Pros & Cons of Various Bio-Metric Authentication Systems

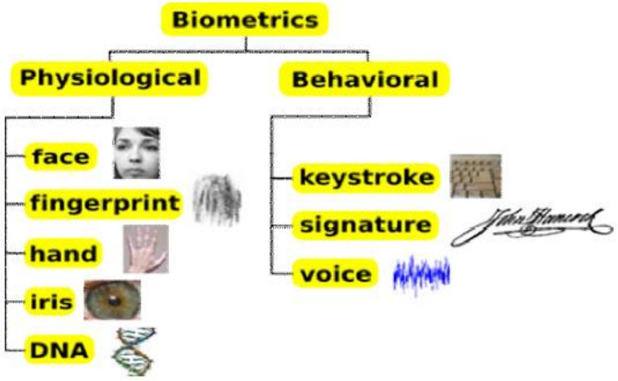
[1]C.Arunkumar, [2]M.Deepanayaki

Abstract— This paper presents pros and cons of various biometric authentication systems. A brief introduction is usually offered regarding commonly used biometrics including, Face, Iris, Fingerprint, Finger Vein, Lips, Voice, Signature Verification, Keystroke dynamic, DNA. With the fast increasing of the electronic crimes and their related issues, deploying a reliable user authentication system became a significant task for both of access control and securing user's private data. Such authentication models have overcome other traditional security methods like passwords and PIN. This paper outlined opinions about the usability of biometric authentication systems & advantages and disadvantages, future development of biometric authentication system.

Keywords—Biometric systems, technique, face, Iris, finger, lips, voice.

1 Introduction

"Biometrics" implies "life measurement" however the term associated with the utilization of unique physiological characteristics to distinguish an individual. It's a new way to verify authenticity. Biometrics utilizes biological characteristics or behavioral features to recognize an individual. In real a Biometrics system is a pattern identification system that uses various patterns such as iris patterns, retina design and biological characteristics like fingerprints, facial geometry, voice recognition and hand recognition and so forth. Biometric recognition system provides possibility to verify one's identity simply by determining "who these people are" instead of "what these people possess or may be remembered. The very fact that makes it really interesting is that the various security codes like the security passwords and the PIN number could be interchanged among people but the physical traits cannot be. The principle use of Biometric security is to change the existing password system. There are numerous pros and cons of Biometric system that must be considered.



2 Biometric Techniques

Jain et al. describe four operations stages of a Unit-modal biometric recognition system. Biometric data has acquisition. Data evaluation and feature extraction. Enrollment (first scan of a feature by a biometric reader, produce its digital representation and create a template, even a few in most of the systems).

3 Numerous Biometric Systems

1. Facial recognition
2. Iris
3. Finger print
4. Lips
5. Voice

New and emerging biometric techniques are

1. Human scent recognition
2. EEG biometrics
3. Skin spectroscopy
4. Knuckles texture
5. Finger nail recognition

4 Biometrics Methods

4.1 Facial recognition

Facial scanning involves scanning of the entireface and checking of critical points and areas in the facewith the template.

Fig 1: facial recognition

- [1]C. Arunkumar, II MCA, Department of Computer Application, Priyadarshini Engineering College, Vaniyambadi, E-mail: arunjai658@gmail.com.
- [2]M. Deepanayaki , Associate Professor, Department of Computer Application, Priyadarshini Engineering College, Vaniyambadi, E-mail: mdeepanayaki@priyadarshini.net.in

4.1.1 Advantages

1. It does not require any co-operation of the test subject to do any work.
2. Systems set up in airports, multiplexes, and other open public areas can easily identify an individual among the massive crowd.
3. This performs massive identification which usually other biometric system can't perform.
4. The systems don't require any direct contact of a person in order to verify his/her identity. This could be advantageous in clean environments, for monitoring or tracking, and in automation systems.
5. Incident monitoring for security with photo which in turn taken by a camera, but there is no such evidence with the fingerprint technology to track these incidents.

4.1.2 Disadvantages

1. Face recognition isn't perfect and faces challenges to perform under certain conditions.
2. One obstacle associated with the viewingposition of face.
3. Face recognition doesn't work effectively in bad/weak lighting, sunglasses/sunshades, lengthy hair, or other objects partly covering the subject's face.
4. Not much effective for low resolution images.

