Biometrics Security System

[1]Midhun Mani, [2]Naveen Vinod, [3]Jewel George

[1,2,3]Student
Computer Science Department, Santhigiri College, Kerala, India

ABSTRACT: In order to serve as a primer on this topic, this essay provides an outline of the major issues surrounding biometric security technologies. Compared to conventional ways of recognizing persons, biometric can provide more security and ease. Even if we don't wish to switch to a biometric system from a traditional one (such as a password or mobile token), we are undoubtedly potential consumers of these technologies, which will even be required for new passport models. Knowing the potential of biometric security technologies is helpful for this reason.

A new era of engineering science has emerged in recent years, and its products are anticipated to spark the growth of a sizable bazaar in the near future. It has been referred to as "biometric." The creators of this novel field hope to develop methods that would allow the identification of a person based on their "biological" characteristics, such as their vocal tone, diminuendos in their movements, facial features, physical characteristics of other body parts, optic nerve pattern, or sword lily pattern. Human beings have been created by nature with unique appearances that can vary from person to person. Biometric technology uses this characteristic to positively identify each person.

Biometric refers to a person's subconscious records based on their physical or social features. For a variety of reasons, this method of identification was designed to make several improvements over antiquated procedures including ID cards (tokens) or PIN numbers (passwords). (i) The human being to be identified is mandatory to physically exist at the point of identification; (ii) Identification grounded on the biometric methods evades the essential to recall a password or carry a token. Through the distended addition of computers and the Internet into our ordinary lives, it is essential to protect penetrating and personal data. By exchanging PINs (or using biometric in totaling to PIN), biometric methods can theoretically avoid illegal access to ATMs, cellular mobiles, workstations, and PC networks. Opposing biometric traits and tokens like permits and driver's licenses may be forged or missing.

INTRODUCTION

The Greek words "bios" (life) and "metrikos" are the origin of the word "biometrics" (measure). In a strict sense, it refers to a science that examines biological traits statistically. Therefore, we should refer to the security applications that examine human traits for identity verification or identification as biometric recognition of people. However, we will refer to "biometric recognition of persons" as "biometrics" in this article. A potential solution for security applications, biometric recognition has several advantages over traditional methods that rely on something you have (key, card, etc.) or something you know (password), is offered by biometric recognition. The fact that biometric qualities are based on things you are or do rather than things you remember or have to keep a token in your possession is a wonderful feature of them.[1]

When a machine that limited finger length was fixed for a timekeeping request at Shearson Hamill on Wall
Street more than 25 years ago, the first marketed biometric device was created. In the following years, the Department of Energy, Western Electric, Naval Intelligence, and related organizations connected hundreds of these hand geometry devices at high-security locations. Currently, access to more than 20,000 workstation rooms, vaults, exploratory labs, daycare centers, blood banks, cash machines, and military fixings is tracked using methods that look for a subject's particular physiological or behavioral characteristics. Reduced values have increased the awareness of biometric machines; this, together with lower overall costs, will undoubtedly be good for this manufacturing as we transition into the next era. The Greek words "bios" (life) and "metrics" are where the word "biometrics" comes from (measure). In a strict sense, it refers to a discipline that connects the statistical analysis of biological traits. The safety applications that analyze human features for individuality confirmation or identification must therefore be referred to as biometric gratitude of individuals. However, we will refer to "biometric appreciation of individuals" by the abbreviation "biometrics." Compared to traditional approaches, which rely on something you have (such a key, card, etc.), or something you know, biometric recognition offers a different approach for safety applications (password, PIN, etc.). Biometric characters have the advantage of being based on something you are or something you do, so you don't need to remember anything or hold onto a token.

Biometrics:

The term "biometrics" refers to the rapidly expanding branch of science that uses biological traits or behaviors to verify people's identities. In advance, this entails capturing a picture of a person's distinctive feature, such as a fingerprint, hand, eye, or face, and comparing it to a template already taken. This has been oversimplified for ease of explanation, but in essence, this is how biometric technology operates.Biometrics is the statistical application of the distinctive characteristics of biological constituents.[1] Why is biometrics necessary? You can avoid the issues of forgetting the passwords and ID codes by using biometrics-based verification, which verifies your voice, iris, and fingerprints for your uniqueness at ATMs, airports, etc. You can avoid the problems of withdrawing money from a bank before or after it closes by simply blinking, tapping your finger, or presenting an uninterested expression. What is biometrics? Biometrics refers to a person's subconscious credentials based on their outward physical or behavioral characteristics. For a variety of reasons, this type of identification is favoured to conventional ones including passwords and PIN codes:

(i) The being to be recognized is obligatory to be existing at the detail of credentials.

