Bachelor's thesis

Bachelor of Engineering, Information and Communications Technology

2021

Sagar Dhakal

MULTI-BIOMETRIC SYSTEMS THEIR APPLICATION AND SECURITY

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR’S | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor of Engineering, Information and Communications Technology

2021 | 61

Sagar Dhakal

MULTI-BIOMETRIC SYSTEMS THEIR APPLICATION AND SECURITY

The advancement of technology is currently showing no signs of settling down in the 21st century. However, the modernization of security systems with the help of human body parts, often called ‘biometrics.’ has aided in the maintenance of proper security to an organization or individuals. The thesis aims to give a dual study related to multibiometrics system, including a literature review of the transformation of biometric applications and their security over the years to protect an individual or an organization’s privacy and safety.

The theoretical part of this thesis provides a brief account of the history of biometric systems. The thesis also discusses the current application of biometric systems in different sectors such as the Military, Law, Healthcare. It also provides a broad understanding of different types of biometric systems and their identifiers. The areas of vulnerability of the system are well pointed out inside this thesis which also discusses the attack made at a different level in a system.

The qualitative method is used to collect information by using secondary data from different sources, including articles, journals, books, internet resources, magazines, websites, and research papers. The thesis also goes through a number of the available protocols for template protection schemes that have been presented by researchers.

The findings of this study include an analysis of the most common biometrics approaches, as well as their benefits and drawbacks. Moreover, the result of this thesis recommends using a multi-biometric system than a unimodal biometric system to maintain the privacy of individuals and organizations.

KEYWORDS:

Biometrics, multi-biometrics, identification, Biometric templates, security protocols, Template protection schemes

CONTENT

FIGURES

LIST OF ABBREVIATIONS (OR) SYMBOLS

AI	Artificial Intelligence
ARL	Army Research Laboratory
ATM	Automated Teller Machine
CAC	Common Access Card
DDS	Defence Digital Service
DNA	Deoxyribonucleic Acid
FMR	False Match Rates
FNMR	False Non-Match Rates
FTA	Failure To Acquire
FTE	Failure To Enroll
GP	General Practitioners
ID	Identity Document
PCR	Polymerase Chain Reaction

1 INTRODUCTION

The human body system works on sense. Each human body possesses a unique mechanism inside its system. There could be a different reaction by the sensory organ of varying individuals towards the same stimulus too. A condition that is adventurous to one could be a breath-taking experience to others. The sensory organs of a different person send different impulses to the brain through the neurons, where they are processed and interpreted, and action is generated. With varying reactions from individuals, there would be other organ mechanisms like heartbeats, pulse rates, blood pressure, and so on. The multi-biometrics system works on those reflexes generated from sudden action or already possessed in the unique structure of the human system, such as fingerprints, DNA, footprints, voice pattern, face recognition, retina scan, odor, etc.

Biometric authentication, simply “biometrics,” refers to a natural and reliable answer to the matter of identity determination by establishing the identity of an individual based on “who he is” instead of “what he knows” or what he carries.” The term “Biometrics” is derived from the Greek words bio and metrics, where bio means life and metrics means to measure. The Merriam-Webster Dictionary defines “Biometrics as the measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity.” In a biometric security system, the identification of a particular person is carried out by matching his/her previously saved data which could either be his/her physiological or behavioral character (e.g., fingerprint, face, iris, hand geometry, signature, etc.) (see Figure. 1) and could not be changed by other external factors (Jain et al., 2004).

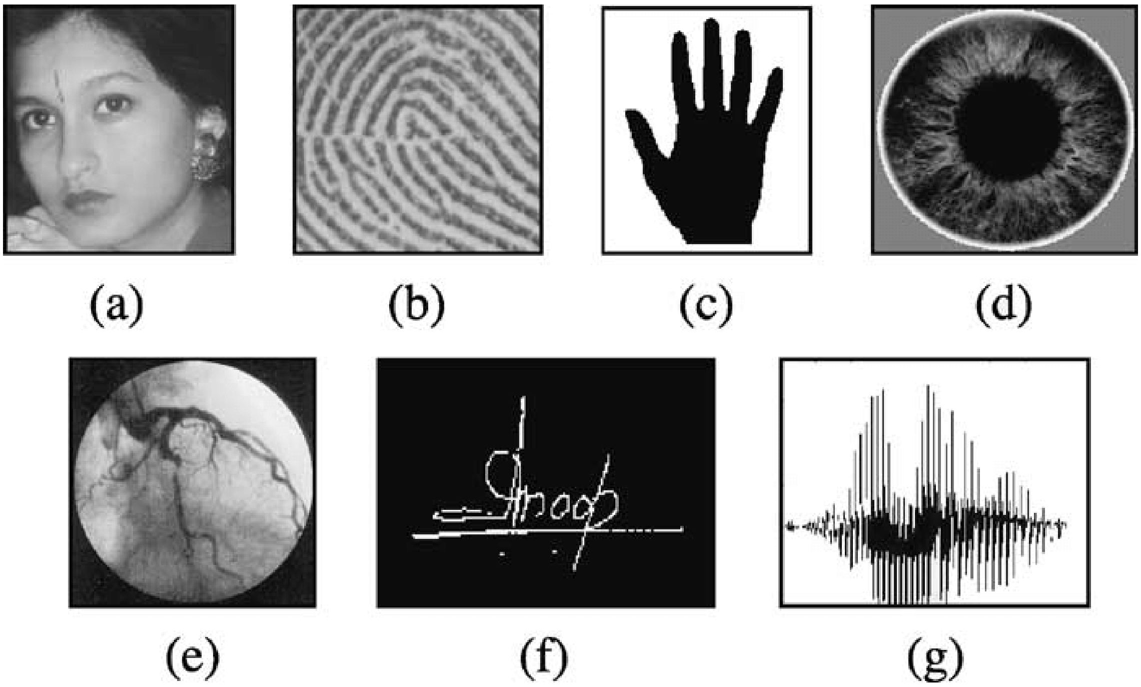


Figure 1. Sample biometric traits: (a) Face recognition (b) Fingerprint (c) Hand geometry (d) Iris (e) Retina (f) Signature (g) Voice (Jain et al., 2004).

For example, an individual's fingerprint is unique, and it cannot be changed; it also remains the same throughout the lifetime of the individual. According to Jain et al. (2004), any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

- Universality: every person should have the characteristics.

- Distinctiveness: people must be sufficiently different in terms of characteristics.

- Permanence: the characteristic should be sufficiently constant (concerning the matching criterion) over a period of time.

- Collectability: the characteristic can be calculated quantitatively.

As we enter the phase of digitalization, the issues of disloyalty, dishonesty, and hacking have become challenging. All of the stored data, secret formulas, or policies could be leaked in a matter of time. Within a second, a person's whole life savings might be moved to another unknown bank account. The biometric security system adopted in several organizations such as business, banking, health, government bodies, and others solves this problem in these terrible scenarios. We are witnessing the so-called strong passwords or code becoming easily accessible by active hackers through the internet. Also, passwords and codes are less convenient as they can be forgotten or lost. However, this is not a problem when using a biometric security system. All data taken are part of our body system, accurate and the same throughout the lifetime. This security system has many advantages over the traditional method. They are much more reliable, unique for every individual, offer no chance for guessing, and do not invade privacy rights.

Furthermore, there is no password for the user to remember and no identification card to lose in the biometric system, making it more user-friendly. Bio-metric methods are used widely in many fields to achieve increased security. The biometric market has grown significantly due to the numerous advancements and innovations in this field in recent decades. As shown in Figure 2, the private sector market share increased significantly between 2007 and 2015, owing to the increasing demand for biometric solutions in smartphones and cameras (Guennouni, Mansouri, & Ahaitouf, 2019).

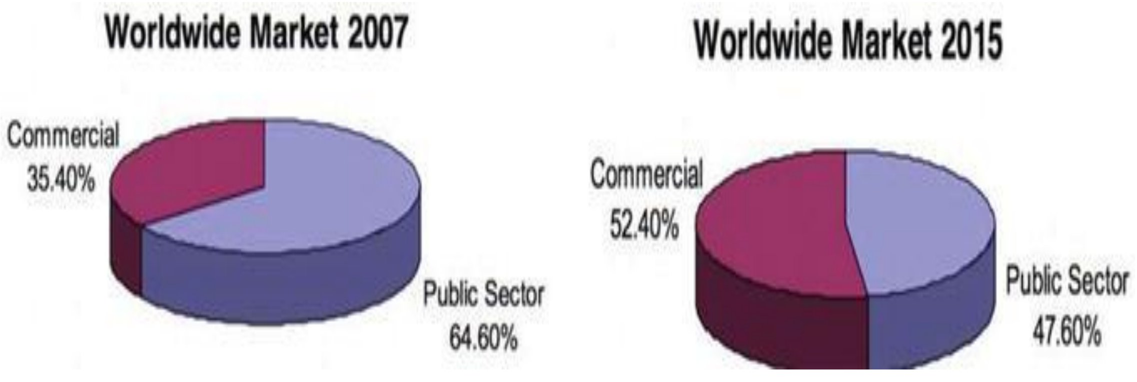


Figure 2. Distribution of the global biometric market between 2007 and 2015 (Guennouni, Mansouri, & Ahaitouf, 2019).

1.1 Aims and objectives

The main aim of this research, “multi-detection biometric and its security,” is to give detailed information on biometrics, their types and areas, their security threats, and solution. The focused objectives of this study are given below:

- To present the detailed information of the topic “Multibiometric System.”
- To give the information about “Why biometric and their applications?”.
- To give the information of advantages and disadvantages of using biometrics.
- To provide information about the security vulnerabilities of biometric and solutions to overcome those threats.
- To research the attacks against biometric systems.
- To research Biometric Encryption: technology for strong Authentication, security, and privacy.

1.2 Structure of thesis

This thesis is structured in six different chapters. It starts with a brief history of biometrics in the first chapter, followed by areas of the prevalence of biometrics in chapter two. The different biometric identifiers are discussed in chapter three. Biometric systems and performance metrics are described in chapter four. In contrast, the biometric security system, its design, advantages, disadvantages, vulnerabilities of biometric authentication, and template protection schemes are discussed in chapter five. Finally, chapter six of this thesis concludes and provides information for future work, respectively.

1.3 History

The new automated techniques and systems widely used in recent days for biometrics security were originally conceived hundreds, even thousands of years ago.

The oldest evidence of the use of biometrics dates back to as early as 500 B.C., in a Babylonian empire where the businessman used to record fingerprints on a clay tablet for identification and verification purposes (Mayhew, n.d.). Traders were classified in early Egyptian history by their physical descriptors to distinguish between trustworthy traders with a strong reputation and a track record of successful transactions and those new to the market (Mayhew, n.d.). The Persian book "Jaamehol-Tawarikh," written in the 14th century, contains comments on identifying people using fingerprints (Mayhew, n.d.). The first biometric identification system was reported in the 1800s in Paris, France. Alphonse Bertillon developed a system for classifying and comparing prisoners based on precise body measurements. Although this system was far from ideal, it was the first step toward using unique biological characteristics to verify identity. The other approach was using fingerprints by the police department in Asia, South America, and Europe. By the late 1800s, a system for indexing fingerprints had been established that allowed for retrieving records in the same way that Bertillon's method did. Still, it was based on the more individualized metric- fingerprint patterns and ridges (Mayhew, n.d.). Azizul Haque was the first creator of a robust system for indexing fingerprints in India for Edward Henry, Inspector General of Police, Bengal, India. This system, known as the Henry System, and its variants are still used to identify fingerprints (Mayhew, n.d.).

In the following century, biometrics systems began to emerge, coinciding with the discovery of computer systems. Some of the highlights from the 20th and 221st century are listed below:

- The Bertillon system collapsed in 1903 when two persons determined later to be twins were sentenced to the U.S. Penitentiary at Leavenworth, KS.

They possessed almost the exact measurements using Bertillon's system of measurement.

- The concept of using iris patterns for identification was proposed by Frank Burch, an ophthalmologist, in 1936.
- Under contract with the U.S. government, Woodrow W. Bledsoe produced the first semi-automatic face recognition system in the 1960s. This system required the administrator to locate features on the images such as eyes, ears, nose, and mouth.
- By 1969, fingerprint and facial recognition had become so popular in law enforcement that the FBI dedicated funds to improving automated systems. This sparked the development of more sophisticated sensors for biometric capture and data extraction (Douglas, 2020).
- The National Institute of Standards and Technology established a Speech Group in the 1980s to research and advance speech recognition technology. These experiments are the cornerstone for today's voice command and recognition systems (Douglas, 2020).
- The ideas of irises and fingerprints being unique to each person were suggested in 1985, and the first iris recognition algorithm was patented by 1994. Furthermore, it was discovered that blood vessel patterns in the eyes were unique to each person and could be used for authentication (Douglas, 2020).
- The face recognition problem was tackled by Kirby and Sirovich using principal component analysis, a standard linear algebra technique in 1988 called the Eigenface technique**.**
- In January 2001, in Tampa, Florida, a facial recognition device was installed at the Super Bowl to recognize "wanted" individuals entering the stadium. Unfortunately, even though no "wanted" individuals were identified, the demonstration managed to misidentify as many as a dozen innocent sports fans.
- Osama bin Laden's body was marked using biometric authentication in 2011. The CIA used facial recognition technology in addition to DNA to

identify Osama bin Laden's remains with 95 percent certainty (Mayhew, n.d.).

Biometric technology research has advanced at a breakneck pace in the last ten years. Biometrics has evolved from a futuristic technology to an integral part of daily life. In 2013, Apple added a fingerprint scanner to the iPhone, paving the way for biometric authentication to become widely accepted. Biometrics are used in many applications nowadays, and most smartphones have them as an authenticator for everyday practices (Douglas, 2020).

2 APPLICATION OF BIOMETRIC SYSTEMS

Biometric systems have been implemented in many fields for security purposes. Biometrics is the fundamental technology that enables human identification, from fingerprint attendance systems at office doors to fingerprint unlock on smartphones. Biometrics is helping the individual by facilitating safer and much reliable transactions, which ultimately makes life easier. It is undoubtedly cost and time-effective. Biometric solutions are used to address the needs of the following domains:

2.1 Law enforcement and public security

As the name implies, law enforcement is the process of ensuring that government-enacted laws are implemented and enforced as intended. The governing bodies set the perimeter of freedom for citizens of their nation to maintain peace and harmony. Any person who violates public regulations or disrupts the rules is brought to justice. Bringing culprits to justice necessitates correct identification as well as evidence showing their participation in criminal activity. To escape the punishment, culprits attempt to elude law enforcement by changing their identities, addresses, and appearances. Law enforcement authorities are always in desperate need of accurate and fast detection of offenders and criminals, in particular. Innocent people can suffer and even die as a result of identification errors. This is where biometrics provide a solution to identifying the correct person who is accused of charges. For a long time, law enforcement agencies have had a close relationship with fingerprints. However, new biometric technology uses various modalities and mixes them to reduce inaccuracies and improve performance. Facial recognition, iris recognition, DNA profiling, and other biometric modalities (see figure 3) are widely used in addition to fingerprint biometrics (Thakkar, n.d.).

Any proposed laws can be taken into action only if a suitable proof is gathered. The run-away of the actual culprit may happen if the process is delayed due to a lack of evidence. Since the introduction of biometric systems in law enforcement agencies, such situations are reduced. The law enforcement agencies gather biometric data of known criminals who have already served or still serve their punishment, such as a thumbprint, hand geometry, iris scan, etc., for future use to identify the criminal if the crime happens in the future. Booking new suspects who are not yet on law enforcement's biometric radar allows them to collect their biometric data and enter it into their system. If they continue their illegal activity, biometric systems help law enforcement authorities to monitor and locate them in the future. Face biometrics and fingerprint recognition are the two most common biometric technologies used by the police department, assisting prison officers in maintaining law and order within the prison. One of the many problems that biometric systems can easily overcome is tracking inmates during their movements inside the prison. Inmate movement from one point to another can be troublesome if they do not arrive at their destination on time. This problem can be solved by conducting a biometric scan on both ends. Similarly, biometric traces left behind by those involved in a crime can be the most successful method of moving a case forward. If such an event occurs, the first action to look for is these prints. The collection of these human prints is the next step which forensic experts perform. These prints are kept safe and taken to forensic laboratories compared to existing biometric scans of suspects.

The biometric system can also be used to secure the public from crimes and terrorist activities. As the world becomes more digitally and physically linked, the threat level rises as well. In recent years, the number of cyber-security and terrorism incidents has increased, and to defend against such threats, biometric systems can play a vital role. Law enforcement authorities in many countries deploy smart traffic cameras that can do much more than just recognizing number plates. These high-resolution cameras will identify people inside the vehicles and send out a warning if they are suspect. The ability to recognize people in a crowd in real-time or after an incident is gaining popularity for public protection in cities, airports, border crossings, and other sensitive areas like stadiums and places of worship. A live-face recognition device can instantly identify the suspects to prevent possible blasts or crime. The advancement of technology has helped discover portable scanning devices, making the law enforcement agencies' tasks significantly more accessible. Earlier, the suspects had to be brought to a specific location to carry out the testing, due to which there would be a time delay to catch the criminal, and the culprits could run away. However, now, this problem is solved due to the invention of mobile I.D. scanners, fingerprint scanners, iris scanners, DNA fingerprinting scanners, etc. (See Figure 4, 5, 6), which are easy to carry and linked directly with the database of suspects through the internet.

