IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 20, Issue 3, Ver. III (May. - June. 2018), PP 68-73
www.iosrjournals.org

A Multimodal Approach To Enhance The Performance of Biometric System

Vijender Singh[1], Dr. Chander Kant[2]
M.tech Scholar[1], Assistant professor[2]
Department of Computer Science and Applications Kurukshetra University Kurukshetra (Haryana) - India
Corresponding Author: Vijender Singh

Abstract: *Biometric security system is used to identify the person either by using their physiological traits (hand geometry, face, fingerprint etc.) or behavioral traits (voice, gait, signature etc.). the unimodal biometric system uses only single trait and do not provide higher security, whereas multimaodal system which is a subset of multibiometric system is resolve all the limitation of unimaodal and provide high degree of security. The biometric system is based on physical and behavioral traits. 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 the performance of biometric system. This work proposes a framework by combining physical traits (FKP and iris) with soft biometric trait (weight) for enhancing biometric system security and performance by assuming weight as invariant.*

Keywords: *Unimodal, Multimodal, Soft Traits, Iris recognition, FKP recognition*

Date of Submission: 07-06-2018 Date of acceptance: 26-06-2018

I. Introduction

Many decades ago, biometric features become very special tools for authentication. Biometric characteristics have the stability for long time and also able to cope with theft forgery [1].Biometric technology is the science of identifying human being by extracting a feature set from data and comparing with template store in the 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 authentication is known as unimodal biometric system. The unimodal biometric system do not provide better authentication for highly secured applications. Multimodal biometric system uses two or more biometric traits, provide high degree of security and solve all the limitations related to unimodal biometric system. A new approach multimodal was developed to overcome the limitation of unimodal system and also improve the security [2].

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.Multimodal biometric system uses more than one trait for better and secure recognition. The aim of multimodal system is to improve the rate of recognition. Different fusion methods are used for making multimodal system by combining more than one trait [3].

Soft Biometric Traits

Multimodal biometric systems provide high degree of security but also suffer 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 [4]

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

A figure is given below to show the show some basic soft traits.

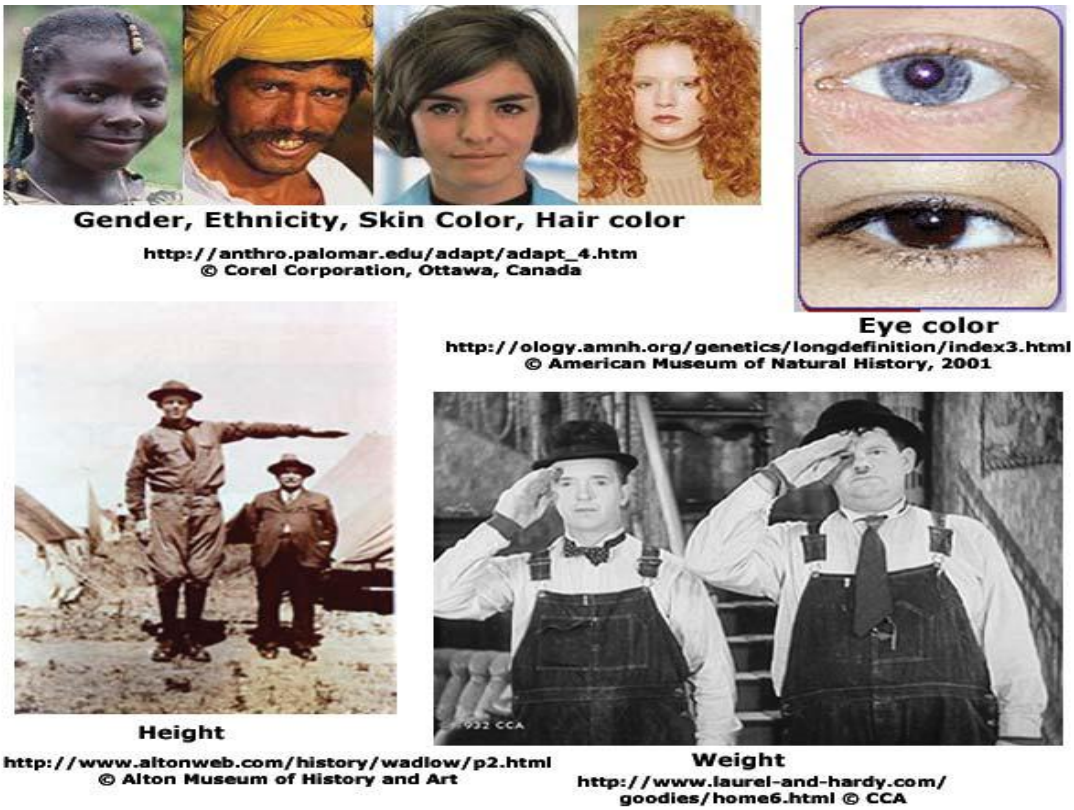

Figure 1 Soft trait for Biometric system

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 highly secure and reliable authentication. These traits are also used to improve the performance of a system by reducing verification time.This work proposes a new biometric approach by combining iris and FKP (physical traits) with weight (soft trait) for enhancing biometric system security and performance.