A serious drawback is that many systems are usually less efficient if facial expressions vary. Even a big grin/laugh can render the system's performance less effectively. (so significantly North america now permits only neutral facial expressions on passport photos)
Additionally, when used for security purposes, it is more costly and complex as compared to some other techniques. Iris recognition offers one of the most secure strategies of authentication and recognition. Once the impression of an iris has been taken using a standard digicam, the authentication process involves, evaluating the present subject's iris with stored version. It is one of the most accurate technique with very low false acceptance as well as rejection rates. This is how the technology becomes very useful.

4.2 Iris Recognition

In Iris and Retinal scanning, the iris and the retina are scanned by a low intensity light source and the image is compared with the stored patterns in the database template. This is one of the fastest forms of biometry.

Fig 2: Iris

4.2.1 Advantages

1. Iris possesses unique structure shaped by 10 months of age, and is always stable throughout life.
2. The iris incorporates fine texture. Even genetically similar people have entirely independent iris textures.
3. An iris scan can be carried out through 10 cm to a few meters apart.
4. Non-intrusive data collection (no actual contact with a scanner is required).
5. Data capturing can be carried out even though a user is putting contact lenses or glasses.
6. High accuracy and High recognition process speed.

4.2.2 Disadvantages

1. Iris scanners might be very easily fooled through a superior quality image of an iris or face instead of the real thing.
2. The scanning devices are often hard to adjust and may annoy multiple people of various heights.
3. The accuracy of scanning devices may impacted by unusual lighting effects and illumination from reflective types of surfaces.
4. Iris scanners tend to be more expensive in comparison with additional biometrics.
5. Because iris is a tiny organ to scan from a long distance, Iris recognition becomes challenging to perform well at a distance larger than a few meters.
6. Iris recognition is vulnerable to inadequate image quality

4.3 Fingerprint Verification

This is one of the oldest forms of biometrictechniques which involves mapping of the pattern of the fingerprint of the individual and then comparing the ridges,furrows, within the template. The fingerprint given to thedevice is first searched at the coarse level in the databaseand then finer comparisons are made to get the result.

Fig 3: fingerprint

4.3.1 Advantages

1. These systems usually are simple to use and install.
2. It requires inexpensive equipment which usually have low power intake.
3. A fingerprint pattern has individually distinctive composition and characteristic remains the same with time.
4. Finger prints are largely universal. Only, of the 2% of human population cannot use finger prints due to skin damage or hereditary factors.
5. Fingerprints are the most preferred biometric.
6. Biometric fingerprint scanner presents a method to record an identity point which is very hard to be fake, making the technology incredibly secure.
7. It is easy to use along with the high verification process speed and accuracy.

4.3.2 Disadvantages

1. Because fingerprint scanner only scans one section of a person's finger, it may susceptible to error.
2. Many scanning system could be cheat employing artificial fingers or perhaps showing another person's finger
3. Sometimes it may take many swipe of fingerprint to register.
4. Fingerprints of people working in chemical sectors often affected.
5. Cuts, marks transform fingerprints which often has negatively effect on performance.

4.4 Lip identification

Essentially the most growing technique of human recognition, which originates from felony and forensic process, is usually human lips identification. This biometric accumulate significant focus recently because it deals with many difficulties of traditional identification. So as to recognize human identity, lips form and color characteristics are taken into consideration. Lip biometric may be used to improve the potency of biometrics such as facial and voice recognition.

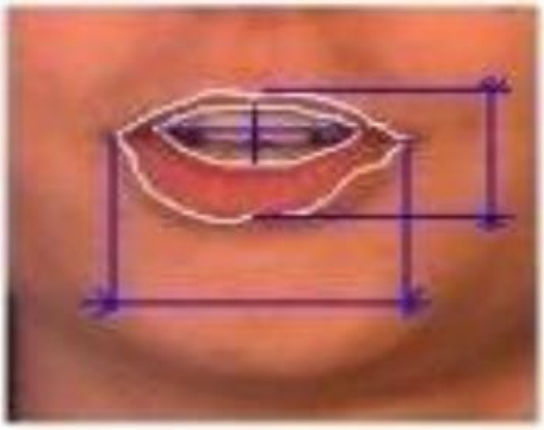


Fig: Lip Identification

4.4.1 Advantages

1. Study proves that lips attributes are usually distinctive and also unchangeable for every single examined person.
2. Lips prints used by forensics professionals and criminal police training.
3. Size of template is small.
4. Lips based human recognition dependent on static mouth/face photos.
5. Lips biometric certainly are passive biometrics – person's interaction is just not necessary.
6. Photos might be obtained from the distance without having analyzed person's knowledge.
7. Lips usually are visible – not hidden/overcast by anything.
8. Lips biometric can be hybrid to use as lips-voice or lips-face biometric systems

4.4.2 Disadvantages

1. The concept of developing hybrid (multimodal) biometric system needs a lot of attention.
2. Main drawback of this method is that the particular facial attributes chosen may not acquire relevant details. E.g. visibility of teeth may present additional details that can't be utilized by a lip shape model alone.
3. A big smile might cause difficulty in recognition of a person with respect to same person with neutral appearance as before.

