THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Generating Virtual Identity Using Mixed Fingerprints

G. Sangeetha
PG Student, Department of Computer Science and Engineering
GKM College of Engineering and Technology, Chennai, India
K. Alice
Assistant Professor , Department of Computer Science and Engineering
GKM College of Engineering and Technology, Chennai, India

Abstract:
The possibility of mixing two different fingerprints, relating to two different fingers, in order to generate a new fingerprint. To mix two fingerprints, each fingerprint is decomposed into two different components are the continuous and spiral components. The continuous component of one fingerprint is combined with the spiral component of the other fingerprint. This is used to generate virtual identities from two different fingers. This proposed system to used Mixed Fingerprint Technique to provide more security. If the fingerprint is valid then the user is generated two onetime passwords. One is sent to the user's mobile number as SMS and another is sent as user's Email ID. Only after authentication of mixed fingerprint, Mobile OTP as SMS and Email OTP. User is allowed to access his/her Banking Application.

Key words: *Fingerprints, image level fusion, mixing biometrics, phase decomposition, privacy protection, virtual identities*

1. Introduction

Image level fusion refers to the consolidation of (a) multiple samples of the same biometric trait obtained from different sensors or (b) multiple instances of the same biometric trait obtained using a single sensor, in order to generate a new image. This is used to combine multiple impressions of the same finger.

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. The mixing process begins by decomposing each fingerprint image into two different components of the continuous and spiral components. The continuous component defines the local ridge orientation, and the spiral component characterizes the minutiae locations. Finally, the continuous component of one fingerprint is combined with the spiral component of the other fingerprint.

The proposed system explores the possibility of fusing images from different fingers at the image level. This is used to mix the prints of the thumb and the index fingers of a single individual, or index fingers of two different individuals in order to generate a new fingerprint. Therefore the concept of mixing fingerprints should be utilized in a multi finger authentication system. This is benefits of storage and security. The mixing fingerprint can be used to generate a large set of virtual identities. These virtual identities can be used to conceal the original identities of subjects or be used for large-scale evaluation of algorithms. The conventional cryptographic systems provide numerous ways to secure important data/images, there are two main concerns for encrypting templates of fingerprints. First, the security of these algorithms relies on the cryptographic keys. Maintaining the secrecy of keys is one of the main challenges in practical cryptosystems. Second, during every identification/verification attempt, the stored template has to be decrypted, to preserve the privacy of fingerprints by fusing two different fingers but only at the feature level.

This work confirms that the mixed fingerprint representing a new identity can potentially be used for authentication. The proposed method can be utilized to generate different-sized databases of virtual identities from a fixed fingerprint dataset. This can be used for de-identifying fingerprints, a detailed analysis of the security aspects, that is the changeable and non-inevitability properties. This security analysis is based on the cancelable biometrics literature.

2. Related Works

Virtual identities [2] method proposed that mixing of two different fingerprints at the image level to generate a new fingerprint. Synthetic fingerprint generation [3] method proposed that described this method for generating synthetic fingerprints on the basis of some mathematical models that describes the main features of real fingerprints. It is used to fingerprint recognition algorithm based on low cost, accurate performance, and simple to testing the fingerprints. Biometric cryptographic [4] method proposed that described the various threats that can be encountered by a biometric system. The original biometric data is stored in the individual template. In this method present the different technique such as biometric template, cancelable biometric, biometric cryptosystem.

Fingerprint reconstruction [5] method proposed that described the reconstruct fingerprint images from the standard templates and investigates to what extent the reconstructed images are similar to the original images. Fingerprint representation [6] method proposed that described reconstruct the phase image, which is then converted into the grayscale image. Combining multiple biometrics [7] method proposed that described the biometric authentication used to two separate biometric features. It combined to obtain a non unique identifier of the person and generate privacy concerns. Fingerprint enhancement [8] method proposed that described the performance of a minutiae extraction algorithm relies heavily on the quality of the input fingerprint images. Security and privacy [9] method proposed that described input fingerprint image is mixed with another fingerprint, in order to produce a new mixed image that the identity of original fingerprint. Cancelable fingerprint [10] method proposed that described a cancelable transform is the process of registering the image and transform the minutiae position. Template transformation [11] method proposed that described the one methodology for biometric template protection is the template transformation approach. The transformed template is stored and performed in the transformed domain.

3. Mixing Fingerprints: The Proposed Approach

The block diagram shown in figure 1 describes our mixing fingerprints technique.

