International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 06 | June 2021 www.irjet.net p-ISSN: 2395-0072

Comparative Study of Biometric Techniques

Nitesh Mishra[1], Pratik Gehlot[2], Priyanshu Gupta[3]

[1,2,3]UG Student, Dept. of Computer Science Engineering, Thakur College of Engineering and Technology, Mumbai, Maharashtra

---

Abstract - *Biometrics is the use of unique physiological (fingerprint, face, retina, and so on) and behavioral (gait, signature, and so on) features for authentication. Physiological and behavioral traits are unique to each individual. Knowledge-based (e.g., passwords) and token-based (e.g., ID cards) procedures are both used to establish a person's identification in the past. These are readily misplaced, shared, and stolen. As a result, in today's environment, they are insufficient for identification verification. A biometric system collects the biometric information from an individual and compares this data with the data present in the database. This paper provides a high-level description of the biometric system, numerous biometric approaches, and comparisons of biometric techniques based on biometric features.*

Key Words: **Biometrics, Biometric Technologies, Attacks**

1. INTRODUCTION

Biometric identification is a basic social activity that we do every day, beginning with our birth. A youngster learns to recognize his or her parents' voice and face first, then relatives, classmates, and friends. However, development of automated biometric identification systems has only recently enabled by these technical advancements. All of these answers may be traced back to techniques utilized thousands of years ago. Facial recognition, for example, is one of the oldest examples. Facial recognition has been used to classify people as acquaintances or strangers since the birth of humanity. However, as mankind advanced and travel choices expanded, this chore became more challenging. Biometrics tries to overcome this problem by connecting evidence of identification to our bodies and behavioral patterns. Few examples of biometric technologies are Fingerprint mapping, facial recognition, retina. Ear shape, Walking and Sitting methods, the veins in one's hands, unique body odors, facial contortions, are all other types.

They can also have other applications, biometric techniques have been used in security, and it can be labelled into three groups:

1. Biological biometrics
2. Morphological biometrics
3. Behavioral biometrics

Genetic and molecular features are used in biological biometrics. These could include things like your DNA or blood, which could be analyzed using a sample of your bodily fluids.

The structure of your body is taken into account in morphological biometrics. More bodily characteristics, such as your eye, fingerprint, or face shape, can be mapped for using with security scanners.

Behavioral biometrics works on patterns which are specific to each individual. If your walking, speaking, or typing behaviors are monitored, they can reveal information about your identity.

2. BIOMETRIC TECHNIQUES

The biometric techniques discussed in this paper are iris and retina, facial biometric, vocal biometric, fingerprintand hand geometry biometric.

2.1 IRIS AND RETINA BIOMETRIC

2.1.1 INTRODUCTION

Both iris recognition and retinal scanning are highly reliable biometric identification methods. Iris recognition is an automated type of biometric identification that applies mathematical pattern-recognition techniques on video images of an individual's irises, whose complex random patterns are unique to a person.

2.1.2 ATTACKS

A. USER LEVEL ATTACK

This attack takes place at the sensor level. Here impostor authenticate himself through fake data. This can be divided into two sub categories: - Masqueradeattack and Print attack or Spoofing.

MASQUERADE ATTACK - The impostor in this assault alters his biometric characteristic to deceive the iris- based authentication system. This can be accomplished by dilating the iris excessively or by using contact lenses. An imposter can utilize these to hide his actual identity, evade security checks, or impersonate someone else.

PRINT ATTACK OR SPOOFING - This assault occurred as a result of the display of a printed picture ofan iris image. The imposter shows a false iris picture to an iris recognition system's sensor. This attack has the ability to interrupt a biometric identification system's enrolment and verification phases. Fake eye attacks maybe classified into three types – printed form of eye,artificial eye made of plastic or rubber, printed form of eye lens, artificial eye and dead eye.

B. USER-SYSTEM INTERFACE ATTACK

This attack takes place at the interface between sensor of the system and matcher. Where in impostor tries to intercept to get access to the system by presenting this data

REPLAY ATTACK - The transmission of sensitive datafrom the sensor to the matcher is vulnerable to eavesdropping. The impostor is able to hack into the recognition system and steal data. It is possible for an adversary to replay this data by bypassing the biometricsensor.

C. STORED DATABASE ATTACK

An imposter tries to break the system and get access to the repository storing sensitive information belonging to the users in this attack, which occurs at the database level.

TEMPLATE HACKING ATTACK- The imposter gains access to the stored iris template, which he or she can use to fool the system. An assault on the iris template leads to three vulnerabilities: a template may be altered to get unauthorized access to the system, used to produce a physical duplicate and therefore utilized for a User-System Interface Level attack, and reused to gain unauthorized access to the system.

2.1.3 ADVANTAGES

1. No physical contact when scanning (more sanitary).

2. It is found to be difficult to spoof comparatively with other biometric techniques.

2.1.4 DISADVANTAGES -

1. Can't use a regular camera; requires IR light source and sensor. Visible light must be minimized for highest accuracy required for search.

2. Iris scanners are relatively higher in cost compared to other biometric modalities.

2.2 FACIAL BIOMETRIC

2.2.1 INTRODUCTION

A facial geometry system is software that uses a digital picture or a video frame from a video source to detect or verify a person. Facial recognition systems matches selected facial features from a input image to faces present in a database. The majority of facial geometry systems are built on the various nodal points. Values evaluated against a variable connected with spots on a person's face helps in uniquely identifying or validating the individuals. Applications can use data acquired from faces to reliably and quickly identify target individuals using this technology.

2.2.2 ATTACKS

A. PRESENTATION ATTACK

Face recognition systems are mostly spoofed by displaying video, an image or 3D mask of a targeted person to the particular system or camera. Alternatively, you might utilize make-up or plastic surgery to trick the system. However, because of the great exposure of the face and the inexpensive cost of high-resolution digital cameras, the most prevalent kind of assault is utilizing images and videos.

Photo attack - This consists of displaying a image of the attacked identity to the face recognition system.

Video attack – In this an attacker could play a video of the legitimate user in any of the devices that reproduces video and then that video can be presented to the sensor/camera.

3D Mask attack - In this, the attacker builds a 3D reconstruction of the face which appears similar to the face and shows it to the sensor/camera.

Other attack - Makeup, surgery

B. INDIRECT ATTACK

Indirect assaults can be carried out on the database, communication routes, and so on. This form of attack helps the attacker to gain access to the interior of the system.

2.2.3 ADVANTAGES

1. User experience is convenient and users just need to pass through the camera view and the recognition task is done.

2. Facial recognition requires fewer human interaction, which helps to work both securely and effectively.

2.2.4 DISADVANTAGES

1. Installation cost is more and there is a need for an advanced camera and complete software setup.

2. Facial recognition technology has the possibility of racial biasness and gender biasness if system is not designed well.

2.3 VOCAL BIOMETRIC

2.3.1 INTRODUCTION

Voice-based biometric systems utilize a technique that uses voice pattern recognition to authenticate an individual's

identification. It relies on the recognition of voice patterns that includes high-level information such as speaking and pause rate, pitch and timing patterns, idiosyncratic word/phrase usage, idiosyncratic pronunciations, etc.

2.3.2 ATTACKS

A. REPLAYING ATTACK

In this attack the attacker tries to get the access of the voice recording of the victim through social media, spam calls or physically if the attacker is in the close proximity of the victim. By replaying this pre-recordedvoice of the victim against the voice-based authentication system, the attacker can gain unauthorized access.

B. DEEPFAKE AUDIOS

Due to advancements in deep learning, voice impersonation attacks have become a major problem of concern. In this attack, the voice of the victims can be cloned easily through their voice samples to gain unauthorized access. A deep learning model is created, that is trained based on the considerable amount of the voice samples, of the victim. Using this model, the attacker can mimic the voice of the victim and can get any desired voice output.

2.3.3 ADVANTAGES

1. Significantly improve customer experiences.

2. Cost-effective.

2.3.4 DISADVANTAGES

1. In an environment where there is a lot of background noise, the voice-based authentication might not function properly.

2. Poor-quality speech samples, such as variations in a speaker's voice owing to sickness, emotion, or changes over time, might further compromise the system's capacity to authenticate individuals.

2.4 FINGERPRINT BIOMETRIC

2.4.1 INTRODUCTION

Another one of the most widely used biometric techniques is fingerprint. A fingerprint scanner takes a digital snapshot of the fingerprint by flashing a bright light over it. The digital picture is created by a light-sensitive microchip that examines the ridges and valleys of the fingerprint, converts them to 1s and 0s, and generates the user's unique code.

2.4.2 ATTACKS

A. USING HIGH-QUALITY IMAGE

It is possible to clone the fingerprint of the victim using high-quality images. A good example of this attack was demonstrated in 2014, where a German hacker revealed how he was able to clone the German defense minister's fingerprint using just publicly accessible pictures in which her hand was visible.

B. MASTERPRINTS

Fingerprint scanners have masterprints same as master keys for physical locks which are used to unlock anything. These are customized fingerprints that include all of the common characteristics present at everyone's fingertips. Attackers can use master prints to gain access to devices with poor scanning. While proper scanners will detect and reject a master print, a mobile phone's scanner may not be as thorough in its checks. As a result, a master print is an efficient technique for an attacker to gain access to devices that aren't scanning often.

C. RESUING RESIDUAL PRINTS

Remnants of the previously used fingerprints can be used to trick the scanner. It is highly likely that the fingerprint residuals are left behind by the person, who uses that device. Since devices like smartphones identify fingerprints by shining light on the fingertips and recording how it reflects back into the sensors, in order to get access, the attacker has to place an opaque reflective surface over the scanner. This reflective surface fools the scanner, by making it believe that the remnant of the fingerprints that is left on the scanner is an actual fingerprint and grants the access.

2.4.3 ADVANTAGES

1. It is easy to use and a cost-effective security solution.

2. No two individuals have the same fingerprint, not even twins.

2.4.4 DISADVANTAGES

1. Certain people will be barred from utilizing the system. Older persons with a history of physical labor, for example, may find it difficult to record worn prints into a system, and persons who have lost fingers or hands would be excluded.

2. Similarly, if a person faces injuries like burn then he might not be able to access the device.

2.5 HAND GEOMETRY BIOMETRIC

2.5.1 INTRODUCTION

Hand geometry based biometric recognition systems are based on the premise that each person's hand geometry is unique. Although there is no documentary evidence that a person's hand geometry is unique but given the likelihood of

anatomical structure variation among individuals, hand geometry can be considered a human physiological trait that can be utilized to uniquely identify an individual.

2.5.2 ATTACKS

A. SPOOFING HAND GEOMETRY SYSTEMS

Plaster is used to make the artificial hands in this method. The first step is to construct a moulding container with peg board as the bottom surface. A combination of alginate and water is put into the container after the pegs have been used to establish the posture of a genuine hand. After 2 to 7 minutes of solidification, the actual hand may be taken out of the alginate mould without damaging it. The mould will next be filled with a plaster powder and water mixture. The time it takes for the plaster to harden depends on the plaster-to-water ratio. It might take anything from 35 mins to 23 hrs. Which then can be used to spoof the system.

2.5.3 ADVANTAGES

1. The performance of the recognition systems is unaffected by the state of the skin surface (for example, skin color, wet/dry skin, smeared or dirty skin, scars, grime, diseases that solely affect the skin surface, and so on).

2. Can be used in some of the most extreme weather situations, such as intense heat and cold, where many other biometrics would fail.

2.5.4 DISADVANTAGES

1. Because there aren't many unique biometric traits, it can't be used for high-security applications. When combined with other kinds of identity verification, it may be used in applications with moderate to high security (biometric or non-biometric).

2. Certain medical disorders, such as edema or an injury to the hand that affects the contour of the hand, can impair the system's performance. Hand shape can also vary as a result of weight gain or loss, as well as ageing.

3. SECURITY ASPECT

Security has always been a problem of major concern for companies and individuals when it comes to the safety of the data. Similar to other systems, biometrics-based authentication systems are not 100% protected from attacks. But by using some of the preventive measures, these attacks can be avoided to some extent.

Multimodal biometric systems are authentication systems that rely on the identification of several biometric features. In recent researches, multimodal biometric systems have proved to be more reliable as compared to biometric systems relying on a single biometric method.

Similarly, there are other measures that are to be considered when dealing with a biometric system that is relying on particular biometric technique like in case of voice-based biometrics a stronger electromagnetic sensor could contribute to preventing a voice impersonation attack.

In the case of fingerprint based biometric, one should wipe the surface of the scanner where the finger is placed to remove the remnants of the fingerprint so that the attacker is not able to perform the residual attack.

In the case of facial biometric systems, one can avoid providing access to social media profiles to strangers by making accounts private.

4. COMPARATIVE TABLE

1. FAR: False Acceptance Rate: This metric indicates how frequently a system will mistake an unauthorized user for an authorized user. It is calculated using percentages.

2. FRR: False Rejection Rate: This metric indicates how frequently the system misidentifies an authorized user as an unauthorized user and denies access. It is calculated using percentages.

3. GFRR: Generalized FRR: The FRR of a device under realistic conditions, including user error. It is calculated using percentages.

4. FTE: Failure to enroll: This shows the number of people who are not enrolled in the system and thus cannot use it. It is calculated using percentages.

