International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 06, 2020
ISSN: 1475-7192

Fact-finding and Upheaval in the field of Biometrics

[1]Abhishek Parashar, [2]Arshad Ali

ABSTRACT-- *There are many different types of techniques used for recording, saving and analyzing data for biometrics. Most of the techniques (Mobile Biometric Technology, Multimodal Biometric Authentication system, Cloud Based Biometric Solutions etc.) are used by the defense organizations such as police, army, banks etc. and as result the software's and the techniques are not feasible for the private security organizations and local defense organizations. This paper deals with the innovation of a new and advanced software and hardware which can bring valuable changes in this field. The software will be basically for combination of data (fingerprint and eye retina) and will pick out the respective individual's data who's fingerprint or eye retina was given as input. and hardware will be for the advanced security of our system (PC, laptops, mobile phones etc.), high security rooms etc. by making the hardware compatible with the basic needs of today's world's concern regarding security which can be monitored and saved with fast functioning and more secure hardware. The hardware will be developed by keeping the security and privacy at highest level. The fingerprint sensor will be equipped with a mechanism to detect human heat and eye retina sensor will be compatible of capturing eye retina from a long distance and save the data as well on the same time.*

Keywords-- *Scanner, Sensor, Thermal imaging*

I. INTRODUCTION

History of biometrics

The first record of a biometric identification system was in 1800s, Paris, France. Alphonse Bertillon developed a method of specific body measurements for the classification and comparison of criminals. While this system was far from perfect, it got the ball rolling on using unique biological characteristics to authenticate identity [I]. Fingerprinting followed suite in the 1880s, not only as a means of identifying criminals but also as a form of signature on contracts. It was recognized that a fingerprint was symbolic of a person's identity and one could be held accountable by it. Through there are debates on who exactly instigated fingerprinting for identification, Edward Henry is denoted for the development of a fingerprinting standard called the Henry Classification System

This was the first system for identification based on the unique architectures of fingerprints. The system was quickly adopted by law enforcement replacing Bertillon's methods becoming the standard for criminal identification. This commenced the century's worth of research on what other unique physiological characteristics could be used for identification.

After this the field of biometrics did not looked back and there was a sudden boom in this field. Though in the year 1960 semi-automated facial recognition methods were developed requiring administrators to analyse

[1] *UG Scholar, Poornima Institute of Engineering and Technology*

[2] *Assistant Professor, Poornima Institute of Engineering and Technology*

Received: 27 Feb 2019 | Revised: 20 Mar 2019 | Accepted: 30 Apr 2020

facial features within an image and extract usable feature points. This was not secure hence constant upgradations were made from then which the result came in the year 1869 which gave a more secure system but still there were some things lacking. In the same year FBI put funding towards developing automated processes. This was a catalyst for the development of more sophisticated sensors for biometric capture data extraction and analyzing data [II]. Many private as well as government organisations stated work on this but the result came in the year1985 the concept of fingerprint, irises, retina were unique to everyone was proposed and by 1994, the first iris recognition algorithm got patented. It was discovered that blood vessels patterns in eyes i.e. eye retina were unique to everyone and can also be used for authentication and identification as well. Soon after this in year 2000 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.

Since after that there is a lot of improvement in this field. Biometrics were used for different purposes by different organisations like private organisations (such as private collages private, limited companies etc) taking attendance, for safety measures etc. and government organisations uses biometrics for making database (example; Aadhaar card database, criminal record).

In 2013, Apple included fingerprint to unlock the iPhone, beginning the wide acceptance of biometric as a means of authentication. Nowadays, most mobile phones have biometric capabilities and that same technology is used by many other famous companies in their personal devices such as mobile phones, laptops etc. therefore this technology is on the boom but still there is always a chance for improvement [II].

II. Literature review

Techniques which are being used in today's world are as follows;

1. Mobile Biometric Technology; It used by both government and private organizations for the process of human identification by biometrics (fingerprint or eye retina)

2. Multimodal Biometric Authentication system; This trend in biometrics is the use of multiple biometric authentication systems for the process of human identification. This system takes input from a single or multiple biometric device for the measurement of two or more different biometric characteristics to ensure the authentication of accuracy.

3. Cloud Based Biometric Solutions; This trend is mainly herd by mobile biometric technology. When you are thinking mobile biometric technology, pairing that PC, laptop or mobile biometric device with a cloud based biometric solution can speed up the identication process even more. Sending the biometric data to cloud is a safer solution than saving the biometric data locally on our device.

4. Vertical Specialized Biometric Solutions; Having a vertical specialized biometric solution for identity management is becoming a popular choice of interest for many industries. These kinds of solutions are designed to meet the unique demand of their respective industries made by them. They are also customized by keeping in mind about the laws made by local and international industrial and standards. When seeking biometric identication management solutions, businesses are very conscious about their unique requirements and are opting

to deploy a customized solution designed specially, for their verticals. These solutions not only provide higher efficiency and control, at times they provide a cutthroat advantage over associates who are still adopting them.

5. Biometric Single Sign on (SSO); Perhaps one of the most popular debates at this point is whether biometrics will replace passwords. The debate came into notice due to the fact that many companies are adopting biometric single sign on (SSO) over traditional passwords to secure their networks from data breaches, data lose and to minimize password management costs. Let's face it, passwords are weak! They not strong because of many reasons: they can be guessed, forgotten, shared or exchanged. Contrarily, biometrics are unique, hard to spoof, and you cannot lose or share them for any kind of misuse.[III]

III. Our Idea

The main idea is to build a software which works with the help of a database. The database comprises of the fingerprint and eye retina stored in a data packet with a unique identification code of for data of every individual. On giving the input as fingerprint, eye retina or both (fingerprint and eye retina) the output displayed will be the name and other details of the person whose biometric data was given as input.

Addition to this a new innovation in the hardware for the biometric security for the finished products for the high-level security devices and high-level security places. The idea of the hardware is, firstly the fingerprint sensor which will not only detect the biometric i.e. fingerprint but the sensor will also detect the human heat for the concept of thermal imaging (thermography) will be used. