International Journal of Electronics Engineering (ISSN: 0973-7383
Volume 11 • Issue 1 pp. 376-379 Jan 2019-June 2019 www.csjournals.com

Raising Biometric System Security and Performance using Multimodal Approach

Neetu Gahlawat[1], Dr. Pankaj Kumar Verma[2], Dr. Chander Kant[3]
[1]Research Scholar, [2]Professor, [3]Associate Professor
[1,2]Department of Computer Science and Engineering, NIILM University, Kaithal
[3]Department of Computer Science & Application, Kurukshetra University Kurukshetra

Abstract: Unimodal biometric system uses only single trait of biometric for recognition and do not provide better authentication for highly secured application. Multimodal biometric systems solve all the limitations related to unimodal biometric system. Multimodal combines different physical and behavioral traits such as face and finger print, fingerprint and signature etc. There are also some other traits such as skin color, age, height, hair color, eye color, gender called "soft biometric traits". Soft biometric traits do not provide reliable authentication because the nature of these traits are not permanent. Due to the lack of permanence and distinct property in soft biometrics, it can be used with other traits for improving performance of biometric system. In this paper, we proposed a framework by combining physical traits (face and iris) with soft biometric trait (eye color) for enhancing biometric system security and performance.
Keywords: Biometric system, Multimodal biometric, Soft biometric, Unimodal biometric.

I INTRODUCTION

Biometric technology is the science of identifying human being by extracting a feature set from data and comparing with template store in database. A biometric system is used for identifying the person either genuine or imposter by using their physiological traits (hand geometry, face, fingerprint etc) and behavioral traits (voice, gait, signature etc.). A Biometric system which uses only single trait for recognition is known as unimodal biometric system. The performance of unimodal system is not good due to some limitation such as noisy sensor data, non-universality etc. A new approach multimodal was developed to overcome the limitation of unimodal system and also improve the security. (S.R.Soruba Sree, December 2014).

1.1 Multimodal Biometric Approach

Multimodal biometric system uses more than one trait for better and secure recognition as shown in Fig1. The aim of multimodal system is to improve the rate of recognition.

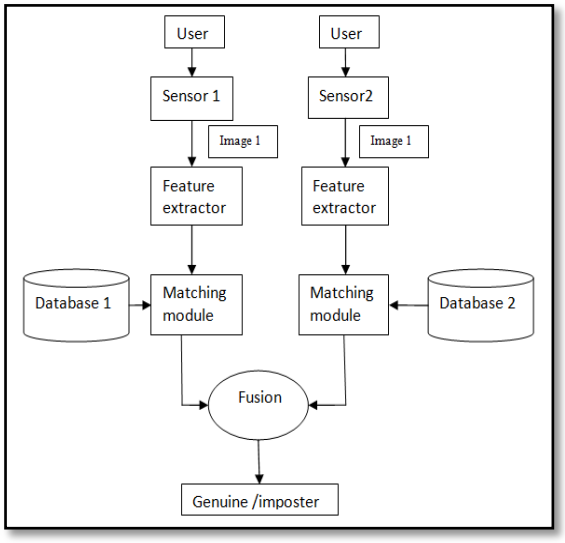

Fig 1 Multimodal biometric system

Multimodal biometric systems are more reliable than traditional authentication system like token based and knowledge based. Different fusion methods are used for making multimodal system by combining more than one trait (Nageshkumar.M, 2009) . This paper presents a proposed approach of multimodal biometric system with integration of face, iris and eye color. In this paper we use two modality face and iris with soft biometric trait eye color. Soft biometric traits are discussed in next section. In this section we only discuss face and iris physiological traits. Iris is a circular diaphragm which is located between cornea and lens of the human eye. Amount of light entering through pupil is the main function of iris. The average diameter of iris is 12 mm and pupil size can be 10% to 80% of the iris diameter (Mohamad Abdolahi, 2013). Iris recognition method provides more stable and secure recognition because the characteristics of iris remain same to the lifetime. Iris and face are highly accurate techniques for authentication because these traits are unique, user friendly, accurate, safe and secure. In the whole world no two iris are same (Sachin Gupta, February 2014).

