Biometric Security Systems

By Rishika Juloori

APID – A 59725470

Major - Computer Science Engineering

EGR 100 Section 10 (Spring 2020)

ACKNOWLEDGEMENTS

I would like to sincerely thank Dr. Jenahvive Morgan, Professor for EGR 100, who has helped me in every stage of this project and has provided me with her valuable suggestions and insights.

I would also like to thank my parents and all those who have provided me with enough resources and time to finish this project to the expected mark.

INDEX

1. INTRODUCTION
2. FINGERPRINT RECOGNITION
3. VOICE RECOGNITION BIOMETRICS
4. OTHER BIOMETRIC SYSTEMS
5. ADVANTAGES AND DISADVANTAGES OF BIOMETRICS
6. APPLICATIONS OF BIOMETRICS
7. RESULTS AND CONCLUSION
8. CITATIONS

Introduction

With growth in almost every field in the world, the need for security and protection of classified details is being as never before. A substantial amount of population is realizing the need to secure anything from physical, like cash, jewelry, documents, etc. to personal and confidential information concerning people and their lives. To tackle this kind of situation, people need to come up with an idea that would not only be impossible for tricksters to steal our entities but also an efficient and convenient way to establish one's identity. Biometrics could play a key role in this. Biometrics uses the concept of using the identity of a person, which are unique to him/her, to improve the security.

Biometrics comes from the Greek words 'bio' and 'metrics' which mean 'life' and 'measure' respectively. It uses the idea of identifying a human based on their distinguishing characteristics. The combination of biometric data systems and biometric recognition technologies forms the biometric security system. Only if the traits match with the data, will the system provide its access to the user. It uses automated schemes to identify people on the grounds of their biological characteristics.

Our security systems have started from the notion of using what we have – particularly something physical – which could be in possession of a person. It then evolved into exploring the aspect of making use of our knowledge and memory. A typical example would be a password utilized for various services. We now use ourselves to serve the purpose of security and identity. The combined use of these ideas may help us shield our information and provide us the assurance towards a riskless safety. Most importantly, the third measure is very strenuous to forge or steal and impossible to forget. Usage of this technology can establish identity based on who a person is rather than their knowledge or acquisition. This combined use of ideas for supplementary security is sometimes called 'duel factor authentication scheme'.

The biometric characteristics could be of two types:

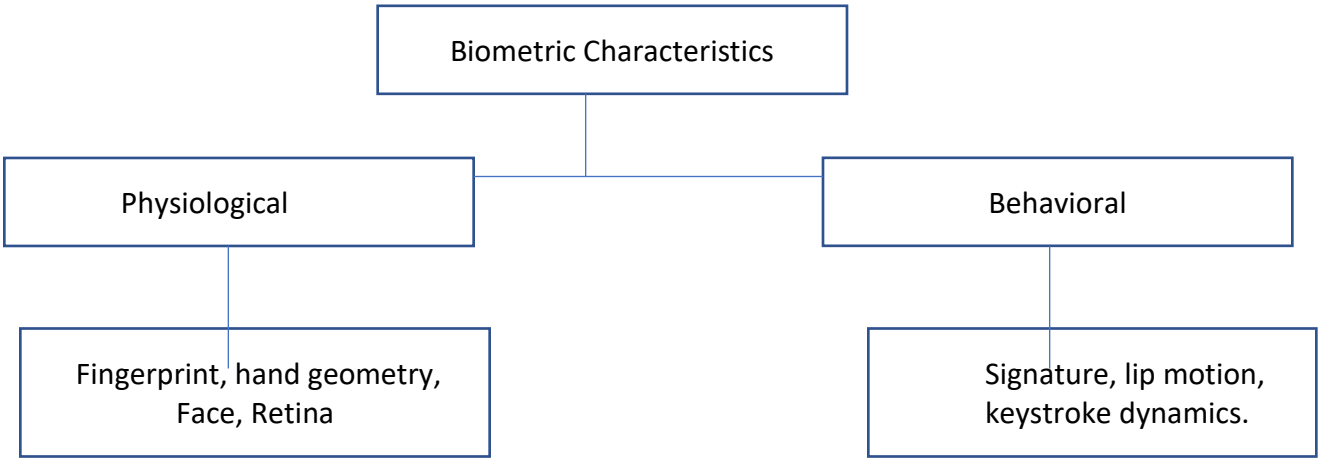

Figure 1 : Basic divisions and examples of biometric characteristics.

The biometric characteristics should typically fulfill some properties like permanence, acceptability, performance, uniqueness, universality, collectability, circumvention.

- Permanence: a trait which is constant over a long period of time must be chosen for it to be stored in the database and not change. This is largely dependent on the age of the person.
- Acceptability: This parameter denotes that required traits are used only where biometrics can be applied and accepted.
- Performance: indicates how well the system is working.
- Uniqueness: The characteristic chosen has to be unique to that person.
- Universality: Though the characteristic chosen has to be unique to that person, it should be such that the whole population should hold it but has to be different for everyone.
- Collectability: The process to obtain the trait should not be complex.
- Circumvention: This characteristic is similar to discussing about an invalid move. It takes into account the failure to acquire the traits which satisfy the above given properties.

A biometric system resembles a pattern recognition system. An all-inclusive universal biometric system can be seen as a process of four modules: a sensor module, a quality assessment and feature extraction module, a matching module and a database module.

- Sensor Module: This needs an apt scanner which could obtain raw data of the individual's traits. The quality of the sensor is very important in this case because the sensor serves as an interface between the man and the system and its poor quality might lead to a failure in acquiring the acceptable traits. For example, some if the biometric system types require image capturing, lack of camera quality may impact the data stored and used by the system.
- Quality Assessment and feature extraction module: Only if the raw data is of a suitable quality, it is further processed. If the quality is not met, the users are requested to provide the raw data once again. The system then gets hold of some salient features for extraction and stores it in the database, which is often referred to as 'template'.
- Matching and Decision-Making Module: Every time the user gives the raw data for identification, the features are matched with the templates previously stored. The match is scored which could help in decision making and assess whether the current information matches with the template. The match module uses a decision-making module for the match scores to validate the claimed identity.
- System Database Module: The data captured during enrollment is stored along with their biographic information. This is because the process may or may not be proceeded under supervision.

The template of the user could be taken as a single sample or multiple samples. For example, in face recognition systems, the data is stored as multiple templates as opposed to the fingerprint system. The whole process generally goes as enrollment followed by recognition (verification or identification). Enrollment refers to data collection. Verification mode validates a person's identity which prevents multiple people from using the same ID. To verify identity, it is typically done using a PIN or smart card or a username. But in identification mode, the system

tries to match the data of the person by searching the templates of all the users in the database. This in contrast to verification, ensures that a single person is not using multiple identities.

With this security system expanding its wings into every profession, 'multibiometric systems' could ensure a higher level of safety than that of the most unibiometric systems. Multibiometrics combines biometric information from multiple sources, which could be possible by 'fusing' multiple traits. This could improve the accuracy of the system and protect the users from any unethical activities. Yet, presently unibiometric systems are in widespread use and are the fundamentals to understand this technology, and hence are focused and highlighted more often.

The picture below sums up the biometrics process aptly.

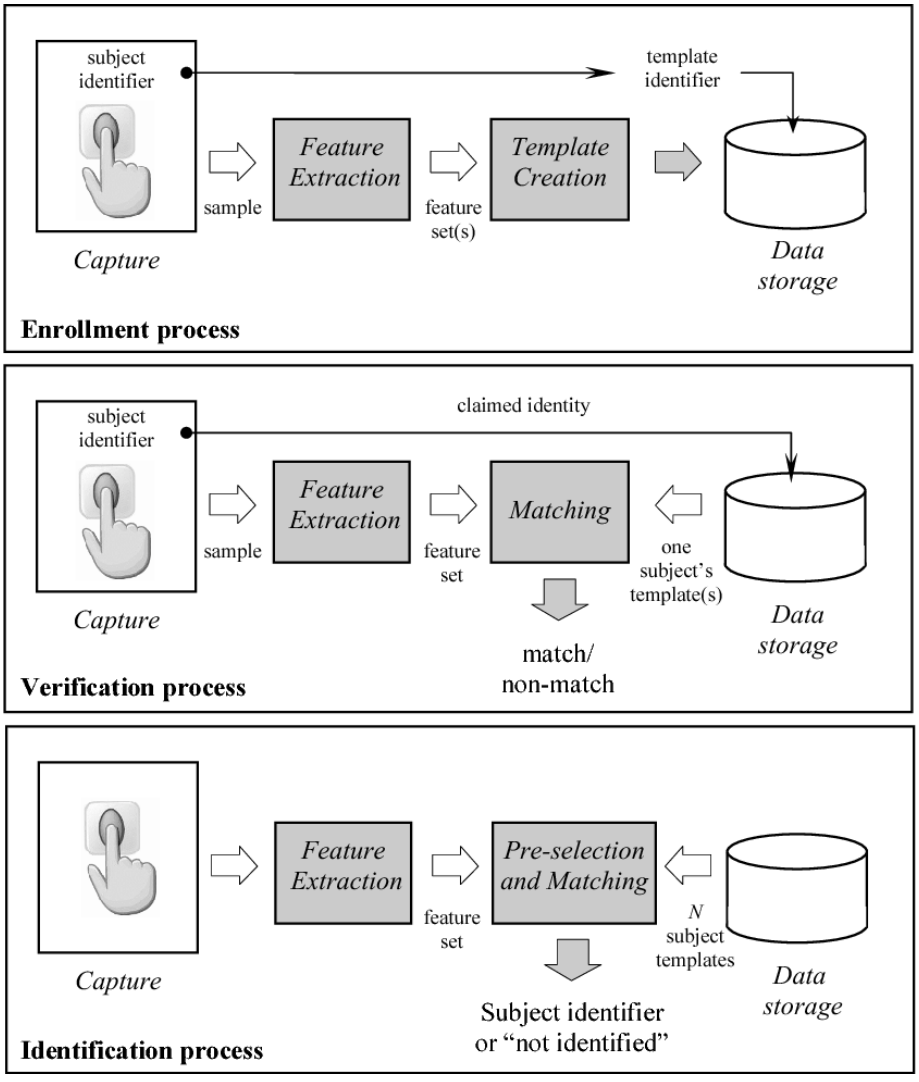

Figure 2: Enrollment and recognition stages (including verification and identification)

But the idea of this technology has been occurred to our ancestors way before than it looks like. In the 19th century, Alphose Bertillion, realized that some physical features of the human body remain unchanged throughout life which led to the development of a method of taking body

measurements of persons to identify them. But this method diminished quickly because it was let out that the persons with same body measurements alone can be falsely taken as one.

The first institutionalized use of biometric data was their usage in crime registers. Naturally, the process involved human experts who used magnifying glasses. In 1903, New York state prison adopted fingerprint identification for verification of criminals which paved way for the founding of the Fingerprint Analysis Department of FBI in 1921. Hence, the biometrics field reached a milestone when the first AFIS (automated fingerprint identification system) was created in the 1960's.

Another such algorithm was the iris recognition which was invented by John Daugman in 1953. It is widely considered as the fastest and most accurate method of identification that captures photos of eyes and maps the unique iris pattern to verify an individual's identity. In 2011, India introduced a mass iris recognition system with an aim to make people use their eyes for any matters concerning the State.

Today, biometric has come up as an independent field of study with precise technologies of establishing personal identities. There are many types in this technology. Some of the prominent and most widely used ones include Fingerprint Recognition, Face Recognition, Iris recognition, Hand Geometry Recognition, gait Recognition, Voice Biometrics, Forensic Dental Recognition, DNA biometrics system, etc. Some of the systems from Multibiometrics include multispectral face regontion and using face and ear. [1][2][3][4][7].

