IJITKM Special Issue (ICFTEM-2014) May 2014 pp. 83-87 (ISSN 0973-4414)

Scale Base Classification of various Biometric Traits

Renu Chahal[1], Dr. Ajay Jangra[2]
[1,2]Department of Computer Science, University Institute of Engineering and Technology
Kurukshetra University, Kurukshetra Haryana(INDIA)
[1]Reenu.chahal10@gmail.com,[2]Ajay.jangra@uietkuk.org

Abstract: This paper critically examines the behavioral/non-behavioral biometrics with a view of security, feasibility, and acceptability. Biometrics may be defined as unique, measurable biometric characteristics, helps to verify the identity of a human being. Biometrics like fingerprint, iris, retina, face, hands, voice, DNA, keystroke etc. may be deployed or identification/verification of individual. Each biometric technology have its own merits and demerits. This paper evaluates the prosperity of each biometric by classifying their performance on 10 point scale and an analytical review is also given to guide the deployment of biometric technology on different application scenarios.

Keywords: Biometrics, identification, verification, behavioral and non-behavioral biometric traits.

1. INTRODUCTION

Biometrics term defines the characteristics which provide some information about individuals but this lack high distinctiveness and performance that can sufficiently differentiate any two individuals. A number of systems which can provide biometric based services. The identification and verification of biometrics has a number of advantages over the traditional methods of security such as pin number and ID cards (tokens). So these new biometric techniques are used because these traits need not to be carried and remembered. Thus, a biometric system operates either in identification mode or in verification mode. Before a biometric system operates its functions, it need to acquire data from an individual, features set are extracted from the acquired data, and thus a result is computed at the end after comparing the extracted features with the template stored in the database. System database consists of biometric templates which are created through a process of enrollment. Depending upon the context, system than behave in identification or verification mode.

Identification- one to many correspondence: Identification is the initial stage to identify the user using his/her biometric trait. In identification , one has to establish a person's identity(who am I ?)

Verification**:** one to one correspondence: Biometrics can also be used to verify a person's identity. Verification involves denying or confirming a person's claim identity.

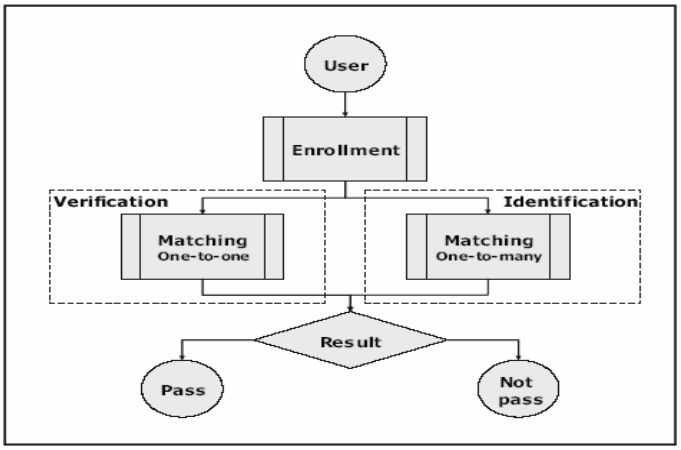


Fig 1.1: verification and identification process

A person can be identified or verified on the basis of - (i) something he holds: e.g. a credit card , a passport ,a key etc. (ii) something he knows: e.g. a PIN, a password etc. (iii) Something he is (biometrics): e.g a fingerprint , handprint, retina, iris etc.

2. METHODS USED FOR IDENTIFICATION AND VERIFICATION PURPOSES

There are a number of mature biometric traits which are also considered as legitimate proof of evidence in courts of law all over worldwide. Numerous biometrics have been researched, studied and analysed for the purpose of determining integrity, accuracy and the other suitability characteristics.

Physical Characteristics based techniques (non-behavioral)

: .

(i) Method of fingerprint verification :

A smooth and flowing pattern which is formed by ridges and furrows on the hand is called a palmprint. In modern time fingerprints are one of the most mature biometric technologies. Fingerprint based verification and identification makes better understanding of a uniqueness of a person.

