International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Biometric system - A Review on its Security

Pradyumna Kumar[1], Yakesh Dogra[2], Naveen Bansal[3]

[1]Student, Dept. of computer Application, CSB, CGC Jhanjeri
[2,3]Assistant Professor, Dept. of computer Application, CSB, CGC Jhanjeri

Abstract
Due to its liability, biometric technology is currently the most in-demand trend. Because of need of largely secured security systems and to cover sensitive documents and valuables, we're also using the biometrics astronomically. Biometrics is measure of natural or behavioural features which are used for identification of individualities. utmost of these features are inherit and can not be guessed or stolen. It's a system that takes an existent's physiological, behavioural or both traits as input, analyses it and identifies the individual as licit or vicious stoner. Another point of biometric is its effectiveness and Convenience of use Biometrics are always with you and can not be lost or forgotten, delicate to steal or impersonate Biometrics ca n't be stolen like a word or key can. It's veritably easy to use and handle. Biometric authentication also includes iris recognition, retinal checkup, fingerprints and voice command. It generally refers to the processes which are used to fete and distinguish persons on the base of their physical and behavioral characteristics. The types and operation of biometric systems are reviewed in this study. Image conformation, Image Processing, and Image Matching are the three basic methods used in biometrics.

Keywords: Fingerprints scanning, Face recognition, DNA, Iris recognition, Signature scanning.

1. Introduction

Biometric refers to the measurement and analysis of unique physical or behavioral characteristics of an individual, which can be used to identify them. Biometric data can be obtained from various parts of the body, such as fingerprints, facial features, iris or retina patterns, voice, and handwriting, among others.
Biometric information is specific to each person and can be used to accurately confirm their identification. Due to its dependability, biometric technology has grown in favour in recent years and convenience. Biometric authentication is being used in various applications, such as unlocking smartphones, accessing secure facilities, and processing travel documents at airports.

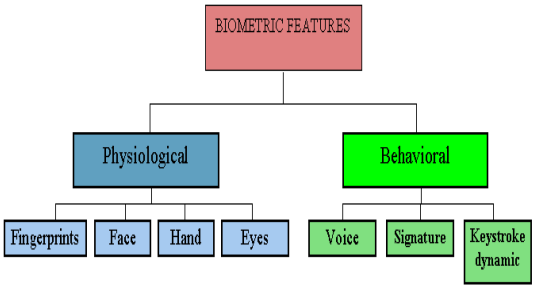

Figure 1. Classification of Biometric system.

Biometric system

All biometric identifier scan be divided into two big groups:

1) Physiological.

2) Behavior.

Physiological or behavioral characteristics: Physiological biometric characteristics are physical characteristics of an individual that are unique to them and cannot be changed easily. Hand geometry, DNA, iris or retina patterns, fingerprints, and facial features are a few examples of physiological biometric traits.

Behavioral biometric characteristics, on the other hand, are traits that reflect an individual's behavior or actions. Examples of behavioral biometric characteristics include voice patterns, typing rhythm, signature dynamics, and gait recognition.

Both physiological and behavioral biometric characteristics can be used to verify an individual's identity, and the choice of the characteristic to be used depends on the application and the level of security required. Some biometric systems use a combination of both physiological and behavioral characteristics to enhance the accuracy of identification.

Fingerprint Scanning: Fingerprint scanning is a biometric technology that uses a person's unique fingerprint patterns to authenticate their identity. Fingerprint scanning is a popular biometric system due to the reliability and ease of use of fingerprint data.

Fingerprint scanning involves capturing an individual's fingerprint image using a specialized scanner, which may use optical or capacitance-based sensors. The scanner captures the ridges and valleys of the fingerprint, which are then analyzed by the system to create a unique fingerprint template. After that, to confirm the person's identification, the fingerprint template is checked against a database of well-known templates.

Fingerprint scanning is commonly used in various applications, such as access control to secure facilities, unlocking smartphones and laptops, and processing travel documents at airports. Fingerprint scanning is considered a secure biometric technology, as the chance of two individuals having the same fingerprint is very low, making it difficult to forge or fake a fingerprint.

Figure 2. Example of Fingerprint Scanning.

Face Recognition: Face recognition is a biometric technology that uses a person's facial features to authenticate their identity. Face recognition involves capturing an image of a person's face using a camera, and then analyzing the unique facial features to create a digital template. To confirm the person's identity, the template is then compared to a database of recognized templates.

Face recognition technology uses various techniques to capture and analyze facial features, such as geometric features, skin texture, and facial landmarks. The technology can work in different lighting conditions and with varying angles and expressions of the face.