Fingerprint Recognition

The fingerprint recognition system makes use of the pattern of ridges and valleys on the surface of the finger that are unique to every human. Ridges and valleys are the upper and lower level segments of the finger respectively. The uniqueness of the pattern is determined by the pattern of ridges, valleys and minutiae points (specific identification spots on the fingerprint). The fingerprint recognition typically takes place in six steps:

- Acquiring the fingerprint image form the user. The quality of the scanner is suggested to be of maximum quality so that there is no further problem in storing this data and matching it for further purposes. The scanner should be able to trace the prints of any kind of finger.
- Image quality is improved using algorithms. In case the image is damaged, this step helps in improving the output. The image is filtered to make the ridge and valley patterns more comprehensible.
- The image is prepared to start minutiae extraction.
- The fingerprints are then classified into different classes. This might be a tedious process even for the system because the patterns at this stage maybe ambiguous and difficult to sort.
- Minutiae is then extracted from the raw data. Only three types of minutiae data is extracted from the data – ridge ending, continuous line and bifurcation. All of this technical data helps in further recognition.
- This set of information is compared with external information for identification and verification.

Acquiring the perfect fingerprint image may not always be as easy as it seems to be. The type of the image procured could also vary depending of the intrinsic finger quality and condition of the finger. To be clear with the standards of the image, some parameters to obtain the fingerprint image have been defined. Some of them include:

- Resolution – refers to the dots (pixels) per inch. A minimum resolution of 500 dpi is encouraged by commercial devices. However, forensics now use 1000 dpi scanners.
- Area – it is the size of the area sensed by the scanner. In case of a multi-finger scanner, a 2 x 3 sq. inch area would be enough for all the four fingers to fit in. While single finger scanners could have an area of about 1 x 1 sq. inch.
- Gray level quantization and gray range - Gray level quantization is the highest number of gray-levels in the image. The gray-range is the concrete number of gray-level spots irrespective of the gray-level quantization. Color does not play a key role in this technology.
- Spatial Frequency response – it refers to the ability of the device to put out the details of output image into various frequencies.
- Signal to noise ratio – The signal magnitude and noise are related to gray-range and standard deviation of fray-levels respectively.

Fingerprint recognition is widely used because of its simplicity to use and install. It requires minimum equipment and consumes nominal resources. However, it is not without any downsides. In case the finger gets damaged or experiences any alterations, it becomes strenuous for the device to carry out the process and pinpoint the identity.

Fingerprint technology has wide range of applications. Due to its ease to store and manage, it is used in stores and institutions for validating the identity of the person and ensuring the security of the of staff and public. Moreover, this technology is seen in airports and checking authorities as the most commonly used method of identification. [5][2].

