ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (1-10), Month: January - March 2015, Available at: www.researchpublish.com

Comparative Study of Security Mechanism of Biometric Technologies

[1]R.Vidhya lakshmi, [2]R.Shobana

[1,2] Department of computer science and application, D.K.M College for women, Vellore, India.

***Abstract*: With the increasing concerns for security, automated systems for authorization and authentication have become enormously important in every sector today. The need to secure information, services, and systems has increased. Conventional methods of authentications are knowledge based like passwords and PIN or object based like tokens, ID. Problem with these methods is that passwords can be cracked, ID can be stolen, and PIN can be forgotten. But Biometric systems that are currently available today examine fingerprints, handprints, iris and retina patterns, and face. Biometric cannot be borrowed; stolen, or forgotten and forging one is also very difficult. Biometrics can be categorized as behavioral and physiological. The main aim of this study is to make a comparative study of multimodal biometrics and declare the best effective method of biometrics that offers both security and convenience.**

***Keywords*: biometrics, identification, verification, Applications.**

1. INTRODUCTION

The term biometric comes from the Greek word “bios” (life) and “metrikos” (measure). A biometric system provides an automated method of recognizing an individual based on the individual's biometric characteristics. Traditional means of access control include token based identification systems such as driver’s license, password and knowledge based identification systems such as password, personal identification number. The password and pin is used to give the user a unique access to certain sectors but text password does not ensure the maximum security of the system .The password can be stolen, forgotten and it may be guessed. The solution to this problem is biometric characters which can’t be stolen, forgotten and copied.

2. BIOMETRIC TECHNOLOGY

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database.

2.1 Advantages of biometrics:

Unique: The various biometrics systems have been developed around unique characteristics of individuals. The probability of 2 people sharing the same biometric data is virtually nil.

Cannot be shared: Because a biometric property is an intrinsic property of an individual, it is extremely difficult to duplicate or share

Cannot be copied: Biometric characteristics are nearly impossible to forge or spoof, especially with new technologies ensuring that the biometric being identified is from a live person.

Cannot be lost: A biometric property of an individual can be lost only in case of serious accident.

2.2 Over view of biometric system

There are number of modalities in these categories which can be used according to application. Functionality of biometric system is defined in terms of identification and verification.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (1-10), Month: January - March 2015, Available at: www.researchpublish.com

A) **Classification of biometric modalities**

Physical modalities: This is related to the shape of the body. This includes fingerprint, iris, hand geometry, face, retina, ear shape, DNA etc. recognition system.

Behavioral modalities: These are related to human behavior that may change over time, like signature, typing rhythm etc.

B) **Functionality of biometric system**

Verification: Task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates

Identification: A biometric is collected and compared to all the templates in a database

There are two types of identification

1. Closed set of identification: The person is known to exist in the database

2. Open set of identification: The person is not guaranteed to exit the database

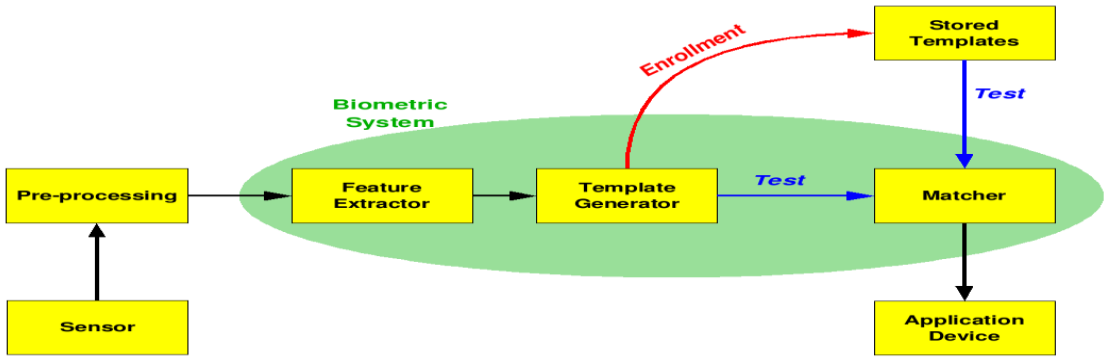


Figure.1: Working of biometric system

3. BIOMETRIC FEATURES USED FOR AUTHENTICATION

As human present biometric data, a number of features extracted from that data are responsible for recognition process. The different biometric consists different biometric features, so this table representing biometrics with its features.

Table1: Biometric samples of biometric modalities

Biometrics	Feature Description
Iris	Texture of the iris such as freckles, coronas, strips, furrow, and crypts
Retinal	Vessel pattern in the retina of the eye as the blood vessels at the back of the eye
Finger Print	A friction Ridge curves-a raised portion, pore structure, indents and marks
Palm Print	Principal lines, wrinkles (secondary lines) and epidermal ridges
Hand Geometry	Estimation of length, width, thickness, shape and surface area of the hand.
Face	Distance of specific facial features (eyes, nose, mouth)
Ear	Dimension of the visible ear
Shape of X-Rayed Teeth	Shape of continuous teeth
DNA	DNA code can be extracted from blood, hair, skin cells and other bodily substances
Voice	Words, tone
Typing Rhythm	Keystroke time interval
Signature	It measures pressure, direction, timing, acceleration and the length of the strokes

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (1-10), Month: January - March 2015, Available at: www.researchpublish.com

4. TYPES OF BIOMETRICS

Iris - An iris-based biometric involves analyzing features found in the colored ring of tissue that surrounds the pupil. This uses a fairly conventional camera element and requires no close contact between the user and the reader. Further, it has the potential for higher than average template-matching performance.

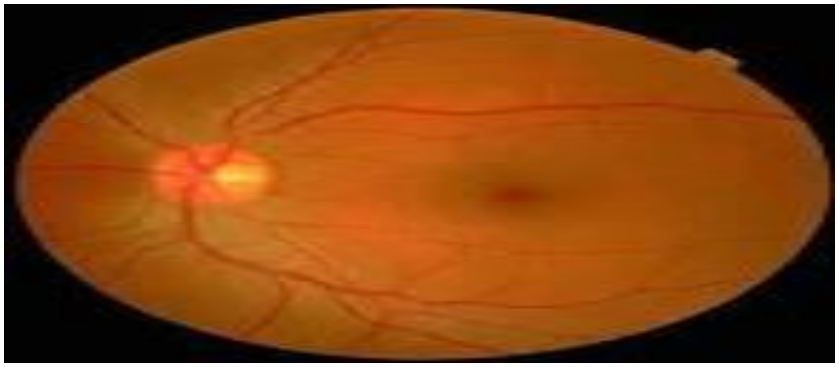
Advantages:

- Highly accurate.1 chances in 1078 that iris pattern of two individual matches
- Highly scalable as iris structure remains same throughout lifetime
- Small template size so fast matching

Problems:

- Iris scanners are relatively expensive
- Scanners can be fooled by high quality image Require cooperation from user

Retina - A retina-based biometric involves analyzing the layer of blood vessels situated at the back of the eye. This technique involves using a low intensity light source through an optical coupler to scan the unique patterns of the retina. Retinal scanning can be quite accurate but does require the user to look into a receptacle and focus on a given point.



Advantages:

- Very high accuracy.
- There is no known way to replicate a retina.
- The eye from a dead person would deteriorate too fast to be useful, so no extra precautions have to been taken with retinal scans to be sure the user is a living human being.

Problems:

- Very intrusive.
- It has the stigma of consumer's thinking it is potentially harmful to the eye.
- Comparisons of template records can take upwards of 10 seconds, depending on the size of the database.
- Very expensive.

Fingerprints - A fingerprint looks at the patterns found on a fingertip. There are a variety of approaches to fingerprint verification, such as traditional police method, using pattern-matching devices, and things like moire fringe patterns and ultrasonic's. This seems to be a very good choice for in-house systems.

Advantages:

- Very high accuracy.
- Is the most economical biometric PC user authentication technique.
- it is one of the most developed biometrics
- Easy to use.
- Small storage space required for the biometric template, reducing the size of the database memory required
- It is standardized.

Problems:

- For some people it is very intrusive, because is still related to criminal identification.
- It can make mistakes with the dryness or dirty of the finger's skin, as well as with the age (is not appropriate with children, because the size of their fingerprint changes quickly).
- Image captured at 500 dots per inch (dpi). Resolution: 8 bits per pixel. A 500 dpi fingerprint image at 8 bits per pixel demands a large memory space, 240 Kbytes approximately → Compression required (a factor of 10 approximately).

