MIXING FINGERPRINTS FOR TEMPLATE SECURITY AND PRIVACY

Arun Ross and Asem Othman

Lane Department of Computer Science and Electrical Engineering, West Virginia University
{arun.ross, asem.othman}@mail.wvu.edu
http://www.csee.wvu.edu/∼ross

ABSTRACT

Securing a stored fingerprint image is of paramount importance because a compromised fingerprint cannot be easily revoked. In this work, an input fingerprint image is mixed with another fingerprint (e.g., from a different finger), in order to produce a new mixed image that obscures the identity of the original fingerprint. Mixing fingerprints creates a new entity that looks like a plausible fingerprint and, thus, (a) it can be processed by conventional fingerprint algorithms and (b) an intruder may not be able to determine if a given print is mixed or not. To mix two fingerprints, each fingerprint is decomposed into two components, viz., the continuous and spiral components. After pre-aligning the two components of each fingerprint, the continuous component of one fingerprint is combined with the spiral component of the other fingerprint image in order to generate a mixed fingerprint. Experiments on the WVU and FVC2000 datasets show that the mixed fingerprint can potentially be used for authentication and that the identity of the original fingerprint cannot be easily deduced from the mixed fingerprint. Further, the mixed fingerprint can facilitate in the generation of cancelable templates.

1. INTRODUCTION

Preserving the privacy of the stored biometric template (e.g., fingerprint image) is necessary to mitigate concerns related to data sharing and data misuse [10]. This has heightened the need to impart privacy to the stored template, i.e., to de-identify it in some way. De-identifying biometric templates is possible by transforming it into a new template using a set of application-specific transformation functions, such that the original identity cannot be easily deduced from the transformed template. A template that is transformed in this way is referred to as a cancelable template since it can be "canceled" by merely changing the transformation function [3] [17]. At the same time, the transformed template can be used during the matching stage *within* each application while preventing cross-application matching. Further, the transformation parameters can be changed to generate a new template if the stored template is deemed to be compromised.

There has been a vast amount of work done in generating a cancelable fingerprint template [16].[1] In this study, we consider the problem of mixing two fingerprint images in order to generate a new cancelable fingerprint image. The mixed image incorporates characteristics from both the original fingerprint images, and can be used in the feature extraction and matching stages of a biometric system. Mixing fingerprints can be useful in several applications: (a) it can be used to obscure the information present in an individual's fingerprint image prior to storing it in a central database; (b) it can be used to generate a cancelable template, i.e., the template can be reset if the mixed fingerprint is compromised; (c) it can be used to generate virtual identities by mixing fingerprint images pertaining to an individual; and (d) it can potentially be used for fingerprint mosaicing [19]. The mixing process begins by decomposing each fingerprint image into two components, viz., the continuous and spiral components (see Figure 1). Next, the two components of each fingerprint are aligned to a common coordinate system. Finally, the continuous component of one fingerprint is combined with the spiral component of the other fingerprint. The experimental results confirm that (a) the new fused fingerprint can potentially be used for authentication and (b) the identity of the original fingerprint cannot be easily deduced from the mixed fingerprint.

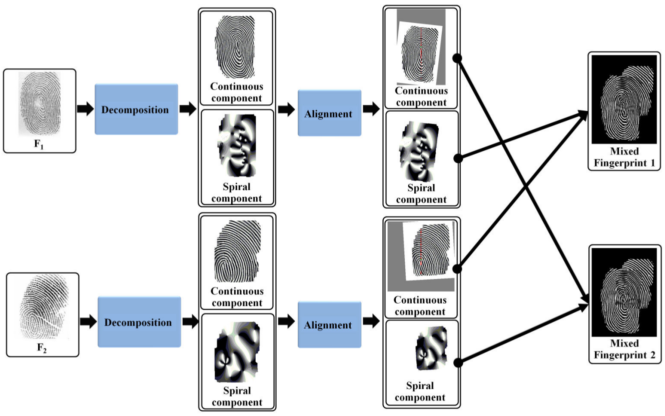


Figure 1: Proposed approach for mixing fingerprints

The concept of fingerprint mixing[2] can be utilized in the following ways.

