IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

The Future Of Identity Management: Exploring Biometric Techniques

Siji P. Joy

Asst.Professor, Department of Computer Science

Nirmala College(Autonomous), Muvattupuzha

Ernakulam District, Kerala, India

Aparna Nair

Student, Master of Computer applications (MCA), Semester 3,

Nirmala College(Autonomous), Muvattupuzha

Ernakulam District, Kerala, India

ABSTRACT

A Biometric system is a safeguard for cyber security and one's identity to ensure personal identification and authentication which revolves around pattern recognition on human behavioural or physiological traits. As the role of digitalization has risen in every nook and corner of our world, risks of thefts have increased where biometrics started shielding such valuable data. Malicious attackers now have involved to breach such highly protected data with various destructive ways. As cyber threats become increasingly sophisticated, traditional methods of identity verification and evidence collection are proving inadequate. Biometrics, which includes fingerprint analysis, facial recognition, and iris scanning and much more as explained in this paper, offers a reliable and secure means of identifying individuals and linking them to cyber activities. A compromised biometric can also result in the impossibility to use it again for security, since it cannot be changed like a password. Furthermore, the template needs to be safeguarded for the privacy of sensitive data. The paper delves into the latest advancements in biometric technologies, tools related, and the challenges associated with privacy and data security. By examining current trends and current practices, this paper aims to underscore the importance of biometrics in strengthening the field of cyber forensics and addressing the evolving landscape of cybercrime.

Keywords: Biometrics, Identification, Authentication, Biometric Characteristics, Physiological and behavioural characteristics, Eigenfaces, Direct and Indirect attacks on biometric system.

1. INTRODUCTION

Today we live in an age of finding loopholes out of security systems, where biometrics is making a reliable solution for identification and authentication of the user, for the user. A biometric system, also known as a verification or identification system, uses specific physiological or behavioural characteristics to identify an

individual which can be a fingerprint, face, palm print, iris, or signature [4]. All small details are taken into consideration to provide definiteness, errorless, accurate and reliable results. It cannot be easily manipulated and helps the user to create a hassle-free environment by not performing any particular action or even remembering keys or passwords. Most reliable of all those characteristics that comes under biometrics is iris detection. There is a lot to study and differentiate, is more complex than fingerprint analysis where it's about ridges on outer surface, iris takes its structure as a whole [1, 2]., such as arching ligaments, furrows, ridges, crypts, rings, freckles and so on.

A biometric system operates in two stages: enrolment and authentication. Enrolment involves using biometrics for extracting features from a scan and generating a template, mostly for the first time. Enrolled and extracted features are compared with features from the template to find a match and is granted access if the match is compatible to a specified threshold [2].

A biometric system works in mainly four modules: sensor, feature extraction, database and decision module [3,5]. In sensor module, images are taken from specimens in different angles and positions. There will be noise or pollutants in these images even if it is taken with the help of high-quality cameras or scanners. These noises are removed for quality enhancement in the feature module. These underlying or hidden traits are taken and added to high-capacity databases in the database module (This varies according to template size). In decision module the feature is compared to available templates for considering the threshold score to determine whether it is a match or not [5]. This is how biometric system works. This paper will provide an idea on characteristics used for biometrics, tools used and challenges faced in the field of biometrics.

2. BIOMETRIC CHARACTERISTICS

a) Physiological

i. Fingerprint Pattern

The ridges and furrows on finger surfaces are distinct from person to person. Patterns such of it which forms swirls, loops, arches, and even distance between lines are different in every case, which makes it the most common way of biometric authentication. Ridges are the elevations and furrows makes the lower layer section [6]. Being called minutiae, these are the basis of finger scanning methods. This uses top and side images parallelly to find match threshold. The length, width and height of the fingers, and / or the hand are also considered.