4.5 Voice Biometry

It is proved that the frequency, stress and accent of speech differ from person to person. Voice biometry uses this concept to solve the problem of illegal user. This system has been implemented in the latest laptops as well.

Fig: Voice Biometry

4.5.1 Advantages

1. Speech can be recommended as a natural input as it does not demand any training and it is considerably quicker as compared to some other input.
2. Voice is usually a quite natural strategy to communicate, and in fact it is not necessary for you to sit at keyboard set or even work with handheld remote control.

3. This technique helps those people who have difficulty of using their hands.
4. It does not require any training for users.
5. It offers a big advantage to those who suffer from problems that may impact their writing capability but they can use their voice toproduce words/text on desktop computers or may be other equipment.

4.5.2 Disadvantages

1. Even the most efficient voice recognition systems very often may make mistakes, when there is disturbance or some noise in the surrounding.
2. Voice Recognition systems works well only if the microphone is actually close to the end user. Much more far-away microphones are likely to boost the number of errors.
3. May hacked with prerecorded voice messages.
4. Possesses primary amount of time for adjustment with each user's voice.
5. Different persons might speak various languages.
6. Several words sound very similarly. Case: two, to, too

5 Comparison Of Biometrics

A biometric system can provide two functions. One of which is verification and the other one is Authentication. So, the techniques used for biometric authentication has to be stringent enough that they can employ both these functionalities simultaneously. Currently, cognitive biometrics systems are being developed to use brain response to odor stimuli, facial perception and mental performance for search at ports and high security areas. Other biometric strategies are being developed such as those based on gait (way of walking), retina, Hand veins, ear canal, facial thermo gram DNA, odor and scent and palm prints. In the near future, these biometric techniques can be the solution for the current threats in world of information security. Of late after a thorough research it can be concluded that approaches made for simultaneous authentication and verification is most promising for iris, finger print and palm, vain policies. But whatever the method we choose, main constraint will be its performance in real life situation. So, application of Artificial System can be a solution for these cases. We have given emphasis on the Iris recognition. According to us, after detection of an iris pattern, the distance between pupil and the iris boundary can be computed. This metric can be used for the recognition purposes because this feature remains unique for each and every individual. Again, an artificial system can be designed which will update the stored metric as the proposed feature may vary for a particular person after certain time period After doing the manual analysis of the above discussed method, we have got a satisfactory result. Due to the dynamic modification of the proposed metric, the rejection ration for a same person reduces blot. The work is being carried out to make the system viable.