Applicationssuch as forensics, access control, and driver license registration, large volumes of fingerprint biometric system is used. To reduce the computational complexity and search time ,it is better to classify these fingerprints in an accurate and consistent manner such as arch, tented arch, right loop, left loop, whorl, and twin loop.

(ii) Face recognition method:

Among other biometric traits face is also most commonly used biometric trait used to recognise a person's identity. When we commonly look at faces, we can differentiate one person to the other. Face recognition records the spatial geometry of unique features of the face using a digital camera or some other video source. Main focuses on key features of the face. Face recognition technique is mainly used to identify terrorists, criminals, and other types of persons for law enforcement purposes. This process although have high degree of variability associated with human faces like complexion, color, texture, pose changes with time and with different conditions.

(iii) Iris Recognition:

Iris is pigmented colored part of the eye. Comparing this biometric trait with other biometric traits, iris is more protected and secure one. In this system user don't need to create a physical contact with the system. He can do it from up to 2 feet away or may need to be as close as a couple of inches depending on the device. He see his own eye's reflection in the system. In iris recognition system, verification generally takes less than 5 seconds. This process usually takes less time than other recognition systems. Also to prevent a fake eye from being used to fool the system, these devices may vary the light that is shown into the eye and watch for pupil dilation.

(iv)Retina Recognition:

This technology is possibly the most accurate and one of reliable technology in today's time. Because it is difficult to use, so it requires well trained people. So it is supposed as highly invasive. The users have to be cooperative and patient to achieve a accurate result. Basically retina is a thin nerve on the back of the eye, and it is that part of the eye which senses light and transmits the impulses through the optic nerve to the brain. Retina scanning analyses the layer of blood vessels at the back of the eye. This scanning works well in both modes, i.e in identification and verification both . Further this technology includes small template size and have good operational speed.

(v)Hand Geometry

This biometric approach is the most commonly used approach in today's time. This technology uses geometric form of the hand for confirming an user's identity. Specific features of a hand such as height and width of the back of the hand , the distances between the joints, finger curves, thickness of hand, length of hand, overall bone structure are usually extracted . Those characteristics do not change in a range of years, and can be determined easily. In this system we generally record and compare the fingerprint's "minutiae points". Minutiae points can be considered the uniqueness of an individual's fingerprint. The distinctiveness of of a fingerprint can be determined by the patterns of ridges and minutae points on the surface of the finger. These unique patterns of the lines can either be in a loop, whorl or arch pattern.

Behavioral Characteristics based techniques:

(i)Voice recognition:.

The features of an individual's voice are based on the shape and size of the appendages (e.g., vocal tracts ,lips , mouth, and nasal cavities,) that are used in synthesis of the sound . In our daily lives we can easily recognise a person through his/her voice, if he/she is known to us. A voice biometric sample is the numerical model of a sound, pattern, and rhythm of a user's voice. But user's voices are changed with the time and the growth. Due to some health reasons also the voice can be changed like because of cold problem or due to other disease.

(ii)Signature Recognition:

Signature verification is the process used to recognize a user's handwritten signature. To validate the identity of a person we uses behavioral biometrics of a hand written signature of that person. This process is often called as dynamic signature verification. This thing can be achieved by analyzing the shape, pen pressure, speed, stroke , and timing information noted during the act of signing.

(iii)Keystroke dynamics:

This technique uses the rhythm and the manner in which the user types characters on the keypad or on the keyboard. However, this behavioral biometric is supposed to be not unique to each individual. Because more than a single person can use the same rhythm pattern and manner in which he/she types on any keyboard or keypad. But this process provides discriminatory information which can be useful for identification and verification process. Mainly this process of keystroke dynamics analyses the way a user types at a terminal by monitoring the keyboard inputs thousands of times per second in an attempt to identify users based on typing the rhythm patterns.

(iv)Odor:

It is known that each object possess an odor that is characteristic of its chemical composition and this thing can be used for distinguishing various objects . Air surrounding an object is blown over an array of chemical sensors, each sensitive to a certain group of (aromatic) compounds. A component of the odor emitted by a human (or any animal) body is distinctive to a particular individual .It is not clear if the invariance in the body odor could be detected despite deodrant smells, and varying chemical composition of the surrounding environment.


