International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 09 | Sept -2020 ISSN: 2582-3930

A Survey Paper on Biometrics

Anjali A Prasad[1]
[1]PG Student, Department of MCA, CHMM College for Advanced Studies, Kerala, India

Abstract: ***Now each day the Biometric is becomes the foremost popular technique thanks to its liability. This technique is mainly used for security identification and authentication device. Due to need of high security systems we also are using the biometrics broadly. Another feature of biometric is its efficiency. it's very easy to use and handle. In this paper we discussed about the various characteristic and uses of biometric system.***

1. Introduction

Biometrics are physical or behavioral human characteristics which will be wont to digitally identify an individual to grant access to systems, devices or data. Biometric Systems are automated methods of verifying or recognizing the identity of a living person on the thought of some physiological characteristics, kind of a fingerprint or face pattern, or some aspects of behavior, like handwriting or keystroke patterns. A number of the foremost used biometric characteristics are shown within the picture below. A biometric system supported physiological characteristics is more reliable than one which adopts behavioral features, albeit the latter could also be easier to integrate within certain specific applications.

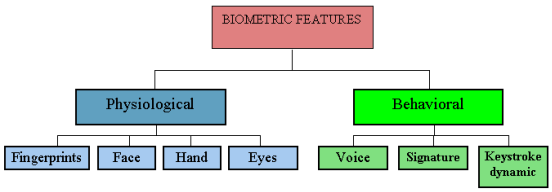

Fig: Classification of biometrics

Using biometric characteristics is that the only thanks to guarantee the presence of the owner when a transaction is formed . especially fingerprint-based systems are proven to be effective in protecting information and resources during a large area of applications. at the present , the quantity of applications employing biometric systems to secure transactions is sort of limited. On one side, some barriers are determined by the shortage of familiarity (and in some cases, of acceptability) of the people, but, probably, the foremost important reasons of the underdevelopment of biometrics within the past were the value of the specified hardware/software and therefore the insufficient performance.

BIOMETRIC SYSTEM

. Biometric Systems are automated methods of verifying or recognizing the identity of a living person.All biometric identifiers can be divided into two

1.Physiological
2.Behavioural

Biometrics is predicted on the measurement of distinctive physiological and behavioural characteristics. Finger-scan, facial-scan, iris-scan, hand-scan, and retina-scan are considered physiological biometrics, supported direct measurements of a neighborhood of the physical body . Voice-scan and signature-scan are considered behaviouralbiometrics; they're supported measurements and data derived from an action and thus indirectly measure characteristics of the physical body . The physiological/behavioural classification may be a useful thanks to view the kinds of biometric technologies, because certain performance- and privacy-related factors often differ between the 2 sorts of biometrics. Behavioural biometrics is predicated partially on physiology, like the form of the vocal cords in voice-scan or the dexterity of hands and fingers in signature-scan. Physiological biometric technologies are similarly informed by user behaviour, like the way during which a user presents a finger or looks at a camera.

FINGERPRINT SCANNING

Today fingerprints consider being one among the oldest and popular among other bio-metric technologies. Fingerprint identification is additionally referred to as dactyloskopy or also hand identification is that the process of comparing two samples of friction ridge skin impression from human fingers, palm or toes.

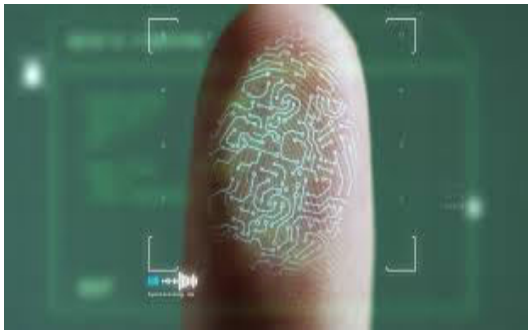

Fig2: Example of finger print scanning

FACE RECOGNITION

During the entire history of humanity, people used face to differentiate one person from the opposite . Facial (face) recognition may be a computer application that automatically identifies or verifies an individual with the assistance of a digital image or a video frame from a video source. one among the ways to try to to this is often to match the given example with the examples within the database.