(ii) Credentials grounded on biometric ways avoids the prerequisite to recollect a Leg or carry a commemorative. By substituting Leg's, biometric styles can actually stop unauthorized admission to or fake use ofA.T.M 's, Keen cards, PC networks.

(iii) PIN passwords might be elapsed, and tokenbased approaches of identification like keywords and driver's licenses might be phony, embezzled or lost. A biometric organization is mainly a pattern obligation scheme which makes an individual identification by important the authenticity of a precise physiological or social characteristic prejudiced by the user.

BIOMETRIC TRAITS

Which attribute can be used for biometric identification, first? A excellent biometric attribute should, according to common sense, accomplish a number of characteristics. Any two people ought to be distinct enough from one another to be distinguished from one another by this quality. Permanence: The characteristic should be sufficiently stable throughout time, in various environmental conditions, etc. in relation to the matching criterion. Collectability: The quality must be attainable and quantifiably quantifiable. Acceptability: Individuals should be ready to accept the biometric system and not find it intrusive or unpleasant. Performance: A successful recognition must have a reasonable degree of identifying accuracy and take only a little amount of time.

Circumvention: The ability of dishonest persons to trick the biometric system should be minimal.

Biometric traits can be goes into two categories they are: a) Physiological biometrics:

It is based on accurate measurements taken of a specific human body part. This group includes the recognition of hand scans, faces, fingerprints, and irises. b) Behavioral biometrics

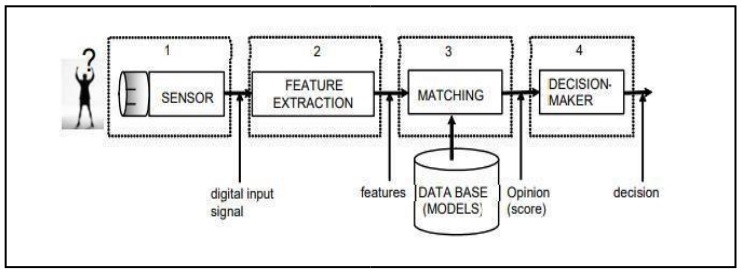
Evaluates various physical traits of the human body indirectly by using measurements and data that are obtained from an activity taken by the user. This area includes the recognition of signatures, gaits, gestures, and keystrokes. But this categorization is incredibly arbitrary. The voice signal, for instance, is influenced by behavioral characteristics like semantics, diction, pronunciation, idiosyncrasy, etc (related to socio-economic status, education, place of birth, etc.) [2]. . The physiology of the speaker, such as the vocal tract's shape, also plays a role. On the other hand, human behavior—such as how a user holds up a finger or looks at a camera— can also have an impact on physiological characteristics.

VERIFICATION AND IDENTIFICATION

There are two operating modes for biometric systems identification and verification. When we do not wish to make a distinction between them, we shall speak about recognition for the general case. still, some pens equate identification andrecognition.identification This system makes no claim to the stoner's identity. Who the stoner is must be determined by the automatic system. Closed set identification occurs when a stoner fits within a preset group of vindicated druggies. still, the system's database of known druggies is plainly vastly lower than the total number of prospective entry attempts. Open- set identification refers to the more general circumstance where the system must manage people who may not be modeled inside the database. Closed-set identification is converted to open- set identification by including the" none- of- the- above" choice. The system's performance can be assessed through identification rate. verification:In this system, the system's ideal is to ascertain whether the person is whom they say they are. This indicates that in order for the system to accept or reject a stoner, identity must first be vindicated successfully or unsuccessfully. This functional mode may also go by the name authentication or discovery.(10) The False Acceptance Rate(FAR, cases where an fraud is accepted) and the False Rejection Rate(FRR), also known as False Alarm and Miss, independently, in discovery proposition, can be used to assess the performance of the system. Both crimes have a trade- off, which must be determined by generally altering a decision threshold. Both a DET(Discovery error trade- off) plot and a ROC(Receiver Operator Characteristic) plot can be used to fantasize the performance(3). The DET wind employs a logarithmic scale for both axes and treats both types of error inversely. This spreads out the plot, makes it easier to identify colorful high- performing systems and generally results in graphs that are close to direct. Also, take note of the fact that the ROC wind depicts the megahit rate rather than the miss probability due to its harmony with respect to the DET. The extreme portions of the wind, which are those that reveal the most information about the performance of the system, are expanded in the DET plot using a logarithmic scale. Figure 1 displays a DET plot illustration, and Figure 2 displays a traditional ROC plot.

