A survey paper on Various biometric security system methods

Ms. Shraddha S. Giradkar[1], Dr. N. K. Choudhari [2]

[1] M. Tech student , Dept. of Electronics & Communication Engineering, Priyadarshini Bhagwati college of Engineering , Maharashtra, India
[2]Principal & Professor, Dept. of Electronics & Communication Engineering , Priyadarshini Bhagwati college of Engineering , Maharashtra, India

---***---

Abstract -- *Security is the major problem in a day to day life. Many high level industry uses biometric security for recognition of their employees such as iris, thumb ,face etc. There are so many systems available for security, but that systems are not so reliable. To ensure the actual presence of a real trait against a fake self generated sample biometric system is used. This developing system is reliable and precise. In this project we present a software and hardware based fake detection method which can be used in multibiometric system to detect different fraudulent access attempts. This paper focuses on iris recognition, fingerprint recognition and face recognition. In this survey we present an overview of various biometric methods for security.*

KeyWords: ***Iris recognition, face recognition, fingerprint recognition, biometrics, security***

1.INTRODUCTION

The science and technology of measuring and analyzing biological data is referred as Biometric. Biometrics are that kind of system which can provide more security to user. Any fake trait can capture the characteristics and behaviour of human beings. But every human being has their own unique identity. That is why it can not easily copied by anyone. There are many biometric security systems available such as iris recognition ,fingerprint recognition, face recognition, signature recognition, voice recognition, hand geometry recognition,etc.

In biometric security system there is no need to remember passwords or PINs ,so there is no chance of stolen or forgotten the passwords or PIN, therefore it is more secure system than any other security systems. Generally biometric system have three steps i.e. receiving data, encryption and analysis of received data.

2. Various Methods Of Biometric security systems:

A] In the year 2003, the authors Salil prabhakar, Sharath Pankanti and Anil k. Jain [5] proposed the biometric security and privacy system for fingerprint recognition. The paper proposed the approach of enrollment, verification and identification to provide confidentiality and security. In proposed Scheme the enrollment module first enroll the person into biometric database. During enrollment process ,the persons characteristics are first scan by the biometric reader to produce digital representation. In verification process already enrolled person claims an identity and system then start verification based on their characteristics. After that identification task identifies the claim persons identity.

But the drawback of this method is that there are two types of errors were introduced : wrong biometric measurement from two different individuals to be from same persons and wrong biometric measurement from same persons to be from two different individuals.

B] Watermarking Scheme for iris:

Authors Jing Dong and Tieniu Tan proposed a biometric security system for iris recognition. In year 2008, they studied two methods for iris recognition, namely protection of iris template by hiding the min cover images as watermarks and watermarking the images of iris. Experimental results suggest embedding of watermark in iris images does not provide better performance instead of that recognition performance drops significantly if iris watermark suffers due to severe attack[1].

C] Canny Edge detection Technique for iris:

In year 2011,the authors Bhavana chouhan and Shailaja Shukla proposed a biometric security system which is based on automatic identification of an individual .Iris recognition totally depend on unique attribute and characteristics of an individual.

Basically it focuses on image segmentation and feature extraction. Especially the iris recognition system depend on edge detection. Most commonly used tool of image processing for edge detection is canny edge detection technique which detects edges very robust .Canny edge detection technique detects unnecessary eges which does not provide appropriate result. This feature extraction method is unable to collect useful information from the image of iris that is not properly segmented[2].

D] AdaBoost algorithm for face and Retinex algorithm for iris:

Authors Yeong Gon Kim ,Kwang Yong Shin, Eui Chul Lee and Kang Ryoung Park in the year 2012 proposed scheme on recognition of face and both irises. In the proposed scheme the face regions are detected by using AdaBoost algorithm where as eye regions are detected by using rapid eye detection. After that the size normalization is performed to remove the variations occured in detected facial region and Retinex algorithm is used to normalized the illumination. Then facial features are acquired by using principal component analysis from normalized result of facial region. At the end matching score of Euclidean distance is calculated which is required as an input to support vector machine.

In case of iris recognition, region of iris is segmented by using integer based CED and with an eyelid/eyelash detection technique. Finally matching score of Hamming distance is calculated and applied as an input to support vector machine.

The drawback of this method is that in case of iris recognition if an iris regions of an individuals are more covered by eyelid/eyelashes can affect the performance of system. In case of face recognition ,facial images of severe rotation and extreme facial expression such as surprise can affect the performance of system[3].

