International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 11 • Issue 1 pp. 812-821 Jan 2019-June 2019 www.csjournals.com

Systematic Review of Biometric Advancement and Challenges

Sakshi Bhatia

Uttaranchal Institute of Management, Uttaranchal University, Dehradun, Uttarakhand

Abstract: Now days when security is the main concern of each and every person, biometrics is the best way to secure the identity of an individual. Biometrics has overcome the traditional method of identification which can be spoofed and stolen. Biometrics is the method of identifying people based on their traits like their body shape(e.g. fingerprint, iris, retina, face recognition) and behavior of the person(e.g. signature, voice, gait etc.). In this paper details are given about different biometric traits which can be used to identify people based on their physiological and behavioural patterns. This paper explicitly states the working of different biometric systems. It also surveys the shortcomings of each biometric approach along with the notable advantages. The authors also proposed the prospective solutions for various biometric recognition categories.

Keywords: Biometrics, Identification, Security, Template.

Introduction

Biometrics is a way to recognize people based on their physical traits. These traits needs to be unique for all the human being, must be easily collectible and must remain permanent so that the id generated remains same throughout the life of a human being. Biometrics is done mainly on two types of traits of humans-physiological and behavioural. Physiological traits means fingerprint, eye scan (iris, retina), face recognition, DNA, palm print and behavioural traits means signature, voice of the person etc.[1] . In Fingerprint recognition scanned image of the finger is taken and is compared with the already stored image which is converted into binary form in the database. In Iris recognition high resolution image of the user's iris is taken and is converted into template using mathematical algorithms and is then compared whenever needed. Face recognition system on the other hand uses image of the face, where face of the person is detected, features are extracted using 40 nodal points and then classification of these features are done to identify the person. Next is voice recognition system which has been explained in this paper, in which the user is asked to speak into a microphone and his/her voice is converted from analog to digital signals and is then compared with the voice stored in database and verification takes place. Signature Recognition has also been explained in which people are asked to write their signature either on paper or on a computerized tablet which checks for various characteristics of the signature like the pressure while writing, velocity, speed of the user etc. Gait Recognition is the identification of a person on the basis of his walking pattern. This recognition can be done from a distance, without the permission of the user and is mostly used for security purpose, to identify a suspect.[2]

Biometrics has made our life very easy in terms of identification and authentication. Earlier a lot of time was consumed standing in queue for identification when fingerprint was taken on paper with ink or signature was taken on paper. But now in the era of technology we cannot expect things to be slow, everything is automated and so is recognition system. Our data will not get stolen or get lost till the time we do not allow someone to do so. Nowadays there are many details which one cannot compromise such as bank account details, business details, mobile phone data like images, videos, call log, chats, etc. For these details to remain secure we need something which is unique, permanent and easy to carry for which biometrics is the best solution. We use biometrics on daily basis, from our offices to airports where fingerprints and facial recognition is done to identify people.

Biometrics has a history of as long as 31000 years when fingerprints were used by prehistoric men as signature. In 500 B.C. Babylonian business transactions were done on the basis of fingerprints on clay tablets as a means of security. In 14th Century Chinese used fingerprints for business transactions and also to differentiate their children. The first record of finger and hand prints which was recorded uniformly was in 1858 by Sir William Herschel who was in Civil Services, India and wanted to make a record of employees to distinguish them. In 1936 the concept of iris pattern to recognize humans was proposed by an ophthalmologist Frank Burch. Even to identify the remains of the body of Osama bin Laden biometric identification was used i.e. facial recognition and DNA by Central Intelligence Agency in 2011[3].

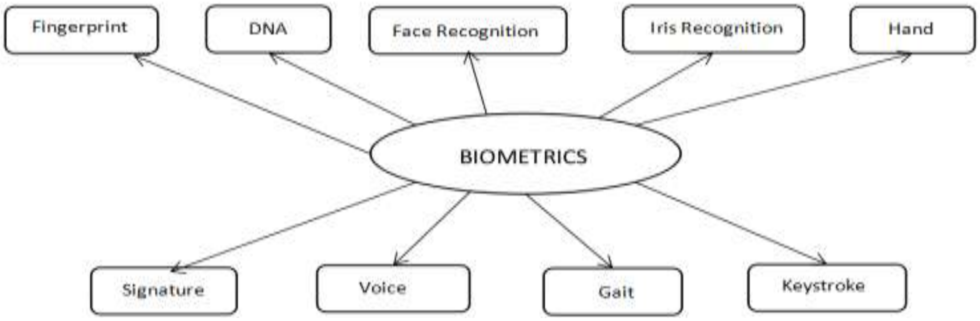

Figure 1: Different types of Biometrics

There are various advantages and drawbacks of biometrics also which are discussed in this paper. Some of the advantages are as follows:

High degree of security: Earlier Pins and passwords were used to secure data which are easily hacked and data can be stolen if someone knows our password or pin number.These methods to store data were not secure which were afterwards replaced by biometrics where human traits are used to recognize the identity of a person. These traits are unique and cannot be stolen from somebody.

Friendly: Biometrics is a system which is very user friendly as people do not have to carry their id cards now or don't have to remember their passwords and pin numbers because we have our physiological and behavioural traits with us all the time which cannot be forgotten at home or does not require to be remembered. Biometrics is also less time consuming avoiding long queues outside offices.

Accurate verification: Nowadays when people are using internet on daily basis and everything is available on internet,accurate verification of individual is provided by biometrics. Biometrics is mostly used on daily basis for mobile transactions where identification is done on the basis of fingerprint or Aadhaar card number.

Time Efficient: Earlier identification was done with passwords and pin numbers which used to take time in matching the data with the database and then giving access to the user. Whereas biometrics just needs your fingerprint or eye scanning and internal processing is done faster as compared to the earlier process used to take.

Drawbacks of the Biometric System are as follows:

Cannot be changed: This is the biggest disadvantage of biometrics that once stolen or hacked, cannot be changed because the traits are not changeable (e.g. fingerprint of a person cannot be changed, it will remain the same throughout his life).

Costly Setup: Biometrics system needs a lot of money for setup as the software and other devices used in biometrics system are costly.The cost of servers used, software, programmers, other devices is huge.

Less accuracy in Iris Recognition: Iris recognition is less accurate because people tend to use glasses at some point of time or may have blurred vision or may be using lenses which causes a difference in recognizing a person.[3]

Face recognition: Face recognition system depends on how the device takes the photograph,lighting of the room,quality and resolution of image taken and also the mood of the person. Sometimes biometric machine may also fail to recognize the person after a certain age when people tend to have wrinkles or aged skin.

Unhygienic: Biometric system requires people to put their finger or face on the same device on which hundreds of other people have already used which transfers bacteria and germs and is harmful for health.[3,5]

There are factors that motivate the research undertaken in this review paper. First, there are various applications of biometrics which is an interesting thing. Biometrics is used from schools and offices to borders for security. More than 82 countries worldwide are using ePassports now which has fingerprint as main trait used for identification[4]. Secondly how biometrics has changed our lives and how biometrics has made everything so secure just with the help of technology. Thirdly how biometrics can be used with the help of human organs and how the biometrics system is working so accurately and efficiently with less error rate.

HOW BIOMETRIC SYSTEM WORKS?

Every biometric system whether it is fingerprint scanner or iris scanner, they use the same steps to identify a person. The steps are as follows:

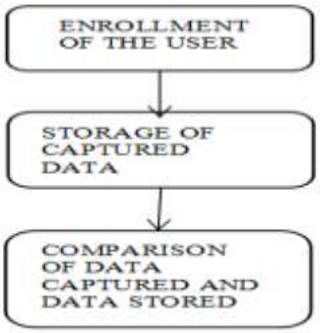

Figure 2. Generic Working Of the Biometric System

STEP 1: Enrolment of the User: First of all the user is asked to give his/her basic information like name, address, pincode and then it takes the sample of our physiological or behavioural trait. After the device captures the information, it creates an electronic representation of the data captured in the device. This captured information is then later used for verification purpose.

STEP 2: Storage of the captured data: The data captured while enrolment is stored in the database for verification or it is stored in a smart card which people carry with themselves like Aadhaar Card which is used in India as Identification proof. To store this data a huge database is needed,like the largest biometric database is of the Aadhaar which is India's national ID program in which 550 million people have been enrolled and 480 million Aadhaar cards have been issued.

STEP 3: Comparison: This is the last step of using a biometric system. Whenever the user again uses the biometric system, they have to provide the device with their trait asked for and that trait is then compared with the already stored data. This process takes place each and every time the user tries to use the biometric system for authentication.