DNA recognition - Human DNA is the genetic material that can be found in every single body cell of an individual. There are number of sources from which DNA patterns can be collected such as blood, saliva, nails, hair and others The collected DNA samples are fragmented into shorter fragments which are organized by size and are then compared. Still this technology is not automated and need to be refined.

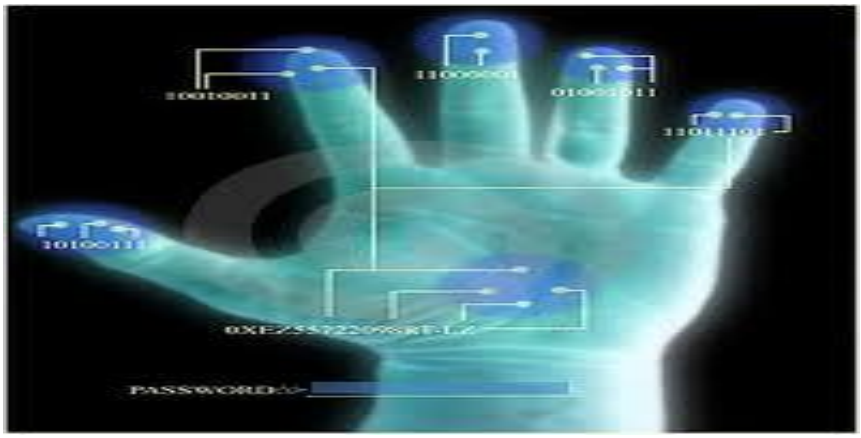
Advantages:

- Very high accuracy.
- It impossible that the system made mistakes.
- It is standardized.

Problems:

- Extremely intrusive.
- Very expensive.

Hand geometry - This involves analyzing and measuring the shape of the hand. It might be suitable where there are more users or where users access the system infrequently. Accuracy can be very high if desired and flexible performance tuning and configuration can accommodate a wide range of applications. Organizations are using hand geometry readers in various scenarios, including time and attendance recording.



Advantages:

- Though it requires special hardware to use, it can be easily integrated into other devices or systems.
- It has no public attitude problems as it is associated most commonly with authorized access.
- The amount of data required to uniquely identify a user in a system is the smallest by far, allowing it to be used with SmartCards easily.

Problems:

- Very expensive
- Considerable size.
- It is not valid for arthritic person, since they cannot put the hand on the scanner properly.

Signature - Signature verification analyses the way user signs his name. Signing features such as speed, velocity, and pressure are as important as the finished signature's static shape. People are used to signatures as a means of transaction-related identity verification.

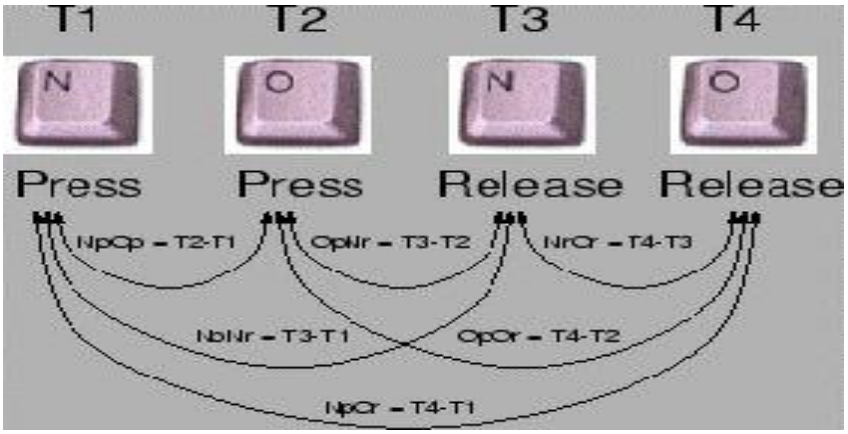
Advantages:

- Non intrusive.
- Little time of verification (about five seconds).
- Cheap technology.

