Mixing the Fingerprint Components to Generate a Virtual Identity

Keerthana S[1], Vijetha[2]

[1,2]Assistant Professor, Dept. of CSE, SIT Mangalore, Karnataka

Abstract - This work explores the possibility of mixing two different fingerprints [4], pertaining to two different fingers, in order to generate a new fingerprint. To mix two fingerprints, each fingerprint pattern is decomposed into two different components, the continuous and spiral components. Each component is then prealigned. After prealigning the spiral of one fingerprint is mixed with the continuous of the other to generate a new fingerprint.

Key Words: Fingerprints, decomposition, mixing biometrics.

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. 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 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 cancellable template since it can be “cancelled” by merely changing the transformation function. At the same time, the transformed template can be used during the matching stage within each application while preventing cross-application matching.

In this paper, two fingerprint impressions acquired from two different fingers are fused into a new fingerprint image resulting in a new identity. The mixed image incorporates characteristics from both the original fingerprint images, and can be used directly in the feature extraction and matching stages of an existing fingerprint recognition system. As shown in Fig. 1, the mixing process begins by decomposing each fingerprint image into two different components, viz., the continuous and spiral components. The continuous component defines the ridge orientation, and the spiral component characterizes the minutiae locations. Next, the two components of each fingerprint are aligned. Finally, the aligned continuous component of one fingerprint is combined with the aligned spiral component of the other fingerprint. The new fingerprint .representing a new identity, can potentially be used for authentication. The mixed fingerprint is dissimilar from the original fingerprints and the proposed method can be utilized to generate different-sized databases of virtual identities from a fixed fingerprint dataset. The rest of the paper is organized as follows. Section II presents the related work. Section III presents the proposed approach for mixing fingerprints. Section IV concludes the paper.

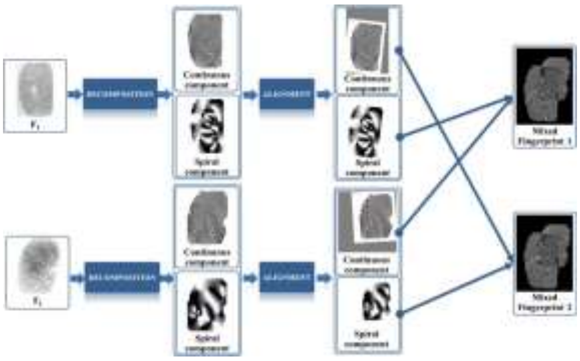

Fig -1: Proposed approach for generating mixed fingerprints

2. RELATED WORK

The major motivation behind the concept of mixing fingerprints was to ensure the security and privacy of fingerprints. There were a number of methods which can be used for fingerprint privacy. Some of them were fingerprint encryption, transformation and combination of multiple biometrics.

Biometric authentication [2] offers a new mechanism for key security by using a biometric to secure the cryptographic key. Instead of entering a passcode to access the cryptographic key, the use of this key is guarded by biometric authentication. When a user wishes to access a secured key, he or she will be prompted to allow for the capture of a biometric sample. If this verification sample matches the enrollment template, then the key is released and can be used to encrypt or decrypt the desired data.

Ratha et al [3] proposed the use of distortion functions to generate biometric data that can be cancelled if necessary. They use a non-invertible transformation function that distorts the input biometric signal (e.g., face image) prior to feature extraction or, alternately, modifies the extracted feature set (e.g., minutiae points) itself. When a stored template is compromised, then the current transformation function is replaced with a new function thereby cancelling the current (compromised) template and generating a new one.

B. Yanikoglu [1] propose a biometric authentication framework to address these privacy concerns. In particular, two biometric features (e.g. fingerprints) are combined to obtain a non-unique identifier of the individual and stored as such in a central database. In this method the person provides two fingerprints. The features (e.g. Minutiae points) of those two fingerprints are extracted. The feature of first fingerprint is combined with the second one to generate a virtual identity.

3. MIXING FINGERPRINTS: THE PROPOSED APPROACH

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

$$I(x,y) = a(x,y) + b(x,y)cos\big(\varphi(x,y)\big) + n(x,y),$$

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,$\varphi(x,y)$ is the phase and $n(x,y)$ is the noise. The phase can be uniquely decomposed into the continuous phase and the spiral phase.

3.1 FINGERPRINT DECOMPOSITION

Since ridges and minutiae can be completely determined by the phase, we are only interested in $\varphi(x,y)$, the other three parameters contribute to the realistic textural appearance of the fingerprint. Before fingerprint decomposition, the phase $\varphi(x,y)$ must be reliably estimated. This process is termed as demodulation. Vortex modulation is the process of extracting phase and amplitude. The extracted phase $\varphi(x,y)$ is divided into two components spiral φ_c and continuous phase $\varphi_{s.}$

3.2 FINGERPRINT PREALIGNMENT

To mix two different fingerprints after decomposing each fingerprint into its continuous component and spiral components, the components should be appropriately aligned. Previous research has shown that two fingerprints can be best aligned using their minutiae correspondences. However, it is difficult to ensure the existence of such correspondences between two fingerprints acquired from different fingers. In this paper, the components of individual fingerprints are prealigned 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.

3.3 MIXING FINGERPRINTS

Let F_1 and F_2 be two different fingerprint images from different fingers, and let $\varphi_c(x,y)$ and $\varphi_s(x,y)$ be the prealigned spiral and continuous components. Two mixed fingerprints can be generated $MF1$ and $MF2$.

$$MF_1 = \cos(\varphi_{c2} + \varphi_{S1})$$

$$MF_2 = \cos(\varphi_{c1} + \varphi_{S2})$$

4. CONCLUSION

In this work, it was demonstrated that the concept of mixing fingerprints can be utilized to generate a new identity by mixing two distinct fingerprints and de-identify a fingerprint by mixing it with another fingerprint. To mix two fingerprints, each fingerprint is decomposed into two components, 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. The proposed approach generates a new entity which looks like plausible fingerprint. This mixed fingerprint obscures the identity of original fingerprint thereby providing security and privacy. Further work is required to enhance the performance due to mixed fingerprints by exploring alternate algorithms for prealigning, selecting and mixing the different pairs.

REFERENCES

[1] B. Yanikoglu and A. Kholmatov, Combining multiple biometrics to protect privacy, in Proc. ICPR-BCTP Workshop, Aug. 2004, pp. 4346.

[2] A. Jain, K. Nandakumar, and A. Nagar, Biometric template security, EURASIP J. Adv.Signal Process., vol. 2008, pp. 1 17, 2008.

[3] N. Ratha, J. Connell, and R. Bolle, Enhancing security and privacy in biometrics-based authentication systems, IBM Syst. J., vol. 40, no. 3, pp. 614634, 2001.

[4] A. Othman and A. Ross, Mixing fingerprints for Template Security and Privacy in Proc. IEEE Int. Workshop Information Forensics and Security (WIFS), Foz do Iguacu, Brazil,Nov. /Dec. 2011.

BIOGRAPHIES

Ms. Keerthana S curently working as Assistant Professor, in Dept. of CSE, SIT Mangalore, Karnataka.

Ms. Vijetha ,curently working as Assistant Professor, in Dept. of CSE, SIT Mangalore, Karnataka.