IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 9, September 2021

DOI: 10.17148/IARJSET.2021.8940

Biometric As Defense Technology

Dr. Harpreet Kaur Sethi[1] , Ashish Bajpai[2]

[1]Assistant Professor,Dept Of Computer Science, Saroop Rani Govt College (W),Amritsar, Punjab

[2]Assistant ProfessorDept Of Computer Science& Applications, SMHS Govt College (Sas) Nagar Mohali, Punjab

Abstract: Biometrics is the process by which a person's unique physical and other traits are detected and recorded by an electronic device or system as a means of confirming identity. The term “biometrics” derives from the word “biometry”, which refers to the statistical analysis of biological observations and phenomena. Biometrics is the measurement of physiological characteristics like – but not limited to – fingerprint, iris patterns, or facial features that can be used to identify an individual.

keywords: Biometrics,, Defense, Identity, Biometry , Biological , Fingerprint, Pattern

1.INTRODUCTION

The term Biometrics is made from two words - **'Bio (Greek work)' and 'Metrics' where bio means life** and metrics indicate measurements. Biometrics is widely used for security purposes as it provides a high degree of accurateness in recognizing an individual. Biometrics are body measurements and calculations related to human characteristics. Biometric authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological characteristics, which are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odor/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, keystroke, signature, behavioral profiling, and voice. Some researchers have coined the term 'behaviometrics' to describe the latter class of biometrics.

2. HISTORY

Within the following century, biometrics grew exponentially as a field of research. There were so many advances within the 1900s that it had from the second half of the century:

- In the 1960s, semi-automated facial recognition methods were developed requiring administrators to analyze facial features within an image and extract usable feature points. Much more manual than the ones we can use to open out phones.
- By 1969, fingerprint and facial recognition was so widely used in law enforcement, the FBI put funding towards developing automated processes. This was a catalyst for the development of more sophisticated sensors for biometric capture and data extraction.
- In the 1980s, the National Institute of Standards and Technology developed a Speech group to study and push forward the processes for speech recognition technology. These studies are the basis for the voice command and recognition systems we use today.
- In 1985, the concept that much like fingerprints, irises, were unique to everyone was proposed and by 1994, the first iris recognition algorithm was patented. In addition, it was discovered that blood vessels patterns in eyes were unique to everyone and were used for authentication as well.
- In 1991, facial detection technology was developed making real time recognition possible. While these processes had many faults, it skyrocketed interest in face recognition development.
- By the 2000s, hundreds of biometric authentication recognition algorithms were functional and patented within the USA. Biometrics were no longer being implemented in just large corporation or a government setting. They were sold in commercial products and were implemented at large scale events like the 2001 Super Bowl.

2.1 Then to Now as defense

In the past 10 years alone, research in biometric technology has continued to advance at a rapid rate. Biometrics have gone from a novelty technology to a part of everyday life. In 2013, Apple included fingerprint to unlock the iPhone,

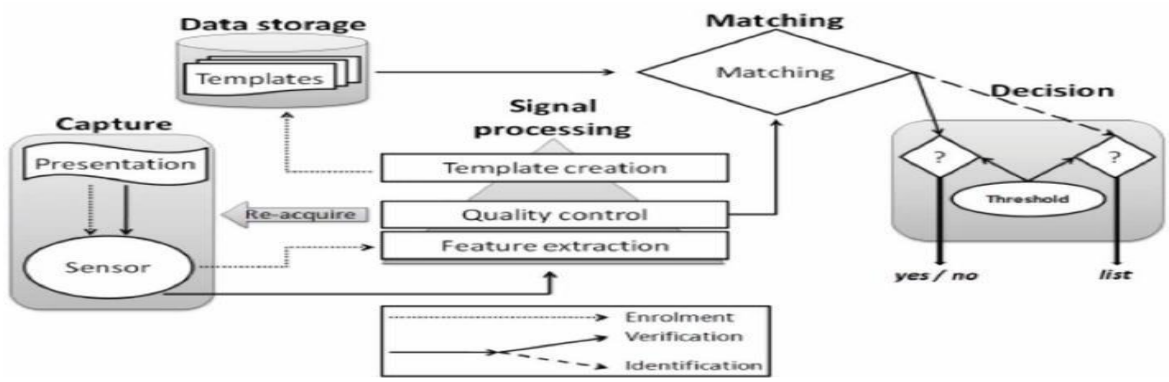
DOI: 10.17148/IARJSET.2021.8940

beginning the wide acceptance of biometric as a means of authentication. Nowadays, most mobile phones have biometric capabilities and many apps use biometrics as an authenticator for everyday functions.