1.2 Soft Biometric Traits

Multimodal biometric systems provide better security but also create inconvenience to the user due to the problem of large verification time. So, soft biometric traits such as age, height, gender, hair color, eye color can be used with multimodal system for improving recognition performance of the system. Soft biometric traits provide some information about the user but information is not distinct and permanence in nature. There are mainly two types of soft biometric traits (Anil K. Jain, may 2004):

1. Continuous traits like height, weight, age etc.
2. Discrete traits like gender, eye color etc.

We cannot use only soft biometric traits for recognition process because the information extracted from these traits is not unique and secure. Soft biometric traits are combined with physiological traits for providing secure and reliable authentication process. These traits are also improving the

International Journal of Electronics Engineering (ISSN: 0973-7383
Volume 11 • Issue 1 pp. 376-379 Jan 2019-June 2019 www.csjournals.com

performance of a system by reducing verification time (Mamta Ahlawat D. C., 2015).

Related work

Sheena (Sheena)Discussed study of multimodal biometrics system for better performance and security. Author discussed, obtained performance of unimodal biometrics system is not so much effective for security and performance of different applications. To enhance the performance and security level of unimodal biometrics system we can use multimodal biometrics system by combining more than one trait. AntitzaDantcheva(Dantcheva, 2011) give introduction about soft biometric trait, their characteristics, advantages and disadvantages in his PhD thesis. Author discussed various things about the soft biometric traits such that soft biometric traits are non-intrusive, preserving human privacy, computationally efficient and classifiable from a distance. Soft biometric traits can be used with multimodal system for improving biometric system performance. Soft biometric traits have lack of permanence but it provides some evidence about user identity and also improve the performance after using it with other biometric traits. Author proves the efficiency of purposed system with the help of MUBI software. MamtaAhlawat(Mamta Ahlawat A. K.) proposed an approach which raised the system security by combining three biometric traits. The proposed approach is a multimodal approach (iris and ear) integrating with soft biometric traits (height). Mostly the developed biometric systems are for adults but the author Shrikanttiwari(Shrikant Tiwari, 2012) defined a new approach of biometric system for recognition of new born. The purposed approach define in the paper is the combination of ear biometric trait and soft biometric traits like gender, blood group etc. the ear recognition for a new born baby is a good source of perfect recognition. There are mainly four characteristics such as universality, uniqueness, permanence and collectability which make it better recognition trait for new born. TanviDhingra(Tanvi Dhingra) proposed a combination of fingerprint and iris using soft computing techniques. In this paper performance ratio is defined in term of percentage error, accuracy, mean square error.

Proposed Approach

In this paper, purposed approach combine two physical traits with one secondary trait called soft biometrics for uniquely identification of a human being.

Mainly, this approach contains three biometric traits of a person to provide better security and faster authentication:

1.Face recognition biometric trait
2. Iris biometric trait
3. Eye color as soft biometric trait

Initially eye color which is a soft biometric trait is capture. It can capture either by using software or by manual method (majority vote decision) from the face image sample. The one of the main property of eye is eye color which is more noticeable. And it's easy to remember for differentiating an individual person (Petru Radu, 2013) by using eye color. Human beings have many eye colors which are detected such as black, brown, green, blue, gray, red etc. If a software uses for detecting various eye color than it can used with other traits for secure identification and verification. On the other side in manual method first step is manually crop the images of iris from eye and decide the eye color on the majority vote decision. There are some rules of majority vote decision which are discussed below (Antitza Dantcheva):

1. If more than 70% pixels of iris are blackthen eye color detected is "black".
2. If majority color is black but pixel ratio is less than 50% then we detect second strongest color is eye color.
3. If majority color is black and less than 50% but brown and green are in same range, so the detect color is green.