Scenario I: Consider a fingerprint system in which the left index finger, FL_s, of subject ID_s is being enrolled. During enrollment, an impression of another finger of the subject (say the right index finger, FR_s) is mixed with FL_s resulting in a mixed print M_s. Next, M_s is stored in the central database while the images FL_s and FR_s are discarded. During authentication, the subject offers a sample of the left index finger, FL'_s, and a sample of the right index finger, FR'_s. These two images are then mixed resulting in a new print M'_s. In order to verify the subject's identity, M'_s is compared with M_s in the database. Therefore, the original fingerprint images of the left and right index fingers are never stored in the database.

Scenario II: Consider a fingerprint system that maintains a small set of pre-determined auxiliary fingerprints, $\mathscr{A}$, corresponding to multiple fingers (each finger in $\mathscr{A}$ is assumed to have multiple impressions). Suppose that subject ID_s offers the left index finger, FL_s, during enrollment. At that time, the system searchers through the auxiliary set to locate a "compatible" fingerprint, say F_A^m (here the superscript m denotes a specific finger in the auxiliary set), which is then mixed with FL_s to generate a new mixed print M_s that is stored in the database; FL_s is discarded. During authentication, when the subject presents a sample of the left index finger, FL'_s, once again, the system determines the most "compatible" fin-

[1] For an excellent review on the topic of Biometric Security in general, please see [9].

[2] This work does not claim that mixing fingerprints is better than other methods for template security and privacy; a more extensive treatment is necessary to establish that. Rather, it provides an alternate way of approaching the problem - an approach that has hitherto not been studied in the literature.

gerprint, say F_A^n, from the auxiliary set. FL_s' is mixed with F_A^n to generate a mixed fingerprint M_s', which is then compared against the database entry M_s. Here, there are 3 possibilities: (a) F_A^m and F_A^n could be the exact same fingerprint from $\mathscr{A}$, i.e., $F_A^m = F_A^n$; (b) F_A^m and F_A^n could be different impressions of the same finger, i.e., $F_A^m \neq F_A^n$ and $m = n$; or (c) F_A^m and F_A^n are from different fingers, i.e., $m \neq n$. Possibilities (a) and (b) are preferable for successful matching of M_s with M_s'.

The rest of the paper is organized as follows. Section 2 presents the proposed approach for mixing fingerprints. Section 3 reports the experimental results and Section 4 concludes the paper.

2. MIXING FINGERPRINTS: THE PROPOSED APPROACH

The ridge flow of a fingerprint can be represented as a 2D Amplitude and Frequency Modulated (AM-FM) signal [13]:

$$I(x,y) = a(x,y) + b(x,y)cos(\Psi(x,y)) + n(x,y), \qquad (1)$$

where $I(x,y)$ is the intensity of the original image at (x,y), $a(x,y)$ is the intensity offset, $b(x,y)$ is the amplitude, $cos(\psi(x,y))$ is the phase and $n(x,y)$ is the noise. Based on the Helmholtz Decomposition Theorem [5], the phase can be uniquely decomposed into the continuous phase and the spiral phase, $\Psi(x,y) = \psi_c(x,y) + \psi_s(x,y)$. As shown in Figure 1, the continuous component, $\cos(\psi_c(x,y))$, defines the local ridge orientation and the spiral component, $\cos(\psi_s(x,y))$, characterizes the minutiae locations.

2.1 Fingerprint Decomposition

Since ridges and minutiae can be completely determined by the phase, we are only interested in $\Psi(x,y)$. The other three parameters in Equation (1) contribute to the realistic textural appearance of the fingerprint. Before the decomposition task, the phase $\Psi(x,y)$ must be reliably estimated; this is termed as demodulation.

