IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 30, 2019, accepted December 16, 2019, date of publication January 9, 2020, date of current version January 17, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2965165

Fuzzy Vault Scheme Based on Fixed-Length Templates Applied to Dynamic Signature Verification

WENDY PONCE-HERNANDEZ[1], RAMON BLANCO-GONZALO[1,2], JUDITH LIU-JIMENEZ[1], AND RAUL SANCHEZ-REILLO[1]

[1]Electronics Technology Department, University Carlos III of Madrid, 28911 Leganés, Spain
[2]European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), 67100 Strasbourg, France

Corresponding author: Wendy Ponce-Hernandez (wponce@ing.uc3m.es)

This work was supported by the Spanish National Cybersecurity Institute (INCIBE) through the Excellence of Advanced Cybersecurity Research Teams Program.

ABSTRACT As a consequence of the wide deployment of biometrics-based recognition systems, there are increasing concerns about the security of the sensitive information managed. Various techniques have been proposed in the literature for the biometric templates protection (BTP), having gained great popularity the crypto-biometric systems. In the present paper we propose the implementation of a Fuzzy Vault (FV) scheme based on fixed-length templates with application to dynamic signature verification (DSV), where only 15 global features of the signature are considered to form the templates. The performance of the proposed system is evaluated using three databases: a proprietary collection of signatures, and the publicly available databases MCYT and BioSecure. The experimental results show very similar verification performance compared to an equivalent unprotected system.

INDEX TERMS Biometrics, biometric cryptosystem, dynamic handwritten signature, fuzzy vault, key binding, template protection.

I. INTRODUCTION

The last decades have seen a widespread deployment of biometric technologies for automatic user recognition. Biometric recognition systems are used in a wide variety of applications, such as border crossings, automated teller machines and cellular phones [1], [2]. The specific advantages offered by biometrics have led to the success of these systems. Biometric characteristics have the property of being intrinsic to each individual and, unlike traditional authentication methods (e.g. PIN or password), they have high immunity to be lost, forgotten or guessed [3]. Compared to traditional authentication methods, biometrics-based recognition systems offer greater reliability and user convenience.

Despite the benefits offered by biometric recognition, there are still major concerns about issues such as privacy and security of biometric technology. In [4], [5] eight vulnerable points were identified on a generic biometric system (see Fig. 1).

The associate editor coordinating the review of this manuscript and approving it for publication was Andrea F. F. Abate.

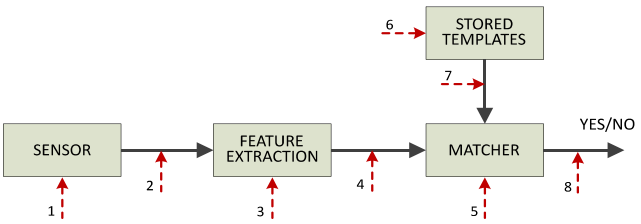

FIGURE 1. Points of attack in a generic biometric system [4].

Attacks at the user interface (sensor) are mostly carried out by presenting the physical reproduction of a biometric characteristic. Also, feature extraction module and system database can be attacked to obtain the generated genuine template, modify it, or replace it by an impostors' template. Other vulnerable points of the system are the interfaces between modules, which could be intercepted to manipulate the biometric information transmitted. Finally, both the comparator score and the final system decision could be conveniently modified by an attacker.

While a biometric system can be compromised in different ways, one of the most damaging attacks is the unauthorized access to stored biometric templates [6]. It has been

showed that biometric samples can be recovered from stolen templates and then used to fraudulently gain access to the system [7]. In addition, as biometric characteristics are permanently linked to the user, if a template is compromised, all the applications using the same biometric sample are also compromised. Moreover, stolen templates could be used to track the activity of enrolled users by cross-comparisons across different databases (e.g. bank's databases, person's health records, criminal databases). Thus, the leakage of stored biometric template compromises both the systems security and the citizen privacy. In order to improve robustness against attacks, biometric recognition systems storing protected reference templates are required.

Among the different biometric characteristics considered for the recognition of individuals, handwritten signature has been historically one of the most used methods [8], [9]. It has been applied in the context of transactions, document certification or forensic applications. In addition, handwritten signatures are acquired in an easy and non-invasive way, which allows high acceptability from the users perspective [10]. Thus, its recognition reliability and its wide social acceptance have consolidated the handwritten signature in the field of biometric recognition.

Depending on the available input information, the handwritten signature recognition can be divided in two main approaches: static and dynamic. In the static case the analysis is performed only from the scanned signature image. In the dynamic approach, electronic pens or digitising tablets are typically used to capture the time functions generated during the writing process (e.g. spatial coordinates, pression, pen tip state switch or azimuth). Traditionally, DSV has reported better results than static approach, as the dynamic features available are more discriminative and difficult to imitate [1], [8], [11], [12].

In particular, the biometric signature has the drawback of presenting high intraclass variability. This variability problem is influenced by factors such as mood or age. As a consequence, protecting signature templates is a difficult task. One of the main challenges in designing a BTP system based on signature is to generate sufficiently invariant and discriminatory templates, allowing efficient comparisons in the protected versions. Furthermore, templates in an appropriate format should be derived according to the input requirements of the selected protection algorithm.

In the present article we propose an implementation of the FV scheme for fixed-length templates introduced in [13], and its application to DSV. To form the signature templates to be protected, we consider only 15 global features, which are encoded to obtain templates without repeated values. In order to improve the system performance, an initial training phase is added, where the system configuration parameters are automatically adjusted according to the target database. The verification performance of the proposed system is analysed and then, the results are compared with respect to an equivalent unprotected system. The irreversibility, unlinkability and time performance of the proposed system are also analysed. Experiments are carried out on three databases: a proprietary data collection [14] and the publicly available databases MCYT [15] and BioSecure [16].

The article is organized as follows: Section II presents the state of the art of the main BTP approaches and some related works are summarized. The proposed system is described in Section III. Verification performance is presented in Section IV, while irreversibility and unlinkability are analysed in Section V. The time performance of the proposed system is studied in Section VI. Finally, conclusions and future works are drawn in Section VII.

II. STATE OF THE ART

The variability problems of the biometric features represent a fundamental challenge in the design of BTP systems [6], [17]. Standard encryption techniques (e.g. RSA, Advanced Encryption Standard (AES)) could be considered to protect the biometric information. However, these encryption algorithms provide large differences in the results even when the input data differ slightly. Thus, intraclass variability invalidates the use of these algorithms in biometrics, since encrypted templates could not be effectively compared. Alternatively, templates could be decrypted before carrying out the comparison. But this option is not secure because the templates are unprotected in every authentication attempt. Hence, standard encryption algorithms are not a suitable solution to protect the biometric templates [6].

A. BIOMETRIC TEMPLATE PROTECTION SCHEME: REQUIREMENTS AND CATEGORIES

In order to overcome the limitations of the standard encryption techniques, over the last years researchers have been working on the development of BTP schemes. According to the ISO/IEC 24745:2011 standard on biometric information protection [18], these schemes must fully meet the following requirements:

- ***Irreversibility***: from a protected biometric template it must be computationally difficult to recover the original template.
- ***Renewability***: if a secure template is compromised, the scheme must be able to revoke it and remake a new different one from the same biometric data.
- ***Unlinkability***: it must be difficult to determine if two or more templates, protected with different keys, belong to the same biometric characteristic. This property avoids possible cross-comparisons with other databases, thus ensuring the users' privacy.

At the same time, it is desirable that the accuracy, the verification time and the storage requirements are maintained similar to an equivalent unprotected system [19].