CATEGORIES OF BIOMETRIC TRAITS

Fingerprint: Fingerprint is the oldest method of checking a person's identity. Earlier ink was used for taking fingerprint for official work which was not that secure. Now optical sensors are used to check fingerprint of a person which are not easy to fake. Every individual has unique pattern of fingerprint with ridges and valleys which makes it easy to verify everyone. Fingerprinting was first used in India for identification by Sir William James Herschel in 1858. He was a British Indian Civil Services Officer in India who started taking fingerprints on contracts from the employees for their identification [6]. Fingerprint Recognition has two processes: Taking image of the finger which includes features which are unique to every person and matching of the valleys and ridges of the image taken by the device with the pre-scanned images. In fingerprint recognition image of the finger is not stored in the database rather a binary code generated after scanning of the finger is stored in the database which is later used for verification. Algorithm is used to convert finger image to binary code but vice-versa is not possible. Fingerprints cannot be lost and are accurate but has chances of getting stolen. Process of identifying a person from fingerprint scanner is less time consuming than the traditional method of identification. Fingerprint recognition system for some people is a concern for cleanliness because a lot of people touch the scanner and germs travel at each touch on the scanning machine. Minutiae features are considered very important in fingerprint recognition.Minutiae features are small details of the fingerprint which are essential for identification. These features are the ridge ending-where the ridge ends in a fingerprint, bifurcation-where a ridge gets distributed into two ridges and the dot-ridges which are shorter than other ridges also called short ridge.[7]

Fingerprint Recognition System has several advantages like:
Fingerprints are not easy to fake as earlier identity cards were.
They are not meant to be remembered which makes it easier for people who forgets passwords and pins.
Fingerprints cannot be stolen unlike an identity card.
Fingerprints are easily collected which is why this method is reliable.
Fingerprints are a unique trait unlike DNA which is same in case of identical twins.
Every technology that has advantages also has negative effects, some of them are:

In US in December 2014, 5.6 million fingerprints were stolen as said by the OPM which is federal government's human resources department and checks for security.[26]
Fingerprint scanner will not identify a person if the finger of that person is injured in any case.
Require large amount of computational resources.
Face Recognition: Face Recognition is a technique where image of face is taken and compared with the already stored image in the database. There are 40 nodal points in a human face which are used to measure length and width of the nose and eyes and cheekbones. Every person has a unique face, even the identical twins have different measure of length of face and space between ear and nose and width of eyes. People have been using this technique to identify people since ages but now it is different just because of technology. Face Recognition was invented in the year 1964-65 by Woody Bledsoe, Helen Chan Wolf and Charles Bisson. This system used to extract coordinates of the face features from the image taken by the camera and was then called man-machine.[19]

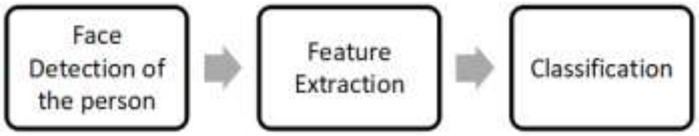

Figure 3: Face recognition process

Face recognition involves three steps i.e. face detection, feature extraction and classification. Face detection is the first process which involves finding the face in the image captured by the camera. The device returns nodal points of the persons face if the face is detected by the device. The device assumes that there is only one face in the image and with this assumption it finds nose, ears, eyes, chin, lips, forehead of the person and returns their width and height and distance between each. For Face recognition there are three approaches which are used:
Holistic approach: In this approach the whole face is considered as a single feature for face detection and feature extraction. Local features like nose, eyes are ignored in this approach. It further consists of two methods: statistical methods and artificial intelligence.
Feature based approach: In this approach local features of human face are used as input data unlike holistic approach. These local features make it easy to detect the face as every individual has different shape and size of the local features. Then these features are matched with the image stored in the database.[8]
Hybrid approach: This approach is a mixture of the holistic and feature based approach mentioned above. This approach provides more accurate results as the whole face and local features are also considered for face detection which makes the identification more reliable.[9]
Face Recognition System has advantages like:
Face pattern of every individual is unique and image of the face can be taken from a range.
Face Recognition is easily accepted because of its user friendly nature.
This technique is inexpensive as it requires less amount of money while installing.
Face Recognition provides accurate result if the image is taken correctly.
Dubai airport uses this technique for identification because of its time saving nature.
With advancement in technology comes drawbacks, some of them are as follows:
With age face recognition system does not provide accurate result and cannot identify a user due to wrinkles on face.
Face recognition system cannot differentiate between identical twins.
Face recognition system cannot identify a user if the user has grown beard or has shaved off completely.
Light, brightness, Pose and posture of the person also plays a vital role in face recognition. Sometimes if the light is not proper, system cannot identify the user.
Iris Recognition: It is a method of identification where photograph of the iris of human eye is taken and compared with the image stored in database. Iris is the coloured part around the pupil. This method uses mathematical pattern recognition technique to identify a person's iris. Iris Recognition System was first patented, developed, published papers and used by John Daugman but in 1949 J. H. Doggart and in 1953 F. H. Adler had already written about Iris as a unique trait to identify people which was a conjecture and was patented by L. Flom and Aran Safir in 1980s but they could not implement this conjecture due to lack of idea on how the algorithm would work.[20] The image taken of the iris is high resolution image and is captured using infrared imaging process which can differentiate between the iris and pupil of the human eye. This image is then converted into templates which provide mathematical