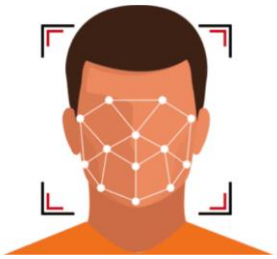

Figure 3. Example of Face Scanning.

DNA: DNA recognition is the process of using an individual's DNA to authenticate their identity. DNA recognition uses certain areas of an individual's DNA to build a genetic profile that can be matched to a database of other known profiles to authenticate the identification of the subject.

DNA recognition is a powerful biometric technology that has high accuracy and reliability, as DNA is unique to each individual and does not change over time. DNA recognition can be used in various applications, such as forensic investigations, paternity testing, and identifying human remains.

A cheek swab, blood sample, or other biological specimen can be used to get a DNA sample from the person for DNA recognition. The DNA sample is then analyzed in a laboratory using various techniques, such as polymerase chain reaction (PCR) or capillary electrophoresis (CE), to create a genetic profile. The individual's identity is then confirmed by comparing the genetic profile to a database of known DNA profiles. DNA recognition is a secure biometric technology, as the chance of two individuals having the same DNA profile is extremely low, making it difficult to forge or fake DNA data. However, DNA recognition has some concerns related to privacy and security, as the collection and storage of DNA data could lead to the possibility of data breaches or misuse of the data.

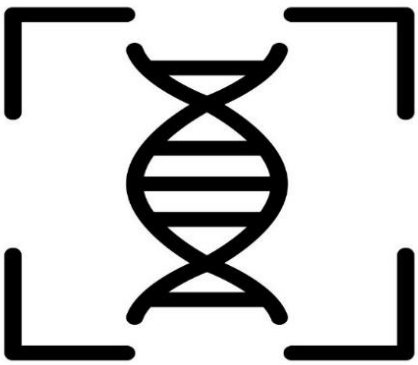

Figure 4. DNA Scanning.

Hand Geometry: Hand geometry recognition involves capturing an image of an individual's hand using a specialized scanner, which measures various physical characteristics such as finger length, hand size, and the distance between fingers. The hand geometry scanner captures an image of the hand and creates a digital template that is unique to the individual. The template is then compared to a database of known templates to authenticate the identity of the individual.

Hand geometry recognition is commonly used in various applications, such as access control to secure facilities, time and attendance systems, and point-of-sale transactions. Hand geometry recognition is considered a reliable biometric technology, as the physical characteristics of an individual's hand are unique and do not change significantly over time. Hand geometry recognition is also less invasive than some other biometric technologies, such as DNA or retina scanning. However, hand geometry recognition does have some limitations. The accuracy of the system can be affected by factors such as hand injuries or deformities, as well as variations in hand positioning during the scanning process. Additionally, some individuals may be uncomfortable with the physical contact required for hand scanning

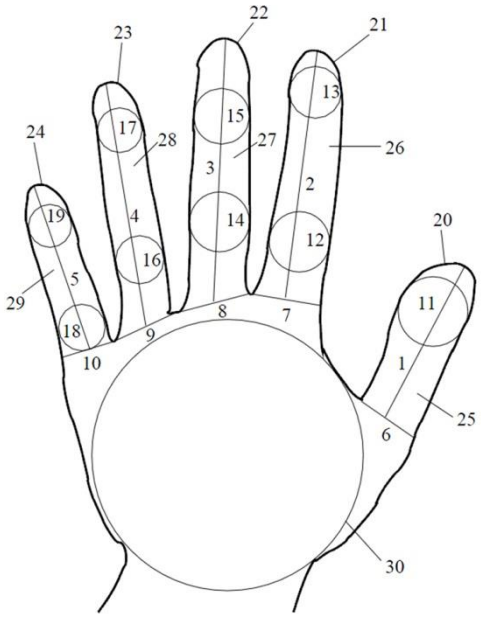

Figure 5. Example of Hand Scanning.

Iris Recognition: Iris recognition is a biometric technology that confirms a person's identity by using the distinctive features of their iris. The iris, which surrounds the pupil and is the colored portion of the eye, has distinctive patterns on each person.

Iris recognition involves capturing an image of the iris using a specialized camera, which uses near-infrared light to create a high-resolution image. The unique iris patterns are then extracted from the iris image through analysis, and a digital template is made. This template is then compared to a database of other known templates to confirm the person's identification.