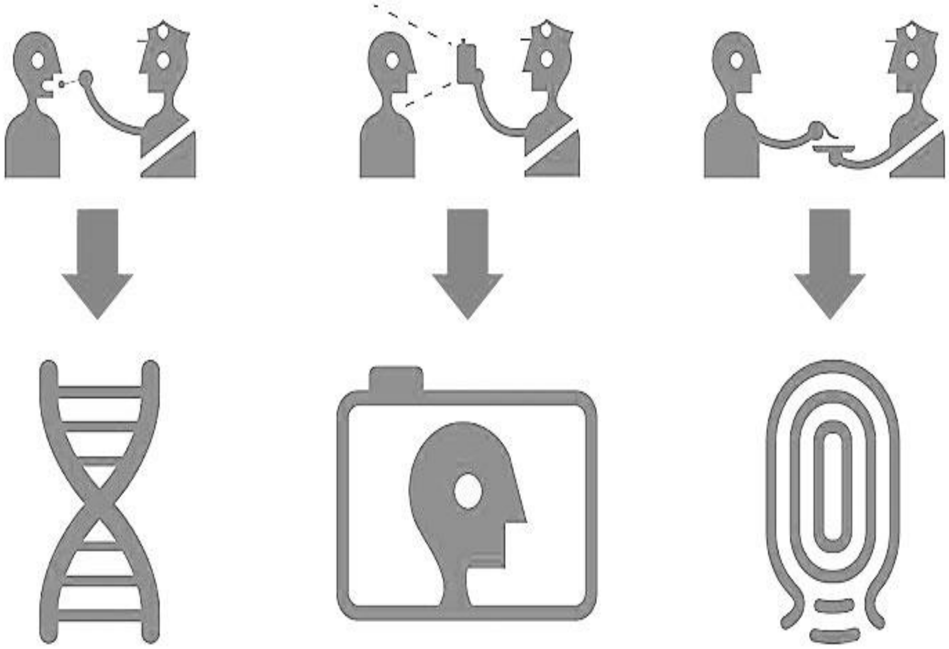


Figure 3. Multimodal biometrics in law enforcement agencies (In order, DNA Profiling, facial recognition, fingerprint) (Thakkar, n.d.).

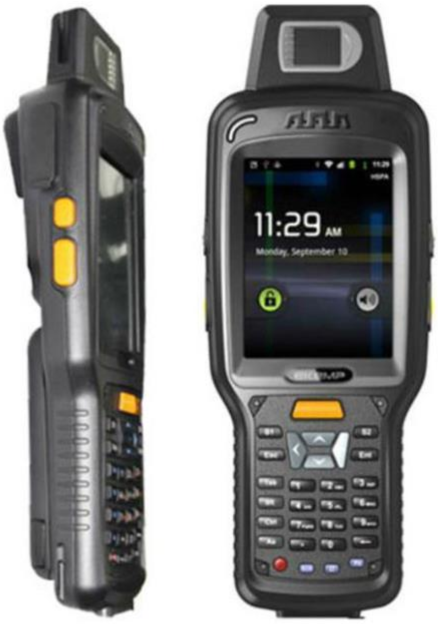


Figure 4. Portable police fingerprint scanner used by law enforcement agencies (Thakkar, n.d.).

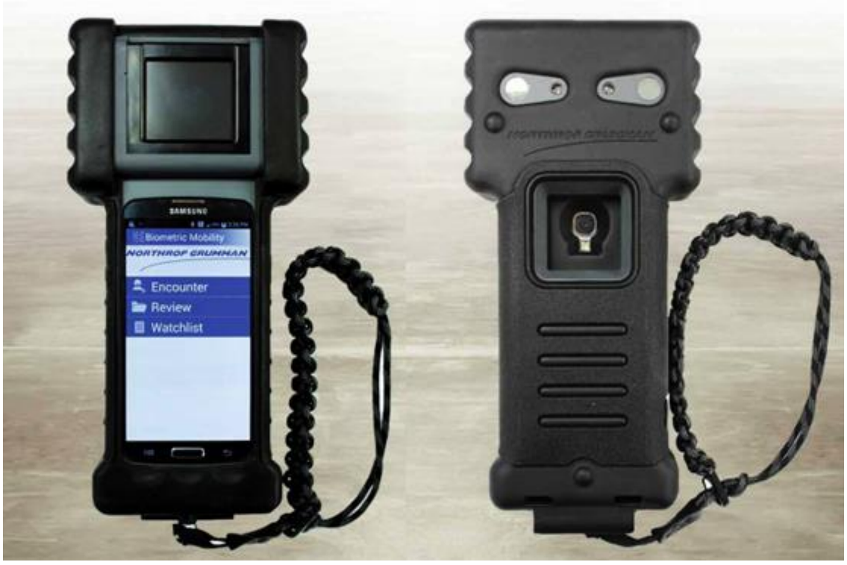


Figure 5. Handheld iris scanner in use by FBI, provided by IriTech (Iritech, n.d.).

Figure 6. DNA Fingerprinting device used inside prison (Insideprison, n.d.).

2.2 Border control, travel, and migration

The interest and research into biometric technology's ability to allow accurate identity checks has sparked in recent years due to a large number of security issues resulting from the rise of transnational crime and terrorism. Biometrics, which has long been used in criminal trials as well as in the private and industrial sectors, has gotten a lot of attention in recent years as a means of "filling the gaps" in traditional methods of border control. The most common biometrics characteristics include the authentication from fingerprints, hand geometry, iris shape, face, voice, ear shape, hand-written signatures in the border area. Border security guards can use these biometric data types to perform one-to-one (authentication) or one-to-many (verification) identity checks quickly and accurately. A one-to-one review, in simple terms, decides if a person is who he claims to be, such as when comparing a signature to one on a legal document. Likewise, when a fingerprint is compared to thousands of fingerprints in a database, a one-to-many search can distinguish one person from among many. The biometrics security method is different among countries. For example, both the E.U. and the U.S. have chosen inkless fingerprints and digital facial recognition by digitized images for border checks, while Saudi Arabia has selected Iris recognition technology (Migrationpolicy, 2005).

The introduction of a biometric passport (Also known as an e-passport or a digital passport) is gaining wide acceptance worldwide for security purposes. The biometric passport is embedded with an electronic microprocessor chip containing biometric information that can be used to authenticate the passport holder's identity. The Common Biometric Passports possess a data structure of traditional text information and personal bio-information (see figure 7). It uses contactless smart card technology, including a microprocessor chip (computer chip) and antenna (for both power to the chip and communication) embedded in the front or back cover, or center page, of the passport (Porwik, 2009). A biometric passport has pages with complicated designs, complex watermarks, and a data chip (see figure 8). Since it uses personal characteristics such as facial or eye maps and fingerprints as primary identification features, biometrics are considered more personal and accurate than a passport picture or a PIN. The International Civil Aviation Organization (ICAO) approved these biometric features after analyzing various biometrics, including retinal scans. Advanced biometric information, such as fingerprint scans and iris scans, is gradually being added to the ePassports of countries worldwide (Mutabazi, 2017).

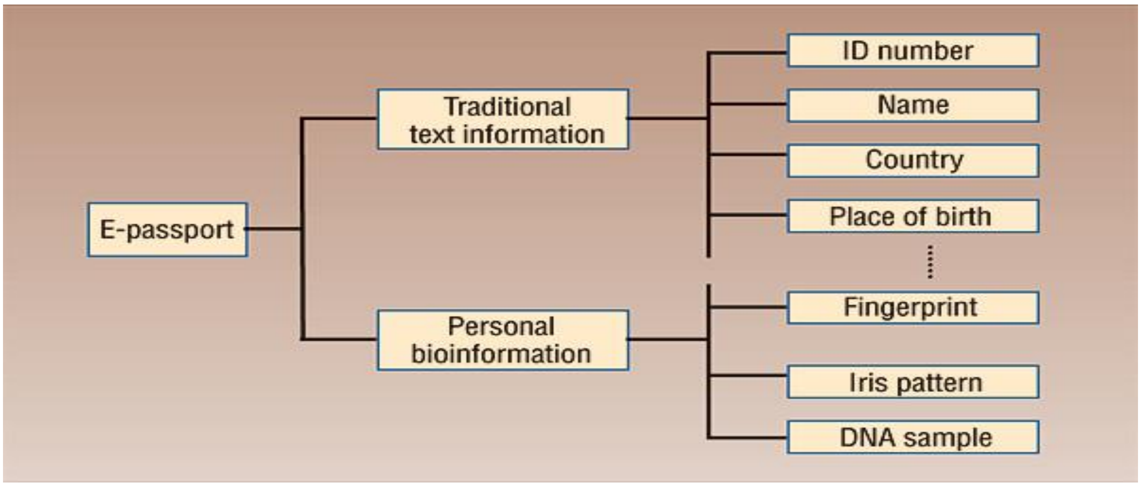


Figure 7. The data structure of biometric passports (Mutabazi, 2017).

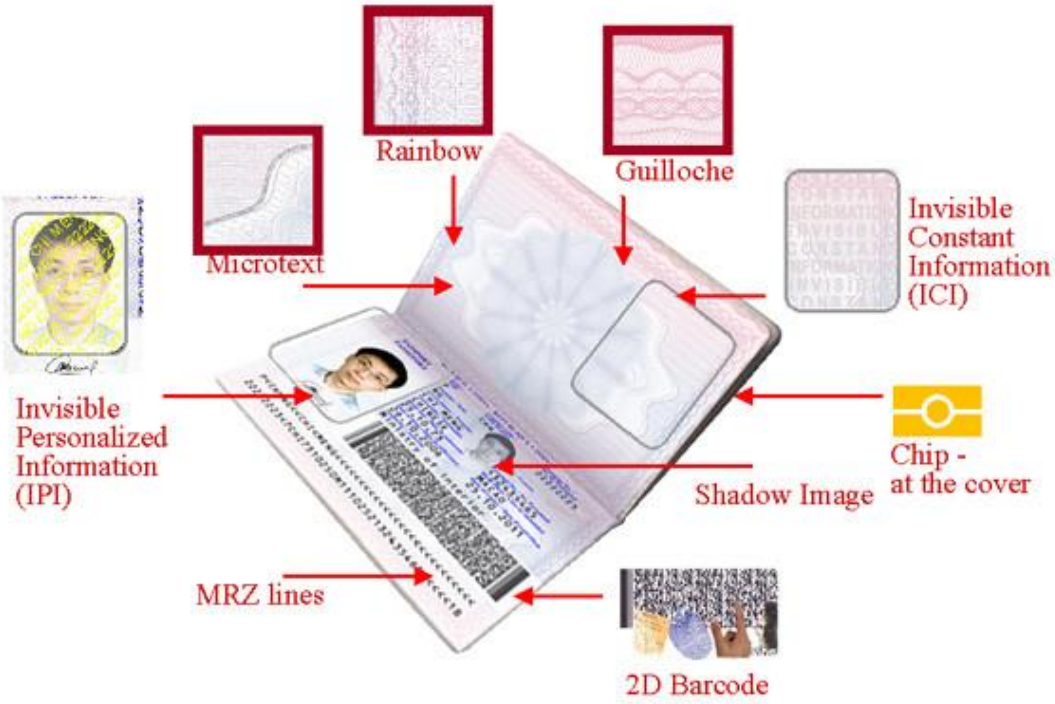

Rainbow
Guilloche
Microtext
Invisible Constant Information (ICI)
Invisible Personalized Information (IPI)
Chip - at the cover
Shadow Image
MRZ lines
2D Barcode

Figure 8. Well labeled Common biometric passport (Mutabazi, 2017).

When a traveler possessing a biometrics passport places a passport in a scanner, it will read all the biographic data and biometric details stored inside a chip. If authenticated, it proceeds to the next step, where face recognition is carried out. The device then communicates with the server to compare the passport holder's face captured by the camera with the image obtained from the Integrated Chip. The consumer is considered authenticated if the two images match. Due to its advanced technology and zero error, this is the most reliable security system for controlling border security. This system helps to identify the criminal if they intend to come inside the country. Biometrics are used to register internally displaced persons, returnees, and vulnerable refugees, administer and distribute humanitarian aid and integration grants, assist governments with identity verification when issuing passports, visas, and other travel documents, and verify traveler identity by government border authorities (Kwon & Moon, 2008). Likewise, it also helps to identify the migrants who are settling inside the country illegally. This system can stop travelers who carry fake passports and travel from one country to another.

2.3 Military operations

Biometrics systems can be used in a variety of ways during military operations. Advances in various technologies, such as wireless, artificial intelligence (A.I.), and machine learning, have fuelled the adoption of biometrics in military operations. As discussed earlier, biometrics encompasses a wide range of identification technologies, such as fingerprints, facial scans, and iris patterns, all of which have improved accuracy and reliability. Fingerprints are the most mature because they have been around the longest and are generally less expensive than other biometrics, while many people consider Iris to be the most secure. The military's focus and spending on biometrics technology have increased due to the war on terrorism. Few advances in biometric technologies led by the military from different nations are discussed below:

2.3.1 The soldier’s wearable authentication token project

Since the prototype system was finalized in 2019, the army's wearable authentication tokens, which support identity authentication, have been in continuous iterative development. The wearable identity tokens combine public-key–based credentials with advances in the commercial wireless payment industry and flexible hybrid electronics (Myerson, 2020). The tokens will use public-key–based authenticators, just like the common access card (CAC). Soldiers can use them to connect to an end-user device wirelessly and safely via Bluetooth Low Energy. The tokens are wireless, lightweight, flexible, and rugged, and they can be slipped into a soldier's pocket, attached to a sleeve, or integrated into a Fitbit-style wristband (Cox, 2019). Currently, the tokens are in the prototype stage. It is expected that commercial development starts in late 2021, and field tests will begin in early 2023 (Myerson, 2020). If this token project successfully comes into implementation, the benefit is surreal. It would help in the tracking of the military soldiers and their positioning. This will help in rescuing the battalion if they need medical or team help.

Figure 9. A wearable authentication token (Myerson, 2020).

2.3.2 Identifying enemies in the dark

The Army Research Laboratory (ARL) of the United States has conducted experimental experiments that combine facial recognition technology with thermal imagery to help troops identify people of interest in the dark. By detecting radiated heat from the skin, the new technology uses Artificial Intelligence, machine learning, and infrared cameras to identify facial patterns. ARL is working on improving its algorithms as well. The initial algorithm that ties the data into the integrated software and hardware platforms has already been developed by the army's corporate research laboratory and a team of scientists. The most significant benefit is that thermal imaging can capture distinct features hidden behind a face mask. Thus, it allows for facial recognition in low-light situations at night. The problem is that the imaging only works with thin, highly tight-fitting facial coverings (Myerson, 2020).

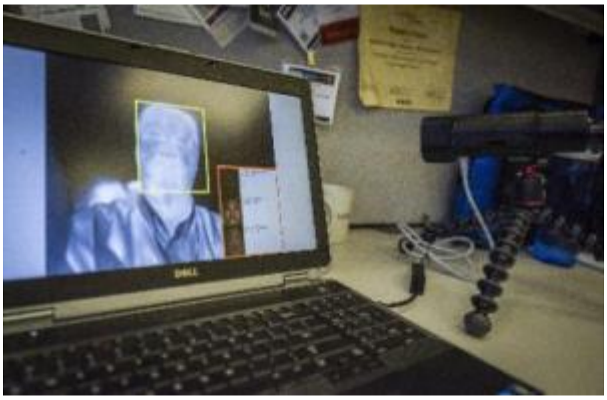


Figure 10. Radiated heat from a thermal image is used to test facial recognition technology (Myerson, 2020).

2.3.3 Basic optical biometric analysis

The Defence Digital Service (DDS) has developed a prototype app that will allow service members on the tactical edge to identify friends and potential enemies using biometric technology quickly. It improves the existing biometric technology used to verify the identity of partner forces and local civilian support staff. This technology developed by DDS will be crucial in ensuring the safety of Soldiers and partners while on a mission to serve their country (Planet biometrics, 2020).

2.3.4 Whoop partnering with U.S. military for health tracking

The United States military has partnered with Whoop to provide biometric health monitoring to the 25th Infantry Division based in Alaska. The performance and sleep data of the ‘Spartan Brigade paratroopers will be tracked using Whoop wearable sensors and an accompanying mobile application to monitor their health biometrics. The brigade commanders will use the biometric data to better understand the troops' resiliency and maximize their hostile environment performance. Approximately 1,000 volunteer paratroopers will use their Whoop wearables to track their exertion, heart rate, and sleep data in areas with little sunshine, strong winds, and temperatures below freezing to improve their performance. The study has two objectives. To begin with, soldiers will gain a better understanding of themselves. Second, troops will be aware that their commanders are working hard to understand the impacts of training and the Arctic environment’s impact on their mental and physical health. The soldiers' strain and recovery patterns will be analyzed using the biometrics gathered (Jarrahi, 2021).