representation of the iris which is later used to identify a person. Diameter of the Iris of human eye varies with light, focus and resolution around the person which is a concern while taking image of the iris. The light, focus and resolution of the place where image of the human iris is taken must be carefully balanced so that there is no error while identification.

Iris recognition is a much secure method in comparison to fingerprint and face recognition because iris is an internal organ and deals with less wear and tear whereas in case of fingerprint and face it is different. With age and time fingerprints are hard to recognize by the scanner due to fade lines and wrinkles on face. Even the identical twins have different iris pattern. People who are concerned about cleanliness are happy with iris recognition because in this method image is taken from about 10cm to some meters away,which means the person does not have to touch any equipment for identification. Also there is no problem for people who wear glasses or contact lenses because iris recognition works well with both of the things.

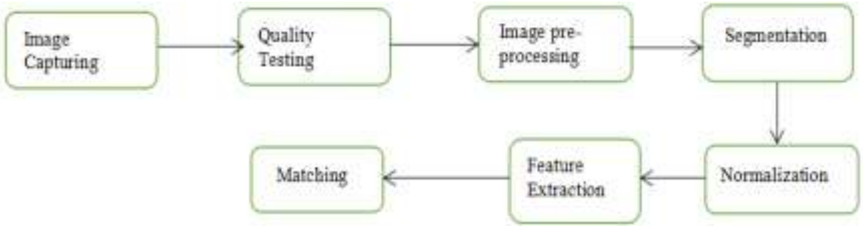

Figure 4: Process of Iris Recognition System

Iris Recognition has pros and cons of its own. Some of the core benefits of iris recognition system are:

Shape of the iris is flat which makes it easy for the system to recognize the person by taking proper image unlike face recognition where face of every individual has different shape.[9]

Iris is an internal organ which makes it less prone to damage unlike fingerprints which fades with age and the type of occupation a person has.

Iris recognition is a user friendly technique because user does not have to touch any device which makes it a more clean way of identification unlike fingerprint scanner.[10]

Iris of a person remains stable for years which makes it reliable and needs less update.

Underlying are the drawbacks of iris recognition system:

After a certain age human tend to have changes in body and pattern of iris changes which makes it difficult for the user in identification.

Some people tend to gain eye disorders like cataract which brings changes in the iris pattern of a person.[10]

Iris recognition system is expensive to install and requires proper training of the people as it needs the user to stand still in front of the device and look straight.[11]

Difficult to perform at a distance, iris recognition system to identify a person needs the person to stand at a minimum distance of certain meters. If the user is not cooperative and is not standing still, identification would not be done properly.

Voice Recognition: Every individual in this entire universe has unique voice pattern in terms of pitch, bass and tone. Voice recognition is also called speaker recognition and is used in many industries like healthcare, military, airports, banking etc. The user needs to speak in a microphone for this and then the electrical signals are translated into digital signals through Analog to Digital Converter. The system then compares these digital signals with the voice template already stored in the database and identifies the person. Voice Recognition System was first invented by Bell Labs in 1952 which could only understand numbers, this system was named Audrey following which came a system named Shoebox which was developed by IBM and could understand 16 English words, 10 numbers and 6 arithmetic commands.[21] Voice recognition has several application like:

In forensic department to identify a person from the best matches, voice recognition is the most common method. To identify a criminal whose voice was used in any criminal offence, voice recognition system is used to recognize the person.[12]

Voice recognition system provides access control to user for using automated cars, automated homes, mobile phones etc.[12]

In February 2016, world's 7th largest bank HSBC offered 15 million customers with voice recognition as password for accessing bank account online.[13]

Everyone is familiar with Google Voice which is provided in every smartphone and allows the user to search the thing asked for.

