International Journal of Research in Engineering, Science and Management
Volume-2, Issue-10, October-2019
www.ijresm.com | ISSN (Online): 2581-5792

Analyzing: Approaches of Pattern Recognition in Biometrics Field

Nidhi
Assistant Professor, Department of Computer Science, Dasmesh Girls College, Mukerian, India

***Abstract*: Pattern Recognition is a mature but exciting and fast developing field. It is an ambitious endeavor of mechanization of the most fundamental function of cognition, which underpins developments in cognate fields such as Biometrics. Many Biometric Methods are closely connected with methods of Pattern Recognition and Image Analysis. Biometrics verifies individuals based on who they are i.e. the characteristics inherent to the individuals. These characteristics (also known as modalities) uniquely identify individuals from an entire population based on their intrinsic physical or behavioral traits. This paper is going to presents a comprehensive view of different Biometric features and their usage along with the comparisons of different biometrics.**

***Keywords*: biometric, fingernail bed, human scent recognition, iris, pattern recognition, skin spectroscopy, thermo grams, vein pattern.**

1. Introduction

Pattern Recognition: It is a study of ideas and algorithms that provide computers with a perceptual capability to put abstract objects, or patterns into categories in a simple and reliable way. The field of Pattern Recognition is concerned with the automatic discovery of regularities in data through the use of computer algorithms and with the use of these regularities to take actions such as classifying the data into different categories. Itis the study of how machines can:

1. Observe the environment.
2. Learn to distinguish patterns of interest.
3. Make sound and reasonable decisions about the categories of the patterns.

A pattern is a set of objects or phenomena or concepts where the elements of the set are similar to one another in certain ways or aspects. A pattern is an entity that could be given a name. Example: Fingerprint Image, handwritten word, human face, speech signal, DNA sequence etc.

A. Pattern Recognition System

Pattern recognition is the procedure of processing and analyzing diverse information (numerical, literal, logical) characterizing the objects or phenomenon, so as to provide descriptions, identifications, classifications and interpretations for them.

"Perceive + Process + Prediction" – It is the study of how machine can,

a) *Perceive:* Observe the environment (i.e. Interact with the real –world).
b) *Process:* Learn to distinguish patterns of interest from their background.
c) *Prediction:* Make sound and reasonable decision s about the categories of the pattern.

B. Design model of a pattern recognition system essentially involves the following 4 steps

1) Data acquisition and pre-processing
2) Data Representation
3) Feature extraction
4) Decision making

1) Data acquisition and sensing
Measurements of physical variables, bandwidth, resolution etc.

2) Pre-processing
Removal of noise in data and Isolation of patterns of interest from the background.

3) Feature extraction
Finding a new representation in terms of features. Classification as well as using features and learned models to assign a pattern to a category.

4) Data acquisition and sensing
Evaluation of confidence in decisions.

2. Biometrics

The term Biometrics is composed of two words – *Bio* (Greek word for Life) and *Metrics* (Measurements). Biometrics is a branch of information technology that aims towards establishing one's identity based on personal traits. Biometrics is presently a buzzword in the domain of information security as it provides high degree of accuracy in identifying an individual. Personal identification systems that use biometrics are very important for security applications in airports, ATMs, shops, hotels, and secure computer access. Recognition can be based on face, fingerprint, iris, or voice, and can be combined with the automatic verification of signatures and PIN codes.

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.

3. Need of Biometrics

In an increasingly digital word, protecting confidential information is becoming more difficult. Traditional passwords and keys no longer provide enough security to ensure that data is kept out of the hands of hackers and unauthorized individuals. Additionally, with more devices and platforms connected to the Internet of Things, the need for ironclad security is paramount. This is where biometric security can transform the technology sector. Where passwords and physical tokens have fallen short, biometric authentication can succeed. Biometric Authentication is an effective way to prove identity because it can't be replicated. Companies today are also realizing the benefits of Biometric Devices for protecting server rooms, work computers and other business assets. In a corporate environment, organizations need to make sure that unauthorized individuals are not allowed into secure systems. Unlike passwords, which can be borrowed and passed along between coworkers, fingerprints scanners will only allow access to the person whose print is required.