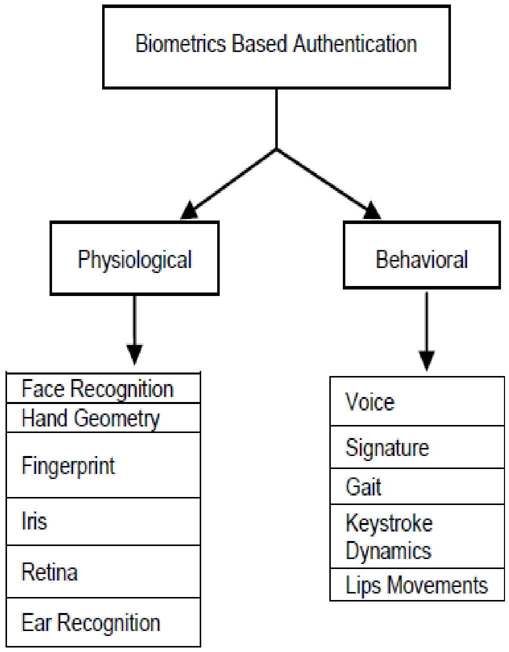


Fig: Block diagram for Biometric Authentication

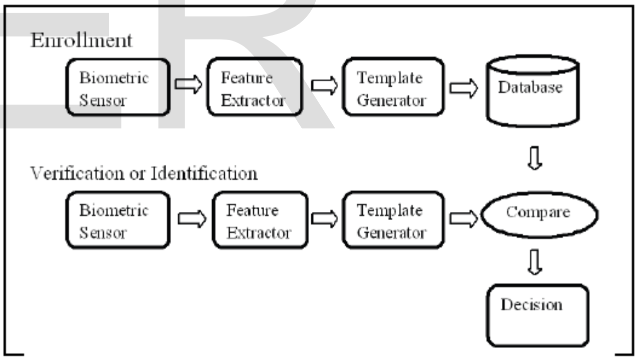


Fig: Block diagram for verification or identification

5.1 Comparison Table of biometrics authentication system

Biometrics	Accuracy	Cost	Size of template	Long term stability	Security level
Facial recognition	Low	High	Large	Low	Low
Iris scan	High	High	Small	Medium	Medium
Finger print	Medium	Low	small	Low	Low
Voice recognition	Low	Medium	Small	Low	Low
Lip recognition	Medium	medium	Small	Medium	High

6 Conclusion

Securing critical and sensitive systems from being illegally accessed by imposters has been a potential research field. Biometric based security authentication obtained considerable attention for its accuracy, reliability, universality and permanence etc. This paper overviewed the most conducted pros and cons of biometric authentication system. The focus of this work is to briefly present various biometric security methods. Such, as Facial recognition, Iris, Finger print, Lips, Voice. Moreover, transforming such security authentication techniques from traditional practical environment into more flexible one such as mobile phones it can potentially upgrade the integration of the overall system.

References

1 John R.Vacca.,"Biometric technologies and verificationsystems"2010.

2 Olufemi Sunday Adeoye. "A Survey of Emerging BiometricTechnologies". International Journal of Computer Applications,2010.

3 A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. Circuits Syst.Video Technology, Special Issue Image- and Video-Based Biomet., Volume 14, Issue 1, Jan. 2004..

4 R. Sanchez-Reillo, C. Sanchez-Avila, and A. Gonzales-Marcos, "Biometric identification through handgeometry measurements,", IEEE Trans. Pattern Anal. Mach. Intell., Volume 22, Issue. 10, Oct. 2000.

5 Jain, A., Bolle, R. and Pankanti S. (1999). BIOMETRICS: Personal Identificationin Networked Society. Kluwer Academic Publishers.

6 Smart Cart Alliance Identity Council (2007): Identity and Smart Card Technology and application.

7 http://www.smartcardalliance.org, as visited on 25/10/2008.

8 Jain,sA.K.;Ross, A. &Pankanti, S., "Biometrics: A Tool for Information Security", IEEE Transactions onInformation Forensics And Security, Volume 1, issue 2, Jun. 2006.

9 R.Cappelli,D.Maio,D.Maltoni,J.L.Wayman, and A.K.Jain, "Performance evaluation of fingerprintverification systems", IEEE Trans. Pattern Anal. Mach. Intell., Volume 28, issue 1, Jan. 2006.

10 S. Hocquet, J. Ramel, H. Cardot, "Fusion of Methods for Keystroke Dynamic Authentication", In Proc. of 4thIEEE Workshop on Automatic Identification Advanced Technologies, USA, Oct. 2005.

11 S. Im, H. Park, Y. Kim, S. Han, S. Kim, C. Kang, and C. Chung, "A Biometric Identification System byExtracting Hand Vein Patterns", Journal of the Korean Physical Society, Korean Publication, Volume 38,Issue 3, Mar. 2001

12 Deutschmann, I., Nordstrom, P., & Nilsson, L. (2013). Continuous authentication using behavioral biometrics. IT Professional,

13 Zaeri, N. (2011). Minutiae-based fingerprint extraction and recognition. INTECH Open Access Publisher.

14 Faundez-Zanuy, M., "Biometric security technology," in Aerospace and Electronic Systems Magazine, IEEE, June 2006

15 Narhar, U.K.; Joshi, R.B., "Highly Secure Authentication Scheme," in Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on , Feb. 2015

16 Jain, A.K.; Ross, A.; Prabhakar, S., "An introduction to biometric recognition," in Circuits and Systems for Video Technology, IEEE Transactions on, Jan. 2004

17 Liu, Simon; Silverman, M., "A practical guide to biometric security technology," in IT Professional, Jan/Feb 2001

18 Delac, K.; Grgic, M., "A survey of biometric recognition methods," in Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium,June 2004