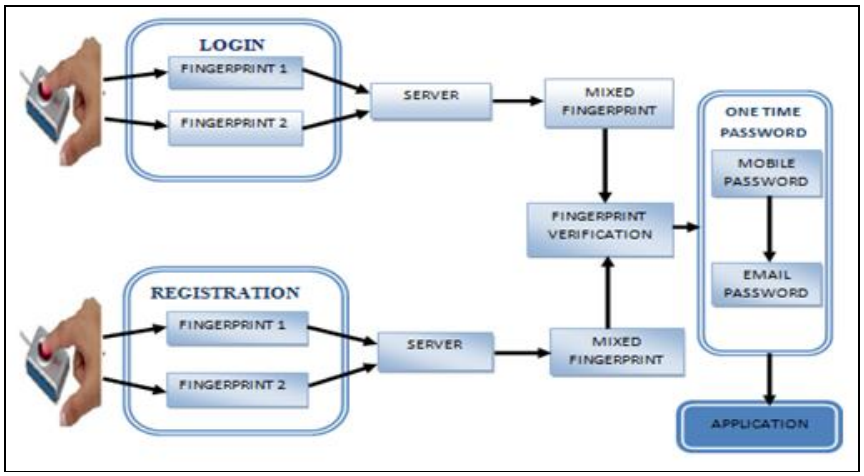

Figure 1: Proposed approach for mixing fingerprints

In this architecture is to generate the two phases. One is login phase and another one is registration phase. The registration phase is described the users want to create an account and then only they are allowed to access the network. All the User details will be stored in the Database of the Server. To provide their two fingerprint and stored in the database of the Server.

The Server will monitor the entire User's information in their database and verify if required. The Server will store the entire User's information in their database. The Server has to establish the connection to communicate with the Users. The Server will update the each User's activities in its database.

Once filled, the User is allowed, and wants to provide their two fingerprints and these captured fingerprint images are mixed and stored in the database of the Server, after getting two fingerprints from the User and it is stored in the separate directory.

Then in the login phase the user enter the sensitive information's. And this information's are stored in the database of the server. To provide their two fingerprint and stored in the database of the server. These fingerprints are merged to form mixed fingerprint and stored in the database on the server.

In the fingerprint verification is described the Login phase, each user is requested to enter the Sensitive information. Once this information's are verified then the User is requested to provide their two fingerprints that they have provided during the registration phase. This information's will be passed to the Server and the Server will verify the mixed fingerprint. If it is valid then the User is allowed for the next level of verification. If it is not valid the user is not allowed to the next level of verification.

In the onetime password verification is described if the fingerprint is valid to generate the two onetime passwords. One password will be generated and send to the user mobile number. It will be transmitted through SMS via specified port. Once the User Enters their mobile password correctly, another one time password will be generated and send to the user Email address. If the User provides the Email password correctly, then they are allowed to access the application. If it is not valid the user is not allowed to access the application.

4. Modules Specifications

4.1. Registration Module

In this module to create a user application by which the user is allowed to access the data from the server. The users want to create an account and then only they are allowed to access the network. The users want to generate a pin number and for access the application. All the User details will be stored in the Database of the Server. To provide their two fingerprint and stored in the database of the Server. The user details and two fingerprints are stored in the user account number and pin number.

4.2. Database Storage

The Server will monitor the entire User's information in their database and verify if required. The Server will store the entire User's information in their database. The server stored in the two fingerprints in their database. All details are stored in the same account number and pin number. All The Server has to establish the connection to communicate with the Users. The Server will update the each User's activities in its database. The Server will authenticate each user before they access the Application, So that the Server will prevent the Unauthorized User from accessing the Application.

4.3. Generation of hash value for mixed fingerprint

In the user registration phase the user is requested to fill, the entire server requested information. Once filled, the User is allowed, and wants to provide their two fingerprints and these captured fingerprint images are mixed and stored in the database of the Server, after getting two fingerprints from the User and it is stored in the separate directory. In this fingerprint is to generate hash value. To generated the hash value using the MD5 algorithm. The MD5 algorithm can be used as a digital signature mechanism. Then the Server will mix the fingerprint image into the mixed one in the server's directory.

4.4. Fingerprint Verification

In the Login phase, each user is requested to enter the Sensitive information. Once this information's are verified then the User is requested to provide their two fingerprints that they have provided during the registration phase. In this module is used to minutiae algorithm. The minutiae algorithm is used to matching the fingerprint. The minutiae points are collected and matching the original minutiae point. These minutiae points are verified. This information's and fingerprints will be passed to the Server and then Server will verify the mixed fingerprint. If it is valid then the User is allowed for the next level of verification. If it is not valid the user is not allowed.

4.5. One Time Password Verification

If the Fingerprint verification is valid, then generate a Onetime Password using a Secure Random Key Generation Algorithm. It is send to the User's Mobile Number. It will be transmitted through SMS via specified port. Once the User Enters their mobile password correctly, another one time password will be generated and send to the Email address. If the User provides the Email password correctly, they are allowed to access the application. Then not allowed to access the application.