4. Basic characteristics of Biometric Technologies

A. *Universality*

Every person should have the characteristic. Biometric trait must be universal. Means every person should posses that biometric trait.

B. *Uniqueness*

Generally, no two people have identical characteristics. However, identical twins are hard to distinguish.

C. *Permanence*

The characteristics should not vary with time. A person's face, for example, may change with age.

D. *Collectability*

The characteristics must be easily collectible and measurable. It should be possible to acquire and digitize the biometric trait using suitable devices.

E. *Performance*

The method must deliver accurate results under varied environmental circumstances. Accuracy should meet the constraints imposed by the application.

F. *Acceptability*

The general public must accept the sample collection routines. Nonintrusive methods are more acceptable.

G. *Circumvention*

The technology should be difficult to deceive. This refers to the ease with which the trait of an individual can be imitated using artifacts (e.g. fake fingers), in the case of behavioral traits.

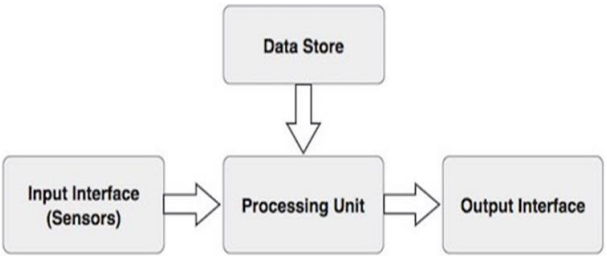

Fig. 1. Basic components of a biometric system

5. Various Biometric Systems

A. *Finger print identification*

The fingerprint recognition technique is a dominant technology in the biometric market. A number of recognition methods have been used to perform fingerprint matching out of which pattern recognition approaches is widely used. Every person in the world possesses a unique set of fingerprints. However, the differences between some can be very subtle. By studying the arrangement, shape, size, and number of lines in each fingerprint, experts have been able to classify them into unique patterns, which are used for identification.

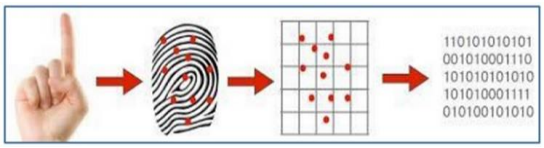

Fig. 2. Finger print identification

For fingerprint Recognition look at: Friction, ridges, crossover, delta, island, ridge ending, and pore.

- The systems are working on the fingerprint recognition technology stores the unique ridge pattern of the fingertips of the people. Many different techniques like optical, capacitive, thermal, etc. are used to collect the fingertips pattern.
- The captured image of the human fingerprint is enriched to make it functional, and then a biometric template is produced using various sophisticated algorithms, that are always unique for an individual.
- When any identity data of an individual is associated with this template, it becomes biometric fingerprint identity. This template is matched against the existing scans, and the biometric system returns a true if it gets a match or returns false if there is no match, as the case may be.
- All the process described above is just a touch away at the user level, and everything else goes underneath a fingerprint recognition system.

Drawbacks: Fingerprints can already be spoofed using relatively accessible technology. One can easily cheat this System by making Artifacts like Wax finger. In addition, some

line patterns are so similar that in practice this can result in a high false acceptance rate. Fingerprints can also wear away as you get older, if you do a lot of DIY or a particular kind of work, for example. As a result, some people may find that their fingerprints cannot be recognized (false rejection) or even recorded. There is even a hereditary disorder that results in people being born without fingerprints.

B. *Facial Recognition*

Software reads the geometry of your face. Key factors include the distance between your eyes and the distance from forehead to chin. The software identifies facial landmarks — one system identifies 68 of them — that are key to distinguishing your face. The result: your facial signature.