Designing BTP schemes that fully meet the aforementioned requirements without degrading the verification performance represents a great challenge. Different approaches have been proposed in the literature, which can be classified into three main categories: Cancelable Biometrics,

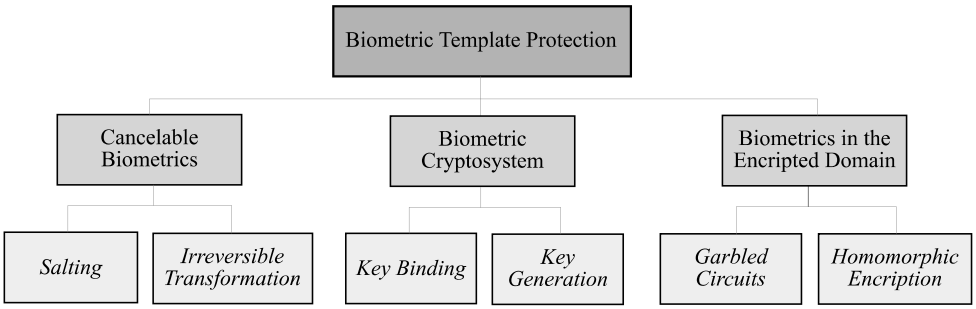

FIGURE 2. Categorization of biometric template protection approaches.

Biometric Cryptosystem and Biometrics in the Encrypted Domain (see Fig. 2).

In the Cancelable Biometrics category, a transformation function defined by a user-specific key is applied to the unprotected template. Both, the modified template and the key (usually referred as auxiliary data (AD)), are stored for verification purposes. Then, the same transformation is applied to the template probe and the comparison takes place in the transformed domain. Depending on the characteristics of the transformation function there are two subcategories:

- *Salting*, where a reversible function (e.g. bio-hashing) is used for the transformation. Thus, the security of these schemes relies on the security of the key.
- *Irreversible Transformation*, where a one-way function (e.g. robust hashing) is applied to the unprotected template, obtaining a transformed template which is hard to invert even if the key is known.

In the Biometric Cryptosystem category, cryptography and biometrics are merged, obtaining a secure sketch (stored as AD), which does not reveal much information about the key or the biometric data. During the authentication, the comparison is performed indirectly by checking the validity of a key extracted from the biometric probe using the AD. If the genuine users' biometric data is not known, to get the key from the AD must be computationally difficult. But, if the template probe is sufficiently close to the enrolled template, it must be easy to decode the AD and recover the key. Typically, error correction coding techniques are used to handle intraclass variability. These schemes allow the protection of the biometric data and facilitate the secure key management. The Biometric Cryptosystem category is divided into:

- *Key Binding*, where the AD is obtained by binding the key to the biometric data. Two well-known schemes in this category are FV [20] and fuzzy commitment [21].
- *Key Generation*, where the AD is obtained only from the biometric data. This category includes the secure sketch and fuzzy extractor concepts [22].

In Cancelable Biometrics and Biometric Cryptosystem approaches, the stored AD should not reveal significant sensitive information in order to preserve both the system security and the privacy of the subject. A more detailed review of these two categories can be found in [6], [23].

As an alternative to the above approaches, *secure multi-party computation* [24] and *homomorphic cryptosystem* [25] have recently been used as BTP methods. These solutions are classified in a new class called Biometrics in the Encrypted Domain. In this class, the most used approaches are based on *Garbled Circuits* [26] and *Homomorphic Encryption* (HE) [27]. Particularly, successful implementations of biometric systems based on HE have been developed, where only encrypted biometric data are handled. HE schemes carry out the recognition in the encrypted domain while obtaining results fully comparable to those achieved by unprotected systems. However, HE allows a limited subset of operations in the encrypted domain. Thus, advanced comparison techniques (e.g. Hidden Markov Models (HMMs)) are more difficult to implement in this approach. Moreover, typically this protection technology requires higher computational cost and bandwidth [24], and it depends on the assumption that encryption keys are always kept secret.

New authentication methods have recently been proposed, where the security of biometric systems is strengthened. These methods are based on Biometric Cryptosystems, providing secure communication through the interfaces. For instance, in [28] and [29], the authors present a secure multi-server authentication protocol using a fuzzy commitment scheme. Also, [30] presents a novel fingerprint-based crypto-biometric scheme where the Diffie-Hellman (DH) algorithm [31] is used to maintain secure communication between two users.

In practice, the choice of a specific BTP approach is mostly influenced by factors such as: the biometric modality used, the security of the acquired template, the capacity to handle the intraclass variations, the recognition performance, the storage requirement or the computational cost [6].

B. RELATED WORKS

Only a few works about template protection based on dynamic signature have been proposed. In [32] and [33], the authors present an irreversible transformation approach to protect signature time sequences, where HMMs used in the comparisons are trained with the transformed features. On the other hand, in [34] and [35] was applied a FV scheme based on local features extracted from dynamic signatures. In [34]

the templates were generated using maximum and minimum of the signature, while in [35] event points (crossing points, ending points and high curvature points) were considered. The fuzzy commitment scheme was applied in [36] to a DSV system based on Universal Background Model (UBM). The approach proposed in [37] use helper data and error correction techniques to protect fixed-length templates of dynamic signature.

More recently, a DSV system based on HE and variable-length templates was presented in [38]. Despite this system meets all the requirements of the ISO/IEC 24745:2011 standard, its comparison time inefficiency prevents its use in real time applications. Another HE scheme applied to DSV is proposed in [39] considering fixed-length template. With respect to the system of [38], the scheme based on fixed-length template achieves better processing times while the verification accuracy is degraded. Then, a multi-algorithm approach based on HE for template of fixed and variable length was suggested in [40], improving both the computational complexity of [38] and the verification performance achieved in [39].

C. FUZZY VAULT: BACKGROUND

The crypto-biometric FV scheme has become one of the most popular BTP methods. This scheme is presented as an error-tolerant cryptographic construction in which an unordered set (e.g. set of biometric features) is used to encrypt/decrypt a secret key, obtaining an indivisible vault. This approach not only secures the key, but also provides protection to the unordered set. The FV scheme works as explained in the following paragraphs.

To secure a biometric feature set, $A = \{a_1, a_2, \ldots, a_n\}$, a user specific key K, of length M bits, is randomly generated. An error-correcting code (e.g. Reed Solomon (RS) [41]) is applied to K and the redundancy generated is concatenated to K, obtaining an encoded key K_c of length N bits ($N > M$). Then, a polynomial P of degree L (being $L < n$) is constructed using K_c as coefficients. The polynomial projections, $P(A)$, are calculated per each element of A, obtaining a set of genuine points $G = \{(a_i, P(a_i))\}_{i=1}^{n}$. To hide the genuine points, chaff points that do not intersect with both the polynomial P and the set A, are randomly generated. Finally, a vault set V is made up of the union of the G set and chaff points (see Fig. 3).

During the authentication, a probe biometric template B, is presented to decode the vault and recover K. If the template B overlaps substantially with A, then B can identify many genuine points from V. Provided that the difference between sets A and B is small enough such that the redundancy present in K_c allows to correct the erroneously identified points, the polynomial P will be successfully reconstructed and hence obtained the associated key K. To successfully reconstruct the polynomial, at least $L+1$ genuine points need to be identified from V.

The FV scheme has the advantage of providing high security [6]. The number of chaff points included in the vault directly influences this property, since by increasing the chaff points, the system security increases. Commonly, the number of chaff points is one order of magnitude greater than the number of genuine points [17]. Another important advantage of this scheme is its ability to handle the intraclass variability problems of biometric data, by means of error correction codes.

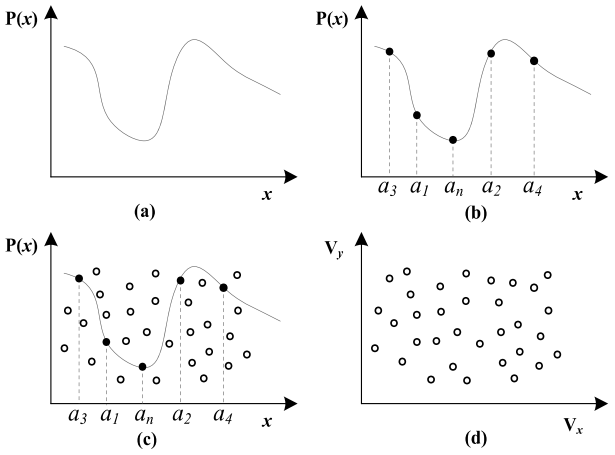

FIGURE 3. Vault coding: (a) Construction of a polynomial using K_c as coefficients. (b) Polynomial projection for the A elements. (c) Randomly generation of chaff points. (d) Obtaining the final vault.