Iris recognition is considered a highly accurate biometric technology, as the patterns in the iris are unique to each individual and do not change over time. Iris recognition can also work in various lighting conditions and with individuals who wear glasses or contact lenses. Iris recognition is commonly used in various applications, such as access control to secure facilities, border control, and national ID programs. However, iris recognition technology can be more expensive and complex to implement compared to some other biometric technologies, such as fingerprint scanning. Additionally, concerns related to privacy and security have been raised regarding the collection and storage of iris data.

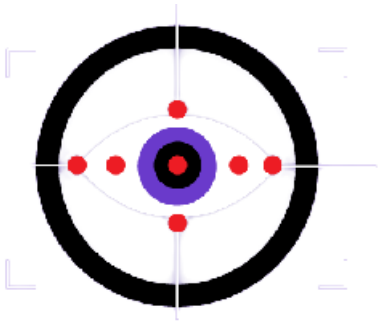

Figure 6. Example of Iris Scanning.

Voice Recognition: Voice recognition, also known as speech recognition, is a technology that enables machines to recognize and interpret spoken language. It involves converting spoken words into digital text, which can then be processed by a computer or other devices to perform various tasks.

Voice recognition technology works by using a combination of hardware and software to capture and analyze an individual's speech. The hardware typically includes a microphone or other audio input device, which is used to capture the spoken words. The software then processes the audio input, using complex algorithms to identify individual words and interpret the meaning of the spoken language.

Voice recognition technology has many applications, including in voice assistants such as Siri and Alexa, transcription and dictation software, and automated customer service systems. It is also used in accessibility technology to enable individuals with disabilities to use computers and other devices.

However, voice recognition technology is not always perfect, as it can struggle to accurately interpret speech in noisy environments or with heavy accents. Additionally, voice recognition technology can raise concerns around privacy and security, as spoken language can contain sensitive information that may be vulnerable to hacking or interception.

Dragon Dictate, the organization's first consumer speaker recognition tool, debuted in 1990. IBM released the first voice recognition device that could recognize continuous speech in 1996.

Figure 7. Voice Scanning.

Key Stroke: A biometric method called keystroke recognition, often referred to as keystroke dynamics, uses the distinctive patterns of a person's typing behaviour to validate their identification. Capturing and analysing several aspects of a person's typing behaviour, such as typing speed, rhythm, and keystroke patterns, is known as keystroke recognition.

Keystroke recognition technology works by capturing an individual's keystrokes, usually as they type in a username and password or other text-based input. The keystroke data is then analyzed to create a

biometric template that is unique to the individual. This template is then compared to a database of known templates to authenticate the identity of the individual.

Keystroke recognition is considered a non-invasive and low-cost biometric technology, as it does not require specialized hardware or physical contact with a device. It is commonly used in various applications, such as remote authentication for online banking and security systems.

However, keystroke recognition technology can be less accurate and reliable compared to some other biometric technologies, as typing behavior can be affected by factors such as mood, fatigue, and physical condition. Additionally, keystroke recognition technology can raise concerns around privacy, as the capture and storage of keystroke data could be perceived as intrusive.

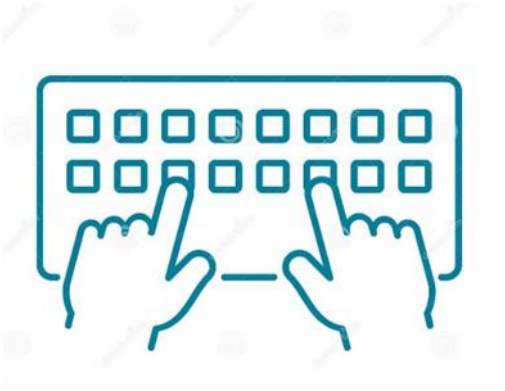

Figure 8. Example of Key Stroke scanning.

Signature Scanning: A biometric technique known as "signature scanning" includes taking a picture of a person's signature and using it to verify their identification. The signature can be captured using a specialized scanner or camera, which creates a high-resolution digital image of the signature.

The image is then analyzed using specialized software that extracts unique features such as stroke width, pressure, and timing to create a biometric template unique to the individual. To confirm the person's identity, this template is then compared to a database of recognised templates.

Signature scanning is commonly used in various applications, such as banking transactions, document signing, and access control to secure facilities. It is considered a convenient biometric technology, as it does not require physical contact or specialized hardware. However, signature scanning can be less accurate compared to some other biometric technologies, as signature patterns can vary depending on the medium used for signing, such as paper or digital devices. Additionally, signature scanning technology can raise concerns around privacy and security, as it involves collecting and storing personal signature data.

Figure 9. Signature Scanning.