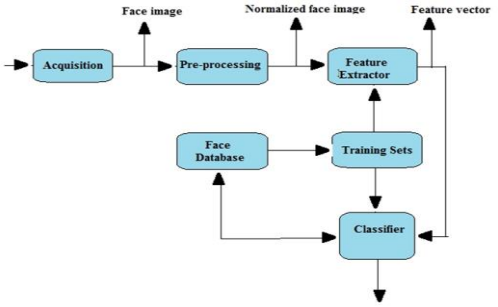

Fig. 3. Facial recognition process

Drawback: However, facial recognition also has a number of significant drawbacks. For example, the technology focuses mainly on the face itself, i.e. from the hairline down. As a result, a person usually has to be looking straight at the camera to make recognition possible. And even though the technology is still developing at a rapid pace, the level of security it currently offers does not yet rival that of iris scanning or vein pattern recognition.

C. *Retinal Scan*

It's a biometric technique that analyses unique patterns on an individual's retina blood vessels. In this method, a beam of infrared light is cast into the person's eye when he looks through the scanner. As the retinal blood vessels readily absorb light, the amount of reflection varies. It is then digitized and stored in the database. Retinal scans map the unique patterns of a person's retina. The blood vessels within the retina absorb light more readily than the surrounding tissue and are easily identified with appropriate lighting. A retinal scan is performed by casting an unperceived beam of low-energy infrared light into a person's eye as they look through the scanner's eyepiece. This beam of light traces a standardized path on the retina.

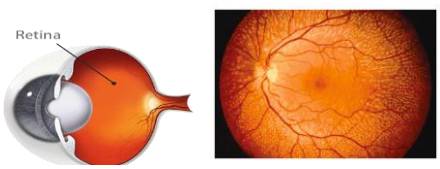

Fig. 4. Retinal scan

Drawback: It is Not very user friendly because Subject should be very close to the camera and Diseases such as cataracts, glaucoma, diabetes etc., affect the accuracy of the results.

D. *Iris Recognition*

In this method of biometric identification, mathematical pattern-recognition techniques are used on the video images of the individual's irises. It utilizes video camera technology with subtle near-infrared illumination to capture the intricate structures of the iris. Then these patterns are subject to mathematical and statistical algorithms to encode digital templates for the identification of the individuals.

Iris recognition is very difficult to perform at a distance larger than a few meters and if the person to be identified is not cooperating by holding the head still and looking into the camera. However, several academic institutions and biometric vendors are developing products that claim to be able to identify subjects at distances of up to 10 meters. As with other photographic biometric technologies, iris recognition is susceptible to poor image quality, with associated failure to enroll rates. As with other identification infrastructure (ID cards, etc.), civil rights activists have voiced concerns that iris-recognition technology might help governments to track individuals beyond their will.

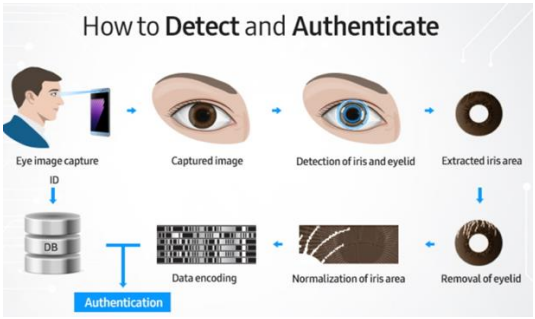

Fig. 5. How to detect and authenticate

Drawback: However, one problem frequently encountered when the technology is introduced is resistance from users. Quite a few people find having their eyes scanned a rather unpleasant experience. You also have to adopt a certain position so the scanner can read your iris, which can cause discomfort. Hygiene is another frequently cited drawback, as many systems require users to place their chin on a chin rest that has been used by countless people before them.

E. *Palm vein pattern recognition*

The hemoglobin in your blood contains oxygen when it is transported from your lungs to the tissues in your body by your arteries. By the time the blood flows back to your heart via different arteries this oxygen has been released. Vein pattern recognition uses this difference between deoxidized and oxygenated hemoglobin. Deoxidized hemoglobin absorbs infrared light, making the vein pattern visible if you use a

scanner to illuminate it with infrared light.