Apple's Siri, Windows Cortana, Amazon Echo are an example of digital assistants provided by the smartphones and laptops to the user to perform activities asked by the user.

Process of Voice Recognition involves these steps: Speech Input, pre-processing of input, similarity, decision, verification result. First step is the Speech Input in which input is taken from the user into a microphone or headset. Input is taken at a place where noise disturbance is less so that clear voice is given as input and system does not make any mistake while giving results. Now this input is processed where electrical signals are translated into digital signals because voice cannot be simply matched with the voice stored in the database, it has to be converted through Analog to Digital Converter. Third step is to match these digital signals with the already stored voice template. If the voice template stored matches with the input of the user, user is identified to be the person he is claiming to be else authentication is not provided to the user and strict actions can also be taken against him for claiming to be someone else.

Voice recognition is easy to implement and is mostly used in phone based applications but it is easy to spoof this system. Voice of a person changes with time and also at the time of illness so this is not a secure method of storing data. Voice recognition needs very less percentage of disturbance, only then the system will be able to recognize the user.

Benefits of this system are as follows:

Voice Recognition can easily be implemented as it is economical and the software can be implemented in a computer also.

Voice Recognition gives result then and there. User does not have to wait for long to get the results.

This technology is non-disruptive and does not require touching of any device, the user just has to speak into the microphone and the results are declared.

Database is reduced as only templates of digital signals are stored in the database which requires less space.

Drawbacks of this system are:

The system must know the language of the user to identify the person.

In voice recognition filtering the background noise is very essential else false results can also be generated and user authentication can be violated.

Tone, pitch, intensity of voice must be kept in mind which was used when enrolling for the system.

Mood of the person also plays and important role while identification through voice.

It is possible to copy someone's voice pattern which makes this technique more prone to theft and hacking.

Signature Recognition: It is a behavioural biometrics which can be done by two ways: Static and Dynamic. In static method the user has to write his signature on a paper using a pen and that signature is then compared to the signature stored in database to recognize the person. Whereas in dynamic method the user has to write his signature on an electronic tablet which is then and there compared with the signature stored in database of the recognition system. Dynamic method is faster in comparison to static method and is more accurate. In static method, signature of a person can be copied but in dynamic method several other characteristics are also used to recognize the person's signature like velocity with which he is writing, pressure of his hand, acceleration, time he consumes in writing his signature, x, y and z axis, writing speed of the person. To copy these characteristics is not easy but the user needs to be trained for using this system. Holding the electronic pen and writing on tablet sometimes can be difficult for the user and may need trainers help. Signature Recognition system has been in practice since 1965. North American Aviation first invented signature recognition system. Whereas first dynamic signature recognition system was invented in 1977 by Veripen Inc. And was first tested on United States Air Force.[22]

Process of signature recognition consists of these steps: Signature is written on the tablet as input. User provides at least 10 samples of his signature with variations possible. This image is then processed where noise cancellation is performed, binarization(process to convert a pixel based image into a binary image) is performed and saved into the database in JPG or JPEG format. After this feature extraction is performed in which features like width, height, pressure points, writing speed of the user etc. is extracted. Finally after feature extraction, image of signature taken is compared with the image stored in the database and verification is performed.[14]

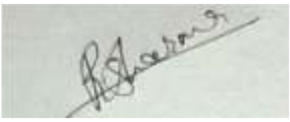

Figure 5: Static method of Signature Recognition

Advantages of Signature recognition are as follows:

This method is highly acceptable by most of the users because this method has been in practice since ages, earlier it was on paper now it is on automated tablets.

Cost of online and offline signature recognition is less in comparison to other methods of identification. In offline system a pen and paper is needed and a scanner to scan the image whereas in online system a digital pen and tablet is needed which do not cost a hefty amount.[14]

Signature recognition system uses 40 different features to identify a signature which provides more accuracy while identification.[15]

Enrollment is done fast, which means it is time saving because people do not have to be trained to write their signature as signature has been used since a long time by the people.

Less database space is acquired by this system as the signatures are compressed and stored, but the compression rates do not affect the quality of image.

