Analysis of Enhanced Security Methods Using Biometrics

Mohamed Basheer.K.P, Research Scholar, Dept. of Computer Science, Jamal Mohammed College, Thiruchirappalli.

Abstract: *This study provides a thorough analysis of the various biometric types, including their advantages and disadvantages. It compares the different types and provides details about false acceptance and false rejection rates, along with their equations. Biometric screening systems are used to test and identify persons using their physiological or behavioral characteristics. Using only one recognition device is not suitable for identification systems. Multi-factor authentication can improve system security by using two or more kinds of security types, such as passwords and cards, but this is not an ideal security scheme. Passwords may be forgotten or inputted incorrectly, or the identification card may be stolen. To verify and classify people using their physiological attributes, biometric devices are used. These technologies can be classified as either behavioral or physiological biometrics. The former has many shortcomings, such as noisy data, inter-class similarity, intra-class variability, spoofing and universality, which reduce the system's accuracy. The success rate of recognition and verification is, however, substantially improved by multimodal biometric sensing and processing systems, which leverage the detection or processing of two or more behavioral or physiological traits.*

Keywords: Biometric Identification, Iris recognition, Fingerprint recognition, Facial Recognition, Biometric Verification.

Introduction

Biometrics screening is a field of science concerned with the statistical analysis of biological data of individuals. It is extremely important in the identification of individuals from a variety of features. Human inheritance is dynamic, rich in combinations and well suited to user identity and authentication systems (Hossain and Chetty, 2011). People around the world support biometrics: Around 70% of global consumers support utilizing biometrics automation, such as fingerprints or voice recognition, regulated by a trustworthy agency (business, medical provider, or legislative body), as a means of verifying the identity of a person based on new international analysis standards (Kumar and Ryu, 2009). In a global survey of consumer safety preferences, 66% of customers around the globe considered biometrics to be the best way to tackle fraud and identity theft (Kumar and Ryu, 2009). Enterprise networks and server records are other approaches that can be used for, e.g., smart or credit cards. These figures represent an improvement from specific studies published by Unisys in September 2005, which found that 61% of the world's leading businesses considered biometrics the tool of choice to tackle fraud and money laundering. This is usually achieved using fingerprints, voice recognition, or eyeball-scanning devices when, for example, an individual is about to unlock a door or make a purchase (Galdi *et al*., 2013).

Objectives

The main objectives of the research are to provide in- depth knowledge and understanding about biometrics and to provide a comparison between the most used biometric types, based on:

- Distinctiveness
- Complexity
- Universality
- Quantifiability
- Comparison
- Collection capacity
- Performance

- Acceptability
- Cost and
- Use

Literature Review

History and Importance of Biometrics

As an early form of recognition, people have used sight to identify each other based on facial images scanned by the human eye, as well as voices recognized by their ears and memorized by the human brain. At the end of the 19th century, Bertillon, a French police officer, took the first steps in scientific policing. He used body measurements taken of specific anatomical characteristics to identify reoffending criminals, a technique that often proved successful.

According to (Kakkad *et al*., 2016), Unimodal biometric technology faces many problems, such as noisy data, intra-class variations and a limited degree of freedom-anti-universality, spoof attacks and an unacceptable level of mistake detection. Some of these limitations can be addressed through the deployment of multimodal biometric systems that incorporate evidence from various sources of data. Because of these inherent issues, attempting to enhance the performance of individual matches in these circumstances cannot prove successful (Ahmad *et al*., 2012).

Multi-biometric systems tend to mitigate a few of these limitations by presenting numerous proofs of the same identity. These systems help to provide efficiency gains that might not be possible with a single biometric indicator. Further, multi-biometric systems incorporate anti-spoofing steps by making spoofing multiple biometric traits simultaneously difficult. An efficient fusion scheme, however, is needed to combine the data in the opinion of various domain experts (Solayappan and Latifi, 2006).

According to (Mondal and Bours, 2014), biometrics is a means of delivering identification using detectable physical properties. It uses body characteristics to encode or to scramble/descramble data as a tool. Physical features like fingerprints, retinas and irises, palm prints, handwritten signatures, finger veins, facial structure and voice recognition are a few biometric identification methods currently used (Jain *et al*., 2004).

Because the mentioned features are unique to every person, biometrics is a viable solution in the fight against fraud and theft, especially concerning the Internet. The reason is that this advanced application is thought to be better than using credentials or Personal Identification Numbers (PINs) as it is not easy to misplace, hack, or replicate biometric features. The idea is that you are your own password, based on these features. This type of identification could soon become the norm. Nowadays, many transfers and trades occur online; an individual must prove to a computer who the individual claim to be (Jacobsen and Sandvik, 2015). The available choices, however, do not represent an excellent method of securing personal data. Individuals lose cards, lose countersigned documents, or write PINs down on pieces of paper so that others may gain access to them. One way to protect data is to use an aspect of yourself-a biometric identifier-that has been registered and can be utilized to confirm your identity. Biometrics will be the next step in network security if the Internet is going to be a genuinely safe place to purchase utilizing delicate data; information protection will require more than just passwords. Based on this rationale, we are now observing the rise of several major biometric security firms specializing in Internet technology. They hope to become the Internet's next Baltimore Innovations.

Biometric Applications

For most organizations, data and computer protection has become crucial, particularly in recent years, with "hackers" growing in number and becoming more skilled in accessing and changing personal details. Hackers understand and can use a range of devices to hack into networks and servers, including sniffers; they crack passwords and rootkits, among other things, that can be found easily on the Internet. Safety has also proved been a daunting challenge, in terms of providing more comprehensive protection, for cities and higher authorities, beneficial monitoring organizations and airport security (Meng *et al*., 2014).

The applications of biometrics can be divided into the following three main groups:

- **Commercial applications:** Such as e-commerce, Internet, access, ATMs, credit cards, physical access control, cellular phones and medical records management

- **Government applications:** Such as national ID cards, correctional facilities, driver's licenses, social security, border control and passport control
- **Forensic applications:** Such as corpse identification, criminal investigations, terrorist identification, parenthood determination and missing children

Traditionally, commercial applications have used data authentication (e.g., PINs and passwords), government applications have used tangible token-based systems (e.g., ID cards) and forensic applications have relied on human and biometrics experts to match biometric features. Biometric systems are being increasingly deployed in large-scale civilian applications. The Schiphol Privium scheme at the Amsterdam airport, for example, employs iris-scan cards to speed up the passport and visa control procedures (Jain *et al*., 2011).

Passengers enrolled in this scheme insert their card at the gate and look into a camera; the camera acquires the image of the traveler's eye and processes it to locate the iris and compute the IrisCode; the computed IrisCode is compared with the data residing in the card to complete user verification (Jain *et al*., 2011). A similar scheme is also being used to verify the identity of Schiphol airport employees working in high-security areas. Thus, biometric systems can be used to enhance user convenience while improving security.

Standardized protection programs safeguard the infrastructure of an enterprise, comprising the system and computer equipment details (Zureik and Hindle, 2004). Data that a company wants to secure can take several forms, such as emails, Electronic Data Interchange (EDI) invoices, new material designs, advertising actions, consumer records and income reports. safety risks include not only information theft; they also include acts such as altering coworkers' credentials, leaving devices unattended while logged into the system and entering dubious sites and computer systems. Vast amounts of money are lost each year because of multiple security breaches.

Biometric Types

According to (Ahmad *et al*., 2012), a person's biometric characteristics are discrete and unique. Some of these characteristics are difficult to replicate or manufacture precisely. These are, ideally, perfect controls. Nevertheless, several specific issues arise while using biometric recognition. Biometrics are more sophisticated, advanced and highly sensitive than ever before. They are used to protect businesses and citizens. Above all, biometrics work on the biological qualities of a person that cannot be duplicated.

Biometrics are less costly and less risky for the individual, with a person's highly accurate identification provided by physiological features. They have higher authentication rates than passwords and cards. Such online recognition systems work with high accuracy, where the characteristics are more or less unique. There are many ways to categorize biometrics techniques for classification purposes, albeit from the user side. There are three essential parameters: How much physical contact is needed by the operating requirements of the device; verification time (including any extra time needed to position oneself or other actions related to identification); and the amount of collaboration needed by the system to allow the individual to be correctly identified (Gatali *et al*., 2016). Contactless systems are also favored since many users have hygiene fears related to objects that many others have touched. This fear unfairly discriminates against biometric identification systems, but consumer awareness is still a significant element in the efficient implementation of such programs. Identification time is typically marginal compared to the whole access process, but this depends on the extent of access.

Biometric identifiers can be classified into two broad groups: Behavioral; and physiological.

Behavioral Biometrics

Behavioral biometrics is the study of the actions of the human beings and animals. This is further broken down into the following subtypes:

- signature recognition
- voice recognition; and
- keystroke dynamics

Signature Recognition

For decades, signatures have been used as proof of identity and for high-quality, secure transactions. It is an observable function and can generate several analytical, accurate details and it can also be electronically captured. Previously, manual methods for verifying signatures have been used, including type validation. Biometric recognition devices can ascertain much more accurately whether an individual is a licensed consumer or an impostor. For authentication and authorization, banks and other financial institutions and service providers often use signatures.

Voice Recognition

The voice relies on the composition of the throat and mouth as well as on its moving components and possesses both behavioral and physiological characteristics. Depending on several variables, voice is used to identify speakers as a critical biometric identifier. Sound can identify both the speaker and what is being said. The voiceprint or vocal print is a visual gathering of the language, which is evaluated for frequency, length and amplitude. Most systems utilize both speaker detection and speech detection, but both have various aims and implementation processes and both rely on a human speaking. Speech recognition is widespread and inexpensive, but it is less precise and often takes longer.

Keystroke Dynamics

There is a reasonably recognizable pattern in which one typing on a keyboard forms the base of the biometric technique known as keystroke dynamics. The striking intensity and style of different people are distinctive. Forseveral security reasons, this can be is evaluated and registered..

Physiological Biometrics

Physiological biometrics is based on the character of aperson's conduct (Patel *et al*., 2015). This includes all thephysical properties, including the mouth, hair, iris and fingerprints. It is broken down into the following types:

- Iris
- Face
- Fingerprint
- Finger veins
- Ear
- Foot dynamics and footprint; and

Iris Verification and Identification

The iris is a flexible, thin, pigmented, circular connector. This tissue controls the size and diameter of the pupil. The pupil limits the amount of light that enters the eye. The iris is unique to each individual, even among twins. The iris is protected by the cornea and it is visible from the outside. It can contain many characteristics, such as arched ligaments, furrows, crests, crypts, rings, corona, freckles, collarets and zigzags. Iris recognition is one of the safest techniques for authentication and recognition. The precision of this method is the most significant aspect. The false rate of acceptance, as well as the rate of rejection, is extremely low for this technique; aspecial camera with a grayscale is used to take the iris pattern in the 10-40 cm range. The appropriate methodology is used to identify the iris in the photo and, if it exists, the net of curves that covers the iris is generated and the Iris Code is also created, based on the darkness of the dots. Iris scans are less invasive than retina scans because the iris is easily seen from a few meters away. The iris responds to light modification and can provide an essential secondary verification.

Iris patterns are not susceptible to modification through age, eye disease, or alcohol intake. An individual can be recognized within a few seconds using an iris recognition device. To conduct an iris scan, an individual need not have physical contact with the device, since the participant and camera do not require direct physical contact (Ganorkar and Ghatol, 2007).

However, the drawback with iris verification is related to the cost relative to other biometric types; iris scanners are comparatively more costly. The cost of iris systems is high as it is an emerging, advanced technology. The iris is small and cannot be identified from more than a few meters away. An individual must be close to the iris scanner to be registered correctly on the system.

Facial Verification and Identification

The essential approach that people use to remember each other is our facial structure. It is also an open biometric system for the recognition and authentication of human beings. Today, with high-quality cameras with zoom capabilities, a target can also be detected from afar, making facial recognition more ideal for safety and security purposes. The technology of facial recognition is easy to implement. The only thing required to set up this recognition system is a digital camera and facial recognition software.

Further equipment such as the camera and infrared light transmitter, multi-camera set-up and so on are used for surveillance applications. Facial recognition is a flexible biometric technology that is rapidly evolving. The reason is that smartphones and personal computing devices are continually increasing in complexity and processing power, with two cameras often on the front and the back of such modern-day gadgets. This makes it easy for user identification to be leveraged (Cook *et al*., 2016).

Facial recognition software is simple to install and no extra hardware is required for today's computing devices such as mobile phones. This flexible biometric technique makes life easier. Even a brief glance can quickly unlock mobile phones. It is also used for identity identification and security applications (Tripathi, 2011).

However, facial recognition can fail to distinguish between identical twins. Facial detection might also be subject to manipulation or scam attacks due to aging. As skin becomes older, or occasionally owing to injuries, it can change in appearance. People can also undergo cosmetic surgery to alter their face. Thus, face detection is of limited value.

Fingerprint Verification and Identification

The identification of fingerprints is one of the oldest, most potent and most widely used biometrics, since people have different fingerprints. As for all biometric technology, it detects and validates a person's identity from data stored in advance. It has been a part of forensic research since the early days of fingerprint recognition. The method of identification and matching fingerprints has also progressed with the application of computers in forensic science departments. Mobile devices, door locks and also high-security access control currently widely use fingerprint recognition. Small and efficient cell phone fingerprint sensors have allowed recognition and authentication on mobile devices. The devices work to store the distinctive ridge structure of people's fingertips in fingerprint detection technologies. There are various techniques used, such as electronic, capacitive, thermal, etc. The captured human fingerprint image is changed to make it accessible and a biometric model is then produced using several sophisticated, person-specific algorithms (Ali *et al*., 2016).

Recognition of fingerprints is a low-cost, secure system that is simple to set up and the most common biometric method (Oloyede *et al*., 2013). Fingerprint identification is the simplest and cheapest process and is used in applications ranging from tool/machine unlocking to touchpads in offices. This system has also been introduced by law enforcement agencies, hospitals, clinics and colleges and universities to help identify and verify citizens. The major drawback to fingerprints is related to personal hygiene, especially in specific government entities, attendance systems and border control solutions. Also, the recognition method performance suffers from fingertip surface texture, such as wet or dirty fingers, scars, skin problems, or diseases.

Finger Vein Verification and Identification

Recognition by the finger vein is a method of biometrics that is used for a person's classification and identification. This technology works on the unique pattern of blood vessels that lies below the skin surface of the human finger. This identification system may correlate with other previously or newly stored vein finger IDs to a human finger's vascular pattern. Infrared light and a vein pattern monochrome CCD

camera are used for vein identification reconnaissance systems. The hemoglobin in the deoxygenated blood of the veins absorbs the infra-red light through your finger and, as a result, a camera captures a picture. The picture shows the pattern of the finger veins as dark lines. These data, which are sent for user authentication, are digitized and processed (Shaheed *et al*., 2015).

The vein pattern, concealed under the finger tissue, is unexposed and can only be checked with a specific device, making it virtually impossible to copy. Found below the skin, the structure of the finger vein is more protected than the fingerprints, facial recognition and related identification methods through which the biometric features are visible and can be obtained without the permission of the subject. However, only a small range of tools and systems are available. This technology is quite sophisticated and the technique is well known to only a few people.

Ear Authentication and Identification

The biometric features of the outer ear (a biological pinna) also represent physiological biometric properties. To determine the ear canal, sound waves are used. Analogous to fingerprints or the iris, the shape of the human ear canal is also unique. External devices are also required for ear authentication. The equipment has an earpiece with a microphone to capture the emitted sound waves from within the ear canal (Nakamura *et al*., 2014). Ear authentication is accurate and easy to customize because there is no need to pay attention to any graphics or testing, which makes it perfect for modern fast-paced life. However, for in-ear verification, special external earphones must be worn by the subject and this adds to the expense because the required headsets are costly.

Foot Dynamics and Footprint

A human footprint is an anatomical trait that makes for distinctive characteristics. The human foot ridge structure remains the same throughout a person's life, like skin ridges on the palm and fingerprints, which do not change over the course of one's life. This allows the use of footprints as a biometric means of personal identification. The basic scanning and sorting footprint technology is the same as most finger ridge identification systems. A human footprint is an anatomical entity that allows the identifying of features.

Footprint scanning technology is an identification method under development. The subject's footprint in motion is used for the identification of an individual in the dynamic footprint approach. If comprehension is advanced, elements like the shape of the foot, structure, frame of friction, etc. can be included. Although extensive forensic science experiments exist for this specific physiological characteristic exist, biometric footprinting is not commonly used to identify or authenticate individuals (Jain *et al*., 2004). For specific special applications, such as spas, thermal baths and discrete identification, the footprint recognition technique can, however, be useful. Footprints are not positioned as high-security applications and therefore the processing of biometric footprint data and foot dynamics is not a threat to safety. Due to several properties, such as user-friendliness of the data acquisition process, the use of dynamic footprint recognition is considered difficult in commercial biometric systems, as people generally wear footwear, which makes foot scanning difficult.

Methodology

The current literature based comparative analysis relied on previous evidence of research to gather all necessary information relative to the scope of the study and deduce knowledge from these sources to come forth with a new theoretical perspective in the field of knowledge, especially as far as the utility of the different biometric systems is concerned. The methodological approach adopted was inductive allowing for an exploration of extant literature in the subject field. Essentially therefore, the study is qualitative in nature and based purely on secondary sources of data whose interaction in the study is openly acknowledged at each stage of the study. A sum of at least 25 credible sources including SCOPUS listed journals, books and conference proceedings on Biometrics identification and verification systems were consulted to assist in the compilation. In making the analysis thereof, the study adopted a thematic approach whereby it pursued a comparative analysis of the different Biometric systems based on the acceptance and rejection rates and sensitivity and security levels among other parameters such as distinctiveness, complexity and universality among others earlier mentioned.

