Issue 9 vol 3 ISSN: 2321-8134

IJFEAT

INTERNATIONAL JOURNAL FOR ENGINEERING APPLICATIONS AND TECHNOLOGY

AUTHENTICATION OF BIOMETRICS

Vaishnavi Kharate[1], Shweta Kharode[2], Shrushti Gite[3]

[1]*Student, CSE Department, Jawaharlal Darda Institute Of Engineering and Technology, Maharashtra, India,* ***vaishnaviytl@gmail.com***

[2]*Student, CSE Department, Jawaharlal Darda Institute Of Engineering and Technology, Maharashtra, India,* ***shwetakharode398@gmail.com***

[3]*Student, CSE Department, Jawaharlal Darda Institute Of Engineering and Technology, Maharashtra, India,* ***shrushtigite99@gmail.com***

Abstract

Over the last few years a new area of engineering science has been established whose products are likely to create a large market in near future .it has been called "Biometrics". The pioneers of these new domain intend to construct devices which would allow identification of person on the basis of his/her "Biological" characteristics like voice, dynamics of a movements ,features of face and other parts of body, retina or iris pattern .Nature has made human beings with different characteristics which may vary from one person to another .These properties use of by Biometric Technology to distinctly identify each person.

Biometric system is essentially a pattern recognition system which recognize a user by determining the authenticity of specific physiological or behavioral characteristics processed user . Several important issues must be considered in designing practical Biometric system. Depending on the context a biometric can operate either in verification or an identification mode. First ,a user must be enrolled in the system so that the biometric template can be captured .this template is retrieved when an individual needs to be identified .Over the traditional methods like ID cards ,PIN number this method of identification offers several advantages. By replacing PINs biometric techniques can potentially prevents unauthorized access to ATMs & Computer network.

Index terms: *Biometrics, recognition.*

---------- *** ----------

1. Introduction

Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solution .As the level of security breaches and transaction fraud is increasing nowadays, the need for highly secure identification and personal verification technologies is becoming apparent.

Biometrics are automated methods of recognizing a person based on a physiological and behavioral characteristics .Among the features measured are face, fingerprint, hand geometry ,iris, retinal, signature and voice. Biometric based solution are able to provide for confidential financial transactions and personal data privacy. The need for biometrics can be found in federal, state, local government , in military and commercial applications.[4]

2. History of Biometric:

Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solution .As the level of security breaches and transaction fraud is increasing nowadays, the need for highly secure identification and personal verification technologies is useful.

Biometrics are automated methods of recognizing a person based on a physiological and behavioral characteristics .Among the features measured are face, fingerprint, hand geometry ,iris, retinal, signature and voice. Biometric based solution are able to provide for confidential financial transactions and personal data privacy. The need for biometrics can be found in federal, local government , state in military and commercial applications.[4],[2].

3. What is Biometric?

Biometrics is the measurement and statistical analysis of people's physical characteristics .The basic premise of biometric authentication is that everyone is unique and individual can be identified by his /her intrinsic physical or behavioral traits. Identification is one to many comparing process for a biometric sample or a code derivate from it against all of the known biometric reference template on a file .if the acquired sample matches a template stored in the error marginal identity of the enrollee should also match to that of the previously stored reference . The stored identity information really should not reveal the physical identity of the owner of the biometric ,but instead a role which authorizes the use of service or access .

4. Authentication

There are various biometrics authentications which are as follows:-

- Bertillonage – measuring body lengths .
- Facial Recognition- measuring facial characteristics.
- Hand geometry – measuring the shape of hand.
- Fingerprint – analyzing fingertip patterns.
- Vascular patterns-analyzing vein pattern.
- Iris scan-analyzing characteristics of colored ring of the eye.
- Retinal Scan-analyzing blood vessels in the eye .
- Voice recognition – analyzing vocal behavior.
- Signature recognition-analyzing signature dynamics.
- DNA analysis – analyzing genetic makeup.

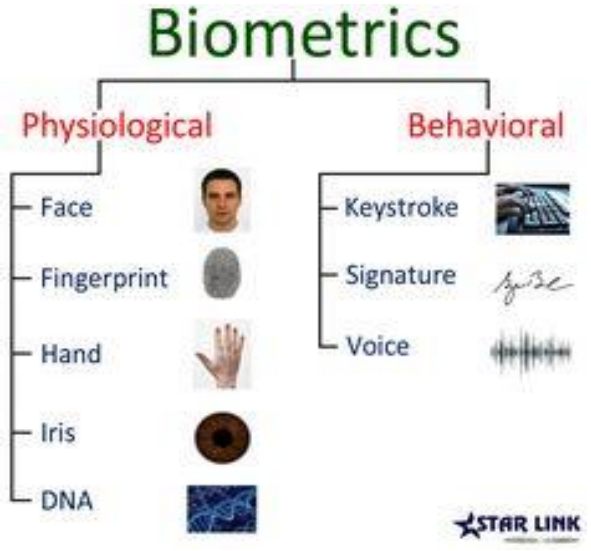


Fig-1: Authentication of Biometrics.

4.1. Voice Recognition

Voice recognition also commonly referred to voice print . It is the identification and authentication arm of vocal modalities .By measuring the sound of a user makes while speaking voice recognition software can measure the unique biological factors that combined produce his/her voice.