BIOMETRIC TECHNOLOGIES

Many biometric characteristics have been shown to be helpful for biometric identification. However, the overall design of a biometric recognition system is always the same as what is depicted in the image



Even though common sense suggests that, at least for humans, doing good acquisition is sufficient for performing good recognition, this is untrue. It must be remembered that the next blocks, labeled 2 through 4, are indeed basic. A quality photo or audio recording is insufficient. Agnosia is a rare condition that can affect people. Even though they are aware of the traits of the things or people, those who have agnosia find it difficult to recognize and identify them. People who have agnosia may find it difficult to identify the geometric aspects of an object or a face, or they may be able to do so but be unsure about the object's purpose or if a face is familiar or not. Agnosia may just affect one sensory system, such as hearing or vision. Face blindness or prosopagnosia is the name given to a specific condition [] (prosopon is a Greek word for face). Prosopagnosics frequently have trouble recognizing their own

faces, those of their loved ones, and even close friends. They frequently employ alternate methods of face recognition, however, these methods are less reliable than face recognition. Strokes, dementia, or other neurological conditions can cause anosia. The National Organization for Rare Disorders (NORD) [14] has further details regarding agnosia. Therefore, biometric recognition is not a simple task, even when carried out by humans. Our brains carry out a really intricate process during it!

Types of biometric devices and their services

Now let's see approximately of the biometric strategies being widely used in numerous areas like computer/network safety, government societies, prisons…. Which are famous,They are:

a) Fingerprint identification.
b) Face recognition.
c) Iris recognition.
d) Hand geometry.

a) **Fingerprint recognition:**

No two cutlet prints are alike, and they are unique to each individual. The most well-established biometric technology now in use is point recognition. Edge and dens designs can be found in fingerprints. in addition to luxuries. Inhabitant edge characteristics known as minutiae points might occur at a crest finish or crest bifurcation. Three methods exist for looking over cutlet prints. three types of scanners: capacitance (solid-state), updraft, and optic There are two accepted methods for looking at print data well:

(1) minutia-grounded methods.
(2) correlation-based methods. The more minuscule of the two is minutia-based. This system assigns them an XY, a match that is also stored in a train, and suggests the crest physiognomies (branches and consummations). Advantages

• High correctness rate
• Can execute 1- to- numerous judgement.
• Affordable outfit.
• Easy to exercise(samples are easy to imprisonment and reservation).
• Most proven and oldest of the biometric knowledge.

Point recognition examines the established patterns on a fingertip. Several algorithms provide an intriguing anthology that can uncover further information (7). The earliest and most widely used method of
computerassisted identification is the use of fingerprints as biometric. The likelihood of finding two people with the same point is thought to be one in a billion. Nevertheless, some drug users may be reluctant to utilize it. In essentially free nations.

(1) There is generally no authority for the compulsory submission of fingerprints unless a felonious offense is being charged.
(2) There is no authority for the retention of the prints until the charge is prosecuted and the offense is proven. Consequently, fingerprints have a common-criminal tinge. Still, the trait is increasingly being used in immigration cases and is being accepted as an identification method that is not inextricably linked to offenders **b) Facial recognition:**

One of the earliest biometric technologies is face recognition. The technology examines facial traits and makes an effort to match them with a library of digital images. Since the 1990s, this technology has only recently become commercially viable. Since the tragedy of 9/11, face recognition has gained popularity for its capacity to recognize known extremists and criminals. Face recognition employs identifying aspects of the face, such as the margins of the mouth, the areas around the cheekbones, and the upper portions of the eye sockets, to verify and identify the subject. Getting an image of a separate and saving it in a database for future use is the first stage in face recognition. Usually, multiple photos (or videos) from various angles are shot. Additionally, individuals may be asked to create other face terms for the database. The descriptions are then reviewed and removed in order to create a template[8]. The first step is to verify the entity's uniqueness by comparing its photos to those that were kept on file in the catalog.