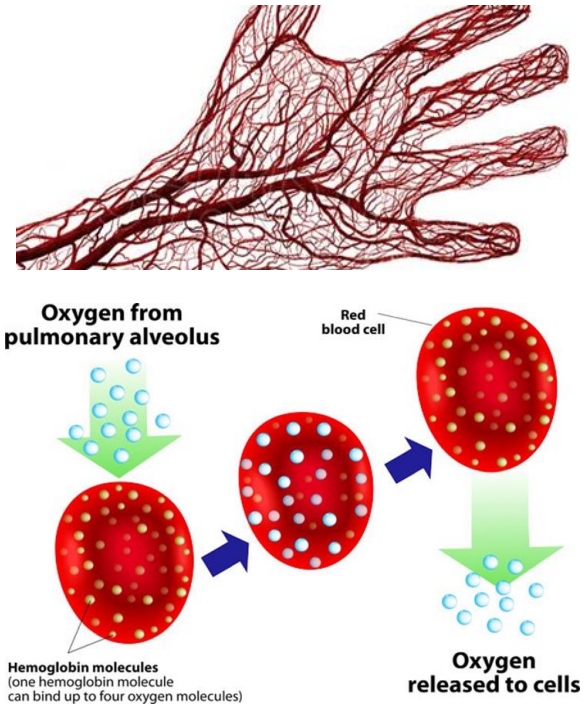

Fig. 6. Palm vein pattern recognition

Everyone has a unique vein pattern in their palm. Reference points in the pattern can therefore be stored and the pattern can be used as an identification and security technique. Most systems that use vein pattern recognition store the vein pattern as an image, which may or may not be encoded. With the Palm-ID, on the other hand, the scanned reference points are stored directly as an encrypted template, which means the vein pattern is converted into code *inside* the scanner itself. This method of palm vein pattern recognition therefore offers an extremely high level of security.

Drawback: Access control systems based on palm vein pattern recognition are relatively expensive. For that reason, such systems are mainly used within sectors that have exacting demands when it comes to security, such as government, the justice system and the banking sector.

F. Finger vein pattern recognition

It is based on the same principle as palm vein pattern recognition. Illuminating the vein pattern in the fingers using near-infrared light makes it possible to discern this pattern, thanks to the deoxidized hemoglobin.

Fig. 7. Finger vein pattern recognition

Drawback: Another point to bear in mind is that very cold fingers and 'dead' fingers (such as those of people suffering from Reynaud's syndrome) are impossible or difficult to read using finger vein pattern recognition. Perhaps the greatest drawback, however, is that this technology is still relatively unknown.

G. Lip Biometrics

Lips biometrics is not so familiar to use as biometric features. Human lips recognition biometrics is the most interesting and emerging way of identifying human and usually lip prints are used in forensic science. The lip features are unique for the individuals and stable over the time. In the speaker recognition the lip movement is used for identification and it is only a subsystem of combination of various biometrics. The lip prints are similar to finger prints and vary from individual to individual. The accuracy can't be obtained if used as alone. The figure 11shows the shape, prints and movements of lip. In general, the features of lips can be classified into three different categories: lips texture features, lips shape features and lips motion features. Researchers also found that lip-prints have been used in the determination of sex. The lips biometrics has the following biometrics. The lips biometrics is Passive, Anatomical, usually visible and Implemented in hybrid.