5. Risk of spoof: It demonstrates how easily the system can be thwarted by some method (e.g., instead of an actual fingerprint, showing only a photo of it to an optical fingerprint scanner).

6. Live sample detection: This demonstrates whether the system can distinguish between a genuine user and a spoofing attempt.

Biometric methods	FAR %	FPR %	GFRR %	FTE %	Risk of spoof	Live sample detection	User acceptance
Iris and retina pattern	10^{-7}	104	10	1	Very low	For certain devices	Low - misconceptions
Facial geometry	10^{-2}	10^{-2}	1-5	1	Medium-low	None	High
Voice	10^{-2}	10^{-2}	1-5	1-3	High	None	Medium
Fingerprint	10^{-2}	10^{-2}	1	0,10	Medium-Low	None	High
Hand geometry biometrics	10^{-2}	10^{-2}	1	0,10	Medium-low	None	Medium – the user must maintain physical contact on a large surface

Biometric methods	Contact requirement	Stability of the biometric sample
Iris and retina pattern	None	Does not change
Facial geometry	None	Changes often
Voice	None	Changes often
Fingerprint	On a small surface	Changes rarely
Hand geometry biometrics	On a large surface	Changes rarely

Biometric methods	Ease of Use	Error Incidence	Accuracy
Iris and retina pattern	Medium	Lighting	Very High
Facial geometry	Medium	Lighting, age, glasses, hair	High
Voice	High	Noise, colds	High
Fingerprint	High	Dryness, dirt, age	High
Hand geometry biometrics	High	Hand injury, age	High

5. CONCLUSION

In today's fast-paced environment, depending on biometrics is the only option to ensure the user's presence. As the industry continues to evolve and emerge in the twenty-first century, biometrics is utilized for authentication in a range of settings. So, taking it into the consideration this paper presents all the necessary details of each emerging biometric technology in order to help new research scholars for their research. It also provides important details which can help individual on choosing the biometric technique during building their own system or application. The number of applications that use biometric technologies is still very limited. Despite this, biometric-based recognition will undoubtedly have a significant impact on how we do our everyday business in the near future.

6. REFERENCES

1. M. Faundez-Zanuy, "Biometric security technology," IEEE Aerosp. Electron. Syst. Mag., vol. 21, no. 6, pp. 15–26, 2006.
2. R. Subban and D. P. Mankame, "A study of biometric approach using fingerprint recognition," Lect. notes softw. eng., pp. 209–213, 2013.
3. S. Hong, J. Han, and G. Kim, "Security issues related to biometric security," Ijitee.org. [Online]. Available: https://www.ijitee.org/wp-content/uploads/papers/v8i8s2/H11460688S219.pdf.
4. M. G. Vaidya, "A study of biometrics technology methods and their applications- A review," Ijiet.com. [Online]. Available: http://ijiet.com/wp-content/uploads/2015/04/34.pdf.
5. A. K. Jain, A. Ross, and K. Nandakumar, "An introductionto biometrics," in 2008 19th International Conference on Pattern Recognition, 2008, pp. 1–1.
6. K. P. Tripathi, "A comparative study of biometric technologies with reference to human interface," Ijcaonline.org. [Online]. Available: https://www.ijcaonline.org/volume14/number5/pxc3872493.pdf.
7. L. Pascu, "Chinese researchers reveal method to bypass biometric fingerprint scanners in smartphones," BiometricUpdate.com, 04-Nov-2019. [Online]. Available: https://www.biometricupdate.com/201911/chinese-researchers-reveal-method-to-bypass-biometric-fingerprint-scanners-in-smartphones.
8. A. K. Yadav and S. K. Grewal, "A comparative study of different biometric technologies," Csjournals.com. [Online]. Available: http://www.csjournals.com/IJCSC/PDF5-1/8.%20Arun.pdf.
9. Researchgate.net. [Online]. Available: https://www.researchgate.net/publication/306064545_Comparison_of_biometric_identification_methods.
10. Researchgate.net. [Online]. Available: https://www.researchgate.net/publication/263847035_Study_on_Biometric_Authentication_Systems_Challenges_and_Future_Trends_A_Review. [Accessed: 23-Jun-2021].
11. "Advantages and disadvantages of fingerprint recognition - NEC NZ," Nec.co.nz, 23-Sep-2019. [Online]. Available: https://www.nec.co.nz/market-leadership/publications-media/advantages-and-disadvantages-of-fingerprint-recognition/.
12. Kaspersky, "What is biometrics security," Kaspersky.com, 13-Jan-2021. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/biometrics.