International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-5, Issue-1, May 2016

A Secure Approach of User Authentication Using Multibiometric Cryptosystem : A Review

Neha G Bhagat, Prof.P.C.Selokar

***Abstract*— Biometric templates are using for different security purpose . By using multibiometric cryptography we provide user security as well as uers authentication. For more security here we provide cryptography on biometric templates that is biometric template convert into helper data and then continuously verify or scan the user's feature. As the session started the sensor device (web camera) continuously scan the retina of eyes , facial parameters ,distance between two points of nose of user which continuously verifies the authorized user and secures the system from session hijacking or from maliciously used by unauthorized person. We use Kalman filter and Gaussian mixture model use for fusion of biometric data of user of system and also use Eigenimag based technique for continuous monitoring the biometric traits of user. Due to continuous identification it required more energy for this we use Reliable Minimum Energy Cost Routing for minimizing the energy.**

***Index Terms*— Biometric template , cryptography , fusion, Security.**

I. INTRODUCTION

With **c**omparing traditional authentication techniques like passwords and token cards, biometric-based techniques is non-repudiable, more universal and reliable option for user's authentication. A typical biometric based authentication system is composed of two processes the enrollment process, in which the system scans a user's biometric image and creates biometric template of biometric features extracted from the image, and stores the template in databases; and authentication process in which system scans an individual's biometric data, extracts biometric features in the same manner and after that they are compares with the template of the user the individual claims to be. System will output a match if according to a similarity measure, whether a query is sufficiently similar to the template or a mismatch . Over the past few years, there has a great work on how to provide security to biometric templates. Biometric protection techniques uses transformed data rather than using original biometric data or else feature-based templates to authenticate users. This proposed methods can be classified into two types feature transformations as well as biometric cryptosystems . The former applies a non-invertible transformations for modification of original biometric data. The transformed template is stored for matching. It provide a solution for cryptographic key generation encryption as well as biometric template protection. In the biometric cryptosystems original templates are converted into biometric-dependent information also known as helper data which is helping in recovering cryptographic keys. Matching of this is performed indirectly by verifying the validity of recovered keys.

Providing Security to Biometric Traits and User authentication is very important as there is increase in complexity of attack. Once the user's identity has been verified the resources are available for fixed period of time or until explicitl logout from the system assumes that a single verification is sufficient and that the identity of the user during the whole session.For example:Consider the user is already logged into the cirtain service and then leave the PC in the work area as while.The user are authenticate at that time someone can be misused it easily.To detect the malicious use of the computer resources and prevent it from unauthorized user replaces an authorized one by providing the security based on the multibiometrics continuous authentication turing the user authentication as the continuous process rather than one time occurrence. It use cryptography for multibiometric template rotection and multibiometric verification merely used to authenticate a session on startup ,but that it is used in a loop throughout the session to continuously authenticate the presence of the user.

II. Related Work

Now a days security is one of the big issue. In previous research they work only on biometric template protection and verification of user but only one time. So for providing more security and authentication of user we use different technique and provide continuous verification and authentication of user.

Brief Review of Literature

- **Jiankun Hu, Josef Pieprzyk, and Willy Susilo [1]** "A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion. " in this paper he proposed Biometric cryptosystems provide a solution for cryptographic key generation, encryption as well as biometric template protection. In biometric cryptosystems, our original templates are replaced by biometric-dependent information that is called helper data , which help in recovering cryptographic keys. Matching of biometric template performed indirectly by verifying the validity of recovered keys. There are two types of judging the biometric cryptosystem performance. MBC offer higher authentication accuracy and flexibility, wider population coverage and stronger security than SBC. MBC i,e multibiometric cryptosystem can be classified into two categories based on different fusion modes first one is fusion at the feature level and second is fusion at the decision level .

- **W. Yang, J. Hu, S. Wang, and C. Chen [2]** "Mutual dependency of features in multimodal biometric systems," in this paper he proposed 'unreal' multimodal databases are

Neha G Bhagat, Computer science & engineering, RTMNU, Nagpur
Prof.P.C.Selokar, Computer science & engineering, RTMNU, Nagpur

used, in which samples of multimodal biometric modules which are supposed to be constructed from different biometric modules of the same subjects are constructed from different persons. Such an ‘unreal’ multimodal database ignores the mutual dependency of features. A simple example of this mutual dependency is intuitive observation that a tall person have bigger hands than a short person. Because of using unreal multimodal databases experimental results cannot reflect real situations, and consequently may misguide the implementation of multi-biometric systems in real applications. To show the existence of feature dependency and also verify its influence on system performance, in this After this we design a face and fingerprintbased multi-biometric system and test it on the ‘real’ and ‘unreal’ multimodal databases.

- **J. Zhang, C. Chen, Y. Xiang, W. Zhou, and Y. Xiang**, “Internet traffic classification by aggregating correlated naive Bayes predictions,” in this paper he proposed a novel traffic classification scheme in which it improve performanceof classification when few training data are available. We solve bag of flow BoF-based traffic classification in a classifier combination framework and then theoretically analyze the performance advantage .