5. Experimental Results

The experimental results are create the user information such as, user name, date of birth, age, sex, address, mobile number, email id are stored in the database of the server. Then generate the account number and pin number. The user provided two fingerprints are stored in the separate directory of the server. These two fingerprints are mixed and generated the hash value. The user information, two fingerprints, hash value are stored in the database of the server. Then the login phase is the user to request the account then to provide their same fingerprint and sensitive informations. It is valid to access the application.

Figure 2: Example of User Registration phase

Figure 3: Example of generated the Account and Pin number

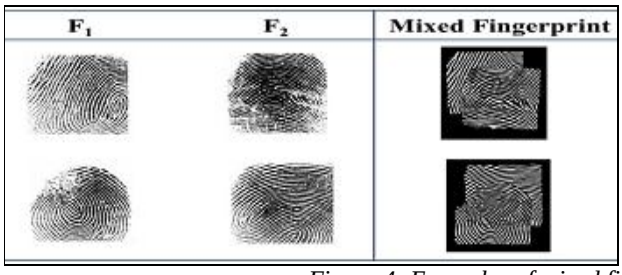

Figure 4: Examples of mixed fingerprints that looks unrealistic

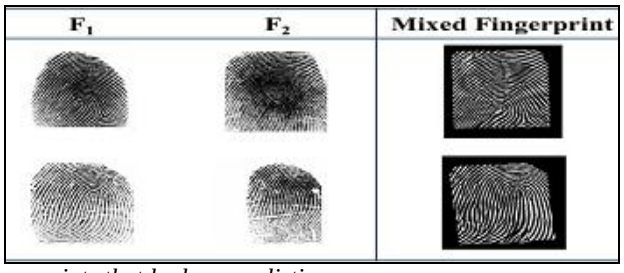

Figure 5: Examples of mixed fingerprints that appear to be visually realistic

If it is valid allow for next level of verification. The fingerprints are valid to generate the two onetime passwords, one is send as the user mobile number and another is send as the user email id. Only after authentication of mixed finger print, Mobile OTP as SMS and Email OTP. User is allowed to access Application.

.

6. Conclusion

In this work, it was demonstrated that the concept of "mixing fingerprints" can be utilized to generate a new identity by mixing two different fingerprints and generate the hash value. Experiments on two fingerprint databases show that (a) the mixed fingerprint representing a new identity can potentially be used for authentication, (b) the mixed fingerprint is dissimilar from the original fingerprints, (c) the mixing fingerprint is generated the hash value, (d) if the fingerprint is valid then generated the two onetime passwords, (e) to generate a database of virtual identities from a fixed fingerprint dataset.

7. References

1. A. Othman and A. Ross, "On Mixing Fingerprints," in Proc. IEEE Int. Workshop Information Forensics and Security (WIFS), VOL 8, NO.1, Jan. 2013.
2. A. Othman and A. Ross, "Mixing fingerprints for generating virtual identities," in Proc. IEEE Int. Workshop Information Forensics and Security (WIFS), Foz do Iguacu, Brazil, Nov./Dec. 2011.
3. R. Cappelli, "Sfinge: Synthetic fingerprint generator," in Proc. Int.Workshop Modeling and Simulation in Biometric Technology, 2004, pp. 147–154.
4. A. Jain, A. Ross, and U. Uludag, "Biometric template security: Challenges and solutions," in Proc. Eur. Signal Processing Conf. (EUSIPCO), 2005, pp. 469–472.
5. R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint image reconstruction from standard templates," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 9, pp. 1489–1503, Sep. 2007.
6. J. Feng and A. K. Jain, "Fingerprint reconstruction: From minutiae to phase," IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 2, pp. 209–223, Feb. 2011.
7. B. Yanikoglu and A. Kholmatov, "Combining multiple biometrics to protect privacy," in Proc. ICPR-BCTP Workshop, Aug. 2004, pp. 43–46.
8. L. Hong, Y.Wan, and A. Jain, "Fingerprint image enhancement: Algorithm and performance evaluation," IEEE Trans. Pattern Anal. Mach. Intell., vol. 20, no.8, pp. 777–789, Aug. 1998.
9. A. Ross and A. Othman, "Mixing fingerprints for template security and privacy," in Proc. 19th Eur. Signal Processing Conf. (EUSIPCO), Barcelona, Spain, Aug. 2011.
10. N. Ratha, S. Chikkerur, J. Connell, and R. Bolle, "Generating cancelable fingerprint templates," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 561–572, Apr. 2007.
11. A. Nagar, K. Nandakumar, and A. K. Jain, "Biometric template transformation: A security analysis," in Proc. SPIE, Electronic Imaging, Media Forensics and Security XII, San Jose, Jan. 2010.