INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

A Study Of Biometrics Security System

Ms. Reetu Awasthi
M.sc.(Comp.SC)
Lecturer, Department of Computer Science, S.F.S College,
Nagpur, Maharashtra, India

Dr. (Mrs) R.A.Ingolikar
M.Sc. (Stat.), M.Phil. (Stat.), M.Sc. (Comp. Sc.)
M.Phil. (Comp. Sc.), P.G.D.C.A. Ph.D (Comp. Sc)
Head, Department of Computer Science, S.F.S College, Nagpur, Maharashtra, India

Abstract:
Security is ubiquitous. Need of security is the basic necessi737ty of any individual or a system. The feeling that you are safe and everything around you is all right is imperative for a peaceful living. But in this unsafe world, when crime, terror and threats are on their peak, how can one attain that sense of security? Cross-border travel, crime and fraud are now easier than ever before. Biometric technology offers a reliable and cost effective way to manage identities for security and authentication purposes.

Biometrics are automated methods of recognizing a person based on a physiological or behavioural characteristic. Among the features measured are; face, Emotion, age, gender, fingerprints, hand geometry, handwriting, iris, retina, vein, signature, DNA and voice. Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The need for biometrics can be found in computer security, federal, state and local governments, in the military, and in commercial applications. Enterprise-wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. Biometric methods can also be multimodal. Biometrics do have pros and cons. They are seductive, unique hard to forge identifiers but, they are not secrets. Some biometrics are easy to steal. However, with few limitations the biometrics technology is currently on a leading edge.

Key words: *Security, Biometrics, Authentication, Unimodal, multimodal, false acceptance system, False Rejection system.*

1.Introduction

With the crime, fraud and threats being central & all pervading, Security is indispensable. “The secret agent places his palm on the grid panel as a thin red scans his entire hand from left to right. A mechanical female voice chimes “Access granted”, as a seamless door opens from the wall. “Biometrics is a technology that has been glorified in movies, television, and comic books as a thing of science fiction and “James Bond” styled security access systems [1]. The origin of the word biometrics come from the Greek word “bios” which means life and “metros”, which means to measure [2]. True to this etymology, biometrics is the identification of an individual based on distinguishing biological traits such as fingerprints, hand geometry, vascular patterns of a person’s palm, retina and iris patterns, voice waves as well as DNA [3].

A Biometric is a unique, measurable characteristics or a trait of a human being for automatically recognizing or verifying Identity. These characteristics of a person include the features like fingerprints, face, hand geometry, voice, and iris biometric features. These features are used to provide an authentication for computer based security systems. The existing computer security systems used at various places like banking, passport, credit cards, smart cards, PIN , access control and network security are using username and passwords for person identification. The username and passwords can be replaced and/or provide double authentication by using any one of the biometric features. The biometric systems offer several advantages over traditional authentication systems. The problem of information security gives the protection of information ensuring only authorized users are able to access the information. They are required the person being authenticated to be present at the point of authentication. Thus biometric-based authentication method is most secure system [4].

But, as we know nothing is perfect. Biometrics Authentication methods have several short comings. The finger print of those people working in Chemical industries are often affected. Therefore these companies should not use the finger print mode of authentication. Similarly, it is found that with age, the voice of a person differs. Also when the person has flu or throat infection the voice changes or if there are too much noise in the environment this method may not authenticate correctly. Therefore this method of verification is not workable all the time. For people affected with diabetes, the eyes get affected resulting in differences. Also, Biometrics is an expensive security solution.

Despite all disadvantages, Biometrics are widely used and in near future will be deployed in some leading edge applications such as:

- Fingerprint scanners (and the necessary software to store and compare fingerprints) have already been installed in laptop computers and PDAs like the iPAQ.
- Sensors installed in automobiles can identify the driver, and adjust mirrors, seat positions and climate controls.
- Special readers can measure various elements of hand geometry, comparing the result with data on file for each person.
- Surveillance cameras can search crowds for missing persons or criminal suspects.
- Face recognition software can be modified to recognize gestures, leading to improved assistive technologies for quadriplegic patients.

2. Biometrics

The last type of authentication, the one relies on measurable physical characteristics that can be automatically checked, and is becoming more popular and demanded. It is called biometrics. Every individual is unique, while the overall human structure is the same; this approach puts biometrics in a great demand in the constantly updating field of security. Though the approach is still in its infancy, many people believe that biometrics will play a critical role in future computers, and especially in electronic commerce.