Disadvantages of Signature recognition are as follows:

People who do not write their signature in a consistent manner can have problem while authentication because the system checks for the pattern of signature, strokes, length, width and height of the signature.

There are people who are uneducated and still do not know how to write their signature, for these people it is impossible to get authentication. These people first needs to know how to write their signature and then use the signature recognition system.

5 dimensional pen may be used to get accurate results which can cost a large amount to the user.

Gait Recognition: This method involves identification through the walking pattern of a person. Gait of every person is unique and can be used as biometric trait. Gait recognition system is the best method to identify a person if the person is at a distance. Gait analysis was first invented by Aristotle in De Motu Animalium to analyze the gait of animals. In 1890s german anatomist Christian Wilhelm Braune and Otto Fischer wrote papers on human gait.[23]Gait recognition is getting popular nowadays because of its features like: 1). Gait recognition can be done without the permission of the user, this is done for the verification of the criminals. 2). Gait recognition can detect the person even if the video is of low resolution. 3). Gait features are difficult to copy as each and every person has different pattern of walking.[16]

Iris recognition and face recognition can also detect the person from distance and do not require the user to be in personal contact but they need high resolution image. There are various parameters taken into account to identify a person on the basis of his gait namely speed of walking of the person, step length taken by the person, weight and height of the person which play an important role in modification of the gait of a person, personality of the person is also an important factor to distinguish the person, foot angle of the person, location of ankle, knee and hip. There are several applications of the gait recognition like: 1) After orthopaedic surgery.Gait analysis allows the doctors to check the gait of the person and whether the gait is normal or not after an orthopaedic surgery. 2). Gait Recognition system is used for Security purpose at airports to identify someone susceptible. Gait recognition takes image of the person from distance with the help of cameras installed at various places.3). A proper analysis of gait is performed before any player is selected in any sport. Also gait analysis is performed after any injury to the player.

Advantages of Gait Recognition are as follows:

This is a technique in which verification is done from a distance and the person who is verified does not get a hint of what is going on.

Gait recognition is a technique in which if the image is blurred or the environment is foggy or rainy, the result is not compromised.

Does not require training to the user for using the system.

Cons of this system are as follows:

Needs special setup for using this system, as cameras need to be setup.

In Gait recognition system it is difficult to understand the working of the administrator part of the system.

Administrator of the system needs proper training to identify the person.[24]

DISCUSSION

Biometrics is a part of authentication on the basis of human traits which has been used since ages now. Biometrics has applications which are used in our day to day work. Today in the era of technology gait recognition and iris recognition and several other techniques are performed with the help of artificial intelligence. In the proposed work 6 biometrics recognition techniques are discussed with their benefits, drawbacks and their working in which according to the author the best technique which has a lot of scope in future is Iris recognition system. Iris recognition system is a technique which is very user friendly and requires no contact with the device which means there is no health concern for people in iris recognition. Iris recognition can work from a distance even if the person is wearing glasses or lens. Iris of the person remains same throughout his life and has been used in India for Aadhaar verification which is India's User identification Initiative. Technique which the author thinks comes after iris recognition system is fingerprint recognition system. This technique has been used from ancient times but came into practice in daily life with technology very lately. Fingerprint recognition system is used in most of the airports, banks, offices and borders for verification for eg. Iraq border patrol security. Implementing this technique is relatively inexpensive and results are mostly accurate which is why this technique is the mostly used and not iris recognition which is quite expensive to implement everywhere. After this comes signature recognition which is also in practice from a very long time.

Signature recognition system is quite inexpensive if talking about static system but the dynamic system is quite expensive because it needs 5D pen and electronic tablet and proper training to the user.Static signature recognition system is still not that accurate as much the dynamic recognition system is. Then in the queue is Face recognition,which is also quite popular for identification of individuals. Face identification measures the bone structure and space between eyes,nose,ears,chin,cheek bones. Every individual has a unique face structure but face is something which can be copied through prosthetics and the cameras can be spoofed which is why this technique is less preferred. Same is considered for voice recognition system.Voice of every individual is not same when talking about the pitch,bass,intensity of the voice. But in the age of technology and AI, spoofing has become very easy with the help of software used to change voice. Voice recognition is therefore not preferred for security as people can change their voice and fool the system through technology. Also with age vocal cords of human being changes and therefore the system fails to recognize the person. Last in the queue according to the author is gait recognition system which is quite costly because a lot of cameras and monitors are needed for proper identification and the administrator also needs to be given proper training to run the system and identify the person.