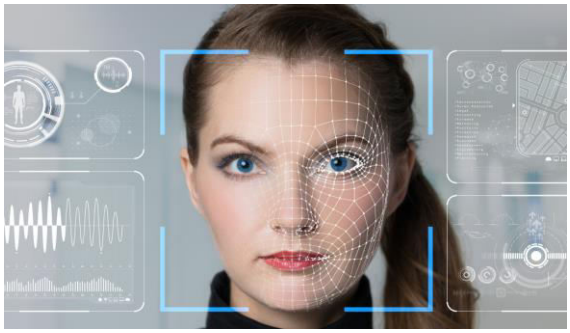

Fig3: Example of face recognition

HAND GEOMETRY

Hand geometry is that the use of geometric shape of the hand for recognition purposes. This method was rather popular 10 years ago but nowadays it's seldom used. The tactic is predicated on the very fact that the form of
the hand of 1 person differs from the form of the hand of another person and doesn't change after certain age. But it's not unique.

Fig4: Example of Hand Scanning

EYES RECOGNITION

The iris may be a thin circular diaphragm, which lies between the cornea and therefore the lens of the human eye. The iris is perforated on the brink of its centre by a circular aperture referred to as the pupil. The function of the iris is to regulate the quantity of sunshine entering through the pupil, and this is often done by the sphincter and therefore the dilator muscles, which adjust the dimensions of the pupil . Iris is that the elastic, pigmented, animal tissue that surrounds the pupil of the attention . Iris biometric is more reliable and accurate as compared to other biometric trait like finger print. Iris texture is stable throughout life and is very secure. Iris is a smaller amount susceptible to attacks. Iris of the attention has different pattern for left and right eye. they're even unique for the identical twins. Iris is employed for various authentication and security applications that include identity cards and passports, prison security, database access and computer login, border control and Government programmes . Iris surface is split into two in cooperative datasets, whereas in non-cooperative major layers: papillary zones and therefore the ciliary zone. Papillary dataset iris region is generally on the brink of the corner of left zone is that the inner part that forms boundary of the pupil. and right eye. to acknowledge the image, iris is split in to An outer ciliary zone is that the remaining a part of the iris, and multiple regions and detection of single region can these are separated by the collarets – shows a pattern recognize an individual . Color information is another important flower or zigzag . to not be confused with another, less prevalent, ocular-based technology, retina scanning and iris recognition uses camera technology with subtle infrared illumination to accumulate images of the detail-rich, intricate structures of the iris. Digital templates encoded from these patterns by mathematical and statistical algorithms allow the identification of a private or someone pretending to be that individual. Databases of enrolled templates are searched by matcher engines at speeds measured within the many templates per second per (single core) CPU, and with

infinitesimally small False Match rates . Iris Normalization may be a Process in image processing that changes the range of pixel intensity values. Applications include photographs with poor contrast thanks to glare, for instance . Normalization is usually called contrast stretching. in additional generalfields ofknowledge processing, like dig ital signal processing, it's mentioned as dynamic range expansion .The purpose of dynamic range expansion within the various applications is typically to bring the image, or other sort of signal, into a variety that's more familiar or normal to the senses, hence the term normalization. Often, the motivation is to realize consistency in dynamic range for a group of knowledge , signals, or images to avoid mental distraction or fatigue.

Fig 5: Example for Iris Recognition

VOICE RECOGNITION

Voice, like many other characteristics that are used for biometric methods, is unique. Like sort of gait, it takes quite little time to research the voice and to spot the person. Voice in biometrics or “voice print” is presented as a numerical model of the sound.

Fig 6: Example of Voice Recognition

KEY STROKE

The keystroke is the behave of the human mean to say that the different humans have the different techniques of pressing keys on such basis the identification takes place.

Fig 7: Example for keystroke

SIGNATURE SCANNING

Another behavioral biometric is signature by which the data can be extract by the signature of that particular person.

