e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

FUTURE OF CYBERSECURITY: A STUDY ON BIOMETRIC SCANS

Gourav Sharma[*1], Gunjan Patidar[*2], Hritik Vishwakarma[*3], Dheeraj Shringi[*4]

[*1,2,3]Student, Department of Computer Science and Engineering, Acropolis Institute of Research and Technology, Indore, Madhya Pradesh, India.

[*4]Proffesor, Department of Computer Science and Engineering, Acropolis Institute of Research and Technology, Indore, Madhya Pradesh, India.

ABSTRACT

Biometrics is statistical analysis of people's unique behavioral characteristics. The technology is used for CYBERSECURITY. The basics of biometric authentication is that to stop the security breaches by analyzing persons unique behavioral characteristics. The term biometrics is derived from the Greek word's *"bios"* meaning life and *"metricos"* meaning to measure. It refers to measurements of physical and biological characteristics of the human body. In this paper we have studied some biometric method such as facial recognition, iris recognition, Retinal Recognition, voice recognition.

Keywords: Biometrics, Cybersecurity, Biometric Scan, Retinal Scan, Iris Scan, Gait, Voice Recognition.

I. INTRODUCTION

The term biometrics is derived from the Greek words *"bios"* meaning life and *"metricos"* meaning to measure. It refers to measurements of physical and biological characteristics of the human body. It is based on the fact that each person has some characteristics which are unique and every person can be accurately distinguished by those intrinsic physical or behavioral traits. Some of those characteristics are fingerprints, voice patterns, facial features, hand geometry, DNA, retinal shape, vein pattern etc.

Biometric authentication, also known as realistic authentication is a system which enables us to identify a person based on some of its physiological(static) and behavioral(variable) characteristics.

Biometric scan is a method which involves the use of a device (mostly a scanner) to verify the identity of a person based However, the system collapsed in 1903 when 2 criminals, later determined as twins had nearly the same physical measurements. Even after the failure of his system, Bertillon went on and is widely credited to be the first person who explored fingerprint and iris scanning but only in theory.

Fingerprints as authentication were first proposed by Dr Henry Faulds in 1880 when he saw fingerprints of potter on a pottery. He suggested in a paper to use fingerprints as a method to identify criminals. Nearly 10 years later, Sir Francis Galton, who was well-versed with Faulds' research, explored the idea of unique ridges in a fingerprint. But 1896 proved to be a dawn of the era of fingerprints when Sir Edward Henry, after consulting Sir Galton, came up with The Henry Classification System in which records of fingerprints of criminals were stored, identified and classified.

The technology of facial recognition was initially pioneered by Woody Bledsoe, Helen Chan Wolf, and Charles Bisson in 1964 as part of their collective study on pattern recognition intelligence. After Bledsoe left the study, it was continued by Peter Hart, who made a major breakthrough in 1965 when his system consistently outperformed humans in identifying human faces from a database of 2,000 photos. The technology has now evolved to a great extent as today we have better resolution cameras and larger data sets.

Despite the fact that iridology dates back to the time of Greece and Egypt, the advancement of technology in the field is fairly new. The idea is said to be first proposed by Frank Burch, an eye specialist, in 1939. The modern pioneer of this technology is John Daugman, who developed and patented the first algorithms for computer-aided identification of iris patterns in 1994. Although the technology has improved to a great extent now but the science behind it is still derived by Daugman's algorithm. on his/her one or the other biological characteristics

Biometric recognition offers a promising approach for security applications, with a remarkable number of advantages over the classical methods which have been used since ages, which depend on something you have (key, card, etc.), or something you know (password, PIN, etc.).

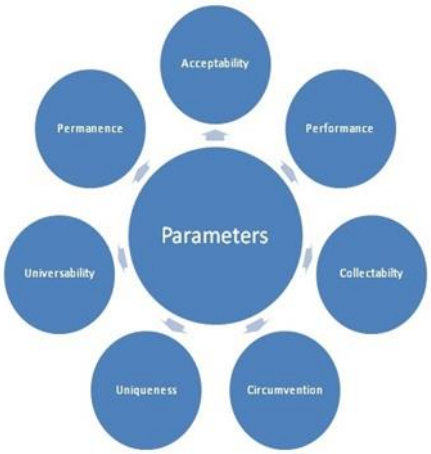
e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

II. EVOLUTION/LITERATURE REVIEW

Biometrics as a security measure has evolved to such a great extent with the time that we can say it has turned from novelty to necessity. A 31,000-year-old cave has the marks of handprints suggesting that even at that time fingerprints were considered to be a factor of authentication. Chinese parents used fingerprints and footprint to differentiate their children from one other. This adaptation of biometrics goes on for centuries until it was spread into the real world by Alphonse Bertillon.