Face

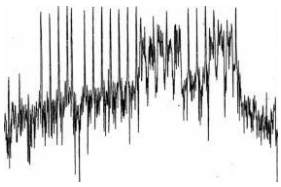

fingerprint


ear

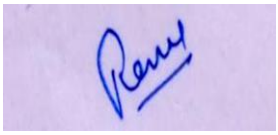

eye


hand


gait


Voice


palmprint


signature


keystroke


veins

Any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

(a)Universality and singularity: Each person must have attribute that is universal and unique.
(b)Invariance: The biometric system should be constant over a long period of time.
(c)Measurability: The properties and attributes must be easy to gather the required data.
(d)Privacy: user information must be kept as secret(private).
(e)Acceptance: extent to which a system is accepted by a large population.
(f)Reducibility: extent to which a large file or data is reduced to a file which is easy to handle.
(g)Circumvention:extent to which how easily a system can be fooled using fraudulent methods.
(h)Collectability: characteristics must be measured quantitatively.

Among the various biometric technologies being considered , the attributes which satisfy the all above requirements are facial features , fingerprints , palm prints , hand geometry , iris , retina , voice, hand veins , DNA , keystroke dynamics , signature , ear shapes , odor etc.

The use of biometrics in authentication mechanism is very inetersting because it has the possibility to establish real connection between the user's identity and physical user. The great advantage of using the biometrics is that we always carry biometrics with us. So we don't need to carry any token or card with us and no need to remember any password or key in our mind. Although biometrics possess some problems also but biometrics can be a promising future method of authentications for systems that don't communicate over common infrastructure.

Here , we show a table that will show the comparison of various biometric systems in terms of above mentioned parameters. We have ranked each biometric based on the categories as being low, medium or high. A low ranking indicates poor performance in the evaluation criterion whereas a high ranking indicates a very good performance.Here, in this table we have divided various biometric traits based on their performance characteristics as high(10), medium(7) and low(3). We can compute total percentage of each biometric trait, and based on this performance we can compute grade system of these biometric traits. Overall performance of each biometric trait is computed by dividing: {total assumed performance of each biometric trait / total expected performance(out of 10)*10}

Table: Performance comparison of various biometric traits(10=high,7=medium,3=low)

Biometrics	Universality	Uniqueness	permanence	Perfor-mance	Accept-tability	Collect-ability	Circum-vention	Total perfor-mance
Face	10	7	7	3	10	10	3	7.14
Finger-print	7	10	10	10	10	7	10	9.14
Hand geometry	7	7	7	7	7	10	7	7.42
keystrokes	3	3	3	3	7	7	7	4.71
Iris	10	10	10	10	3	7	10	8.57
Retinal scan	10	10	7	10	3	3	10	7.57
Voice	7	3	3	3	10	7	3	5.14
Odor	10	10	10	3	7	3	3	6.57
Signature	3	3	3	3	10	10	3	5.0
Hand veins	7	7	7	7	7	7	10	7.2
DNA	10	10	10	10	3	3	3	7.0
Ear	7	10	10	7	10	7	7	8.8
Gait	7	3	3	3	10	10	7	6.14

Now, as per this average performance of each biometric trait we can compute grade system which divides all biometric traits in good or bad quality performance , eg. Fingerprint trait is in A++ category. That means it have high level of performance among all biometric traits.

(i)≤ 9.1 - 10.0 = A++ (very excellent) (ii) ≤ 8.1 - 9.0 = A(excellent)
(iii)≤ 7.1 - 8.0 = B++ (super good) (iv)≤ 6.1 - 7.0 = B++(good)
(Vi)≤ 4.1 - 5.0 = C (average) (Vi)≤ 3.1 - 4.0 = C(poor)

As per this performance criteria, following calculations can be made :
(a)Security: Iris and retina are best biometric traits as per security.
(b)Easy to access and deploy: Fingerprints are easy to access and deploy because of its liveliness.
(c)Cost effective: A s fingerprint have most high permanence and performance percentage ,it is the most cost effective biometric trait among all traits.
(d) Long term effective: Retina is effective over a long time as it is highly stable over life time.

The scale base classification plot shown in Fig 1.2 indicates the performance evaluation of each biometric trait. Based on this evaluation , biometric traits are divided in good and bad quality taits in this paper.