2.4 Healthcare and subsidies

Biometrics security is becoming increasingly commonplace. Biometric technology has recently been hailed as the way of the future in healthcare, both in terms of patient security and better time management. According to Just, at al., (2016) medical errors cause approximately 195,000 deaths in the United States each year, with identity errors accounting for 10 of the 17 deaths. Preventing patient identification errors has been and continues to be an essential research topic. Many hospitals and general practitioners (G.P.) surgeries now rely entirely on key cards for access to areas inside the building. Unfortunately, if key cards are misplaced or lost, they can lead to serious security breaches, putting the lives of those inside the building at risk. Biometrics, on the other hand, would only allow access to those who have the appropriate permissions. As a result, sensitive information, equipment, and so on are only accessible to specific individuals, for example, a fingerprint which is nearly impossible to duplicate. Patient information in hospitals is sensitive and highly classified, and it must be kept secure at all times. Biometric technology can help control the visibility of this information in this way, allowing only those with permission to access the files and even the rooms where they are kept (Just, at al., 2016)

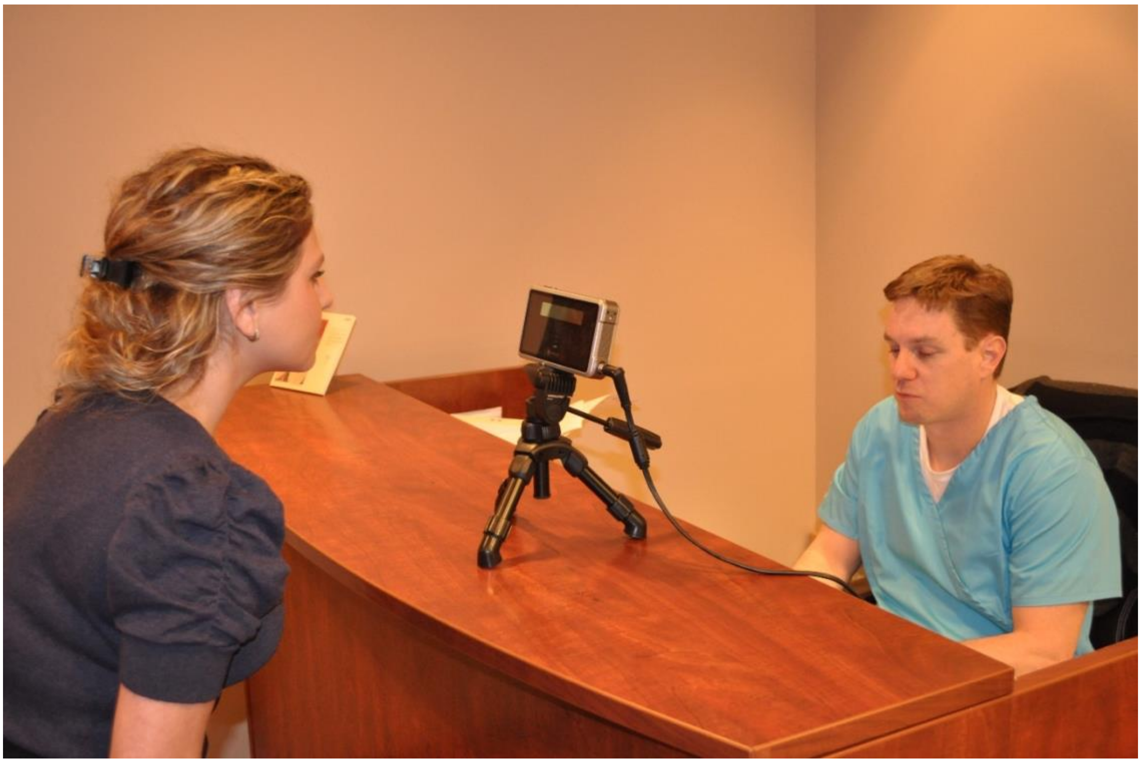


Figure 11. Iris biometrics patient identification system using Iris Scanner (Trader, 2012).

Increasing patient identification accuracy to prevent avoidable medical errors and duplicate medical records saves money and time. It improves data integrity by preventing a chain reaction of mistakes across networks resulting in irreversible physical harm and even death (Trader, 2012). There is also a future option for biometrics, which could benefit both patients and workers in all areas of healthcare. To ensure that patients receive the best treatment for their disease, it's critical that their information is up to date and accurate. However, if records are lost or, worse yet, violated, it could significantly impact the ability to look after and care for patients. However, this is where biometrics could come into play. For example, healthcare workers may use a biometric scan to identify patients and easily access their records. This capability could be extended beyond hospitals and used for things like pop-up clinics and blood donation drives. A biometric scan could confirm a person's identity and, of course, blood type if they wanted to donate blood. Biometric technology will, in this case, replace the need for blood donor cards, reducing the risk of displacement and human error. Because of the improved reliability and security, this is a significant benefit for biometrics in general. It's also nearly impossible to hack and share the information stored on readers. There is another future use in the medical sector; Telemedicine, for example, has become a more common method for improving access to care in remote or underserved medical areas. Biometric authentication can be used to make telemedicine portal logins more secure and convenient. A Canadian healthcare technology firm has already tested Biometric-enabled mobile drug dispensaries. These at-home devices use facial recognition to dispense medications and track whether or not they were taken as prescribed (Aware, n.d.).

Biometrics in healthcare has the potential to minimize patient fraud in the future. Biometric authentication, which includes facial and fingerprint recognition, can shape the industry and remove any attempts by people to impersonate other patients to gain access to treatments and medications. As previously stated, Fingerprints are nearly impossible to reproduce with biometric readers, as images of the fingerprints are not stored on the reader. As a result, the appropriate care and treatment can be provided to the appropriate persons. In addition, biometrics has the potential to solve the issue of the language barrier. Where there are communication errors between healthcare workers and patients, biometrics will significantly improve treatment. For example, a healthcare worker may use a biometrics scan to access their medical history (Westgate, 2018).

2.5 Commercial applications

For many reasons, we've seen an increase in employers switching from conventional modes of protection and access control to biometric technology over the years. Biometric technology helps employers to streamline their authentication process. Since physical characteristics are involved in identifying employees, biometric technology offers a more efficient, sophisticated authentication solution and access control than a conventional system. Some essential purposes of use of biometrics in commercial sectors are discussed below:

2.5.1 Security

Security is the most common justification for using biometrics in the workplace. As the world becomes more linked, it is clear that conventional security approaches are no longer sufficient to secure what matters most. Thankfully, biometric technology is more available than ever before, ready to add protection and convenience to everything that needs to be secured, from a car door to a phone's PIN. It applies to all sectors due to its ability to stratify security settings using biometrics. Biometrics have been used to the utmost extent possible in healthcare, improving patient protection while reducing liability. Violations of health records can cost a healthcare facility hundreds of thousands of dollars (The Guardian, 2019). Biometrics security can be of great importance for retailers in the business. Retailers may use face detection to recognize a premium customer or a former shoplifter as soon as they enter the store. When the machine detects one, it notifies the store manager. According to the stat from the guardian(2019), "Retailers in the U.K. are losing an annual $900 Million loss due to the theft, and they are looking forward to using face recognition technology to prevent the loss as it has become pointless to report shoplifting to the police".

2.5.2 Finance

Financial recognition, verification, and authentication in commerce are among the most popular applications of biometric technology, and they help make banking, ordering, and account management safer, more convenient, and responsible. Biometric solutions in the financial sector help ensure that a customer is who he or she appears to be while accessing confidential financial data by matching his or her specific biometric characteristics to a model stored in a device or on a secure server (Guennouni, Mansouri, & Ahaitouf, 2019).

2.5.3 Time loss prevention

The use of biometrics in business is not limited to security or finance. Biometrics has proved to be successful in avoiding time loss in many companies. Rather than using a pin code or an employee number, biometric time clocks depend on the individual's presence at their place of business. Since buddy punching can cost an organization up to 5% of its annual gross payroll, workers must be physically present while they're on the clock. Likewise, an employee identification card can quickly be passed on to another employee for early arrival or late-exit, but a fingerprint is more challenging to leave behind. Biometrics in the workplace prevents these types of time theft and allows more precise adherence to employee attendance policies (Ahmad & Hariri, 2012).

2.6 Examples of companies adopting biometric technology

Over the years, it has been clear that many companies are switching over their security system from traditional to modern ones, i.e., biometric technology. The purpose of shifting was discussed in the points above. Few examples of such companies, devices they are using, and the system of working of that modern technology are discussed in points below:

2.6.1 American airlines facial recognition biometrics

American Airlines is one of the major airlines in the United States using biometric technology by developing a biometric facial recognition software that aims to streamline a customer's boarding process. Biometric technology has removed the need for paper boarding passes for passengers departing from Dallas Fort Worth International Airport. This one-step facial recognition program scans each customer passing through the boarding gate and compares it to a database maintained by U.S. Customs and Border Protection, verifying their identity. Customers' identification is cleared in seconds if their passport photo is already on file with Custom Border Patrol, and they can proceed to the gate in record time. This innovative use of biometric technology makes identifying passengers much more effective, reliable, and safe (Ievo, 2019).

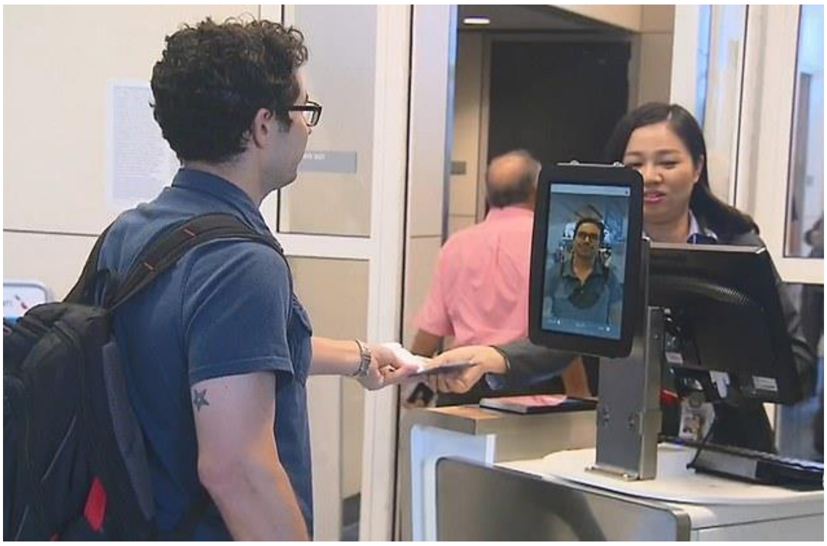


Figure 12. American Airlines using facial recognition to board passengers at Dallas/Forth Worth International Airport in Texas (Insider, 2019).

2.6.2 Disney biometric fingerprint scanner

Disney has used fingerprint biometrics as part of its access system since 2013, making it one of the most well-known examples of a multinational corporation using biometrics as part of its entry structure. All guests aged three and up must check their entry tickets and put their finger on a scanner to confirm identification at Disneyland and Walt Disney World's entry gates. This security mechanism allows visitors to enter and exit Disney's various theme parks at their own comfortable, saving them time and preventing theft if anyone gains access to an individual's park tickets (Ievo, 2019). This security system certainly helps to generate a lot of revenue for Disneyland, which was going a waste; for example, The cost of a one-day entry ticket in early 2013 was $89. During the same era, a ten-day admission ticket cost $318, or $31.80 per day. Bear in mind that if you buy a ten-day ticket, you must use all ten days. Therefore, Disney would lose $57.50 a day, compounded by ten days, or $575 in extra income if they resold each of those days to a different individual (Leibacher, 2013).

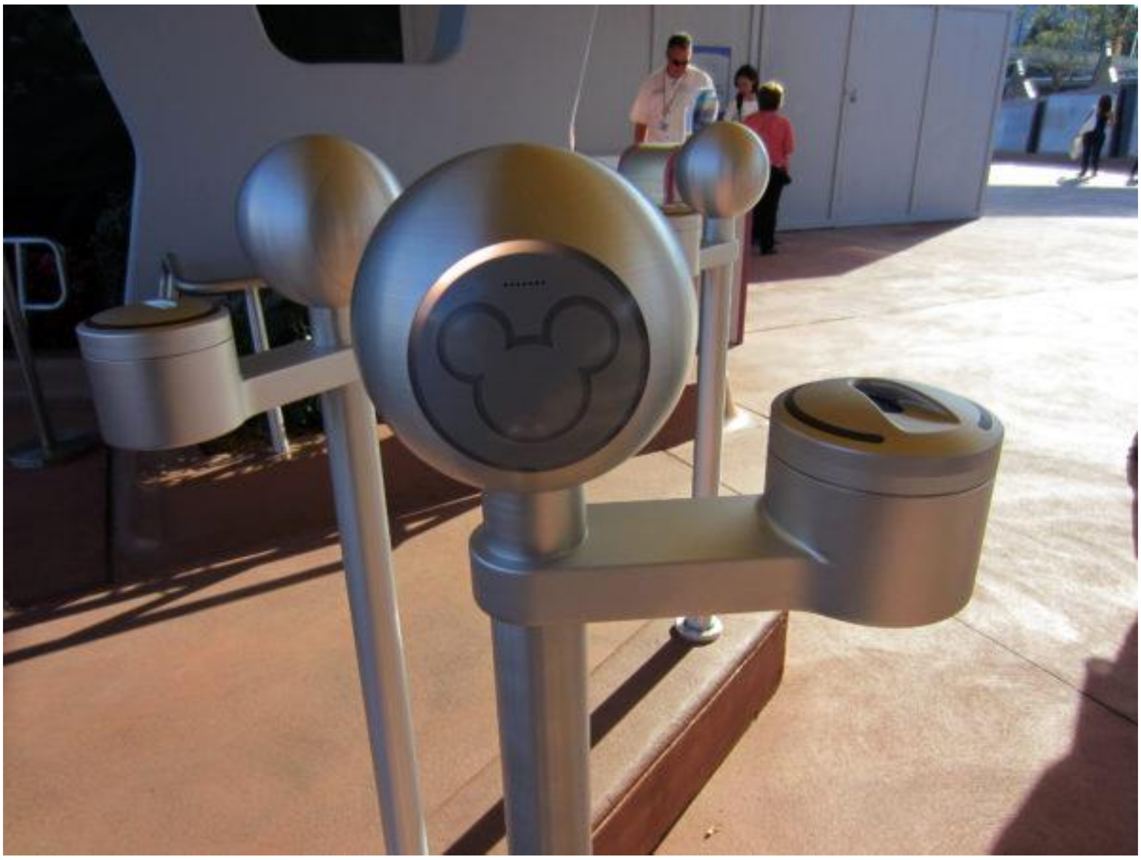


Figure 13. Disney operates one of the world’s largest biometric scanning installations (Leibacher, 2013).

2.6.3 Barclays biometric technology

Barclays was one of the first to introduce one-touch fingerprint banking access, and their biometric strategy has since grown to include voice-enabled biometrics. This biometric technology helps the Barclays bank contact center to recognize customers based on the first few words they say on the phone. In addition, Barclays voice recognition technology analyzes each customer's unique voice to instantly authorize their identity, replacing the need for conventional security codes that are often lost and misplaced by customers. This provides Barclays with a more straightforward authorization method while also offering a more vigorous defense against fraudulent calls (Ievo, 2019).

2.7 Civil Identity, voter registration, and election

Unlike conventional methods of authentication, biometrics do not require a tag or card to prove a person's identity. Friction ridge patterns, facial shape, iris pattern, voice pattern, and even the way a person walks can all be used to recognize them. Biometrics makes use of what a person already has, such as the patterns on their body. It does not depend on external artifacts to prove their identity, such as I.D.s or records that they bring with them. Biometric features such as fingerprints or facial structures, unlike these external artifacts, cannot be lost or stolen. Once registered in the database, it will help identify the person if they tried to change their original record and try to live the next person's life. Many criminals who were yet to be caught by law agencies apply this technique to pretend innocent and live everyday life; biometrics technology cannot be hidden because the fingerprints and eyes pattern could never be changed.

Similarly, biometrics helps find the lost person who cannot communicate or lost their mental status. For example, many homeless people in the streets are either in the stage of an unsound mind or one who could not talk; in this case, the biometrics test can help them find their home if their data were previously stored before they were away from home. Many countries have added biometric data to their citizenship card (see figure 14) (Thakkar, n.d.). It possesses the chip that stored information of a person like fingerprints pattern, iris pattern linked to the government database. This aids in the correct identification of a particular person.