It seems like every part of a human body was tested to determine if it is produce a unique pattern: face and ear shapes, voice and odour, retina and iris, fingerprints, DNA, gait and veins of a hand. Fig(1) shows the classification of biometric devices. Obviously for convenience reasons, only normally visible parts of a body were implemented; probably users wouldn't want to take the shoes off to measure a toes pattern or the pressure applied while walking. May be someday we will be authenticating people by a heartbeat or a spit out, it all depends on the progress we are making in the field, the demand of different identifiers and hackers success in reproducing characteristics.[5]

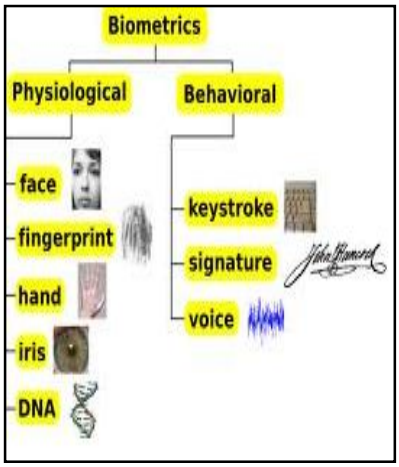


Figure 1: Classification of Biometrics

2.1.Unimodal Biometrics

Most biometric systems deployed in real-world applications are unimodal, i.e., they rely on the evidence of a single source of information for authentication (e.g., single fingerprint *or* face). Fig.2 shows a Traditional Unimodal Biometric system. These systems have to contend with a variety of problems such as:

2.1.1.Noise In Sensed Data

A fingerprint image with a scar, or a voice sample altered by cold are examples of noisy data. Noisy data could also result from defective or improperly maintained sensors (e.g., accumulation of dirt on a fingerprint sensor) or unfavourable ambient conditions (e.g., poor illumination of a user's face in a face recognition system).

2.1.2.Intra-Class Variations

These variations are typically caused by a user who is incorrectly interacting with the sensor (e.g., incorrect facial pose), or when the characteristics of a sensor are modified during authentication (e.g., optical versus solid-state fingerprint sensors).

2.1.3.Inter-Class Similarities

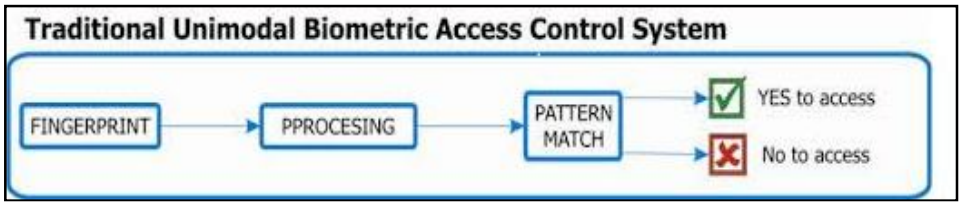
In a biometric system comprising of a large number of users, there may be inter-class similarities (overlap) in the feature space of multiple users. #

2.1.4.Non-universality

The biometric system may not be able to acquire meaningful biometric data from a subset of users. A fingerprint biometric system, for example, may extract incorrect minutiae features from the fingerprints of certain individuals, due to the poor quality of the ridges.

2.1.5. Spoof Attacks

This type of attack is especially relevant when behavioural traits such as signature or voice are used. However, physical traits such as fingerprints are also susceptible to spoof attacks. [6]



Figurer 2: Traditional Unimodal Biometric Access control system

2.2.Multimodal Biometrics

The limitations imposed by unimodal biometric systems are that they lead to considerably high false acceptance rate (FAR) and false rejection rate (FRR), limited discrimination capability, upper bound in performance and lack of permanence .Therefore, to overcome these limitations multiple sources of information for establishing identity are included. These systems allow the integration of two or more types of biometric systems known as multimodal biometric systems. Fig.3, depicts a multimodal biometric system. These systems are more reliable due to the presence of multiple, independent biometrics .The term “multimodal” is used to combine two or more different biometric sources of a person (like face and fingerprint) sensed by different sensors. Two different properties (like infrared and reflected light of the same biometric source, 3D shape and reflected light of the same source sensed by the same sensor) of the same biometric can also be combined. In orthogonal multimodal biometrics, different biometrics (like face and fingerprint) are involved with little or no interaction between the individual biometric whereas independent multimodal biometrics processes individual biometric independently [7].

Multimodal biometric systems are those that utilize more than one physiological or behavioural characteristic for enrolment, verification, or identification. In applications such as border entry/exit, access control, civil identification, and network security, multi-modal biometric systems are looked to as a means of

- Reducing false non-match and false match rates,
- Providing a secondary means of enrolment, verification, and identification if sufficient data cannot be acquired from a given biometric sample, and
- Combating attempts to fool biometric systems through fraudulent data sources such as fake fingers.

  A multimodal biometric verification system can be considered as a classical information fusion problem i.e. can be thought to combine evidence provided by different biometrics to improve the overall decision accuracy. Generally, multiple evidences can be integrated at one of the following three levels.
- Abstract level: The output from each module is only a set of possible labels without any confidence value associated with the labels; in this case a simple majority rule may be used to reach a more reliable decision.
- Rank level: The output from each module is a set of possible labels ranked by decreasing confidence values, but the confidence values themselves are not specified.
- Measurement level: The output from each module is a set of possible labels with associated confidence values; in this case, more accurate decisions can be made by integrating different confidence values.