2.2 Looking forward for defense

Even with all the growth, the development possibilities of biometric authentication and identification are far from being exhausted. As biometrics research continues, we see it being merged with artificial intelligence. The intention is to construct biometric devices and systems that can learn and adapt to its users. Creating a seamless and frictionless authentication experience. As biometrics become more common, the use of identification proxies may cease to exist. When you can use yourself as proof of your own identity, you don't have to carry around keys, card or fobs anymore. A future that has a rightfully identified society with frictionless transactions, interactions, and access control could be horizon.

3. ARCHITECTURE OF BIOMETRIC SYSTEM



The architecture of a biometric system, which consists of the following elements. The capture module that represents the entry point of the biometric system and consists in acquiring the biometric data in order to extract a digital representation. This representation is used later in the following phases.

1. The module of signal processing makes it possible to optimize the processing time and the digital representation acquired in the enrollment phase in order to optimize the processing time of the verification phase and the identification.
2. The storage module that contains the biometric templates of the system enrolees.
3. The matching module that compares the data extracted by the extraction module with the data of the registered models and determines the degree of similarity between the two biometric data.

The decision module that determines whether the similarity index returns through the matching module is sufficient to make a decision about the identity of an individual.

4. APPLICATIONS OF BIOMETRICS AS DÉFENSE TECHNOLOGY

There are numerous applications for the use of Biometric Technology, but the most common ones are as follows:

1. Logical Access Control
2. Physical Access Control
3. Time and Attendance
4. Law Enforcement
5. Surveillance

4.1 Logical Access Control

This market application refers to gaining access to a computer network either at the place of the business or corporation or via a secured remote connection from a distant location.The security tool that is most commonly the traditional username and password. Although this combination may have worked effectively in the past, it is now definitely showing signs of severe weaknesses, by being a primary target for Cyberattacks. Usernames and passwords can be very easily compromised and hijacked via a Denial of Service or a dictionary style attack. Because of the frequency of these types of attacks, many organizations are now requiring their employees to create long and complex passwords. They have to contain a combination of upper and lower case letters, punctuation marks, spaces, numerals, and other types of special characters. and these are so difficult to remember, employees are literally writing

their newly created passwords on Post-It Notes and attaching it to their workstation monitor. This phenomenon has become known as the "Post It Syndrome. To combat this and the other security weaknesses posed by using passwords, the use of Biometric Technology has been called upon to replace it in its total entirety.
In this regard, the two modalities which are used the most are that of Fingerprint Recognition and Iris Recognition. With one swipe of the finger or one scan of the iris, the employee can be logged into their workstation within just one second.
Because of this "one scan" capability, these modalities have also become known as "Single Sign On Solutions." These devices can be connected to the workstation via a USB connection, or the sensor can be embedded into the computer or wireless device itself.

- An individual can be logged into a network just a matter of two seconds or less, versus the number of minutes it can take with a password;
- An individual's unique physiological or behavioral traits cannot be stolen or hijacked, unlike a password..

4.2 Physical Access Entry

Physical Access Entry refers to giving an employee of a business or a corporation access to a secure building, or even a secure office from within it. Traditionally, keys and badges have been used. However, the main problem is that these tools can be very easily stolen, lost, replicated, or even given to other employees who do not belong in those secure areas.
Smart Cards have been used to help alleviate these security weaknesses, but they too have their own set of limitations as well. Fingerprint Recognition and Hand Geometry Recognition are used in this application the most, along with Vein Pattern Recognition. In these instances, one of these Biometrics is hard wired to an electromagnetic lock strike.Once the identity of an individual has been confirmed by either their fingerprint or through the shape of their hand, the lock strike will, within seconds, open the door to the secure area .In Physical Access Entry scenarios, the Fingerprint Recognition device or the Hand Geometry scanner can either operate either in a standalone or a client-server mode. The advantages of the latter are as follows:

- Greater Biometric Template storage capacity;
- Larger applications (such as physical access to multiple buildings and multiple doors) can be much better served.
- All of the Biometric information and data can be stored on a central server for the efficient processing of the Verification and/or Identification transactions.
- The Biometric modalities which are wired to each and every door in an organization can be centrally administered at the server level, without having to perform these same functions separately at each device.

