International Journal Of Scientific & Engineering Research, Volume 9, Issue 4, April-2018
ISSN 2229-5518

# Recent Application of Biometric Technology

[1]Rekha.S,[2]A.Santhiya, [3]Mrs.M.Dukitha

**Abstract—**biometric information has been a broadly discussed topic in the past and it still is. recent discussions consist of proposals for storing biometric facts on passports. there are for example video shops using fingerprints for authentication, an increasing number of laptops have a fingerprint sensor incorporated, and banks are beginning to apply biometric facts as well. this paper discusses why authentication using biometric information isn't always a not unusual standard up to now. it additionally analyses if the usage of biometric records makes structures greater cozy and if it's far really worth spending more money on such systems. the dialogue and evaluation in the paper ends in the conclusion that during most instances the trade-offs which want to be made aren't proper enough to remember biometric consumer authentication as a better opportunity to standard strategies consisting of login/password authentication. on the cease the paper provides a quick outlook about the destiny use of `biometric information. Human biometric traits which include face, finger, iris scanning, voice, signature and other functions offer a dependable security degree.

**Keywords—**Biometrics,Authentication, identification, verification, physical type of biometrics, behavior type of biometrics.

.– – – – – – – – – – ◆ – – – – – – – – – –

## 1 INTRODUCTION

Mostwell-known and popular situation that everybody of us meet easiest way to open the door is to use what each of us has: voice, hands, eyes, fingerprints. Nowadays the interest to different systems of biometric identification among users of computersystems grows up. The interested in technologies of fingerprints, face, voice, iris recognition in order to prevent penetration of outside people to their net. Bill Gates depends on the person based on something that one has (key, magnetic cal or chip card) or one knows (PIN, password).
Fingerprint sensors in laptops ad PDAs,banks start using biometric authentication systems and there exist even video stores which use this technology. (e.g. fingerprint,iris or face) or that you can do or produce (e.g. handwriting or voice).Most common user authentication systems.

## 2 LITERATURE EVALUATION

**T**he main goal of the present take a look at is to increase multimodal biometrics the usage of fingerprint and face reputation with neural community structure. the researcher has studied a lot of associated literature to apprehend the related paintings in this place. this observe has cleared the idea of the paintings here is the short of literature

- [1]*S.Rekha, Second year MCA masters computer application Er.Perumal Manimekalai College of Engineering, Hosur. PH-8056751780. E-mail: rekhamca8697@gmail.com*
- [2]*A.Santhiya, Second year MCA, Er.Perumal Manimekalai College of Engineering -Hosur, PH-9943343199. E-mail: santhiyass9396@mail.com*
- [3]*Mrs.M.Dukitha,Assistant Professor, Master of Computer Application in Er.Perumal Manimekalai College of Engineering - Hosur, PH-, E-mail: dukitha.m@yahoo.co.in.*

## 3 PURPOSE

fingerprint biometric era solutions to decorate safety in company the motive of this white paper is to summarize the numerous applications of fingerprint biometric era to provide a higher degree of protection for data get entry to via intranets, extranets, the net, bodily get admission to and for more cozy financial and ecommerce transactions. This white paper will no longer deal with the other eight biometrics inclusive of, iris experiment, retina test, facial scan, hand geometry, voice, signature, keystroke sample and gait. It'll focus on software of it, aviation, banking and financial, healthcare and the government sectorsassessment.

## 4BIOMETRIC

A Biometric is a physiological or behavioral characteristic of a human being that can distinguish one person to another and that theoretically can be used identification and verification to identify. Themost common physical characteristics explored and used are facial features, eyes (iris and retina), fingerprints and hand geometry. Handwriting and voice are examples of personal traits which could be used to distinguish between individuals. Fingerprint two biometric recognition technologies.Facial recognition, and eye scans (iris, retina). Behavioral biometrics includes voice recognition and handwritten signatures.