II. Related Works

First works in soft biometrics [tried to use demographicinformation (e.g., gender and ethnicity) and softattributes like eye color, height, weight and other visible marks like and tattoos as ancillary information to improve the performance of biometric systems. They describedthat soft biometrics can complement the traditional biometric identifiers (like face recognition) and can also be useful as a source of evidence in courts of law. But in most cases, this ancillary information by itself is not sufficient to recognize a user [5].

Kuehn studied the descriptions provided by victims in 100 police investigations [6]. Despite the prominence given to faces in eyewitness testimony, it was discovered that gender, age, height, build, race, weight, complexion, and hair color were mentioned over 70% of the time, whilst facial features were rarely mentioned.

Ailisto H, Lindholm M, Mäkelä S, Vildjiounaite E, experiment with 62 test subjects was conducted. In verification type of application total error rate of 11% was achieved using weight data alone and fusion with height data reduced the error rate to 2.4%. With a short list of five best scoring identities the percentage of cases with the correct identity on the list was 90% for weight alone and 100% for the combination of weight and height. The application domain for light biometrics is seen in non-security applications, such as homes, small offices and health clubs [7].

Ashraf Aboshosha, Kamal A. El dahshan, Ebeid A. Ebeid and Eman K. Alsayed experiment on the Fusion of Fingerprint, Iris and Face Biometrics at Decision Level and give the result FVC2004 DB3_A database is collected to evaluate fingerprint recognition systems by using minutia-based algorithm, the best accuracy given by the system equal 82.5 %. The experimental resultof iris recognition system evaluated by use ofGabor filter algorithm on CASIA database; the best accuracy achieved by the system is 95.15%. the experimental results on face94 (university of Essex, UK) database are presented to evaluate face recognition system which use local binary pattern algorithm, the system gives accuracy equal to 97.58 %.[8]

III. Proposed Approach

Proposed approach is combination of two physical traits with one soft trait for uniquely identification of an individual. This approach mainly contains three biometric traits of a person for better security and faster authentication:

1. Finger Knuckle Print recognition biometric trait
2. Iris biometric trait
3. Weight as soft biometric trait

FKP: - Recently the Finger Knuckles Print recognition technique becomes a robust biometric identifier for authentication. Researcher has found that FKN is correlated modality with a fingerprint. Finger-knuckle print is one of the emerging and highly secure biometric modality uses for authentication[9]. Fingers knuckle of the human hand are characterized by the creases on back of finger as shown inFig. 2

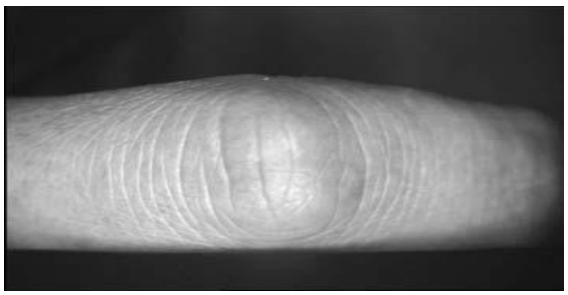

Figure 2. Finger Knuckle Print modality

Iris: - the iris is the highly secure physical traits for biometric system but the acceptance is less than the other physical traits due to the use of laser light which can damage or harm the eyes.The iris system is made of a number of subsystems, which correspond to each stage of iris recognition [10]. Figure 3 shows the iris recognition system.

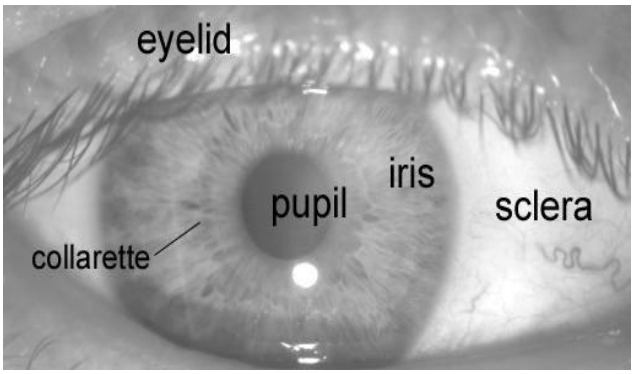

Figure 3 Iris modality

Weight: - this is a soft trait which is used for enhancing the performance of the biometric system.

