Advance Access publication on 15 October 2016
doi:10.1093/comjnl/bxw081

Biometric Layering with Fingerprints: Template Security and Privacy Through Multi-Biometric Template Fusion

MUHAMMET YILDIZ[1], BERRIN YANIKOĞLU[1*], ALISHER KHOLMATOV[2], ALPER KANAK[2], UMUT ULUDAĞ[2] AND HAKAN ERDOĞAN[1]

[1]*Sabanci University, Department of Computer Science and Engineering, Tuzla, 34956 Istanbul, Turkey*
[2]*TUBITAK BILGEM UEKAE, Gebze, 41470 Kocaeli, Turkey*
[*]*Corresponding author: berrin@sabanciuniv.edu*

As biometric applications are gaining popularity, there is increased concern over the loss of privacy and potential misuse of biometric data held in central repositories. We present a biometric authentication framework that constructs a multi-biometric template by layering multiple biometrics of a user, such that it is difficult to separate the individual layers. Thus, the framework uses the biometrics of the user to conceal them among one another. The resulting biometric template is also cancelable if the system is implemented with cancelable biometrics, such as voice. We present a realization of this idea combining two or three different fingerprints of the user, using four different methods of template construction. Three of the methods use less and less information of the constituent biometrics, so as to lower the risk of leakage and cross-link rates. Results are evaluated on publicly available Finger Verification Championship (FVC) 2000, 2002 and NIST fingerprint databases. With the FVC databases, we obtain 2.1%, 3.9% and 3.4% Equal Error Rate on average using the three proposed methods, while the state-of-the-art commercial system achieves 1.9%. Furthermore, we show low cross-link rates under 63% under different scenarios, while genuine identification rates are 100%, with such a small gallery of 55 templates.

Keywords: multi-biometrics; privacy; security; fusion; layering; fingerprint; minutiae; template

Received 20 January 2016; revised 27 July 2016
Handling editor: Steven Furnell

1. INTRODUCTION

Biometric data are increasingly used in authentication and identification of individuals, replacing the token and password-based security systems. In biometric authentication, a questioned biometric is verified against a previously registered reference, for which a template is extracted and stored during enrollment. There are two approaches for storing biometric templates. In one alternative, the user carries a smart card containing her biometric template, and the verification of questioned sample is done within the smart card, without ever being stored in a repository (i.e. *match-on-card*). In the second alternative, the enrolled users' biometric templates are kept at a central repository and authentication is carried out by matching the query with the template stored at the repository. There are disadvantages associated with each of these two approaches. The most commonly known disadvantages of the *match-on-card* scheme are (i) low matching performance due to the limited processing power and memory of the smart card chip, (ii) vulnerability to *man-in-the-middle attacks* if the card generates plain matching results, (iii) inconvenience of carrying the card and maintaining its physical security, (iv) overhead associated with card issuance. Consequently, the use of central repositories is by far the more common of the two alternatives; however, there is increased concern over the loss of *privacy* and potential misuse of biometric data held in central repositories.

The term *privacy* is difficult to precisely define, as it has different meanings in different situations and cultures. The common denominator can be stated as keeping personal information, such as one's actions, whereabouts, or personal information, from others' view. Within the biometric domain, loss of privacy occurs if the biometric is compromised or accessed to obtain unintended information about a person (such as their health condition). Loss of privacy also occurs if the biometric data are used to track individuals by linking biometric databases belonging to different applications.

Biometric *template protection* is seen as a direct way to address privacy concerns and has been an active research area in biometrics for the last 10 years. Template protection refers to storing a transformed or modified version of a biometric template in such a way that it is impossible to reconstruct or reveal the original biometric template from the stored version. Ideally the protected biometric template need not be revealed and verification should be done in the protected template domain. This may be possible with one-way functions that are applied to both the reference and the query biometrics, which allow matching to be done in the transformed space [1]. While this is a very nice idea, finding such one-way functions that are applicable to noisy/fuzzy biometrics has been challenging, along with the need to register the biometrics before applying the transform. Similarly, the biometric data cannot be directly used as an encryption key within the framework of well-established cryptographic algorithms because of the noisy/fuzzy nature of biometrics.

Providing *cancelability* and *renewability* are two other important properties. Since people cannot change their biometrics as they can change their passwords, if the existing template is compromised, it should be cancelled or revoked, and ideally a new template is generated from the same biometric data. A good treatment of these concepts is given in Ref. [2].

Several schemes have been proposed in recent years for protecting the biometric templates [3–8]: in particular the *fuzzy commitment* [4], *fuzzy vault* [9] and *biohash* [8] schemes are successfully implemented with many biometric modalities. However, research is active in finding better methods that provide template protection, while not inconveniencing the user or degrading system performance.

In this paper, we propose a biometric authentication framework for increased security and privacy, extending and improving the work done in Ref. [10]. The main principle of the framework is to conceal the biometric of a person using another biometric, rather than a cryptographic construct. In particular, we demonstrate an implementation of the proposed framework combining multiple fingerprints. The proposed method, called *Biometric Layering*, is shown to be more robust against privacy leaks and achieves a higher level of security due to its use of multiple modalities, in comparison to corresponding uni-modal systems. Although the use of this method is demonstrated with fingerprints, it can be used with landmark points obtained from voice, face or minutiae points obtained from iriscode or other applicable biometrics [11].

The organization of this paper is as follows. In Sections 2 and 3, we discuss previous studies and overview the proposed framework. Then, we describe the implementation of the proposed method in Section 5, with four different variations in constructing the multi-biometric templates. We provide and discuss experimental results of our implementation in Section 6. Finally, we summarize the strengths of the proposed system in Section 9 and conclude with Section 10.

2. PREVIOUS WORK ON TEMPLATE PROTECTION

In the past two decades, several biometric template protection mechanisms were proposed in the literature. Ratha *et al.* [1] first suggested a framework of cancelable biometrics, where biometric data undergo a predefined non-invertible transformation during enrollment and testing, with the matching done in the transform space. If the transformed biometric is compromised, the user is re-enrolled to the system using a new transformation. Likewise, different applications are also expected to use different transformations for the same user. While this work has been influential, finding one-way transformations that preserve distances has been elusive. Furthermore, managing the transform functions is also an issue.

Another class of template protection schemes uses some form of user-specific *helper data* that is extracted from the original biometric, in order to tolerate the variations observed in biometric data. One such technique is called the *fuzzy commitment*, which is a secure key release scheme proposed by Juels and Wattenberg [4]. In this scheme, a secret key is encoded as an error-correcting code c and the difference of codeword and the presented biometric of the user ($\delta = t - c$) is stored in the database, together with the hash of c. During verification, a probe template t' is used to obtain a probe word as $w' = t' + \delta$. Then c', the closest codeword to w', is selected from W. If $h(c') = h(c)$ then the verification succeeds. The scheme was inspired by the work of Dodis *et al.* [12] and later inspired a scheme called *secure sketch* by Sutcu *et al.* [13].

The fuzzy commitment is used in several studies. Hao *et al.* [14] have used *iris* biometrics to generate a repeatable cryptographic key up to 140 bits. Sutcu *et al.* [15] used fuzzy commitment in a multi-biometric system comprised of fingerprint and face.

Later, Juels and Sudan [9] introduced the *fuzzy vault* scheme to address the problem of unordered feature representations. The fuzzy vault is a general scheme to hide some data in a vault such that it can only be released when sufficiently matching data are provided; as such, it is very suitable

for biometric template protection and indeed several applications have been implemented using fingerprints [16–19], face [19] and iris [18, 19]. To obtain a fingerprint vault, a secret is encoded as the coefficients of a polynomial that is evaluated at the minutiae points (x), such that $(x, p(x))$ are then hidden among a large number of chaff points. During verification, the biometric of the user is matched to the vault and only a sufficient match of the minutiae points reveals the secret, through polynomial reconstruction and unlock the vault.