Working of Biometric System: The working of a biometric system generally involves the following steps:

- Enrollment: During the enrollment process, an individual's biometric data is captured and stored in a database. This may involve scanning fingerprints, taking a photo of the face or iris, recording voice patterns, or capturing other physiological or behavioral characteristics.
- Pre-processing: The captured biometric data is then pre-processed to extract the relevant features, such as the unique ridge patterns in a fingerprint, or the distinctive facial features in a photograph.
- Feature extraction: The extracted features are then converted into a mathematical representation known as a biometric template, which is unique to the individual.
- Template storage: The biometric template is stored in a database along with other identifying information, such as name, date of birth, and other relevant data.
- Authentication: A person's biometric information is taken and compared to a biometric template that has been stored whenever they try to enter a system or facility that requires biometric identification. Access is allowed to the individual if the two match. If not, access is denied.
- System update: The biometric system may be periodically updated to incorporate new templates, remove outdated data, and improve overall accuracy.

From physical access control to banking and electronic voting, biometric technologies may be utilised for a variety of tasks. They offer a high degree of accuracy and security, as biometric data is unique to each individual and difficult to falsify or replicate. However, concerns around privacy and data protection must be carefully considered when implementing biometric systems.

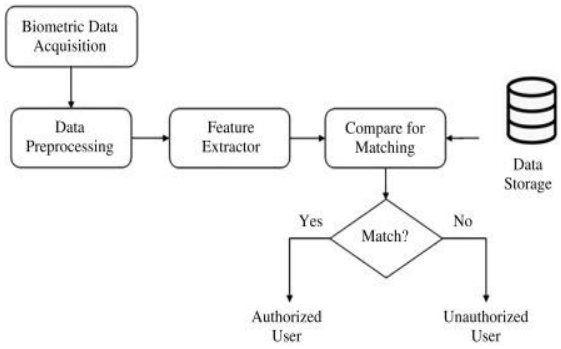

Figure 10. Working of Biometric System.

2. Work Already Done:

Asima Akber Abbasi,M.N.A. Khan and Sajid Ali Khan They have demonstrated in their work that the enforced method of eye iris discovery A biometric system is an automated identifying system based on a characteristic template or point matching. The biometric system is one of the techniques now employed as a workable identifying system. The iris detection system is one of the most trustworthy and unique biometric identification technologies. Similar tactics are used in this study to develop an iris recognition-based biometric authentication system.

Sukhwinder Singh, Ajay Jatav In their work, they have shown how the eye iris is utilised in high-security settings. The iris recognition technology serves a variety of purposes, including border control in ports and airports, access control in offices and labs, identity for ATMs, and restricted access to police

substantiation residences. This article offers a summary of the main iris recognition studies. One of the most reliable methods of identifying people was iris recognition. For accurate and secure identification, it provides enough degrees of freedom. The human body's most physically unique and information-rich component is thought to be the iris. It does work when people are wearing contact lenses or sunglasses.

Essam- EldeanF. Elfakhrany, Ben BellaS. Tawfik They have depicted ocular iris in their works. People typically use identification cards, usernames, or watchwords to help them identify themselves in a reliable and distinctive way. Even though watchwords and ID cards can be lost or stolen, They use Abhilash Sharma et al./(IJCSIT) International Journal of Computer Science and Information Technologies,Vol. 6(5), 2015,4616-4619www.ijcsit.com 4618 to define their uniqueness. People cannot lose or forget their physical qualities the way they might lose their identities or watchwords. cards, so biometric identification methods that are based on behavioural or physical characteristics are of interest. Biometric systems based on fingerprints, facial features, voice, hand shape, handwriting, the retina, and the iris, which is the one discussed in this work, have been created. Because of pre-processing, iris is a sensitive problem.

Senbhaga S They have demonstrated in their work that the iris of the eye now has a novel segmentation frame that can effectively join iris images taken under visible or near-infrared light. To reliably categorise the pixels in the eye region into iris or non-iris regions, the suggested approach takes advantage of numerous advanced order original pixel dependencies. The unified frame incorporates face and eye discovery modules to instantly provide the localised eye area from facial image for iris segmentation.

Mojtaba Najafi, Sedigheh Ghofrani In their work, they have demonstrated the eye's novel point birth system in accordance with the crest let transform for associating the handed iris images. At first, the collarets region of eye images has been uprooted following segmentation and normalisation. Additionally, we use the median sludge, histogram equalization, and the two-dimensional (2- D) Wiener sludge to improve image clarity. Finally, the double bit sluice vector is produced along with the use of crest let transfigure for rooting characteristics.