Analysis and Findings

Biometric Systems Components

A software-based biometric system consists of multiple vital components that are important for the overall identification and verification process. Biometric identification systems consist of: A biometric enrolment device to capture the biometricimage, such as a fingerprint device, facial camera, iriscamera, palm device to capture the image of the palm,or a mobile-based fingerprint camera

- A matching engine (algorithm) distributed over multiple servers or installed locally to support in converting the captured images into templates accepted by the matcher

Identification and Verification

A biometric network is a system for pattern recognition that works by obtaining biometric information from a human, extracting and comparing a set of features from the information acquired as a function set for the system. Within such a system, a person who wishes to be remembered uses verification, usually by a PIN, a username, or a smart card and the system tests one-to-one to decide if the verification is valid or not. Identity verification is usually used for positive recognition to avoid using the same identity being used by many people. Verification and identification are often used interchangeably, although both terms have different meanings in biometric recognition. Verification implies 1:1 Matching; it means that people assert their program identity and then get self-checked (Fig. 2). Identification refers to a situation where it is not known who the useris; they instead present their biometric data for the purpose of matching with the entire database.

The process of identification is aimed at identifying someone. It gives clients a unique number when they first register in a biometric program, which is related to the biometric prototype. As its name implies, the process of identification is designed to recognize an individual. The entire system must comprise unique numbers to "recognize" users checked for the device. The pattern is one to many (1: N) relationships in the biometric system (Fig. 3). The system recognizes a person in identification mode by checking for a match in the dataset against the templates of all users. Thus, the program makes an identity comparison (one of several) to identify a person without the person needing to assert an identity or to check if the subject is not registered on the system database.

An example of the biometric enrolment, verification and identification process is represented in Fig. 1.

Acceptance and Rejection Rates *False Acceptance and False Rejection*

The False Rejection Rate (FRR), the number of authentication rejections made for genuine users and the Fake Acceptance Rate (FAR), the number of people incorrectly accepted, are two of the main features of a biometric authentication system.

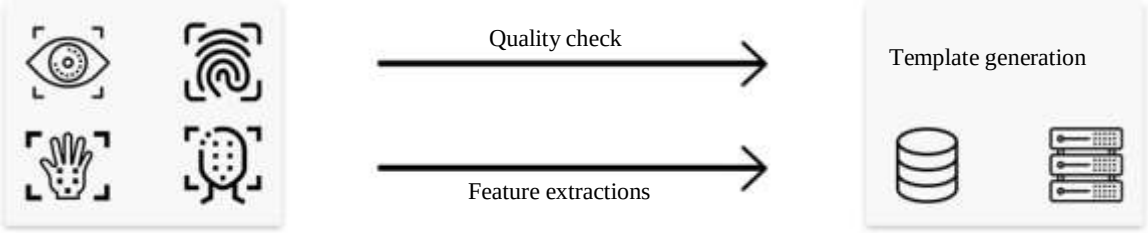
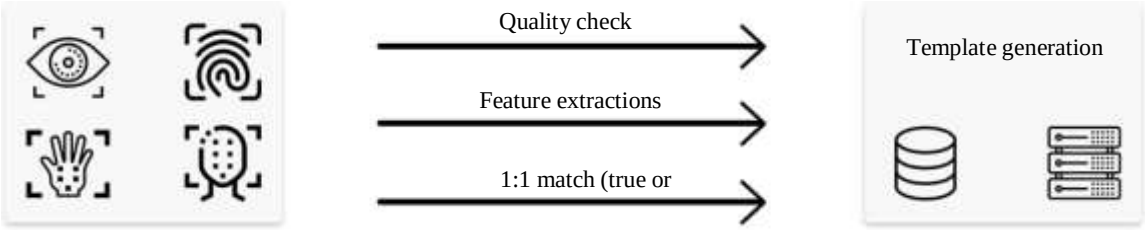
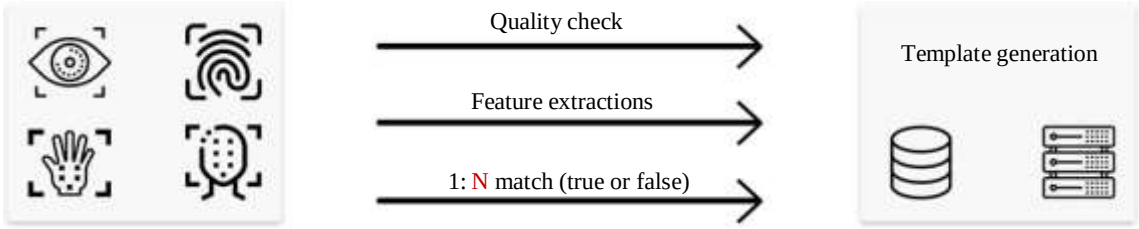