Fig 8:Example for Signature Scanning

APPLICATION

There are various application for the use of biometric technology.The most commonly used are

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

Logical Access Control

This market application refers to gaining access to a network either at the place of the business or corporation or via a secured remote connection from a foreign location.The security tool that's most ordinarily the normal username and password. Although this mix may have worked effectively within the past, it's now definitely showing signs of severe weaknesses, by being a primary target for Cyberattacks. Usernames and passwords are often very easily compromised and hijacked via a Denial of Service or a dictionary style attack. Because of the frequency of those sorts

of attacks, many organizations are now requiring their employees to make long andsophisticated passwords. they need to contain a mixture of upper and small letter letters, punctuation marks, spaces, numerals, and other sorts of special characters. Because these are so difficult to recollect , employees are actually writing their newly created passwords on Post-It Notes and attaching it to their workstation monitor. This phenomenon has become referred to as the "Post It Syndrome."To combat this and therefore the other security weaknesses posed by using passwords, the utilization of Biometric Technology has been called upon to exchange it in its total entirety.

PHYSICAL ACCESS CONTEOL

Physical Access Entry refers to giving an employee of a business or a company access to a secure building, or perhaps a secure office from within it. Traditionally, keys and badges are used. However, the most problem is that these tools is very easily stolen, lost, replicated, or perhaps given to other employees who don't belong in those secure areas.

Smart Cards are accustomed help alleviate these security weaknesses, but they too have their own set of limitations additionally. Fingerprint Recognition and Hand Geometry Recognition are utilized in this application the foremost, together with Vein Pattern Recognition. In these instances, one amongst these Biometrics is tough wired to an electromagnetic lock strike.

Once the identity of a personal has been confirmed by either their fingerprint or through the form of their hand, the lock strike will, within seconds, open the door to the secure area. the first advantages of using Biometrics are as follows:

No more lost, stolen, or fraudulent use of keys and ID badges;
Only legitimate employees whose identity has been 100% confirmed will gain access to any secure areas that he or she needs entry to.
In Physical Access Entry scenarios, the Fingerprint Recognition device or the Hand Geometry scanner can either operate either during a standalone or a client-server mode. the benefits of the latter are as follows:

Greater Biometric Template storage capacity;
Larger applications (such as physical access to multiple buildings and multiple doors) may be far better served;
All of the Biometric information and data is stored on a central server for the efficient processing of the Verification and/or Identification transactions;
The Biometric modalities which are wired to every and each door in a company may 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 may work together to form a Multimodal Biometric solution and even operate with other non-Biometric security systems in addition. In fact, Fingerprint Recognition devices may be installed into a doorknob itself, thus alleviating the requirement for any electromagnetic lock strike.

TIME AND ATTENDENCE

Businesses and corporations, in the least levels of industry, served, need 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 big administrative headache, but there also are many security vulnerabilities related to it also , like that of "Buddy Punching."

This is where one employee fraudulently reports the time worked for an additional employee once they didn't show up for his or her required shift , and he or she still gets purchased it.

The use of Biometric Technology can play an integral role in Time and Attendance based applications, by combatting the weaknesses mentioned above. almost any quite modality can add these situations, but it's been Hand Geometry Recognition and Fingerprint Recognition which are used the foremost .

Vein Pattern Recognition and even Iris Recognition are beginning to gain traction, due to their non-contactless nature. These technologies can once more operate in either a stand-alone or client-server mode, depending upon the precise requirements of the organization. But, it's the latter selection which offers the foremost advantages.

For example, there's centralized control and administrative functionality from within one location (namely the server), and every one of the executive tasks related to processing payroll are often fully automated.

Also, all of the punch in and punch out times of every and each employee is electronically recorded, thus resolving any problems with the particular shift worked. As a result, the safety threat posed by "Buddy Punching" is completely eliminated.