There are four main methods actually used for facial recognition:

• Eigen face: a tool established by MIT that excerpts characteristics over the practice of two-dimensional grayscale descriptions.
• Feature Examination (also recognized as Native Feature Analysis (LFA)): is the most lengthily used system because of its competence to the neighborhood for facial changes and aspects. LFA uses a procedure to harvest a face print (84 bytes in size) for judgment.

Advantages:

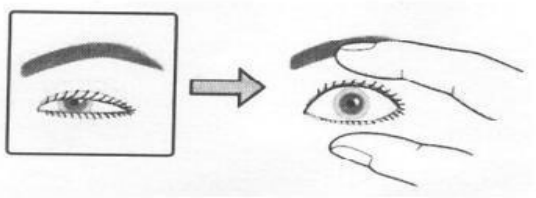
• High accuracy rate.
• Can be accomplished from a remoteness.
• Accepted by most users.
• Non-intrusive.

c) Iris recognition:

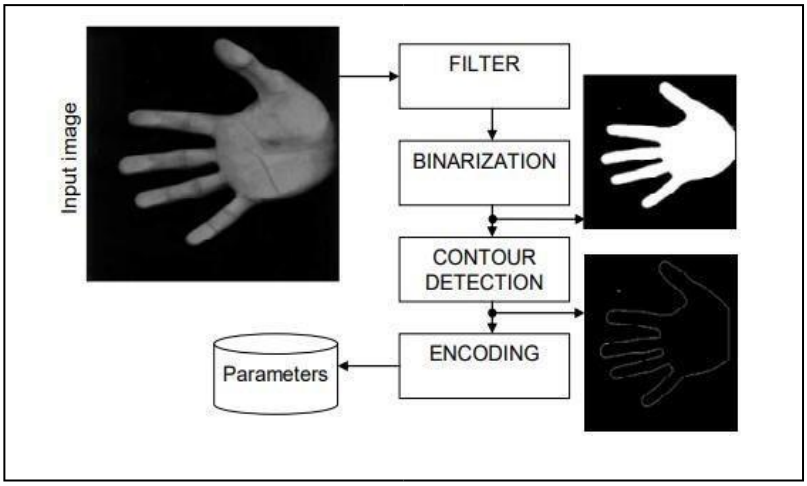
Not even identical or equivalent clones can be used to compare two irises. Over 400 noteworthy appearances are covered by the iris. As a result, iris scanning is much more accurate than using imprints or even DNA testing to identify distinctive traits. By measuring the diameter of the colorful circle that encircles the pupil, the iris is scanned. A camera analyses the iris design, which includes the corona, pits, crypts, filaments, striations, and radial troughs, using audio-visual technologies (page). Iris scanning is simple, accurate, and appropriate. The initial start-up costs are a significant drawback of Iris's appreciation because they are very high. Passive and dynamic techniques for knowing one's iris are both rejected by iris documentation schemes[6]. According to the active Iris system technique, the user must be between six and fourteen inches away from the camera. In order for the camera to concentrate on the user's iris and adapt, the user must also move back and forth. The camera(s) that find and focus on the iris can be up to three feet away from the user with the passive system. Advantages:

• High accuracy rate
•Imitation is almost incredible

Due to the eyelid's ability to obstruct the iris, several users—particularly those from the East—experiment with Iris scanner issues. In this situation, some manual actuation is required to clear the obstruction.

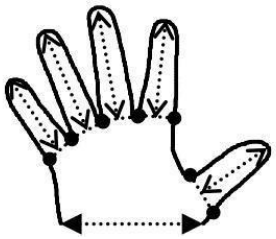


d) Hand geometry:



The measurement of the user's needle and digit corporal properties is a problem for hand geometry, which is theorized to be sufficiently distinctive for use as a biometric verification method. The device stores a wide range of human hand sizes is relatively simple to operate and offers a reasonable balance of performance qualities. The reader's body position varies between holding a softball-shaped object in his pointer, a flat bowl in which he places his hand, a bar that he holds as if opening a door, and a smooth plate on which he places his hand. In addition to period and presence recording, where they must demonstrate to be very popular, hand geometry readers are well-known in a wide range of circumstances. In areas with a big operator base or users who occasionally access the system, the method might be appropriate[5]. If desired, precision can be quite high. Despite being rather huge and opulent, hand geometry readers have a tiny pattern size and are easy to incorporate into various schemes and operations (only 9 bytes for a pure hand geometry template).