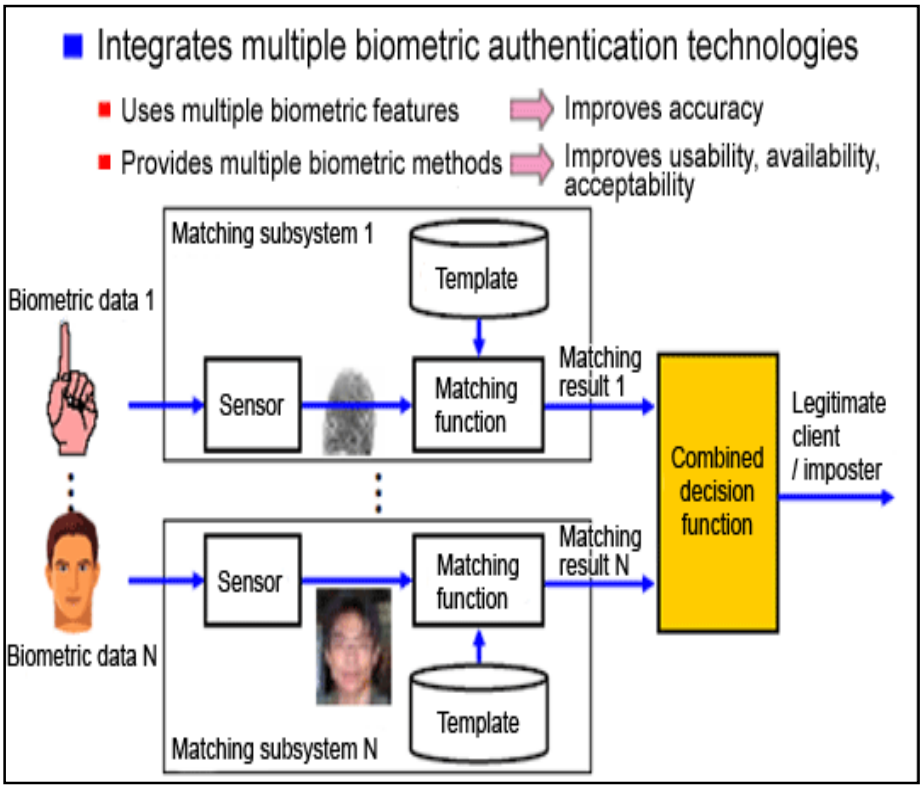


Figure 3: Multimodal Biometric System

2.2.Characteristics Of Biometrics

A number of biometric characteristics may be captured in the first phase of processing. However, automated capturing and automated comparison with previously stored data requires that the biometric characteristics satisfy the following characteristics:

- Universal: Every person must possess the characteristic/attribute. The attribute must be one that is universal and seldom lost to accident or disease.
- Invariance of properties: They should be constant over a long period of time. The attribute should not be subject to significant differences based on age either episodic or chronic disease.
- Measurability: The properties should be suitable for capture without waiting time and must be easy to gather the attribute data passively.
- Singularity: Each expression of the attribute must be unique to the individual. The characteristics should have sufficient unique properties to distinguish one person from any other. Height, weight, hair and eye colour are all attributes that are unique assuming a particularly precise measure, but do not offer enough points of differentiation to be useful for more than categorizing.

- Acceptance: The capturing should be possible in a way acceptable to a large percentage of the population. Excluded are particularly invasive technologies, i.e. technologies which require a part of the human body to be taken or which (apparently) impair the human body.
- Reducibility: The captured data should be capable of being reduced to a file which is easy to handle.
- Reliability and tamper-resistance: The attribute should be impractical to mask or manipulate. The process should ensure high reliability and reproducibility.
- Privacy: The process should not violate the privacy of the person.
- Comparable: Should be able to reduce the attribute to a state that makes it digitally comparable to others. The less probabilistic the matching involved, the more authoritative the identification.
- Inimitable: The attribute must be irreproducible by other means. The less reproducible the attribute, the more likely it will be authoritative.

Among the various biometric technologies being considered, the attributes which satisfy the above requirements are fingerprint, facial features, hand geometry, voice, iris, retina, vein patterns, palm print, DNA, keystroke dynamics, ear shape, odour, signature etc.

2.3 Types Of Biometrics

The different category of biometrics in use today are discussed in this section [8].

2.3.1 EYE

There are two main types of biometric analysis of the eye. One involves the iris, which is the coloured ring that surrounds the pupil, and the other uses the retina, which is the layer of blood vessels at the back of the eye. Fig.4, Shows a biometric image of an eye.