However, the FV scheme is vulnerable to some specific attacks [42]. In particular, this scheme *i)* can be directly attacked via record multiplicity. If diverse vaults generated from the same biometric sample (using different keys) are known, the genuine points can be easily identified by correlating the different vaults. Thus, the FV scheme does not provide renewability and unlinkability. Also, *ii)* stolen key inversion attacks could take place in these systems. If the key embedded in the vault is known, the vault can be easily decoded to obtain the protected biometric data. Furthermore, *iii)* a FV system can be compromised by blended substitution attacks. Since the vault involves numerous chaff points, some of them could be replaced by the attacker biometric features. Consequently, both the genuine user and the attacker could successfully unlock the same vault.

To overcome these limitations, in [43], the authors propose the application of a transformation function to the biometric template and then, to construct the vault from the transformed template. Finally, an encryption technique is used to secure the generated vault. This way, the transformation function provides renewability and unlinkability, avoiding attacks via record multiplicity, while the encryption algorithm provides robustness against stolen key inversion and blended substitution attacks. Such solutions, where more than one approach is used to protect the biometric templates, are known as hybrid schemes.

D. FUZZY VAULT: APPLICATIONS

Several works have been reported, where the FV scheme is applied to protect different biometric modalities.

TABLE 1. Summary of FV applications.

Modality	Database	Features used to conform the templates	Results
Fingerprint [44]	100 users with 2 fingerprint images each. (using 1 image to encoding the vault)	coordinates of minutia points	False Reject Rate (FRR) = 21% False Accept Rate (FAR) = 0%
Handwritten Signature [34]	330 users with 25 genuine signatures and 25 skilled forgeries each. (using 5 genuine signatures to encoding the vault)	maximum and minimum in the signature	FRR = 57.3% FAR = 0.3% (random) FAR = 1.2% (skilled)
Handwritten Signature [35]	10 users with 4 genuine signatures and 3 skilled forgeries each. (using 1 signature genuine to encoding the vault)	signature event points (crossing points, ending points and high curvature points)	FRR = 8.33% FAR = 2.50% (skilled)
Face [45]	40 users with 10 images each. (using 5 images to encoding the vault)	Principal Component Analysis (PCA) features	FRR = 0.5% FAR = 7.38%
Palmprint [46]	85 users with 2 left-hand images each. (using 1 image to encoding the vault)	Discrete Cosine Transform (DCT) features	FRR = 0% FAR = 0.35%
Iris [13]	99 users with 10 images each. (using 5 images to encoding the vault)	Independent Component Analysis (ICA) features	FRR = 0.775% FAR = 0%
Multibiometric (fingerprint + iris) [47]	108 users with 2 fingerprint images and 2 iris images each. (using 1 fingerprint image and 1 iris image to encode the vault)	Iris: feature extraction using Gabor filters Fingerprint: coordinates of minutia points A unique template is derived from the individual templates.	Genuine Accept Rate (GAR) = 98.2% FAR = 0.01%

In [44], a FV scheme based on fingerprint templates is presented. In this case, due to the difficulties encountered to reconstructing the polynomial via error correction, authors propose a modified version of the FV scheme introduced in [20]. During vault encoding, no error corrector code is applied. Instead, bits of Cyclic Redundancy Check (CRC) are generated from the user key. These bits are appended to the key, and the L-degree polynomial involved in the construction of the vault is represented using the encoded key. The rest of the vault coding process is the same as the original FV scheme. During the authentication, candidate points are selected from the vault using the probe sample. If less than $L + 1$ points are found, the authentication fails. Otherwise, they find all the possible combinations of $L + 1$ points and a candidate polynomial per combination is constructed and verified by applying CRC. In case of error detection, the checked polynomial is discarded, and the same procedure is repeated for the next point combination. If no error is detected, it means that the correct polynomial has been found and therefore, the associated key is valid. As a limitation, this scheme needs to evaluate many candidate's polynomial for each authentication attempt, resulting in a high time inefficiency. However, this FV scheme variant has been one of the most used.

Both [34] and [35] protect dynamic signature templates following the FV approach proposed in [44]. Implementations of the FV scheme applied to face [45] or palmprint [46] modalities have also been reported. Furthermore, a multibiometric-based FV is proposed in [47], where the template to be protected is derived from individual fingerprint and iris templates. In this case, the multibiometric vault provided better performance and higher security compared to the unibiometric vaults.

Another variant of the original FV scheme is proposed in [13] to secure iris biometric data. In this case, the authors propose a scheme where error correction and interpolation procedures are separated. Specifically, our implementation is based on this FV scheme variant, mostly because the use of the error-correcting code RS accelerates the decoding step [20], and allows to manage the intraclass variability.

A summary of the FV applications reported is presented in Table 1, indicating in each case the used database size, the features used to conform the templates and the results obtained.

III. PROPOSED SYSTEM

In this section, the proposed FV scheme based on signature fixed-length templates is presented. As shown in Fig. 4, the system is divided into three phases. In the first phase the system configuration parameters are automatically adjusted according to the target database. In the second phase the reference templates are created and secured using the FV encoder. Finally, the verification takes place, keeping the security of reference templates. The following subsections provide an in-depth explanation for each of these phases.

A. PHASE 1. ADJUSTMENT OF CONFIGURATION PARAMETERS

The configuration process is initiated from 15 global features of the signature, which are candidates to form the final templates that will consist of 8 features. Table 2 shows the

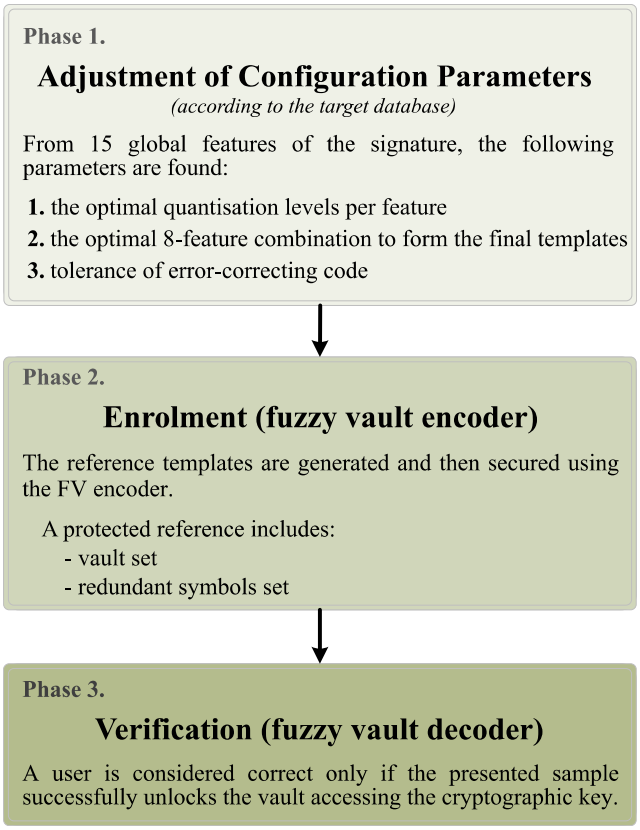

FIGURE 4. Operating phases of the proposed FV scheme.

description of the features used, as well as the notations assigned to each one.

In order to achieve greater verification accuracy, both static and dynamic information have been considered. These include, features related to signature dimensions, stroke measures and time. To obtain these metrics, only the channels associated with spatial coordinates (X and Y), pen tip switch state (S) and time (T) are used. Pressure has not been used, as some capture devices (e.g. capacitive touch screens) cannot provide it.

1) SELECTION OF OPTIMAL QUANTISATION LEVELS

In the proposed FV scheme, all the operations take place in Galois fields with cardinality 65536, namely GF(2^{16}). For this reason, the features involved in the templates must be quantised on 16 bits maximum. Based on this, the first objective of the configuration phase is to individually select optimal quantisation levels to represent each of the 15 starting features.