Assumption- the weight is remains same (constant).

Firstly, the weight of a user can be measured by installing a weight sensor at the placewhere the users stand while providing the primary biometric. In this proposed approach we assume that the weight is constant. In enrollment phase the weight is also calculated by the sensor and stored in the database for future use. The proposed approach by combing two primary traits (FKP and iris) and weight as secondary trait is shown in 4.

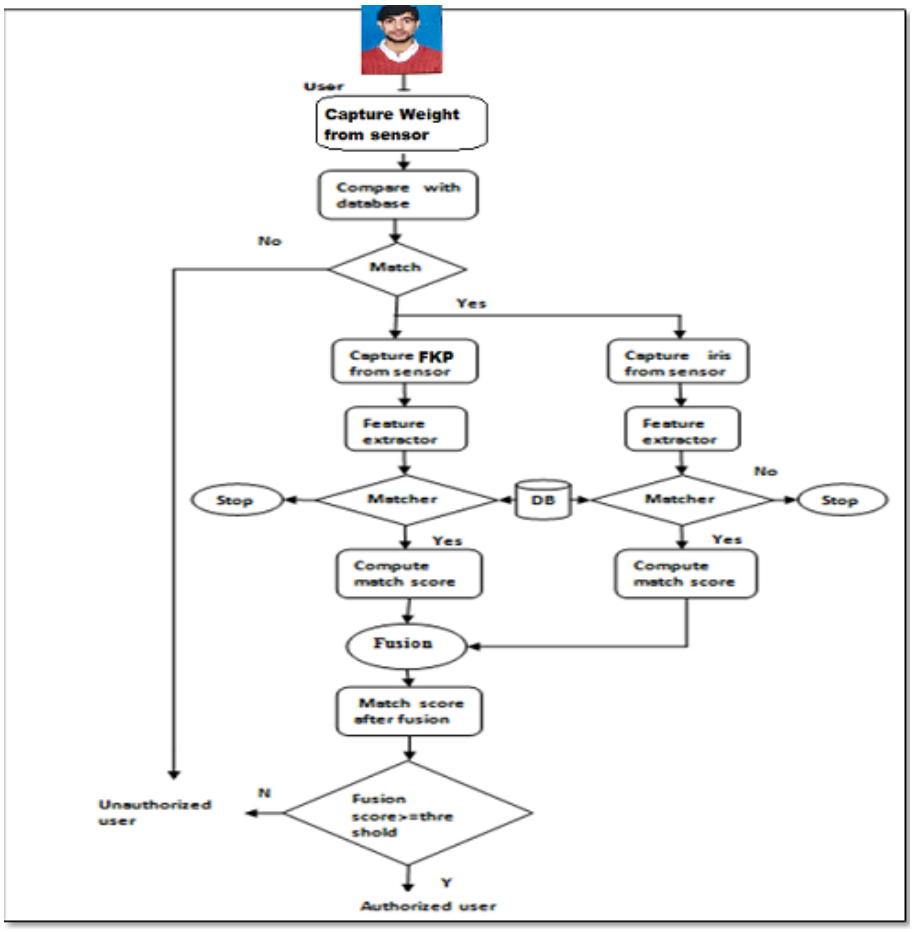

Figure 4 Diagram of the proposed approach

Whenever an individual is authenticated by this system, the weight of the individual is calculated and compared with existing database. If, the weight is matched then our proposed approach proceeds for extracting feature set of other traits such as FKP and iris otherwise recognize unauthorized user. FKP and iris feature set are extracted and forward to the matcher which generate match score after comparing with stored database of biometric device. The main thing in that approach is fusion type. Here we used matcher level fusion by using simple sum rule. Matcher level fusion combines the match scores of both primary and secondary traits and gives a single fused match score by used min-max normalized method[14]. This method normalizes the score in same domain such that map all match score results in to [0, 1] value. After this match scores result generated after fusion is compared with threshold value. If, the resulted fused match score is greater than threshold value then individual is authorized otherwise user is unauthorized or imposter.

a. Algorithm for proposed scheme

1) Calculate weight as a soft biometric trait
2) Compare calculated weight with stored database
3) If weight matched in the database then
Next step is capture FKP from sensor
Else
Person is unauthorized user
End If
4) Extract FKP feature set and send to matcher
5) Matcher matches with existing database
6) If captured feature set exist in database then
Compute FKP 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 weight, FKP and iris for making normalized score

11) Now combine all the modalities using simple sum rule

$$Sum = \sum_{i=1}^{n} Si$$

12) If fusion score>= threshold value
Person is authorized user
Else
Person is unauthorized
End If

13) End

The proposed approach also haslimitation that the storage space is required for storing database of three biometric traits will be large and increases the system complexity.

b. Experiment result

i. System Feature: - the experiment is done on HP pavilion G6 with 4GB RAM, Windows 10.

ii. Database: - in our proposed systemwe used three databases set to evaluate the performance of multimodal system. The dataset for the iris is taken from the CASIA iris database [11],PolyUfinger knuckle print dataset is taken for FKP [12] and the weight is taken manually.

iii. Performance metric

In this research work, two measures are selected named false Genuine Accept Rate and False Accept Rate (FAR) which are computed on the given databases. False accept rate is the probability of accepting an imposter as a genuine and false reject rate is the probability of rejecting a genuine as imposter. Here the aim to reduce the FAR and FRR for better accuracy.