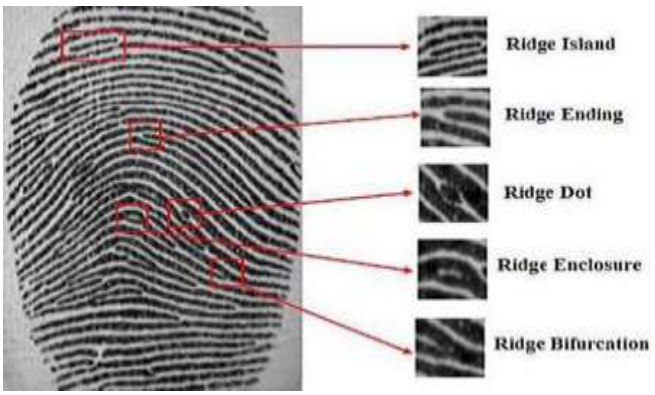

Fig 2.1[17]: Minutiae based extraction in feature recognition

ii. Iris Pattern

Professor John Daugman invented Iris recognition System developed and patented the first useful algorithms to perform this biometric recognition system. It is an automated method of biometric identification that makes use of video images of one or both of an individual's irises, which have complex patterns that are distinct, stable, and visible from a distance. This approach applies mathematical pattern-recognition algorithms to the images.[7] This is based on the creation of a digital code from the visible elements that constitute the structure of the iris, such as arching ligaments, furrows, ridges, crypts, rings, freckles among others.

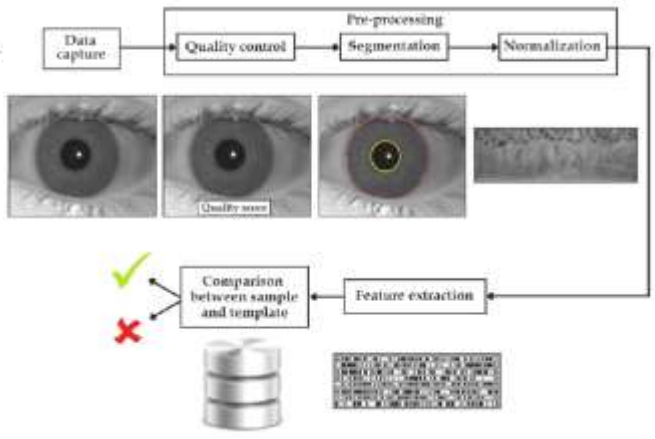

Fig 2.2: Iris pattern recognition [18] working and detection

iii. Retinal Pattern

The retina's blood vessel pattern is illuminated by a device using infrared light. Infrared light is less evasive for the user since the blood vessel pattern in the retina can "absorb" it faster than other regions of the eye tissue. The scanning equipment records the reflected light for processing throughout this imaging phase. [8] Meanwhile, distinct retinal characteristics are extracted using several methods. Following Figure is an example of retinal pattern.

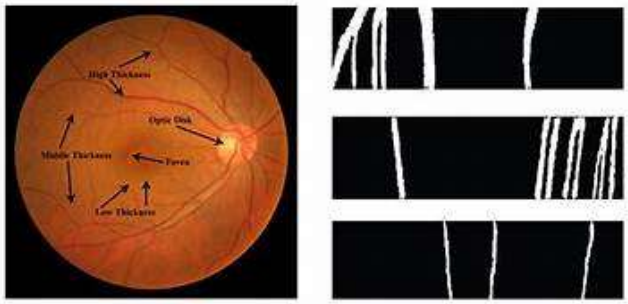

Fig 2.3: [16] Retinal pattern recognition based on multi resolution feature

iv. Face Recognition

Face recognition is intricate physiological biometrics. The matching of faces is a difficult work since there are a lot of potential variations in the face (with spectacles, expressions etc.) and external variables (such as lighting, camera angle, etc.). There are two primary methods for facial recognition: using eigenfaces or using facial measurements. The upper borders of the eye sockets, the skin around the cheekbones, and the sides of the mouth are among the parts of the face that are used for facial measurements because they are less prone to change. Eigenfaces, [1] first created at Massachusetts Institute of Technology (MIT), are two-dimensional, greyscale, normalized representations of faces.

