Abstract—Biometric cryptosystems have been applied to secure secret keys for encryption and digital signatures by means of biometric traits, e.g., fingerprint, face, etc., where the fuzzy vault (FV) mechanism has been extensively employed. Recently, the authors proposed a FV system based on the offline signature images, so that digitized documents can be secured with the embedded handwritten signatures. However, the FV design concerns mostly with alleviating biometric variability with less focusing on its power in discriminating forgeries. Accordingly, the decoding accuracy of implementations is below the level required in practical banking transactions. On the other hand, signature verification (SV) systems have shown higher accuracy in discriminating forgeries. In this paper, accuracy of signature-based biometric cryptosystems is enhanced by cascading SV and FV modules. Signature samples are first verified by the SV module. Then, only verified samples are processed by FV decoders for unlocking cryptographic keys. Hence, the upper limit of the false accept rate is determined by the more accurate SV module. Simulation results obtained with the Brazilian signature database indicate the viability of the proposed approach. Cascaded SV-FV system increases decoding accuracy by about 35% compared to the pure FV systems.

Keywords—Biometric cryptosystems; signature-based fuzzy vault; offline signature verification; cascaded biometric cryptosystems and biometric classifiers.

I. INTRODUCTION

Cryptography schemes like encryption and digital signature have been employed to enforce confidentiality and integrity of information, respectively. These schemes rely on secret keys that are too long to be guessed by impostors. However, they are also too long to be memorized by legitimate users. This key management problem maybe alleviated by applying a password-token scenario where a cryptographic key is secured by means of a short easy to remember password stored in a user token, e.g., a smart card. A legitimate person must provide a valid token and a correct password to retrieve his cryptographic key, and to access secured information. However, this scenario does not provide a trusted tool for user identification. For instance, any person who guesses or steals the password can bypass the cryptographic algorithm and break system security.

Biometric cryptosystems (bio-cryptography) have been introduced to enforce user identification of cryptographic applications [1]. Instead of simple passwords, biometrics like fingerprint, face, voice, handwriting, etc., are employed to secure the cryptographic keys. Although biometric traits are attached to user identity and they are harder to be stolen or forgotten, the fuzzy nature of biometrics may produce inaccurate recognition results. Variability of intra-personal samples and similarity of inter-personal samples may result in rejection of legitimate users and acceptance of impostors, respectively.

Fuzzy vault (FV) is a bio-cryptography mechanism that alleviates variability of biometrics [2]. During enrollment, a biometric template locks user cryptographic key in a FV. During authentication, a user provides a query biometric sample to release the locked key. A FV can be considered as an error correction decoder. The key is unlocked only if the dissimilarity between a query and a template are within the error correction capability of the FV.

In literature, FVs are realized using various physiological biometrics like fingerprints [3] and iris [4]. However, application of this scheme to the behavioral offline signature images have shown too much fuzziness to decode a FV with acceptable level of accuracy [5].

Recently, the authors have proposed a FV based on offline signature images by employing a multi-feature extraction and boosting feature selection (BFS) approach based on the dissimilarity representation (DR) [6]. The proposed system is employed to produce digital signatures by means of handwritten signatures [7]. Accordingly, details of digital security is transparent, as users continue to employ their traditional handwritten signature, while benefiting the security tools.

Signature-based FVs are designed in a dissimilarity space, where distances between feature pairs are the space constituents. Feature representations selected in such dissimilarity spaces have shown acceptable level of robustness against signature variability, while they lack discriminative power against skilled forgeries [6].

In literature, the limited discriminative power of FVs is alleviated by using an additional password, so that the false accept rate (FAR) is reduced without significantly affecting the false reject rate (FRR) [9]. This method has been applied to the signature-based FV systems [6], where enhancing system accuracy comes with the expense of the user inconvenience.

In this paper, a novel user-convenient approach is proposed
features overlap substantially, enough genuine points are located and they are used to reconstruct the polynomial equation, and hence the locked key.