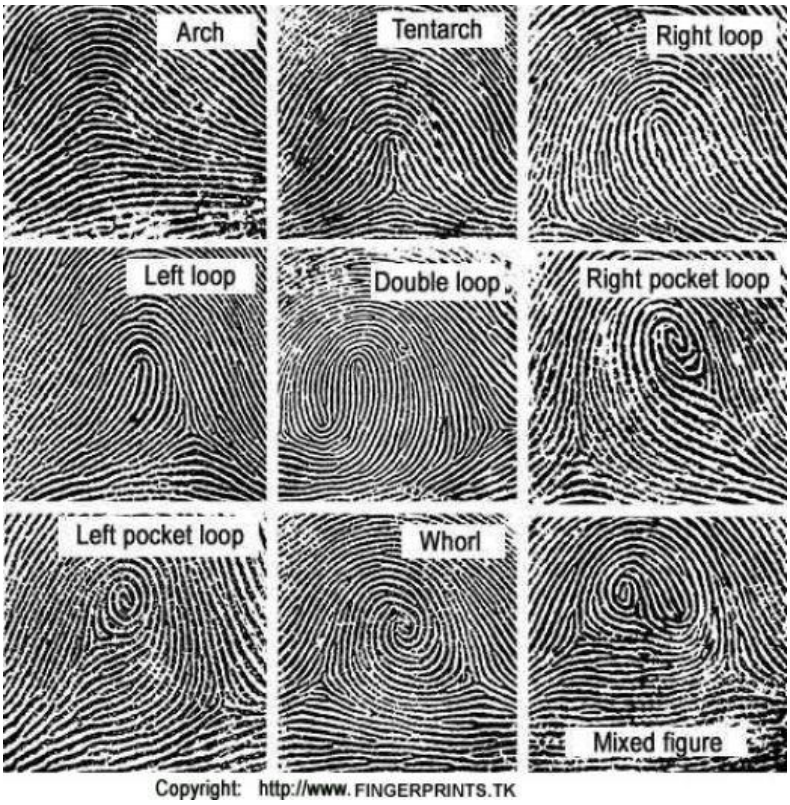

Figure 3: Types of finger patterns

Voice Recognition Biometrics

Voice biometrics makes use of qualities of vocal tracts, mouth, nasal activities and lips from the user. It is a combination of both physical and behavioral biometric characteristic. There are usually two steps in this process: enrollment and authentication. Enrollment captures the samples and stores as a reference model (reference voiceprint or speaker model). Speaker authentication includes three different types: text dependent, text prompted and text independent.

Text–dependent dialogs: This type of technology is based on pre-determined passwords.

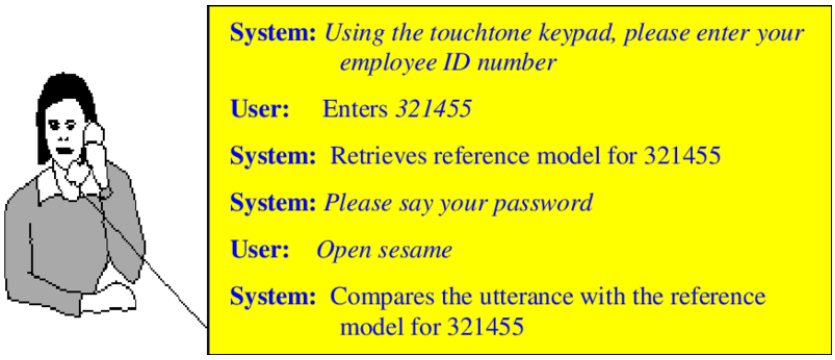

Figure 4: Text dependent dialogs

This is a multi-factor authentication as it first requires manually entrance of the password and then voice authentication. But this may not be fully convenient as passwords may be forgotten or lost and text-dependent voice biometrics may need passwords in the process. The technology might prove to be difficult to use when the user's voice is disturbed by external voices as the system cannot filter unwanted disturbances. Abstractly, text-dependent authentication may be prone to recordings, but it depends on how protected and anti-spoof the system is.

Text prompted technology: In this system, the user is prompted for an ID or password and then is asked to utter a phrase given by the system itself unlike text-dependent dialog where the user utters the same password every time he or she tries to login.

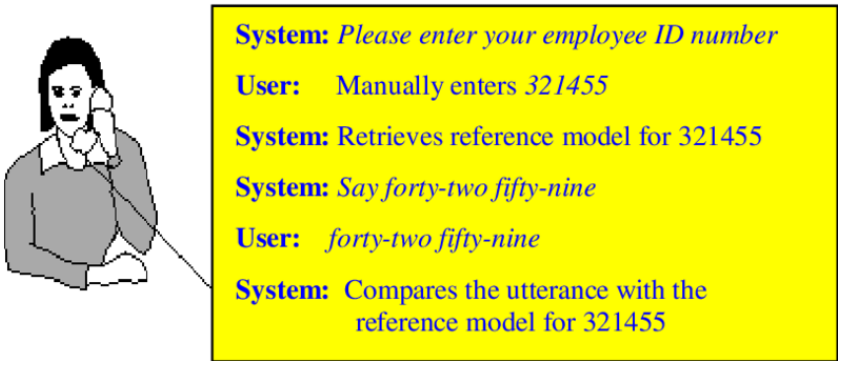

Figure 5: Text-prompted dialogs

This technology is much safer from being recorded as the requested items cannot be predicted. Also, the prompted phrases are extremely simple to utter. But this technology might likely not suit customers who do not prefer the long procedure. In case the customer becomes stressed up, the system cannot capture the stress speech patterns.