Another important method is the *Biohash* scheme that projects the biometric features onto a user-provided random key [8]. Randomness (and secrecy) of this key, which can be stored in a user-specific physical token, provides non-invertibility. Furthermore, matching accuracy increase is also gained, as the biometric signal is combined with an added source of entropy. However, (i) the need to store/access a random bit string that requires a token (with the well-known disadvantages of token-based authentication, such as loss, theft, etc. of the cited token) and (ii) the assumption that the keys are not known, are pointed out as the problems of these schemes [20].

The use of multi-biometric templates provides another alternative for template protection [10, 11, 21, 22]. In this approach, the template is constructed from multiple-biometrics or one biometric is used to hide another biometric data, rather than using data hiding or cryptographic techniques. Yanikoglu and Kholmatov [10] proposed multi-biometric templates in order to increase privacy as well as security. They combined minutiae points from two distinct fingers of the same person using superimposition, creating a template with two biometric layers. While multi-biometric systems were proposed for increased security before [23–31], to the best of our knowledge, this was the first work that used multi-biometrics for increased privacy and template protection. As an extension of this work, Camlikaya *et al.* [11] combined fingerprint minutiae with a spoken password. In this way, cancelability is provided since the spoken password can be replaced, if the template is compromised.

Most similar to our work, Othman and Ross [21] proposed an approach for creating synthetic fingerprint images for a person, by mixing complementary phase components of two corresponding fingerprints. The advantage of this method is that it can be easily integrated to any existing fingerprint verification system, where the created virtual fingerprints would be used for authentication instead of real ones. Mixing two different fingers from the West Virginia University database, authors report a rank-1 accuracy of ∼85% and an Equal Error Rate (EER) of ∼6% on a data-set with a total of 500 fingers. In another experiment, they evaluated the *changeability* property and showed that the mixed fingerprints do not match well (30% rank-1 accuracy) with the original ones. To evaluate *cancelability*, they ran matching and identification tests involving templates obtained from two impressions of the same fingerprint that were combined with 500 separate fingerprints. They obtained a high 85% identification rate, and 7% EER, showing the promise of the model, despite having similar templates in the gallery. One issue with this work is that to obtain realistic looking fingerprints, their constituents must pass a compatibility criterion.

In another similar work combining two fingerprints, Li and Kot [22] propose an approach where the combined fingerprint template is created using minutiae locations of one of the fingerprints whose angles are replaced with ridge orientation angles from the other one. The coupling between the minutiae and their replaced angles is performed after alignment of both fingers about their corresponding reference points. During verification, two candidate fingerprints are similarly combined and matched against the template, obtaining 0.4% False Reject Rate (FRR) at 0.1% False Accept Rate (FAR) using the FVC 2002-DB2-A database. To evaluate privacy of their proposed methods, Li *et al.* defined two types of attacks based on their scheme: using the combined template to attack a database that contains (i) the first fingerprint (using the minutiae location correlation) and (ii) the second fingerprint (using the minutiae angle correlation). They call the two attacks *Attack Type A* and *Attack Type B*, respectively. Using FVC 2002-DB2_A and generating databases of 100 combined templates, they report low rank-1 rates of 25% for *Attack Type A* and 57.5% for for *Attack Type B*, showing the promise of the system. The main issue with this technique is the need for detecting reference points, which may not exist or be located reliably.

The current work improves upon the work done in Ref. [10], which had limited experimental evaluation.

3. OVERVIEW OF THE PROPOSED SCHEME

The proposed scheme consists of combining multiple biometric modalities into a single multi-biometric template, concealing the constituent biometrics among one another. The scheme is based on the fact that without possession of genuine biometric data, it is computationally hard for a forger to separate the combined template into its constituent biometrics.

In the implementation shown in this paper, we superimpose two fingerprints to form a multi-biometric template comprised of two biometric layers. Furthermore, we layer three fingerprints to explore the capacity of the proposed system.

The overall workflow of the system is depicted in Fig. 1. In the *Enrollment* phase, the acquired biometric signals are processed and each one is converted into a set of unordered feature points (i.e. minutiae points) and layered together to create the multi-biometric template. In the *Verification* phase, the user is verified when she presents query samples of each of the constituent biometric modalities; whose features are matched and removed from the multi-biometric template,

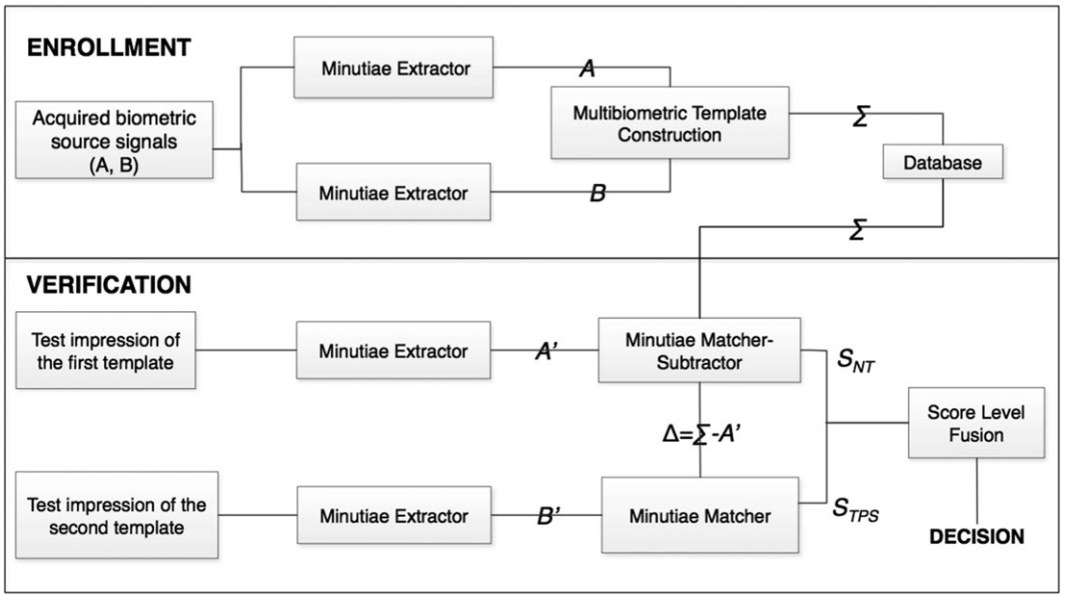

FIGURE 1. Overview of the proposed system.

each match resulting in a match score. The matching scores obtained at each step are then linearly combined to obtain a final matching score.

The layering is done using different methods, each one using less information of the constituent biometrics, such as randomizing minutiae angles and using a subset of minutiae points are suggested, so as to reduce the chance of leakage at some cost in performance.

While the main aim is to protect the biometric data, the scheme also enjoys increased security for the overall system due to the multi-modal biometric paradigm. The scheme suggests to create different multi-biometric templates for different security applications by combining different constituent biometrics (e.g. two different fingerprints) or by using behavioral biometrics that can be changed for each application (e.g. a spoken password).

4. CONTRIBUTIONS

The idea of layering multiple-biometrics has been suggested before Refs [10, 11], although with limited experimental evaluation. The main contribution of this work is an in-depth exploration of the idea of combining multiple biometrics through layering, using fingerprints. We improve and extend our previous work by:

- introducing three new methods that aim (i) to make it more difficult to separate the multi-biometric template into its constituent biometric samples ($Method_2$); (ii) to prevent the possibility of full leakage of the original template ($Method_3$) and (iii) to explore the limits of biometric layering with three modalities ($Method_4$);
- using state-of-the-art fingerprint matchers for improved results: one commercial and one developed in this work to work with minutiae locations only, as required in one step of the algorithm;
- presenting new theoretical and experimental evaluation of security and privacy aspects of the proposed method;
- performing experiments on large and public databases (all subsets of FVC and NIST databases);
- achieving results that are close to the state-of-the-art verification performance using the public FVC dataset, while demonstrating increased difficulty in cross-linking databases.

4.1. Multi-biometric template generation

The important issue in creating the multi-biometric template is that the constituent biometrics should not be easily separated. In order to merge, the two minutiae sets as much as possible, we follow these steps:

- Create an empty template that is large enough to include both A and B even without much overlap.
- To minimize the number of overlapping minutiae in Σ, we translate B with respect to A by 50 pixels in each of the four directions. The translation amount was decided to allow some flexibility, while still overlapping the majority of the two minutiae sets.