Voice prints can be measured passively as user speaks naturally in conversation or actively ,if she is made to speak passphrase. The key is that true voice recognition measure the minutia of the voice and it is not wholly dependent on the spoken code or passphrase.[3]

Fig-2: Voice recognition

4.2 Face recognition

Often leveraging a digital or connected camera, facial recognition software detects the faces in the images, quantify their characteristics, and then match them against the stored templates in a database.

For the purpose of identification or authentication face recognition technology measures and matches the unique characteristics.

With growing technologies facial recognition can convert a photograph or a video image into a code that describes a face physical characteristics this can be used to identify the common person from over distance without introducing into there personal space.

Computer software for facial identification reads the peak valleys of an individual facial features .These peak & valley are known as nodal points .Facial recognition is most natural means of biometric identification .This method distinguishing one individual form another is an inherent ability of virtually every human .wearable computers will allow this technology be ubiquitous and be the more effective in huge crowds.[1]

4.3 Hand Geometry

Hand geometry is a type of biometric that identifies the user by the shape of their hands. Hand geometry readers measure the user's hand along many dimensions and compare those measurements to measurements to the previously stored in a file. The Viable hand geometry devices has been manufactured since the early 1980s, making hand geometry the first biometric to find widespread computerized use. It

remains popular; common applications include access control and time-and-attendance operations.

Fig-3: Hand Recognition

Advantages of Hand Geometry Biometrics:

- Environmental factors, such as, dry weather that causes the drying of the skin is not an issue.
- Usually considered less intrusive than fingerprints, retinal, etc.
- Simple, relatively easy to use and inexpensive.
- Hand geometry data is easy to collect, but as in the fingerprints where a good frictional skin is required by the imaging systems, and retinal data where special lighting is required.

Disadvantages of Hand Geometry Biometrics:

- Not ideal for growing children
- Jewellery (rings, etc), limited dexterity (arthritis, etc) etc may pose a challenge in extracting the hand geometry information.
- The hand geometry is not unique and cannot be used in identification system.[3],[1].

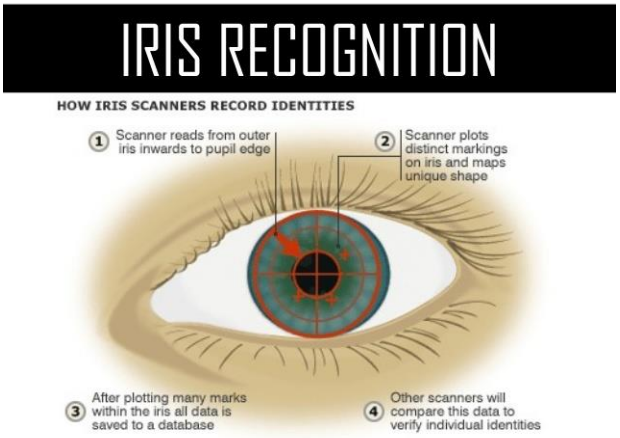
4.4. Iris recognition

Iris scanning biometrics can measure the unique patterns in the colour circle of the users eye to verify and authenticate the identity. Fast, renowned and Contactless for its accuracy, biometric iris recognition can operate at longer distances, with some solutions that leverage the modality requiring only a glance from a user.

Iris-based identification is required to specify the hardware to be used, unlike software based modalities like face and voice recognition, so it is not common in consumer facing deployments. Only because of recent innovations in biometrics that have made the technology more accessible in terms of cost and installation, iris biometrics is becoming more prominent over the vertical markets and can be also in the consumer electronics sphere.

Iris recognition is commonly used as a physical access control modality, ideal for high throughput environments that demand speed and accuracy. It can be used frequently in border control deployments, which is able to identify travellers as they enter and exit countries by land, sea and air. Recently, iris scanners have made their way to the users mobile devices, a development that has some heralding the rise of iris recognition. Iris scanning plays a important role in the biometric border control pilot project underway at the Otay Mesa US-Mexico land border.

Fig-5: Iris Recognition.



Advantages of Biometric

1. Improved customer.
2.Lost Reduced operational costs.
3. Improve d security.

Disadvantages of Biometric

1. Environment and usage can affect measurements.
2. Systems are not 100% accurate.
3. Require integration and/or additional hardware.
4. Cannot be reset once compromise.

5. CONCLUSION

Biometric points are useful for making identification with cameras systems, but they depend on the existence of a previously generated databases so that distances can be compared. With the adoption of standards and community awareness, this technology will become more mainstream . Although still a relatively new entry into the biometrics market, facial recognition is quickly emerging as a viable authentication method .Current implementations of this technology are visible in airports, at ATM machines and border control checkpoints. Any good authentication system will not rely on only one technology but will include a combination of technologies[2]

REFERENCES

[1]. http://www.creativeworld9.com/2011/03/abstract-on-biometrics.html?m=1
[2]. http://www.findbiometrics.com/solutions/voice-speech-recognition/
[3]. https://googleweblight.com/i?u=https;//findbiometrics.com/solution/facialrecognition/&grqid=pUEwt_OJ&hl=en-IN
[4]. https://www.findbiometrics.com/solutions/iris-scanner-recognition/