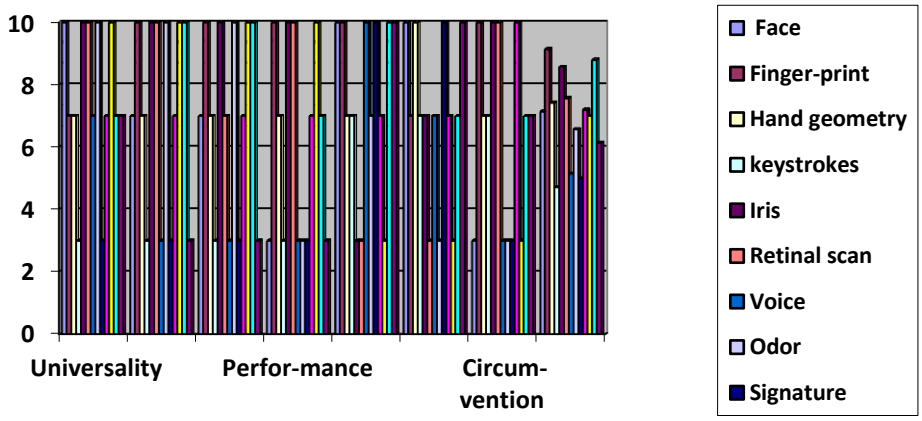


Figure1.2: Performance classification plot of multiple biometric traits

3. CONCLUSION

Biometrics is one of the important and interesting pattern recognition approach used in today's time. From the above scale base comparative analysis , it can be concluded that iris and retina are the most secure biometric traits at the current time ,as they have high performance rate all over. Only their acceptability is low because this scanning is potentially harmful to the eye. Fingerprints might be assumed as the most cost effective , easy to access and deploy biometric trait. As the fingerprints have features like liveness detection which can be used to assign real or fake finger prints. On the other way, Iris can be assumed as the most long term effective biometric trait as it is believed to be highly stable over lifetime.

REFERENCES

[1] Dr. Chanderkant " Effeciency and security optimization for fingerprint biometric system" PhD Thesis "KUK, Kurukshetra, 2009

[2] Nataliya B. Sukhai " Access Control & Biometrics" , published in InfoCD Conference'04, oct. 8, 2004, Copyright 2005, pp 124-127.

[3] Sachin Gupta, Dr. Chanderkant, "Iris Recognition: The Safest Biometric" "International Journal of Engineering & Science"Vol- 4,September 25-26,2011,pp265-273,ISSN: 2229-6913,(2011).

[4] Chander kant, Sheetal Verma "Biometric Recognition System: An Introduction" published in National level seminar on Convergance of IT and Management on 24-Nov.2007 at TIMT, Yamunanagar,(2007).

[5] Anil K. Jain, Arun Ross, Salil Prabhakar, " An Introduction to Biometric Recognition" Proceeding of IEEE, Vol-14, No.1, January 2004.

[6] Biometrics Books and Notes, Department of Computer Science & Applications, KurukshetraUniversity,Kurukshetra.

[7] A. Ross and A. K. Jain. Information Fusion in Biometrics. Pattern Recognition Letters,Special Issue onMultimodalBiometrics,24(13):2115–2125,2003.

[8] Shweta Malhotra "A Novel Approach for securing biometric template" published in international journal of advance research in computer science and software engineering IJARCSSE) ISSN:2277-128X" Volume -3 Issue fifth, may 2013. Impact factor: 2.082.

[9] Julian Fierrez and Javier Ortega Garcia, "online Signature Verification", Handbook ofBiometrics, Springer, New York, USA, 2008.

[10] A.K Mohapatral, Madhvi Sandhu2, "biometric template encryption", Published inInternational journal of Advanced Engineering &Application,January2010

[11] A.K Jain, P.J Flynn, and A. A. Ross, Handbook of Biometrics. Springer- Verlag, 2008.

[12] Arun Ross, Karthik Nandakumar, Anil k. Jain, Handbook of Multibiometrics, Springer,USA, 1th Edition, 2006.

[13] Jain, A.K., Bolle, R., Pankanti, S., eds.: Biometrics: Personal Identification in NetworkedSecurity. Kluwer Academic Publishers (1999).