Accepted in Int. Conference on Frontiers in Handwriting Recognition (ICFHR), 2014

Improving Signature-Based Biometric Cryptosystems Using Cascaded Signature Verification–Fuzzy Vault (SV-FV) Approach

George S. Eskander, Robert Sabourin and Eric Granger
Laboratoire d'imagerie, de vision et d'intelligence artificielle
École de technologie supérieure, Université du Québec
Montréal, Canada
Email: geskander@livia.etsmtl.ca, robert.sabourin@etsmtl.ca, eric.granger@etsmtl.ca

***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

DOI: 10.1109/ICFHR.2014.39

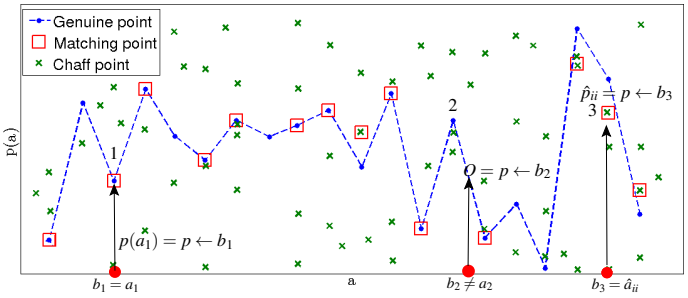


Fig. 1. Illustration of the FV scheme: a locking set $A = \{a_i\}_{i=1}^{t}$ is projected to polynomial p and produces FV genuine points $(A, p(A))$. To conceal genuine points, chaff (noise) points $\{\hat{a_{ii}}, \hat{p_{ii}}\}_{ii=t+1}^{r}$ are added to constitute a FV. To unlock p from the FV, an unlocking set $B = \{b_i\}_{i=1}^{t}$ is matched with all FV points. Due to variability, some unlocking points cannot locate their corresponding points, e.g., $b_2 \neq a_2$. Moreover, some chaffs incorrectly match with the unlocking set, e.g., $b_3 = \hat{a}_{ii}$.

for enhancing the accuracy of signature-based biometric cryptosystems. Since signature verification (SV) systems designed in the original feature space have demonstrated higher discriminative power to detect impostors [8], they can be used to improve the FV systems. Instead of using an additional password, the same signature sample is processed by a SV classifier before triggers the FV decoders. Using this cascaded approach, the high FAR of FV decoders is alleviated by the higher capacity of SV classifiers to detect impostors.

To this end, SV module is designed in the feature space by applying a two-step BFS approach as proposed in [8]. Also, FVs are produced through a dissimilarity based approach as illustrated in [6]. During authentication, a query signature is verified by the SV module. The sample is processed by FV decoders for cryptographic key unlocking, only if it is verified by SV module.

Proof-of-concept simulations are performed using the Brazilian signature DB [10]. The viability of exploiting decisions of SV for improved FV accuracy is investigated by comparing performance of pure FV decoders to the proposed cascaded system. For performance evaluation, genuine and signature samples with different forgeries (random, simple and skilled forgeries) are used.

The rest of this paper is organized as follows. The next section describes the signature-based FV module. Section 3 describes the SV module. Section 4 describes the proposed cascaded SV-FV system. The experimental results and system performance are presented and discussed in Section 5.

II. Signature-Based Fuzzy Vault Module

A. Fuzzy vault scheme

This scheme relies on the concept of polynomial reconstruction [2]. The cryptographic key is used to generate a polynomial equation. Some locking features are extracted from a biometric template and projected on the polynomial. To conceal the locking points from attackers, some noise (chaff) points are added to constitute a FV. For authentication, a query biometric sample produces some unlocking features that filter the chaffs from genuine points. If both locking and unlocking 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 $C = \{c_0, c_1, c_2, ..., c_k\}$. A polynomial p of degree k is encoded using C, where $p(x) = c_k x^k + c_{k-1} x^{k-1} + ... + c_1 x + c_0$. 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 $p(a_i) = c_k {a_i}^k + c_{k-1} {a_i}^{k-1} + ... + c_1 a_i + c_0$.

