International Journal of Research in Advent Technology, Special Issue, March 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Biometrics Methodologies for Security Systems

S.KOWSALYA[1]
Assistant Professor,
Department of Computer Science and Application
Sri Krishna Arts and Science College, Coimbatore-641008.
kowsalya.selvaraj@gmail.com

PRADEEP KUMAR.B [2]**, AMARNATH.J** [3]**, LIBIN.M** [4]
**Student 2nd year B.Sc,*
Department of Computer Science and Application
Sri Krishna Arts and Science College, Coimbatore-641008.

Abstract - The recent days of invention has produced one of many scientific discoveries and technological advancements in day today life. There has been many technologies being invented perhaps there raise the issue of privacy & security as well. As the computing systems extends its boundary and became more complicated, there was an increasing need for privacy & security. In this paper, I have taken the concept of Biometrics which gives security to various ways. There are two security methodologies that I have focused in my paper viz token-based security and secret based security. These methodologies identify and behave based on the psychological and behavioral characteristics of the end user. There are many security mechanisms followed in protecting the secure passwords, In this paper, I have portrayed some of those techniques. Many verification methods has been tried using various techniques. Two major such verification methods are namely psychological verification and behavioral verification. The above said methods have sub methods bounded or inherited from them that hold their advantages and disadvantages.

Keywords— Bertillonage, Dilation, Vascular patterns**.**

1. INTRODUCTION

Biometrics includes strategies for unambiguously recognizing humans based mostly upon one or a lot of intrinsic physical or activity traits. In the technology world of science, biometrics is employed as a style of identity access management and security control. It helps to determine people in teams that are within the monitoring scale. In most up to date life science applications, the term "life measurement" adapts a rather totally different role. In the engineering sector, it refers to a specific category of identification technologies. These technologies use a person's distinctive biological traits to work out one's identity. The traits that are thought of embrace fingerprints, tissue layer and iris patterns, facial characteristics and lots of a lot of.

It is potential to grasp if a person’s characteristic may be used for biometric in terms of the subsequent parameters.

- Universality – every individual shall have the characteristic.
- Uniqueness - is however well the biometric separates a person from another.
- Permanence - measures however well a biometric resists aging and different variance over time.
- Collectability - simple acquisition for mensuration.
- Performance - accuracy, speed, and strength of technology used.
- Acceptability - Position or compatibility of approval of a technology.
- Circumvention - simple use of a substitute.

A biometric system will operate within the following 2 modes

A. Verification

This is a method that does one to one comparison of a biometric that is being captured as input with an in-built templet to verify that the captured individual stands unique. This process shall be carried out using a scanning card or pre-loaded image or a printed image.

B. Identification

This is a one to many comparisons of the biometric that is being captured as input against an in-built biometric available in the database and identify an unknown individual. This type of identification can only be succeeds provided the comparison of the input biometric captured to an in-built template in the database falls within a previously set threshold.

2. PERFORMANCE

The following are used as metrics to determine the performance for biometric system:

A. False Accept Rate or False Match Rate (FAR or FMR).

This is a method of determining the probability that how far the system incorrectly get match with the input pattern to a not or non-matching template available in the database. Result of this method measures the percentage of invalid/false inputs that are incorrectly accepted.

B. False reject rate or false non-match rate (FRR or FNMR)

This is a method of determining the probability that how far the system fails to get or detect a correct match between the given input pattern and a predefined matching template available in the database. The result of this method measures the percentage of valid or correct inputs that are incorrectly rejected.

C. Receiver operating characteristic or relative operating characteristic (ROC)

The ROC plot is measured or referring to as visual characterization of the lay-off between the FAR and the FRR. Perhaps, the matching algorithm works as a decision based on a threshold that determines how close to a template the given input data needs to be framed for it to be considered a successful match. In case the threshold is reduced, then possibilities are there the results will be less false or non-matches but more false accepts. Respectively, a higher threshold will reduce the FAR eventually the same increase the FRR. A common variation is the Detection error trade-off (DET), this is obtained using a normal or standard deviation scales on both axis. This behaves in more linear graph that illuminates the differences for higher performances (rarer errors).

D. Equal error rate or crossover error rate (EER or CER)

This is a method that determines the rates at which both accept and reject errors are equal. The resulting value of the EER can be easily derived from the ROC curve. The EER is an easy way and less time consuming approach to compare the accuracy and correctness of the devices with various ROC curves. Eventually in common acceptance, the device with the lowest EER is considered to be most accurate.

E. Failure to enroll rate (FTE or FER)

This is the method that rate at which the system attempts to create a pre-defined template from a given or scanned input is unsuccessful. This kind of results is most commonly caused due to the low quality inputs.