- Superimpose the two minutiae sets (A and B) with respect to the optimal translation found in the previous step and store that combined point set as the combined multi-biometric template (Σ).

5. MULTI-BIOMETRIC TEMPLATES USING MULTIPLE FINGERPRINTS

5.1. Enrollment and verification

Each person who enrolls into the system provides impressions from two different fingers, A and B. Minutiae points defined by ridge endings and bifurcations on the fingerprint pattern are used as features (see Section 5.2). Then, the center of masses of the two minutiae sets is aligned and one set is superimposed on the other so as to minimize the number of the overlapping minutiae (see Section 4.1). The created multi-biometric template (Σ) thus consists of two *biometric layers* and becomes the biometric ID/template of the person, stored into the database.

A sample biometric template is shown in Fig. 2c, obtained from two fingerprints shown in Fig. 2a and b. Note that in this figure we show the two components of Σ with separate markers for the sake of clarity; whereas the source of the minutiae points is not stored in the multi-biometric template.

When a person is to be authenticated, she gives two query fingerprint impressions (A' and B'), both of which are used to verify her identity. The matching is done by finding the correspondence between the minutiae of these two query fingerprints and multi-biometric template Σ: first, the first fingerprint, namely A', is matched against the combined biometric ID (Σ). Then, the matched minutiae points are removed from Σ, and the second fingerprint B' is matched against the remaining minutiae points. The person is authenticated if the fusion of the scores obtained from the two steps is above a certain threshold (see Section 5.6).

5.2. Feature extraction

We extract and use minutiae points as features representing a fingerprint. Minutiae points are the discontinuities of fingerprint ridges, such as bifurcation and end points [24]. In our

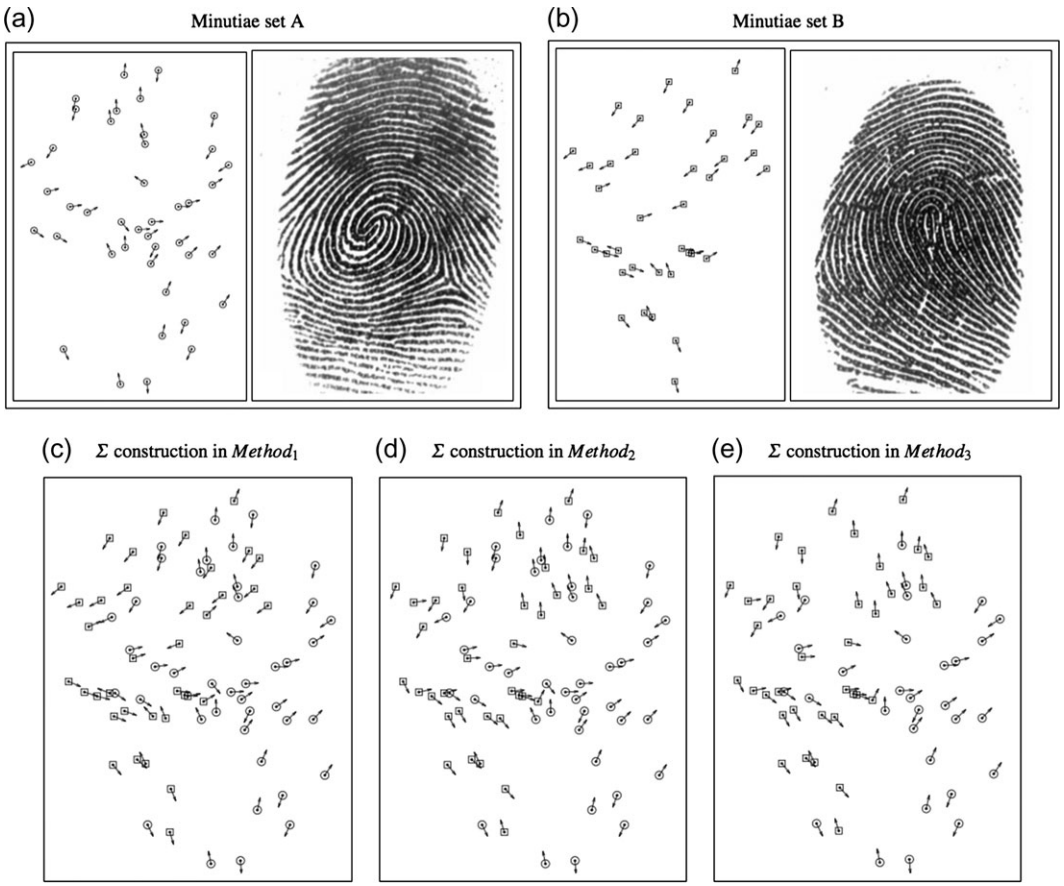

FIGURE 2. Two distinct fingerprint minutiae templates A and B combined for different methods. ⊙ is used for A and ⊡ is used for B, but this information is only for visual depiction only and is not stored in the final template. (**a**) Minutiae set A, (**b**) minutiae set B, (**c**) Σ construction in $Method_1$, (**d**) Σ construction in $Method_2$, (**e**) Σ construction in $Method_3$.

case, we only keep the two-dimensional coordinates and the ridge orientation of a minutiae point, while other systems may use more information, such as the type of the discontinuity.

Since this work does not focus on minutiae extraction, we preferred to use a commercial, state-of-the-art fingerprint minutiae extractor [32]. In this way, we can demonstrate real life feasibility of the proposed concept, while avoiding errors due to a sub-optimal system. After the extraction process, all of the information, except the coordinates and ridge angles of the minutiae (e.g. core type and location), was discarded in order to get*minutiae only* templates.

A sample multi-biometric template generated using this procedure is shown in Fig. 2c, for two minutiae sets shown in Fig. 2a and b. This method forms the first and simpler proposed template creation method (called $Method_1$ from now on).

5.3. Hiding angle information

Considering that it may be possible to separate the minutiae of Σ into their corresponding source sets using the coherence of minutiae angles within local regions [33], we propose an alternative method for template generation. In this method, we use an extra step wherein the minutiae angles of the minutiae set B are replaced to mimic those of A. This method enhances the privacy of the user since it should be more difficult to separate the two fingerprint templates A and B apart.

In this method (called $Method_2$ from now on), in addition to the template creation step given in Section 4.1, we take the following steps to replace the orientation angles of the B's minutiae:

For each minutiae m of B in Σ:

(1) Find the minutiae of A within an arbitrarily chosen proximity of 30 pixels to m and create a histogram of their angles (L).
(2) Quantize the angles of the minutiae in L to eight directions and find the most frequent quantized angle q.
(3) Set m's angle to a random angle in the range [q -22.5, q$+22.5$] (A total range of 45' corresponding to eight directions).

The perturbation is done so as to reduce the chances of clustering minutiae points of the same source fingerprint using minutiae angle coherence.

The multi-biometric template obtained in this way is shown in Fig. 2d. Note that this template is similar to the one generated by $Method_1$ (shown in Fig. 2c) except for the modified angles of the second minutiae set.

5.4. Using a subset of the minutiae

Modifying the angles of the second the fingerprint (B) makes it more difficult to isolate constituent fingerprints; something that could be done with some success, by considering minutiae angles [33]. However the minutiae of the first fingerprint (A) are used as is, in the multi-biometric template. Therefore, after a successful verification, this fingerprint is exposed to the system, to a large extent (except for extra and missing minutiae points resulting from an error-prone matching of the first template (A).

To remedy this situation, in this section we propose a new method called $Method_3$ that is identical to $Method_2$, except for the fact that it only uses a subset of A's minutiae. In the experiments, we have tried using 50% and 75% of the minutiae points, with acceptable verification performance being obtained with the latter.

5.5. Layering three fingerprints

In order to explore the capacity of biometric layering, we propose a new method, $Method_4$ that combines three fingerprints into one multi-biometric template.

In this method, we use 75% of the minutiae points in each fingerprint so as to prevent full leakage of any of them during a successful match. The minutiae angle orientations are kept intact, unlike $Method_2$ and $Method_3$. This is because we intended to see the performance using three layered fingerprints, without the additional step of minutiae angle perturbation; so as to study its contribution alone.