Fingerprint Recognition devices and Hand Geometry scanners can also work together to create a Multimodal Biometric solution (either in a synchronous or an asynchronous format) and even operate with other non-Biometric security systems as well. In fact, Fingerprint Recognition devices can also be installed into a doorknob itself, thus alleviating the need for any electromagnetic lock strike.

4.3 Time And Attendance

Businesses and corporations, at all levels of industry, served, have to keep track of the hours their employees have worked. However, using manual based methods (such as a time card or a spreadsheet) have proven not only to be a gigantic administrative headache, but there are also many security vulnerabilities associated with it as well, such as that of "Buddy Punching."This is where one employee fraudulently reports the time worked for another employee when they did not show up for their required work shift, and he or she still gets paid for it.The use of Biometric Technology can play an integral role in Time and Attendance based applications, by combatting the weaknesses mentioned above. Just about any kind of modality can work in these situations, but it has been Hand Geometry Recognition and Fingerprint Recognition which have been used the most.
Vein Pattern Recognition and even Iris Recognition are starting to gain traction, because of their non-contactless nature. These technologies can once again operate in either a stand-alone or client-server mode, depending upon the specific requirements of the organization. But, it is the latter selection which offers the most advantages.Also, all of the clock in and clock out times of each and every employee is electronically recorded, thus resolving any issues of the actual shift worked. As a result, the security threat posed by "Buddy Punching" is totally eliminated.

4.4 Law Enforcement

Law enforcement agencies across all levels of the Federal Government are also starting to use Biometric Technology to confirm the identity of any suspects or wanted felons. It has been traditionally Fingerprint Recognition which is the most widely used modality. Iris, Facial, and even Vein Pattern Recognition are starting to make their entrance into this market application, but they are being used as a supplement to Fingerprint Recognition.The only way to truly identify the suspect is by taking their fingerprint and running that image through a massive database known as the "Automated Fingerprint Identification System," or also known as "AFIS" for short.

This is a huge database repository that contains all of the fingerprint images of known suspects and criminals not just here in the United States, but worldwide as well. It is currently administered and maintained by the FBI.To upgrade the current AFIS processes, a new database is known as the "Integrated Automated Fingerprint Identification System" (also known as the "IAFIS") has been introduced. It possesses a number of key advantages over AFIS, which are as follows:

- The fingerprint images (as well as other metadata) on some 55 million plus suspects and criminals are now electronically connected to all of the law enforcement agencies in all fifty states and through INTERPOL.
- Results from criminal searches can be sent to the requesting law enforcement agency in less than 24 hours.
- Latent fingerprint images which are collected from a crime scene are also stored into IAFIS databases.
- Highly digitized criminal photographs are available immediately upon request, 24 X 7 X 365.
- The IAFIS databases also support remote connectivity. For example, law enforcement officers in the field can now connect to a specific database via a secured Wi-Fi connection from their handheld Fingerprint Recognition scanner.

4.5 Surveillance

Surveillance is simply keeping tabs of a large group of people, and from there, determining any abnormal behavior from an established baseline. In this instance, it is Facial Recognition which is used the most, and in fact, is the most feared amongst the American public. The primary reason for this is that this modality can be secretly deployed into CCTV cameras, in order to positively identify any known criminals or suspects.

At the present time, there are five current Surveillance techniques which can be used:

- Overt Surveillance:

The public, as well as businesses and corporations, know that they are being watched, whether it is directly disclosed or it is perceived. The primary goal of this type of surveillance is to prevent and discourage unlawful behavior in public settings.