F. Failure to capture rate (FTC)

This is a method that takes place within automatic systems, determining the probability for a system that fails to detect a biometric input when presented correctly.

G. Template capacity

This is a method that determines the maximum number of set of data that shall be stored in the system.

3. BIOMETRICS CLASSIFICATIONS

A. *Physical Biometrics:*

- Bertillonage – This classifies the measuring of an individual’s body length.
- Fingerprint – This classifies the method of analyzing an individual’s fingertip patterns.
- Facial Recognition – This classifies the method for measuring an individual’s facial characteristics
- Hand Geometry – This classifies the method of measuring an individual’s hand, palm shape.
- Retinal Scan – This classifies the method of analyzing an individual’s blood vessels from eyes.
- Vascular Patterns – This classifies the method of analyzing an individual’s vein patterns.
- DNA – This classifies the method of analyzing individual’s genetic makeup.

B. *Behavioral Biometrics Solutions:*

- Speaker Recognition – This classifies the method of analyzing individual’s vocal /voice behavior.
- Signature – This classifies the method of analyzing each individual’s signature dynamics.
- Keystroke – This classifies the method of measuring the individual’s time spacing of typed words.

4. BERTILLONAGE BIOMETRICS

Bertillonage biometrics is a nineteenth century method of distinguishing people by the utilization of multiple bodily measurements. Bertillonage biometrics is now no longer being used in practical routine life.

A. *The Process*

The process kicks off by making an individual person to undergo a measurement for duration of twenty to sixty minute time duration as examination hours. There will be various body measurements taken during this exam. These measurements will include the data related to height, length, and breadth of the head, the measuring length of different fingers, the length of individual’s forearms, etc.

The results obtained from this examination are then recorded and/or compared to a predefined template in the database. Even though all these were done manually by hand, the process of record filing and verification steps was bit fast during that time. (Since this was happened in nineteenth century!)

B. *Evaluation Results for Bertillonage biometrics*

This process was predicted and assessed as accurate at the ranging of 278,429,569 to 1 allowing for possible (this was eventually proven at that time) duplications, human manual error in measuring conceded to a smaller od a considerable effective accuracy. Non-unique measurements that are allowed for more than one people holds the same results, this eventually reduce the usefulness of this method. In addition, the time consumed to measure a subject was prohibitive for usage other than prison records.

5. BIOMETRICS FINGERPRINT

Before getting into this method or the technology, let me emphasize about "fingerprinting" the meaning and understanding. Fingerprinting as common term means to take an image of an individual person's fingertips and then to store or records its characteristics. The arches, loops and whorls are those make these characteristics of a fingertip. These are usually recorded along with the patterns of furrows, minutiae and ridges.

A. *The Process*

The procedure kicks off by making an individual to places his/her fingers of a palm against a small biometrics fingerprint reader (or the same shall be termed as biometrics fingerprint scanner device) surface (usually the surface is coated with optical or silicon) of about two inch square size. This biometrics fingerprint reader will be attached to a system and that takes the information from the scan device and passes to the database. The transferred scan images are then compared to the information stored within the database. The individual is obviously required to take off his finger from the reader after five seconds during which time the identification or verification process takes place.

In order to prevent fake access and invalid use of fingers, many biometric fingerprint systems are designed to measure the blood flow and will check for the correctness in the arrayed ridges at the edge of the fingers.

B. *Evaluation*

In the present world of digital era, the software that is designed to map the minutiae points in a relative placements on the individual's fingertip and then the same will also search for the similar minutiae information that are stored in the database.

Most often an algorithm that is used for a biometrics fingerprint systems. These algorithms will do encode the read or scanned information into a character string that shall be searched in the database; this is to improving the search time.

This method was often meant to improve the public's fear and hesitation of their biometrics fingerprint data being recorded are stolen and misused, but most of the people still do not understand and also less belief over the actual method use.

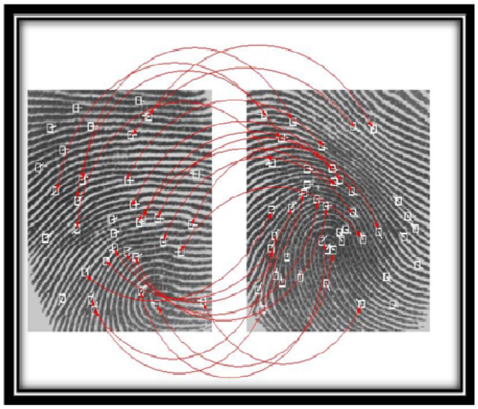

Fig 1. Finger print Evaluation

6. BIOMETRIC FACIAL RECOGNITION

Biometric Facial recognition performs analyzing the characteristics of an individual's face images captured using a digital video camera. It records the complete structure of facial, including the distance measure between eyes, nose, mouth, and jaw edges. These measurements are then stored in a database which will be then used for comparison process when an individual stands in front of the camera.