In 1870, Bertillon, a French police officer was tired of having no proper system to sort criminals. He came up with a method named Anthropometries, which was a set of body measurements that reportedly had a failure rate of only one in 286,435,456. Law enforcement all around the world were quick to adopt this method.

Factors of Biometric Security



Study of Different Biometrics

Facial Recognition

What is it?

Facial recognition is a way of recognizing facial features of a person through technology. A facial scanner uses deep learning algorithms to match a face captured live or in an audio or video and compare it to the database.

Every face has unique landmarks which makes up the peaks and valleys of a face. These landmarks are called nodal points and according to Face It there are 80 like, distance between the eyes, the width of the nose, depth of the eye sockets, the shape of the cheekbones, the length of the jaw line, etc. These nodal points are stored as a mathematical code called as face print. When a software recognizes a face it actually compares this mathematical code stored in the database to the face print of the face it wants to recognize.

The newest trend in facial recognition is doing it in a 3-dimensional way. 3-D face recognition is preferred more as it is more accurate. While using 2-D face recognition, the face of the person has to be at least 35 degrees turned to the camera whereas 3-D face recognition can detect a face even at 90 degrees.

How does it work?

1. Detection: One can acquire a 2-D image by digitally scanning a photograph or by capturing a live video image(3-D).
2. Alignment: After the face is detected, the head position, pose and size are determined.
3. Measurement: The system then measures the curves of the face on a sub-millimeter (or microwave) scale and creates a template.
4. Recognition: The templates are the face prints which are given a unique numerical code.
5. Matching: The derived code is matched with the system's database.
6. Verification or Identification: When the authorities want to match the face in a particular database or "verify" the person, then our goal is verification (1:1). However, if one wants to "identify" the person then our goal is to identify the face by comparing it to all the available databases (1: n).

Applications:

The following uses facial recognition technology:

1. U.S. government at airports
2. Mobile phone makers in products
3. Colleges in the classroom
4. Social media companies on websites
5. Businesses at entrances and restricted areas
6. Religious groups at places of worship
7. Retailers in stores

Advantages and Disadvantages:

Facial recognition supports security on all basis, with its help we can easily identify burglars, thieves etc. The processing of the system is very fast and accurate which saves time. It is a non-contact process so people need not to worry about germs and bacteria.

However, facial recognition system requires a high initial cost of installation because it requires high resolution cameras to ensure accuracy and security. People have raised the concerns of privacy breach which is a real issue. The system requires massive data sets which, in return, require massive space to store that data. Also, if one is using 2-D facial recognition then he should keep in mind that in order to recognize a face, the face needs to be at least 30 degrees facing the camera.

Security and Facial Recognition:

There's no denying the fact that facial recognition has proved to improve a patch of security in the world of technology. The technology has no room for human error and facial recognition's no-contact nature has allowed people to be recognized even in crowded places. Authentication becomes easy and secured when facial recognition is used.

In a recent survey conducted on US residents, 54 percent of Americans plan to use face recognition to protect their personal data or already own a device that uses face recognition. Nearly two thirds (64 percent) of Americans think security personnel guarding airports, concerts, sporting events and other public areas should be allowed to use face recognition to help recognize terrorists and prevent crime. 77 percent of Americans think that security guarding airports and tourist attractions are not likely to remember the names and faces of potential terrorists on a watch list without face recognition

Iris Recognition

What is it?

In human eye, iris is the ring-shaped structure which is present around the pupil. It is responsible for controlling the size of pupil and gives color to the eye. It closes the pupil or contracts its size when the light entering is high and does the opposite in the case of low light.

Iris recognition is the process in which the unique patterns in a person's iris are recorded by taking high quality photographs of the iris. This is done by using infrared or near-visible light. In the iris, there are certain unique patterns in the form of colored rings and many others which are not visible with bare eye. So, the iris scanners use invisible infrared light to detect, scan and record all those patterns which are unique for each person and remain the same throughout adult life. In order for the iris recognition or iris scanning to work properly and produce accurate results, the person must be within a few meters of the camera.