2.1.1 Vortex demodulation

The objective of vortex demodulation [12] is to extract the amplitude $b(x,y)$ and phase $\Psi(x,y)$ of the fingerprint pattern. First, the DC term $a(x,y)$ has to be removed since the failure to remove this offset correctly may introduce significant errors in the demodulated amplitude and phase [12]. To facilitate this, a normalized fingerprint image, $f(x,y)$, containing the enhanced ridge pattern of the fingerprint (generated by the VeriFinger SDK[3]) is used. From Equation (1), $f(x,y) = I(x,y) - a(x,y) \simeq b(x,y)cos(\Psi(x,y))$. The vortex demodulation operator $\mathbf{V}$ takes the normalized image $f(x,y)$ and applies a spiral phase Fourier multiplier $\exp[i\Phi(u,v)]$:

$$\begin{aligned} \mathbf{V}\{f(x,y)\} = F^{-1}\{\exp[i\Phi(u,v)].F\{b(x,y).\cos[\Psi(x,y)]\}\} \\ \cong -i\exp[i\beta(x,y)].b(x,y).\sin[\Psi(x,y)] \end{aligned} \qquad (2)$$

where, F is the Fourier transform, F^{-1} is the inverse Fourier transform and $\exp[i\Phi(u,v)]$ is a 2-D signum function [12] defined as a pure spiral phase function in the spatial frequency space (u,v):

$$\exp[i\Phi(u,v)] = \frac{u+iv}{\sqrt{u^2+v^2}}. \qquad (3)$$

Note that in Equation (2) there is a new parameter, $\beta(x,y)$, representing the perpendicular direction of the ridges. In Equation (4), this directional map is used to isolate the desired magnitude and phase from Equation (2), i.e.,

$$-\exp[-i\beta(x,y)].\mathbf{V}\{f(x,y)\} = ib(x,y).\sin[\Psi(x,y)]. \qquad (4)$$

Then, Equation (4) can be combined with the normalized image, $f(x,y)$, to obtain the magnitude $b(x,y)$ and the raw phase map $\Psi(x,y)$ as follows:

$$-\exp[-i\beta(x,y)].\mathbf{V}\{f(x,y)\} + f(x,y) = b(x,y).\exp(i\Psi(x,y)). \quad (5)$$

Therefore, determining $\beta(x,y)$ is essential for obtaining the amplitude and phase functions, $b(x,y)$ and $\Psi(x,y)$, respectively. The direction map $\beta(x,y)$ can be derived from the orientation image of the fingerprint by a process called unwrapping. A sophisticated unwrapping technique using the topological properties of the ridge flow fields is necessary to account for direction singularities such as cores and deltas [13] [4].

2.1.2 Direction Map $\beta(x,y)$

Direction is uniquely defined in the range 0° to 360° (modulo 2π). In contrast, fingerprint ridge orientation is indistinguishable from that of a 180° rotated ridge (modulo π). Therefore, the fingerprint's *orientation* image, denoted by $\theta(x,y)$, should be unwrapped to a *direction* map, $\beta(x,y)$ [13]. Phase unwrapping is a technique used to address a 2π phase jump in the orientation map. The unwrapping process adds or subtracts an offset of 2π to successive pixels whenever a phase jump is detected [5]. This process proceeds by starting at any pixel within the orientation image and using the local orientation information to traverse the image pixel-by-pixel, and assigning a direction (i.e., the traversed direction) to each pixel with the condition that there are no discontinuities of 2π between neighboring pixels. However, the presence of flow singularities means that there will be pixels in the orientation image with a discontinuity of $\pm 2\pi$ in the traversed direction and, therefore, the above unwrapping technique will fail. In fingerprint images, the flow singularities arise from the presence of singular points such as core and delta. Figure 2(a) illustrates that estimating the direction of ridges in the vicinity of a core point by starting at any point within the highlighted rectangle and arbitrarily assigning one of two possible directions, can result in an inconsistency in the estimated directions inside the dashed circle. This inconsistency in the estimated direction map can be avoided by using a branch cut [5]. The branch cut is a line or a curve used to isolate the flow singularity and which cannot be crossed by the unwrapping paths. Consequently, branch cut prevents the creation of 2π discontinuities and restores the path independence of the unwrapping process. As shown in Figure 2(b), tracing a line down from the core point and using this line as a barrier resolves the inconsistency near the core point (i.e, inside the dashed circle) by selecting two different directions in each side of the branch cut within the same region (i.e, inside the highlighted rectangle).

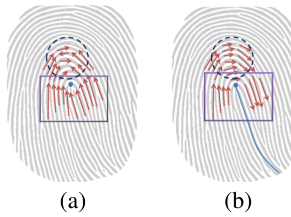


Figure 2: A portion of the estimated direction map (a) without assigning a branch cut and (b) after assigning a branch cut [7]

The adopted strategy, based on the techniques described in [13] [7] [4] to estimate the direction map $\beta(x,y)$, is summarized in the following three steps.

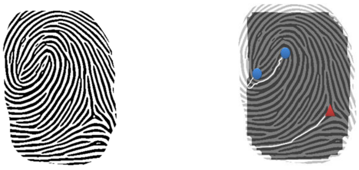
1. The orientation image $\theta(x,y)$ of the normalized fingerprint $f(x,y)$ is determined via the least mean-square method [8]. Then the Poincaré [14] index is used to locate the singular points, if any.

2. In case there are singular points, an algorithm is applied to extract the branch cuts along suitable paths such as ridge contours, as shown in Figure 2(b), to resolve the inevitable direction ambiguities near those singularities. The branch cuts are extracted by tracing the contours of ridges (rather than the orientation field) in the skeleton images. The algorithm starts from each singular point in a skeleton image until the trace reaches the border of the segmented foreground region of the fingerprint or

[3] http://www.neurotechnology.com

when it encounters another singular point. To generate the skeleton images, first, a set of smoothed orientation maps are generated by applying a smoothing operation at different smoothing scales ($\sigma \in \{1,2,3,5,10,15,20,32,50,64\}$) on $\theta(x,y)$. Next, a set of Gabor filters, tuned to the smoothed orientation maps [8], is convolved with the normalized image $f(x,y)$. Then, a local adaptive thresholding and thinning algorithm [20] is applied to the directionally filtered images producing 10 skeleton images. Thus, there are at least 10 branch cuts and the shortest one, associated with each singular point, is selected. Figure 3 shows the final extracted branch cuts from all singular points.

3. The phase unwrapping algorithm [6] [5] starts from any arbitrary pixel in the orientation map $\theta(x,y)$ and visits the other pixels, which are unwrapped in the same manner as in images without singularity, with the exception here that the branch cuts cannot be crossed. Then, each branch cut is visited individually and its pixels are traced and unwrapped.



(a) Normalized Fingerprint (b) Branch Cuts

Figure 3: Example of a fingerprint with three singular points (2 cores and 1 delta). (a) The normalized fingerprint. (b) The extracted branch cuts obtained by tracing the ridges instead of the orientation.

Finally, the direction map of the wave normal $\beta(x,y)$ is determined from the unwrapped $\theta(x,y)$ by adding $\pi/2$ which allows for the determination of the amplitude $b(x,y)$ and phase $\Psi(x,y)$ modulations of fingerprint image from Equation (5).

2.1.3 *Helmholtz Decomposition*

The Helmholtz Decomposition Theorem [5] is used to decompose the determined phase $\Psi(x,y)$ of a fingerprint image into two phases. The first phase, ψ_c is a continuous one, which can be unwrapped, and the second is a spiral phase,ψ_s, which cannot be unwrapped but can be defined as a phase that exhibits spiral behavior at a set of discrete points in the image. The Bone's residue detector [1] [5] is first used to determine the spiral phase $\psi_s(x,y)$ from the demodulated phase $\Psi(x,y)$. Next the continuous phase, is computed as $\psi_c(x,y) = \Psi(x,y) - \psi_s(x,y)$. Finally, the extracted branch cuts from the previous step are used again to unwrap the continuous phase.

2.2 Fingerprint Pre-alignment

To mix two different fingerprints after decomposing each fingerprint into its continuous component $cos(\psi_c(x,y))$ and spiral component $cos(\psi_s(x,y))$, the components themselves should be appropriately aligned. Previous research has shown that two fingerprints can be best aligned using their minutiae correspondences. However, it is difficult to insure the existence of such correspondences between two fingerprints acquired from different fingers. In this paper, the components are pre-aligned to a common coordinate system prior to the mixing step by utilizing a reference point and an alignment line. The reference point is used to center the components. The alignment line is used to find a rotation angle about the reference point. This angle rotates the alignment line to make it vertical. The two phase components of each fingerprint are rotated by the same angle.

