COMPARISON OF VARIOUS BIOMETRIC METHODS

Rupinder Saini , Narinder Rana
Rayat Institute of Engineering and IT
errupindersaini27@gmail.com, narinderkrana@gmail.com

Abstract
This paper presents comparison concerning various biometric systems simply by defining their advantages and disadvantages. A brief introduction is usually offered regarding commonly used biometrics, including, Face, Iris, Fingerprint, Finger Vein, Lips, Voice. The comparison criteria list introduced is restricted to accuracy, size of template, cost, security level, and long term stability.

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" [4]. 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 uni-modal biometric recognition system [1]:

- Biometric data acquisition.
- Data evaluation and feature extraction.
- Corresponding scores creation (analyzed data is then compared with what is actually saved in the database).
- 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).

2. Numerous Biometric Systems :

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

New and emerging biometric techniques are:

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

2.1 Facial recognition

Face recognition involves an evaluation of facial features. It is a computer system application for automatically determining or verifying an individual from a digital image or a video framework from a video source. One of the techniques to do this is simply by evaluating selected facial features from the image as well as from facial database.

Advantages

- It does not require any co-operation of the test subject to do any work.
- Systems set up in airports, multiplexes, and other open public areas can easily identify an individual among the massive crowd.
- This performs massive identification which usually other biometric system can't perform [2].
- 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 [2].
- User-friendly design: Contactless authentication.
- 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.

Disadvantages

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

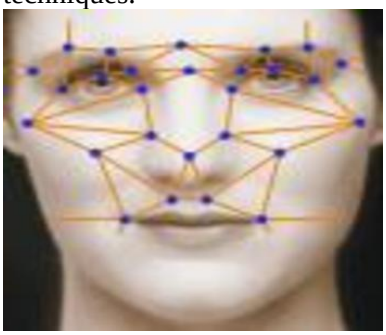


Fig.1 Image sample for Facial recognition

2.2 IRIS

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.

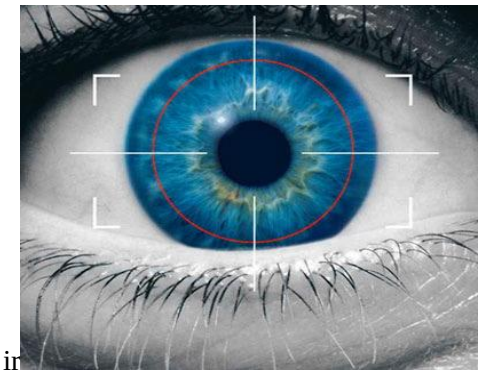
Advantages

- Iris possesses unique structure shaped by 10 months of age, and is always stable throughout life.
- The iris incorporates fine texture. Even genetically similar people have entirely independent iris textures [2].
- An iris scan can be carried out through 10 cm to a few meters apart.
- Non-intrusive data collection (no actual contact with a scanner is required)[2] .
- Data capturing can be carried out even though a user is putting contact lenses or glasses [2].
- High accuracy and High recognition process speed [2].
- Easy recognition of fake irises (e.g. when somebody wear color contacts).
- Scalability along with the speed is significantly advantageous [4].
- Minimal false acceptance rate.
- Two seconds processing time.

- Iris recognition security systems are viewed as one of the most appropriate security system nowadays. It is truly a distinctive and easy way to identify a user.

Disadvantages

- Iris scanners might be very easily fooled through a superior quality image of an iris or face instead of the real thing.
- The scanning devices are often hard to adjust and may annoy multiple people of various heights.
- The accuracy of scanning devices may impacted by unusual lighting effects and illumination from reflective types of surfaces.
- Iris scanners tend to be more expensive in comparison with additional biometrics [1].
- 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.
- Iris recognition is vulnerable to inadequate image quality.
- People suffer from diabetes or some other serious disease cause alterations in



is.

Fig.2 Image sample for Iris Recognition

2.3 Finger print

Our fingerprint is constructed of numerous ridges and valley on the surface of finger which are unique to each and every human [1]. "Ridges are the top skin layer portions of the finger and valleys are the lower portions". The particular individuality of a fingerprint could be determined by the several patterns of ridges and furrows plus the minutiae points. Fingerprint authentication in actual an automated method of verifying a match among different human fingerprints.