Before carrying out this task, the following pre-processing steps are applied to the signals used:

1. The X and Y coordinates are smoothed using a low pass filter to remove possible noise introduced during the acquisition process.
2. A statistical normalization is applied to X and Y signals, using their mean and standard deviation [48].
3. The X and Y coordinates corresponding to the first and last 5% of the signature length are discarded due to the high instability typically present in these signature regions [34].

Once the channels are pre-processed, an individual reference is calculated per feature, using the first 5 genuine signatures. The value of 5 samples to enrol was chosen taking into account that in a real scenario, requesting a higher number of samples during the enrolment could cause rejections from users [49].

Then, the influence of applying different quantisation levels in the individual verification of each feature is evaluated. This is performed by using, in each case, the corresponding individual references. From the results obtained per feature, the quantisation that generates the lowest False Match Rates (FMR) and False Non-Match Rates (FNMR) simultaneously, is selected as optimal. Although this has been our criterion to consider a result as optimal, other criteria could also be used (e.g. minimum FMR accepting high FNMR, or vice versa).

According to empirical analysis, it was determined that a maximum of 8 bits is enough for optimal quantisation. Assuming this, we decided to encode the features into 16 bits according to the binary distribution shown in Fig. 5. The 4 most significant bits are reserved for the feature identification number, and the remaining bits are used to represent the feature value according to the corresponding optimal quantisation. This way, there are enough bits to quantify the features and during the template generation, none of the features involved is encoded with the same binary sequence.

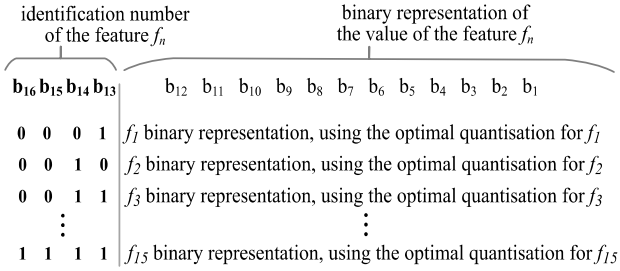

FIGURE 5. Binary distribution used to represent the features with 16 bits.

2) SELECTION OF OPTIMAL 8-FEATURE COMBINATION AND ERROR-CORRECTING CODE TOLERANCE

The proposed FV scheme has been designed to work with templates of 8 elements. Thus, the next step in the configuration is to find the optimal 8-feature combination to represent the handwritten signatures.

First, a database with the reference 15-feature templates is generated, using the previously calculated individual references (encoded into 16 bits). All the possible combinations of 8 features, among the previous 15 are found (obtaining a total of 6435 candidate reference templates per genuine user). Then, a performance evaluation is carried out considering all these alternatives of reference templates

TABLE 2. Set of 15 features candidate to form the final templates.

No. of feature	Global Feature	Description
1	$L_{iS/t} = L_{iStroke}/L_{total}$	Ratio of initial-stroke to total signature length.
2	$L_{eS/t} = L_{eStroke}/L_{total}$	Ratio of end-stroke to total signature length.
3	$sX = \Delta X/L_{total}$	Ratio of total shift of X in pen down to total signature length.
4	$T_{iS/t} = T_{iStroke}/T_{total}$	Ratio of initial-stroke to total signature time.
5	$T_{eS/t} = T_{eStroke}/T_{total}$	Ratio of end-stroke to total signature time.
6	$T_{d/t} = T_{pd}/T_{total}$	Ratio of pen-down to total signature time.
7	$T_{u/t} = T_{pu}/T_{total}$	Ratio of pen-up to total signature time.
8	$T_{d/top\_d} = T_{pd}/top\_T_{pd}$	Ratio of pen-down to top-pen-down time[2].
9	$T_{t/top\_t} = T_t/top\_T_t$	Ratio of total-signature to top-total-signature time[2].
10	# Strokes	Total number of strokes.
11	$A_{iS/t} = A_{iStroke}/A_{total}$	Ratio of initial-stroke to total signature area.
12	$A_{eS/t} = A_{eStroke}/A_{total}$	Ratio of end-stroke to total signature area.
13	$P_{iS/t} = P_{iStroke}/P_{total}$	Ratio of initial-stroke dots to total dots recovered.
14	$P_{eS/t} = P_{eStroke}/P_{total}$	Ratio of end-stroke dots to total dots recovered.
15	$sX_{0-min} = (X_0 - X_{min})/\Delta X$	Ratio of difference between X (1st pen down) and min(X) to total shift of X.

[2] Using the genuine signatures of the experiment databases, a small statistical study of the global parameters *pen-down-time* and *total-signature-time* was carried out. The longest values obtained were 7.5s in *pen-down-time* and 11.6s in *total-signature-time*. Based on these results, in order to quantify these features within a range, it was decided to establish the following top value for each parameter: *top-pen-down time* of 15s and *top-total-signature time* of 23s.

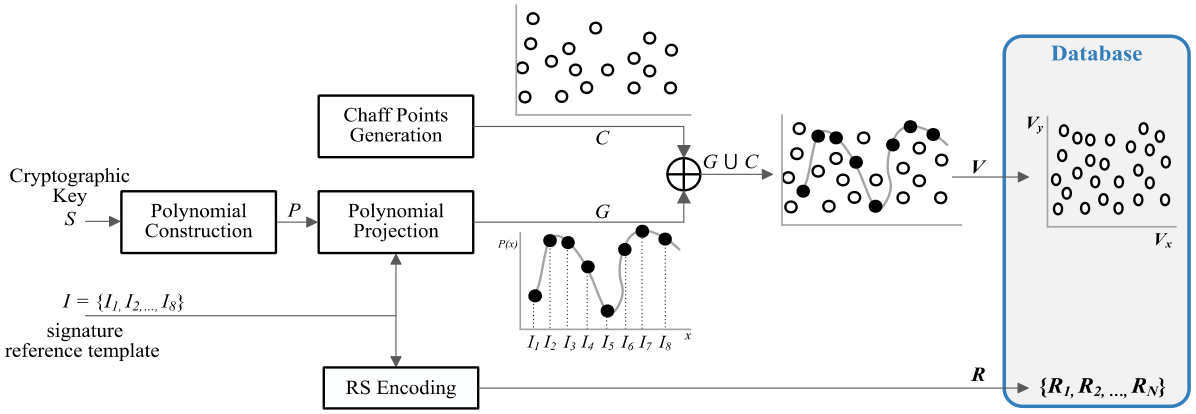

FIGURE 6. Fuzzy vault encoder.

(unprotected). Finally, the 8-feature combination that best discriminate among target database users is selected to conform the unprotected signature templates.

During this evaluation, the number of equal elements between the probe and the reference template is used as comparison score. Then, from the results obtained with the optimal 8-feature combination, the score that has generated the lowest error rates is selected as the decision threshold. Finally, with the selection of the threshold, the tolerance of the error-correcting code used in the FV scheme is established.

Once the optimal quantisation per feature has been found and both the optimal 8-feature combination and the tolerance of the error correction code have been selected, the system is properly parametrized according to the target database.

The next phases (2 and 3 in Fig. 4) correspond to the FV scheme implementation. From this point on, all the calculations are performed in GF(2^{16}).

B. PHASE 2. ENROLMENT (FUZZY VAULT ENCODER)

During the enrolment phase, the signature reference templates are generated and protected using FV encoder.

As shown in Fig. 6, in the vault encoding process two inputs are necessary: the reference template to be protected (I), comprising 8 elements of 16 bits each,

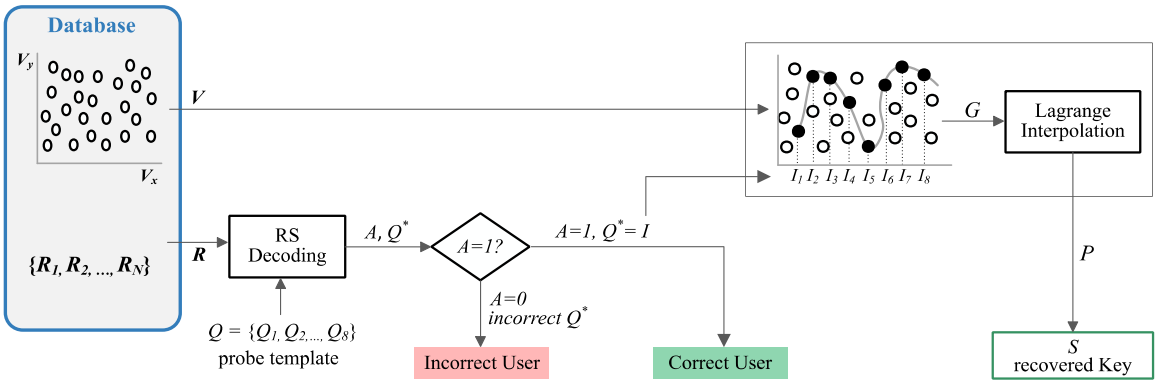

FIGURE 7. Fuzzy vault decoder.

$I = \{I_1, I_2, \ldots, I_8\}$, and a cryptographic key (S) of 128 bits. The individual references corresponding to the optimal 8-feature combination, are used to form the final reference template I.

The 128-bit key S is divided into 8 non-overlapping 16-bit packets, $\{S_1, S_2, \ldots, S_8\}$, which are used to represent the coefficients of a polynomial with degree $d = 7$, resulting in $P(x) = S_1 + S_2x + \ldots + S_8x^7$. Then, the projection of I on the polynomial P is calculated, obtaining the set of genuine points $G = \{(I_1, P(I_1)), (I_2, P(I_2)), \ldots, (I_8, P(I_8))\}$. To hide G from an attacker, a set C of 292 chaff points is randomly generated in the range of the finite field (no chaff point is located on the polynomial and their x-axis values do not overlap with the elements of I). From the union of these two sets, the vault set is formed, $V = (G \cup C)$. Note that the feature vector size used to encode/decode the vault has been set to 8, $(d + 1)$, because during the decoding phase the 8 genuine points (G) need to be identified from V to reconstruct the polynomial.

On the other hand, an RS code is applied to the unprotected reference I, obtaining a set R of redundant N-symbols. This redundancy has a correction capability of up to $N/2$ errors and it is used during the vault decoding. Finally, the sets V and R, forms the protected reference template.

C. PHASE 3. VERIFICATION (FUZZY VAULT DECODER)

The verification phase is represented in Fig. 7. The input parameters of this stage are a probe template Q, and the R and V sets stored. To obtain Q, the optimal 8 features are extracted from the probe signature and represented with 16 bits using the binary distribution of Fig. 5.

As the probe template Q may contain errors due to the intraclass variability, first the RS decoding is applied, using the redundancy set R. On one hand, if the errors contained in Q cannot be corrected, the output A of the RS decoding is set to 0 and the user is immediately considered incorrect. On the other hand, if the probe Q can be corrected or does not show errors, A is set to 1 and the user is immediately considered correct. In this case, a corrected template Q^*, identical to the one enrolled is obtained and the genuine points are perfectly identified in the vault. From the genuine points the polynomial $P(x) = S_1 + S_2x + \ldots + S_8x^7$ is reconstructed by Lagrange interpolation, and finally, the key S represented in the coefficients of P is recovered.

IV. EXPERIMENTS

This section gathers the results obtained in the experiments carried out. All these results are presented following the operation methodology described in Section III.

A. DATABASES DESCRIPTION

To evaluate the verification performance of the proposed system, three databases were used: *i*) the public version of the MCYT signature corpus (DB_1 from now on), *ii)* a proprietary database (DB_2 from now on), and *iii)* the signature subcorpus of the DS2 BioSecure database (DB_3 from now on).

DB_1 comprises 25 genuine signatures and 25 skilled forgeries of 100 users. The capture device used was a Wacom STU-500 digitiser especially designed for handwritten signature acquisition.

DB_2 contains the real signatures of 48 users, with 20 genuine signatures per user. During the generation of this database all samples were collected in a controlled environment and the acquisition process was as realistic as possible (e.g. non-biometric related test subjects, signatures subjectively accepted by the signing user, etc.). A detailed description of the protocol applied to generate this database is presented in [14]. All the samples were acquired using a Wacom STU-500 tablet.

BD_3 comprises 210 subjects, with 30 genuine signatures and 20 skilled forgeries per subject, acquired with a digitalizing tablet Wacom Intuos 3.

During the experiments, no skilled forgeries were used in this work. To calculate FMR, only signatures from other users as random forgeries have been considered.

B. EVALUATION: SELECTION OF CONFIGURATION PARAMETERS

The evaluation was initiated by obtaining the 15 individual references of the starting features for each user. To make the experiment as close as possible to a real scenario, these

references were generated from the first 5 signatures accepted by user, instead of the best resulting set of 5, as is commonly used.

1) OPTIMAL QUANTISATION LEVELS PER FEATURES

Once the individual references have been obtained, the optimal quantisation levels to represent the features (calculated through ratios) were found.

As an example, Fig. 8 shows the FMR to FNMR comparison obtained when the recognition of the feature $P_{iS/t}$ (ratio of initial-stroke dots to total dots recovered) was evaluated on DB_2 using from 3 to 15 quantisation levels. According to the criterion of optimal result assumed (lowest FMR and FNMR simultaneously), from Fig. 8 it can be seen that this feature performs better on DB_2 when it is quantised uniformly using 8 levels (point closest to the equal error rate (EER) line).

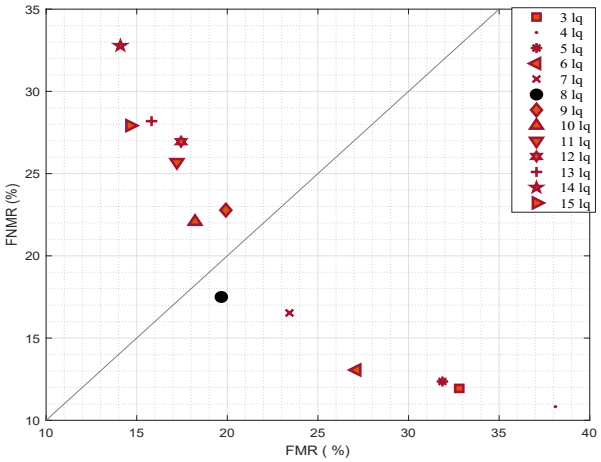

FIGURE 8. Error rates obtained after evaluating the individual verification of ($P_{iS/t}$) on DB_2, using from 3 to 15 quantisation levels (lq) to represented it.

A similar analysis was carried out for the remaining features. Table 3 gathers the optimal quantisation levels obtained per feature and database.

As shown, different optimal quantisation levels were obtained for the features evaluated on the same database. In addition, for the same feature, different values were obtained in each database. Therefore, these results show that, to achieve better verification performance, quantisation levels must be individually assigned according to the specific feature and target database.

2) OPTIMAL 8-FEATURE COMBINATION AND ERROR CORRECTING CODE TOLERANCE

Following the initial configuration, the most discriminative 8-feature combination was automatically found. Fig. 9 shows the 8-feature vectors selected to represent the samples in each database, as well as the verification performance achieved.

Note that, although the representation vectors are not identical, they include 3 equal features. Therefore, among all

TABLE 3. Optimal quantisation levels obtained per feature.