Figure 1 illustrates how a FV locks and unlocks a cryptographic key by means of a biometric trait. First, a cryptographic key $K$ encodes some polynomial $p$. For instance, $K$ is split into $k+1$ strings of length $l$-bit and constitutes a coefficient vector $C = \{c_0, c_1, c_2, \ldots, c_k\}$. A polynomial $p$ of degree $k$ is encoded using $C$, where $p(x) = c_k x^k + c_{k-1} x^{k-1} + \ldots + c_1 x + c_0$. Second, the polynomial is locked by a biometric template $T$. To this end, a feature representation $F^T = \{f_i^T\}_{i=1}^t$ is extracted from $T$. The $t$ elements of $F^T$ are then quantized in $l$-bit strings and constitute a locking set $A = \{a_i\}_{i=1}^t$, where $a_i$ is the quantized value of the feature $f_i^T$. Then, $A$ is projected on $p$, and constitutes the set $p(A) = \{p(a_i)\}_{i=1}^t$ where $p(a_i) = c_k a_i^k + c_{k-1} a_i^{k-1} + \ldots + c_1 a_i + c_0$.

The points $(A, p(A))$ constitute the genuine vault points. To conceal these points from attackers, $z$ chaff (noise) points $(A, P)$ are generated, where $A = \{a_i\}_{i=t+1}^{i+1}, a_{ji} \neq a_i \forall i \in [t+1, n], i \in [1, t]$, and $P = \{p_i\}_{i=t+1}^{i+1}$, $p_i \neq p(a_i) \forall i \in [t+1, r]$, $r = z + t$. This implies that chaff points neither interfere with genuine points nor lie on the polynomial. Finally, both the genuine point set $(A, p(A))$, and the chaff point set $(A, P)$ are merged to constitute the vault points $(A, \tilde{P})$, where $A = A \cup \tilde{A}$, and $\tilde{P} = p(A) \cup \tilde{P}$. The vault $FVT$ is stored as a user template which consists in the vault points $(A, \tilde{P})$, and the vault parameters $(k, t)$.

To learn $K$ from the vault $FVT$, the set $(A, p(A))$ should be firstly isolated by filtering the chaff points $(A, P)$ out of the vault set $(A, \tilde{P})$. Then any subset of only $k+1$ genuine points in $(A, p(A))$, could be used to reconstruct the polynomial $p$ of degree $k$. To this end, a feature representation $F^Q = \{f_j^Q\}_{j=1}^t$ is extracted from a biometric query sample $Q$. The $t$ elements of $F^Q$ are then quantized in $l$-bit strings, to constitute an unlocking set $B = \{b_j\}_{j=1}^t$, where $b_j$ is the quantized value of the feature $f_j^Q$. Then, the chaff points are filtered by matching items of $B$ against all items in $A$. This process results in a matching set $(A, \tilde{P}) = (B \cap A), p \leftarrow (B \cap \tilde{A})$, where $p \leftarrow (B \cap \tilde{A})$ represents the projection of the matching features on the polynomial space.

It is important to note that, for practical FV implementations, length $t$ of the locking/unlocking set must be compact, as it impacts the decoding complexity. For the example shown in Figure 1, only 20 genuine points $(t = 20)$ are encoded in the FV, by projecting them on the polynomial space $p$. During decoding, only 10 of them could be isolated and added to the matching set. For instance, point 1 is isolated by means of the unlocking element $b_1$, where $b_1 = a_1$. While, the other 10 genuine points could not be isolated by means of the corresponding unlocking elements. For instance, point 2 could not be isolated from chaffs as $a_2$ did not match with the corresponding unlocking element $b_2$. Also, there are 4 chaff points added to the unlocking list and considered as noise $\delta$. For instance, point 3 is incorrectly added to the matching set because $b_3$ matches with $a_{ji}$.