2.2.1 *Locating a reference point*

The reference point used in this work is the northern most core point of extracted singularities. For plain arch fingerprints or partial fingerprint images, Novikov et al.'s technique [15] [18], based on the Hough transform, is used to detect the reference point.

2.2.2 *Finding the alignment line*

The first step in finding the alignment line is to extract high curvature points from the skeleton of the fingerprint image's continuous component. Next, horizontal distances between the reference point and all high curvature points are calculated. Then, based on these distances, an adaptive threshold is applied to select and cluster points near the reference point. Finally, a line is fitted through the selected points to generate the alignment line.

2.3 Mixing Fingerprints

Let F_1 and F_2 be two different fingerprint images from different fingers, and let $\psi_{ci}(x,y)$ and $\psi_{si}(x,y)$ be the pre-aligned continuous and spiral phases, $i = 1,2$. As shown in Figure 1, there are two different mixed fingerprint image that can be generated, MF_1 and MF_2:

$$\begin{aligned} MF_1 &= \cos(\psi_{c2} + \psi_{s1}), \\ MF_2 &= \cos(\psi_{c1} + \psi_{s2}). \end{aligned} \tag{6}$$

The continuous phase of F_2 (F_1) is combined with the spiral phase of F_1 (F_2) which generates a new fused fingerprint image MF_1 (MF_2).

2.4 Compatibility Measure

Variations in the orientations and frequencies of ridges between fingerprint images can result in visually unrealistic mixed fingerprint images, as shown in Figure 4. This issue can be mitigated if the two fingerprints to be mixed are carefully chosen using a compatibility measure. In this paper, the compatibility between fingerprints is computed using non-minutiae features, viz., orientation fields and frequency maps of fingerprint ridges.

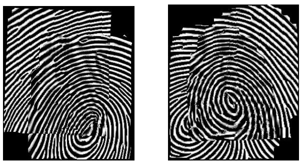


Figure 4: Examples of mixed fingerprints that look unrealistic.

The orientation and frequency images are computed from the pre-aligned continuous component of a fingerprint using the technique described in [8]. Then, Yager and Amin's [21] approach is used to compute the compatibility measure. To compute the compatibility between two fingerprint images, their orientation fields and frequency maps are first estimated (see below). Then, the compatibility measure C between them is computed as the weighted sum of the normalized orientations and frequency differences, OD and FD, respectively:

$$C = 1 - (\alpha.OD + \gamma.FD), \tag{7}$$

where α and γ are weights that are determined empirically.

Figure 5 shows examples of mixed fingerprints after utilizing the compatibility measure[4] to select the fingerprints pairs, (F_1, F_2).

[4] Perfect compatibility ($C = 1$) is likely to occur when the two prints to be mixed are from the same finger - a scenario that is *not* applicable in the proposed application. On the other hand, two fingerprints having significantly different ridge structures are unlikely to be compatible ($C = 0$) and will generate an unrealistic looking fingerprint. Between these two extremes, lies a range of possible compatible values that is acceptable. However, determining this range automatically may be difficult.

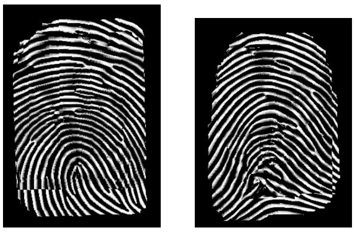


Figure 5: Examples of mixed fingerprints that appear to be visually realistic.