Problems:

- Signature verification is designed to verify subjects based on the traits of their unique signature. As a result, individuals who do not sign their names in a consistent manner may have difficulty enrolling and verifying in signature verification.
- Error rate: 1 in 50.

Keystrokes - It is the way a person types on keyboard. I include speed, how the buttons are pressed and released. It changes from person to person



Advantages:

- Except keyboard no additional hardware required
- Simple to deploy
- No end user training required
- Cost effective

Problems:

- Dynamic changes in timing pattern
- Injury
- Changes in keyboard hardware

Voice - Voice authentication is based on voice-to-print authentication, where complex technology transforms voice into text. Voice biometrics requires a microphone, which is available with PCs nowadays. Voice biometrics is to replace the currently used methods, such as PINs, passwords, or account names. But voice will be a complementary technique for finger-scan technology as many people see finger scanning as a higher authentication form.

Advantages:

- Non intrusive. High social acceptability.
- Verification time is about five seconds.
- Cheap technology.

Problems:

- A person's voice can be easily recorded and used for unauthorised PC or network.
- Low accuracy.
- An illness such as a cold can change a person's voice, making absolute identification difficult or impossible.

5. BIOMETRIC COMPARISON BASED ON VARIOUS ASPECTS

As the aim of this paper is to provide the comparative study about various biometrics, so in this section after studying a number of research papers and articles, I am giving a number of comparison tables based upon various aspects under the heading as biometric features used for authentication, characteristics of biometric entities, social point of view, technical point of view, evaluation point of view and biometric market point of view.

5.1 Characteristics of Biometric Entities:

In table 2, High, Medium, and Low are denoted by H, M and L respectively. We can define first six characteristics as essential characteristic of biometric entities and last four as system dependent characteristic of biometric entities.

Uniqueness: Each individual should have features but different with other. It means distinctive information content.

Permanence: The biometric should be sufficiently invariant over a certain period of time

Universality: The population coverage. Each individual should have the biometric feature.

Measurability: Measurable with simple technical equipments. It means simplicity of extraction.

Comparability: Simplicity of comparison between two templates as one is stored and second one is live template.

Collect ability: How well can the identifiers be captured and quantified

Invasiveness: Introduction of instrument into a body part. For example DNA required blood for testing.

Performance: Accuracy, speed, security.

Acceptability: To which extent society is supporting.

Circumvention: The act of cheating someone

Table 2

	Uniqueness	Permanence	Universality	Measurability	Comparability	Collect ability	Invasiveness	Performance	Acceptability	Circumvention
Iris	H	H	H	M	M	H	M	H	M	L
Retinal	H	H	H	L	M	M	H	H	L	L
Finger Print	H	H	M	H	M	M	M	M	H	M
DNA	H	H	H	L	L	L	H	H	H	L
Hand geometry	M	L	H	H	M	H	M	M	M	M
Signature	H	L	L	M	M	H	M	M	H	H
Voice	L	L	M	M	L	M	L	L	H	H

5.2 Social Point of View:

In table 3, High, Medium, and Low are denoted by H, M and L respectively.

Privacy Concept: Worries that it might lead to remote tracking and one is giving its personal part information to other about some biometric.

Hygiene Factors: Applies to contact technique such as finger print.

Safety Concern: If my car starts only with my finger print, then thieves might chop off my finger. It happens

Cost Factor: The initial investment and operating cost both are important factors. The initial cost includes modifications to existing systems, initial training of operators as well as procuring biometric equipments. The operating cost depends on maintainability and reliability.

Socially Introduced: The year when particular biometric comes into light and used for society.

Popularity: To which extent a society aware about a particular biometric instrument.

Ease of Use: It should be easy to use the device and especially for non habituated applications.

Error of Incidence: Various reason which occur and make sense of error.

Table 3

	Privacy Concept	Hygiene Factors	Safety Concern	Cost	Socially Introduced	Popularity	Ease of Use	Error of Incidence
Iris	H	L	H	H	1995	M	M	Poor lighting, glasses
Retinal	L	L	H	H	1999	L	L	Glasses, contact lens
Finger Print	H	M	M	L	1981	H	H	Dryness, dirt, age, moisture
DNA	L	M	H	H	1965	H	L	Equipments
Hand geometry	L	H	M	H	1986	L	H	Hand injury, age
Signature	H	H	H	M	1970	H	H	Changing signature
Voice	M	L	H	L	1998	H	H	Noise, cold, weather

5.3 Technical Point of View

In table 4, High, Medium, and Low are denoted by H, M and L respectively. Processing Speed: The speed with which two templates can be generated and compared for problems involving identification, because the user's biometric data must be compared to each and every record in the database.