The points $(A, p(A))$ constitute the genuine vault points. To conceal these points from attackers, z chaff (noise) points $(\hat{A}, \hat{P})$ are generated, where $\hat{A} = \{\hat{a_{ii}}\}_{ii=t+1}^{r}$, $\hat{a_{ii}} \neq a_i \vee ii \in [t+1, r], i \in [1, t]$, and $\hat{P} = \{\hat{p_{ii}}\}_{ii=t+1}^{r}$, $\hat{p_{ii}} \neq p(\hat{a_{ii}}) \vee ii \in [t+1, r]$, $r = z + t$. 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 $(\hat{A}, \hat{P})$ are merged to constitute the vault points $(\tilde{A}, \tilde{P})$, where $\tilde{A} = A \bigcup \hat{A}$, and $\tilde{P} = p(A) \bigcup \hat{P}$. The vault FV^T is stored as a user template which consists in the vault points $(\tilde{A}, \tilde{P})$, and the vault parameters (k, t).

To learn K from the vault FV^T, the set $(A, p(A))$ should be firstly isolated by filtering the chaff points $(\hat{A}, \hat{P})$ out of the vault set $(\tilde{A}, \tilde{P})$. 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 $\tilde{A}$. This process results in a matching set $(\bar{A}, \bar{P}) = ((B \bigcap \tilde{A}), p \leftarrow (B \bigcap \tilde{A}))$, where $p \leftarrow (B \bigcap \tilde{A})$ 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 δ'. For instance, point 3 is incorrectly added to the matching set because b_3 matches with $\hat{a}_{ii}$.

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

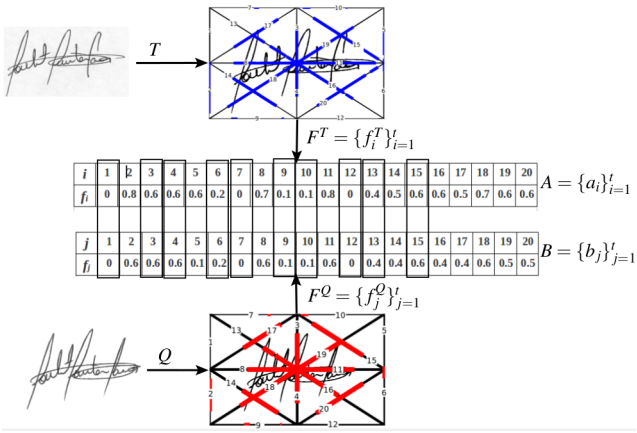


Fig. 2. Illustration of FV lock/unlock with offline signature images: a locking element a_i matches an unlocking element b_j, only if their indexes and feature values are identical.

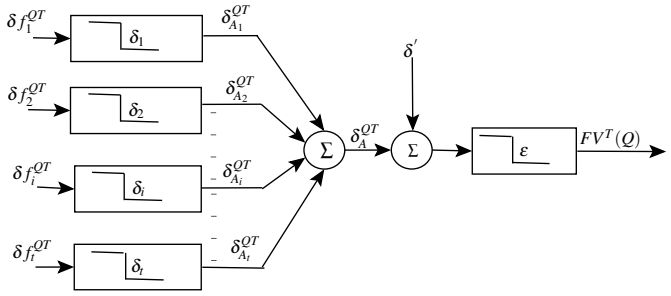


Fig. 3. Dissimilarity-based FV model: every unlocking element f_i^Q is matched against all locking elements $\{f_i^T\}_{i=1}^t$, where it succeeds to locate the corresponding element only if their dissimilarity is within the modeled dissimilarity threshold δ_i. To correctly decode the FV, the overall dissimilarity between the locking and unlocking messages δ_A^{QT}, besides the noise error δ' (resulting from false matching with chaffs), should not exceed the error correction capacity ϵ of the decoder.

set A and the unlocking set B is within the error correction capacity ϵ, 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 $F^T = \{f_i^T\}_{i=1}^t$ and $F^Q = \{f_j^Q\}_{j=1}^t$ are extracted from the template signature T and the query sample Q, respectively. Then, they are quantized in l-bits and produce the FV locking set A and the unlocking set B, respectively, where $A = \{a_i\}_{i=1}^t = \{(i, f_i^T)\}_{i=1}^t$ and $B = \{b_j\}_{j=1}^t = \{(j, f_j^T)\}_{j=1}^t$. 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 $f_i^T = f_j^Q$.