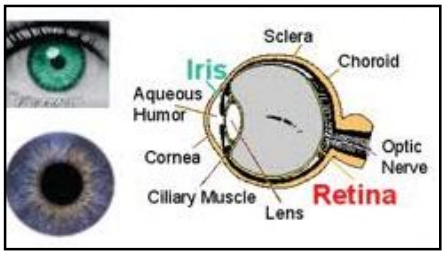


Figure 4: Eye Biometrics

2.3.1.1..Iris

Each iris has a unique pattern such that even a person's right and left iris patterns are completely different. It has been claimed that the system is "fool proof" [12] because artificial duplication of the Iris is virtually impossible due to its properties and number of measurable characteristics. The Iris is stable throughout one's life and is not susceptible to wear and injury. Contact lenses do not interfere with the use of this biometric identifier. Iris recognition technology involves use of a camera to capture a digital image of the eye from which data are extracted.

2.3.1.2.Retina

As with the iris, the retina forms a unique pattern that begins to decay quickly after death. Unauthorized access to a retinal system is reported to be virtually impossible.

A precise enrolment procedure is necessary. A user must focus on a specific point and then the system uses a beam of light to capture the unique retinal characteristics. The limitation of this approach is people's reluctant to have light shone into their eyes to gather information [13]. Retinal Biometrics usually are found in high security applications where inconvenience and user comfort are not important considerations.

2.3.2.Face

There are two main types of facial recognition systems: the most common uses video, while the other uses thermal imaging.

Video face recognition technology analyse the unique shape, pattern and positioning of facial features. A video camera is used to capture an image from a distance of a few feet away from the user. A number of points on the face (e.g. position of eyes, mouth and nostrils) are usually mapped out. With other system, athree-dimensional map of the face can be created. Face recognition systems are designed to compensate for expression, glasses, hats and beards [14]. Fig.5, depicts the facial biometric system.

A facial thermo gram uses an infrared camera to scan a person's face and then digitize the thermal patterns [15]. Apparently no two people, not even identical twins, have the same facial thermo gram.

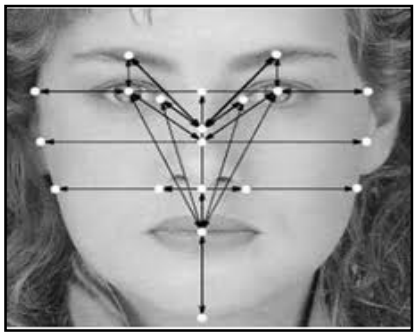


Figure 5: Face Recognition

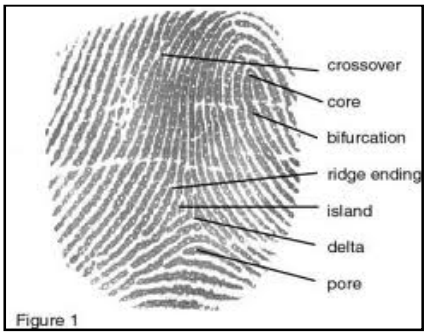


Figure 6: Fingerprint

2.3.3.Finger Scanning

The use of fingerprints by law enforcement for identification purpose is common and widely accepted. However, the technology has diversified, migrating away from law enforcement towards civil and commercial markets. In the context of commercial applications, the preferred term is “finger scanning”, which is the process of finger image capture [16]. Fig.6, shows a typical image of a biometric finger.

There are a number of different types of finger scanning systems in the market. Some analyse the distinct marks on the finger called “minutiae” points. Others examine the pores on the finger that are uniquely positioned. Finger image destiny or the distance between ridges also may be analysed. The way in which the image is captured also differs among vendors.

Finger scanning can be used for both verification and recognition purposes.

2.3.4.Hand Geometry

This technique uses a three-dimensional image of the hand and measures the shape, width and length of fingers and Knuckles.Fig.7, shows a hand geometry Biometric. A

user places a designated hand on a reader, aligning fingers with specific positioned guides. A camera is used to capture both a top view, which gives length and width information, and a side view which gives a thickness profile.

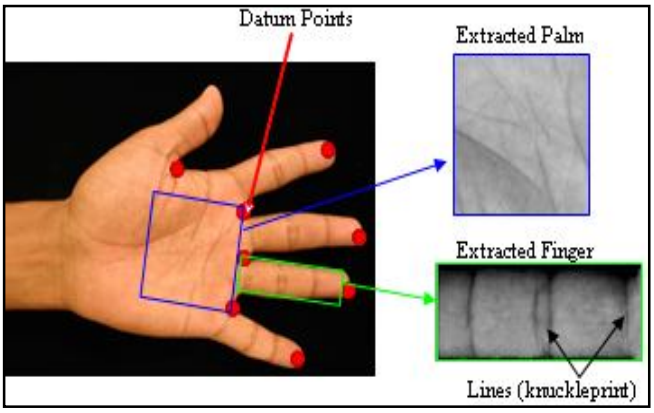


Figure 7: Hand Geometry

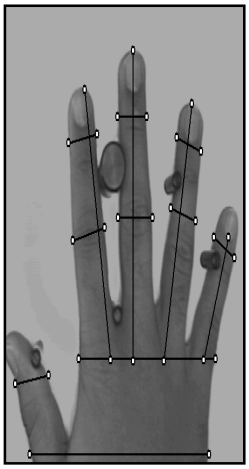


Figure 8: Finger Geometry

Hand Geometry is predominantly used for one-to-one verification. It is one of the most established biometrics in commercial use today. Applications continue to grow because it is easy to use, convenient and very fast.