Biometric facial recognition system has been widely, flaunted as a fantastic and effective system for recognizing potential threats (to determine and identify the terrorists, scam artists, or known criminals) but until now, this has been unproven in high-level applicability. It is currently used in verification only systems with a moderate deal of success.

A. *The Process*

This process kicks off by making the user face the camera, standing about 2 feet away from it. The system will then locate the user's face and do perform a match against the claimed identity with the facial database that was already captured and stored. Possibilities are there for an individual need to move and adjust him to reattempt the verification based on his facial scan position. In this process, the system usually gets a decision in less than 5 seconds.

In order to prevent a fake face and mold from faking out the system, many systems are now require the user to smile, blink, or move in a way to determine that the object standing in front of the scanning is human before verifying.

B. *Skin texture analysis:*

There is an emerging trend in using the visual details of the skin as captured in standard digital or scanned images. This technique very often called as a skin texture analysis, this process turns the unique lines, patterns, and spots apparent in an individual's skin into a mathematical space. Test results have already shown that with the addition of skin texture analysis, result performance in recognizing the faces shall increase 25 to 30 percentage.

1.
2.

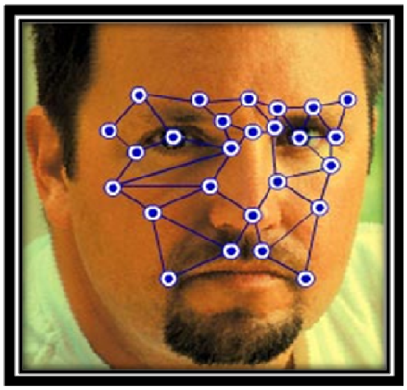

Fig 2. Skin texture analysis

C. *Comparative Study*

So far we have seen the different biometric techniques from them the facial recognition method may not be look as the most reliable and efficient. However, one key advantage in the same method is that it does not require assistance (or consent terming) from the test subject. Well profiled and designed systems that were involved in good quality process are installed in airports, multiplexes, and some other crowded public places can perfectly identify the individuals among the n number of people. On the other hand, the other biometrics like fingerprints, iris scans, and speech recognition finds difficult in performing the same kind of mass identification.

Perhaps, questions have been already raised over the effectiveness and reliability of facial recognition software system in view of railway and airport security kind of places.

D. *Criticisms*

Face recognition system is not as perfect as it struggles to perform in certain conditions. There have been instances that this system getting pretty good and functioning at full complete frontal faces and 25 degrees off, eventually as soon as you go towards profile, there've been problems that remains unaddressed.

Similar conditions or areas where face recognition does not function well also includes poor environment with lighting, using of sunglasses, detecting with long hair, or other objects that are partially covering the actual subject or the individual's face, and low resolution images reading cameras.

Most serious disadvantage in this system is that many are less effective in case of facial expressions being varied. Even a big smile can render in the system that results less effective.

7. BIOMETRIC HAND SCANNING

This method of Hand scanning involves the process of measuring and analysis of the shape of individual's hand. It is obviously a straight forward case of working procedure and is more interestingly is accurate. Even though it requires additional special hardware utilities to use and implement, it can also be easily integrated into other third party devices or systems.

We have to agree that unlike fingerprints, the individual's human hand is not unique. Also the Individual hand features are not collectively descriptive enough for determining the identification. However there are possibilities to devise a method by combining different individual features and measurements of fingers and hands for verification purposes.

A. *The Process*

The process in this method kicks off by making the individual to place his or her palm on a metal surface containing guidance pegs on it. Individual's hand is then properly adjusted and aligned by the pegs so that the device able to read the hand attributes as input data for comparison. The device then checks its database for verification of the input scanned image. This kind of process usually takes less than ten seconds.

Fig 3. Hand Scanning

B. *Evaluation*

This is a very easy evaluation process for users to work on the system as simple as placing an individual's hand on the device. There exist no public attitude problems as it is associated most commonly with evaluated authorized access only. The volume of data required to distinctly identify a user in this system is the smallest by far, this allow to use with Smartcards more efficiently and easily. It is also a quite resistant approach to attempt in fooling the system. The amount of time and energy required to sufficiently emulate an individual's hand is generally too much worth the effort, specifically since it is commonly used for verification purposes only.