Feature	Quantisation levels		
	DB 1	DB 2	DB 3
$L_{iS/t}$	8	6	7
$L_{eS/t}$	7	6	6
sX	24	25	21
$T_{iS/t}$	8	7	7
$T_{eS/t}$	8	6	5
$T_{d/t}$	8	10	137
$T_{u/t}$	8	6	117
T_{d/top_d}	15	26	17
T_{t/top_t}	15	23	20
# Strokes	-	-	-
$A_{iS/t}$	5	7	5
$A_{eS/t}$	5	6	4
$P_{iS/t}$	10	8	9
$P_{eS/t}$	8	5	5
sX_{0-min}	6	6	7

DB_1: $[sX, T_{d/top\_d}, T_{t/top\_t}, A_{iS/t}, \#\,Strokes, L_{iS/t}, L_{eS/t}, T_{d/t}]$
DB_2: $[sX, T_{d/top\_d}, T_{t/top\_t}, A_{iS/t}, \#\,Strokes, A_{eS/t}, P_{eS/t}, sX_{0-min}]$
DB_3: $[sX, T_{d/top\_d}, T_{t/top\_t}, T_{iS/t}, L_{iS/t}, T_{d/t}, P_{eS/t}, sX_{0-min}]$

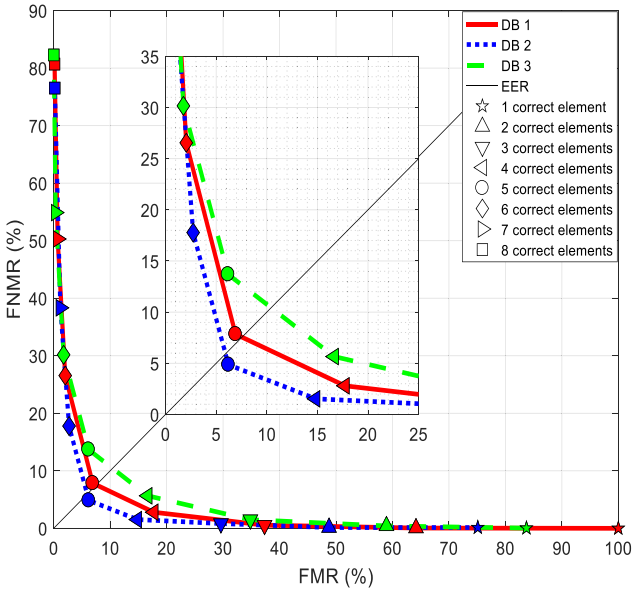

FIGURE 9. DET curves using unprotected reference templates (comparison based on the number of correct elements).

the features considered, it seems that these 3 are the most discriminative.

Regarding the graphs of Fig. 9, in each case, 8 discrete values marked with different symbols are shown. The symbols represent the percentage of probe templates that, during the comparison with the corresponding reference template, presented at least (from right to left) 1, 2, ..., 7 and 8 correct elements. The discrete values have been connected using a straight line to appreciate that the disposition of the results corresponds to DET curves. Table 4 gathers the numerical value of the reported error rates.

TABLE 4. Results achieved using unprotected reference templates.

No. of equal elements between the probe template and the reference template	DB_1		DB_2		DB_3	
	FMR (%)	FNMR (%)	FMR (%)	FNMR (%)	FMR (%)	FNMR (%)
1	100	0	75.11	0.14	83.72	0.03
2	64.16	0.05	48.76	0.14	58.93	0.41
3	37.34	0.55	29.62	0.83	34.83	1.50
4	17.72	2.8	14.82	1.53	16.65	5.65
5	**6.91**	**7.85**	**6.21**	**4.86**	**6.16**	**13.6**
6	2.04	26.55	2.74	17.78	1.76	30.15
7	0.7	50.3	1.18	38.33	0.34	54.88
8	0.16	80.7	0.2	76.53	0.02	82.28

According to the results, in all databases the best performing conditions (lowest FMR and FNMR) are achieved setting the decision threshold at 5 correct elements (points next to the ERR line), reaching FMRs and FNMRs below 7% and 14%, respectively (see Table 4). Based on this, it was decided to configure the RS coding to tolerate up to 3 errors in the probe templates.

C. VERIFICATION PERFORMANCE

After finding the optimal configuration parameters (feature quantisation levels, 8-feature representation and error correcting code tolerance), the verification performance of the FV scheme was evaluated. Results are gathers in Table 5.

TABLE 5. Verification performance achieved by FV scheme.

Maximum No. of errors in the probe template	DB_1		DB_2		DB_3	
	FMR (%)	FNMR (%)	FMR (%)	FNMR (%)	FMR (%)	FNMR (%)
3	**6.91**	**7.85**	**6.21**	**4.86**	**6.16**	**13.6**
2	2.04	26.55	2.74	17.78	1.76	30.15
1	0.7	50.3	1.18	38.33	0.34	54.88
0	0.16	80.7	0.2	76.53	0.02	82.28

It should be noted that, the error rates achieved by the template protection system are the same as those obtained during the configuration phase. These results allow us to validate the implemented FV scheme.

As shown, by tolerating up to 3 errors in the probe templates, the results obtained were: 6.91% of FMR with 7.85% of FNMR using DB_1, 6.21% of FMR with 4.86% of FNMR for DB_2, and 6,16% of FMR with 13,6% of FNMR using DB_3. In all experiments, similar error rates were achieved, though the system performance is slightly better on DB_2. In addition, despite having optimized the system to achieve low FMR and FNMR, it should be noted that, by tolerating up to 2 errors, an FMR lower than 3% is achieved (without a significant increase of the FNMR).

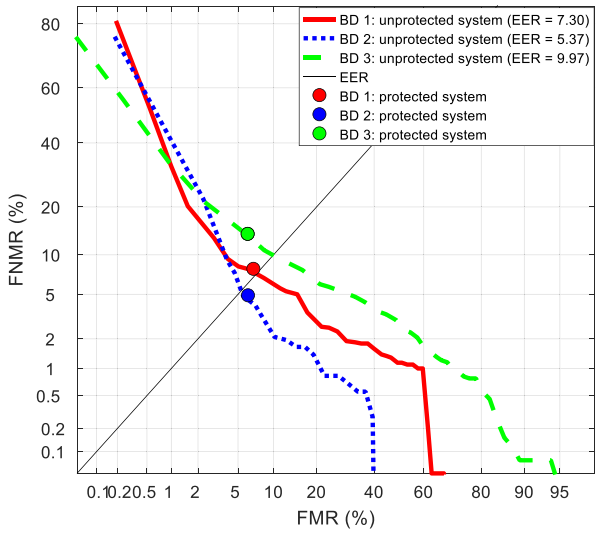

FIGURE 10. DET curves of the unprotected system (comparison based on Euclidean distance), and performance of FV system tolerating up to 3 errors in the probe templates (circle mark).

As described in Section II, the ISO/IEC 24745:2011 standard on biometric information protection states that a BTP system should not degrade the verification performance with respect to the equivalent unprotected system. To check the compliance with this requirement, a signature recognition system based on the same fixed-length templates as our FV scheme, was implemented and evaluated. In this case, the similarity scores between the templates Q and I were computed using the Euclidean distance, (d_{Euc}), defined as follows:

$$d_{Euc}(Q, I) = \sqrt{\sum_{f=1}^{F} (Q_f - I_f)^2}$$

where F represents the number of features included in the templates.

Fig. 10 shows the DET curves obtained for the unprotected system and the performance of the FV system tolerating up to 3 errors in the probe templates (circle mark). In our FV scheme, the error correction code does not allow to operate at the multiple operating points of the unprotected system. Thus, for comparison purpose, we will consider an FMR fixed value (the one corresponding to the protected system) to analyse the FNMR of both systems. As can be observed, the circle marks (protected system performance) are practically located on the DET curves. These results reveal that, at the operating points supported by the protection scheme, the performance is almost preserved with respect to the baseline unprotected system.

V. IRREVERSIBILITY AND UNLINKABILITY

According to the ISO/IEC 24745:2011 standard the BTP systems must also meet the properties of irreversibility and unlinkability. In our case, the irreversibility of the proposed

system can be mathematically quantified. Given that the vault has 300 points and only 8 of them are genuine, the expected number of combinations that need to be evaluated by an attacker using brute force, is $C(300, 8) = 1.5 \times 10^{15}$ (corresponding with a security of 15 bits). Hence, the probability of a successful attack in our system is $\left(1/(1.5 \times 10^{15})\right) = 6.7 \times 10^{-16}$. On the other hand, the stored redundant symbols do not reveal information about the protected templates. However, if an attacker in the attempt to decode the vault uses this redundancy, the success probability will be increased, but not significantly.

While the proposed system provides high security in terms of irreversibility, it does not meet the unlinkability and renewability properties. Following the hybrid approach [43] mentioned in Section II.C, this problem could be addressed by first applying a transformation function to the original template and then generating the vault from the transformed template. A possible transformation is to combine the original template with a user password (independent of the key involved in the vault) using the binary XOR function. This password-based transformation allows the creation of revocable vaults and prevents cross-comparisons of vaults across different applications.

