A Review on Security of Multimodal Biometrics

Muskaan
Research Scholar
Department of ECE
MMEC, Mullana (Haryana)

Tarun Gulati
Assoc. Prof.
Department of ECE
MMEC, Mullana (Haryana)

ABSTRACT
The unique parts of body that identifies a person are known as biometrics. The different biometrics used now-a-days are fingerprints, iris, face recognition, handwriting, gesture, retina, ear height etc. The biometrics when used in conjunction for the identification or verification of an individual are called as MULTIMODAL BIOMETRICS. This is assumed to be a better approach for security. It overcomes some of the limitations of single biometrics as this approach is more reliable. ID cards, Access cards, Punch, PIN, USER ID, passwords are used for identification but ID cards can be stolen or can be lost and user id s and passwords can be forgotten. So biometrics overcomes all these and has become the emerging trend. Further the security of the database is improved using cryptosystem. It takes a key and changes plain text into cipher text and back.

Keywords
Recognition, Security, Biometric, Retina, Multi modal.

1. INTRODUCTION
Biometrics is automated methods of recognizing a person based on a physiological or behavioural characteristic. The past of biometrics includes the identification of people by different body features such as height of a person, scars on the skin, complexion and colour of eye. The present features are face recognition, fingerprints, hand writing, hand geometry, iris, vein, voice and retinal scan. Better security is ensured than the password systems or the number systems with these. Biometrics are very well explained with the help of a diagram. User IDs, passwords, PIN etc are something that we know[20]. ID cards, Access cards are something that we possess or something that we have. But biometrics are something that we are. This is very well explained with the help of the figure given below.

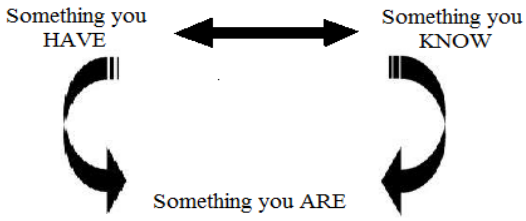

Fig 1: Explanation of biometrics

2. CATEGORIES OF BIOMETRICS
Biometric techniques can be divided into two categories viz. physical characteristics and behavioral characteristics based techniques.

2.1 Biometrics techniques based on physical characteristics are: Fingerprints, hand geometry, palm-print etc are the biometric techniques based on physical characteristics of human being. They are called physical characteristics based techniques. Following are examples of biometric techniques based on physical characteristics.

· Face recognition
· Hand geometry recognition
· Fingerprint recognition
· Vein pattern recognition
· Retina recognition
· Iris recognition

2.2 Biometrics techniques based on behavioral characteristics are: Voice, signature, keystroke, gait etc are the biometric techniques which are based on the behavior of human being. They are called behavioral characteristics based techniques. Following are examples of biometric techniques based on behavioral characteristics[21].

· Voice recognition
· Signature recognition
· Keystroke dynamics
· Gait recognition

3. MULTIMODAL BIOMETRICS
Single biometrics recognises a person based on single source of biometric information. They have following problems:

1. Noisy sensor data
2. Non- universality
3. Lack of individuality
4. Lack of invariant representation
5. Susceptibility to circumvention

Multimodal biometrics system achieves much greater accuracy then the single feature systems. Even if one of the feature is disturbed, the other will still lead to a accurate result as it provides more resistance against spoofing because it is difficult to simultaneously spoof multiple biometric sources.

4. CLASSIFICATION OF CURRENT AUTHENTICATION METHODS
Classification of current authentication methods can be done into three main categories [19]

1) Token based
2) Biometrics based
3) Knowledge based

4.1. BIOMETRIC RECOGNITION
Biometrics recognition is done through two distinct methods Evidence Identity, Confirmation of Template.

- **Evidence Identity**

In identity provision the unknown person's template is first checked with the stored database then the unrecognized person is given the identity for further security process. The

identification number and name is given as the identity and the record is stored successfully.

- **Confirmation of Template**

Giving identity to a person and verifying him on giving his identity is known as confirmation of template.

4.2. ADVANTAGES OF MULTI BIOMETRICS

In single biometric system we use only one system e.g. Iris System, Fingerprint system or Face Recognition System. Hence we face lots of problems while using single biometrics system. Sometimes noise enters with the Biometrics of a person that we have to store, this results in higher the false rejection rate. Database template can be stolen and it can be revoked by any intruder when we use the single biometric system as it contains only one template. Many people face the difficulties in giving template because of injury or damage of physical part of that person and are unable to use that system. The advantages of multi biometrics system are as follows:

(i) The system operation gets better in multimodal biometrics.
(ii) The accuracy is improved as compared to the single biometric system.
(iii) As it stores two characteristics of biometric system in the database, hence prevents from stolen templates of biometrics system.
(iv) Multi modal biometric systems are capable of addressing the non universality issue (with respect single biometric system for example: 2% of the population do not have proper fingerprint [15]) by accommodating a large population of users.