Text-independent dialogs: this type of system requests the user to talk multiple times and answer different questions every time.

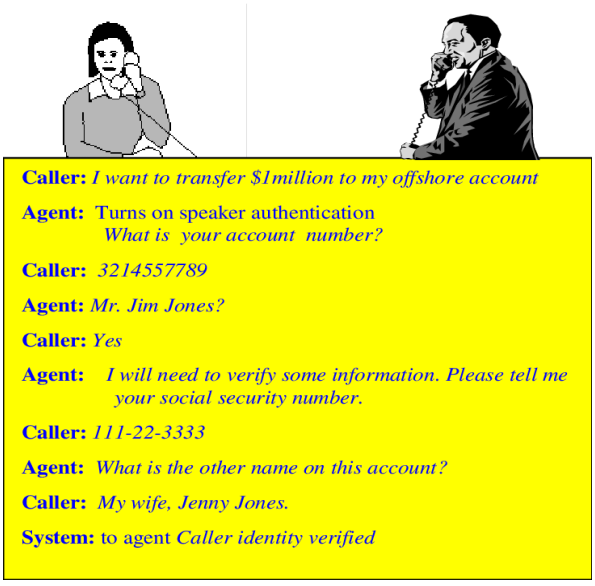

Figure 6: Text-independent dialog

This system could be much safer than the above-mentioned ones. But this could be a difficult one to deal with as every utterance would be different from each other and comparing them might need the system a huge data. This would also be time-taking. Moreover, matters over privacy issues have been raised. Some institutions ask for the customer's approval for recording their voice, while some just record the voice without any notification. Though it is safer than the previous methods, it has its own downsides.

Speech authentication may pose a problem to those who cannot use the technology, i.e., people who cannot speak, whose have hoarse voices and people with soft tone. These can be brought to the notice of the institution and required arrangements could be made for alternative security systems. The technology can be used for basic usage where voices can be easily detected, and problems resolved within few moments. The selected authentication may not always provide convenience for the users but may provide secure locking systems. [8]

Other Biometric Systems

The fingerprint recognition system in the previous pages provides an overview of how a typical biometric system works. This section gives an overview of many other biometric systems present.

1. Face recognition - The output of this system is usually acquired by the location and shape of the facial attributes like eyes, eyebrows, nose, lips, etc. This is a complicated one because face anatomy is rigid, and most faces have similar structures. The case would become even more complicated if this system is used by identical twins.
2. Hand geometry – This system is bases itself on the information taken from the hand of the user such as size of palm and fingers. This is inexpensive and any minor changes to skin such as dryness or wetness does not affect its detection. But this may not be effective when considering large populations. It might not be highly efficient with growing children and even when people have jewelry on them. Its physical size also serves as a restraint.
3. Palmprint – This is parallel to the structure of fingerprint recognition, but the area of the palm is bigger than that of the fingers. When used a high-resolution scanner, the ridge and valley patterns, principal lines and wrinkles could help identify the user.
4. Iris recognition – Iris is the central region of the eye. The iris could be very effective in differentiating every human being from each other. Though the present iris recognition systems are not very satisfactory, many researchers are optimistic about its future possibility in proving to be able to handle large amount of information. This could be competent even in case of identical twins and could even successfully differentiate between the normal and fake lens.
5. Keystroke recognition – This system may not prove to be unique but could be considered as secondary identification information. This takes behavioral trait into consideration where it recognizes people based on the way a person types on keyboard.
6. Signature – This refers to the manner a person signs his or her name. This system takes in a behavioral biometric. Though this is accepted at many places, it could be forged by professionals.
7. Gait – Gait refers to the way the user walks. This can enable users to track anyone over a period of time. But this may not prove to be effective due to several factors such as footwear, clothing, walking surface, etc.
8. DNA – DNA is the most unique characteristic found in humans. This system proves good in forensics but is not used widely due to lack of technology and privacy issues. This information could be misused for fraudulent purposes.
9. Ear – There are suggestions that the shape of the ear and the structure of its part called pinna are distinctive in every human. The important points on the pinna could be used to distinguish between different individuals.
10. Odor – It Is believed that odor is emitted from pores in from the skin which could be detected using chemical sensors. These collected templates could be later classified into a template. [2][1][7]
11. Face Thermography – measures the thermal radiations from the face. It is successful in verifying the identity of the person without contact.