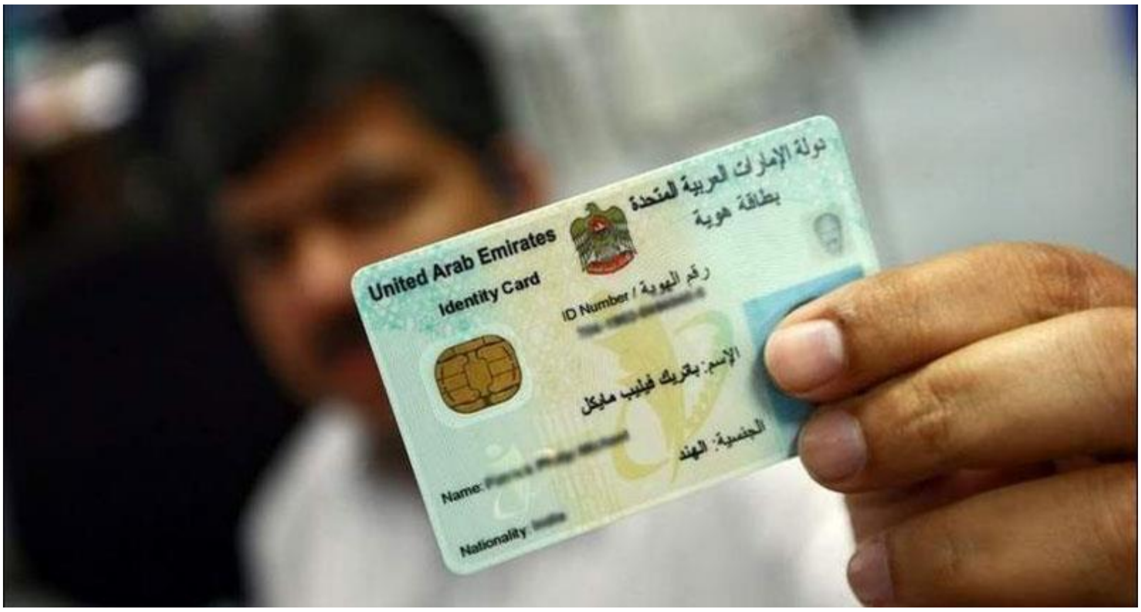


Figure 14. National identity card of UAE resident, which contains all his personal information and biometric data (Thakkar, n.d.).

Earlier, the voter registration system has had many disadvantages due to the multiple registrations by a single person. After the inclusion of biometrics data in the registration process, the record of voters has been perfectly correct. Since a person can only provide one kind of data no matter how many times, they try the risk of multiple registrations has been down to zero. The traditional method of voting system possesses several threats on the conduction of transparent election due to the numerous voting by one person. The use of biometric systems in electoral processes makes it possible to overcome the difficulties of implementing the "one person, one vote" concept, a requirement for conducting fair, accessible, and transparent elections. Biometrics is the most accurate and easy way to identify and authenticate people based on their specific physical features, such as fingerprints. Those prints are linked to reference fingerprints stored on an identification card or in a fingerprint database for voter authentication, allowing the owner to be safely authenticated as the document's holder. Electronic voting saves a lot of time and money by reducing the amount of work needed for voting and counting. An electronic system using biometrics also helps minimize the misuse of the vote, which happens in a traditional voting system. The lack of idea regarding proper folding of the ballot paper, incomplete markings, and double markings are common problems in the conventional method. This is not a case of problem in the electronic system.

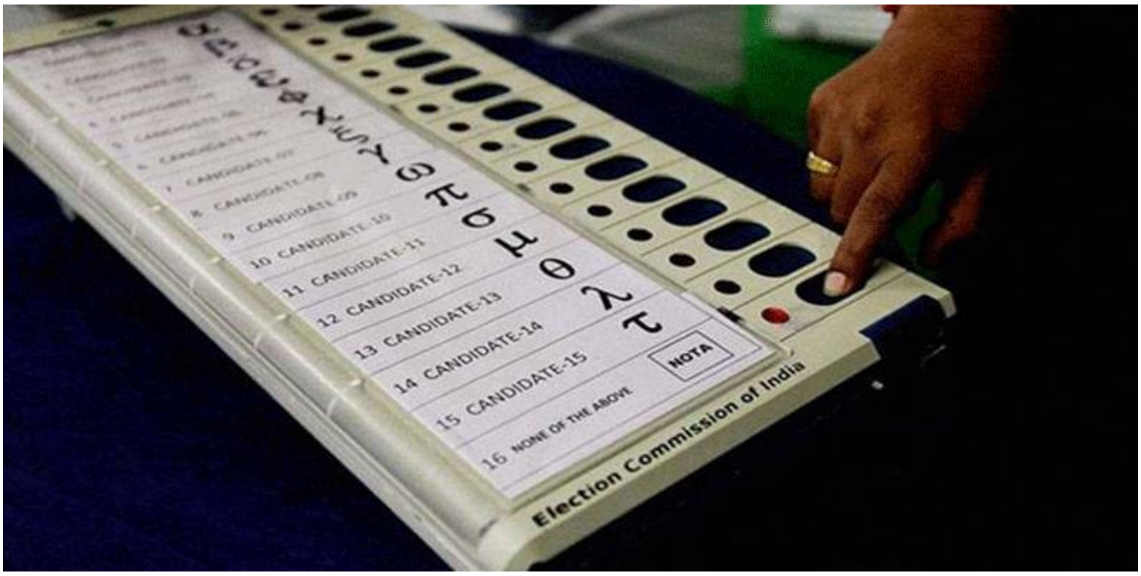


Figure 15. An electronic voting machine in use while in an election in India (Thakkar, n.d.).

3 BIOMETRIC IDENTIFIERS

Biometrics includes data from a human physiological, biological or behavioral characteristic that is unique compared to others. It is used nowadays to identify persons to grant access to data, systems, or devices. Biometrics can significantly improve enterprise security by providing a maximum level of trust in authenticating a person with less friction for the user. When computers and devices detect the fingerprints of a trusted user, they will unlock automatically. When the faces of authorized system administrators are recognized, server room doors will swing open. Biometric identifiers, once recorded it does not require regular updates or anything. Biometric identifiers are classified into two types (see figure 16), which are shown below:

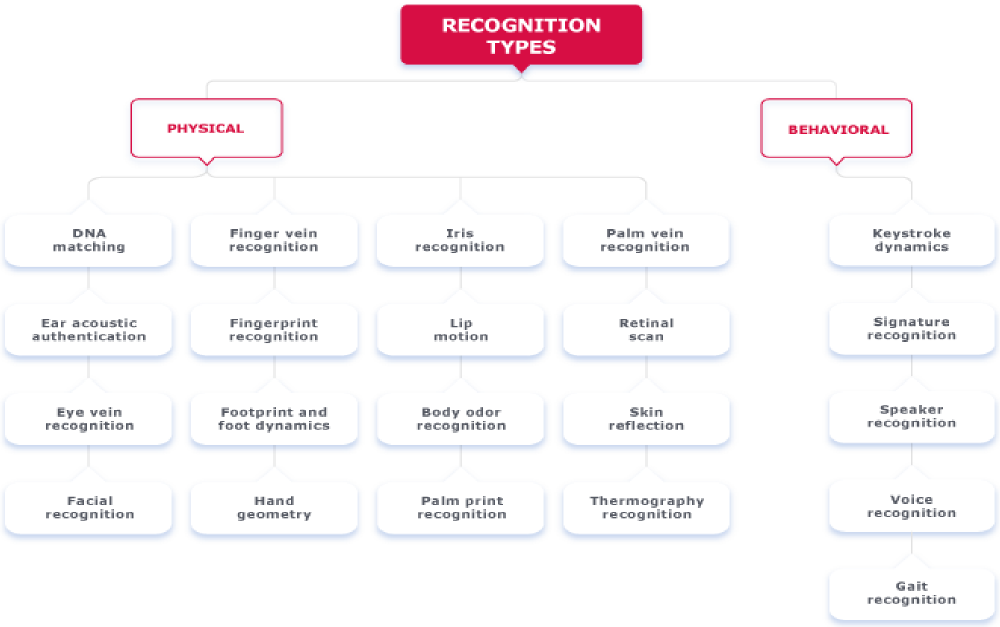


Figure 16. Classification of biometrics Identifiers of humans (Recfaces, 2020).

3.1 Physiological types of Biometric Identifiers

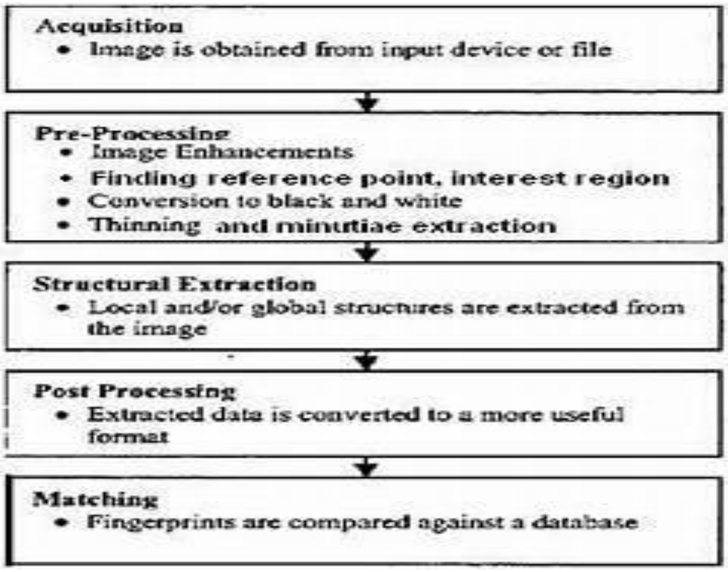
Physiological identifiers are based on the analysis of the invariable physiological characteristics of a person. They are used widely, from smartphones, laptops, airport security to forensics. They are further classified into two types. The most commonly used identifiers are listed and discussed below:

3.1.1 Morphological Identifiers

Morphological identifier relates to the specific measurements, dimensions, and characteristics of the human body. The most commonly used morphological identifiers are Fingerprints, Iris scan, face recognition, hand geometry.

a) Fingerprints

Fingerprints are the most widespread, convenient, and easy-to-use technology. This identifier was among the oldest biometric identifiers in use. Verification and identification are the two categories of fingerprint systems. The verification system verifies a person's identity by comparing the captured biometric characteristic to the system's biometric template. It makes a one-to-one comparison to see if the individual's alleged identity is correct. The submitted claim of identity is either rejected or accepted by a verification system, whereas the identification system recognizes an individual by searching the entire template database for a match. It uses one-to-many comparisons to determine the individual's identity (Bhattacharya & Mali, 2011). The recognition of fingerprints undergoes the following stages (see figure 17).



Acquisition
- Image is obtained from input device or file

Pre-Processing
- Image Enhancements
- Finding reference point, interest region
- Conversion to black and white
- Thinning and minutiae extraction

Structural Extraction
- Local and/or global structures are extracted from the image

Post Processing
- Extracted data is converted to a more useful format

Matching
- Fingerprints are compared against a database

Figure 17. Stages of the fingerprint recognition process (Bhattacharya & Mali, 2011).

The image is changed from greyscale to black and white during the pre-processing stage. Calculating the average background intensity and subtracting it from the greyscale image accomplishes this (see figure 18). Another important stage before minutiae extraction is thinning, where the ridge is thinned to a width of one pixel (Bhattacharya & Mali, 2011). Our fingerprints are defined by the ridge pattern on the tips of our fingers. Fingerprint formation has a genetic component, as evidenced by people with epidermal ridge formation defects, but are strongly influenced by environmental factors (Burger et al., 2011). Fingerprints are made up of ridges and furrows on the surface of the finger and patterns such as swirls, loops, and aches that surround the core, making them unique to each person. The outer layer segments of the finger are called ridges, while the lower layer segments are called furrows. Both are distinguished by irregularities known as minutiae, which serve as the foundation for finger scanning technologies. Minutiae has the form of a ridge ending, bifurcation, and dot (see figure 19). The ridge comes to an end at the ridge ending. Bifurcations occur when a single ridge splits into two, and dots are ridges that are considerably shorter than the fingerprint's average ridge length. During the enrollment process, the minutiae points are identified, along with their relative positions and directions. Next, the image is digested in the matching stage to differentiate its minutiae points, which are then compared to the registered template (Faridah, at al., 2016).

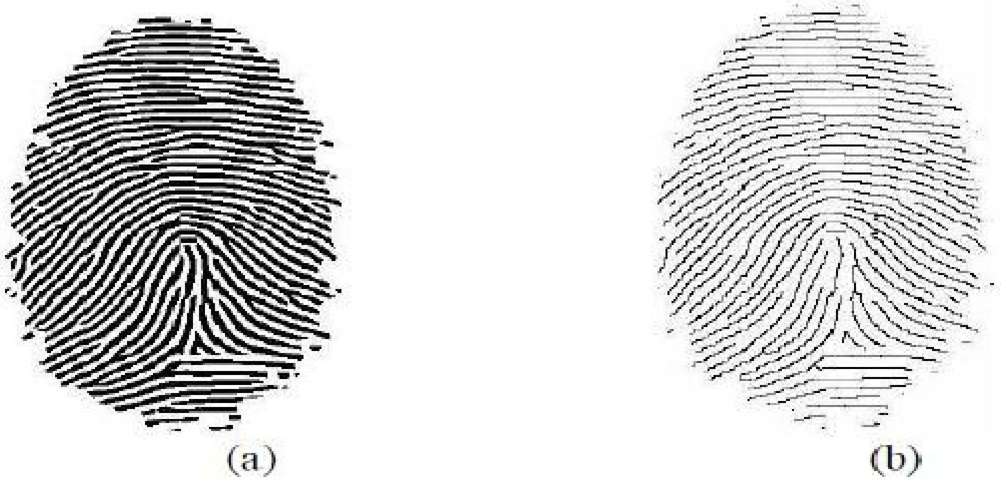


Figure 18. (a) black and white fingerprint (b) fingerprint after thinning (Bhattacharya & Mali, 2011).

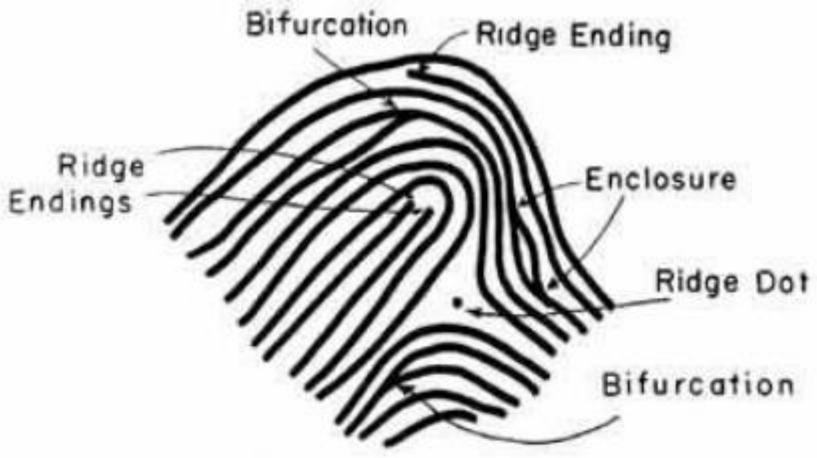


Figure 19. Fingerprint images showing minutiae (Bhattacharya & Mali, 2011).

Pattern detection is another foundation for scanning technology. The arch, loop, and whorl are three simple patterns found in fingerprint ridges (see figure 20). During the matching process, all fingerprint features are compared, rather than just individual points. Sub-areas of interest, such as ridge thickness, curvature, or density, may be included in the characteristics. During the enrolment process, small parts of the fingerprint and their relative distances are differentiated. The areas of interest are the area around the minutia point, areas with a low curvature radius, and areas with an unusual combination of ridges (Faridah, at al., 2016).

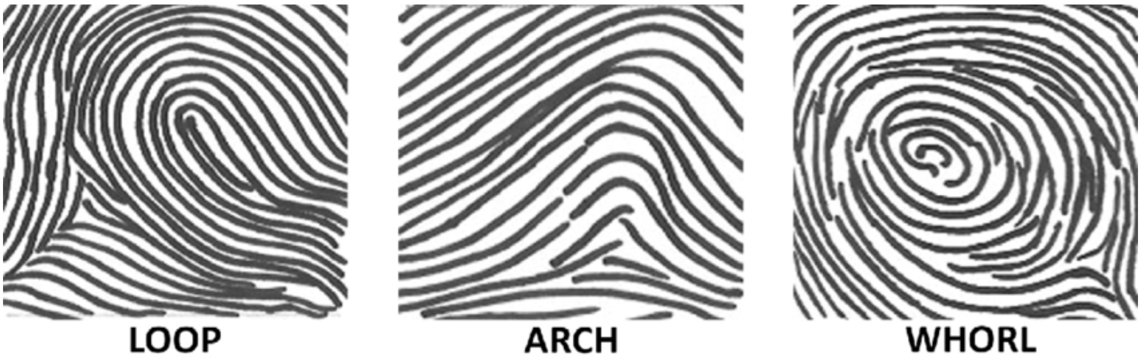


Figure 20. Fingerprint patterns (Walsh, Pośpiech & Branicki, 2016).

b) Iris Scan

Iris is an organ inside the eye of human beings. The structure of the iris remains constant throughout life. As a result, it is an excellent biometric for determining an individual's identity. In addition, Iris recognition has become one of the most reliable verifying methods due to its low margin of error and quick speed. According to Wikipedia,(n.d.), “Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex patterns are unique and stable.”

Figure 21. Iris-based authentication in ATM (Thakkar, n.d.).

Iris scanning is a method for determining the distinctive patterns in people's irises or colored circles in their eyes. Iris recognition scanners work by lighting the iris with infrared light that is invisible to the naked eye. Iris recognition technology works on two distinct stages, they are discussed below:

- Enrolment

At the first stage, the Iris image is captured of a person whose identity needs to be verified. Then, a clear image with a proper focus on the iris is taken into consideration. The iris borders are recognized by the iris recognition system, which is then followed by the center of the pupil, which is also the center of the circular iris. Afterward, it examines the iris image region that is suitable for feature extraction and analysis. Finally, the iris recognition system analyses the photos and creates a profile of a person. It removes extraneous features such as eyelashes and identifies about 240 features that distinguish each person's iris, which is five times the number of features than in a fingerprint recognition system (Mehedi, 2018). The system then converts these features into a 512-digit code number. This information, along with a person's name, address, and other information, will now be stored in the database.