International Journal Of Scientific & Engineering Research, Volume 9, Issue 4, April-2018
ISSN 2229-5518

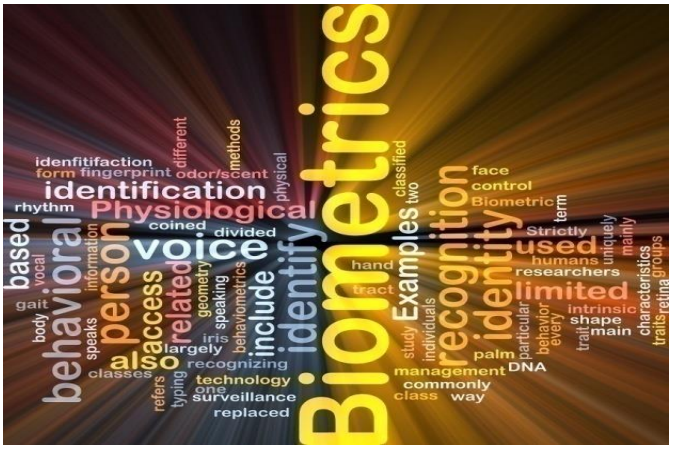


Fig.1 Biometrics

### 4.1 Biometric Characteristics

1. Robustness
2. Distinctiveness
3. Availability
4. Accessibility

### 4.2 Current Biometric Modalities

Biometric characteristics can be divided in two main classes, as represented in figure on the right:

- Physiological are related to the shape of the body. The oldest traits that have been used for more than 100 years are fingerprints. Other examples are face recognition, hand geometry and iris recognition.
- Behavioral are related to the behavior of a person. The first characteristic to be used, still widely used today, is the signature. More modern approaches are the study of keystroke dynamics and of voice.

### Physiological:

- Finger and Palm Prints
- Hand/Finger Geometry
- Vascular Imaging
- Facial Recognition
- Voice Pattern
- Retina Scan
- DNA
- Odor, Earlobe, Sweat
- 2pore, Lips.

### Behavioral

- Signature
- Keystroke
- SpeechRecognition
- Gay.

### 4.3Biometric Techniques

There are lots of biometric techniques available nowadays. A few of them are in the stage of the research only (e.g. the odoranalysis), but a significant number of technologies is already matureand commercially available (at least ten different types of biometricsare commercially available nowadays: fingerprint, fingergeometry, hand geometry, palm print, iris pattern, retina pattern,facial recognition, voice comparison, signature dynamics and typingrhythm).Biometric technologies can provide a means for uniquely recognizing humans based upon one or more physical or behavioral characteristics and can be used to establish or verify personal identity of individuals previously enrolled. Examples of physical characteristics include face photos, fingerprints, and iris images. An example of behavioral characteristic is an individual's signature. Used with other authentication technologies, such as tokens, biometric technologies can provide higher degrees of security than other technologies employed alone. For decades, biometric technologies were used primarily in law enforcement applications, and they are still a key component of these important applications. Over the past several years, the marketplace for biometrics solutions has widened significantly and today includes public and private sector applications worldwide.

### 4.4Fingerprint Technology

Fingerprint identification is perhaps the oldest of all the biometrictechniques. Fingerprints were used already in the Old China asmeans of positively identifying a person as an author of the document.Their use in law enforcement since the last century is well the oldestknown and actually let to an association fingerprint = crime. This causes some worries about the user acceptance of fingerprint-basedsystems.

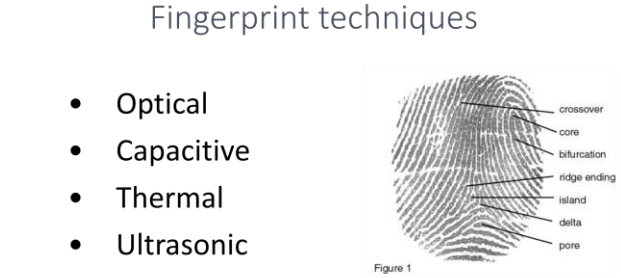


Fig.2 Fingerprint Techniques

They can be distinguished by the epidermal ridge and furrow structure of each finger, which is used and development focus on the fingerprint technology since its release.

International Journal Of Scientific & Engineering Research, Volume 9, Issue 4, April-2018
ISSN 2229-5518

### Fingerprint Readers

Before we can precede any further we need to obtain the digitalizedfingerprint. The traditional method uses the ink to getthe fingerprint onto a piece of paper. This piece of paper is thenscanned using a traditional scanner.

### 4.5 The use of fingerprint authentication

- Eliminate password problems
- Consolidate multiple passwords to one single biometric login
- Control and manage user access to corporate network database
- Control and manage physical access to authorized areas
- Secure important confidential corporate information Benefits
- Higher corporate security
- Time/cost efficiencies

### 4.6 Iris

Iris is a unique structurefeaturing a complex pattern.This can be a combination ofspecific characteristics knownas corona, crypts, filaments,freckles, pits, furrows, striations and rings. Even twins have differentiris patterns and everyone's left andright iris is different.iris identification is greater than of the DNA testing

Each iris is a unique structurefeaturing a complex pattern.This can be a combination ofspecific characteristics knownas corona, crypts, filaments,freckles, pits, furrows, striations.and rings.