LAW ENFORCEMENT

Law enforcement agencies across all levels of the federal also are beginning to use Biometric Technology to verify the identity of any suspects or wanted felons. it's been traditionally Fingerprint Recognition which is that the most generally used modality. Iris, Facial, and even Vein Pattern Recognition are beginning to make their entrance into this market application, but they're getting used as a supplement to Fingerprint Recognition.

The only thanks to truly identify the suspect is by taking their fingerprint and running that image through a huge database referred to as the "Automated Fingerprint Identification System," or also referred to as "AFIS" for brief .

This is an enormous database repository that contains all of the fingerprint images of known suspects and criminals not just here within the us , but worldwide also . it's currently administered and maintained by the FBI.

To upgrade the present AFIS processes, a replacement database is understood because the "Integrated Automated Fingerprint Identification System" (also referred to as the "IAFIS") has been introduced. It possesses variety 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 or any of
the enforcement agencies altogether fifty states and thru INTERPOL.
Results from criminal searches are often sent to the requesting enforcement agency in but 24 hours.

Latent fingerprint images which are collected from a criminal offense scene also are 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
instance , enforcement officers within the field can now hook up with a selected database via a secured Wi-Fi connection from their handheld Fingerprint Recognition scanner.

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:

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

CONCLUSIONS

As these applications continue to grow regarding using Biometric technology, there will be one theme that will be prevalent. That is the movement towards using the non-contactless modalities. As it has been stated in this and previous articles, one of the key drivers for this trend is that of hygiene related issues.

Although there is no scientific proof of an end user actually contracting a serious illness, this fear is expected to persist well into the future.

As a result, it is forecasted that Vein Pattern Recognition and Facial Recognition will become the dominant technologies for the applications reviewed.

However, the latter will primarily serve the Surveillance based applications, and the former will be involved with all of the others, because of its versatility and low cost of deployment.

In the end, there are three levels of access control which must be met in order to fortify any type of application truly. These are as follows:

1. What a person has (such as an ID Badge or a related Smart Card);
2. What a person knows (such as a PIN Number or a password);
3. What a person is (their unique physiological or behavioral traits).

REFERENCE

[1]. Anil K. Jain, Arun Ross, and Sharath Pankanti, "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp 21-38, June 2005.
[2]. Anil. K.Jain, Arun Ross, Salil Prabhakar, "An introduction to biometric recognition", IEEE Transactions on circuits and systems for video technology, vol. 14, no. 1,pp 67-80, Jan 2004.
[3].http://www.weexcel.in/NewsDesc1.aspx?cod=86.
[4].http://www.theseus.fi/bitstream/handle/10024/44684/Babich_Ale ksandra.pdf?sequence=1.
[5]. Essam-Eldean F. Elfakhrany, Ben Bella S. Tawfik, "IRIS Recognition using Conventional Approach" IEEE 9th International Colloquium on Signal Processing and its Applications, 8 - 10 Mac,2013.
[6]. Geetika, Manavjeet Kaur " Fuzzy Vault with Iris and Retina: A Review" International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 4, April 2013.
[7]. Asima Akber Abbasi, M.N.A. Khan and Sajid Ali Khan "A Critical Survey of Iris Based Recognition Systems" Middle-East Journal of Scientific Research 15 (5): 663-668, 2013.
[8].http://www.griaulebiometrics.com/en-us/book/understanding biometrics/introduction/history
[9].http://www.nationalbiometric.org/about_history.php
[10]https://users.ece.cmu.edu/~jzhu/class/18200/F06/L10A_Savvides_Biometrics.pdf
[11]http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf
[12]https://fas.org/irp/congress/2013_hr/biometric.pdf
[13]http://www.planetbiometrics.com/creo_files/upload/article-files/btamvol1update.pdf
[14]http://www.planetbiometrics.com/creo_files/upload/article-files/Overview_of_biometric_apps.pdf
[15]http://www.cedar.buffalo.edu/~govind/CSE717/papers/IntroductionToBiometricRecognition.pdf
[16]https://www.google.com/#q=biometric+application+pdfs&start=10
[17]http://www.fns.usda.gov/sites/default/files/biomvend.pdf