2.4.1 Orientation Fields Difference (OD)

The difference in orientation fields between F_1 and F_2 is computed as

$$OD = \left(\frac{1}{S}\right) \sum_{(x,y)\in S} d(\theta_1(x,y), \theta_2(x,y)), \tag{8}$$

where S is a set of coordinates within the overlapped area of the aligned continuous components of two different fingerprints, and θ_1 and θ_2 represent the orientation fields of the two fingerprints. If orientations are restricted to the range $[-\pi/2, \pi/2]$, the operator $d(.)$ is written as

$$d(\alpha,\gamma) = \begin{cases} \pi - (\alpha-\gamma), & \text{if } \frac{\pi}{2} < \alpha - \gamma \\ |\alpha-\gamma|, & \text{if } -\frac{\pi}{2} < \alpha-\gamma < \frac{\pi}{2} \\ \pi + (\alpha-\gamma), & \text{if } \alpha-\gamma \leq -\frac{\pi}{2}. \end{cases} \tag{9}$$

2.4.2 Frequency Maps Difference (FD)

Local ridge frequencies are the inverse of the average distance between ridges in the local area in a direction perpendicular to the local orientation. Hong et al.'s approach [8] is used to find the local ridge frequencies of the continuous component of a fingerprint image. The difference function is computed as

$$FD = \left(\frac{1}{S}\right) \sum_{(x,y)\in S} |Freq_1(x,y) - Freq_2(x,y)|, \tag{10}$$

where S is a set of coordinates within the overlapped area, and $Freq_1$ and $Freq_2$ represent the frequency maps of the two fingerprints F_1 and F_2, respectively.

3. EXPERIMENTS AND DISCUSSION

The performance of the proposed fingerprints mixing approach was tested using two different datasets. The first dataset was taken from the West Virginia University (WVU) multimodal biometric database [2]. A subset of 300 images corresponding to 150 fingers (two impressions per finger) was used. The second dataset was the FVC2000 DB2 fingerprint database containing 110 fingers with 8 impressions per finger (a total of 880 fingerprints). The VeriFinger SDK was used to generate the normalized fingerprint images and the matching scores. Also, an open source Matlab implementation [11] based on Hong et al.'s approach [8] was used to compute the orientation and frequency images of the fingerprints. In order to establish the baseline performance, for each finger in each dataset, N impressions were used as probe images and an equal number were added to the gallery ($N = 1$ for the WVU dataset and $N = 4$ for the FVC2000-DB2). This resulted in a rank-1 accuracy of $\sim$ 100% for the WVU dataset and $\sim$ 99.7% for the FVC2000 dataset. The EERs for these two datasets were 0% and 1.4%, respectively. With regards to mixing fingerprints for de-identification, the following questions are raised:

1. What impact does mixing fingerprints have on the matching performance, i.e., can two mixed impressions pertaining to the same identity be successfully matched?

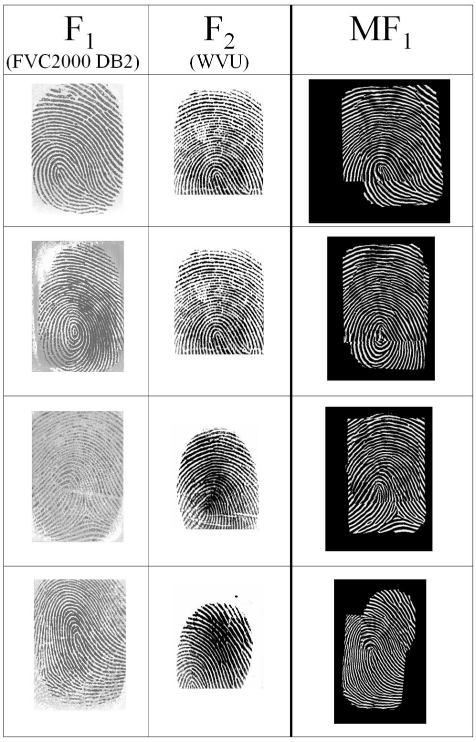


Figure 6: Examples of mixing fingerprints where F_1 and F_2 are fingerprints from the FVC2000 and WVU datasets, respectively.

2. Are the original fingerprint and the mixed fingerprint correlated? It is essential to assure that the proposed approach prevents identity linking, by preventing the possibility of successfully matching the original print with the mixed print.