IV. Conclusion And Future Work

The main objective of this paper is to combine the soft biometrics such as weight with the FKP and Iris modality of a person for the enhancing the biometric system performance. This purposed work could beused in an environment where authentication is required for large numbers of users. Only, when the weight is match with the existing database the system will perform the next phase for authentication, if the weight is not match with the existing database, the system will close or end the authentication process.

In future, the work will extend to build the hybrid biometric system for enhancing the biometric system's performance by using FKP and the iris as the primary traits and ethnicity, height, skin color, hair color etc., and other parameters as the soft biometric parameters and the fusion may be apply at sensor level, feature extraction level or at decision level.

References

[1]. R Raghavendra, Rao Ashok, and G Hemantha Kumar. Multimodal biometric score fusion using gaussian mixture model and monte carlo method. Journal of Computer Science and Technology, 25(4):771–782, 2010.
[2]. Dr. N.Radha S.R.Soruba Sree, "A Survey On Fusion Techniques For Multimodal Biometric Identification," Vol. 2, No. 12, December 2014.
[3]. Mahesh.Pk And M.N. Shanmukha Swamy Nageshkumar.M, "An Efficient Secure Multimodal Biometric Fusion Using Palmprint And Face Image," Vol. 2, 2009.
[4]. Karthik Nandakumar, Xiaoguang Lu, And Unsang Park Anil K. Jain, "Integrating Faces, Fingerprints, And Soft Biometric Traits For User Recognition," In Proceedings Of Biometric Authentication Workshop, Lncs 3087, Pp. 259-269, May 2004.
[5]. Pedro Tome, Julian Fierrez, Ruben Vera-Rodriguez, and Mark S. Nixon, Soft Biometrics and Their Application, ieee transactions on information forensics and security, vol. 9, no. 3, march 2014
[6]. M. D. MacLeod, J. N. Frowley, and J. W. Shepherd, "Whole body information: Its relevance to eyewitnesses," in Adult eyewitness testimony: Current trends and developments. Cambridge University Press, 1994, ch. 6
[7]. Ailisto H, Lindholm M, Mäkelä S, Vildjiounaite E. Unobtrusive user identification with light biometrics. Proceedings of the 3rd Nordic Conference on Human-Computer Interaction (NordiCHI '04, pp. 327–330;); October 2004.
[8]. Ashraf Aboshosha Kamal A. El dahshan, Ebeid A. Ebeid Eman K. Alsayed, Fusion of Fingerprint, Iris and Face Biometrics at Decision Level, International Journal of Advanced Research Computer Science and Software EngineeringVolume 5, Issue 2ISSN: 2277 128X ; , February 2015
[9]. Zhenhua Guo, Lei Zhang, and David Zhang. Rotation invariant texture classification using lbp variance (lbpv) with global matching. Pattern recognition, 43(3):706–719; 2010
[10]. Ashraf Aboshosha, Kamal A. El dahshan, Ebeid A. Ebeid and Eman K. Alsayed experiment on the Fusion of Fingerprint, Iris and Face Biometrics at Decision Level in IJARCSSE Volume 5, Issue 2, February 2015

[11]. Konstantinos Sirlantzis, Gareth Howells, Sanaul Hoque And Farzin Deravi Petru Radu. A Colour Iris Recognition System Employing Multiple Classifier Techniques; 2013.
[12]. CASIA Iris Image Database Version 1.0 http://biometrics.idealtest.org/dbDetailForUser.do?id=1
[13]. PolyU Finger Knuckle Print database Society, available at:http://www.comp.polyu.edu.hk/~biometrics/FKP.htm, last visited 2017.
[14]. Madhavi M. Kulkarni, "Study Of Multimodal Biometric System: A Score Level Fusion Approach," International Journal Of Engineering Research & Technology (Ijert), Vol. 3, No. 6, June 2014

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

* Vijender Singh. " A Multimodal Approach To Enhance The Performance of Biometric System." IOSR Journal of Computer Engineering (IOSR-JCE) 20.3 (2018): 68-73.