- Verification

After the successful enrolment of a person’s data, if the iris scan is performed at any time for authentication, the computer system would then compare the information to its database. If the code matches the database, the person would be successfully identified and is allowed to proceed.

A complete block diagram of the Iris Recognition System is shown below:

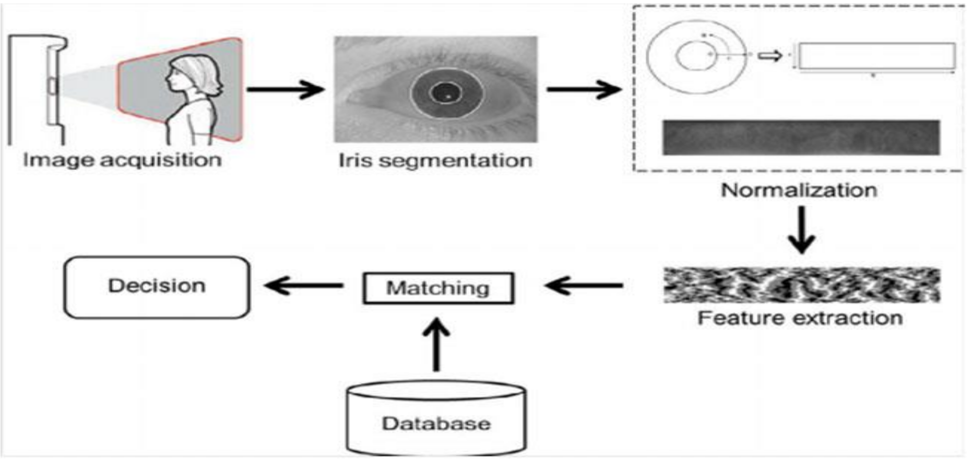


Figure 22. A block diagram of an Iris recognition system (Thakkar, n.d.).

c) Face Recognition

Facial recognition is a technology-based method of identifying a human face. A facial recognition system uses biometrics to map facial features from an image or video. To find a match, it compares the details to a database of recognized faces. A person's face has a variety of distinguishable features. There are 80 nodal points on the face; some of the examples used in comparison by the face recognition system are the width of the nose, depth of the eye sockets, contours of the cheekbones, measurement of the length of the jawline, etc. By measuring these nodal points, a specific numeric code is gathered, which serves as a recognition measure while comparing an individual's face. A diagram showing the face recognition process is given (see figure 23) below:

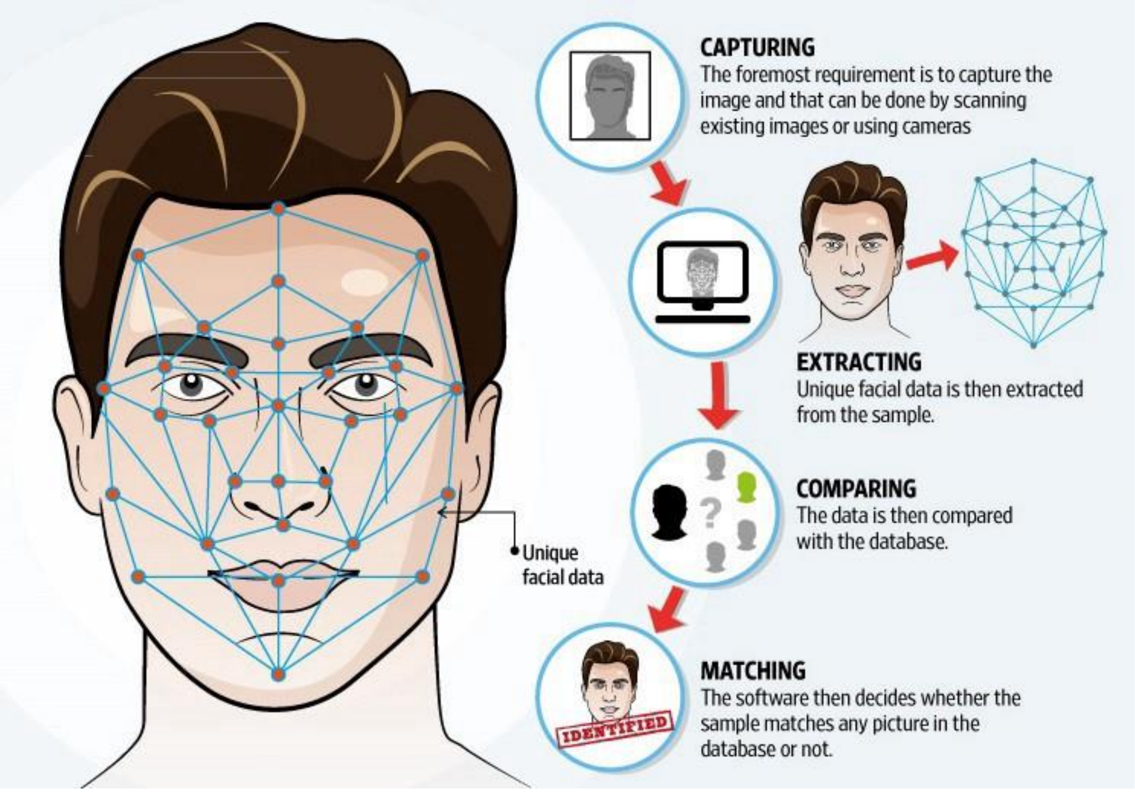

Unique facial data
CAPTURING
The foremost requirement is to capture the image and that can be done by scanning existing images or using cameras
EXTRACTING
Unique facial data is then extracted from the sample.
COMPARING
The data is then compared with the database.
MATCHING
The software then decides whether the sample matches any picture in the database or not.
IDENTIFIED

Figure 23. A diagram showing face recognition data sources and stages (Villaverde, 2018).

The face recognition process outgoes the following steps:

- Face detection: At first, the system detects the part of an image or video representing the face. This task for the system will be much easier when the face has a white background rather than other colors.

- Normalization: The data are then converted into a normalized, monolithic format which means all images must have the exact resolution, zoom levels, brightness, and orientation.

- Feature extraction by system: The device then derives useful information from facial images, recognizing the most important data points. The distance between two eyes and the distance from the forehead to the chin are important considerations. The program recognizes facial landmarks (one device recognizes 68 of them) that are important in the identification of the face. A facial signature is created as a result of this stage.

- Face recognition: The obtained facial signature is then compared to the known database already stored in a database. If authentication is performed, the image will be matched to one image in the database. In contrast, if the image is being used for identification, it will be compared to all other images in the database.

d) Hand Geometry

Hand geometry recognition biometrics is based on the notion that each person's hand geometry is unique. A hand geometry reader is a device that captures and processes human hand geometry to create a digital biometric template that can determine the identity and later validate it. Since hand geometry recognition is based on the idea that the shape of a human hand is unique, recognition systems are built to measure the hand's shape, including surface area, thickness, length, and width of an individual's hand, finger width, height, and length, joint distances, and knuckle shapes. The measurement is precise, and a biometric template created out of it also represents it uniquely. The typical image of a hand geometry scanner (see figure 24) is shown below:

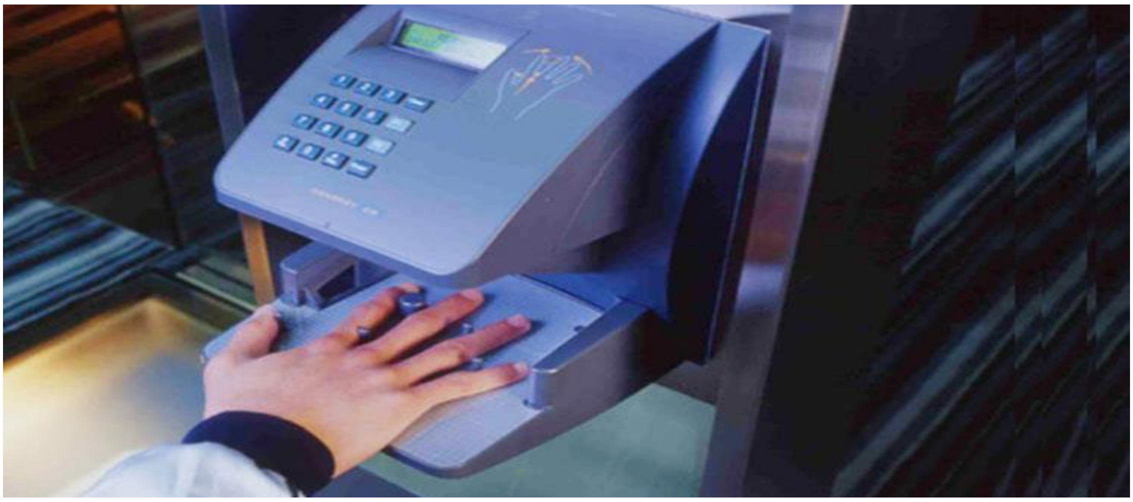


Figure 24. An individual with hand placed on hand geometry reader scanning platen (Thakkar, n.d.).

Employee attendance and physical access applications often use hand geometry readers. To remove any unnecessary details, the recognition system creates a silhouette image from the captured raw image. To perform geometry measurement, both the top and side images of the hand are created. At least 90 measurements are taken, and the produced silhouette image is analysed at

31,000 points. The underlying hand, geometry recognition algorithm, performs these calculations and measurements, and the subject's biometric template is created. The memory size of the template created by hand geometry recognition systems is very small, only 9 bytes, compared to other biometric recognition systems. As a result, hand geometry recognition systems require very little storage space (Thakkar, n.d.).

3.1.2 Biological Identifiers

A biological identifier is widely used in the forensics department. Biological biometrics use traits at a genetic and molecular level. The most commonly used biological identifiers are DNA tests.

a) DNA test

DNA or Deoxyribonucleic acid is the part of a cell that contains genetic information unique for each person. The human body is made up of about 60 trillion cells. DNA, which can be thought of as the blueprint for the human body's design, is folded within each cell's nucleus. DNA is a polymer made up of nucleotide units, which are made up of three parts: a base, sugar, and phosphate. Adenine, guanine, cytosine, and thymine, abbreviated A, G, C, and T respectively which are the bases. These four letters reflect the informative content of each nucleotide unit, and the differences in nucleotide sequence led to biological diversity, not just in humans but in all living things. The human body comprises 23 pairs of chromosomes that include one set of chromosomes coming each from parents to offspring. 99.7% of human DNA is shared, and the remaining 0.3% is different from each other. This tiny part is the basis for DNA identification in biometrics. These variable regions are also called Short Tandem Repeats or “STR.” Inside the STR, it has been discovered around 13 areas that are highly variable and are used in DNA profiling. At every 13 regions, there are repeated sequences of bases, for example, ATTC repeated at one locus and TTAC at another locus. These whole sequences could never be identical between individuals, which is used as a medium for a DNA test (Painting valley, n.d.).

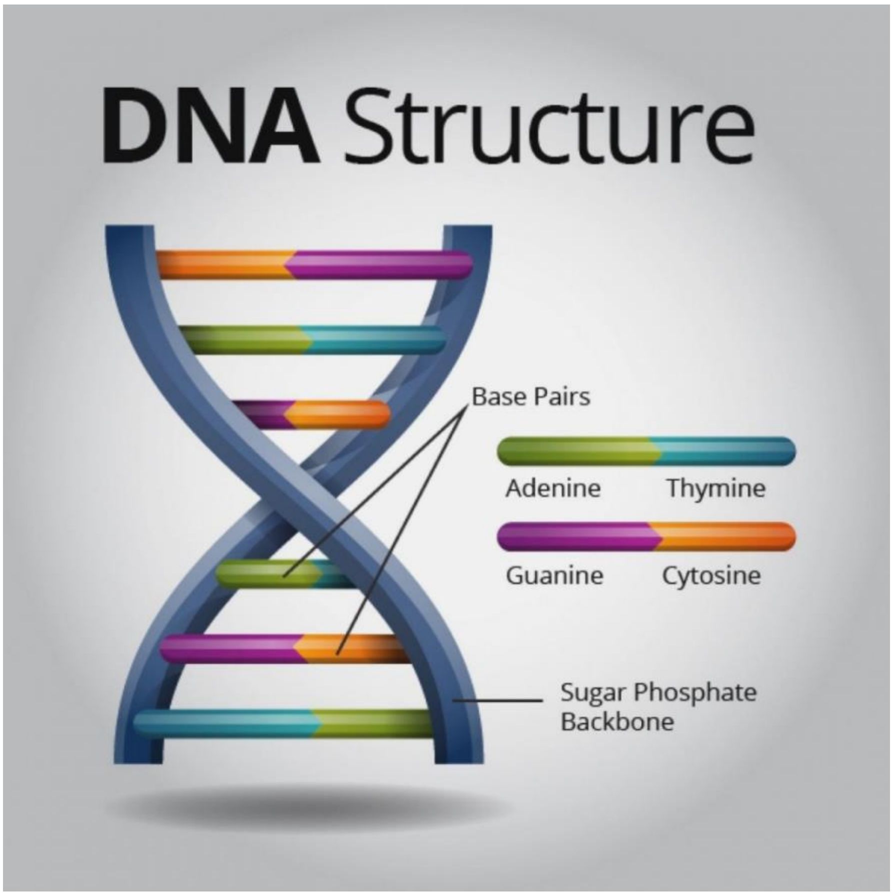


Figure 25. A well labeled DNA structure (Painting valley, n.d.).

To obtain unique data of DNA, it undergoes three stages. At first, the DNA is extracted from samples done either by using chemicals such as phenol, chloroform, alkaline, or drying, boiling the model. Afterward, it undergoes an amplification process to increase the number of copies of DNA. The common method for DNA amplification is Polymerase Chain Reaction (PCR). Finally, the DNA samples are then loaded into a genetic analyzer with fluorescently labeled A, T, C, and G attached to the DNA where the data are analyzed. A DNA profile is created, which is used for verification.

3.2 Behavioral types of Biometric Identifiers

Behavioral biometrics is a new technology that authenticates users based on their behavior patterns. Rather than recognizing parts of people's bodies, it recognizes certain individual regularities in the way they type and move. The Behavioural types of identifiers commonly in use for authentication purposes are:

(a) Keystroke Recognition
(b) Gait Recognition
(c) Voice Recognition

3.2.1 Keystroke recognition

The use of computers prevails inside every household. It is used nowadays not only for work purposes but also for communication, entertainment purposes. Due to this, using a keyboard, which is an integral part of the computer, is frequent. Keystroke recognition relies upon the way we type while performing any task on a computer. There is a distinct pattern to everything a person types on their office or home computers. The individuality often shows itself in the amount of time they type and the ways in which they press the keys on the computer keyboard (Das, 2016). The raw measurements used for keystroke recognition are:

- The cumulative typing speed of an individual.
- The time duration while holding each key is also known as Dwell time.
- The time duration it takes while moving from one key to another, also known as Flight time.
- The order in which the keys are pressed to type a capital letter (for example, whether the shift or letter key is released first) (Das, 2016).

The major distinctive characteristics used for keystroke recognition are Dwell time and Flight time (see figure 26). For the enrolment process to underway, the individuals are required to type some words or phrases. While in most cases, the individual’s username or password is used because it is the most repetitive and daily used word while doing any task on the computer. In some cases, a specific sentence was given to type. The profile is created by taking data from those measurements and is used for authentication.

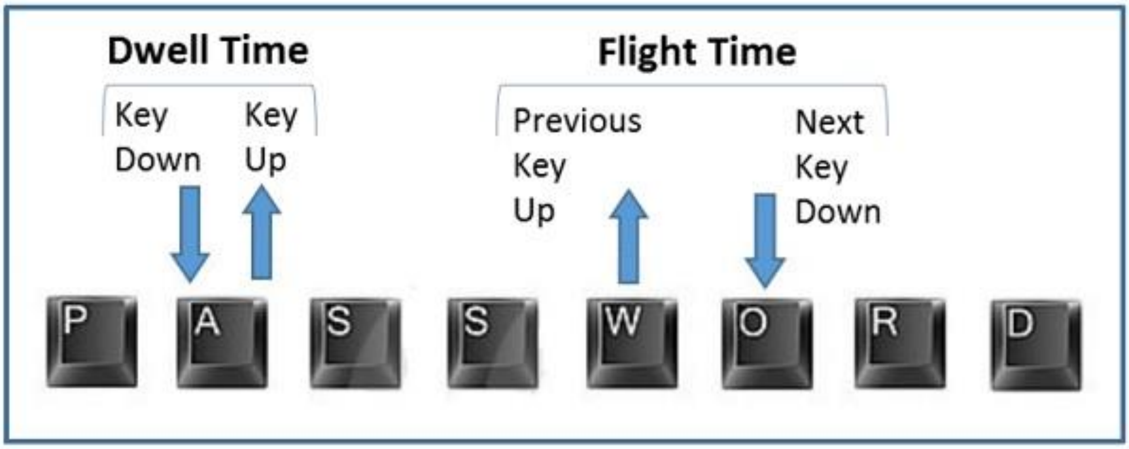


Figure 26. Illustration of Dwell time and Flight time used in keystroke recognition (Wisdomjobs, n.d.).