Fig. 1: An example of the biometric enrolment, verification and identification process



Interface Matching engine/algorithm

Fig. 2: Verification (1:1 Matching)



Interface **Fig. 3:** Identification (1: N matching) Matching engine/algorithm

False Rejection Rate (FRR)

The FRR attempts to measure the rejection of approved people when the decision criteria are reduced; if the corresponding score falls under the threshold, although it may be valid, the individual is seen as an impostor. In essence, it is the proportion of allowed users declined compared to the total approved user count. The FRR (also called FNMR: False Non- Match Rate) is a metric often used to measure the success of biometrics-based sensors. The FRR reveals how often the sensor incorrectly rejects valid biometric data in the corresponding algorithm (FRR = number of false rejections/number of client access*es)* ratio is dependent on both the hardware and the sensor system's software (algorithm). The typical FAR values of fingerprint scanners in smartphones is approximately 1/100,000 today, which essentially means that one in 100,000 persons on average will succeed when you allow randomly selected people to log on to your phone using the fingerprint sensor. Therefore, when a person is a genuine imposter and the threshold has a high match score, he/she is considered a valid user during matching and this leads to misrepresentation. FAR (number of false acceptances/numbers of client accesses is calculated based on the below equation:

and it is calculated based on the below equation:

$$FRR = \sum t = TTRA(t) / \sum t = 0 \infty AG(t) \quad (1)$$

Where:

$$FAR = \sum t = T \max TFA(t) / \sum t = 0 \infty AI(t) \quad (2)$$

Where:
T = The Threshold value
FA = The number of Falsely Accepted users

T = Threshold value
RA = Number of Rejected Authorized users
AG = The total number of all genuine verificationattempts.

False Acceptance Rate (FRR)

The FAR (sometimes called FMR: False Match Rate) is a metric often used for evaluating the safety of biometric systems. The FAR value indicates how many times, without the correct biometric data, the device I = The number of All Imposter authentication attempts

Failure to Enroll

This happens when the biometric system fails to recognize an enrolled user at the point of identification because the user fails to produce the required biometric trait. Failure To Enroll (FTE) It is described as the ratio of the number of unrecognized authorized users to the total number of authorized users and is calculated using the equation below:

$$FTE = \sum t = TTUA(t) / \sum t = 0 \infty AU(t) \quad (3)$$

Where:
T = The Threshold value
UA = The Unrecognized authorized users
AU = The total number of authorized users

Failure to Acquire and Failure to Capture

use, how rapidly it wakes up, how often the feature is needed and how the sensor is integrated in the final product. The compilation of the FRR-to-FAR-ratio for different types of biometric authentication systems gives an interesting insight into the compromises between safety and ease of use. If the biometrical characteristic of a person are present but cannot be identified due problems in the program, authentication/verification will not occur as the sensor is unlikely to recognize the biometric element.

Crossover Error Rate (ERR)

The crossover Error Rate (EER) shows whether the number of errors for false rejection and acceptance is equal. The balance between FAR and FRR is apparent, i.e., one will reduce as the other increases.

Sensitivity and Security Level

A compromise exists in every biometric system between the wrong Match Rate (FMR) or the wrong Non-Match Rate (FNMR). In addition, both FMR and FNMR are device threshold functions. If the device sensitivity is decreased (to reduce input and noise sensitivity), then the FMR increases. In comparison, if the device sensitivity is increased, then the FNMR increases.

Therefore, in the form of a Receptor Operating feature (ROC), the device output at all operating points (thresholds) can be depicted. A ROC curve is a FMR (1-FNMR) or FNMR plot with different threshold values. Convenience is often correlated with other characteristics of the sensor, such as how easy it is to low security (high FAR) or vice-versa (Fig. 4). The point at which the lines cross is termed the Equal Error Rate (EER), meaning that the proportion of false acceptances and false refusals is the same.

The FRR will probably rise rapidly when attempts are made to decrease the FAR to the lowest possible point. This means that the more secure the access control, the less convenient the system is. The FAR and FRR may typically be adjusted by changing the specifications to make them stringent in a security system program. From the above details, we may infer that it will lead to either a more stable (but less user- friendly) or less secure system.