Accuracy: How much accurately our device is working in the given environment.

Template Size: The size of template can impact the cost and performance of a system in several ways. A smaller code will require less system storage space and can be transmitted between sites more quickly than a larger code.

Device Used: It describe about the hardware used by our application and give the answer of many questions as, It is handy or not, bulky in size or small, required operator or not. For example in iris recognition a camera is required.

Technology Used in Device: We have a number of methods to implement our device.

Stability: The time duration to which the biometric data changes over time. For example a person's voice can change due to cold or any other factors.

Table 4

	Processing speed	Accuracy	Template Size	Device Used	Technology used In device	Stability
Iris	M	H	5-50 kb	Camera	CCD/CMOS image sensor	H
Retinal	M	H	-	Retinal scanner	Laser light, IR light	H
Finger Print	H	M	-	Finger print reader	Optical, thermal, silicon or ultrasonic principles	H
DNA	L	H	100kb	Lab environment	Testing in lab	H
Hand geometry	H	M	-	CCD Camera	CCD Camera	M
Signature	H	M	20kb	Tablet, Touch Panel	Capacitive, resistive, acoustic	M
Voice	H	L	-	Keyboard, special Software	Software based	L

6. CONCLUSION

Biometric authentication refers to automated methods of identifying or verifying the identity of a living person in real time based on a physical characteristic or personal trait. The phrase, "living person in real time" is used to distinguish biometric authentication from forensics, which does not involve real-time identification of a living individual. Biometrics is, essentially, based on the development of pattern recognition systems. Today, electronic or optical sensors such as cameras and scanning devices are used to capture images, recordings or measurements of a person's „unique" characteristics. This digital data is then encoded and can be stored and searched on demand, via a computer. Such biometric search is not only very rapid, it is also a process that is accepted globally in establishing forensic evidence in a law court. Consequently, there are numerous forms of biometrics now being built into technology platforms.

REFERENCES

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

[2] James L. Wayman, Anil K. Jain, Davide Maltoni, and Dario Maio, Biometric Systems: Technology, Design and Performance Evaluation, Springer.

[3] K P Tripathi,"Comparative Study of Biometric Technologies with Reference to Human Interface," International Journal of Computer Applications (IJCA), vo.l 14, no.5, 2011.

[4] Jain, A. K.; Ross, A. & Pankanti, S., "Biometrics: A Tool for Information Security," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp 125 – 144, 2006.

[5] S. Z. Li and A. K. Jain, Eds., Handbook of Face Recognition. New York: Springer Verlag, 2004.

[6] L. Hong and A. K. Jain, "Integrating faces and fingerprints for personal identification", IEEE Trans. Pattern Anal. Mach. Intell., Volume 20, No. 12, Dec. 1998, pp. 1295–1307.

[7] R. Sanchez-Reillo, C. Sanchez-Avilla, and A. Gonzalez-Macros, "Biometrics Identification Through Hand Geometry Measurements", IEEE Transactions on Pattern Anakysis and Machine Intelligence, Volume 22,Issue 18, Oct. 2000, pp. 1168-1171.

[8] Arpita Gopal, Chandrani Singh, e-World: Emerging Trends in Information Technology, Excel Publication, New Delhi (2009).

[9] James L. Wayman, Anil K. Jain, Davide Maltoni, and Dario Maio, Biometric Systems: Technology, Design and Performance Evaluation, Springer

ABOUT THE AUTHORS

Prof. Vidhya Lakshmi R is an Assistant Professor in the Department of Computer Science at DKM College for Women. Her special research interests are in software engineering, data mining, VB, Information technology and Networking.

Prof. Shobana R is an Assistant Professor in the Department of Computer Science at DKM College for Women, vellore. Her special research interests are in software engineering, data mining, and programming in c, VB and Digital electronics.