2.3.5.Finger Geometry

This technology operates on similar principles and hand geometry, but utilizes one or fingers.Fig.8, depicts a finger geometry image. Measurements of unique finger characteristics, such as width, length, thickness and knuckle size are taken.

Finger geometry systems can perform one-to-one identification. The main advantage is that these systems are fast and designed to accommodate "a high throughput of users" [18]. According to one company, its system confirms identity within one second [19].The systems confirms identity approximately within one second. Finger geometry systems are considered very durable and able to cope well with external conditions[20].

2.3.6.Signature Verification

This behavioural biometric involves the analysis of the way in which a person signs their name. Signature biometrics are often referred to as dynamic signature verification (DSV). A typical Signature Biometric system is depicted in Fig.9. With this technique, the manner in which someone signs is as important as the static shape of their finished signature. For example, the angle at which pen is held, the time taken to sign, the velocity and acceleration of the signature, the pressure exerted and the number of times the pen is lifted from the paper, all can be measured and analysed as unique behavioural characteristics. As DSV is not based on a static image, forgery is considered to be difficult.

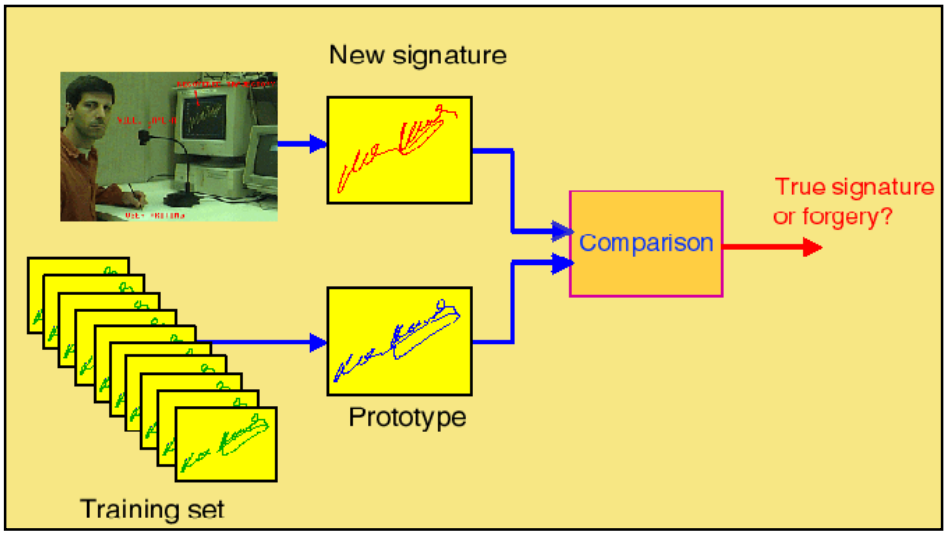


Figure 9: Signature Biometric system

Signature data can be captured via special pen or tablet, or both. The pen-based method incorporates sensors inside the wiring instrument, while the tablet method relies on sensors embedded in a writing surface to detect the unique signature characteristics.

2.3.7.Speaker Verification

Speech related computer software recognize words as they are spoken. Biometric systems involve the verification of the speaker's identity based on numerous characteristics, such as cadence, pitch, and tone. Speaker Verification is considered a hybrid behavioural and physiological biometric because the voice pattern is determined, to a large degree, by the physical shape of the throat and larynx, although it can be altered by the user.

The technology is easy to use and does not require a great deal of user education. However, background noise greatly affects how well the system operates. Speaker verification works with a microphone or with a regular telephone handset. It is well suited to telephone-based applications where identity has to be verified remotely [21].

2.3.8.Keystroke Dynamics

Typing biometrics are more commonly referred to as keystroke dynamics. Verification is based on the concept that how a person types, in particular their rhythm, is distinctive. Keystroke dynamics are behavioural and evolve over time as users learn to type and develop their unique typing pattern.

2.3.9.Palm Print

This is a physical biometric that analyses the unique patterns on the palm of a person's hand, similar to fingerprinting [22].

2.3.10.Vein Patterns

This physical biometric analyses the patterns of veins in the back of person's hand. One proprietary system focuses on the unique pattern of blood vessels that form when a fist is made. The underlying vein structure, or "vein tree" can be captured using a camera and infrared light [23].