Biometric Types Comparison

As the purpose of this study is to draw comparisons between the different biometric systems available, comparisons are drawn based on different factors in this field, such as biometrics used for identification, biometric features, physical features, technological features, evaluation and other features, following a review of many different research articles and documents. It is hard, however, for biometric systems to be precisely compared; many causes have been identified by researchers for this (Jain *et al*., 2004).

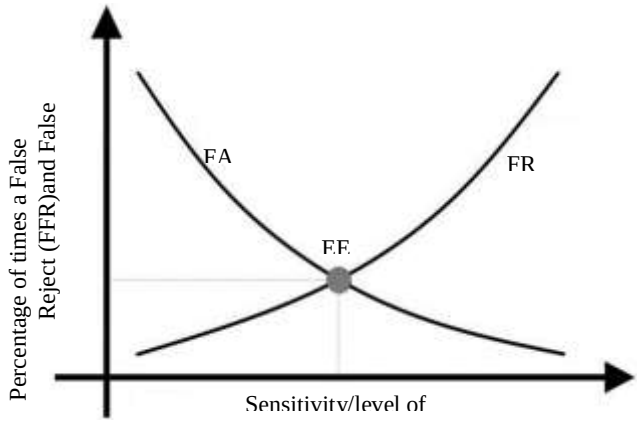


Fig. 4: *The relationship between False Rejection Rate (FRR), False* Acceptance Rate (FAR) and Equal Error Rate (EER)

Table 1: A comparison of biometrics types based on the characteristics of biometric entities

Biometric identifier	Distinctiveness	Complexity	Universality	Quantifiability	Performance	Comparison	Collect capacity	Acceptance	Cost	Use
Fingerprint	M	L	H	H	M	H	H	H	M	H
Iris	H	M	H	H	H	H	H	H	H	M
Facial	M	M	H	H	M	M	H	H	M	M
Palm	M	H	H	H	M	M	L	L	H	M
Ear	M	H	H	H	L	L	L	L	H	L
Footprint	M	H	M	M	L	L	L	L	H	L
Finger vein	H	H	H	L	H	H	L	L	H	L
Voice	M	H	H	M	M	M	L	L	H	L
Signature	L	H	H	H	L	L	M	H	L	L
Keystroke	L	M	M	L	L	L	L	L	H	L
dynamics										

H = High; M = Medium; L = Low

Table 1 presents a comparison of biometrics types based on the characteristics of biometric entities. The terms used are described in detail below:

- Distinctiveness: Each person must have various characteristics that differ from other individuals' features
- Complexity: The biometric, after a certain time, willbe fairly invariant
- Universality: Distribution of population. The biometricfeature should be present for each person separately
- Quantifiability: Quantifiable with basictechnological tools. This makes extraction simple
- Comparison: Compares consistency between two models, one being saved and the second the living model
- Collect capacity: how well the data can be collected and quantified
- Performance: precision, speed, stability
- Acceptability: to what degree the system isacceptable to users, including impact of culture.
- Cost: the financial aspects of the biometric type
- Use: the spread of the biometric type worldwide

Conclusion:

Recent progress in biometric technology has led to greater precision at a lower cost for some the biometric types, such as fingerprint and facial recognition; biometric systems are the foundation for many extremely secure identification solutions and personalized testing. Biometric solutions are now able to achieve fast, easy-to-use authentication with high precision at relatively low cost. Biometric technologies will benefit many areas. For example, highly secure and reliable e-commerce is necessary for the healthy growth of the global economy. Many suppliers of biometric devices already supply biometric verification to fulfill these and other needs for a wide range of web and client/server applications. Continuous technological advancements bring better results at a lower cost. Alternate approaches to authenticating the identity of an individual are not just a good idea to make biometric systems available to different people; they also serve as a viable alternative way to deal with identity verification and registration errors. The frequent monitoring of systems during and after installation is an excellent way to ensure that the biometric system works within normal parameters. Not only is an impostor immediately identified and denied access, but also a safe transaction activity log to track impostors can be maintained via a well-organized biometric identification solution. In many civilian areas, biometric devices will certainly be more involved in the future. Perhaps in a few years, iris scans will be used to allow access to conventional homes or cars, making keys obsolete. Perhaps money, credit cards and cheques will also become obsolete, being replaced by fingerprint recognition. However, despite the advantages brought about by the broader usage of biometric technology in our everyday lives, this technology also entails a whole new range of difficulties and problems. Therefore, it will not suffice to study only factors like cost versus performance tradeoffs or usability and security issues before deploying biometric systems. Exceptional care must be taken regarding what may be done with the acquired biometric data, who may use it and for what purposes.