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	high	low	medium	high	low	high	low
Fingerprint	medium	high	high	medium	high	medium	high
Hand Geometry	medium	medium	medium	high	medium	medium	medium
Keystrokes	low	low	low	medium	low	medium	medium
Hand Vein	medium	medium	medium	medium	medium	medium	high
Iris	high	high	high	medium	high	low	high
Retinal Scan	high	high	medium	low	high	low	high
Signature	low	low	low	high	low	high	low
Voice Print	medium	low	low	medium	low	high	low
F.Thermogram	high	high	low	high	medium	high	high

Figure 7: Comparison between various types of biometrics and the extent of their properties being fulfilled.

Figure 8: Various types of biometrics

Advantages and Disadvantages of Biometrics

Biometrics provides its users with the most unique features, which are not provided by any other security system. This technology empowers the users to possess the key to the security system with themselves. The possibility of two users having the same data for identification in this technology is nearly zilch. Even identical twins have different information to provide to the biometrics security system.

This technology also makes it less possible for unethical hackers to guess or forge the access to highly sensitive information. It is highly impossible for others to replicate the access data, which could security from unauthorized users.

The data stored in the biometrics database can never be lost or forgotten and hence it makes it easier for the users to maintain high level security to their assets with minimal knowledge or memory. Except the modern and most sophisticated biometric security systems, most of these are facile to install and use. Even the investment for the same once the research for the technology is accomplished is minimal.

Whilst minor changes in our body, the behavioral and physical characteristics used to provide data are less prone to sudden changes. It also requires negligible training and consumes least time compared to the other security systems. Due to its flexibility, it can be used in various departments ranging from general store or mobile lock to security and forensics departments. Passwords and PINS which are highly vulnerable to be forgotten by the users could be replaced with face recognition or other similar systems which would ensure more safety and convenience.

Though this system seems to be very modern, flawless and appealing to use, it has its own complications and limitations. For example, in case of fingerprint recognition, if a person experiences finger damage or slight modifications, the device would find it difficult to recognize his or her identity. Or, in case the users have lost their fingers in a mishap, then there would be no means for them to prove their identity. In case of voice recognition system, voice patterns might differ for aging users. Even a problem in throat or a noise disturbance in the environment could make it hard for the system to identify the users.

For iris and retina biometric recognitions, users halt the process in the opinion that the technology might tamper their health. Most of the users believe that it the scans might affect their eyes negatively. Furthermore, the biometrics system has not developed itself to the extent that it could store a large amount of database such as in this case and hence needs new technology in doing so. This would shoot up the costs for this technology and hence may not be a great viable option to look into. This concern is accompanied by accuracy and privacy due to lack of adequate information and technology. [7][1][2][6]

Applications of Biometric Security Systems

Biometrics security system is being assimilated into many different fields today because of the need of security. These applications could be labelled into three different types:

- Commercial applications – examples are ATMs, computer login, mobile phone, internet, smart card, mobile banking, etc.
- Government applications – examples are national IDs, licenses, border and passport control, etc.
- Forensic applications – examples are in case of missing children, parenthood determination, criminal identification, corpse identification, etc.

One of the best examples of successful application if biometrics include the 'Schiphol Privium' scheme at Amsterdam airport. Here, passengers could voluntarily sign up for the iris-scan smart scans where passengers would need to insert the card and look through a camera which would finish their verification process. This has improved security and has also reduced the time for the procedure.

Some of the ATMs in Japan have palm-vein authentication system to validate the customer and carry out a transaction. The users would not even need to place their hand on any device. A sensor would identify the pattern of the user's veins and help them carry out the transaction.

The US supermarket chain, Kroger has installed fingerprint scanners in few of the stores to help the customers pay and transact in a convenient manner. The US-VISIT, the border security system requires its foreign visitors arriving to the US have their fingerprints stored to validate the visitor's travel documents at the port of entry.