5.6. Matching and scoring

For matching, query fingerprint impressions A' and B' (and C' in case of $Method_4$) are matched against the combined template Σ. Each query fingerprint is successively matched to and subtracted from the multi-biometric template. At each subtraction step, a matching score is obtained. Finally, all the matching scores are linearly fused to obtain a final matching score. We describe this process by going over the steps below.

Step 1: We used Neurotechnology's fingerprint matcher (NT) for matching A' against Σ. The proprietary match score S_{NT} is obtained for this first match and the matching minutiae are then removed from the template, leaving Δ.

Step 2: The remaining template Δ is matched to B' using our own matcher that uses Thin-Plate-Splines (TPS). Our TPS matcher is based on the work of Bazen and Gerez [34], but our implementation can be set to ignore the angles of the minutiae during the matching procedure. In fact, this is the reason for using different matchers for the two steps; Neurotechnology's system depend on minutiae angles for its successful performance, while the minutiae of the second

fingerprint are modified in $Method_2$ of the proposed system. The S_{TPS} score is calculated to measure the success of this second step.

$$S_{\text{TPS}} = \sqrt{\frac{|\Delta \cap B'|^2}{|\Delta| * |B'|}}$$

The $|\Delta \cap B'|^2$ is the *the square of the number of matching minutiae between* Δ *and* B'.

Step 3: To obtain the final match score, we linearly combine the two match scores after normalizing S_{NT}, to bring it to the same scale with S_{TPS}:

$$S = \alpha * S_{\text{TPS}} + \mathcal{T}(S_{\text{NT}})$$

$$\mathcal{T}(S_{\text{NT}}) = \left(\frac{2}{1 + e^{\sigma * S_{\text{NT}}}} - 1 \right)$$

While the combination is essential to bring together all the sources of information, the accuracy is not very sensitive to the weighting coefficient α, and we have obtained the reported results with $\alpha = 1$.

The list of variables used in this work is summarized below:

- A: First minutiae set obtained from a fingerprint during enrollment.
- B: Second minutiae set obtained from a fingerprint during enrollment.
- Σ: Multi-biometric template created: $\Sigma = A \cup B$.
- A': Second impression of the first fingerprint used in query.
- B': Second impression of the second fingerprint.
- Δ: The remaining template after removing the first layer: $\Delta = \Sigma - A'$
- S_{NT}: Proprietary integral score returned by the NT matcher. It has a minimum of 0, a threshold value that mostly occurs on the range $[0 - 50]$ and no maximum. It represents the similarity between two different templates.
- S_{TPS} Fractional score obtained from the match with Δ versus B', using the TPS matcher (Section 5.6).
- $Method_1$: Basic template construction with the superimposition of two minutiae sets.
- $Method_2$: Proposed template construction method with the superimposition of two minutiae sets where the second minutiae points are assigned pseudo-random angles.
- $Method_3$: Same as $Method_2$ except for using only 75% of the minutiae from the first template (A).
- $Method_4$: Same as $Method_1$ except for using three fingerprints and 75% of each minutiae set.

6. THEORETICAL EVALUATION OF TEMPLATE SECURITY AND PRIVACY

We evaluate the proposed method in terms of its verification performance, along with some measures of privacy enhancement. Specifically, using the criteria defined in Ref. [2], we can make the following claims that are argued in this section or in subsequent experiments:

Full-leakage irreversibility refers to the difficulty of determining, exactly or with tolerable margin, from the multi-biometric template, the biometric sample(s) or features used during enrollment to generate that template. We cannot guarantee full-leakage irreversibility with $Method_1$, as it may be possible to use minutiae angle coherence, using techniques similar to ones used in Ref. [35] to reconstruct the fingerprint image from minutiae angles. On the other hand, for $Method_2$ and $Method_3$, where the minutiae angle of the second template is modified, we assert that this requirement is satisfied as it is not feasible to split the multi-biometric template into its two constituent fingerprint minutiae since there are too many combinations to try in the absence of other information such as minutiae angles; and there is no way to know when one achieves the right split. Note that with these two schemes, the minutiae angle of the second template matches that of the first template locally, thus eliminating the potential use of minutiae angle information for finding the right split; or recovering the second template at all.

Altogether there are $C(2N, N)$ potential splits of the multi-biometric template into two equal parts, where N is the average number of minutiae in a single template. Hence the probability of finding the correct split is $1/C(2N, N)$. This number is roughly 0.56×10^{-18} for $N = 32$, which is the average number of minutiae in FVC fingerprint databases.

On average, only 55% of the minutiae points in the first matched template (A) are correctly identified during the proposed verification step, as measured over the FVC data-set using $Method_2$. This is partly due to usual matcher errors and also the existence of the second template. Hence, the original templates are not revealed fully, even after a successful matching step. Nonetheless, $Method_3$ is suggested to prevent this situation with certainty (all of minutiae points will not be revealed in full to the system that may potentially be unreliable. With this method, both templates are modified and it is impossible to fully recover any of the individual templates. As for $Method_4$, as we only use a portion of each of the constituent minutiae sets, it is guaranteed that there is no full leakage.

Since there will always be an uncertainty about the leaked information about the constituent biometrics even if the right split was found, the irreversibility is *unconditional*, according to the definition of Ref. [2].

Authorized-leakage irreversibility refers to the difficulty of determining a biometric sample or features from the multi-biometric template that would be useful for an attacker to break into an unprotected system (i.e. an unprotected unimodal system).

The probability of one of the random splits to have K or more of its constituent minutiae points coming from the same fingerprint, when splitting a template with N points, is:

$$P(K) = \sum_{k=K}^{N} \binom{N}{k} p^k \times (1-p)^{(N-k)}$$

where p is 0.5. For $N = 32$ and $K = 24$ (i.e. $24/32 = 75\%$ or more of the minutiae in the chosen set to be correct), this probability is 0.0035, but drops sharply as K approaches N (e.g. $P(K = 28) = 0.00001$).

Revocability refers to the ability of revoking a template, in case of a compromised template or generally a need of renewal. Simoens *et al.* [2] view this as an operational aspect that can be achieved by removing a compromised template from the database or by blacklisting it. In this sense, our system provides revocability by removing a compromised multi-biometric template from the database. Note that this removal does not affect the constituents, some of which may be re-used to form a new multi-biometric template, as discussed below.

Renewability refers to the ability to generate a *new* template from the *same* biometric data of a user, which may be used in renewing a revoked template. Using the proposed method ($Method_3$), renewability is deemed possible as two multi-biometric templates formed from the same constituents will be different thanks to the randomization in angle modification and minutiae removal of the second fingerprint. This is evaluated in cross-link tests with two separate templates created from the same two fingerprints ($\Sigma = A + B$ versus $\Sigma = A + B$) are matched, where the top-5 identification rate is found to be low (%65), even in the small FVC gallery of 55 multi-biometric templates. On the other hand, an implementation of biometric layering with voice pass-phrases is previously claimed to be fully renewable [11], as it involves an important random component, namely the pass-phrase.

Unlinkability is demonstrated via cross-link tests involving templates sharing one of the constituent biometric samples and differing in the other (e.g. $\Sigma = A + B$ versus $\Sigma' = A' + X$). Moreover, uni-modal search/identification tests are done by cross-linking with an unprotected database (e.g. $\Sigma = A + B$ versus A'). *Genuine Identification* rates are also reported as comparison. It is desirable for the system to obtain high genuine identification rates, while obtaining low cross-link and unimodal search rates. The unlinkability tests are reported in Section 8.

7. EXPERIMENTAL EVALUATION OF VERIFICATION PERFORMANCE

We perform four types of tests, shortly summarized below, to evaluate the performance of the proposed system:

- Uni-Modal Verification (UMV) Performance tests are performed to assess the baseline performance of matching algorithms employed in the proposed scheme, when applied to a single modality.
- Multi-Modal Verification (MMV) with the Proposed Scheme aim to measure the verification performance of the proposed schemes, where two query biometric samples (A' and B') are matched against the claimed multi-biometric template.
- Multi-Modal Score Level Fusion (SLF) tests are realized for completeness (i.e. compare against a system without template fusion to measure the loss caused by template fusion).