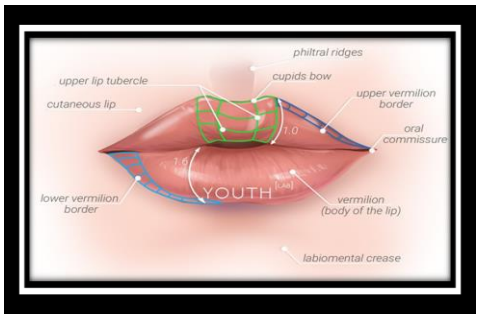

Fig. 8. Lip biometrics

H. Finger nail bed

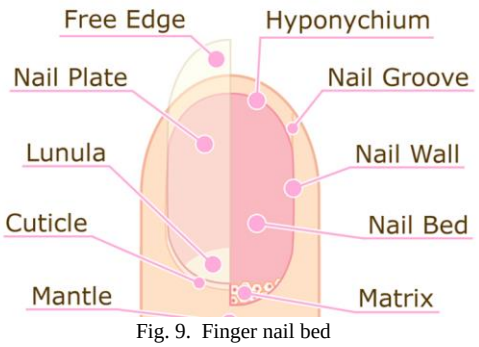

Fig. 9. Finger nail bed

One of the emerging technologies is Nail recognition and the study of nail recognition is on progress. The nail bed is one of the essential methods of recognizing fingernail. It is a parallel epidermal located directly below/beneath the fingernail and the travels over the nail bed during growth. It appears on the outer surface of the nail in the form of ridges. This technology is developed by Biometrics, which uses a RFID chip. Depending on the individual, the chip is capable of sensing the electrical

capacitance of the nail and flesh. The following figure depicts the nailbed.

I. Thermograms

Thermograms are defined as the visible quantity of infrared energy emission, transmission and reflection of an object. Then, it is converted into a temperature and shown as the distributed image of temperature. Also, known as Thermal imaging or Infrared Thermography (IRT). It is developed in mid-1990s. Thermography is similar to facial recognition and facial Thermography is used to detect the heat patterns produced by bifurcation of blood vessels, diffused by the skin. These patterns are known as Thermography. It is distinct and even it is different for two identical twins

J. Human scent recognition

Each human smell is unique and it is made up of chemicals called volatiles which could be distinguishable for every individual. It is physical biometrics without any contact to the human body to recognize a person by analyzing olfactory properties of the human body scent. The olfactory means the sense of smell. The sensors which are capable of acquiring the smell are used to get the odor from the back hand or armpit, the nonintrusive parts of the body and are converted into a template or unique data string, which are extracted by the system. The body odor consists of significant sensitive personal information. By analyzing the body odor, few diseases or activities happened in the last hours (for example sex) can be possible to diagnose. The functions such as attracting mates, assertion of territorial rights, communication and protection from a predator are served by the body odor. The individual's distinctiveness could be reduced by the usage of deodorants and perfumes.

K. Skin spectroscopy

Another emerging trend uses the visual details of the skin, as captured in standard digital or scanned images. This technique, called Skin Texture Analysis, turns the unique lines, patterns, and spots apparent in a person's skin into a mathematical space It is also described as a Biometric Artificial Intelligence based application that can uniquely identify a person by analyzing patterns based on the person's facial textures and shape People tend to believe that, since we live in a free society, we should be able to go out in public without the fear of being identified and surveilled. People worry that with the rising prevalence of facial recognition, they will begin to lose their anonymity.

L. Voice

Voice is a combination of physical and behavioral biometric characteristics. The physical features of an individual's voice are based on the shape and size of the appendages that are used in the synthesis of the sound. These physical characteristics of human speech are invariant for an individual, but the behavioral aspect of the speech changes over time due to age, medical conditions, emotional state etc. Voice is also not very distinctive and may not be appropriate for large scale identification. A text dependent voice recognition system recognizes the speaker independent of what he speaks. a disadvantage of voice based recognition is that speech features are sensitive to a number of factors such as back ground noise. Speaker recognition is most appropriate in telephone based applications but the voice signal is typically degraded in quality by the communication channel.