CONCLUSION AND FUTURE SCOPE

In this paper we have explained 6 biometric techniques, their benefits, how these techniques work and their drawbacks too. The results of these techniques are quite accurate but can be spoofed and stolen. Recently in a report of Accenture, the company claimed that no biometric system is impenetrable and can be hacked as the hackers are now preying on the new biometric technologies. According to Accenture the most preyed biometric techniques are fingerprint recognition technique and face recognition technique.[25] Also in U.S. happened the biggest fingerprint hack in which 5.6 million people's fingerprint were stolen from OPM which is federal government's human resource department.[26] The solution proposed after this was cancellable biometrics which is a much more secure option as it does not save the fingerprint for example in original but creates multiple copies of the fingerprint with distortion performed on it and creates templates of these and these templates are stored in database which is afterwards compared with the user data. Cancellable biometrics was proposed by Bolle et al. in 2002 and has been growing since then.[27].

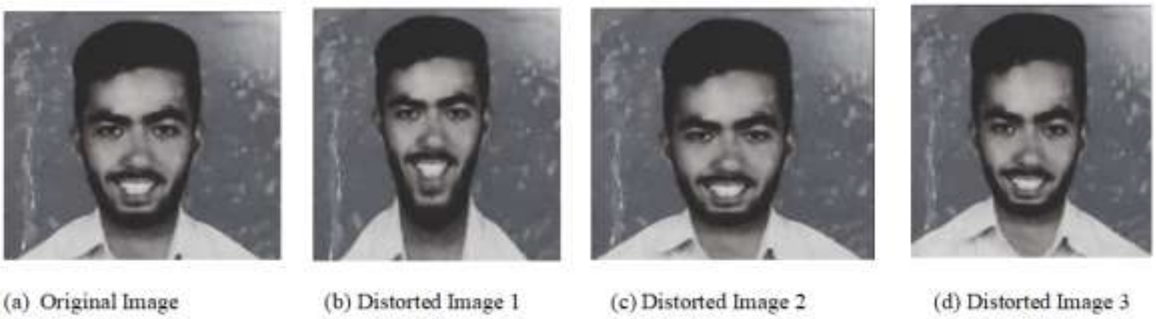
(a) Original Image
(b) Distorted Image 1
(c) Distorted Image 2
(d) Distorted Image 3

Figure 6. First image (a) is the original image of an individual whereas the other three image (b), (c) and (d) are distorted images

Earlier if the fingerprint was stolen there was no option for generating another fingerprint but with cancellable biometrics if the user thinks his fingerprint is hacked or is stolen he can issue another template of his fingerprint. But in cancellable biometrics it is very necessary that no two applications use the same template of one fingerprint. This will make hacking of the fingerprint easier. For cancellable biometrics it was not easy to make an algorithm which is non-invertible, which means once the fingerprint is distorted, original image cannot be acquired from the distorted image. Multiple number of templates need to be issued on the same trait, so that there is different template for every application. This is the only solution which the author thinks can secure data and privacy of the user.