Figure 10: Vein Patterns

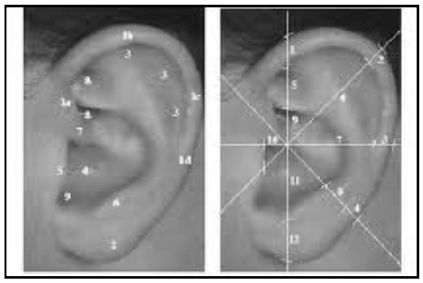


Figure 11: Ear Shape

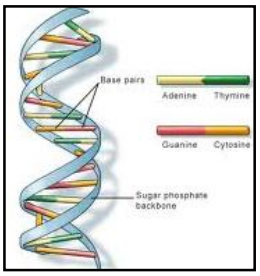


Figure 12: DNA

2.3.11.Ear Shape

Another physical biometric is the shape of the outer ear, lobes and bone structure [24]. Apparently, police are able to capture ear prints of criminals left when they listen at windows and doors. A typical ear shape Biometric is depicted in figure.11.

2.3.12.Body Odour

The physical biometric which analyses human body smell. Sensors are capable of capturing body odour from non-intrusive parts of the body such as the back of the hand. Each unique human smell is made up of chemicals which are extracted by the system and converted into a template [25].

2.3.13 Gait

It is a behavioural Biometric .An individuals walking style or gait is used to determine identity.

2.3.14.DNA

DNA is an abbreviation of deoxyribonucleic acid. Deoxyribonucleic acid (DNA) provides the most reliable personal identification. It is intrinsically digital, and does not

change during a person's life or after his/her death.. Fig. 12, shows an biometric image of DNA.

2.4.How Biometrics System Work

Simply stated, biometrics is the automated identification or verification of human identity through measurable physiological and behavioural traits. Although it must be acknowledged that there are many variations in how specific products and system work, there are a number of common processing elements. Fig 13, Depicts the casual working of a biometric system.

2.4.1.Collection

As a first step, a system must collect or "capture" the biometric to be used. One essential difference between the various techniques is the characteristic (i.e., body part or function being analysed. Obviously, this will influence the method of capture.

All biometric systems have some sort of collection mechanism. This could be reader or sensor upon which a person places their finger or hand, a camera that takes a picture of their face or eye, or software that captures the rhythm and speed of typing.

In order to "enrol" in a system, an individual presents their "live" biometric a number of times so the system can build a composition or profile of their characteristics, allowing for slight variations (e.g., different degrees of pressure when they place their finger on the reader). Depending upon the purpose of the system, enrolment could also involve the collection of other personally identifiable information.

2.4.2.Extraction

Commercially available biometric devices generally do not record full images of biometrics the way law enforcement agencies collect actual fingerprints. Instead, specific features of the biometric are "extracted". Only certain attributes are collected (e.g., particular measurements of a fingerprint or pressure points of a signature). Which parts are used is dependent upon the type of biometric, as well as the design of the proprietary system.

This extracted information, sometimes called "raw data", is converted into a mathematical code. Again, exactly how this is done varies amongst the different proprietary systems. This code is then stored as a "sample" or "template". The specific configuration of a system will dictate what, how, and where that information is stored.

Regardless of the variations, all biometric systems must create and retain a template of the biometric in order to recognize or verify the individual.

While the raw data can be translated into a set of numbers for the template, commercial biometric systems are generally designed so that the code cannot be re-engineered or translated back into the extracted data or biometric.

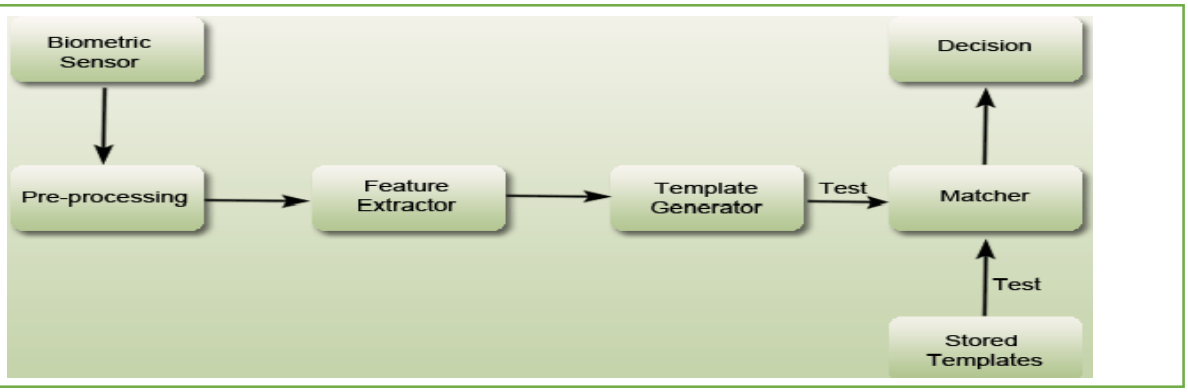


Figure 13: Working of a biometric system

2.4.3.Comparison And Matching

To use a biometric system, the specific features of a person's biometric characteristic are measured and captured each time they present their "live" biometric. This extracted information is translated into a mathematical code using the same method that created the template. The new code created from the live scan is compared against a central database of templates in the case of a one-to-many match, or to a single stored template in the case of one-to-one match. If it falls within ascertain statistical range of values, the match is considered to be valid by system.[17]

2.5.Advantages Of Biometrics

The benefits of a biometrics system as previously stated are that it is unique to each individual user. Biometrics is unique to each individual, thus creating a "personalized key" for each user. It also reduces the need to remember passwords and PIN numbers. This is very convenient, especially for those who are handicapped and the elderly, who may have complications reading and accessing the system(s) through conventional interfaces [3].