Since not all the genuine points are needed to reconstruct the polynomial, a FV is considered as a decoder with error correction capacity. If the dissimilarity between the locking
set $A$ and the unlocking set $B$ is within the error correction capacity $\epsilon$, the polynomial $p$ (and hence, the key $K$) can be unlocked. Otherwise, the query $Q$ fails to unlock the key.

**B. Locking fuzzy vaults with offline signatures**

Figure 2 illustrates a way to encode FVs with the offline signature images. In this example, extended shadow code (ESC) features are extracted from signature images [11]. An ESC consists in the superposition of bar mask array over the binary image of a handwritten signature. Each bar is assumed to be a light detector related to a spatially constrained area of the 2D signal. A shadow projection is defined as the simultaneous projection of each black pixel into its closest horizontal, vertical and diagonal bars. A projected shadow turns on a set of bits distributed uniformly along the bars. After all the pixels of a signature are projected, the number of on bits in each bar is counted and normalized to the range of $[0,1]$ to constitute the ESC feature value. The ESC feature vectors $F_{T} = \{f_{T}^{i}\}_{i=1}^{Q}$ and $F_{Q} = \{f_{Q}^{j}\}_{j=1}^{Q}$ are extracted from the template signature $T$ and the query sample $Q$, respectively. Then, they are quantized in $b$-bits and produce the FV locking set $A$ and the unlocking set $B$, respectively, where $A = \{a_{i}\}_{i=1}^{T} = \{(i, f_{T}^{i})\}_{i=1}^{T}$ and $B = \{b_{j}\}_{j=1}^{Q} = \{(j, f_{Q}^{j})\}_{j=1}^{Q}$. Accordingly, a locking element $a_{i}$ matches an unlocking element $b_{j}$ only if they have identical indexes and feature values, i.e., when $i = j$ and $f_{T}^{i} = f_{Q}^{j}$.

Due to signature variability, it is not easy to find enough matching features to unlock the FV. For the above example, despite the two signature images are similar, only half of the extracted features are matching (matching error = 10). Accordingly, the cryptographic key can be unlocked only if the FV error correction capacity $c = 10$. Practical FVs have lower correction capacity (for 128-bit cryptographic keys and locking size $t = 20$, $c = 6$), so that even this stable query image cannot unlock the FV.

It is clear that accuracy of a FV relies on the extend to which two intra-personal signature representations are similar, and two inter-personal representations are dissimilar. This motivates designing the FV based on a dissimilarity representation (DR) instead of the traditional feature representation (FR).

**C. Dissimilarity-based fuzzy vault design**

The DR approach is introduced to the pattern recognition community by Pekalska et al., [13]. Instead of training classifiers in the FR space, some proximity measure produces an alternative classification space, called a DR space (for a review on application of DR approach to SV, see [14]). Recently, the authors have proposed a dissimilarity-based approach to design FV systems [15]. Error correction capacity $\epsilon$ of a FV is considered as a threshold in a dissimilarity space by which a FV classifies genuine and impostor samples.

Figure 3 illustrates this design approach. FV functionality is modeled as follows:

$$ FV^{T}(Q) = \text{sign}(\epsilon - (\delta_{A}^{QT} + \delta')) $$

where, $FV = 1$ implies that the locked cryptographic key is released, and $FV = 0$ otherwise, $\epsilon$ is the error correction capacity of the FV decoder, and $\delta'$ is the error term due to false matching between unlocking points and the chaff points.

An adaptive dissimilarity measure between a locking template $T$ and an unlocking query $Q$ is defined as follows:

$$ \delta_{A}^{QT} = \sum_{i=1}^{t}(\delta_{A_{i}}^{QT}), \quad \delta_{A_{i}}^{QT} = \begin{cases} 0 & \text{if } (\delta_{i}^{QT} < \delta_{i}) \\ 1 & \text{otherwise} \end{cases} $$

where, $\delta_{i}^{QT} = \| f_{i}^{Q} - f_{i}^{T} \|$ is the distance between the two signature images as measured by a feature $f_{i}$, and $\delta_{i}$ is the expected intra-personal variability of signature images when measured by feature $f_{i}$.