7.1. Databases

We use three different databases for evaluating the proposed system, first two databases are the FVC 2000 [36] and 2002 [37] databases, which are commonly used, including the public fingerprint verification contests. Each of these two databases consists of four subgroups, where each subgroup consists of 880 images (subjects(11) $\times$ fingers(10) $\times$ impressions(8)). The third data-set used in our evaluations is the NIST's fingerprint database-4 [38]. In this database, there are a total of 2000 subjects, where each subject has provided two impressions of only a single finger. The properties of each subgroup for FVC databases are outlined in Table 1.

The main purpose of using the FVC databases is to measure the verification performance of our method and compare

TABLE 1. Fingerprint databases used in this study (FVC 2000, FVC 2002 and NIST).

	FVC 2000				FVC 2002				
	DB1	DB2	DB3	DB4	DB1	DB2	DB3	DB4	NIST
Sensor type[a]	LCO	LCO	O	S	O	O	C	S	RS
Image size	300 × 300	256 × 364	448 × 478	240 × 320	388 × 374	296 × 560	300 × 300	288 × 384	512 × 512
Num. images	11 subjects × 10 fingers × 8 impressions								2000 × 1 × 2
Resolution	500 dpi				569 dpi				500 dpi

[a]LCO, low-cost optical; C, capacitive; O, optical; S, synthetic; RS, rolled and scanned.

it to the state-of-the-art, whereas the NIST database is used for the identification and cross-linking tests, as it includes more subjects compared to FVC data-sets. Please see Section 8 for further details. Throughout the evaluations, we used all of the available data of the corresponding data-sets.

7.2. Uni-Modal Verification

We report UMV performance results of the fingerprint matchers that are used in the proposed framework in order to establish the baseline performances of both our developed TPS matcher and the selected commercial fingerprint matcher from Neurotechnology [32]. The reason for utilizing this particular commercial matcher is 2-fold. First of all, we wanted to demonstrate the adaptability of the proposed framework to already available systems. The other reason is that the NT demonstrated a successful performance at FVC 2000 and FVC 2002 evaluations, making it a good candidate to compare against. In particular, the average EER values reported for NT in FVC 2000 and 2002 are 1.37% and 0.99%, respectively. In our evaluations, we obtained similar results for this matcher.

For these tests, we used all of the available impressions of genuine fingerprints in FVC 2000 and FVC 2002 databases. Since there are 110 different fingers and 8 impressions per finger in each database (11 persons $\times$ 10 fingers), matching all impressions of the same finger to each other results in 28 genuine tests per finger. This gives a total of 3080 ($=110 \times 28$) genuine tests for each FVC group. As for forgery tests, for each FVC group, we matched every first impressions of all the fingers to the first impressions of all the other fingers, resulting in 5995 ($=110 \times 109$) forgery tests.

The top two rows of Table 2 indicate the NT and TPS matcher performance on the FVC and NIST databases, with an average EER value of 1.9% versus 3.7% for the FVC databases, respectively. The NT system has state-of-the-art performance and the TPS matcher has a moderate performance and is included here for completeness. In the proposed system, the TPS matcher is only used when the NT matcher does not perform well; namely when matching minutiae sets for which the angles are modified. In that case, performance results are lower as expected: the average EER increases by about a factor of two for each database, becoming 7.5% and 9.7% for the FVC and NIST databases, respectively. The results for the case of modified angles are not reported for the NT system as it does not have an option to disregard the minutiae angle information.

7.3. MMV—proposed system

The lower part of Table 2 reports the verification rates for the proposed scheme where multi-biometric templates are created with two fingerprints and verification is done using both fingerprints. As described in Section 5, $Method_1$ constructs the template by simple layering, while in $Method_2$ and $Method_3$ the minutiae angles of the second constituent fingerprint are replaced, with or without using all the minutiae points, respectively. Finally, $Method_4$ explores the capacity of biometric layering by combining three biometrics into one multi-biometric template.

For these tests, a gallery of 55 templates is created for each FVC subgroup, by pairing each two consecutive template into one multi-biometric template. As for the NIST database, it is possible to create a gallery of 2000 multi-biometric templates by following the same strategy used for each FVC subgroup. However, to accommodate cross-link tests as well, we created a gallery of $2000/3 = 666$ templates to be used in verification tests.

As can be seen in Table 2, using $Method_1$, we obtained a 0.5% average EER over the eight FVC data-sets on average, which is significantly better than the state-of-the-art uni-modal performance of the NT system. Using $Method_2$ that provides higher template security, the results are close to the state-of-the-art uni-modal performance, with 2.1% average EER on the FVC database. With $Method_3$ and $Method_4$ that trade verification performance for additional template security, the results are 3.9% and 3.4% average EER on the FVC data-sets, respectively. Although, there is performance degradation when using $Method_2$ and even more in $Method_3$ compared to $Method_1$, the minutiae angle replacement and

TABLE 2. Verification performance (% EER).

	FVC 2000				FVC 2002					
Methods	DB1	DB2	DB3	DB4	DB1	DB2	DB3	DB4	FVC avg.	NIST
UMV-NT	2.4	1.1	4.7	1.6	0.7	1.4	2.1	1.4	1.9	2.8
UMV- TPS	3.6	2.3	7.1	5.1	2.0	1.8	5.2	2.8	3.7	4.3
UMV- TPS[a]	8.8	5.8	13.3	7.3	4.5	4.4	10.0	6.3	7.5	9.7
MMV-$Method_1$	0.9	0.1	1.4	0.4	0.1	0.1	1.9	0.4	0.5	4.6
MMV-$Method_2$	3.6	1.0	5.0	1.8	0.6	0.3	3.1	1.1	2.1	9.0
MMV-$Method_3$	5.1	2.1	7.6	4.1	2.3	0.8	5.8	3.3	3.9	12.2
MMV-$Method_4$	3.8	2.9	5.3	3.1	2.9	2.9	3.1	3.0	3.4	–

[a]No angle information was used.

additional random removal of minutiae from the first template provide a stronger template security and resilience to privacy threats, which we discuss in Section 8.

For all three methods, there is a significant decrease in comparison to the uni-modal systems, when using the NIST database. This can be explained by the fact that the fingerprints in the NIST database typically contain a very large number of minutiae points (195 versus 32 in FVC databases, on average), which causes a higher number of minutiae collision during multi-biometric template creation. $Method_4$ was not tested with this database, because it was not deemed suitable due to the large number of minutiae points in the fingerprints in this database.

Detection Error Tradeoff (DET) plots for the performances of the three methods are given in Fig. 3, along with uni-modal systems.

7.4. Multi-modal SLF

For the sake of completeness and comparability with other multi-modal approaches, a MMV system using a simple SLF is also implemented using the TPS matcher. Everything in this system is done the same way as for the proposed system whenever applicable. For instance, the same feature extraction and matching algorithms are used as in the proposed system. During matching, we tested two alternatives in line with the proposed method: using the minutiae angles or ignoring them. In either case, the match score between two fingerprint templates is calculated as the ratio of matched minutiae in the reference fingerprint. The individual scores obtained from the two matches are linearly combined for the final decision.