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 $\epsilon = 10$. Practical FVs have lower correction capacity (for 128-bit cryptographic keys and locking size $t = 20$, $\epsilon = 6$), 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 ϵ 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:

$$FV^T(Q) = sign(\epsilon - (\delta_A^{QT} + \delta^{'})). \tag{1}$$

where, $FV = 1$ implies that the locked cryptographic key is released, and $FV = 0$ otherwise, ϵ 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:

$$\delta_A^{QT} = \sum_{i=1}^{t} (\delta_{A_i}^{QT}), \;\; \delta_{A_i}^{QT} = \begin{cases} 0\,; & if\ (\delta f_i^{QT} < \delta_i) \\ 1\,; & otherwise \end{cases} \tag{2}$$

where, $\delta f_i^{QT} = \| {f_i}^Q - {f_i}^T \|$ is the distance between the two signature images as measured by a feature f_i, and δ_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 with a tolerance δ_i. So, a locking element is successfully located when the corresponding unlocking elements is similar enough (has limited dissimilarity δ_i). For genuine queries, the total matching error $(\delta_A^{QT} + \delta^{'})$ should not exceed the error correction capacity (ϵ) of the FV decoder, while it should exceed this threshold in case of applying impostor query samples.

To this end, signature representations of concise size t are selected in a dissimilarity space, where distances between feature pairs are the space constituents. Huge number of

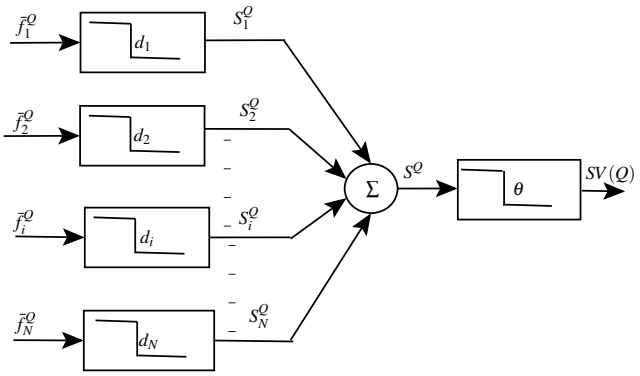


Fig. 4. SV classifier: similar model is applied as that for the FV system. However, it is designed in the original feature space producing a secure classifier since no templates are needed for verification. A feature $\bar{f}_i$ shares in the classification decision by a share S_i that reflects the confidence in classifying a sample with respect to a threshold d_i.

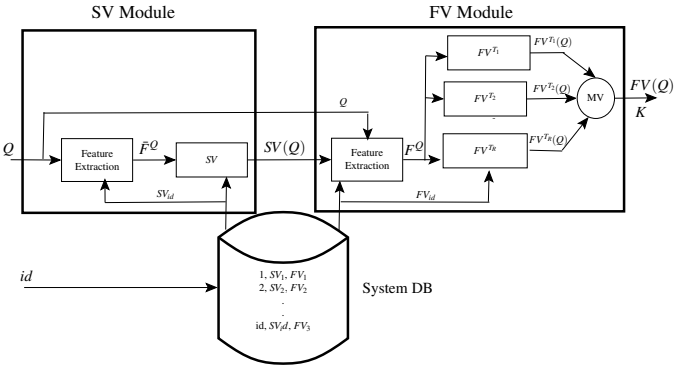


Fig. 5. Proposed cascaded SV-FV system in the verification mode: different feature representations $\bar{F}$ and F are processed by a SV classifier and a set of FV decoders, respectively. The FV module is triggered only if the SV module produces a positive classification label.

features are injected in this space, and a BFS algorithm [16] selects the best features that minimize δ_A^{QT} 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 δ_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 δ_i. Moreover, impact of chaff points $\delta^{'}$ 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 prower 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 $\bar{F}$ of dimensionality $N < L << M$.