C. *Criticism*

There still exists some limitations to biometric hand readers; the most prominent is its proprietary hardware cost and the size. In addition, if there exists injuries to hands then it may cause difficulty in using the reader effectively, In general, the is a lack of accuracy that results verification process failure one.

8. RETINAL BIOMETRICS

Retinal biometrics is methods that do scans the retina and analyze the layers of blood vessels at behind eye ball. The blood vessels located behind the eye balls do have a unique pattern. This differs between eyes and between individual people. Basically this Retinal scanning method involves use of low-intensity light source with an optical coupler that can read the patterns from the vessels at a great level of accuracy. Hence it does require and mandate the user to remove spectacles and place their eyes close to the device in the provided lid, and focus of the vision to be on a certain point. Perhaps there still remains an unanswered area that the accuracy of this method can outweigh the public discomfort or not.

A. *The Process*

The process followed in this method is the user requested to place their face as close to the device and look into a small opening in the retinal biometrics device. The focus or the vision of the sight must be at a small green light. Users shall keep their head steady and eye sight focused on the light for few seconds. During this course of time the device will verify the user's identity. This process normally takes about 10 to 15 seconds depending on the performance of the system configuration.

So far, there has been no way in getting a fakeness to replicate a human retina, also the retina from a dead person would deteriorate rapidly to be useful. Hence no extra precautions needed with retinal scans to ensure the user is a living human being.

B. *Evaluation*

To be contradictory with the most of popular public misconceptions, the method of retina scan was used almost exclusively across high-end security applications. It is often used for the purpose of controlling access to certain areas or privacy rooms in army installations, nuclear power plants, and those like that are considered to be a high risk security areas.

Fig 4. Retinal Biometrics

C. *Criticism*

The main critic that was faced in this method is the cost. The cost of the proprietary hardware used in this method as well as the inability to get in easily with new technology for the accessing people make or project retinal scan devices not good or a bad fit for most situations. In addition, there also exists the stigma of consumer's thinking that it is potentially harmful or damage the eye.

9. VASCULAR PATTERNS BIOMETRICS

Vascular pattern biometrics technology or the method that involves the concept of measuring the characteristics that are related to the veins in a individual's hand or their face. The subject in this method here is the thickness and location of the veins. It is strongly believed that the veins with its thickness are to be unique enough to identify an individual's identity.

A. *The Process*

The process of this method kicks off from hand-based, that require individual to place their hand on a curved reader that will take an infrared scan. The result of this scan will create a picture that can be compared to a predefined and stored one in database to verify the identity.

Fig 5. Vascular Patterns Biometrics

B. *Evaluation*

As evaluation goes deep, the vascular patterns biometrics technology is still be considered as new and there are very few awareness among public. Also there are very less published details about it, indicating its use. Even though it is very minimally used at the moment, vascular patterns scanners shall also be found in testing at major army installations and scanner rooms and is being evaluated by some well established companies in the security market and multi-outlet retailers. At present this method is still building acceptance.

C. *Criticism*

The main criticism in this method is the human age that effects directly in implementing. This also expects to have impact for those with heart attacks; other medical problems in an individual's arteries on the scans have yet to be determined completely. This method also requires a large volume of space in order to mount the device so as to scan the entire hand which might restrict its usability.

10. APPLICATIONS OF BIOMETRICS

-
- Biometric Time Watches or Biometric time based attendance devices that are being increasingly utilized in various companies to control their employees.
- Biometric access control devices, that provides strong security controls at entrances of the premises.
- Identifying the DNA for a person to match the patterns in order to get prove themselves in law & criminal cases.
- Biometrics security devices were implemented in some of the world's famous airports to enhance the security standards.

11. CONCLUSION

As a whole the Biometrics has fast emerged promising technology for authentication and has already found place in most hi-tech security areas. It has always been a forerunner in the security and the access control arenas too. It is this specific aspect of the technology that this generation likes to focus on.

REFERENCES

[1]Michael J.A. Berry, Gordan Linoff, "Biometric Techniques for Marketing and Customer Relations", Special Edition.

[2] Phipps Arabae Lawrence, J.Herbret, "Clustering and Classification", 2005.

[3] Ralph Kimball, "The Biometrics Toolkit", a complete guide to dimensional modeling.

[4] Claudia Nicholas, G.Geiger, "Mastering Data Warehouse Design", John wisely 2003 Edition.

[5] www.reportmining.com/dataextraction/conv

[6]www.datawatch.com/_solutions/data_analysis/whitepapers.php

[7] www.thearling.com/text/datawhite/d_text.php

[8]www.xclustering.com/dt_extraction/report_analysis/dem.odt

[9] Developersfusion.ac.uk/beginners.org