An unlocking element $f_{i}^{Q}$ is matched against all locking elements $\{f_{i}^{T}\}_{i=1}^{T}$, where it succeeds to locate the corresponding element only if their dissimilarity is within the modeled dissimilarity threshold $\delta_{i}$. To correctly decode the FV, the overall dissimilarity between the locking and unlocking messages $\delta_{A}^{QT}$, besides the noise error $\delta'$ (resulting from false matching with chaffs), should not exceed the error correction capacity $\epsilon$ of the decoder.
features are injected in this space, and a BFS algorithm [16] selects the best features that minimize $\sigma^2_A$ in case that $Q$ and $T$ come from same person, and that maximize this measure when the two signature images belong to different persons. In this space, expected variability range $\delta_i$ for each feature $f_i$ is learned. In the authentication time, two feature instances $f_i^Q$ and $f_i^T$ are considered matching if their difference is within the expected variability $\delta_i$. Moreover, impact of chaff points $\delta_i$ is minimized through generation of chaff points adaptively according to feature expected variability, so it is less likely that a genuine unlocking point matches with a chaff point [15].

Although this approach alleviates variability of signature images, complex decision boundaries between genuine signatures and forgeries cannot be modeled accurately with the simple FV functionality (using a simple dissimilarity threshold). Besides, only concise feature representations are allowed to encode a FV, and feature values must be quantized, which degrades FV discriminative power. On contrary, these limitations do not apply to designing SV systems. SV systems have therefore shown higher discriminative power, specially in detecting skilled forgeries [6]. In this paper, a SV module is cascaded with the signature-based FV for higher accuracy.

III. SIGNATURE VERIFICATION MODULE

SV systems are either writer-independent (WI) or writer-dependent (WD). For WI-SV systems, a global classifier is designed using a development database and it is used to verify signatures of real users who are enrolled after the design phase. On the other hand, WD-SV systems consist in individual classifiers that are designed after user enrollment. Recently, the authors proposed a methodology that adapts WI-SV systems to specific users producing more secure, simpler, and more accurate WD-SV systems [8]. It has been demonstrated that signature representations that are designed in a dissimilarity space and embedded in the global WI-SV (as proposed by Rivard et al., [12]), can be further tuned to individuals by executing a BFS process in the feature space. The feature-based WD representations have demonstrated higher discriminative power, specially in detecting skilled forgeries.

In this paper, this methodology is applied to produce WD-SV classifiers that boost the discriminative power of signature-based FVs. To this end, signature representations of huge dimensionality $M$ are extracted from a development database and used to design a WI-SV system. The universal representation embedded in this system is extracted and translated from the dissimilarity space to a feature space of reduced dimensionality $L << M$, where it is possible to build a WD-SV using limited user samples (Details of designing the universal representation is out of the scope of this paper, and more details are found in [8]). Then, a WD-SV is designed by executing a BFS process in the reduced feature space producing a compact representation $F$ of dimensionality $N < L << M$.

Figure 4 illustrates the produced SV classifier in the verification mode. A signature representation $F^Q = \{f_i^Q\}_{i=1}^N$ is extracted from a query signature $Q$ according to the WD representation $F$. A feature $f_i^Q$ shares in the final classification by a share $S_i$ that relies on its expected accuracy. Finally, the total score is compared to a classification threshold $\theta$.

Functionality of the SV classifier is modeled as follows:

$$SV(Q) = sign(S^Q - \theta).$$ (3)

where

$$S^Q = \sum_{i=1}^{N} S_i^Q, \quad S_i^Q = \begin{cases} p_i^{left} & \text{if } (f_i^Q < d_i) \\ p_i^{right} & \text{otherwise} \end{cases}$$ (4)

$S_i^Q$ is the classification share based on a specific feature $f_i^Q$, $p_i^{left}$, $p_i^{right}$ represent confidence of a decision taken by a feature $f_i^Q$, when feature value lies to the left or to the right of the splitting threshold $d_i$, respectively. Refer to [8] for more detailed algorithms of the SV design process.