3.2.2 Gait recognition

Gait recognition is a type of biometric identifier in which the authentication process is carried out by the manner of a person walk. The theory behind this recognition system is that every person has a unique gait. People walk in different ways, including body posture, keeping a comfortable distance between two feet, swaying, and so on, all of which help differentiate them from others. It is one of the few tools for recognizing people from afar. Some of the parameters taken into account when developing the framework for human gait analysis include step length, stride length, speed, cadence, progression line, dynamic base, hip angel, foot angle, and squat performance.

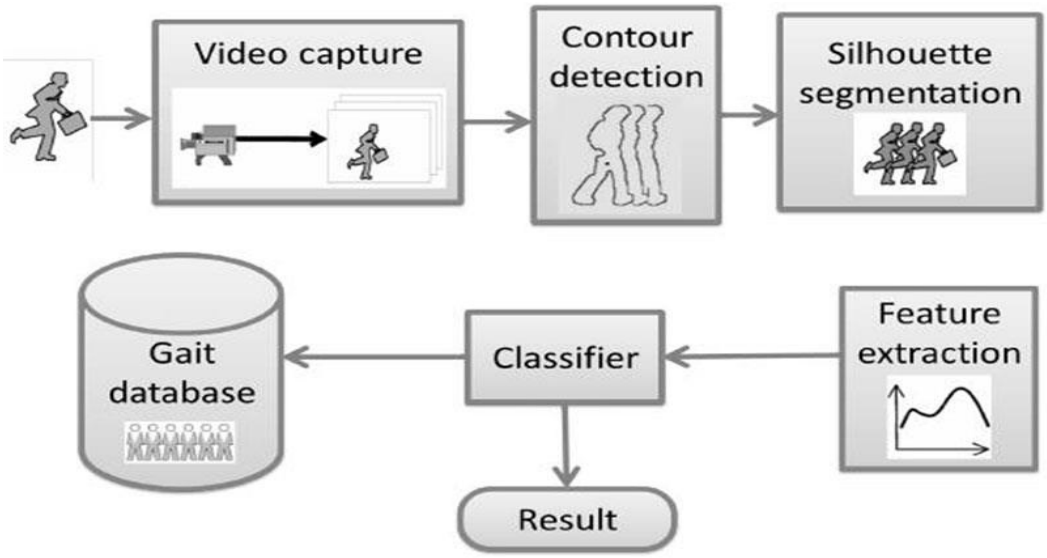


Figure 27. Stages of Gait recognition system (Thakkar, n.d.).

The gait recognition system undergoes the following stages:

a) Data Capture: The first step includes capturing the gait data of individuals. In this process, if the data is to be taken from the remote identification, then the video camera is used to capture the video of individual motion. Similarly, if the data is to be taken of particular who is about to authenticate their identity, then it can be performed either in-floor sensor or using wearable censors indirect contacts.

b) Contour detection: In this stage, the contour of the person is detected to remove the outer background for more precise data extraction.

c) Silhouette segmentation: In this stage, a silhouette image of the individual is derived from the recorded video. Silhouette is a binary image (see figure 28) obtained after contour detection. Thus, obtained silhouettes are then segmented into a part in this stage.

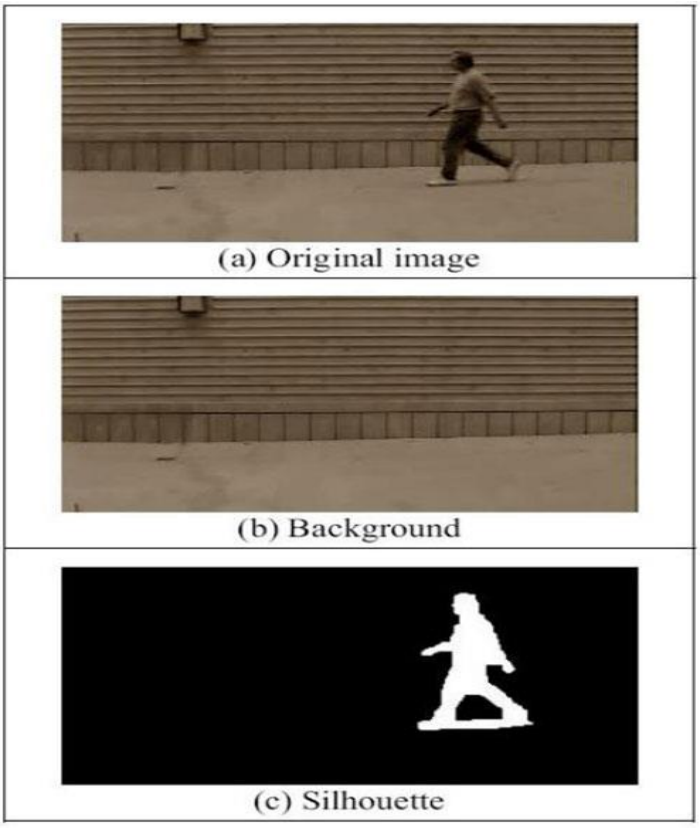


Figure 28. Silhouette image Extraction (Thakkar, n.d.).

d) Feature extraction and classification: The last stage involves the extraction of gait features of an individual. The classifier is used to identify the person; inside this, the person's data is compared to the already stored database and helps to reveal the identity.

3.2.3 Voice recognition

Voice Biometrics is a speech technology that uses a distinct voice as an input to recognize false inputs and detect fraud. It relies on the principle that each individual has their unique way of speaking. Through biometric technology, an individual speech is reduced into segments that consist of various dominant frequencies known as formants. Every segment possesses several tones which can be recorded digitally. The techniques work together to recognize the speaker's distinct voice pattern. The voice recognition system undergoes the following stages (see figure 29).

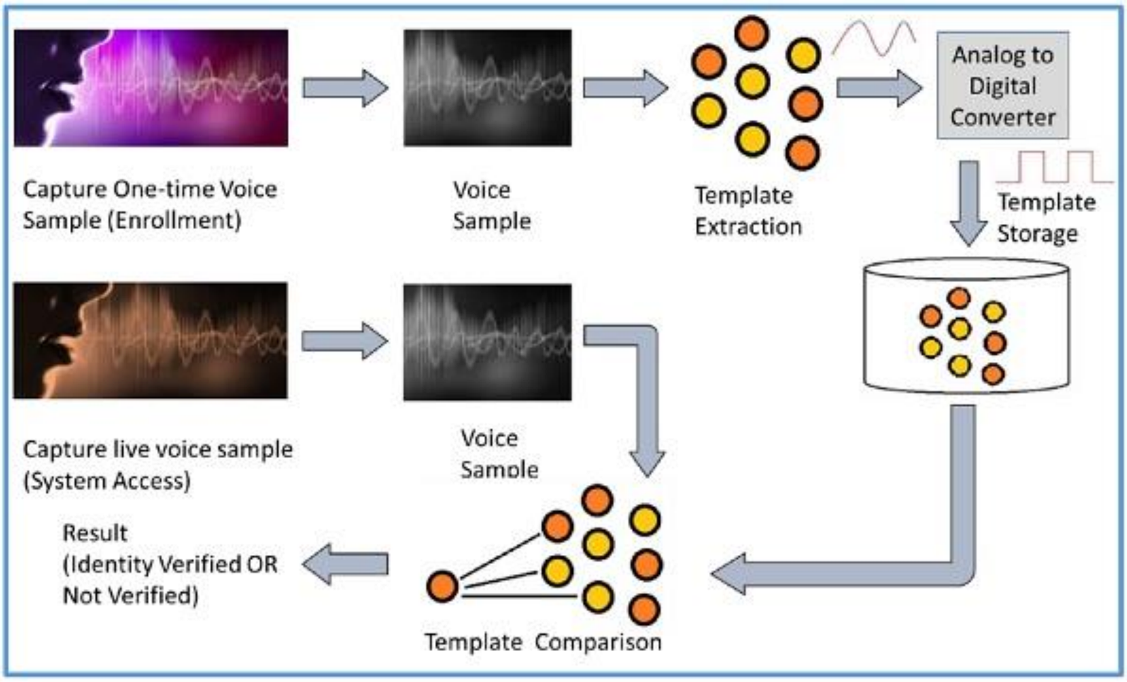

Capture One-time Voice Sample (Enrollment)
Voice Sample
Template Extraction
Analog to Digital Converter
Template Storage
Capture live voice sample (System Access)
Voice Sample
Result (Identity Verified OR Not Verified)
Template Comparison

Figure 29. Flow chart of a voice recognition system (Tutorialspoint, n.d.).

4 BIOMETRICS SYSTEM AND THEIR TYPES

With the advancement of biometrics technology, the existing biometrics system can be categorized into two types; they are Unimodal biometric system and Multimodal biometric system. The brief information of these two prevailing systems is discussed below:

4.1 Unimodal biometric system

It is a type of biometric identification system which uses a single biometric trait of an individual for the process of identification or verification. (For example, Fingerprints, Face recognition, hand geometry, etc.). A simple block diagram of a unimodal biometric system using hand geometry is shown (see figure 30) below:

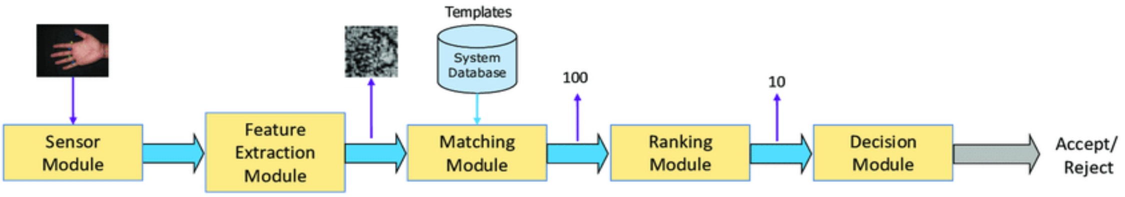


Figure 30. A unimodal biometric system using hand geometry (Kabir, Ahmad, & Swamy, 2019).

The Unimodal biometric system possesses several limitations, and these drawbacks lead to the use of a multimodal biometrics system. Several limitations of unimodal and how they are solved by multimodal biometrics system are discussed below:

4.1.1 Limitations

a) Noisy Data: Owing to poor acquisition conditions, the captured biometric trait can be skewed. This limitation can be seen in facial recognition applications where lighting conditions and facial expressions can affect the accuracy of the captured facial images.

b) Non Universality: A biometric system is said to be universal if all users can reveal their traits. However, due to physical disabilities due to accidents, burns, or by birth, some individuals are unable to reveal their traits for authentication purposes. This is why it is not considered a universal system.

c) Lack of individuality: In some cases like twins there may arise the problem of face recognition because both twins may have exact face and will be very hard to recognize.

d) Risk of Imitation: In unimodal system there could be the greater risk of imitation of traits by unknowns. Fingerprints can be duplicated using technology and can be used in accessing the person's privacy.

4.2 Multimodal biometric system

A multimodal biometric system refers to the technology that involves more than two individual traits for the purpose of identification and authentication. A multimodal biometric system, unlike a unimodal biometric system, which can result in non-universality, employs multiple biometric modalities to produce a highly accurate and reliable biometric identification system. A typical example of a process involving a multimodal biometrics system using face geometry and iris is shown (see figure 31) below.

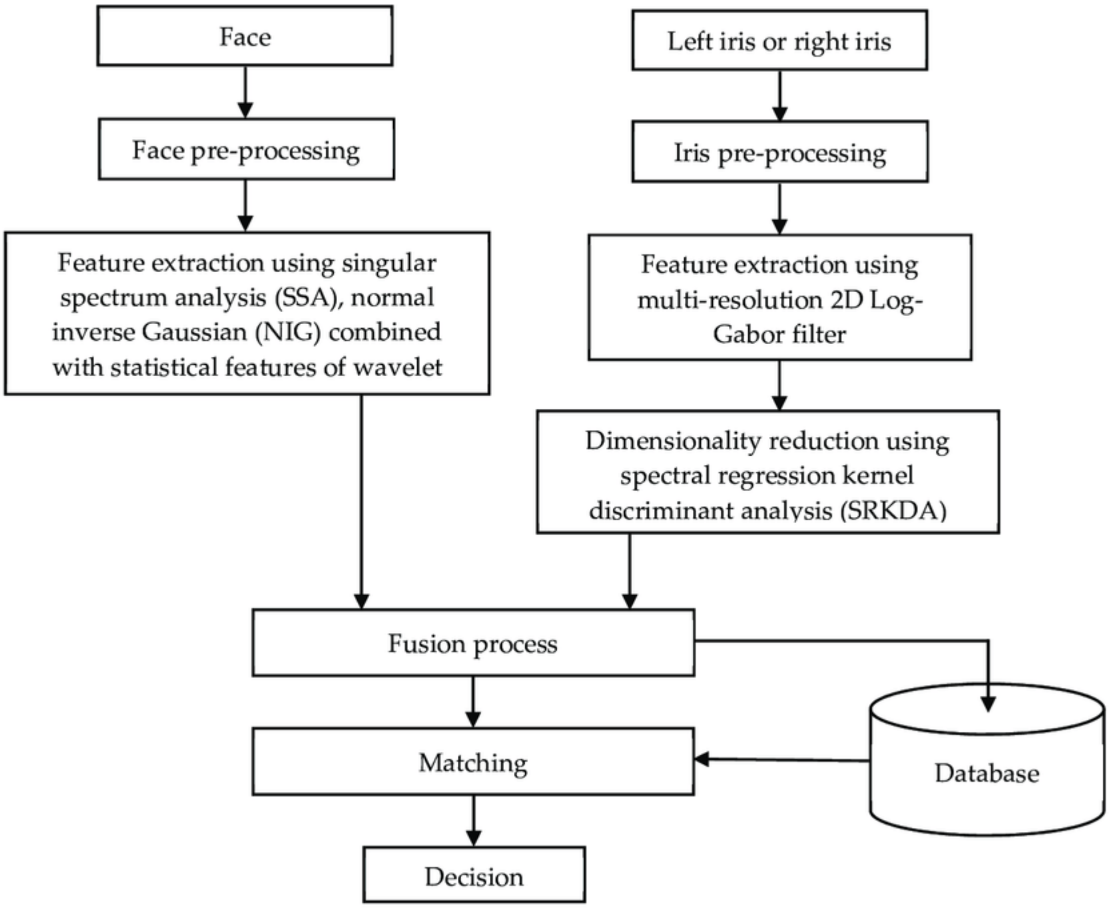

Face
Face pre-processing
Feature extraction using singular spectrum analysis (SSA), normal inverse Gaussian (NIG) combined with statistical features of wavelet
Left iris or right iris
Iris pre-processing
Feature extraction using multi-resolution 2D Log-Gabor filter
Dimensionality reduction using spectral regression kernel discriminant analysis (SRKDA)
Fusion process
Matching
Database
Decision

Figure 31. Block diagram of the multimodal biometric system (Ammour at al., 2020)

4.2.1 Fusion level in multimodal biometrics system

The goal of biometric fusion is to develop a procedure that incorporates classification results from each biometric channel. Biometric fusion is commonly used in the industry to minimize the disadvantages of individual measurements and to improve the strengths by integrating various biometric attributes. Multimodal biometrics can be implemented using degrees of fusion in a biometrics framework. Robustness, applicability, precision, performance, and universality are some of the issues. Various degrees of fusion is used for fusing the biometrics traits to improve the robustness of the multimodal biometrics. Four types of fusions are available they are as follows: sensor level, feature level, matching score level, and decision level (Krishnakumari and Savitha, 2017).

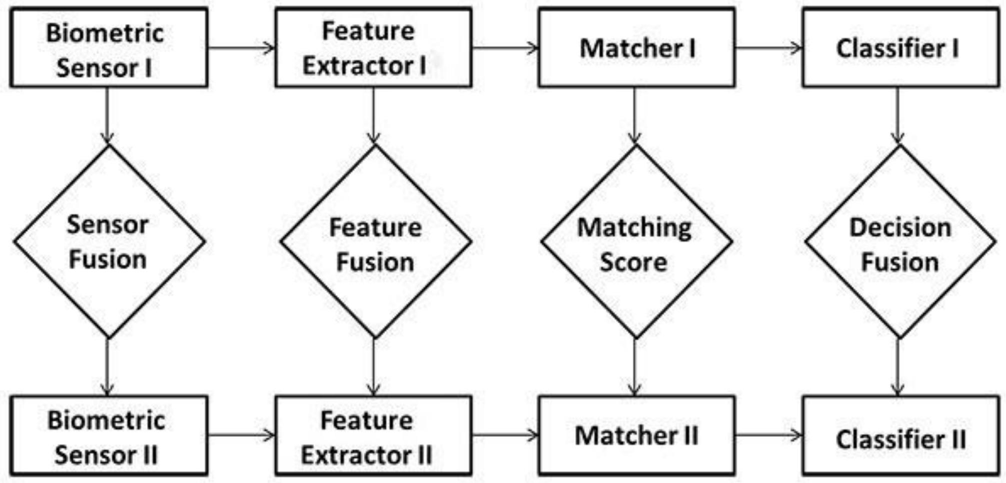


Figure 32. Multimodal biometrics fusion levels (Krishnakumari and Savitha, 2017).

a) Fusion using sensory level: Various sensors are used to construct a merged biometric trait. For instance, fingerprint scanners, iris scanners, and video cameras. Biometric data is combined at the sensor level, and new biometric data is generated as a result.

b) Fusion using feature level: Signals originating from various biometric traits at the feature level are processed first. Later, feature vectors are derived separately from each biometric trait. In feature level fusion, signals from various biometric channels are first analyzed, and then feature vectors from each biometric trait are recovered independently. At the feature level, reduction strategies are used to pick valuable features. Feature level fusion yields better recognition results than matching score fusion because feature level fusion contains more biometric information. Furthermore, when the characteristics of different biometric traits are compatible, feature level accuracy improves.

c) Fusion using matching score level: In this fusion level, The input and enrolled models are integrated to achive the final decision and hence the match scores from different matches demonstrate the degree of similarity. To integrate match scores, a variety of techniques are utilized, including mean fusion, highest rank, and logistic regression. The important advantage of this fusion is that it allows for the normalization of scores using different traits. Some of the methods used to accomplish this normalization of match scores include z-score, piecewise linear, min-max, etc. Compared to other fusions, the matching score level produces less difficulty, and as a result, this level of fusion is commonly used.

d) Fusion using Decision level: In the decision level, each biometric trait is first pre-classified separately. Individual biometric traits are captured first in biometrics, and features are extracted from the captured trait. Based on extracted characteristics, traits are listed as either accepts or rejects. The final classification of biometrics is accomplished by integrating the outputs of various traits.