The EER results shown in Table 3 are the lowest error rates for both the FVC and NIST databases, with 0.3% and 1.2% EER, respectively. The success of the fusion system is

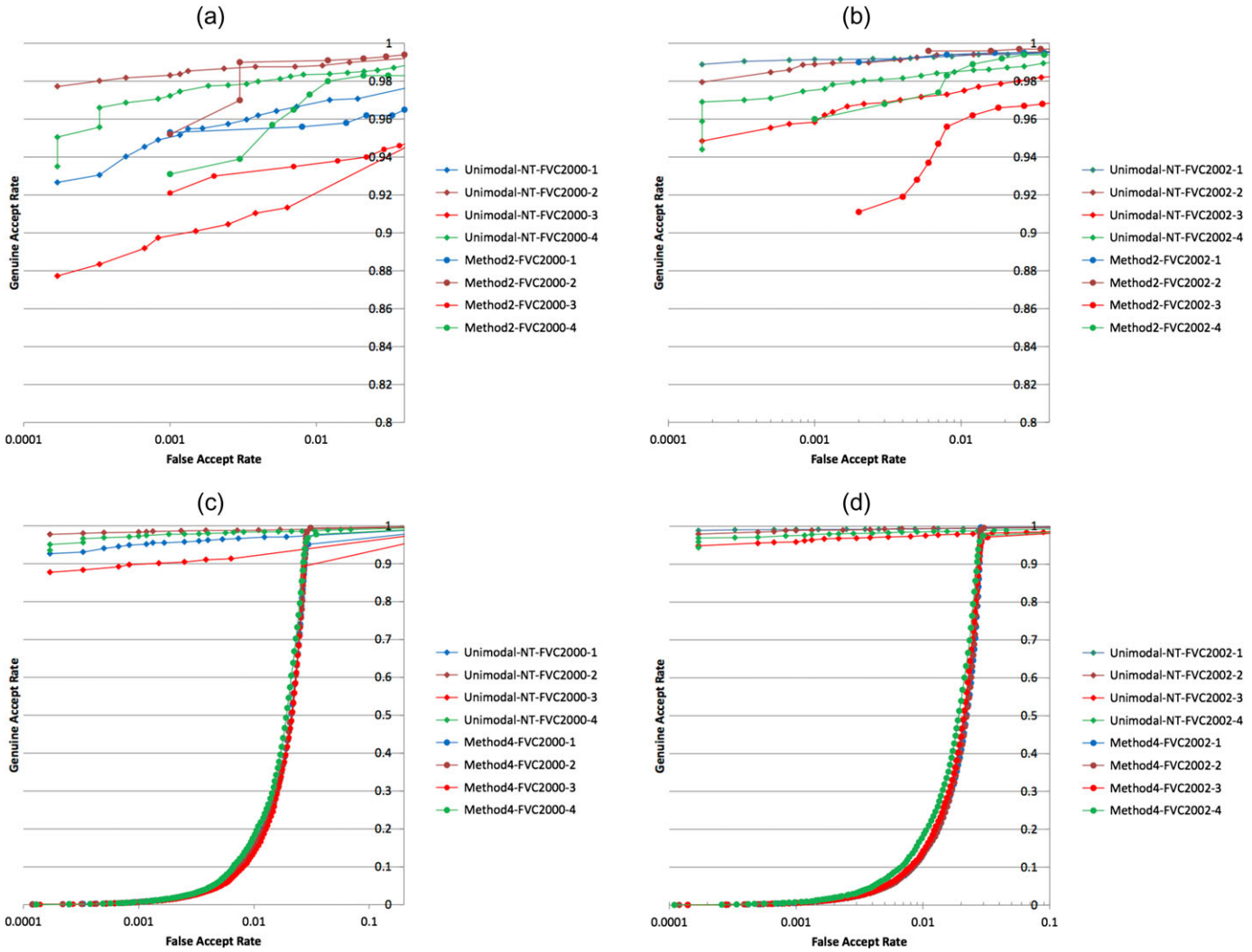

FIGURE 3. DET plots for the uni-modal and suggested multi-biometric system with FP–FP layers for FVC 2000 in (**a,c**) and FVC 2002 in (**b,d**). For ease in comparison, corresponding plots share the same color, with different markers.

TABLE 3. Verification performance (% EER) of a multi-biometric system with SLF.

	FVC 2000				FVC 2002					
Methods	DB1	DB2	DB3	DB4	DB1	DB2	DB3	DB4	FVC avg.	NIST
MM-SLF	0.4	0.0	1.0	0.4	0.0	0.0	0.8	0.0	0.3	1.2
SLF[a]	0.8	0.4	3.2	1.2	0.0	0.0	2.0	0.8	1.0	1.8

[a]No angle information was used.

expected, because on one hand it benefits from twice the discrimination power of two fingerprints and on the other hand, it does not sacrifice anything for the sake of privacy and template security. The performance degradation that comes with the lost angle information in the fusion system (1.0% versus 0.3% for FVC) parallels that observed with the proposed schemes.

We observed that in the first match (Σ versus A'), on average 92% of all matched minutiae are correct, while 8% of the matched minutiae come from the second fingerprint, as calculated over the FVC data-sets using $Method_2$. On average 55% of the minutiae points in A are correctly identified.

8. UNLINKABILITY TESTS

Irreversibility, revokability and renewability issues were addressed theoretically in Section 6; here we report the results of three types of tests to demonstrate unlinkability, by showing decreased success in cross-link rates in comparison to genuine identification rates:

- *Genuine Identification (GID)*—$(A + B)$ versus (A', B'): The aim of this evaluation is to measure the genuine identification rate of the system, when the multi-biometric template is searched using a genuine pair of query fingerprints within a gallery of templates. The identification is performed by sequentially matching the query pair to each of the multi-biometric templates in the gallery, using the method described in Section 5.6.
- *Uni-Modal search (UMS) attack*—$(A + B)$ versus A', $(A + B)$ versus B', $(A + B + C)$ versus A': This attack measures how easily one can identify a person's template having only one matching fingerprint. Since the role of all the fingerprints used in the template is not symmetric, we evaluate this scenario separately for the first, second and third templates, using the commercialNT matcher. $(A + B + C)$ versus A' and $(A + B + C)$ versus (A', B') are only meaningful for $Method_4$, where the multi-biometric template consists of three layered fingerprints and the attacker has access to one or two latent imprints of the fingers used in the multi-biometric template, respectively. When the attacker has access to two latent imprints (i.e. $(A + B + C)$ versus (A', B')), she performs two subsequent subtractions as described in $Method_4$.
- *Cross-Link (XLNK) attack*—$(A + B)$ versus $(A' + X)$, $(A + B)$ versus $(X + B')$ and $(A + B)$ versus $(A' + B')$: This is an attack scenario where the attacker is assumed to have access to two different multi-biometric databases and would like to find corresponding identities. During this attack, each multi-biometric template of a database is matched to all templates of the other database, as if they are uni-modal templates. In this attack scenario, corresponding templates may share the first fingerprint (A), the second fingerprint (B) or both.

Identification of a correct template with only a single fingerprint is undesired, as it would lead to the identification of the user by searching with a latent fingerprint, or cross-linking with an unprotected database. Similarly, if a user is enrolled in multiple databases, cross-linking may identify, which templates in the two databases belong to the same person, posing a privacy threat.

As evaluation metric, we report the percentage of cases where identification returns the correct template among the top-k candidates, for top-1, top-5 and top-10.

8.1. Databases

We used the FVC and NIST databases throughout these evaluations, with results given in Tables 4 and 5. While both databases are commonly used in literature, they each present some challenges for these tests. The FVC database is very small to run multi-biometric tests (especially XLNK tests), while the NIST fingerprints contain very large number of minutiae points, which is not very amenable for layering.

To maximally use the NIST database, we grouped the 2000 fingers such that three fingers were used as if they belonged to the same user. The two fingerprints (A and B) of one user are used to construct one multi-biometric template for the main gallery, for which the matching impressions (A' and B') are used for GID and UMS tests. Then, a third fingerprint (X) from another user is used to create two matching galleries ($A' + X$ and $X + B'$). In this way, we obtained a total of $2000/3 = 666$ multi-biometric templates in three matching galleries.

TABLE 4. Identification and XLNK results for the NIST gallery (666 multi-biometric templates).

		GID	UMS		XLNK		
	Top-#	Σ vs. (A', B')	Σ vs. A'	Σ vs. B'	Σ vs. $(A' + X)$	Σ vs. $(X + B')$	Σ vs. $(A' + B')$
$Method_1$	1	93	75	75	21	32	76
	5	93	75	75	37	39	76
	10	93	75	75	38	39	76
$Method_2$	1	82	74	40	20	10	48
	5	85	75	46	33	16	48
	10	86	75	51	34	19	48
$Method_3$	1	79	58	48	1	37	11
	5	82	59	55	5	47	11
	10	83	59	60	6	50	11

TABLE 5. Identification and XLNK results for the FVC gallery (55 multi-biometric templates).