It is important to note that a similar BFS approach is applied to design the SV classifier as that for the FV design. However, instead of running BFS algorithm in a dissimilarity space, SV learning operates in the original feature space, which have demonstrated higher discriminative power to detect impostors. Moreover, weighted feature selection is also employed for higher accuracy, where a feature share in the classification decision according to its classification ability. Finally, the
representation \( \bar{F} \) selected in the feature space is different than the representation \( F \) selected in the dissimilarity space for FV encoding, and it has higher dimensionality \( N > t \).

IV. A Cascaded SV-FV System

The proposed cascaded SV-FV approach alleviates the low accuracy level of FV decoders by means of the higher discriminative power of SV classifiers. Figure 5 illustrates the proposed cascaded SV-FV system in the verification mode. First, a feature representation \( FQ \) is extracted from a query signature \( Q \) according to the WD-SV representation stored in system database. The WD-SV classifier is used to verify the signature sample as illustrated in Figure 4. Since SV classifiers have demonstrated higher discriminative power than that of the FV systems, so a range of forgeries are filtered at this step.

Then, the FV module is triggered only if \( Q \) is verified as a genuine signature, i.e., \( SV(Q) = 1 \). In such case, a feature representation \( FQ \) is extracted from \( Q \) according to the user FV stored in system database. Instead of unlocking a single FV, a set of FV templates \( \{FVT_{i}\}_{i=1}^{R} \) are used for improved recognition. Every FV is unlocked as illustrated in Figure 3, where a FV produces a positive label \( (FV(Q) = 1) \) when it is successfully unlocked. Finally, a majority vote \( (MV) \) rule is applied so that unlocked cryptographic key \( K \) is released to the user only if majority of FVs are successfully unlocked.

V. Simulation Results

A. Methodology

The Brazilian database [10] is used for proof-of-concept simulations. It contains 7,920 samples of signatures that were digitized as 8-bit grayscale images over 400X1000 pixels at resolution of 300 dpi. This DB contains three types of signature forgery: random, simple and skilled. For random forgery, the forger does not know neither the signer’s name nor the signature morphology. For simple forgery, the forger knows the writer’s name but not the signature morphology. For the skilled forgery, the forger has access to a sample of the signature image. To this end, the feature values are quantized in \( l = 8 \)-bits. To conceal the genuine points, \( z = 180 \) chaff points are injected, so total number of FV points \( r = 200 \). Length of encoded cryptographic key \( K \) is 128-bits, that encodes a polynomial \( p \) of degree \( k = 7 \).

To design the SV module, features are extracted from the 30 genuine signature/user. A single SV classifier is produced for each user, where a BFS process runs for 100 boosting iterations. Average dimensionality of the resulting WD representations is \( (N = 40) \). A zero classification threshold is used in all experiments (\( \theta = 0 \));

To investigate the viability of the proposed cascading approach, both pure FV and SV systems are compared with the cascaded SV-FV system. The impact of fusion of multiple FVs on the decision level is tested by repeating the experiments for single FV decoding \( (R = 1) \) and for multiple FVs where \( R = 15 \).

For the 60 users in the testing set, 40 test samples per user are employed \( (10 \) genuine, 10 random, 10 simple, and 10 skilled forgeries). In case of FV systems (either pure FVs or cascaded SV-FV systems), each test sample is verified against the 30 genuine FV templates, for a total of 72000 \( (60 \times 40 \times 30) \) verification trials. For the SV systems, each of the 40 queries per user are verified once against the SV model, for a total of 2400 \( (60 \times 40) \) verification trials. For performance evaluation, the average error rate \( (AER) \) is computed as follows:

\[
AER = \frac{FRR + FAR_{rand} + FAR_{smp} + FAR_{skl}}{4} \tag{5}
\]

where \( FAR_{rand} \), \( FAR_{smp} \), and \( FAR_{skl} \) are computed for random, simple, and skilled forgeries, respectively.