References:

(1) Ahmad, S. M. S., Ali, B. M., & Adnan, W. A. W. (2012).Technical issues and challenges of biometric applications as access control tools of information security. international journal of innovative computing,information and control, 8(11), 7983-7999.

(2) Boulkenafet, Z., Akhtar, Z., Feng, X., & Hadid, A. (2015). Face anti-spoofing in biometric systems. In Biometric security and privacy (pp. 299-321). Springer, Cham.

(3) Cook, C. M., Howard, J. J., Sirotin, Y. B., Tipton, J. L., & Vemury, A. R. (2016). Demographic effects in facial recognition and their dependence on image acquisition: An evaluation of eleven commercial systems. IEEE Transactions on Biometrics, Behavior and Identity Science, 1(1), 32-41.

(4) Dua, M., Gupta, R., Khari, M., & Crespo, R. G. (2015). Biometric iris recognition using radial basis function neural network. Soft Computing, 23(22), 11801-11815.

(5) Galdi, C., Nappi, M., Riccio, D., Cantoni, V., & Porta,M. (2013, June). A new gaze analysis based soft- biometric. In Mexican Conference on Pattern Recognition (pp. 136-144). Springer, Berlin, Heidelberg.

(6) Ganorkar, S. R., & Ghatol, A. A. (2007, February). Iris recognition: an emerging biometric technology. In Proceedings of the 6th WSEAS International Conference on Signal Processing, Robotics and Automation (pp. 91-96). World Scientific and Engineering Academy and Society (WSEAS).

(7) Gatali, I. F., Lee, K. Y., Park, S. U., & Kang, J. (2013, August). A qualitative study on adoption of biometrics technologies: Canadian banking industry. In Proceedings of the 18th annual international conference on electronic commerce: e-Commerce insmart connected world (pp. 1-8).

(8) Hossain, S. M. E., & Chetty, G. (2011). Human identity verification by using physiological and behavioural biometric traits. International Journal of Bioscience, Biochemistry and Bioinformatics, 1(3)

(9) Jacobsen, K. L., & Sandvik, K. B. (2015). UNHCR and the pursuit of international protection: accountability through technology?. Third World Quarterly, 39(8), 1508-1524.

(10)Jain, A. K., Ross, A. A., & Nandakumar, K. (2011). Introduction to biometrics. Springer Science & Business Media.

(11) Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on circuits and systems for video technology, 14(1), 4-20.

(12)Kakkad, V., Patel, M., & Shah, M. (2016). Biometric authentication and image encryption for image

security in cloud framework. Multiscale and Multidisciplinary Modeling, Experiments and Design, 2(4), 233-248.

(13)Kumar, D., & Ryu, Y. (2009). A brief introduction of biometrics and fingerprint payment technology. International Journal of advanced science and Technology, 4(3), 25-38.

(14)Meng, W., Wong, D. S., Furnell, S., & Zhou, J. (2014). Surveying the development of biometric user authentication on mobile phones. IEEE Communications Surveys & Tutorials, 17(3), 1268-1293.

(15)Mondal, S., & Bours, P. (2014). A study on continuous authentication using a combination of keystroke and mouse biometrics. Neurocomputing, 230, 1-22.

(16)Nakamura, T., Goverdovsky, V., & Mandic, D. P. (2014). In-ear EEG biometrics for feasible and readily collectable real-world person authentication. IEEE Transactions on Information Forensics and Security, 13(3), 648-661.

(17)Oloyede, M. O., Adedoyin, A. O., & Adewole, K. S. (2013). Fingerprint biometric authentication for enhancing staff attendance system.

(18)Patel, A. N., Howard, M. D., Roach, S. M., Jones, A. P.,Bryant, N. B., Robinson, C. S., ... & Pilly, P. K. (2014). Mental state assessment and validation using personalized physiological biometrics. Frontiers in human neuroscience, 12, 221.

(19)Shaheed, K., Liu, H., Yang, G., Qureshi, I., Gou, J., & Yin, Y. (2015). A systematic review of finger vein recognition techniques. Information, 9(9), 213.

(20) Solayappan, N., & Latifi, S. (2006). A survey of unimodal biometric methods. In Proceedings of the 2006 International Conference on Security and Management (pp. 57-63).

(21) Tripathi, K. P. (2011). A comparative study of biometric technologies with reference to human interface. International Journal of Computer Applications, 14(5), 10-15.