		GID	**UMS**				**XLNK**			
	Top-#	Σ vs. (A', B')	Σ vs. A'	Σ vs. B'	$\Sigma_3$vs. (A', B')	Σ_3 vs. C'	Σ vs. $(A' + X)$	Σ vs. $(X + B')$	Σ vs. $(A' + B')$	Σ_3 vs. Σ_3'[a]
$Method_1$	1	99	93	92	–	–	82	85	98	–
	5	99	94	93	–	–	84	86	98	–
	10	99	95	95	–	–	87	88	98	–
$Method_2$	1	97	96	81	–	–	85	5	85	–
	5	98	96	82	–	–	87	16	87	–
	10	98	96	96	–	–	90	29	88	–
$Method_3$	1	96	83	74	–	–	53	6	60	–
	5	98	86	81	–	–	60	16	65	–
	10	98	87	87	–	–	67	30	70	–
$Method_4$	1	100	76	77	87	77	–	–	–	63
	5	100	78	80	88	79	–	–	–	68
	10	100	80	83	89	82	–	–	–	75

[a]$\Sigma_3 = (A + B + C)$ and $\Sigma_3' = (A + B + X)$.

Since there are only 11 subjects and 110 different fingers in each of the FVC subgroups, we ran GID tests and UMS attacks with a gallery of 55 templates, obtained by pairing fingerprints two-by-two, for each subgroup. For XLNK tests, we paired the fingers three-by-three such that three fingers were used as if they belonged to the same user, as was done for the NIST database. In this way, we obtained a very small gallery of 36 templates.

8.2. Results

8.2.1. NIST database

For the larger NIST gallery, high genuine identification (GID) rates are achieved showing the premise of the scheme for providing high identification performance. The identification rate decreases as expected as more information is omitted in the template creation. These rates are not very high, but comparable to rank-1 identification rates (∼85% and ∼83%) reported in Ref. [21], obtained using a similar and alternative multi-biometric template creation scheme and a similar size database.

The UMS evaluation that tests whether a multi-biometric template database can be searched with a single fingerprint, results in low identification rates as desired. Compared to GID rates, there is ∼20% points difference between GID and UMS rates, for $Method_1$ and $Method_3$.

The UMS with the second fingerprint achieves roughly the same rate as for the first fingerprint using $Method_1$, as the two fingerprints have a symmetric role in this method. However the top-1 identification rates drop even further (40% and 48%) with $Method_2$ and $Method_3$ where the minutiae angles of the second fingerprint are modified to match the angles of the first fingerprint.

The cross-link (XLNK) evaluations for Σ versus $A' + X$ and Σ versus $X + B'$ where the adversary wants to cross-link

two templates sharing one fingerprint, result in very low identification rates resulted in low success rates, 20% and 10% using $Method_2$ and 1% and 37% for $Method_3$.

The final cross-link evaluation Σ versus $(A' + B')$ results are 76%, 48% and 11% for three methods, respectively. Compared to the genuine identification rates, the results show that the proposed methods provides sufficiently high diversification capability even if the fingers used in two databases are the same.

8.2.2. *FVC database*

With the FVC database, GID rates are very high (99%, 97%, 96% and 100% for the four methods), as shown in Table 5. Unfortunately, the UMS rates are also very high for the first two methods. As for $Method_3$ and $Method_4$, we observe that the UMS rates (83% and 74%) are significantly lower compared to GID rates, as desired. The UMS rates for $Method_4$ have been performed in two types: (i) Σ_3 versus (A', B') and (ii) Σ_3 versus (C') where $\Sigma_3 = (A + B + C)$. In the first one, the attacker has access to two new imprints of the constituent fingers (A', B'), and in the second one she has access to only one (C'). For those attacks, the top-1 rates are 87% and 77%. This shows the protection capability of the system even when the attacker has more resources, using $Method_4$.

The XLNK rates are low in this database too; in particular for $Method_3$, we obtain a 53% rate when the first fingerprint is shared among the two corresponding multi-biometric templates, 6% when the second fingerprint is shared and 60% when both fingerprints are shared. $Method_4$ that combines three fingerprints obtains even higher GID rates and lower UMS and XLNK rates.

In summary, we observe that $Method_3$ obtains significantly lower uni-modal search rates compared to genuine identification rates, as well as very low cross-link rates for both databases. While not applicable in all applications and databases, $Method_4$ obtains even better results, with higher genuine identification rates and lower cross-link rates.

8.3. Time cost for enrollment and verification

The multi-biometric template creation process takes 300 ms for the FVC DB and 1 s for the NIST DB. The matching process takes <10ms with the FVC DB for $Method_1$, and up to 50 ms for $Method_2$ and $Method_3$. For the NIST DB, matching takes <50 ms for $Method_1$, and up to 500 ms for $Method_2$ and $Method_3$. Note that, while verification times are longer than the commercial uni-modal system, they are still acceptable for use in a commercial application.

9. SUMMARY AND DISCUSSION

We have proposed different methods for implementing the biometric layering idea first proposed in Ref. [10]. Below, we discuss the relative merits of these methods in order, based on results observed on the FVC data-sets; but the observations apply to the NIST database for the most part as well.

The first method ($Method_1$), which was the proposed method in Ref. [10], has very good verification rates that are better than the state-of-the-art fingerprint verification rates of theNT matcher (see Table 2) and its GID rate is high, but its UMS rates are also high (see Table 5). Furthermore, since the two fingerprints are layered without extra precaution, there may be a possibility of separating the two fingerprints using minutiae angle coherence.

As the methods try to protect the template more ($Method_2$ and $Method_3$), verification and identification rates fall, but UMS and XLNK rates also decrease as desired. Particularly in $Method_3$, which is the suggested layering method for two fingerprints, the average verification rate for the FVC databases is quite good (3.9%, while NT matcher achieves 1.9%) and the UMS (83% and 74% in a 55-template gallery, Table 5) and XLNK rates (1% and 37%, Table 4) are very low as desired. The performance decrease with respect to $Method_2$ is due to the random removal of minutiae from the primary template. As some genuine minutiae are missing from the multi-biometric template, it is expected that the FRR will increase, for sake of increased template security. Considering that the gallery sizes used for UMS is very small and XLNK tests identification rates are already very low, the significant difference between these rates and the GID rates show the potential of the method in increasing template security.

Combination of three fingerprints (i.e. $Method_4$) is the most successful and suggested method, if the application allows for the use of three modalities. The verification rate in this case is 3%, GID rate is 99%, while UMS rates are low (63–77% in a very small database) and XLNK rates are very low (11–33%).

For the NIST database where the fingerprint templates contain an excessive number of minutiae points, identification and cross link rates are lower in general compared to the FVC database. Hence, while GID rates are not as high as desired (*93%, 82% and 79% for Methods 1, 2 and 3*), cross linking rates are very low (*21%, 20% and 1%, respectively*).

In terms of comparison to other similar systems, we consider the work of Othman and Ross [21] and Li and Kot [22]. As summarized in Section 2, these two systems obtain high identification and verification rates and much lower XLNK rates as desired; however, our method does not have any requirements such as the need to have compatible fingerprints or locate reference points.

A potential weakness is that if Σ is compromised, the attacker can break it into two templates in a random manner, obtaining two dummy constituent templates C and D. She can then use these two templates to break into the system, in *unattended* scenarios. However, note that the attacker does not obtain the real fingerprints and the success would be

limited with $Method_2$ or $Method_3$ due to the replaced angles and randomly removed minutiae.

Finally, we propose $Method_3$ as the best method for biometric layering when the system is required to use two fingerprints. The renewability property of this method may be enhanced by using non-deterministic techniques in random minutiae removal or angle modification phases.

On the other hand, if the application allows for it, we propose $Method_4$ as the best method, since we combine three different fingerprints and achieve even better results than $Method_3$. However due to a large number of minutiae in the template, this method is not suitable for applications requiring very low FAR values.

10. CONCLUSION

We propose to use multi-biometric templates for increased performance, template security and enhanced privacy, and our aim in this work has been to fully explore the potential of this idea. We evaluated three different methods of constructing a multi-biometric template from two fingerprints, using less and less information of the constituent fingerprints for increased template security. Furthermore, a fourth method combines three biometric modalities, to explore the limits of biometric layering.