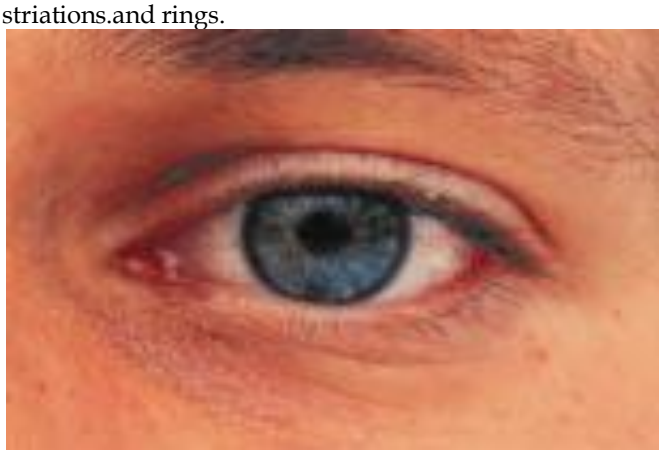

Fig.4 iris

### 4.7 Retina

Eye identify retina is not directly visibleand so a coherent infraredlight source is necessary to illuminate the retina. Theinfrared energy is absorbed faster by blood vessels in the retina than by the surrounding tissue. The image of the retina blood vessel pattern is then analyzedfor characteristic points within the pattern. The retinascan is more susceptible to some diseases than the iris scan,but such diseases are relatively rare.Retina scan is based on the blood vessel pattern in the retina of the eye.

Fig.3 retina

The retina infrared energy is absorbedfaster by blood vessels in theretina than by the surroundingissue. The image of the retina blood vessel pattern is then analyzedfor characteristic points within the pattern.

### 4.8 HandGeometric

Hand geometry is based on thefact that nearly every person's handis shaped differently and that theshape of a person's hand does notchange after certain age. Hand geometry system.

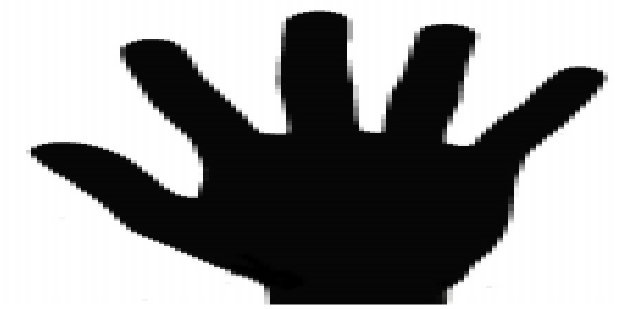

Fig.4Hands Geometric

This is a 2D pictureof the handshape. Most modern systems use allthree dimensions to measure the hand'sCharacteristics.

### 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

International Journal Of Scientific & Engineering Research, Volume 9, Issue 4, April-2018
ISSN 2229-5518

identify a user in a system is the smallest by far, allowing it to be used with Smartcards easily.

**Disadvantages**

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

### 4.9Signature Dynamics

The signature dynamics recognition is based on the dynamicsof making the signature, rather than a direct comparison of the signatureitself afterwards. The dynamics is measured as a means ofthe pressure, direction, acceleration and the length of the strokes, dynamics number of strokes and their duration.

E-pad

Smart pen

Fig.5 Signature dynamic

special purpose devices used to capture the signature dynamics. Both are wireless. The E-pad devices show the signature on the digital display while the Smart pen has got its own ink cartridge and can be used to write onto any paper.

**Advantages**

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

**Disadvantages**

- 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.

### 4.10 FacialRecognition

Facial recognition is the most natural means of biometric identifiable. The method of distinguishing one individual from another is an ability of virtually every human.

Eg: Camera The first task of the processing software is to locate theface (or faces) within the image. Facial recognition technologyhas recently developed into two areas: facial metrics and eye faces.

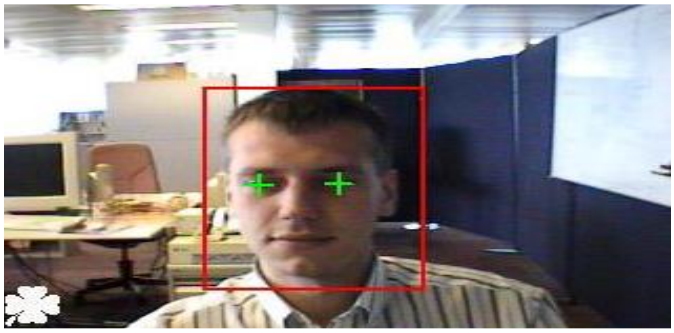

Fig.6 Facial recognition

After locating the facein the image the system locates eyes withinthe face region.