E] Fingerprint and Iris recognition using Fuzzy Logic Scheme:

In year 2013, authors Mohamad Abdolahi, Majid Mohamadi, Mehdi Jafari studied the biometric security fusion system using fingerprint and iris with fuzzy logic. In the fingerprint recognition, bifurcations and terminates are stored and recognised as one feature, so that each minutia can be easily determined , identified and stored with parameters X,Y and its tangent angle. In addition to proposed method, two 64 bits code is used, one for terminates and another for bifurcations which collectively combine them to 128 bits unique code. After getting 128 bit code from new image of fingerprint it starts comparing with the code stored in database and starts finding code with minimum difference. This difference number is then stored in fuzzy logic engine. Iris is a part of eye, which control the amount of light entering in to pupil. In case iris recognition the first obtain the image of iris with good resolution which is referred as image acquisition. In segmentation ,first find out the size of image and centre pixel by dividing row and column. So that pixel is in the pupil region and its clear pupil is the part of eye that is why it can move to the right side of pixel

with a high amount of difference intensity and mark it, move left to the pixel with a high amount of difference intensity and mark it and find the centre of these points. Do the same and find top and bottom and centre of them. Now with these centre and peripheral acquired points we can find the real pupil centre with centre point and maximum distance drawing a pupil circle performing the same task to find the iris region and extract iris from eye image. In this way segmentation is carried out .After that gabor filter is used for feature extraction. After compairing the new images of iris with the stored database by using hamming code algorithm, code obtained with minimum difference is stored in fuzzy logic engine[4].

To overcome the drawbacks of previous papers ,The authors Javier Galbally, Sébastien Marcel and Julian Fierrez [6]in the year 2014 they proposed a scheme where iris, fingerprint, face are used as an input to the system which is then compared with stored database. If applied image is matched with stored database of any of three inputs then data is transferred to the microcontroller by wireless technology using transreceiver. By making comparative analysis with previous papers this paper achieved better performance in terms of security.

3. CONCLUSIONS

Preserving Security is very important nowadays. Various methods of biometrics has been heavily researched in the recent years. This survey summarizes the various methods and algorithm used for biometric recognition like iris, fingerprint and face.

By making use of image quality measurement it is very easy to identify the real and fake user because fake identities few different features than the original one it always consists of different colour, general artifacts, luminance levels, quantity of information and quantity of sharpness, which may be found in both types of images, structural distortions and natural appearance. Multibiometric system is a challenging system than unibiometric system as well as it is more secure. This paper focuses on only three biometric system such as face recognition, iris recognition, fingerprint recognition. This type of multibiometric system is used for various applications. In future for making this multibiometric system more reliable and secure then add one more type of biometric system and try to make system more improving.

REFERENCES

[1] Jing Dong, Tieniu Tan," Effects of Watermarking on Iris Recognition Performance", 10th Intl Conf. on Control, Automation, Robotics and Vision, Hanoi, Vietnam, 17–20 December 2008

[2] Bhawna chouhan, shailja shukla." Iris Recognition System using canny edge detection for Biometric Identification", Interrnational Journal of engineering Sciences and Technology (IJEST), ISSN: 0975- 5462 Vol. 3 No. I Jan 2011

[3] Yeong Gon Kim, Kwang Yong Shin, Eui Chul Lee and Kang Ryoung Park ''Multimodal Biometric System Based on the Recognition of Face and Both Irises''

International Journal of Advanced Robotic system 2012, Vol. 9, 65:2012

[4] Mohamad Abdolahi, Majid Mohamadi, Mehdi Jafari '' Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic '' International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013 504

[5] Salil prabhakar, Sharath Pankanti and Anil k. Jain,'' Biometric Recognition: Security and Privacy Concerns",published by the IEEE computer society 1540-7993/03/2003

[6] Javier Galbally, Sébastien Marcel and Julian Fierrez,'' Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint,and Face Recognition",IEEE Transactions on Image Processing vol. 23, no. 2, feb2014

[7] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.*, vol. 2008, pp. 113–129, Jan. 2008.

[8] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia,"A high performance fingerprint liveness detection method based on quality related features," *Future Generat. Comput. Syst.*, vol. 28, no. 1, 2012.

[9] K. A. Nixon, V. Aimale, and R. K. Rowe, "Spoof detection schemes," *Handbook of Biometrics*. New York, NY, USA: Springer-Verlag, 2008, pp. 403–423.2009

[10] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda, *et al.*, "Competition on countermeasures to 2D facial spoofing attacks," in *Proc. IEEE IJCB*, Oct. 2011, pp. 1–6.

[11] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz,"Evaluation of direct attacks to fingerprint verification systems,"*J. Telecommun. Syst.*, vol. 47, nos. 3–4, pp. 243–254, 2011.

[12] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in *Proc. IEEE IJCB*, Oct. 2011, pp. 1–7.

[13] (2010). Trusted Biometrics Under Spoofing Attacks (TABULA RASA) [Online]. Available: http://www.tabularasa-euproject.org/

[14] J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni, J. Fierrez, *et al.*, "An evaluation of direct and indirect attacks using fake fingers generated from ISO templates," *Pattern Recognit. Lett.*, vol. 31,no. 8, pp. 725–732, 2010.

[15] J. Hennebert, R. Loeffel, A. Humm, and R. Ingold, "A new forgery scenario based on regaining dynamics of signature," in *Proc. IAPR ICB*, vol. Springer LNCS-4642. 2007, pp. 366–375.

[16] A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietikainen, J. Bustard, and M. Nixon, "Can gait biometrics be spoofed?" in *Proc. IAPR ICPR*, 2012, pp. 3280–3283.

[17] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Evaluation of serial and parallel multibiometric systems under spoofing attacks," in *Proc. IEEE 5th Int. Conf. BTAS*, Sep. 2012, pp. 283–288.