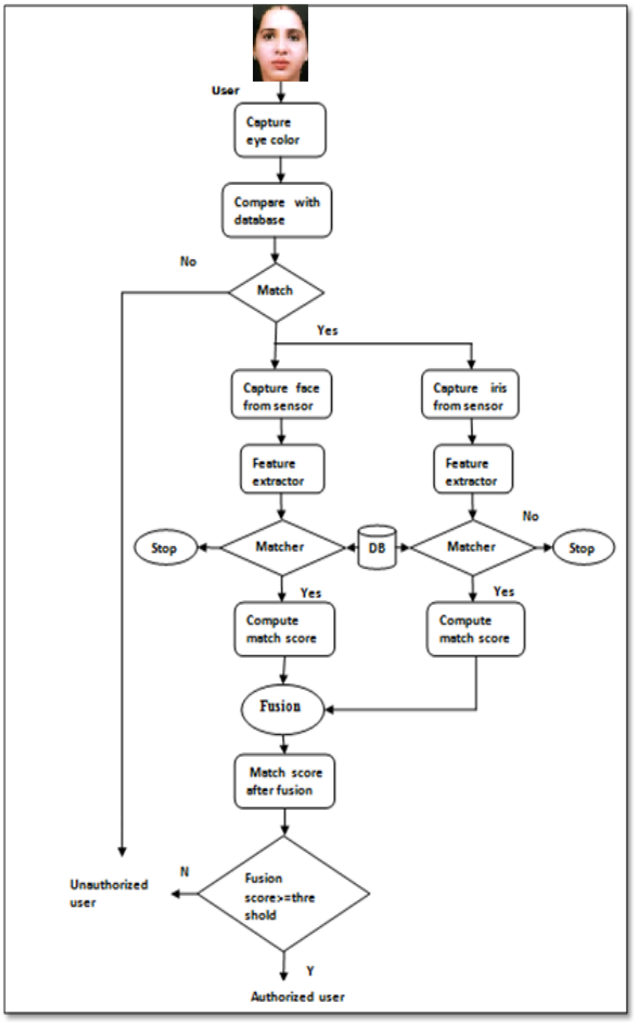

Fig 2 Proposed Approach

The captured eye color is compared with existing database. If eye color is matched then our proposed approach proceeds for extracting feature set of other traits such as face and iris otherwise recognize unauthorized user.Face and iris features are extracted and send to matcher which generates match score after comparing with stored database. The main thing in the

given approach is matcher level fusion which is done by using simple sum rule method.

Matcher level fusion combines the match score of all the modalities and provides a single fused match score result with min max normalization. This normalization technique normalize the match score in same domain such that map all match score results map into [0, 1] value. After this match score result generated through fusion is compared with threshold value. If fused match score is greater than threshold value then person is authorized otherwise user is unauthorized or imposter. The proposed algorithm by combing two primary traits (face and iris) and eye color as secondary trait is shown in Fig 2.

Algorithm for Purposed Scheme

1. Capture eye color as a soft biometric trait
2. Compare capture eye color with stored database
3. If eye color matched in the database then
   Next step is capture face from sensor

Else
Person is unauthorized user
End If

4. Extract face feature set and send to matcher
5. Matcher matches with existing database
6. If captured feature set exist in database then
   Compute face recognition match score

Else
Stop
End If

7. Capture iris from sensor
8. Extract feature set of iris and send to matcher
9. If matcher matches with existing database then
   Compute iris match score
   Else
   Stop
   End If
10. Apply min max normalization technique on face and iris for making normalized score
11. Now combine all the modalities using simple sum rule
12. If fusion score>= threshold value
    Person is authorized user
    Else
    Person is unauthorized
    End If
13. End

The purposed approach also has limitation such that large storage space is required for storing database of three biometric traits.