Figure 4 illustrates the produced SV classifier in the verification mode. A signature representation $\bar{F}^Q = \{\bar{f}_i^Q\}_{i=1}^N$ is extracted from a query signature Q according to the WD representation $\bar{F}$. A feature $\bar{f}_i^Q$ 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 θ.

Functionality of the SV classifier is modeled as follows:

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

where

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

S_i^Q is the classification share based on a specific feature $\bar{f}_i^Q$, p_i^{left}, p_i^{right} represent confidence of a decision taken by a feature $\bar{f}_i^Q$, 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 shares 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 $\bar{F}^Q$ 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, ie., $SV(Q) = 1$. In such case, a feature representation F^Q is extracted from Q according to the user FV stored in system database. Instead of unlocking a single FV, a set of FV templates $\{FV^{T_r}\}_{r=1}^{R}$ 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 and imitates the genuine signature.

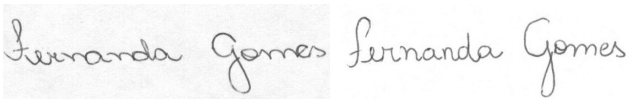
The signatures were provided by 168 writers and are organized as follows: the first 60 writers have 40 genuine signatures, 10 simple forgeries and 10 skilled forgeries per writer. First 30 genuine signatures are used to design the SV and FV modules. The other 10 genuine and all forgeries are used for performance evaluation. However, signatures of the other 108 users are used for dimensionality reduction through producing the universal representation (Details of dimensionality reduction is out of scope of this paper and more details are found in [8]).

Extended-shadow-code (ESC) [11], and directional probability density function (DPDF) [17] features are extracted based on different grid scales, hence a range of details are detected in the signature image. These representations are then fused to produce a feature representation of huge dimensionality ($M = 30,201$). A dimensionality reduction process is executed and produced a universal representation of reduced dimensionality ($L = 555$).

To design the FV module, the first 30 genuine signatures of each user are used to produce 30 different FVs/user. For FV encoding, $t = 20$ genuine vault points are produced from a 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.

TABLE I. Comparison of the SV and FV systems to the proposed cascaded SV-FV system

Performance measure	Method				
	SV only	FV only		Proposed approach	
		$R = 1$	$R = 15$	$R = 1$	$R = 15$
FRR	7.83	11.53	7.69	14.00	10.87
FAR_{random}	0.01	2.05	0.00	0.00	0.00
FAR_{simple}	0.17	2.39	1.92	0.30	0.33
$FAR_{skilled}$	13.50	24.38	23.26	10.80	11.38
AER	5.38	10.08	8.21	6.55	5.64



Genuine template Skilled forgery

Fig. 6. Example of skilled forgeries that are filtered by the SV module.

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 (60×40) verification trials. For performance evaluation, the average error rate (AER) is computed as follows:

$$AER = (FRR + FAR_{rand} + FAR_{smp} + FAR_{skl})/4. \quad (5)$$

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 (error = 10). For FVs with error correction capability $\epsilon = 6$, 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, $FAR_{skilled} = 16\%$.

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, $FAR_{skilled} = 0\%$, when the cascaded SV-FV system is employed.

Table I presents the simulation results for all users in the testing dataset. The pure FV system, with a single template ($R = 1$), has shown $AER = 10.08\%$. 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 ($AER = 5.38\%$). 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 $AER_{skilled}$ 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 future 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

[1] U. Uludag, S. Pankanti, S. Prabhakar, and A. Jain. 2004. "Biometric Cryptosystems: Issues and Challenges". *Proc. of the IEEE*, vol.92, no.6, pp. 948-960.