4.2.2 Advantages of multimodal biometrics system

a) Increased accuracy: The errors in image acquisition and matching of biometric traits are used to determine the accuracy of a multimodal biometric system. The fact that multimodal biometrics uses data from at least two biometric sources is the first benefit it has over the unimodal system. Failure-to-acquire (FTA) and failure-to-enroll (FTE) rates are two types of image acquisition errors. False non-match rates (FNMR) occur when a valid subject is denied, while false match rates (FMR) occur when an attacker is given entry. FTA, FTE, FNMR, and FMR rates are almost non-existent in multimodal systems. [48]. Thus, it overcomes the limitations of the unimodal system.

b) Rectify Noisy data: During the matching procedure, the data acquired during authentication may be differ from the data input during enrollment due to a misplaced finger. Hence, Multiple biometric data for verification can be used to correct the noisy data and intra-class differences with multimodal biometric systems.

c) Universality: Due to physical limitations, some individuals are unable to have a standalone biometric credential. A multimodal biometric device, on the other hand, may use any kind of biometric credential to authenticate.

d) Spoof attacks: Comparing to multimodal systems, Unimodal systems can be more vulnerable to spoof attacks where attackers can impersonate a user’s biometric trait in order to obtain access to sensitive information. Integrated Iris sensors and fingerprint scanners including liveness detection can be used to prevent spoofing.

5 BIOMETRIC TEMPLATE SECURITY

This study aims to classify the various factors that leads to biometric system failure and determine the consequences of such failures. This thesis does not claim to be comprehensive in terms of all security threats listed, but it does include a high-level classification of potential security threats.

A secured identity management system is urgently required to combat the epidemic of identity theft and to fulfill the rising security standards in a range of applications ranging from international border crossings to database security. In every identity management system, establishing a person's identity is a vital activity. Surrogate identities, such as passwords and I.D. cards, are insufficient for determining identity since they are easily lost, shared, or stolen. The science of determining a person's identity based on anatomical and behavioral characteristics is known as biometric recognition. Fingerprints, faces, iris, hand geometry, expression, palmprints, hand-written signatures, and gait are common biometric traits. In terms of their use, biometric traits have a different kind of properties, such as reliability, convenience, universality, and so on. Biometric authentication systems have become very popular as a result of these characteristics. More or less there are still some issues that needs to be solved to insure the public recognization and their integrity in biometric security.

A general biometric authentication system has five significant components: a sensor, a feature extractor, a template database, a matcher, and a decision module, as shown in figure 33.

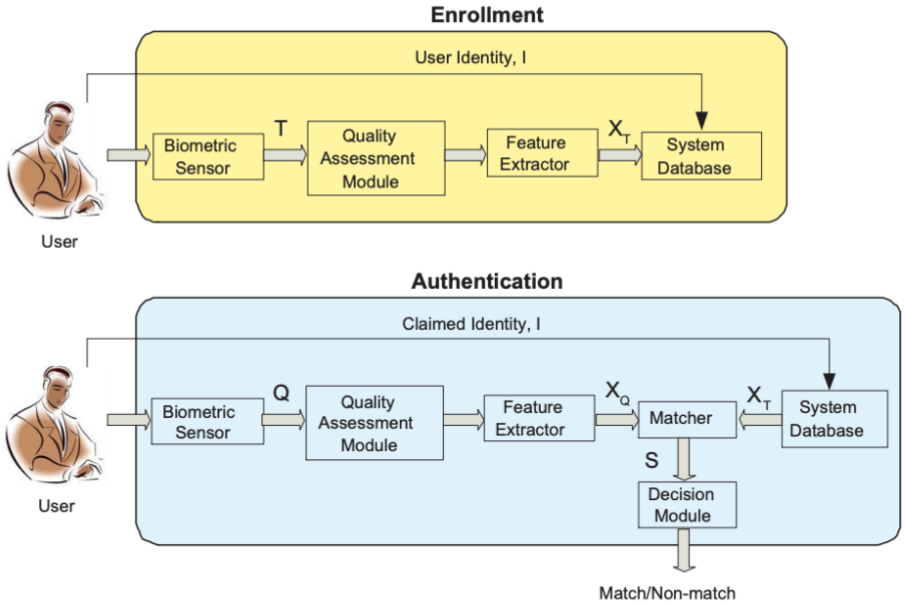


Figure 33. Enrollment and recognition stages in a biometric system (Jain at al., 2008).

In the given figure, *T* stands for the biometric enrollment sample, *Q* for the biometric query sample collected during recognition, *X*.T. and X.Q. for the prototype and query feature sets, and *S* for the match score.

The sensor serves as an interface between the user and the authentication device, scanning the user's biometric trait. The feature extraction program examines scanned biometric data to extract the most critical information (feature set) for differentiating users.. In a database as a prototype (X.T.) indexed by the user's identity information during enrollment, an extracted feature set is saved. It's not easy to keep the template database secure, especially when it's geographically spread and contains millions of records (as in a national identity system). The matcher module is a program that accepts two biometric feature sets, X.T. and X.Q. (from template and query, respectively), as inputs and returns a match score (S) that indicates how close these two sets are. And hence, the decision module determines the identity of the query and starts a response to it. Due to the rapid rise of sensing and computer technology lately, biometric system is reliable and easy to integrate into a different consumer devices such as mobile phones, key fobs and so on, making them resistant to terrorists and criminals malevolent designs. (Jain at al., 2008).

5.1 Biometric system vulnerability

The use of biometric technologies has been accepted widely by many organizations worldwide due to its high-performing capability and reliability. This system has saved a lot of time, effort, and cost of an organization that used to be lost while securing their valuable goods. Like other technologies, this one is also not a hundred percent perfect as it possesses some vulnerabilities. This system also faces several types of attacks during the process of authentication. These several attacks harness the purpose of the system established in an organization, which eventually leads to the failure of a technology.

5.2 Attacks against biometric system

The attacks against biometrics system or device can be mainly categorized into four parts, which are described below.

5.2.1 Input level attacks

Spoofing and bypassing are the most common input-level attacks or vulnerabilities at the point of sample acquisition and initial processing. However, spoofing is the most commonly mentioned input-level vulnerability; other input-level vulnerabilities, such as "overloading," may be just as dangerous. An effort to defeat or circumvent a system by destroying or overwhelming the input device to produce errors is known as "overloading"(Alaswad at al., 2014). For other protection frameworks, this is known as a buffer overflow attack. This type of assault against a biometric system includes fast flashing of bright lights against optical fingerprint sensors or face recognition capture systems is an example of this form of attacks on biometric systems. Short-circuiting or submerging silicon sensors in water can quickly destroy them.

5.2.2 Processing and transmission level attacks

Though attacks on the input level are the most obvious example of biometric system vulnerability, attacks on the processing and transmission levels are also worth paying attention. Since many biometric devices send sample data to local or distant workstations for processing, this information must be sent securely to avoid being intercepted, read, or altered. While the majority of biometric solutions encrypt data in transit, not all apps and devices can. Anti-spoofing steps, data protection in transmission, and the use of acceptable fallback strategies are all essential aspects of biometric device security when taken together. Multi-factor authentication and randomization can be added to these methods to improve them even more.

5.2.3 Back-end attacks

Attacks on the input and transmission levels were discussed in the previous two parts. Attacks on the back end will largely seek to modify the matching or decision subsystem or damage the integrity of stored templates, assuming the back end consists of a matching subsystem, a decision subsystem, or a mix of the two. The template storage database is the most visible kind of back-end attack. Depending on the attacker's motivations, the threat of unauthorized alteration or replacement of stored templates may result in false accepts or rejects (Alaswad at al., 2014). The most apparent form of back-end attack is on the template storage database. Depending on the attacker's motivations, the threat of unauthorized alteration or replacement of stored templates may result in false accepts or rejects. If an intruder can insert models directly into the storage database, he or she may gain access to the system without having to go through the proper enrollment procedures. By replacing the original prototype with their own, the intruder may steal the identity of an approved person. Encryption and data integrity (hashing) methodologies may be used to avoid these types of attacks. Using standard database protection methodologies can also make an attacker's job more difficult.

5.2.4 Enrollment attacks

The practical application of biometrics for E-Authentication is identity binding. The identity proofing method plays a crucial related role in biometric enrollment because of the necessary binding requirement. The underpinnings of biometric-based E-Authentication are trust in the process of vetting a person's claimed identity, faith in the validity of associated documents, and trust in the authenticity of provided electronic credentials (Alaswad at al., 2014).

Examples of threats to identity proofing include:

1. Fake documents are used to verify a claimant's identity.
2. Collaboration with dishonest employees who have access to the system.
3. Electronic impersonation attacks to obtain electronic access to the I.D. program, proofing procedure, and issuance system by impersonating legitimate system users (Alaswad at al., 2014).

These Identity Proofing risks can be countered by using the following countermeasures :

1. The roles and responsibilities of those involved in the processing, acceptance, and credential issuance processes are clearly defined.
2. Thorough examination of records for forgery or tampering, as well as the use of third-party substantiation, such as written inquiries.
3. Safety of electronic systems – strict access controls, data encryption, firewalls, and so on.

5.3 Vulnerable points of biometric systems

A pattern recognition system can be used to cast a generic biometric system. A pattern recognition system can be used to launch a general biometric system. Figure 35 illustrates the stages of such a generic system. This framework can also accommodate password-based authentication schemes. The keyboard is used as an input device. The feature extractor replaces the password encryptor, and the comparator replaces the matcher. The encrypted password database is the same as the template database.

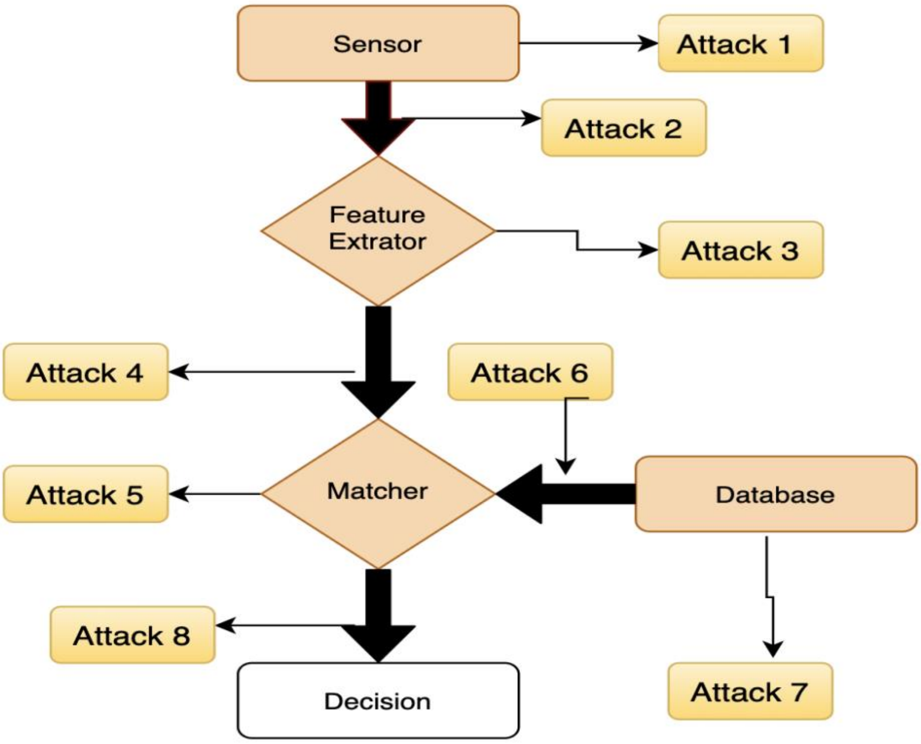


Figure 34. Possible attack points in a generic biometrics-based system (Prasad, 2013).

According to Prasad (2013), There are in total eight possible sources of attack on generic biometric systems as shown in figure 35, which is described below in brief:

1. Fake biometric at the sensor: A fictitious biometric trait, such as a dummy finger, may be presented to the sensor. In this attack, the attacker should have access privilege or comprehensive device knowledge.
2. Resubmission of old digitally stored biometrics signal: Illegally intercepted data from the bypass sensor may be resubmitted to the device
3. Override feature extract: A Trojan horse program that generates pre-determined feature sets may replace the feature extractor.
4. Tampering with the feature representation: Synthetic feature sets may be used to replace legitimate feature sets.
5. Override matcher: The matcher could be replaced by a Trojan horse program that consistently produces high scores and defies system security.
6. Tampering with stored templates: The templates in the database can be modified or deleted, and new templates can be added to the database.
7. Channel attack between stored templates and the matcher: The data in the communication channel between the system's different modules can be manipulated.
8. Decision override: The biometric system's final decision result could be overridden (Prasad, 2013).

At various times, there are different strategies to thwart attacks. Simple attacks can be stopped at point 1 by monitoring finger conductivity or pulse. At the very least, encrypted communication methods can prevent remote attacks at points 4 and 8. The most straightforward way to avoid attacks on points 5, 6, and 7 is to keep the matcher and database in a secure location. Some types of attack 6 can be avoided by storing templates on a smart card that a user presents to the service point. Of course, even this will not preclude attacks in which a hacker and security professionals work together (Ratha at al., 2001).

5.4 Template protection schemes

The ideal biometric template protection scheme should possess the given four properties.

Diversity: The secured template must not allow cross-matching across databases, thereby ensuring the user’s privacy. A stolen fingerprint template from a bank's database may be used to scan a criminal database or connection to a user's medical records. Safe biometric models should not allow cross-matching across databases to prevent any unauthorized access. As a result, the user's privacy is safeguarded (Grassi and Faundez, n.d.).

Revocability: It should be straightforward to revoke a compromised template and reissue a new one based on the same biometric data (Grassi and Faundez, n.d.).

Security: It must be computationally hard to obtain the original biometric template from the secure template. This property prevents an adversary from creating a physical spoof of the biometric trait from a stolen template (Grassi and Faundez, n.d.).

Performance: The biometric template protection scheme should not degrade the biometric system's recognition performance (FAR and FRR). The necessity to handle intra-user variability in the collected biometric identifiers is a significant problem in building a biometric template protection method that meets all of the specifications mentioned above. The commonly proposed approach is storing a transformed version of the original biometric template rather than the original template itself to solve this dilemma (Shrestha, 2014.).

According to Jain et al (2008) the biometric template protection scheame are divided into two categories such as Feature Transformation method and Biometric

Cryptosystem. The technique for defining the category is illustrated in Figure 35 below.

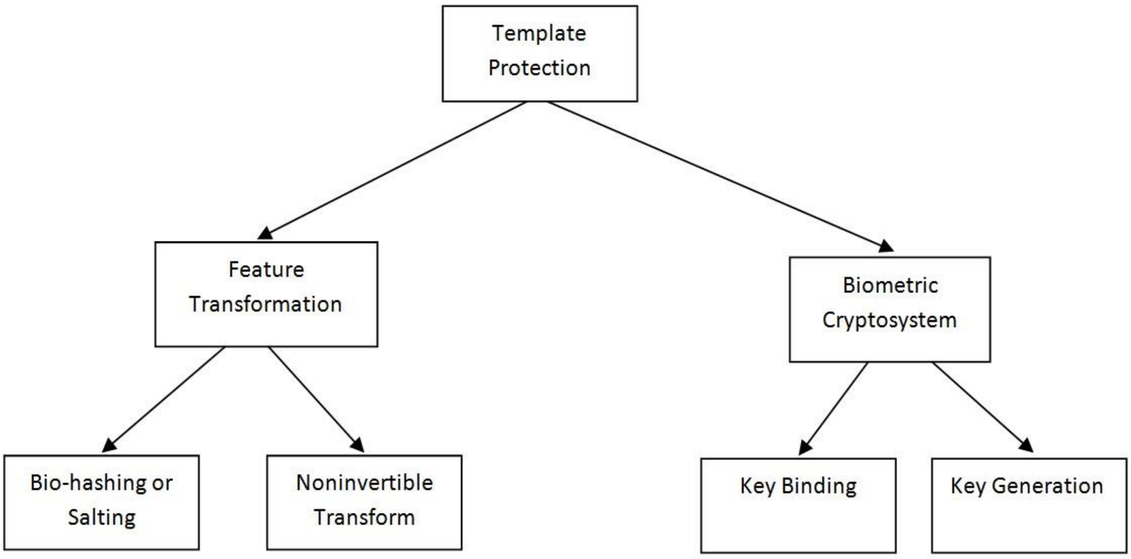


Figure 35. Categorization of template protection schemes (jain et al., 2008).

The categorization of template protection schemes proposed by Jain et al.,(2008) i.e., Feature Transformation method and Biometric Cryptosystem, is described below.

5.4.1 Feature transformation

A transformation function (F) is applied to the biometric template (T) in the feature transform approach, and only the transformed template (F(T; K) is stored in the database. The transformation function's parameters are usually extracted from a random key (K) or password. The query features (Q) are transformed using the same function, and the transformed query (F(Q; K) is directly matched against the transformed template (F(T; K) (jain et al., 2008).

According to the property of the transformation element, feature transformation techniques can be further divided into two categories:

Salting transformations: The biometric characteristics are transformed using an invertible function that is controlled by a user-specific key or password that must be kept secure. Revocability is ensured by the inclusion of a secret key. In reality, if a template is damaged, revocation and creation of a new one with a different user-specific key is straightforward. Because the transformation is generally invertible, if the user-specific key is stolen, the template is no longer secure. Different types of salting functions have been used for template transformation, such as symmetric hash functions (polynomials) or Gaussian functions (jain et al., 2008).

Non-invertible transformations: To secure the biometric template, which is "simple to compute" but "hard to reverse," a non-invertible transformation function is applied. Even if the key and/or modified template are found, retrieving the original biometric template is computationally difficult. Compared to salting, this approach is more secure. Application-specific and user-specific transformation functions may also be used to achieve diversity and revocability, which are the ideal properties of biometric template protection schemes (jain et al., 2008).

5.4.2 Biometric cryptosystems:

Biometric cryptosystems retain some public information about the biometric template, known as helper data. Although the helper data does not provide any important information about the original biometric templates, it is required during matching to derive a cryptographic key from the query biometric characteristics. Matching is done in a roundabout way by ensuring that the extracted key is correct (jain et al., 2008). Depending on how the helper data is collected, biometric cryptosystems may be categorized as key binding and key generation systems which are explained in brief below:

Key binding biometric cryptosystem: In a key binding cryptosystem, the biometric template is protected by monolithically binding it with a key within a cryptographic framework. A key-binding biometric cryptosystem gets helper data by binding a key to the biometric template that is independent of the biometric characteristics. Without knowing the user's biometric data, decoding the key or template is computationally challenging. The helper data is often made up of a link between the biometric template and an error-correcting code (selected using the key). When a biometric query deviates from the template within a certain error tolerance, the corresponding codeword can be retrieved with the same level of error and decoded to provide the same codeword and therefore the embedded key. The recovery of the correct key indicates a successful match (jain et al., 2008).

Key generation biometric cryptosystems: Biometric cryptosystems that generate keys often have low discriminability, as assessed by key stability and entropy. The repeatability of the key created from biometric data is referred to as key stability. The number of different keys that can be generated is referred to as key entropy. The helper data and the query biometric characteristics are used to create the cryptographic key, and the helper data is obtained directly from the biometric template. Direct biometric key generation is an interesting template security approach that may potentially be used in cryptography. It's difficult to create a key with high stability and entropy because of intra-user variation in the template (jain et al., 2008).

6 CONCLUSION

Doubtlessly biometric systems have made our day-to-day life more accessible because of their more reliability and safety features. This thesis has tried to cover all the important areas of a biometrics system and also to provide insight into the risk and vulnerability of such systems. In conclusion, biometric systems have a wide range of applications because of their advancement with respect to time. Earlier, such systems could be applied in very limited fields. Still, now the fields range from law enforcement agencies, the military to public health care, where the biometric systems are playing a vital role in guaranteeing safety and privacy. Biometric systems also provide information of different biometric identifiers and it can be concluded that behavioral characteristics of humans can also be used sanctifiers for authentication purposes which can be more reliable. This thesis also compared the authentication mechanism of contemporary unimodal and multimodal biometric systems and concluded that multi-modal biometrics systems have several advantages over unimodal biometrics systems. This study also provides knowledge of potential risk factors of the biometric system from hackers or organizations. Therefore, the biometric template requires a secured protection to maintain privacy as the attacks on the biometric systems. The necessary protection schemes must be followed to control these attacks.

However, with the increased development of advanced computer systems and encryption to crack passwords and security measures in today's security structure, biometrics and multi-biometrics for authentication applications are becoming progressively credible. Thus, biometric systems help build much safer and reliable security for any organization, which can eventually make the world a much easier place to maintain security. Nevertheless, biometric systems need to be properly updated and maintained; otherwise, losses will occur.

REFERENCES

Ahmad, D. T., & Hariri, M. (2012). User Acceptance of Biometrics in E-banking to improve Security. *Business Management Dynamics*, *2*(1), 1-4. Retrieved 27 March 2021 from https://www.researchgate.net/profile/Dhurgham-Al-Karawi/publication/341215049_User_Acceptance_of_Biometrics_in_E-banking_to_improve_Security/links/5eb41b0745851523bd4a4798/User-Acceptance-of-Biometrics-in-E-banking-to-improve-Security.pdf

Alaswad, A. O., Montaser, A. H., & Mohamad, F. E. (2014). Vulnerabilities of Biometric Authentication “Threats and Countermeasures”. *International Journal of Information & Computation Technology*, *4*(10), 947-58. Retrieved 11 May 2021 from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1064.3610&rep=rep1&type=pdf

Ammour, B., Boubchir, L., Bouden, T., & Ramdani, M. (2020). Face–iris multimodal biometric identification system. *Electronics*, *9*(1), 85. Retrieved 15 April 2021 from https://www.mdpi.com/2079-9292/9/1/85/htm

Aware. (n.d). Biometrics in healthcare: Improved safety and privacy for patients. Retrieved 19 March 2021 From https://www.aware.com/blog-biometrics-in-healthcare/

Bhattacharya, S., & Mali, K. (2011). Fingerprint recognition using minutiae extraction method. *Proc. of International Conferance on Emerging Technologies (ICET-2011): International Journal of Electrical Engineering and Embedded Systems*, 0975-4830. Retrieved 07 April 2021 from https://www.researchgate.net/profile/Dr-Samayita-Bhattacharya/publication/257430785_Fingerprint_Recognition_Using_Minutiae_Extraction_Method/links/00b49525442b997158000000/Fingerprint-Recognition-Using-Minutiae-Extraction-Method.pdf

Burger, B., Fuchs, D., Sprecher, E., & Itin, P. (2011). The immigration delay disease: Adermatoglyphia–inherited absence of epidermal ridges. *Journal of the American Academy of Dermatology*, *64*(5), 974-980. Retrieved 05 April 2021 from https://www.sciencedirect.com/science/article/pii/S0190962209014753?casa_token=8s7_a25c0xwAAAAA:uNgsPDl0YFvxfJmP1qDp0fwl5T1WiwjUmygjnyoRCPv0dxU30Td2vo8RmDckTuXhKNNE3qnE

Cox, M., (2019). Soldiers to Get Wearable Token in Place of CAC Card for Battlefield Computer Access. *Military.com.*Retrieved 19 March 2021 from https://www.military.com/daily-news/2019/08/06/soldiers-get-wearable-token-place-cac-card-battlefield-computer-access.html

Das, R., (2016). A Behavioral Biometric – Keystroke Recognition. Blog publication 05 October 2016. Retrieved 10 April 2021 from https://resources.infosecinstitute.com/topic/a-behavioral-biometric-keystroke-recognition/#:~:text=The%20first%20Keystroke%20Recognition%20device%20came%20out%20in,used%20in%20either%20the%20public%20or%20private%20space

Douglas, A. (2020). A brief history of Biometrics. *Bioconnect.* Retrieved 13 March 2021 from https://www.bioconnect.com/a-brief-history-of-biometrics/

Faridah, Y., Nasir, H., Kushsairy, A.k., Safle, I. S., Khan, S., Gunawan, S.T. (2016). Fingerprint biometric systems. Trends in Bioinformatics, 9(2), 52-58. Retrieved 07 May 2021 from https://www.researchgate.net/publication/309961589_Fingerprint_Biometric_Systems

Grassi, M., & Faundez-Zanuy, M.(n.d.). A protection scheme for enhancing biometric template security and discriminability. Retrieved 13 May 2021 from http://jrbp10.unizar.es/papers/S1.C1.pdf

Guennouni, S., Mansouri, A., & Ahaitouf, A. (2019). Biometric systems and their applications. In *Visual Impairment and Blindness*. IntechOpen. Retrieved 17 March 2021 from https://www.intechopen.com/books/visual-impairment-and-blindness-what-we-know-and-what-we-have-to-know/biometric-systems-and-their-applications

Ievo, (2019). How Companies across the globe are using biometric technology. Ievoreader.Edition 8 October 2019. Retrieved 28 March 2021 from https://ievoreader.com/category/general-news/

Insideprison (n.d). Biometric Technology. Offenders in the Global Biometric Market. Retrived 16 March 2021 from https://insideprison.com/article_biometrics_prisons.asp

Insider. (2019). American Airlines has launched facial recognition at the boarding gate, part of a trend sweeping US airports. Businessinsider.Edition 29 August 2019. Retrieved 28 March 2021 from https://www.businessinsider.com/american-airlines-facial-recognition-boarding-dfw-aviation-trend-2019-8?r=US&IR=T

Iritech (n.d). Technology with the Iris. Biometrics for law enforcemet. Retrieved 15 March 2021 from https://www.iritech.com/iris-biometric-law-enforcement

Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric template security. *EURASIP Journal on advances in signal processing*, *2008*, 1-17. Retrieved 16 April 2021 from https://dl.acm.org/doi/abs/10.1155/2008/579416

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.

Jarrahi, J, (2021). Whoop provides biometric health monitoring for Arctic paratroopers. *Biometric update.*Retrieved 19 March 2021 from https://www.biometricupdate.com/202102/whoop-provides-biometric-health-monitoring-for-arctic-paratroopers

Just, B. H., Marc, D., Munns, M., & Sandefer, R. (2016). Why patient matching is a challenge: research on master patient index (MPI) data discrepancies in key identifying fields. *Perspectives in health information management*, *13*(Spring). Retrieved 19 March 2021 from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4832129/

Kabir, W., Ahmad, M. O., & Swamy, M. N. S. (2019). A multi-biometric system based on feature and score level fusions. *IEEE Access*, *7*, 59437-59450.Retrieved 13 April 2021 from https://ieeexplore.ieee.org/abstract/document/8708906

Krishnakumari Y, Savitha G., (2017) A Review on Unimodal and Multimodal Biometric Systems. International Journal of Innovative Science and Research Technology, 2(5), 514-521.Retrieved 15 April 2021 from: https://ijisrt.com/A-Review-on-Unimodal-and-Multimodal-Biometric-Systems

Kwon, T., & Moon, H. (2008). Biometric authentication for border control applications. *IEEE transactions on knowledge and data engineering*, *20*(8), 1091-1096. Retrieved 17 March 2021 from https://ieeexplore.ieee.org/abstract/document/4384481

Leibacher, H., (2013). Why disney care about your fingerprints. Retrieved 03 April 2021 from https://www.worldofwalt.com/disney-world-fingerprints-us-government.html

Mayhew, S. (n.d.). History of biometrics. Retrieved 13 March 2021 from https://www.biometricupdate.com/201802/history-of-biometrics-2

Mehedi, k. (2018). What is Iris Recognition and How Does it Work?Blog publication 24 March 2018. Retrieved 08 April 2021 from https://biometrictoday.com/what-is-iris-recognition-how-does-it-work/

Merriam-Webster. (n.d.). Biometrics. In *Merriam-Webster.com dictionary*. Retrieved from https://www.merriam-webster.com/dictionary/biometrics

Migrationpolicy (2005). Biometrics, migrants, and human rights. Retrived 16 March 2021 from https://www.migrationpolicy.org/article/biometrics-migrants-and-human-rights

Mutabazi, P., (2017). Biometric Passports/ePassports and their Benefits. Retrieved 17 March 2021 from https://www.linkedin.com/pulse/biometric-passportsepassports-benefits-patrick-mutabazi

Myerson, J., (2020). Military Taking Biometrics to a New Level. Retrieved 17 March 2021 from https://www.eetimes.com/military-taking-biometrics-to-a-new-level/

Painting valley, (n.d). DNA drawing labeled. Retrieved 07 April 2021 from https://paintingvalley.com/dna-drawing-labeled/

Planet biometrics, (2020). Defense Digital Service delivers biometric prototype to army. *Planet biometrics.*Retrieved 19 March 2021 from https://www.planetbiometrics.com/article-details/i/11151/desc/defense-digital-service-delivers-biometric-prototype-to-army/

Porwik, P. (2009). The Biometric Passport: The Technical Requirements and Possibilities of Using. In *2009 International Conference on Biometrics and Kansei Engineering* (pp. 65-69). IEEE. Retrieved 17 March 2021 from https://ieeexplore.ieee.org/abstract/document/5223261

Prasad, P. S. (2013). Vulnerabilities of biometric system. *International Journal of Scientific & Engineering Research*, *4*(6), 1126-1129.

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). An analysis of minutiae matching strength. In *International Conference on Audio-and Video-Based Biometric Person Authentication* (pp. 223-228). Springer, Berlin, Heidelberg.

Recfaces. (2020). Types of Biometrics: Complete Guide. Retrieved 05 April 2021 from https://recfaces.com/articles/types-of-biometrics

Shrestha, A., (2014). Multi-biometric systems – Templates, Template Protection and Remote Authentication. Retrived 19 March 2021 from https://www.theseus.fi/bitstream/handle/10024/79722/Multibiometric?sequence=1

Thakkar, D. (n.d). Bayometric. Gait Recognition Systems Can Identify You with Your Manner of Walking. Retrieved 13 April 2021 from https://www.bayometric.com/gait-recognition-identify-with-manner/

Thakkar, D. (n.d). Bayometric. An Overview of Biometric Iris Recognition Technology and Its Application Areas. Retrieved 07 April 2021 from https://www.bayometric.com/biometric-iris-recognition-application/

Thakkar, D. (n.d). Bayometric. Biometric Identification for Law Enforcement Agencies: From Local Crimes to National Security. Retrieved 15 March 2021 from https://www.bayometric.com/biometric-identification-law-enforcement-agencies/

Thakkar, D. (n.d). Bayometric. Biometrics for Civil Identification: Your Fingerprint is All You Need to Prove Your Identity. Retrieved 03 April 2021 from https://www.bayometric.com/biometrics-civil-identification/

Thakkar, D. (n.d). Bayometric. Biometrics for Elections and Voter Registration: One Person One Vote Finally Becomes a Reality. Retrieved 03 April 2021 from https://www.bayometric.com/biometrics-elections-voter-registration/

Thakkar, D. (n.d). Bayometric. Hand Geometry Recognition Biometrics: All You Need to Know. Retrieved 07 April 2021 from https://www.bayometric.com/hand-geometry-recognition-biometrics/

Thakkar, D. (n.d). Bayometric. Portable Fingerprint Scanners for Law Enforcement: Identity Verification on the Street. Retrieved 15 March 2021 from https://www.bayometric.com/portable-fingerprint-scanners-law-enforcement/

The Guardian. (2019). Facial recognition… coming to a supermarket near you. The Guardian International Edition 4 August 2019. Retrieved 20 March 2021 from https://www.theguardian.com/technology/2019/aug/04/facial-recognition-supermarket-facewatch-ai-artificial-intelligence-civil-liberties

Trader, J., (2012). Biometrics and Healthcare Data Integrity. Blog publication 05 September 2012. Retrieved 19 March 2021 from https://www.m2sys.com/blog/health-care/biometrics-and-healthcare-data-integrity/

Tutorialspoint, (n.d.). Voice Recognition. Retrieved 13 April 2021 from https://www.tutorialspoint.com/biometrics/voice_recognition.htm

Villaverde, R., (2018). Facial recognition system. Blog publication 07 August 2018. Retrieved 08 April 2021 from https://medium.com/adalab/facial-recognition-system-5642f57c220a

Walsh, S., Pośpiech, E., & Branicki, W. (2016). Hot on the trail of genes that shape our fingerprints. *Journal of Investigative Dermatology*, *136*(4), 740-742. Retrieved 7 April 2021 from https://www.sciencedirect.com/science/article/pii/S0022202X16004528

Westgate, A., (2018). How can biometrics benefit the healthcare industry? Blog publication 4 December 2018 Retrieved 19 March 2021 from https://www.itproportal.com/features/how-can-biometrics-benefit-the-healthcare-industry/

Wikipedia. (n.d.). Iris Recognition. Wikipedia.org. Retrieved 7 April 2021 from https://en.wikipedia.org/wiki/Iris_recognition

Wisdomjobs. (n.d.). BEHAVIORAL MODALITIES – BIOMETRICS. What are Behavioral Modalities? How does it help in Biometrics? Retrieved 11 April 2021 from

https://www.wisdomjobs.com/e-university/biometrics-tutorial-2329/behavioral-modalities-25348.html