5. SECURITY OF MULTIMODAL BIOMETRICS

Security of multi biometric templates is very important as they contain information regarding multiple traits of the same user. A number of techniques have been proposed to secure biometric templates[11]. These techniques can be categorized into two main classes:

- Biometric cryptosystem
- Template transformation

Biometric Cryptosystem is a technique that involves a pair of algorithms which takes a key and converts plain text into cipher text and back into plain text. Plain text is what we want to protect.

Template transformation technique modifies the biometric template using a specific key which makes it difficult to recover the original template from the transformed template.

6. FINGERPRINT TECHNOLOGY

An impression of the friction ridges of all or any part of the finger is known as fingerprints. A raised portion of the on the palm or digits (fingers and toes) or plantar (sole) skin, consisting of one or more connected ridge units of friction ridge skin is the friction ridge. These ridges are also known as Dermal ridges or dermal[7]. The traditional method used to get a finger print involves the use of ink and a piece of paper. Live finger print readers are used now a days for scanning the fingerprints. These modern fingerprint scanners are based on thermal, optical, silicon or ultrasonic principles. Fingerprint is the oldest of all the biometric techniques. The most common scanner at present is Optical finger print reader.

Fig2: Image of fingerprint

The fingerprints are enhanced using following steps:

- Histogram Equalization
- Segmentation
- Ridge orientation
- Ridge frequency Estimation
- Filtering
- Minutiae Extraction

7. IRIS TECHNOLOGY

Iris is the biological feature of human which remains stable over a person lifetime[20][7].The colored area that surrounds the pupil is known as the iris of the eye which is used for recognition purpose. Video based image acquisition system are used to obtain the various iris patterns. A complex and a unique pattern is featured by each iris pattern[4].

Fig 3: Image of Iris

7.1 Segmentation of Iris

Eyelids and eyelashes obstruct the upper and the lower parts of the iris region. The specular reflections within the iris region can also obstruct the iris pattern. The circular iris region is detected and the artefacts are separated. The quality of eye images will greatly influence the success of segmentation. Two procedures involve segmentation algorithm are: iris localization and noise reduction[4]. Iris localization process is used to find the boundary between the iris and the sclera and the boundary between the pupil and iris of the acquired image. Localisation process involves the reduction of noises (non-iris parts) from the acquired image and this process is referred as noise reduction. The noises present in the acquired image are Pupil, sclera, eyelids, eyelashes and artefacts.

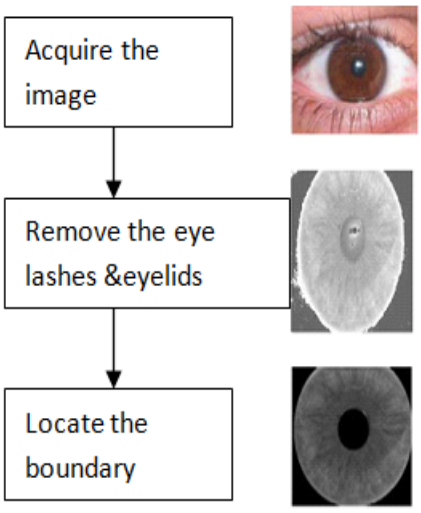

Fig 4: Steps of Segmentation

8. LITERATURE SURVEY

The various approaches used in multimodal biometrics are:

8.1. Fusion of multi biometrics at feature level

This process involves the feature level framework to simultaneously protect multiple templates of a user as a single secure sketch. It includes: Practical implementation of proposed feature level fusion framework using two well known biometric cryptosystem and the detailed analysis of trade off between matching accuracy and security in the proposed multi biometric cryptosystem based on two different databases, each containing the three most poplular biometric modalities: fingerprint ,iris, face. Hence, results in the increased security and better system performance.

8.2. Enhancing the security of multi biometrics

This approach focuses on enhancing the security of multi biometrics using cryptosystem. Biometric template can be misused if it is stolen. Hence, improving the security of biometric template is the main discussion of this approach. Cryptography is used in biometrics for keeping it safe and away from frauds or unauthenticated users. The two biometrics used here are fingerprints and iris. Features are stored at feature level and mixing is done extracting important features and characteristics of modalities.

8.3. Security using fuzzy vault

Here the author discussed that Security concerns regarding the stored biometric data is impeding the widespread public acceptance of biometric technology. A number of bio-crypto algorithms have been proposed but they have a bounded practical usage due to the trade-off between recognition performance and security of the template. This involves the improved recognition performance as well as the security of a fingerprint based biometric cryptosystem, called finger print fuzzy vault. Minutiae descriptors capture the orientation and frequency information in a minutia's neighbourhood, in the vault construction using the fuzzy commitment approach. Hence as a result, the fingerprint matching performance is improved with some improvement in security as well with the use of minutiae descriptors.