- Covert Surveillance:

Individuals and organizations have no knowledge whatsoever that they are being watched or even being recorded. This is where Facial Recognition is the most widely deployed.

- Tracking individuals on a watch list:

The primary objective is to find an individual whose identity can be confirmed, but their whereabouts are completely unknown. A good example of this are the so-called terror watch lists used at the major international airports worldwide.

- Tracking individuals for suspicious behavior:

The goal here is to question individuals whose behavior tends to be very erratic, abnormal, or totally out of the norm. This is considered to be a macro type of surveillance because the intention is to filter out the undesirable behavior of an unknown individual, or even a group of people.

- Tracking individuals for suspicious types of activities:

With this, the CCTV camera (coupled with Facial Recognition technology) is looking out for suspicious activity either amongst an individual or group of people. In this fashion, the CCTV camera will capture the video of the suspicious behavior, and from there, it will be the Facial Recognition system which can then identify the individual(s) in question.

5.CONCLUSION

Now, as biometric as defense technologies appear poised for broader use, increased concerns about national security and the tracking of individuals as they cross borders have caused passports, visas, and border-crossing records to be linked to biometric data. A focus on fighting insurgencies and terrorism has led to the military deployment of biometric tools to enable recognition of individuals as friend or foe. Commercially, finger-imaging sensors, whose cost and physical size have been reduced, now appear on many laptop personal computers, handheld devices, mobile phones, and other consumer devices.

REFERENCES

1. R. Palaniappan, "Electroencephalogram signals from imagined activities: A novel biometric identifier for a small population", published in E. Corchado et al. (eds): Intelligent Data Engineering and Automated Learning – IDEAL 2006, Lecture Notes in Computer Science, vol. 4224, pp. 604–611, Springer-Verlag, Berlin Heidelberg, 2006. DOI:10.1007/11875581_73]

2. *Jiang, DaYou; Kim, Jongweon; Jiang, DaYou; Kim, Jongweon (26 September 2018).* "Video Searching and Fingerprint Detection by Using the Image Query and PlaceNet-Based Shot Boundary Detection Method". *Applied Sciences. 8 (10): 1735.* doi:10.3390/app8101735.

3. https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html

4. Breckenridge K. (2005). "The Biometric State: The Promise and Peril of Digital Government in the New South Africa". Journal of Southern African Studies, 31:2, 267–82

5. Epstein C. (2007), "Guilty Bodies, Productive Bodies, Destructive Bodies: Crossing the Biometric Borders". International Political Sociology, 1:2, 149–64

6. Pugliese J. (2010), Biometrics: Bodies, Technologies, Biopolitics.New York: Routledge

7. French National Consultative Ethics Committee for Health and Life Sciences (2007), Opinion N° 98, "Biometrics, identifying data and human rights" Archived 23 September 2015 at the Wayback Machine

8. Agamben, G. (2008). "No to bio-political tattooing". Communication and Critical/Cultural Studies, 5(2), 201–202. Reproduced from Le Monde (10 January 2004).

9. Agamben G.(1998), Homo Sacer: Sovereign Power and Bare Life. Trans. Daniel Heller-Roazen. Stanford: Stanford University Press

10. Jump up to:$^{a\ b}$ *Gao, Wei; Ai, Haizhou (2009).* "Face Gender Classification on Consumer Images in a Multiethnic Environment". *Advances in Biometrics. Lecture Notes in Computer Science. 5558. pp. 169–178.* doi:10.1007/978-3-642-01793-3_18. ISBN 978-3-642-01792-6. Archived *from the original on 9 October 2016.*

11. *Walker, Elizabeth (2015).* "Biometric Boom: How the private sector Commodifies Human characteristics". *Fordham Intellectual Property, Media & Entertainment Law Journal. Archived from* the original *on 20 January 2017*. Retrieved 1 May 2017.

12. Minakshee Sarmah; Nibir Kashyap; Dimpee Sonowal; Priety Chakravarty. "Screening of Bioactive compounds and antimicrobial properties from plant extracts of Biscofia javanica". *International Research Journal on Advanced Science Hub*, 2, Special Issue ICARD 2020, 2020, 256-260. doi: 10.47392/irjash.2020.129