Conclusion

To remove the remedies and increase the efficiency of unimodal biometric system, a multimodal approach is defined. By the use of multimodal approach we can increase the aspect of security level in different application of different fields. In the purposed approach author combines the soft biometric trait with multimodal system. The purposed approach is combination of two primary traits (face and iris) and one secondary soft biometric trait (eye color). To reduce the time period during matching of database, purposed multimodal approach can be used for better recognition. In future the proposed approach with three modalities can be used where the high level of security in less verification time is required.

REFERENCES

[1] A.G. Bors, I. (1996). Image Watermarking Using DCT Domain Constraints. *IEEE International Conference On Image Processing*, (pp. 231-234).

[2] Akhil Pratap Singh, A. M. (2011). Wavelet based watermarking on digital image. *Indian Journal of Computer Science and engineering*.

[3] Anil K. Jain, K. N. (may 2004). Integrating Faces, Fingerprints, and Soft Biometric Traits for User Recognition. *Proceedings of Biometric Authentication Workshop, LNCS 3087, pp. 259-269.*

[4] Antitza Dantcheva, N. E.-L. (n.d.). On the reliability of eye color classification as soft biometric trait. france.

[5] Baisa L. Gunjal, R. M. (2010). An Overview of transform domain robust digital image watermarking algorithms. *Journal of Emerging trends in Computing and Information Sciences*.

[6] Dantcheva, A. (2011). *Facial Soft Biometrics : Methods, applications, and solutions.* Image Processing. telecom ParisTech.

[7] Kant, D. C. (2014). Performance Improvement of Biometric System using Multimodal Approach. *Volume 4*.

[8] Mamta Ahlawat, A. K. (n.d.). A Multimodal Approach to Increase the Security of Biometric System. *6*(2).

[9] Mamta Ahlawat, D. C. (2015). A Multimodal Approach to Enhance the Performance of Biometric System. *Volume 4*(Issue 6).

[10] Mohamad Abdolahi, M. M. (2013). Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic. *2*(6).

[11] N.Ratha, J. C. (june 2001). An analysis of minutiae matching strength. *Audio and video based biometric person authentication*, (pp. 223-228).

[12] Nageshkumar.M, M. a. (2009). An Efficient Secure Multimodal Biometric Fusion Using Palmprint and Face Image. *2*.

[13] Petru Radu, K. S. (2013). A Colour Iris Recognition System Employing Multiple Classifier Techniques . *12*. Canterbury.

[14] Pratibha Sharma, S. S. (2013). Digital Image Watermarking Using 3-level Discrete Wavelet Transfrom . *Conference on Advances in Communication and Control Systems 2013.*

[15] R.G. Van Schyndel, A. T. (1994). A Digital Watermark. *International Conference in Image Processing*, (pp. 86-90).

[16] S.Jayaraman, S. T. (2009). *Digital Image Processing.* New Delhi: Tata McGraw Hill.

[17] S.R.Soruba Sree, D. N. (December 2014). A Survey on Fusion Techniques for Multimodal Biometric Identification. *2*(12).

[18] Sachin Gupta, A. G. (February 2014). Proposed Iris Recognition Algorithm through Image Acquisition technique. *4*(2).

[19] Sheena, S. M. (n.d.). A STUDY OF MULTIMODAL BIOMETRIC SYSTEM.

[20] Shijun Xiang, H. J. (june 2008). Invariant Image watermarking based on statistical Features in the low frequency domain. *IEEE transaction on circuits and system for video technology* , (pp. 777-790).

[21] Shrikant Tiwari, A. S. (2012). Fusion of Ear and Soft-biometrics for Recognition of Newborn. *3*(3).

[22] T. Zong, Y. X. (2015). Robust Histogram Shape Based Method for Image Watermarking. *IEEE Transactions on Circuits and Systems for Video Technology*, (pp. 717-729).

[23] Tanvi Dhingra, M. K. (n.d.). Fusing Fingerprint and Iris Multimodal Biometrics using Soft Computing Techniques .

[24] Tianrui Zong, Y. X. (2014). Histogram shape based Robust image Watermarking Method. *IEEE ICC Communication and Information System Security Symposium*, (pp. 878-883).