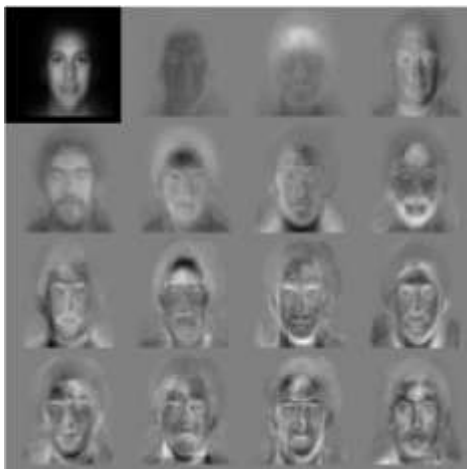

Fig 2.4:[1] Small set of eigenfaces, MIT

b) Behavioural

i. Signature Dynamics

Signature recognition biometrics involve analysing variables like acceleration, wave, speed, and velocity, as well as the signature's dynamic/static shape. Neural network technology can be integrated to identify variations in signee approaches and update the database. Practical use involves using a specialized writing device and pen connected to a centralized server for data processing.[9] However, there are constraints, such as the signature's length and the FAR (False Acceptance Rate). No single biometric technology is optimal, but a range of them, including signature recognition, can be considered "admissible."

ii. Vocal dynamics

Voice is recorded when a user speaks, records and a sample is registered. The AI-powered voice biometrics analyses the different traits in the voice sample(s) like speed, accent, tone, pitch, also using neural networks to filter out ambient noise. Vocal dynamics biometric systems utilize human body dimensions such as vocal tract, mouth, and nasal cavities to analyse speech processing mechanisms.

iii. Keystroke Dynamics

By analysing how we type, keystroke dynamics can verify our identities. The technology behind keystroke dynamics is called keystroke recognition. Keystroke recognition technology analyses the timing and rhythm of keystrokes to create a profile of an individual's typing behaviour. This profile is called a biometric template. There are two types – static and dynamic keystroke dynamics. Static Keystroke Dynamics analyses the timing and rhythm of keystrokes. It is used as an alternative or add on to traditional password-based authentication methods.

Dynamic Keystroke Dynamics analyses the timing, rhythm, and pressure of keystrokes. It is less common than static keystroke dynamics. [10] Both static and dynamic keystroke dynamics can be used to verify the identity of a user, but dynamic keystroke dynamics are generally more effective.

A number of systems – palm print, body odour, Ear geometry, Gait, Hand-vein pattern, Facial thermographic,[1] Fingernail ridgelines are under development and studies.

3. TOOLS RELATED

a) Fingerprint Recognition

The person's fingertip image is taken using a fingerprint scanner. The ridges, valleys are identified from the fingertip surface and algorithms work on it to obtain precise details of the images – minutiae points. The pattern is represented mathematically to a template, which is not exactly the image as it is but it is a condensed representation of its main features or details. This is kept safely under a database. When a fingerprint is to be authenticated, its image is taken and this new template is compared with stored templates using advanced technologies. If this comparison possesses high threshold of accuracy by its minutiae points and spatial arrangement, person's identity is verified and access is granted

b) Iris Scanning and Recognition

Iris matching uses Gabor wavelet analysis to represent texture in iris images. The complex values are quantized to create a binary code. The Hamming distance determines match degree between iris codes. Authentic pairs have small Hamming distances, impostor pairs have large. Hamming distances Although the iris code gives excellent results when iris images are acquired in controlled conditions, the recognition rates deteriorate in less controlled conditions where the images exhibit impairments such as deformations, occlusions, specular reflections,[12] and geometrical changes from gaze differences.

c) Retinal Pattern Recognition

Neuroscience and clinical research are using adaptive optics scanning laser ophthalmoscopes (AOSLO), which are high resolution retinal imaging equipment. But creating reliable, automated techniques for handling and analysing these photos is a significant task. A simulation program called ERICA (Emulated Retinal Image CApture) creates realistic synthetic pictures of the human cone mosaic with related ground-truth data, simulating images that would be taken by an AOSLO and with a set image quality. [13] A self-organizing mosaic of photoreceptors, potential eye movements made by an observer during the taking of a picture, and data collection using a genuine system that incorporates noise, diffraction, and residual optical aberrations are all included in the simulation through ERICA.

d) Face Recognition Tools

Some of the best Facial Recognition Software's are provided as SaaS (software as a service),[14] Self-hosted Rest API solutions, Open-Source frameworks and libraries.

i. CompreFace - CompreFace is one of the few self-hosted REST API face recognition solutions on this list.

ii. Ageitgey/face recognition (GitHub Repository) - Python API or their binary command line tool.

iii. FaceNet - Created by Google researchers and the open-source Python library that implements it.

iv. DeepFace - This library also supports different face recognition methods like FaceNet and InsightFace.

v. InsightFace - It uses one of the most recent and accurate methods for face detection and face recognition.

e) Signature Dynamics Tools

The Israeli company Sign'Buy developed a signature recognition system that enables users to create custom signature motions, a feature the company calls finger signature. It is completely connected with the systems of AMEX (SafeKey), Mastercard (SecureCode), and VISA (VBV), enabling businesses and card issuers to provide enhanced customer service. The primary goal of Sign'Buy's product is to dominate the signature recognition market across a number of industries, including web-based systems, banking, and IoT access control.