The proposed framework has been evaluated using public well-known data-sets, which have already been captured from real users or fingerprints that are generated synthetically. The results show that the proposed framework is effective for template security, as well as increased or on par biometric performance. However, in the case of real life tests, there may be issues related to the fatigue due to extra enrollments and complaints about loss of privacy due to giving more fingerprints, as well as other physiological and psychological factors that might affect the quality of the enrolled templates, which in turn might affect the overall system performance. These issues might be addressed in the future research works.

Additionally, we will explore other methods of combination, especially for fixed-length biometric representations.

REFERENCES

[1] Ratha, N.K., Bolle, R., Pandit, V.D. and Vaish, V. (2000) Robust Fingerprint Authentication Using Local Structural Similarity. In *5th IEEE Workshop on Applications of Computer Vision,* pp. 29–34.

[2] Simoens, K., Yang, B., Zhou, X., Beato, F., Busch, C., Newton, E. and Preneel, B. (2012) Criteria Towards Metrics for Benchmarking Template Protection Algorithms. In *5th IAPR Int. Conf. Biometrics (ICB)*, New Delhi, March, pp. 498–505.

[3] Davida, G., Frankel, Y. and Matt, B. (1998) On enabling secure applications through on-line biometric identification. *IEEE Symposium on Security and Privacy*, pp. 148–157.

[4] Juels, A. and Wattenberg, M. (1999) A Fuzzy Commitment Scheme. *Conference on Computer and Communications Security*, ACM Press., pp. 28–36.

[5] Lee, C. and Kim, J. (2010) Cancelable fingerprint templates using minutiae-based bit-strings. *J. Netw. Comput. Appl.*, **33**, 236–246. Recent Advances and Future Directions in Biometrics Personal Identification.

[6] Ratha, N., Connell, J. and Bolle, R. (2001) Enhancing security and privacy in biometrics-based authentication systems. *IBM Syst. J.*, **40**, 614–634.

[7] Linnartz, J. and Tuyls, P. (2003) New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates. In *Proc. Int. Conf. Audio and Video Based Biometric Person Authentication*, pp. 393–402.

[8] Teoh, A., Ngo, D. and Goh, A. (2004) Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognit.*, **37**, 2245–2255.

[9] Juels, A. and Sudan, M. (2002) A fuzzy vault scheme. *IACR Cryptology ePrint Archive*, **2002**, 93.

[10] Yanikoglu, B. and Kholmatov, A. (Aug. 2004) Combining Multiple Biometrics to Protect Privacy. In *Int. Conf. Pattern Recognition, BCTP Workshop, Cambridge, England*.

[11] Camlikaya, E., Kholmatov, A. and Yanikoglu, B. (2008) Multi-biometric templates using fingerprint and voice In Proc. SPIE 6944, Biometric Technology for Human Identification V, pp. 69440I–69440I–9.

[12] Dodis, Y., Reyzin, L. and Smith, A. (2004) Fuzzy Extractors: How to Generate Strong Keys From Biometrics and Other Noisy Data. In *Proc. Int. Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT).*

[13] Sutcu, Y., Li, Q. and Memon, N.D. (2007) Protecting biometric templates with sketch: Theory and practice. *IEEE Trans. Inf. Forensics Security*, **2**, 503–512.

[14] Hao, F., Anderson, R. and Daugman, J. (2006) Combining crypto with biometrics effectively. *IEEE Trans. Computers*, **55**, 1081–1088.

[15] Sutcu, Y., Li, Q. and Memon, N. (2007) Secure Biometric Templates From Fingerprint-Face Features. In *CVPR*, IEEE Computer Society.

[16] Nandakumar, K., Nagar, A. and Jain, A. (2007) Hardening Fingerprint Fuzzy Vault Using Password. Advances in Biometrics: International Conference, Seoul, Korea, pp. 927–937.

[17] Uludag, U., Pankanti, S. and Jain., A. (2005) Fuzzy Vault for Fingerprints. In *Proc. Int. Conf. Audio and Video Based Biometric Person Authentication*, pp. 310–319.

[18] Nandakumar, K. and Jain, A. (2008) Multibiometric Template Security Using Fuzzy Vault. In IEEE Second Int. Conf. on Biometrics: Theory, Applications and Systems, Washington D.C., USA, pp. 1–6.

[19] Nagar, A., Nandakumar, K. and Jain, A. (2012) Multibiometric cryptosystems based on feature-level fusion. *IEEE Trans. Info. Forensics Security*, **7**, 255–268.

[20] Kong, A., Cheung, K., Zhang, D., Kamel, M. and You, J. (2006) An analysis of biohashing and its variants. *Pattern Recogn.*, **39**, 1359–1368.

[21] Othman, A. and Ross, A. (2013) On mixing fingerprints. *IEEE Trans. Info. Forensics Security*, **8**, 260–267.

[22] Li, S. and Kot, A.C. (2013) Fingerprint combination for privacy protection. *IEEE Trans. Inf. Forensics Security*, **8**, 350–360.

[23] Snelick, R., Uludag, U., Mink, A., Indovina, M. and Jain, A. (2005) Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems. *IEEE Trans. Pattern Anal. Mach. Intell.*, **27**, 450–455.

[24] Maltoni, D., Maio, D., Jain, A. and Prabhakar, S. (2009) *Handbook of Fingerprint Recognition* (2nd edition). Springer, London.

[25] Brunelli, R. and Yau, W.Y. (Oct. 1995) Person identification using multiple cues. *IEEE Trans. Pattern Anal. Mach. Intell.*, **17**, 955–966.

[26] Toh, K. and Yau, W.Y. (2003) Fingerprint and speaker verification decisions fusion. In IEEE Transactions on Systems, Man, and Cybernetics, Part C, pp. 626–631.

[27] 2005) Fingerprint and speaker verification decisions fusion using a functional link network. *IEEE Trans. Systems, Man Cybernetics*, **35**, 357–370.

[28] Anzar, S. and Sathidevi, P. (2013) Adaptive score level fusion of fingerprint and voice combining wavelets and separability measures. *Int. J. Electron. Commun.*, **67**, 733–742.

[29] Ben-Yacoub, S., Abdeljaoued, Y. and Mayoraz, E. (1999) Fusion of face and speech data for person identity verification. *IEEE Trans. Neural Netw.*, 10, 1065–1075.

[30] Kittler, J., Hatef, M., Duin, R. and Matas, J. (Mar. 1998) On combining classifiers. *IEEE Trans. Pattern Anal. Mach. Intell.*, **20**, 226–239.

[31] Hong, L. and Jain, A.K. (1998) Integrating faces and fingerprints for personal identification. In Chin, R.T. and Pong, T.-C. ACCV (1), *Lecture Notes in Computer Science*, **1351**, 16–23. Springer.

[32] NEUROTechnology (2014). Neurotechnology, biometric and artificial intelligence technologies. http://www.neurotechnology.com/. (accessed September 20, 2014).

[33] Feng, J. and Jain, A. (2011) Fingerprint reconstruction: From minutiae to phase. *IEEE Trans. Pattern Anal. Mach. Intell.*, **33**, 209–223.

[34] Bazen, A. and Gerez, S. (2003) Fingerprint matching by thin-plate spline modelling of elastic deformations. *Pattern Recogni.*, **36**, 1859–1867.

[35] Ross, A., Shah, J. and Jain, A.K. (2007) From template to image: Reconstructing fingerprints from minutiae points. *IEEE Trans. Pattern Anal. Mach. Intell.*, **29**, 544–560.

[36] FVC (2000). *FVC2000 finger verification competition databases*. http://bias.csr.unibo.it/fvc2000/databases.asp. (accessed September 20, 2014).

[37] FVC (2002). *FVC2002 finger verification competition databases*. http://bias.csr.unibo.it/fvc2002/databases.asp. (accessed September 20, 2014).

[38] NIST (2010). *NIST special database 4*. http://www.nist.gov/srd/nistsd4.cfm. (accessed September 20, 2014).