The geometry of the hand is measured. This technology offers compact templates (between 9 and 25 bytes) with minimal storage requirements. Since feature extraction is rather simple, inexpensive processors are used.



Additionally, utilizing the inner surface between the wrist and the fingers, it is possible to recognize palm prints. This area displays a wealth of information, including folds, ridges, and valleys resembling fingerprints but on a bigger surface. Even though there are no commercial systems that use palm prints, certain university tests have been done using this data alone and hand geometry for enhanced accuracy.

Computer/Network security:

Numerous networked and standalone computers transmit sensitive and valued information. Another significant application of biometric authentication systems is regulating access to these systems[10].

Internet transactions: Many people consider online transactions to be a natural use for biometrics due to the increasing security concerns brought on by the surge in e-commerce. Because he is confident that the person at the store is who he says he is, the salesperson's confidence is increased by biometric authentication.

a) Physical area security:

Military, Government, and Commercial connections have satisfactorily strong confidentiality concerns.

b) Banking:

In order to combat card fraud, a number of top banks are looking at using biometrics with ATMs. Beginning in 2002, certain businesses will start offering smart credit cards that have the customer's fingerprint data implanted.

c) Voting: A logical application of biometric is in the voting process, where it is required of qualifying candidates to prove their identities. This should put an end to "proxy" voting.

d) Prisons: An intriguing application of biometric is in prisons, where visitors to inmates are required to go through verification procedures so that identities cannot be exchanged.

SECURITY AND PRIVACY

The security level is essentially the same for every user in a system, which is a desirable feature of biometric security systems. For other security technologies, this is not accurate. For instance, with a password-based access control system, all a hacker needs to do to get access is guess one password out of all the employees. A weak password in this situation jeopardizes the total security of every system to which the user has access. As a result, the security of the entire system is only as strong as the weakest password [10]. This is crucial since strong passwords tend to be illogical string combinations of letters and numbers that are hard to remember, such as "Jh2pz6R+." Sadly, some individuals continue to utilize passwords like "password," "Homer Simpson," or their own names. Although there are many benefits to biometric, they have not yet been widely used [7]. The fact that biometric information is not private and cannot be changed if it is stolen by a third party is one of its key disadvantages. This can only be a small issue in situations when a human supervisor is present, such as border entry control, because the operator may verify if the supplied biometric trait is authentic or not. However, some sort of liveliness detection and anti-replay attack measures should be offered for distant applications like the internet. This is a new area for study. In terms of security, it is generally advised to update frequently in order to maintain protection. If improvements are not made on a regular basis, a system that is appropriate for the moment may become outdated. Because of this, no one can assert that their security system is perfect or that it will stand the test of time[9].

Conclusion

The improvements in precision and biometric technology are now a safe, sensible, and affordable option thanks to serviceability and cost reduction excellent method of identifying people. Biometric requirements including fingerprint, face recognition, hand geometry, voice verification, and others are well known and each has its own distinctive qualities. Now that speed and bandwidth are no longer limiting constraints, their actual performance may frequently be better than expected.

REFERENCES

1. R. Clarke “Human identification in information systems: management challenges and public information issues”
2. Available in http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html
3. S. Furui Digital Speech Processing, synthesis, and recognition., Marcel Dekker, 1989.
4. A. Martin, G. Doddington, T. Kamm, M. Ordowski, and M. Przybocki, “The DET curve in assessment of detection performance”, pp.1895-1898, European speech Processing Conference Euro speech 1997
5. A. J. Mansfield, J. L. Wayman, “Best Practices in Testing and Reporting Performance of Biometric Devices”. Version 2.01. National Physical Laboratory Report CMSC 14/02. August 2002.
6. M. Faundez-Zanuy “Door-opening system using a low-cost fingerprint scanner and a PC”. IEEE Aerospace and Electronic Systems Magazine. Vol. 19 nº 8, pp.23-26. August 2004
7. "Biometrics for Secure Authentication", (PDF)Retrieved.
8. [online] Available: http://www.bioelectronix.com/what_is_biometrics.html.
9. [online] Available: http://www.biometricnewsportal.com/biometricsissues.asp.
10. http://en.m.wikipedia.org/wiki/biometrics
11. https://globalsign.com