REFERENCES

1. K. Porter, "Biometrics and biometric data: What is it and is it secure?", Us.norton.com, 2019. [Online]. Available: https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html. [Accessed: 01- May- 2019]
2. K. CH, "Various Biometric Authentication Techniques: A Review", www.omicsonline.org, 2019. [Online]. Available: https://www.omicsonline.org/open-access/various-biometric-authentication-techniques-a-review-2155-6180-1000371-94978.html. [Accessed: 01- May- 2019]
3. S. Mayhew, "History of Biometrics", Biometric Update, 2019. [Online]. Available: https://www.biometricupdate.com/201802/history-of-biometrics-2. [Accessed: 01- May- 2019]
4. Dharavath, K.; Talukdar, F.A.; Laskar, R.H., "Study on biometric authentication systems, challenges and future trends: A review," in Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on , vol., no., pp.1-7, 26-28 Dec. 2013
5. Kataria, A.N.; Adhyaru, D.M.; Sharma, A.K.; Zaveri, T.H., "A survey of automated biometric authentication techniques," in Engineering (NUiCONE), 2013 Nirma University International Conference on , vol., no., pp.1-6, 28-30 Nov. 2013 Ross, S. Dass, and A. K. Jain, "A deformable model for fingerprint matching", Journal of Pattern
6. Recognition, Elsevier, Volume 38, No. 1, Jan. 2005, pp. 95–103.
7. "Sir William Herschel, 2nd Baronet", En.wikipedia.org, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Sir_William_Herschel,_2nd_Baronet. [Accessed: 01- May- 2019]
8. T. Matsumoto, H. Hoshino, K. Yamada, and S. Hasino, "Impact of artificial gummy fingers on fingerprint
9. systems", In Proc. of SPIE, Volume 4677, Feb. 2002, pp. 275–289.
10. Gökberk B., Salah A. A. and Akarun L., "Rank-based decisionfusion for 3D shape-based face recognition",
11. Audio-andVideo-Based Biometric Person Authentication, Springer,1019-1028 (2005)
12. Supriya D. Kakade,"A Review Paper on Face Recognition Techniques",International Journal for Research in Engineering Application & Management (IJREAM),Vol-02, Issue 02, MAY 2016
13. Adams W. K. Kong, David Zhang, Mohamed S. Kamel, "An Analysis of IrisCode", IEEE transactions on image processing, vol. 19, no. 2, pp 552,2010.
14. R. Roizenblatt, P. Schor et al. Iris recognition as a biometric method after cataract surgery. Biomed Eng Online. 2004; 3: 2
15. Martin, Zach (2011-03-23). "Biometric Trends: Will emerging modalities and mobile applications bring mass adoption?". SecureIDNews. Retrieved 2013-07-14.
16. Nisha,Voice Recognition Technique: A Review,International Journal for Research in Applied Science & Engineering Technology (IJRASET),Volume 5 Issue V, May 2017,pp. 263
17. Julia Kollewe (February 19, 2016). "HSBC rolls out voice and touch ID security for bank customers | Business". The Guardian. Retrieved February 21, 2016
18. Vineeta Malik , Anil Arora,A Review Paper on Signature Recognition,International Journal for Research in Applied Science & Engineering Technology (IJRASET),Volume 3 Issue VI, June 2015,pp 670-671.
19. Rapanjot Kaur , Gagangeet Singh Aujla,Review on: Enhanced Offline Signature Recognition Using Neural Network and SVM,International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, pp. 3649.
20. Changsheng Wan,Li Wang,Vir V. Phoha,A Survey on Gait RecognitionACM Computing Surveys (CSUR),Volume 51 Issue 5, January 2019,Article No. 89
21. "Facial recognition system", En.wikipedia.org, 2019. [Online]. Available:https://en.wikipedia.org/wiki/Facial_recognition_system. [Accessed: 01- May- 2019]
22. "Iris recognition", En.wikipedia.org, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Iris_recognition. [Accessed: 01- May- 2019]

23.]A. Tiwari, S. Kesipeddi and S. Jagda, "History of Voice Recognition", Tips on Transcription and Audio to Text Conversion, 2019. [Online]. Available: http://www.happyscribe.co/blog/history-voice-recognition/. [Accessed: 01- May- 2019]
24.]S. Mayhew, "History of Biometrics", Biometric Update, 2019. [Online]. Available: https://www.biometricupdate.com/201802/history-of-biometrics-2. [Accessed: 01- May- 2019]
25. "Gait analysis", En.wikipedia.org, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Gait_analysis#History. [Accessed: 01- May- 2019]
26. L. Masupha, T. Zuva and S. Ngwira, "A Review of Gait Recognition Techniques and their Challenges", Academia.edu, 2015. [Online]. Available: https://www.academia.edu/13580680/A_Review_of_Gait_Recognition_Techniques_and_their_Challenges. [Accessed: 01- May- 2019]
27.]A. Hudson, "Biometric fraud: A new generation of hacker - SecureIDNews", SecureIDNews, 2013. [Online]. Available: https://www.secureidnews.com/news-item/biometric-fraud-a-new-generation-of-hacker/. [Accessed: 02- May- 2019]
28. M. Koren, "The OPM Hack Continues to Be Worse Than Everyone Thought", The Atlantic, 2015. [Online]. Available: https://www.theatlantic.com/technology/archive/2015/09/opm-hack-fingerprints/406900/. [Accessed: 02- May- 2019]
29. Teoh Beng Jin and L. Meng Hui, "Cancelable biometrics", scholarpedia, 2010. [Online]. Available: http://www.scholarpedia.org/article/Cancelable_biometrics. [Accessed: 02- May- 2019]