The primary advantage of biometric authentication methods over other methods of user authentication is that they really do what they should, i.e., they authenticate the user.

These methods use real human physiological or behavioural characteristics to authenticate users. These biometric characteristics are (more or less) permanent and not changeable. It is also not easy (although in some cases not principally impossible) to change one's fingerprint, iris or other biometric characteristics. Users cannot pass their biometric characteristics to other users as easily as they do with their cards or passwords. Biometric objects cannot be stolen as tokens, keys, cards or other objects used for the traditional user authentication, yet biometric characteristics can be stolen from computer systems and networks. Biometric characteristics are not secret and therefore the availability of a user's

Fingerprint or iris pattern does not break security the same way as availability of the user's password. Even the use of dead or artificial biometric characteristics should not let the attacker in.

Most biometric techniques are based on something that cannot be lost or forgotten. This is an advantage for users as well as for system administrators because the problems and costs associated with lost, reissued or temporarily issued tokens/cards/passwords can be avoided, thus saving some costs of the system management. Another advantage of biometric authentication systems is their speed [9].

2.6.Disadvantages Of Biometrics

Biometrics authentication methods also have their own shortcomings. The performance of biometric systems is not ideal. Biometric systems still need to be improved in the terms of accuracy and speed. Biometric systems with the false rejection rate under 1% (together with a reasonably low false acceptance rate) are still rare today. Although few biometric systems are fast and accurate (in terms of low false acceptance rate) enough to allow identification (automatically recognising the user identity), most of current systems are suitable for the verification only, as the false acceptance rate is too high [10].

Another Disadvantage is the Fail to Enrol Rate. Not all users can use any given biometric system. People without hands cannot use fingerprint or hand-based systems [11]. Visually impaired people have difficulties using iris or retina based techniques. As not all users are able to use a specific biometric system, the authentication system must be extended to handle users falling into the FTE category. This can make the resulting system more complicated, less secure or more expensive. Even enrolled users can have difficulties using a biometric system.

Some biometric sensors (particularly those having contact with users) also have a limited lifetime. While a magnetic card reader may be used for years (or even decades), the optical fingerprint reader (if heavily used) must be regularly cleaned and even then the lifetime need not exceed one year.

Biometric systems may violate user's privacy. Biometric characteristics are sensitive data that may contain a lot of personal information. The DNA (being the typical example) contains (among others) the user's preposition to diseases. This may be a very interesting piece of information for an insurance company. The body odour can provide information about user's recent activities. It is also told that people with asymmetric fingerprints are more likely to be homosexually oriented, etc. [9].

2.7.Pros And Cons Of Various Biometric Features

The pros and cons associated with specific biometrics are highlighted below:

Biometric Feature	**Advantages**	**Disadvantages**
Facial recognition:	a. Non-intrusive b. Cheap technology.	a. 2D recognition is affected by changes in lighting, the person's hair, the age, and if the person wear glasses. b. Requires camera equipment for user identification; thus, it is not likely to become popular until most PCs include cameras as standard equipment.
Voice recognition:	a. Non-intrusive. High social acceptability. b. Verification time is about five seconds. c. Cheap technology.	a. A person's voice can be easily recorded and used for unauthorised PC or network. b. Low accuracy. c. An illness such as a cold can change a person's voice, making absolute identification difficult or impossible.
Signature recognition:	a. Non-intrusive. b. Little time of verification (about five seconds). c. Cheap technology.	a. 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. b. Error rate: 1 in 50.

DNA:	a. Very high accuracy. b. It impossible that the system made mistakes. c. It is standardized	a. Extremely intrusive. b. Very expensive.
Retinal scanning:	a. Very high accuracy. b. There is no known way to replicate a retina. c. 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.	a. Very intrusive. b. It has the stigma of consumer's thinking it is potentially harmful to the eye. c. Comparisons of template records can take upwards of 10 seconds, depending on the size of the database. d. Very expensive.
Iris recognition:	a. Very high accuracy. b. Verification time is generally less than 5 seconds. c. 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.	a. Intrusive. b. A lot of memory for the data to be stored. c. Very expensive
Fingerprint:	a. Very high accuracy. b. Is the most economical biometric PC user authentication technique. c. it is one of the most	a. For some people it is very intrusive, because is still related to criminal identification. b. It can make mistakes

	developed biometrics d. Easy to use. e. Small storage space required for the biometric template, reducing the size of the database memory required f. It is standardized.	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). c. 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).
Hand Geometry:	a. Though it requires special hardware to use, it can be easily integrated into other devices or systems. b. It has no public attitude problems as it is associated most commonly with authorized access. c. The amount of data required to uniquely identify a user in a system is the smallest by far.	a. Very expensive b. Considerable size. c. It is not valid for arthritic person, since they cannot put the hand on the scanner properly.