3. Does mixing result in cancelable templates? In case a stored fingerprint is compromised, a new mixed fingerprint can be generated by mixing the original with a new fingerprint. The new mixed fingerprint and the compromised mixed image must be sufficiently different, even though they are derived from the same finger. Another way of looking at this is as follows: if two different fingerprints, F_1 and F_2, are mixed with the same fingerprint F_m, are the resulting mixed fingerprints, M_1 and M_2, correlated? From the perspective of security, they should *not* be correlated.

- **Experiment 1:** The purpose of this experiment was to investigate the impact of the proposed approach on the matching performance. Therefore, fingerprints from FVC 2000-DB2 were de-identified by mixing them with fingerprints from the WVU dataset. For each fingerprint in FVC 2000-DB2 noted by F_1, its compatibility measure with each fingerprint in the WVU dataset (300 images of 150 subjects) was computed using Equation (7) with $\alpha = 0.6$ and $\gamma = 0.4$. Based on the computed compatibility measures, the spiral component of F_1 was combined with the continuous component of the most compatible fingerprint image F_2 in the WVU dataset, resulting in the mixed fingerprint MF_1. Figure 6 shows examples of mixed fingerprints. Because there are 8 impressions per finger in FVC2000-DB2, the mixing process resulted in 8 impressions per mixed finger. Four of these mixed impressions were used as probe images and the rest (four impressions) were added to the gallery set. The obtained rank-1 accuracy was $\sim$ 81% and the EER was $\sim$ 9%. This indicates the possibility of matching mixed fingerprints. Currently, ways to further improve the rank-1 accuracy of mixed fingerprints is being examined.
- **Experiment 2:** In this experiment, the possibility of exposing the identity of the FVC2000-DB2 fingerprint image by using

the mixed fingerprint images was investigated. The mixed fingerprints MF_1 (8 impressions per finger) were matched against the original images in FVC2000-DB2. The resultant rank-1 accuracy was less than 30% (and the EER was more than 35%) suggesting that the original identity cannot be easily deduced from the mixed image.

- **Experiment 3:** The purpose of this experiment was to investigate if the proposed approach can be used to cancel a compromised mixed fingerprint and generate a new mixed fingerprint by mixing the original fingerprint with a new fingerprint. To evaluate this, the 8 impressions of one single fingerprint in the FVC2000-DB2 database were selected. Next, this fingerprint was mixed with each of the 150 fingers in the WVU dataset. This resulted in 150 mixed fingerprints with 8 impressions per finger. Four of these mixed impressions were used as probe images and the rest (four impressions) were added to the gallery set. Thus, each image in the probe set was compared against all images in the gallery set in order to determine a match. A match is deemed to be correct (i.e., the probe is correctly identified) if the probe image and the matched gallery image are from the same finger. In the resulting experiments, the rank-1 identification accuracy obtained was 89%. The reasonably high identification rate suggests that the 150 mixed fingerprints are different from each other. This means, the fingerprint from the FVC2000-DB2 database was successfully "canceled" and converted into a new "identity" based on the choice of the fingerprint selected from the WVU database for mixing.
- **Experiment 4:** In this experiment, two different fingerprints from FVC2000-DB2, F_1 and F_2, were mixed with each of the 150 different fingers in the WVU dataset. This resulted in two set of mixed fingerprints - one based on F_1 and the other based on F_2. Matching these two sets against each other resulted in a rank-1 accuracy of 5% and an EER of 45%. This suggests that two different fingerprints mixed with a common fingerprint cannot be easily matched against each other. This further confirms the cancelable aspect of the proposed approach.

4. CONCLUSIONS

In this work, it was demonstrated that a fingerprint can be de-identified by mixing it with another fingerprint. To mix two fingerprints, each fingerprint is decomposed into two components, viz., the continuous and spiral components. After aligning the components of each fingerprint, the continuous component of one fingerprint is combined with the spiral component of the other fingerprint image. Experiments on two fingerprint databases show that (a) the new mixed fingerprint can potentially be used for authentication, (b) the original fingerprint cannot be easily matched with the mixed fingerprint, (c) the same fingerprint can be used in various applications and cross-matching between applications can be prevented by mixing the original fingerprint with a different fingerprint, and (d) mixing different fingerprints with the same fingerprint resulted in different identities. This work is preliminary and, hence, a more formal analysis of the security aspect is necessary. Further work is required to enhance the performance due to mixed fingerprints by exploring alternate algorithms for selecting and mixing the different pairs.