At the same time, by using this hybrid approach an improvement in template security could be achieved. Assuming the system is able to protect the password, if an impostor gets the genuine points from the vault (which correspond to the transformed template), he will not be able to reverse the transformation and recover the original template. Note that, the XOR operation is irreversible if only the result is known. However, the impact of this modification on the system performance should be analysed.

VI. TIME PERFORMANCE

In the design of a verification system the processing time is relevant, and the requirements of the application scenario play a fundamental role in this aspect. In scenarios where a high security is demanded, the priority is to guarantee low error rates, although that brings longer processing time. Nevertheless, for scenarios that require user interaction (e.g. access control), it is important that the system responds immediately.

With the goal of having a more complete evaluation of the proposed FV scheme, it was decided to analyse the time performance of the proposed system. Two scenarios were considered for this evaluation: *i*) the time elapsed in verifying a probe template and obtaining its key (when applicable), and *ii)* the time elapsed only until the verification (without recovering the key). The probe templates were grouped according to the number of errors, and then the time performance was calculated for each group. The system was implemented in MATLAB®using a PC Intel Core ×64 i7-6700 CPU at 3.40GHz with 16GB RAM.

Fig. 11 shows the results obtained, which are very similar in all databases. In templates that show from 0 to 3 errors, the process of verification and recovery of the key lasted 40ms approximately. Although, when the probe and reference

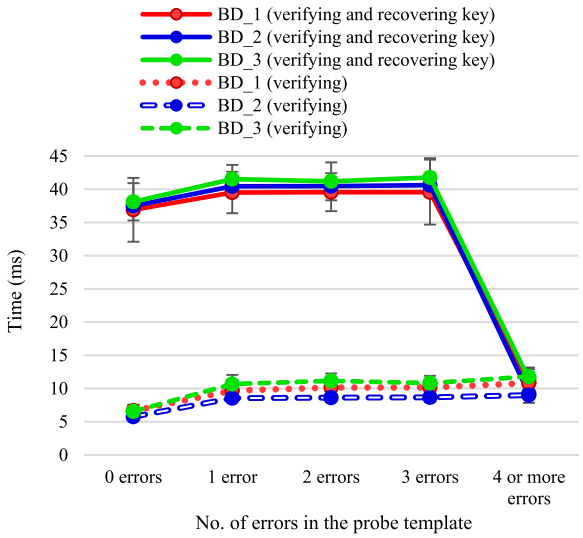

FIGURE 11. Average time elapsed for classifying one sample with respect to the number of errors in the probe templates.

template were equal, this process took less time (37ms) since no error had to be corrected.

On the other hand, if during the decoding phase the templates are only classified as correct or incorrect (without extracting the key from the vault), the time elapsed is around 10ms, at the vectors with 3 or fewer errors.

In the case of probe templates with 4 or more errors, the time elapsed in both scenarios is the same (around 10ms). This result was expected because during the decoding phase when a user is classified as incorrect, no key is extracted from the vault.

As can be seen, the difference between the results obtained in each scenario is associated with the time spent by the system to recover the correct user key.

VII. CONCLUSIONS AND FUTURE WORKS

In this paper we have proposed a FV scheme based on fixed-length templates with application to DSV, where only 15 global features of the signature have been considered to form the templates. The system performance has been evaluated using three databases: a proprietary collection of signatures and the public databases MCYT and BioSecure. As an outcome, protected references more robust against attacks are obtained, while the verifications accuracy is not significantly degraded with respect to an equivalent unprotected system.

Evaluation results show that, the proposed FV scheme can achieve low error rates tolerating up to 3 errors in the probe templates (FMR of 6.91% and FNMR of 7.85% using MCYT database, FMR of 6.21% and FNMR of 4.86% with the proprietary database, and FMR of 6.16% and FNMR of 13.6% for BioSecure database). However, these rates could be individually reduced, adjusting during the initial phase, the configuration parameters according to the desired optimization criterion (e.g. minimum FMR accepting high

FNMR, or vice versa). Moreover, very low times were spent by the system during verification phase (around 40ms).

It was learned that all the features do not achieve their best performance using the same quantisation levels. Also, it was confirmed that the system performance varies depending of the features involved in the representation vector. Therefore, the individual choice of quantisation levels for each feature and the correct selection of the representation features improve the system performance.

Once the operating methodology of the FV has been studied, we consider that in applications where it is not necessary to ensure a key, a simplified version of this scheme could be used. Alternatively, during the enrolment just the RS encoding would be applied to the reference template, storing for each enrolled user only the redundant symbols obtained. Then, during verification, the RS decoder using the corresponding redundancy can determine whether the user is correct. This alternative eliminates the generation of the vault set, avoiding storing any sensitive information of the enrolled biometric characteristic.

As a future work, we will extend this study, analysing the robustness of the system against skilled forgeries. Also, the system performance could be evaluated using a personal 8-feature combination per user, instead of a unique combination for the entire database.

Also, in order to counter the attacks described in Section II.C, we intend to adapt the hybrid approach of [43] to our particular signature case. To that end, we plan to use the XOR logic function to combine the original template with a password (independent of the user key) before the vault creation. Finally, we will protect the generated vault by applying an encryption technique. In this way, renewability and unlinkability can be achieved while the security is improved. Consequently, the influence of the initial transformation on the system performance should be studied.

REFERENCES

[1] A. K. Jain and A. Kumar, *Second Generation Biometrics: The Ethical, Legal and Social Context*, vol. 11. Dordrecht, The Netherlands: Springer, 2012, doi: 10.1007/978-94-007-3892-8.

[2] A. K. Jain and K. Nandakumar, "Biometric authentication: System security and user privacy," *Computer*, vol. 45, no. 11, pp. 87–92, Nov. 2012.

[3] S. Prabhakar, S. Pankanti, and A. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security Privacy*, vol. 1, no. 2, pp. 33–42, Mar. 2003.

[4] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Proc. Int. Conf. Audio Video Based Biometric Person Authentication*, 2001, pp. 223–228.

[5] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, 2001.

[6] K. Nandakumar, A. K. Jain, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.*, vol. 2008, Jan. 2008, Art. no. 113.

[7] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 9, pp. 1489–1503, Sep. 2007.

[8] A. K. Jain, F. D. Griess, and S. D. Connell, "On-line signature verification," *Pattern Recognit.*, vol. 35, no. 12, pp. 2963–2972, 2002.

[9] R. Sanchez-Reillo, J. Liu-Jimenez, and R. Blanco-Gonzalo, "Forensic validation of biometrics using dynamic handwritten signatures," *IEEE Access*, vol. 6, pp. 34149–34157, 2018.

[10] H. Gamboa and A. Fred, "A behavioural biometric system based on human computer interaction," *Proc. SPIE, Biometric Technol. Hum. Identificat.*, vol. 5404, pp. 381–392, Aug. 2004.

[11] F. Leclerc and R. Plamondon, "Automatic signature verification: The state of the art–1989-1993," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 8, no. 3, pp. 643–660, Jun. 1994.

[12] R. Plamondon and S. Srihari, "Online and off-line handwriting recognition: A comprehensive survey," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 22, no. 1, pp. 63–84, Jan. 2000.

[13] Y. J. Lee, K. Bae, S. J. Lee, K. R. Park, and J. Kim, "Biometric key binding: Fuzzy vault based on iris images," in *Proc. Int. Conf. Biometrics (ICB)*, Seoul, South Korea, vol. 4642, Aug. 2007, pp. 800–808.

[14] R. Blanco-Gonzalo, R. Sanchez-Reillo, J. Liu-Jimenez, and O. Miguel-Hurtado, "Performance evaluation of handwritten signature recognition in mobile environments," *IET Biometrics*, vol. 3, no. 3, pp. 139–146, Sep. 2014.

[15] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, A. Satue, M. Faundez-Zanuy, V. Espinosa, I. Hernaez, J.-J. Igarza, C. Vivaracho, D. Escudero, and Q.-I. Moro, "MCYT baseline corpus: A bimodal biometric database," *IEE Proc.-Vis. Image Process.*, vol. 150, no. 6, p. 395, 2003.