Iris recognition is used mainly for security purpose but some countries have implemented this technique at the airports and government sites as well. Although its use at airports is not as popular in most parts of the world but countries like Canada and the USA are using it to secure border crossings.

How does it work?

If we look at the human eye very closely then we can notice that the iris has tiny lines and waves all over its surface. The iris scanner reads this pattern and translates it into code. This digital code is then saved into the database.

When the same iris is scanned by the iris scanner, it again produces the same digital code which is again compared to all the already present codes in the database and when we get a successful match, the identity of a person is known to us by the use of none other than the Iris Recognition.

Applications:

1. In Cell phones for authentication
2. In workplaces
3. For secure border crossings
4. Banks and Financial Organizations
5. Ticketless Travel

Advantages:

1. Iris Recognition systems have been proved to be very accurate.
2. These are highly scalable even for bigger sized projects.
3. Unlike fingerprint, iris recognition is much more hygienic.
4. Iris scanners also detect the movement of the iris which requires the liveness of the individual and hence increasing security factor.

Disadvantages:

1. Distance is the first disadvantage. It cannot be performed at a distance greater than a few metres.
2. High cost of iris scanners is another disadvantage of iris scanner.
3. Iris recognition cannot be performed if the person is in movement continuously i.e. the person should be stationary for the scanner to work properly.
4. Since this technology uses infra-red light, continuous and long-term use of this technology can harm a person's eye.

Voice Recognition

What is it?

The voice recognition system is used to identify and authorize a person's identity by verifying his voice from the set of database available. This system uses voice prints which are basically a set of characteristics which are helpful in uniquely identifying the voice of an individual. A voice print contains a voice sample, a mathematical formula and a graphical representation.

Unlike the belief of majority of people, a voice recognition system does not make and analyze the voice of the user by making waveforms like the ones we see in oscilloscope. Instead the system uses a spectrogram which makes a graph of voice frequency against time.

A voice recognition system usually makes the user say some specific sentences or words through which it can identify any word you will ever speak. An Automatic Speech Recognition [ASR] software is used for this work.

The physiological component is based on the persons' vocal tract. The voice recognition system recreates this component because as no one can have similar vocal tract hence they can't have similar voice imprint too. Another component is the behavioral component which is based on the physical moments of the jaw, tongue and larynx.

How does it work?

1. An Analog-To-Digital Convertor (ADC) is used to convert the analog signals to the digital data so that the computer can understand what is being said. It samples or digitizes the sound at frequent intervals with the measurement of waves.
2. After making the sound "readable" unwanted noises are filtered out and the sound is normalized.
3. Analysis of the sound is done by comparing the said words with the ones stored in data dictionaries made by the system of the user.

This working is the simplest among all the others because it is done for a specific person. If the magnitude of people increases then the complexity of the system increases with it and so it becomes more difficult to recognize voices clearly.

Applications:

1. In work places, voice recognition system can be used to increase efficiency and break the norm of having some tasks performed specifically by humans.

2. In banking, the system will be available to the customer in need 24*7 and it will also decrease the workload on bank employs.
3. User friendliness of the search engines have increased since this system came into use.
4. Automated identification is possible.

Advantages:

1. It allows user to operate the computer with just his voice.
2. One can dictate commands which result in hassle free communication.
3. The speed of any work done by this system is increased drastically.
4. Eliminates spelling problems.

Disadvantages:

1. One has limited vocabulary when it comes to voice recognition system.
2. Memory is required to store data in voice format.
3. Noise interference can reduce the quality of the voice notes.

Retinal Recognition

What is it?

Retina is basically a thin multilayered tissue in the back of the eye. It contains a special type of cells called photoreceptors. The process of conversion of light into signals that can be interpreted by the brain is carried out by the retina. It is actually a complex structure of blood vessels. This structure can be so complicated that even identical twins do not share a similar pattern, the retina of each person is unique.

Although it has been scientifically proven that the retina patterns can get altered in diabetes, degenerative disorders of the retina, the retina remains unchanged from birth to death. This is the reason this method of identity verification remains to be one of the most reliable, most accurate and widely used around the globe.