Acknowledgments

This project was funded by US NSF CAREER Grant No. IIS 0642554. Thanks to Aglika Gyaourova for her valuable comments.

REFERENCES

[1] D. Bone. Fourier fringe analysis: the two-dimensional phase unwrapping problem. *Applied Optics*, 30(25):3627–3632, 1991.

[2] S. Crihalmeanu, A. Ross, S. Schuckers, and L. Hornak. A protocol for multibiometric data acquisition, storage and dissemination. Technical report, Lane Department of Computer Science and Electrical Engineering, WVU, 2007.

[3] G. I. Davida, Y. Frankel, and B. J. Matt. On enabling secure applications through off-line biometric identification. In *IEEE Symposium on Security and Privacy*, pages 148–157, 1998.

[4] J. Feng and A. K. Jain. Fingerprint reconstruction: From minutiae to phase. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 33(2):209 –223, Feb. 2011.

[5] D. Ghiglia and M. Pritt. *Two-dimensional phase unwrapping: theory, algorithms, and software*. Wiley New York, 1998.

[6] R. Goldstein, H. Zebker, and C. Werner. Satellite radar interferometry- Two-dimensional phase unwrapping. *Radio Science*, 23(4):713–720, 1988.

[7] B. Hastings. An integrated representation of fingerprint patterns. In 16^{th} *School of Computer Science & Software Engineering Research Conference, Yanchep, Western Australia*, June 2008.

[8] L. Hong, Y. Wan, and A. Jain. Fingerprint image enhancement: algorithm and performance evaluation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20(8):777 –789, Aug. 1998.

[9] A. Jain, K. Nandakumar, and A. Nagar. Biometric template security. *EURASIP Journal on Advances in Signal Processing*, 2008:1–17, 2008.

[10] A. Jain, A. Ross, and U. Uludag. Biometric template security: Challenges and solutions. In *Proceedings of European Signal Processing Conference (EUSIPCO)*, pages 469–472, 2005.

[11] P. D. Kovesi. MATLAB and Octave functions for computer vision and image processing. Centre for Exploration Targeting, School of Earth and Environment, The University of Western Australia. Available at: <http://www.csse.uwa.edu.au/∼pk/research/matlabfns/>.

[12] K. G. Larkin, D. J. Bone, and M. A. Oldfield. Natural demodulation of two-dimensional fringe patterns. I. General background of the spiral phase quadrature transform. *J. Opt. Soc. Am. A*, 18(8):1862–1870, 2001.

[13] K. G. Larkin and P. A. Fletcher. A coherent framework for fingerprint analysis: are fingerprints holograms? *Opt. Express*, 15(14):8667–8677, 2007.

[14] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar. *Handbook of fingerprint recognition*. Springer-Verlag New York Inc, 2009.

[15] S. O. Novikov and V. S. Kot. Singular feature detection and classification of fingerprints using hough transform. volume 3346, pages 259–269. SPIE International Workshop on digital image processing and computer graphics, 1998.

[16] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle. Generating cancelable fingerprint templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pages 561–572, 2007.

[17] N. Ratha, J. Connell, and R. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614–634, 2001.

[18] A. Ross, J. Shah, and A. Jain. From template to image: reconstructing fingerprints from minutiae points. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):544–560, 2007.

[19] A. Ross, S. Shah, and J. Shah. Image versus feature mosaicing: A case study in fingerprints. In *Proceedings of SPIE Conference on Biometric Technology for Human Identification III*, pages 620208–1 – 620208–12, 2006.

[20] R. Thai. *Fingerprint image enhancement and minutiae extraction*. PhD thesis, School of Computer Science and Software Engineering, The University of Western Australia, 2003.

[21] N. Yager and A. Amin. Fingerprint alignment using a two stage optimization. *Pattern Recognition Letters*, 27(5):317–324, 2006.