The Government of India has deployed a project to create unique identity cards for every citizen of the country. This card makes use of the fingerprints of every citizen. This card would enable every citizen to prove his or her identity in any part of the country. [2]

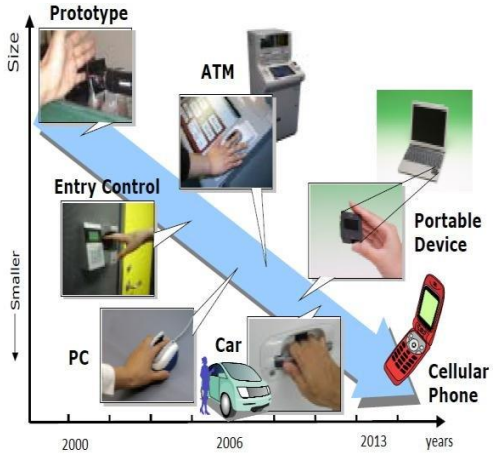

Figure 9: Various applications of biometrics

Results and Conclusion

The world is witnessing a rapid growth in computer networking and commerce which makes it a complicated for everyone to run the society. But this advancement is being accompanied by frauds and burglaries, posing a threat to both personal and societal assets – be it material or information. The society therefore needs a secure system to protect everyone from the situation.

Currently, biometrics has proven to be one of the best ways we can ensure security and convenience at the same time. Though most of the systems we have today may not seem to compensate for our needs today, we definitely have scope to improve our technology and implement the systems which do not prove to be helpful.

The advantages do seem to overweigh the disadvantages in the present situation for us to use the biometrics for our security but there are definitely questions lingering around about technologies involved, privacy issues, about who would control the information and fears about the huge amount being lost after the hard work. Yet the world is working collectively towards providing others the luxury of safety and security accompanied by convenience.

References

[1] Harbi Mohammad Ahmad AlMahafzah, "*Person verification based on Multibiometric systems,*" Feb-2013. [Online]. Available: http://hdl.handle.net/10603/35959. [Accessed: Apr-2020].

[2]. Jain A.K., Ross A. (2008) *Introduction to Biometrics*. In: Jain A.K., Flynn P., Ross A.A. (eds) *Handbook of Biometrics*. Springer, Boston, MA

[3] "*Biometrics - Overview*," *Tutorialspoint*. [Online]. Available: https://www.tutorialspoint.com/biometrics/biometrics_overview.htm. [Accessed: 19-Apr-2020].

[4] "*THE PAST, PRESENT AND FUTURE OF BIOMETRICS*," May-2017. [Online]. Available: http://annals.fih.upt.ro/pdf-full/2017/ANNALS-2017-2-24.pdf. [Accessed: Apr-2020].

[5] D. Maltoni, D. Maio, A. k Jain, and S. Prabhakar, "*Handbook of Fingerprint Recognition*" 2009. [Online]. Available: https://books.google.com/books/about/Handbook_of_Fingerprint_Recognition.html?id=1Wpx25D8qOwC. [Accessed: Apr-2020].

[6]. S. Newaz, "Top ten mind blowing advantages of biometric technology," *M2SYS Blog On Biometric Technology*, 18-Dec-2019. [Online]. Available: http://www.m2sys.com/blog/biometric-hardware/top-ten-mind-blowing-advantages-of-biometric-technology/. [Accessed: Apr-2020].

[7]. C. Le, "*Survey of Biometrics Security Systems*," 2011. [Online]. Available: https://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet.pdf. [Accessed: Apr-2020].

[8]. J. Markowitz, "*Voice Biometrics*," *researchgate,* Sep-2000. [Online]. Available: https://www.researchgate.net/publication/27293606_Voice_Biometrics. [Accessed: Apr-2020].

[9]. A. Ross, A. K. Jain, and S. Prabhakar, "*An Introduction to Biometric Recognition*," Feb-2004. [Online]. Available: https://www.researchgate.net/publication/3308596_An_Introduction_to_Biometric_Recognition. [Accessed: Apr-2020].