Retinal Recognition is a subfield of ocular biometrics and is an identity verification technique that uses unique retinal patterns (discussed earlier) to identify/distinguish a person. For this purpose, we use a Digital Retinal Camera and the eye is positioned in front of the retinal scanner at a capture distance which is from 8cm to 1m. The idea for retinal identification was first conceived by Dr. Carleton Simon and Dr. Isadore Goldstein.

How does it work?

1. First the person is supposed to place his eye in front of the retinal scanner at a very less distance of about 8cm.
2. When he/she looks into the scanner for about 10 to 15 seconds, an invisible low energy infrared beam in cast into the eye.
3. This light ray then traces the unique pattern made up by the blood vessels in the retina.
4. What happens is that blood vessels absorb some of the infrared light and reflects some back. This is the phenomenon of Partial Internal Reflection.
5. Hence, the amount of light reflected depends on the amount of blood vessels in the eye.
6. The scanner measures this reflection at 320 points along the beam path and assigns an intensity grade between zero and 4,095. The resulting numbers are compressed into an 80-byte computer code.
7. Now the different points of thickness and path are translated into a sequence of bar code.

After carrying out this process, all the information is stored in a database and when the scanning is done again, the scan results are compared to the previous results stored in the database.

Applications:

1. Retinal Scanners can easily detect diseases such as Malaria, AIDS, Chicken Pox and Lyme Disease because they first appear in the eye.
2. Finance and banking: Iris recognition technology is being used in banks and financial organizations, replacing the pin based, and password-based systems.
3. Immigration and Border Control: Rising security concerns has led to radical changes in airport security systems all across the world.

4. Public Safety: For more than a century, law enforcement has been using biometric technology to track and identify criminals, helping to enhance public safety and facilitate justice.
5. Hospitality and Tourism: Tourism and hospitality industry has also started taking the first steps toward biometric iris recognition-based authentication facilities.

Advantages:

1. The texture of the iris remains incredibly stable, it usually remains unchanged throughout its life, except in extreme cases of eye injury.
2. High accuracy is achieved by using this type of identity verification.
3. Retinal scans are about 70 times more accurate than iris scans and 20,000 times more accurate than fingerprint-based methods.
4. Lowest or no margin of error.

Disadvantages:

1. Users of retinal scans complain of discomfort from the technology as they must lean in and keep their eye close to the machine for 30 seconds in order for a scan to be accurate.
2. It has been observed that regular retinal scans for a long period of time can damage vision of human eye.
3. According to the SANS Institute (an Information Security Company report, users of the same technology have reported that it is uncomfortable and intrusive.

III. RESULTS AND DISCUSSION

In the study of different biometrics methods, we have found that every method has its own importance its own advantages and disadvantages but we found some key results that are mentioned below:

1. Fingerprint scanning is most commonly used biometric security method worldwide.
2. Gait Analysis is a Breakthrough of Modern Biometrics
3. Retina recognition is considered as most secured biometrics

IV. CONCLUSION

In this paper, we have carefully studied and concluded different biometric methods, their applications, advantages and disadvantages. We came to the conclusion that there is no “single best” biometrics method for security every method works best according your need and your security concern because the selection of your biometrics method will depend on the major factors like its accuracy, anti-spoofing capabilities, acceptability, cost effectiveness, budget, etc. Based on these factors, you can easily decide which biometrics is best for you.

ACKNOWLEDGEMENTS

We as the authors would like to give a special vote of thanks to the reviewers of this paper for their valuable advice to improve this paper. We also want to thank Prof. Dheeraj Shringi for his invaluable guidance and support.

V. REFERENCES

[1] BIOMETRIC SECURITY TECHNOLOGY 1 Marcos Faundez-Zanuy Escola Universitaria Politècnica de Mataró Avda. Puig i Cadafalch 101-11108303 MATARO (BARCELONA) SPAIN
[2] Anil K Jain, Arun Ross and Salil Prabhakar, “An Introduction to Biometric Recognition,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no.1, pp. 1-29, 2004.
[3] Arun Ross and Anil Jain, “Information Fusion in Biometrics,” Pattern Recognition Letters, vol. 24, pp. 2115-2125, 2003.
[4] https://geek.digit.in
[5] https://www.makeuseof.com/
[6] https://www.biometricsinstitute.org/
[7] https://us.norton.com/
[8] https://www.bayometric.com
[9] http://www.m2sys.com/blog/