Advantages

- These systems usually are simple to use and install.
- It requires inexpensive equipment which usually have low power intake.
- A fingerprint pattern has individually distinctive composition and characteristic remains the same with time [2].
- Finger prints are largely universal. Only, of the 2% of human population cannot use finger prints due to skin damage or hereditary factors [10].
- Fingerprints are the most preferred biometric.
- One should not have to remember passwords, you simply swipe your finger on scanner and done it.
- Biometric fingerprint scanner presents a method to record an identity point which is very hard to be fake, making the technology incredibly secure.
- It is easy to use along with the high verification process speed and accuracy [1].

Disadvantages

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

- Finger prints aren't private. We all leave fingerprints almost everywhere. Once the finger prints are stolen, they are stolen for life time! You possibly in no way get back to a secure situation [10].

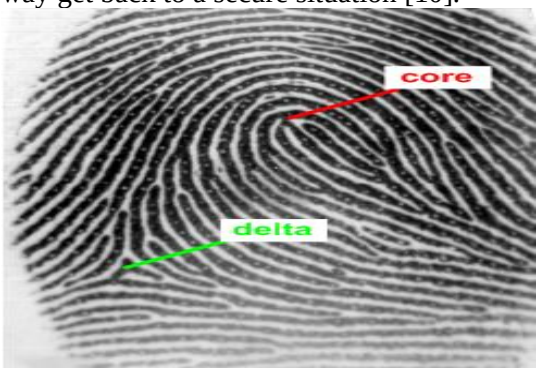


Fig.3 Image sample for Finger Print Recognition

2.4 Finger Vein

Finger vein authentication is often a biometric technology which specifies an individual when using the vein pattern inside of the fingers. Veins are usually the blood vessels which carry blood towards the heart. Every single person's veins are having unique physical and behavioral features. It provides a greater degree of security that protects information and access control much better. As deoxyhemoglobin in the blood absorbs infrared lights, vein patterns appear as several dark outlines. The infrared lights combine with special camera capturing an image of the finger vein pattern. This image is then transformed into pattern data along with saved as a template of any person's biometric authentication data. While authentication, the particular finger vein image is taken and is compared against the saved template of the person.

Advantages

- Finger vein patterns are generally distinctive to every person; even among identical twins, so the actual false acceptance rate is quite low (near to zero).
- Placing a hand or finger is actually less invasive in comparison to other biometric technologies.
- Because blood vessels/veins are located inside the human body, it is quite hard to read or steal. There is minor risk of forgery or thieves.
- As finger veins do not depart any trace during the authentication process and thus can't be duplicated.
- Finger vein patterns stay continuous throughout the adult years and so re-enrollment of the vein pattern does not required once singed up.
- Finger veins are less likely to be affected by changes in the weather conditions or health conditions of the specific.
- Rashes, cracks and rough epidermis do not have an impact on the result of authentication.
- The level of accuracy from vein recognition systems is quite outstanding.
- Time which delivered to validate each individual is smaller as compared to other methods (average is 1/2 second).
- Vein patterns need only low image resolution.
- Finger vein authentication technology is inexpensive and having smaller size of templates.

Disadvantages

- In case an accident causes a user to lose his/her finger then it can be a problem during the verification process.
- Expensive: The actual technologies seriously aren't cheap enough for bulk deployment.
- Larger Size: The existence of CC camera makes the system larger than a fingerprint scanner.
- This technology is still untested mainly because only vendor companies affirm the accuracy levels. Governments and standards companies have not proven its capability yet.
- Not for bulk recognition.

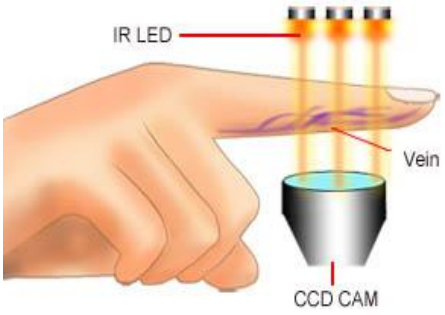


Fig.4 Image sample for Finger vein Recognition

2.5 Voice recognition

Voice recognition is a technology through which sounds, phrases and words voiced by human beings are transformed into electrical signals, and then these signals are converted into code design [9]. Here we emphasize on the human voice because we generally and most often use voices to communicate our thoughts, our ideas with others in surrounding environment [9].

Advantages

- 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.
- 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.
- This technique helps those people who have difficulty of using their hands.
- It does not require any training for users.
- It offers a big advantage to those who suffer from problems that may impact their writing capability but they can use their voice to produce words/text on desktop computers or may be other equipments.
- One of the major advantages of voice recognition technique is to cut back misspelled texts of which many typists may perhaps suffers a problem during typing.
- The particular support significantly eliminates the amount of time period to edit and fix spelling corrections. And so the general advantages could be the time management.
- The majority of people can speak more rapidly in comparison with they can type with fewer errors.

