. *Handbook of Biometrics*, chapter On-Line Signature Verification, pages 189–209. Springer, 2007.

[11] C. Fontaine and F. Galand. A survey of homomorphic encryption for nonspecialists. *EURASIP J. on Inf. Security*, 2007:1–15, 2007.

[12] M. R. Freire, J. Fierrez, et al. Biometric hashing based on genetic selection and its application to on-line signatures. In *Proc. ICB*, pages 1134–1143, 2007.

[13] M. R. Freire, J. Fierrez, and J. Ortega-Garcia. Dynamic signature verification with template protection using helper data. In *Proc. IEEE ICASSP*, pages 1713–1716, 2008.

[14] J. Galbally, J. Fierrez, and J. Ortega-Garcia. Performance and robustness: a trade-off in dynamic signature verification. In *Proc. ICCASP*, 2008.

[15] O. Goldreich. *The foundations of cryptography - Vol 2*. Cambridge University Press, 2004.

[16] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of computer and system sciences*, 28(2):270–299, 1984.

[17] M. Gomez-Barrero, J. Galbally, et al. Hill-climbing attack based on the uphill simplex algorithm and its application to signature verification. In *Proc. BioID*, pages 83–94. LNCS-6583, 2011.

[18] M. Gomez-Barrero, J. Galbally, and J. Fierrez. Efficient software attack to multimodal biometric systems and its application to face and iris fusion. *Pattern Recognition Letters*, 36:243–253, 2014.

[19] T. Ignatenko and F. Willems. Biometric systems: Privacy and secrecy aspects. *IEEE Trans. on Information Forensics and Security*, 4(4):956 – 973, 2009.

[20] T. Ignatenko and F. Willems. Information leakage in fuzzy commitment schemes. *IEEE Trans. on Information Forensics and Security*, 2(5):337–348, 2010.

[21] ISO/IEC JTC1 SC27 Security Techniques. *ISO/IEC 24745:2011. Information Technology - Security Techniques - Biometric Information Protection*. ISO, 2011.

[22] A. K. Jain, K. Nandakumar, and A. Ross. Score normalization in multimodal biometric systems. *Pattern Recognition*, 38:2270–2285, 2005.

[23] 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 Processing Magazine*, 30(1):82–105, 2013.

[24] A. Levi, E. Savas, et al. Biometric cryptosystem using online signatures. In *Proc. ISCIS*, volume 4263 of *LNCS*, pages 981–990, 2006.

[25] E. Maiorana, G. E. Hine, and P. Campisi. Hill-climbing attack: Parametric optimization and possible countermeasures. an application to on-line signature recognition. In *Proc. ICB*, pages 1–6, 2013.

[26] M. Martinez-Diaz, J. Fierrez, et al. Mobile signature verification: Feature robustness and performance comparison. *IET Biometrics*, 3(4):267–277, 2014.

[27] K. Nandakumar and A. K. Jain. Biometric template protection: Bridging the performance gap between theory and practice. *IEEE Sign. Proc. Magazine*, pages 1–12, 2015.

[28] J. Ortega-Garcia, J. Fierrez, et al. The multi-scenario multi-environment BioSecure multimodal database (BMDB). *IEEE TPAMI*, 32:1097–1111, 2010.

[29] M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich. SCiFI: A system for secure face identification. In *Proc. IEEE Symp. Security and Privacy*, page 239254, 2010.

[30] P. Paillier. Public-key cryptosystems based on composite residuosity classes. In *Proc. EUROCRYPT*, pages 223–238, 1999.

[31] K. Simoens, B. Yang, et al. Criteria towards metrics for benchmarking template protection algorithms. In *Proc. ICB*, pages 498–505, 2012.

[32] J. R. Troncoso-Pastoriza, D. Gonzalez-Jimenez, and F. Perez-Gonzalez. Fully private noninteractive face verification. *IEEE Trans. on Information Forensics and Security*, 2013.

[33] S. Ye, Y. L. ad J. Zhao, and S. S. Cheung. Anonymous biometric access control. *EURASIP J. on Inf. Security*, 2009:1–17, 2009.