- **Nagar, K. Nandakumar, and A. K. Jain,** ,“Multibiometric cryptosystems based on feature-level fusion,” in this paper he proposed a feature-level fusion framework to protect and providing security multiple biometric templates of a user as a single secure sketch. It contain firstly practical implementation of the feature-level fusion framework using two biometric cryptosystems, namery,fuzzy vault and fuzzy commitment. And secondly Detailed analysis of the trade-off between matching accuracy and security in proposed multibiometric cryptosystems based on two different databases each containing the three most popular biometric templates like iris, fingerprint, and facial parameters.

III. Proposed MODEL and OVERVIWE

Firstly User have to register their information in database like name ,address,mobail number and images of biometric template of user etc. After that we providing cryptography to provide security to biometric template for this we are using SHA algorithm .After this we make fusion of biometric template which is present in the database with user at login phase through web camera. And for this we are using kalman filter and (GMM) Gaussian mixture model algorithm . And for continuos monitring we use Eigenimage Base Recognition Technique ,due to continuous monitoring of user required more energy to reduce energy we are using RMECR (Reliable Minimum Energy Cost Routing).

1)Biometric template detection

This detect the biometric template of the user which is got through the web camera and after this it stress the position of template like eye, nose facial parameter etc.

2) Biometric template Segmentation

Because the position of biometric template computed by the template detection is not accurate, a more previous location is realy nessesary for a good maching performance. Since the size of a user’s face appearing in a video frame and it also varies on the distance of the user from the web camera, the face image must be normalized to a standard size. There are some features in face image that may changes from time to time . For example, the hairstyle we can change from one day to another. In order to reduce the effect of such dynamic feature a standard elliptical region with a fixed aspect ratio is used to extract the face region.

3)Relighting

This provide a histogram-based intensity mapping function for normalizing the intensity distribution of the segmented image.

4) Biometric template matching

It help to improve the performance of the eigen face method , it is important to have good alignment between the live and the stored image. It means that the nose has to be in the , redius of retrica has to be proper and scale the face images must be normalized.Here each face image is first converted to vector.This vector is projected onto eigen faces through inner product calculation ,distance also mapped to normalized matching score.

5) Biometric template Database

Here we store the image of biometric template of different users and authentication of user is performed by maching those image in this database and user who accessing the system.

IV. Conclusion

Ensuring the correct identity of a user throughout a full session is important especially for high security application. Security as well as accuracy are two major factors influencing the performance of a biometric cryptosystem. In this paper we provide security to biometric template and focus on continuous user authentication using multibiometrics template or gait recognition **.**This proposed approach firstly provide security to biometric templates by using cryptoghraphy and then started continuous authentication process based on multi biometrics i.e by continuous scanning the retina of eyes, facial curve parameter, distance between two points of nose etc.

Acknowledgment

I thank to Ms. Purnima Selokar for her valuable guidance and also thank to IEEExplore.org for references.

References

[1] Jiankun Hu, Josef Pieprzyk, and Willy Susilo, “A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion.” June 2015

[2] Cai Li, Jiankun Hu, Josef Pieprzyk, and Willy Susilo, “A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion” IEEE Transaction on Information forensics and Security, VOL. 10, No. 6, June 2015

[3] W. Zhou, J. Hu, S. Wang, I. Petersen, and M. Bennamoun, “Performance evaluation of large 3D fingerprint databases,” *Electron. Lett.*, vol. 50, no. 15, pp. 1060–1061, Jul. 2014.

[4] W. Zhou, J. Hu, S. Wang, I. Petersen, and M. Bennamoun. *3D Fingerprint Database and Associated Multimodal 2D Fingerprint Database*. [Online].

[5] W. Yang, J. Hu, S. Wang, and C. Chen, “Mutual dependency of features in multimodal biometric systems,” *Electron. Lett.*, vol. 51, no. 3, pp. 234–235, Feb. 2015

[6] Y. Sutcu, Q. Li, and N. Memon, “Secure biometric templates from fingerprint-face features,” in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Minneapolis, MN, USA, Jun. 2007, pp. 1–6.

[7] A. Ross, J. Shah, and A. K. Jain, “From template to image: Reconstructing fingerprints from minutiae points,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 544–560, Apr. 2007.

[8] S. Wang and J. Hu, “Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach,” *Pattern Recognit.*, vol. 45, no. 12, pp. 4129–4137, Dec. 2012.

[9] T. Ahmad, J. Hu, and S. Wang, “Pair-polar coordinate-based cancelable fingerprint templates,” *Pattern Recognit.*, vol. 44, nos. 10–11, pp. 2555–2564, Oct./Nov. 2011.

[10] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, “Generating cancelable fingerprint templates,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[11] C. Lee, J.-Y. Choi, K.-A. Toh, and S. Lee, “Alignment-free cancelable fingerprint templates based on local minutiae information,” *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 37, no. 4, pp. 980–992, Aug. 2007.

[12] A. Cavoukian and A. Stoianov, “Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy,” Information Privacy Commissioner, Toronto, ON, Canada, Tech. Rep., 2007