Signotec GmbH, situated in Germany, is another such. Financial institution branch managers and customer care representatives may provide their clients electronically signed claim paperwork for expedited processing by utilizing SignoSign software and signature pads.

f) Vocal Dynamics Tools

Some of the speech recognition tools are [15]:

i. **Speechmatics**: An AI speech recognition tool that accurately records speech via machine learning algorithms. It is one of the few transcriptions software that supports more than 30 languages and is quick and

accurate in translating low-quality audio files.

ii. **Amazon Transcribe**: an AI voice recognition tool in the cloud, particularly intended for text-to-audio conversion in apps.

iii. **Microsoft Azure Speech Services**: Offers a variety of speech recognition and generation features, such as speaker detection, text-to-speech, speech translation, and speech transcription.

iv. **Otter.ai:** transcribe voice conversations with the tool, which is compatible with iOS, Android, and desktop operating systems.

v. **Google voice-to-text:** An AI voice recognition technology from the Google cloud platform that enables businesses to swiftly and effectively extract valuable information from audio data

g) Keystroke dynamics software

There are a lot of GitHub repositories for detecting and analysing keystroke dynamics. [19,20]. It is for analytical use, authentication use and fraud detection. Fewer forks is a C# analyser for that, and many python libraries like pyHook are used for such purposes.

4. CHALLENGES

Since biometric systems purely depends on physiological and behavioural characteristics, it is not pertinent to change the details or reauthenticate. The templates are going to be exact copies or maybe Analogous. Even if there is a need for change, for example someone's voice, it can be mimicked by someone else, so there is a chance for increased vulnerability. Masquerade attacks, where someone finds these vulnerabilities, impersonating as an authenticated user [1], can steal copies of anyone's biometric template. Synthetic copies could be created and then used for months or years after the theft, it might not necessarily happen just after the theft. It could be recorded by someone without the holder's knowledge. This leads to identity theft. Secure storage of the templates is more important than its production. These templates can be encrypted and hashed to make it safe, secure and less vulnerable. Some other set of challenges rather than masquerade is Deepfakes,[21] in case of face recognition, photo editing tools, physical artifact, image forgery and others.

Types [22] of biometric attacks are listed below:

a) **Direct Attacks or sensor attack**: Does not need any specialized algorithms or system operation knowledge

i. **Type 1 attack -Attack at the sensor:** Physically damages the system by flooding it with a load of access requests or by providing an artificial biological trait.

b) **Indirect attacks:** information about the authentication system is required to break into the system.

i. **Type 2 attack - replay attack:** The sensor sends raw biometric data to a feature extractor module for pre-processing with the help of a communication channel. This channel, is between sensor and feature extractor module, which is intercepted to steal the biometric trait. Trait is then replayed to feature extractor to bypass the sensor.

ii. **Type 3 attack - Attack on feature extractor module:** An imposter manipulates the feature extractor module to output features chosen by the intruder instead of the original data from the sensor.

iii. **Type 4 attack - Attack on the channel between the feature extractor and matcher:** similar to type 2 but the attack is on matcher module than the sensor. An imposter intercepts the communication channel between feature extractor and matcher modules, stealing genuine user feature values, which can be replayed to the matcher later.

iv. **Type 5 attack - Attack on matcher module:** The imposter is targeted to generate a high matching score, bypassing the biometric authentication system, regardless of the input feature set values.

v. **Type 6 attack: Attack on the database**: with security risks on databases, the deceiver adds new templates, modifies

existing templates and removes existing templates

vi. **Type 7 attack- Attack on the communication channel between system database and the matcher:** attacker modifies or alters the contents of a transmitted template, intercepting the communication channel between the system database and matcher module.

vii. **Type 8 attack:** An imposter can override the matcher module's result by tampering the match score transmitted through the communication channel between the matcher module and application device.