8.4. Multimodal biometrics

Various approaches to multi-modal biometrics based on the type of sensing used, the biometric source and the depth of collaborative interaction in the processing has been categorized here by the author. Multi biometric systems are being increasingly deployed in many large scale biometric applications because they have several advantages such as lower error rates and larger population coverage compared to single biometric systems. Attempts are made to identify some of the challenges and issues that confront research in multimodal biometrics

8.5. Enhancing images using fingerprints

Author has proposed a new method in fingerprint enhancement with application of wavelet transform which is more efficient. Fingerprint image enhancement and minutiae matching are two key steps in an automatic fingerprint identification system. An algorithm for enhancement of finger print image based on orientation fields has been designed. Ridge information are introduced into the minutiae matching process in a simple but effective way. And it solves the problem of reference point pair selection with low computational cost. Variable sized bounding box are used to make the algorithm more robust to non-linear deformation between fingerprint images. Simple alignment method is used in the algorithm.

9. CONCLUSION

Multi biometrics systems are better than the single biometrics systems as they provide better security and improves the system performance. Fusion of the different biometrics modalities is done. Fusion before matching is believed to be a better approach than fusion after matching. The template stored in the database is not secure as a number of attacks are possible like modification of template etc. Cancelable biometrics is used to provide security to the template which hides the original template from the intruders. To raise the security to the next level the template thus obtained from Cancelable biometrics is encrypted using cryptography.

10. REFRENCES

[1] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, Review Article Biometric Template Security, Department of Computer Science and Engineering, Michigan State University, 3115 Engineering Building, East Lansing, MI48824, USA.

[2] A. K. Jain, R. Bolle, and S. Pankanti, eds., Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers, 1999.

[3] T. Gulati, M. Pal, "Interpreting Low Resolution CT Scan Images Using Interpolation Functions," International Journal of Computer Applications, Vol 74– No.3, July 2013, pp. 50-57.

[4] A. Juels and M. Sudan, "A fuzzy vault scheme," in Proceedings of the IEEE International Symposium on Information Theory, p. 408, Piscataway, NJ, USA, June-July 2002.

[5] Binsu C. Kovoor, Supriya M.H. and K. Poulose Jacob, "Effectiveness of feature detection operators on the performance of iris biometric recognition system", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013

[6] K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 561–572, 2007.

[7] Y. Sutcu, H. T. Sencar, and N. Memon, "A secure biometric authentication scheme based on robust hashing," in Proceedings of the 7thMultimedia and SecurityWorkshop (MMand Sec '05), pp. 111–116, New York, NY, USA, August 2006.

[8] T. Gulati, H.P.Sinha, "Interpreting Low Resolution MRI Images Using Polynomial Based Interpolation," International Journal of Engineering Trends and Technology (IJETT) – Volume 10 Number 13 - Apr 2014, pp. 626-631.

[9] Debnath Bhattacharya, Rahul Ranjan, Farkhod Alisherov A. and Minkyu Choi," Biometric Authentication: A Review", International Journal of u- and e- Service, Science and Technology, Vol. 2, No. 3, September, 2009.

[10] RajkumarYadav, Rahul Rishi &SudhirBatra, "A New Steganography Method for Gray Level Images using Parity Checker",International Journal of Computer Applications (0975-8887) Volume 11-No. 11, December 2010

[11] RajkumarYadav et al. / International Journal on Computer Science and Engineering (IJCSE)

[12] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, Berlin, Germany, 2003.

[13] Abhishek Sagar,Karthik Nandakumar, Anil K.Jain,"Multi biometric cryptosystems based on feature level fusion" ,Department of Computer Science and Engineering,Michigan State University, 3115 Engineering Building, East Lansing, MI48824, USA.

[14] Wayman, J. L., "A path forward for multi-biometrics,"ICASSP '06.

[15] R.N. Kankrale, Prof. S. D. Sapkal, " Template Level Fusion of Iris and Fingerprint in Multimodal Biometric Identification Systems", Department of Information Technology SRES.

[16] A Ross and A.K. Jain, "Information fusion in biometrics", Pattern Recognition Letters, vol. 24, no. 13, pp. 2115–2125,

[17] 2003.

[18] A.Ross, K.Nandakumar, and A.K. Jain, Handbook of

[19] Multibiometrics, Springer-Verlag edition, 2006.

[20] L.Lan and C.Y Suen, ―Application of majority voting to pattern recognition,‖ IEEE Transactions on Systems, Man,

[21] and Cybernetics, Part A: Systems and Humans, vol. 27, no.

[22] 5, pp. 553–568, 1997.

[23] G Hemantha Kumar and Mohammad Imran," Research avenues in multimodal biometrics", IJCA, RTIPPR, 2010.

[24] J.Heo, S.Kong, B.Abidi, and M.Abidi, ―Fusion of visible and thermal signatures with eyeglass removal forrobust face recognition,‖ in IEEE workshop on Object Tracking and Classification Beyond the visible spectrum in conjunction with (CVPR-2004), Washington, DC, USA, 2004, pp. 94–99.

[25] Poonam, Santosh Kumar Mishra, "Encryption of secutiy of multimodal biometric using Encryption method", IJAGET, vol-2, issue-09, September 2014.

[26] Sulochna Sonkamble, DR. Ravindra Thool, Balwant Sonkamble,"Survey of biometic recognition systems and their applications",JATIT,2005.

[27] Renu Bhatia,'Biometrics and face recognition techniques',IJARCSSE, vol-3, issue-5, May 2013.