Table 1

2.8 .Application Of Biometrics

The application of biometrics can be divided into the following three main groups.

- Commercial applications such as computer network login, electronic data security, e-commerce, Internet Access, ATM, Credit card, Physical access control, Cellular phone, PDA, Medical records management and distance learning.
- Government applications such as national ID card, correctional facility, driver's license, social security, welfare disbursement, border control and passport control.
- Forensic applications such as corpse identification, criminal investigation, terrorist identification, parenthood determination, and missing children.

Note: There are two kinds of errors that biometric systems do: false rejection occurs when a legitimate user is rejected and false acceptance occurs when an impostor is accepted as a legitimate user.

3.Reference

1. Bjorn, V.. (2009, April). One Finger at a Time: Best Practices for Biometric Security. Hoosier Banker, 93(4), 34-36. Retrieved February 8, 2012, from Banking Information Source. (Document ID: 1697301411).
2. Pocovnicu, A.. (2009). Biometric Security for Cell Phones. Informatica Economica, 13(1), 57-63. Retrieved February 8, 2012, from ABI/INFORM Global. (Document ID: 1912951021).
3. Anonymous, . Institutions Adopt Biometric atms Around the Globe. (2012, January). Teller Vision,(1413), 2-3. Retrieved February 8, 2012, from Banking Information Source. (Document ID: 2552867651).
4. [1]Sulochana Sonkamble, [2]Dr. Ravindra Thool, [3]Balwant Sonkamble, "Survey of Biometric Recognition Systems And their applications", Journal of Theoretical and Applied Information technology © 2005 - 2010 jatit.
5. Nataliya B. Sukhai, "Access Control & Biometrics", infoseccd Conference'04, October 8, 2004, Kennesaw, GA, USA.
6. Arun Ross and Anil K. Jain, "MULTIMODAL BIOMETRICS: AN OVERVIEW", 12th European Signal Processing Conference (EUSIPCO), (Viena, Austria), pp. 1221-1224, September 2004.
7. Prof. Vijay M. Mane, Prof. (Dr.) Dattatray V. Jadhav , "Review of Multimodal Biometrics: Applications, challenges and Research Areas", International Journal of Biometrics and Bioinformatics (IJBB), Volume 3, Issue 5.
8. Ann Cavoukain, Ph.D.Information and Privacy Commisioner/Ontario. September 1999.
9. V´aclav Maty´aˇs and Zdenˇek ˇR´ıha, BIOMETRIC AUTHENTICATION — SECURITY AND USABILITY
10. Department of Defense (1985). Trusted Computer System Evaluation Criteria.
11. [11] Jain, A., Bolle, R. and Pankanti S. (1999). BIOMETRICS: Personal Identification in Networked Society. Kluwer Academic Publishers.
12. Guy Gugliotta, "Bar Codes for the body make it to the market: Biometrics may alter Consumer Landscape," Washington Post, June 21, 1999, p. A1, http://www.washingtonpost.com/wp-adv/front.htm,9/7/99.
13. Robert McKnight, "The second coming of biometrics," Canadian security, April/May 1998, p.37.

14. International Biometric Group, "Overview of Biometrics – Face Geometry," http://www.biometricgroup.com,8/13/99.
15. Association for Biometrics and International Computer Security Association,"1998 Glossary of Biometric Terms," as cited in Roethenbaugh, "ICSA Biometric Buyer's Guide," Appendix I, <http://www.iCSA.net/services/consortia/cbdc/bg/app1_glossary.shtml>,8/13/99.
16. Association for Biometrics and International Computer Security Association, "1988 Glossary of Biometric Terms."
17. Corien Prins, "Biometric Technology Law: Making our body identify for us: Legal implications of bioetric technology,"Computer Law & Security Report, Vol. 14, No.3,1998,p.160.
18. Roethenbaugh, "Biometrics Explaines," section 3-Technology Overview.
19. BioMetPartners, Inc., "New 3D Finger Geometry Biometrics For OEM's and Systems Integrators, "Press Release, January 15, 1999, <http:www.bionet.ch/press.htm>,5/5/99.
20. Roethenbaugh, "ICSA Biometrics Buyer's Guide," chapter 4-Types of Biometric, http://www.iCSA.net/services/consortia/cbdc/bg/chap4.shtml, 12/29/99.
21. Roethenbaugh, "ICSA Biometrics Buyer's Guide," chapter 4-Types of Biometrics.
22. Roethenbaugh, "Biometrics Explaines," section 3-Technology Overview.
23. Roethenbaugh, section 3-Technology Overview.
24. Association for Biometrics and International Computer Security Association,"1998 Glossary of Biometric Terms."
25. Roethenbaugh, "Biometrics Explaines," section 3-Technology Overview.