The author found that most adversary attacks target templates stored in databases, which can be tampered by adding, modifying, or removing them.

5. CONCLUSION

This paper discussed about the latest advancements in biometric technologies, tools related, and the challenges associated with privacy and data security. Characteristics- physiological and behavioural – physiological - fingerprint pattern, iris pattern, retinal pattern, facial recognition and behavioural – signature, vocal, keystroke dynamics are also discussed. Conclusion on types of attacks, tools and software's related to biometric identifications and authentication about the previously discussed biometric characteristics are also listed in this paper. An author found that most of the attacks makes target to the biometric templates which are stored in system database. There is still scope for research work on biometric data and its storage to protect it from vulnerabilities and establish an efficient and errorproof way of execution.

6. REFERENCES

[1]. Hill, C. J. (2001). Risk of masquerade arising from the storage of biometrics. *Bachelor of Science thesis, The Department of Computer Science, Australian National University*.

[2]. Daimi, K., Francia III, G., & Encinas, L. H. (Eds.). (2022). *Breakthroughs in digital biometrics and forensics*. Springer Nature.

[3]. Ross, A. A., Nandakumar, K., & Jain, A. K. (2006). *Handbook of multibiometric* (Vol. 6). Springer Science & Business Media

[4]. Kour, J., Hanmandlu, M., & Ansari, A. Q. (2016). Biometrics in cyber security. *Defence Science Journal*, *66*(6), 600-604.

[5]. Bera, A., Bhattacharjee, D., & Nasipuri, M. (2014). Hand biometrics in digital forensics. *Computational Intelligence in Digital Forensics: Forensic Investigation and Applications*, 145-163.

[6]. Yahya, Faridah & Nasir, Haidawati & Kadir, Kushsairy & Safie, Sairul & Khan, Sheroz & Gunawan, Teddy. (2016). Fingerprint Biometric Systems. Trends in Bioinformatics. 9. 52-58. 10.3923/tb.2016.52.58.

[7]. Robert smith (2018) https://biometrictoday.com/what-is-iris-recognition-how-does-it-work

[8]. Mikaela Pisani (2022) Retinal Recognition: The Ultimate Biometric: https://shorturl.at/gXNlp

[9]. Dan Virgilio (2019) https://www.infosecinstitute.com/ resources/general-security/signature-recognition-biometrics/

[10]. John Griffin (2022) https://www.fleksy.com/blog/ keystroke-dynamics-and-the-types-of-behavioural-biometrics/

[11]. Simon Burge (2023) https://securityjournaluk.com/ types-of-biometrics/

[12]. Handbbook of statistics (2013) Application of Bayesian Graphical Models to Iris Recognition

[13]. Young, L.K., Smithson, H.E. (2021). Emulated retinal image capture (ERICA) to test, train and validate processing of retinal images. *Sci Rep* **11**, 11225 https://doi.org/10.1038/s41598-021-90389-y

[14]. Serhii Pospielov (2021):https://shorturl.at/oaCNW

[15]. https://www.geeksforgeeks.org/ai-tools-for-speech-recognition/

[16]. Asem MM, Oveisi IS (2018) . Biometric retinal authentication based on multi–resolution feature extraction using mahalanobis distance. Biom Biostat Int J. 2018;7(1):28-46. DOI: 10.15406/bbij.2018.07.00188

[17]. Mary Clark: https://www.bayometric.com/minutiae-based-extraction-fingerprint-recognition/

[18]. Tomeo-Reyes, Inmaculada. (2015). Robust Iris Recognition using Decision Fusion and Degradation Modelling.

[19]. njanakiev: repository on GitHub https://github.com/njanakiev/keystroke-biometrics

[20]. deepakjayaprakash: repository on GitHub: https://github.com/deepakjayaprakash/Keystroke-Authentication

[21]. Ross, A., Banerjee, S., & Chowdhury, A. (2020). Security in smart cities: A brief review of digital forensic schemes for biometric data. Pattern Recognition Letters, 138, 346-354.

[22]. Jain, R., & Kant, C. (2015). Attacks on biometric systems: an overview. *International Journal of Advances in Scientific Research*, *1*(07), 283-288.