Fig. 10. Skin spectroscopy

Table 1
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

Table 2
Applications

Biometric	**Application**
Finger Prints	Law enforcement, entry devices for offices and colleges, enterprise security; medical and financial
Facial Recognition	Automated bank tellers- user verification purposes
Hand Geometry	Time and attendance systems, physical access
Iris Scan	Law Enforcement, Employee Security Check, banking
Retina Scan	High-end security, military, DNA Medical applications, Paternity Tests, Criminal identification and forensics
Voice Recognition	Call Centers, Law enforcement – house arrest authentication
Signature	Access to documents, Banking services

Table 3
Advantages and Disadvantages of the Various Biometric Modalities

Modalities	Advantages	Disadvantages
Fingerprint	• Relatively inexpensive • More secure and highly reliable. • Template size is small and so matching is fast • Consumes less memory space. • Most widely used technology • High accuracy	• Cuts, scars or absence of finger can produce obstacle for the recognition process. • Easily deceived through artificial finger made of wax. • Has physical contact with the system Worn out or may be altered over time • Exposed to noise and distortion due to dirt and twists
Face	• User-friendly design: Contactless authentication. 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 Storing of templates in database is easy.	• One obstacle associated with the viewing position offace • Face recognition doesn't work effectively in bad/weak lighting, sunglasses/sunshades, lengthy hair, or other objects partly covering the subject's face. • Even a big grin/laugh can render the system's performance less effectively.
Retina	• Highly reliable since no two people have the same retinal pattern • Rate of error is 1 out of 10,000,000 (virtually 0%) Highly accurate technology. • Provides most security in authentication • Low occurrence of false positives • Very quick Verification.	• Diseases such as cataracts, glaucoma, diabetes etc., affect the accuracy of the results. • Medical conditions such as hypertension causes privacy issues • Intrusive to Individuals and Enrolment and scanning are slow. • Limited usage • Expensive technology i.e. high equipment cost • Subject should be very close to the camera
Iris	• 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 • An iris scan can be carried outthrough10cm to a few meters apart. • Data capturing can be carried out even though a user is putting contact lenses or glasses • High accuracy and High recognition process speed	• Iris scanners might be very easily fooled through ha 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 have impacted by unusual lighting effects and illumination from reflective types of surfaces. • Iris scanners tend to be more expensive in comparison with additional biometrics
Human scent	Identification is possible by mixture of odors by recognizing the mixture's components.	Still there are no existing applications. • Artificial noses are not comfortable to do all the job\ • Senses of quantification are difficulty. • Distinctiveness is reduced by Deodorants and perfumes.
Lip motion	• Used by forensics professionals and criminal police training. • Template Size is small and depends on static mouth/face photos. • Interaction of user is not necessary and can be used without the knowledge of user. • Visible and not hidden/overcast by anything. • Can be hybrid -lips-voice or lips-face biometric systems	• Needs more attention for hybrid system • The relevant information may not be acquired from the specific facial attributes. • Variations (smile) may cause difficulty in recognition

6. Conclusion

Several biometric characteristics are in use in various applications. Each biometric has its strengths and weak-nesses, and the choice typically depends on the application. No single biometric can effectively meet the requirements of all applications—none is "optimal." We match a specific biometric to an application depending on the application's operational mode and the biometric characteristic's properties. For example, both the finger-print-and iris-based techniques are more accurate than the voice-based technique.

References

[1] https://en.wikipedia.org/wiki/Pattern_recognition
[2] https://www.tutorialspoint.com/biometrics/pattern_recognition_and_biometrics.htm
[3] https://www.geeksforgeeks.org/pattern-recognition-introduction/
[4] http://www.biometric-solutions.com/fingerprint-recognition.html
[5] https://en.wikipedia.org/wiki/Fingerprint
[6] https://findbiometrics.com/topics/fingerprint-recognition/
[7] https://umetrics.com/kb/spectroscopy-skin
[8] https://whatis.techtarget.com/definition/pattern-recognition
[9] https://www.sciencedirect.com/topics/neuroscience/pattern-recognition
[10] https://www.techopedia.com/definition/8802/pattern-recognition-computer-science
[11] https://www.elprocus.com/different-types-biometric-sensors/
[12] https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/
[13] http://www.m2sys.com/blog/biometric-technology/what-are-the-different-types-of-biometric-technology/
[14] https://www.bayometric.com/types-of-biometrics/
[15] https://www.biometric-security-devices.com/types-of-biometric-devices.html
[16] http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=16
[17] https://en.wikipedia.org/wiki/Biometrics