B. Results

Performance of dissimilarity-based FVs is encouraging. For instance, for a user with signatures shown in Figure 2, the single-type–single-resolution feature extraction technique produced FVs with \( FRR = 100\% \). In this case, out of the 20 locking points, only 10 points are filtered by the unlocking sets \( \text{error} = 10 \). For FVs with error correction capability \( e = 6 \), these errors are not canceled by the FV decoder. On the other hand, applying multi-feature extraction and the dissimilarity-based BFS approach produced FVs with \( AER = 0\% \), as the
mismatch errors are within the FV error correction capacity (error < 6).

However, due to FV scheme limitations, such accurate recognition does not apply for all users in the testing database. For instance, for the user with signatures shown in Figure 6, although his signatures are stable (FRR = 0%), they are easy to imitate by skilled forgeries. For this user, \( \text{FAR}_{\text{skilled}} = 16\% \).

On the other hand, SV classifiers have shown higher accuracy due to the relatively complex model of the SV classifiers, as compared to simple FVs. For instance, for the user with signatures shown in Figure 6, all skilled forgeries are detected by the SV classifier.

In case of the proposed cascaded SV-FV solution, the accuracy is enhanced through filtering most of forgeries by the SV classifier. For instance, impostor signature, shown in Figure 6 (right), could unlock a FV by the template shown in Figure 6 (left), when a pure FV is used. On the other hand, for the cascaded SV-FV solution, this forgery is detected by the SV classifier and it is filtered before triggering the FV. For this user, \( \text{FAR}_{\text{skilled}} = 0\% \), when the cascaded SV-FV system is employed.

Table I presents the simulation results for all users in the testing database. The pure FV system, with a single template \( (R = 1) \), has shown \( \text{AER} = 10.08\% \). When multiple FVs are decoded \( (R = 15) \), the AER is reduced by 18.5% (from 10.08% to 8.21%). However, this comes with expense of increased decoding complexity. For the pure SV systems, the performance is much better \( (\text{AER} = 5.38\%) \). However, this solution produces simple classification labels and can not secure cryptographic keys.

In case of the cascaded SV-FV solution, the AER of cryptographic key decoding is decreased by 35% (from 10.08% to 6.55%). More specifically, accuracy of detecting skilled forgeries is much increased, without high impact on the genuine accept rate, where \( \text{AER}_{\text{skilled}} \) is decreased by 58.65% (from 24.38% to 10.80%). When multiple FVs are fused \( (R = 15) \), the AER is decreased by 13.89% (from 6.55% to 5.64%). Generally, this result is comparable to that of the pure SV classifier. Hence, using the proposed approach facilitates securing cryptographic keys by means of offline signature images with similar level of accuracy as that of the classical SV systems.

VI. CONCLUSION

In this paper, a methodology is proposed for enhancing the accuracy of biometric cryptography systems through cascading of fuzzy vault and biometric classifier modules. The proposed approach is applied to the offline handwritten signature images, and has shown enhanced performance. Considerable amount of impostor samples that are hard to detect by pure FV decoders are filtered by the SV classifier before triggering the FVs. Applying this method, accuracy levels comparable to state-of-the-art SV systems are reached with the less accurate biometric cryptosystems. This proof of concept motivates further research on enhanced design of the cascaded system. For instance, instead of designing the SV and FV modules separately, different system parameters and feature representations can be optimized taking in consideration the overall cascaded system. Also, this proposed approach might be applied to different biometric traits, e.g., fingerprint, face, iris, etc., for enhancing state-of-the-art of biometric cryptosystems.

ACKNOWLEDGMENTS

This work was supported by the Natural Sciences and Engineering Research Council of Canada and BancTec (Canada) Inc.

REFERENCES