Disadvantages

- Even the most efficient voice recognition systems very often may make mistakes, when there is disturbance or some noise in the surrounding.
- 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.
- May hacked with prerecorded voice messages.
- Possesses primary amount of time for adjustment with each user's voice.
- Different persons might speak various languages.
- Several words sound very similarly. Case: two, to, too.
- Largely expensive.

Fig.5 Image sample for Voice Recognition

2.6 Lip identification

Essentially the most growing technique of human recognition, which originates from felony and forensic process, is usually human lips identification [8]. 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 [8]. Lip biometric may be used to improve the potency of biometrics such as facial and voice recognition.

Advantages

- Study proves that lips attributes are usually distinctive and also unchangeable for every single examined person.
- Lips prints used by forensics professionals and criminal police training [8].
- Size of template is small.
- Lips based human recognition dependent on static mouth/face photos.
- Lips biometric certainly are passive biometrics – person's interaction is just not necessary [8].
- Photos might be obtained from the distance without having analyzed person's knowledge.
- 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 [8].

Disadvantages

- The concept of developing hybrid (multimodal) biometric system needs a lot of attention.
- 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.
- A big smile might cause difficulty in recognition of a person with respect to same person with neutral appearance as before.

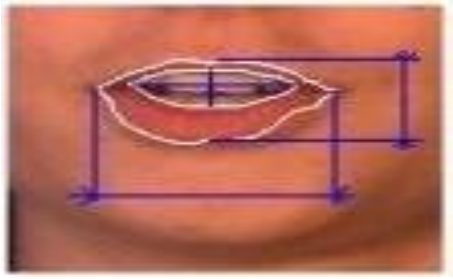


Fig.6 Image sample for Iris Recognition

3. Comparison table of all biometrics

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**
Finger vein	**High**	**Medium**	**Medium**	**High**	**High**
Voice recognition	**Low**	**Medium**	**Small**	**Low**	**Low**
Lip recognition	**Medium**	**medium**	**Small**	**Medium**	**High**

4. Conclusion

This paper presents a shorter introduction on numerous biometric techniques undertaking the comparison examination regarding widely used biometric identifiers and also the identification strategies. As this is a new technology for most of the peoples since it has simply been implemented in public areas for short time period. There are numerous apps along with alternative solutions used in security techniques. It provides benefits that may improve our lives in such a way by increasing security and efficiency, decreasing scams and reducing password administrator cost. Despite the fact the biometrics security systems still have many issues like data privacy, physical privacy, and spiritual arguments etc.

5. Future work

Biometrics technology is used in a number of ways and in different fields of our daily lives. In future we mainly focus on facial expression recognition technology. Using this technology, we can easily identify a person in a crowd and by so we can verify their identity. We can furthermore make use of this technology to detect previously identified terrorists, criminals or scammers in society. It may help us to reduce the criminal offense in the world. But as we can see from the above given comparison between different biometrics, it is clear that face recognition faces a challenging problem in the field of accuracy, effeiciency, speed cost and security. So we need to work upon it to make it more effective.

References

[1] Anil K. Jain, Arun Ross and Salil Prabhakar (2004), "*An Introduction to Biometric Recognition.*"

[2] Alina Klokova, "*Comparison of Various Biometric Methods".*

[3] Rabia Jarfi and Hamid R. Arabina, "A *Survey of Face Recognition Techniques",* Journal of Information Processing Systems, Vol.5, No.2, June 2009.

[4] Joseph N. Pato and Lynette I. Millett, Editors; Whither Biometrics Committee; National Research Council (2010), *"Biometric Recognition: Challenges and Opportunities".*

[5] National Science & Technology Council's (NSTC) Subcommittee on Biometrics (September 2006), "*Biometrics Frequently Asked Questions".*

[6] Michelle C. Frye, B.A. (April 27, 2001), University Thesis, "*The Body as A Password: Considerations, Uses, and Concerns of Biometric Technologies".*

[7] Penny Khaw ; SANS Security Essentials (GSEC) Practical Assignment Version 1.3*," Iris Recognition Technology for Improved Authentication".*

[8] Michal Choras (2009) ," *The lip as a biometric".*

[9] Jim Baumann, "*VoiceRecognition*".

[10] David Weiss (2009), "*Fingerprint Biome*