[2] A. Juels and M. Sudan., A Fuzzy Vault Scheme. *In proc. IEEE Int'l Symp. of Information Theory*, Switzerland, pp.408, 2002.

[3] K. Nandakumar, K. Jain, and S. Pankanti. 2007. "Fingerprint Based Fuzzy Vault: Implementation and Performance". *IEEE Trans. on Information Forensic and Security*, vol.2, no.4, pp. 744-757.

[4] Y. Lee, K. Park, S. Lee, K. Bae, and J. Kim. 2008. "A new method for generating an invariant iris private key based on the Fuzzy Vault system". *IEEE Trans. on Systems, Man, and Cybernetics- part B: Cybernetics*, vol.38, no.5, pp. 1302-1313.

[5] M. Freire-Santos, J. Fierrez-Aguilar, M. Martinez-Diaz and J. Ortega-Garcia., 2007. "On the applicability of off-line signatures to the Fuzzy Vault construction". In *ICDAR2007*. (Curitiba, Brazil 2007).

[6] G. Eskander, R. Sabourin, and E. Granger. 2014. "Bio-Cryptographic System Based on Offline Signature Images". *Information Sciences*, vol. 259 (2014), pp. 170-191.

[7] G. Eskander, R. Sabourin, and E. Granger. 2013. "Towards Automated Transactions based on the Offline Handwritten Signatures". In *9th Int'l Conference on Machine Learning and Data Mining*. (New York, USA 2013). pp. 141-150

[8] G. Eskander, R. Sabourin, and E. Granger. 2013. "Hybrid Writer-Independent–Writer-Dependent Offline Signature Verification System". *IET-Biometrics Journal, Special issue on Handwriting Biometrics*, vol.2, no.4, pp. 169 -181

[9] K. Nandakumar, A. Nagar, A.K. Jain. 2007. "Hardening fingerprint Fuzzy Vault using password". In *Lecture Notes in Computer Science*. 4642 (2007), pp. 927937

[10] C. Freitas, M. Morita, L. Oliveira, A. Yacoubi, E. Justino, and E. Lethelier, F. Bortolozzi, and R. Sabourin. 2000. "Bases de dados de cheques bancarios brasileiros". In *XXVI Conferencia Latinoamericana de Informatica*. (Mxico 2000).

[11] R. Sabourin, and G. Genest. 1994. "An Extended-Shadow-Code based Approach for Off-Line Signature Verification". In *Proc. of the 12th Int'l conf. on Pattern Recognition*. (Jerusalem 1994), pp. 450-453.

[12] D. Rivard, E. Granger, and R. Sabourin. 2013. "Multi-Feature extraction and selection in writer-independent offline signature verification". *Int'l Journal on Document Analysis and Recognition*, vol.16, no.1, pp. 83-103.

[13] E. Pekalska, and R . Duin. 2002. "Dissimilarity Representations Allow for Building Good Classifiers". *Pattern Recognition Letters*, vol.23, no.8, pp. 161-166.

[14] G. Eskander, R. Sabourin, and E. Granger. 2013. "Dissimilarity Representation for Handwritten Signature Verification". In *2nd Int'l Workshop on Automated Forensic Handwriting Analysis*. (Washington DC, USA 2013), pp. 371-376.

[15] G. Eskander, R. Sabourin, and E. Granger. 2013. "A Dissimilarity-Based Approach for Biometric Fuzzy Vaults–Application to Handwritten Signature Images". In *Int'l Workshop on Emerging Aspects in Handwritten Signature Processing*, LNCS, vol. 8158, pp. 95-102 (Naples, Italy 2013).

[16] K. Tieu, and P. Viola. 2004. "Boosting image retrieval". *Int'l Journal of Computer Vision*, vol.56, no.1, pp. 17-36.

[17] J. Drouhard, R. Sabourin, and M. Godbout. 1996. "A Neural Network Approach to Off-line Signature Verification Using Directional PDF". *Pattern Recognition*, vol.29, no.3, pp. 415-424.