**Advantages**

- Non intrusive
- Cheap technology.

**Disadvantages**

- 2D recognition is affected by changes in lighting, the person's hair, the age, and if the person wear glasses.
- Requires camera equipment for user identification; thus, it is not likely to become popular until most PCs include cameras as standard equipment.

## 5OTHERBIOMETRIC TECHNIQUES

### 5.1 Palm print

Palmprint verification is a slightly different implementation ofthe fingerprint technology. Palmprint scanning uses optical readersthat are very similar to those used for fingerprint scanning, theirsize is, however, much bigger and this is a limiting factor for theuse in workstations or mobile devices.

### 5.2 Hand vein

Hand vein geometry is based on the fact that the vein patternis distinctive for various individuals. The veins under the skin absorbinfrared light and thus have a darker pattern on the image ofthe hand taken by an infrared camera.

### 5.3 DNA

DNA analysis has not been sufficientlyautomatic to rank the DNA analysis as a biometric technology.The analysis of human DNA is now possible within 10 minutes. Assoon as thetechnology advances so that DNA can be matched automaticallyin real time, it may become more significant.

### 5.4Thermal imaging

This technology is similar to the hand vein geometry. It also uses an infrared source of light and camera to produce an image of the vein pattern in the face or in the wrist.

International Journal Of Scientific & Engineering Research, Volume 9, Issue 4, April-2018
ISSN 2229-5518

### 5.5Ear shape

Identifying individuals by the ear shape is used law enforcementapplications where ear markings are found at crime scenes.Whether this technology will progress to access control applications is yet to be seen. An ear shape verifier (Otophone) is produced by a French company ART Techniques.

## 6 Applications

The world would be a fantastic place if everything were secure and trusted. But unfortunately, in the real world there is fraud, crime, computer hackers, and theft. With our lives becoming more and more dependent on digital technology and automation, how do we know if people are really who they claim to be? Following the events of September 11th, there is a compelling need for a more secure future, yet it's held back due to the lack of wide deployment of authentication technology solutions for information and physical access security. How can we securely identify and authenticate who is who? The answer lies in fingerprint authentication solutions. Fingerprints have been legally accepted for verifying identity for over a century. They cannot be altered, forgotten or cracked by hackers running a software routine. They are universally accepted as unique to each individual, and they are used in situations where there can be no mistake of identity, such as criminal proceedings and high security access control. A fingerprint-based biometric security solution can assure people's personal identities through digital recognition. Fingerprint authentication provides a dependable, legally acceptable method for authenticating users. With focus on information security, physical access control and management, and embedded solutions, fingerprint authentication can be integrated and applied to a wide range of industries, which will be discussed later in this white paper

## 7 Advantages of Biometric Systems

- No more forgotten or stolen passwords.
- Positive and accurate Identification
- Highest level of security
- Offers mobility
- Impossible to forge
- Serves as a *Key* that cannot be transferred.
- Safe & user friendly

## 8 Disadvantages of Biometric Systems

- The iris-scan are someindividuals are difficult to capture.
- Also the iris can be easily obscured by eyelashes, eyelids, lens and reflections from the cornea.
- There is also a lack of existing data which deters the ability to use for background or watch list checks

## 9 Conclusion

The biometric technique is not perfectyet, there are many mature biometric systems available now. Properdesign and implementation of the biometric system can indeedincrease the overall security; especially the smartcard based solutionsseem to be very promising. Making a secure biometric systems
is, however, not as easy as it might appear. The word biometricsis very often used as a synonym for the perfect security. This isa misleading view. There are numerous conditions that must be takenin account when designing a secure biometric system. First, itis necessary to realize that biometrics is not secrets. This implies be carefulthat biometric measurements cannot be used as capability tokensand it is not secure to generate any cryptographic keys from them.

## References

[l]American Biometric Company,http://www.abio.com/
[2] Biometric Access Corporation,http://www.biometricaccess.com/
[3] C. Calabrese: The trouble with biometrics, login:, Volume24, Number 4
[4] Digital Persona, http://www.digitalpersona.com/
[5] EyeIdentify, http://www.eyedentify.com/
[6] I/O Software, http://www.iosoftware.com/
[7] Iridian Technologies, http://www.iriscan.com/