[16] J. Ortega-Garcia *et al.*, "The multiscenario multienvironment biosecure multimodal database (BMDB)," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 6, pp. 1097–1111, Jun. 2010.

[17] A. K. Jain, K. Nandakumar, and A. Nagar, "Fingerprint template protection: From theory to practice," in *Security and Privacy in Biometrics*. London, U.K.: Springer, 2013, pp. 187–214, doi: 10.1007/978-1-4471-5230-9.

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

[19] K. Simoens, B. Yang, X. Zhou, F. Beato, C. Busch, E. M. Newton, and B. Preneel, "Criteria towards metrics for benchmarking template protection algorithms," in *Proc. 5th IAPR Int. Conf. Biometrics (ICB)*, Mar. 2012, pp. 498–505.

[20] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proc. IEEE Int. Symp. Inf. Theory*, vol. 38, Jun./Jul. 2002, p. 408,

[21] A. Juels and M. Wattenberg, "Fuzzy commitment scheme," in *Proc. ACM Conf. Comput. Commun. Secur.*, 1999, pp. 28–36.

[22] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, 2008.

[23] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *Eurasip J. Inf. Secur.*, vol. 3. London, U.K.: Springer, 2011, pp. 1–25.

[24] 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.

[25] 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.

[26] A. C.-C. Yao, "How to generate and exchange secrets," in *Proc. 27th Annu. Symp. Found. Comput. Sci. (sfcs)*, Oct. 1986, pp. 162–167.

[27] C. Fontaine and F. Galand, "A survey of homomorphic encryption for nonspecialists," *EURASIP J. Inf. Secur.*, vol. 1, pp. 41–50, Jan. 2009.

[28] S. Barman, H. P. H. Shum, S. Chattopadhyay, and D. Samanta, "A secure authentication protocol for multi-server-based E-healthcare using a fuzzy commitment scheme," *IEEE Access*, vol. 7, pp. 12557–12574, 2019.

[29] S. Barman, A. K. Das, D. Samanta, S. Chattopadhyay, J. J. P. C. Rodrigues, and Y. Park, "Provably secure multi-server authentication protocol using fuzzy commitment," *IEEE Access*, vol. 6, pp. 38578–38594, 2018.

[30] R. Dwivedi, S. Dey, M. A. Sharma, and A. Goel, "A fingerprint based crypto-biometric system for secure communication," 2018, *arXiv:1805.08399*. [Online]. Available: https://arxiv.org/abs/1805.08399

[31] T. Kivinen and M. Kojo, "More modular exponential (MODP) Diffie-Hellman groups for Internet key exchange (IKE)," Internet Eng. Task Force, Fremont, CA, USA, Tech. Rep. RFC 3526, May 2003.

[32] E. Maiorana, P. Campisi, 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. Conf. Comput. Vis. Pattern Recognit. Workshops*, Jun. 2008.
[34] M. Freire-Santos, J. Fierrez-Aguilar, and J. Ortega-Garcia, "Cryptographic key generation using handwritten signature," *Proc. SPIE*, vol. 6202, pp. 225–231, Apr. 2006.
[35] A. Kholmatov and B. Yanikoglu, "Biometric cryptosystem using online signatures," in *Proc. Int. Symp. Comput. Inf. Sci.*, vol. 4263, 2006, pp. 981–990.
[36] 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 Security*, vol. 7, no. 1, pp. 269–282, Feb. 2012.
[37] M. R. Freire, J. Fierrez, and J. Ortega-Garcia, "Dynamic signature verification with template protection using helper data," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Mar. 2008, pp. 1713–1716.
[38] M. Gomez-Barrero, J. Fierrez, and J. Galbally, "Variable-length template protection based on homomorphic encryption with application to signature biometrics," in *Proc. 4th Int. Conf. Biometrics Forensics (IWBF)*, Mar. 2016.
[39] M. Gomez-Barrero, J. Fierrez, J. Galbally, E. Maiorana, and P. Campisi, "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.
[40] M. Gomez-Barrero, J. Galbally, A. Morales, and J. Fierrez, "Privacy-preserving comparison of variable-length data with application to biometric template protection," *IEEE Access*, vol. 5, pp. 8606–8619, 2017.
[41] S. B. Wicker and V. K. Bhargava, *Reed-Solomon Codes and Their Applications*. Piscataway, NJ, USA: IEEE Press, 1994.
[42] W. J. Scheirer and T. E. Boult, "Cracking fuzzy vaults and biometric encryption," in *Proc. Biometrics Symp. (BSYM)*, Sep. 2007, pp. 1–6.
[43] K. Nandakumar, A. Nagar, and A. K. Jain, "Hardening fingerprint fuzzy vault using password," in *Advances in Biometrics*. Berlin, Germany: Springer, 2007, pp. 927–937, doi: 10.1007/978-3-540-74549-5_97.
[44] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy vault for fingerprints," in *Proc. Int. Conf. Audio Video Based Biometric Person Authentication*, vol. 3546, 2005, pp. 310–319.
[45] Y. Wang and K. Plataniotis, "Fuzzy vault for face based cryptographic key generation," in *Proc. Biometrics Symp. (BSYM)*, Sep. 2007, pp. 1–6.
[46] A. Kumar and A. Kumar, "Development of a new cryptographic construct using palmprint-based fuzzy vault," *EURASIP J. Adv. Signal Process.*, vol. 2009, no. 1, Dec. 2009, Art. no. 967046.
[47] K. Nandakumar and A. K. Jain, "Multibiometric template security using fuzzy vault," in *Proc. IEEE 2nd Int. Conf. Biometrics, Theory, Appl. Syst. (BTAS)*, Sep./Oct. 2008, pp. 1–6.
[48] R. Tolosana, R. Vera-Rodriguez, J. Ortega-Garcia, and J. Fierrez, "Preprocessing and feature selection for improved sensor interoperability in online biometric signature verification," *IEEE Access*, vol. 3, pp. 478–489, 2015.
[49] R. Ros-Gomez, H. C. Quiros-Sandoval, R. Blanco-Gonzalo, and R. Sanchez-Reillo, "A comparative analysis on the performance of static handwritten verification systems on realistic scenarios," in *Proc. IEEE Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2016, pp. 1–7.

WENDY PONCE-HERNANDEZ received the degree in telecommunication engineering from the Technological University of Havana Jose Antonio Echeverria, Cuba, and the master's degree in electronic systems engineering from the University Carlos III of Madrid (UC3M), in 2015, where she is currently pursuing the Ph.D. degree. Since 2015, she has been researching in biometric template protection with the University Group for Identification Technologies (GUTI), UC3M.

RAMON BLANCO-GONZALO received the Ph.D. degree in biometric recognition systems from the University Carlos III of Madrid (UC3M), in 2016. He was a Researcher with the UC3M. In that period, he has been a member and an editor of international standards within the ISO/IEC JTC1/SC37-Biometrics. Afterwards, he was a Biometric Analyst in the banking sector focused on digital and handwritten signature processes. He is currently a Biometrics Senior Consultant with eu-LISA.

JUDITH LIU-JIMENEZ received the degree in telecommunication engineering from the Polytechnic University of Madrid, in 2004, and the Ph.D. degree in electronics from the University Carlos III of Madrid (UC3M), in 2010. Since 2004, she has been with the UC3M. She has participated in several national and European funded projects, besides working on ID management, evaluation, and anti-spoofing mechanisms. Her focus of work is on biometrics and hardware/software codesign, specifically for iris biometrics.

RAUL SANCHEZ-REILLO received the Ph.D. degree. He is currently a Full Professor with the University Carlos III of Madrid. He is also the Head of the University Group for Identification Technologies (GUTI), where he is involved in project development and management concerning a broad spectrum of applications, ranging from social security services to financial payment methods. He has participated in several European projects, such as eEpoch and BioSec, by virtue of being the WP Leader. He is an expert in security and biometrics. He served as a member of the SC17, SC27, and SC37 Standardization Committees. He is also the Spanish Chair of SC17 and the Secretariat of SC37.