D R Prithvi, R Madhu They have demonstrated in their work that styles are more capable and reliable than singular knowledge-based methods that use an auni-modal system. The theoretical difficulties of multimodal biometric have recently gotten more and more notice due to its features and operations. They demonstrate how iris and fingerprint biometrics can be combined with a secure key to accomplish advanced performance that might not be possible with just one biometric index.

Savita Borole,Prof.S.D. Sapkal Utilizing binary-tree complex sea points and support vector machines, a novel descriptor for iris recognition is proposed.(SVM). In the experiment, some kernel functions and SVM are used as classifiers. To show the efficacy of the suggested approach, they compared it to the k-NN and Naive Bayes classifier. The support vector machine (SVM) is trained as an iris classifier using the 2D DT-CWT that is uprooted from the eye images.

Conclusion:

The biometric system may find operations in attendance system, security systems, and identification purposes and may find indeed more operations in the time to come. The current systems would be worked upon and modified for error free secure system. The delicacy situations need to be increased for effective security system. Proper selection of fashion has to be considered according to the demand. Scientific work is being carried out for future operations and progress in the biometrics.

Future scope:

Simplicity is probably where biometric protection will go in the future. The most straightforward method to provide a high position of protection is by perfecting ultramodern styles. A 3D representation of a point can be ignored, and all of its implications examined. There are many biometric applications being developed and tested right now. Still, these fingerprint technologies will be widely adopted in a few years. Soon, plastic cards will become obsolete, and point evaluations will become a daily routine.

References:

1. Senbhaga S " A Survey on Iris Segmentation using Distantly Acquired Face Images" International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 118 ISSN 2229-5518.
2. Mojtaba Najafi and Sedigheh Ghofrani "A New Iris Identification Method Based on Ridge let Transform" International Journal of Computer Theory and Engineering, Vol. 5, No. 4, August 2013.
3. D R Prithvi, R Madhu "Recognition Using Secret Key in Iris Feature Extraction and Palm Print Features" Proceedings of AECE-IRAJ International Conference, Tirupati, India, ISBN: 978-81-927147-9-0, 14th July 2013.
4. Savita Borole, Prof. S. D. Sapkal "Extraction of Dual Tree Complex Wavelet Feature for IRIS Recognition" International Journal of Advanced Research in Computer and Communication Engineering Volume 2, Issue 7, July 2013.
5. Sukhwinder Singh, Ajay Jatav "A closure looks to Iris Recognition system" IOSR Journal of Engineering (IOSRJEN) e-ISSN: 2250-3021, p-ISSN: 2278-8719 Vol. 3, Issue 3 (Mar. 2013).
6. Some website reference: weexcel, theseus.fi/bitstream, wikipedia, Image reference from google images, .nationalbiometric, Griaulebiometrics, techtarget.
7. Arnau- González, Pablo; Katsigiannis, Stamos; Arevalillo- Herráez, Miguel; Ramzan, Naeem(February 2021)." BED A new dataset for EEG- grounded biometrics". IEEE Internet of effects Journal.(Beforehand Access)(15) 12219 – 12230. doi10.1109/JIOT.2021.3061727. ISSN 2327-4662. S2CID 233916681.
8. Langston, Jennifer(8 May 2015)." Experimenters hack Teleoperated Surgical Robot to Reveal Security excrescencies". Scientific Computing. New Jersey. Archived from the original on 4 March 2016. recaptured 17 May 2015.
9. McConnell, Mike(January 2009). KeyNote Address. Biometric Consortium Conference. Tampa Convention Center, Tampa, Florida. Archived from the original on 18 February 2010. recaptured 20 February 2010.
10. Schneier, Bruce." The Internet Anonymous Forever". Archived from the original on 12 October 2011. recaptured 1 October 2011.
11. White, Anna(April 2019)." The High- Tech, Humane Ways Biologists Can Identify creatures". Smithsonian. recaptured 22 March 2019.
12. BreckenridgeK.(2005)." The Biometric State The Promise and Peril of Digital Government in the New South Africa". Journal of Southern African Studies, 312, 267 – 82
13. EpsteinC.(2007)," shamefaced Bodies, Productive Bodies, Destructive Bodies Crossing the Biometric Borders". transnational Political Sociology, 12, 149 – 64
14. PuglieseJ.(2010), Biometrics Bodies, Technologies, Biopolitics. New York Routledge

15. French National Consultative Ethics Committee for Health and Life lores(2007), Opinion N ° 98," Biometrics, relating data and mortal rights"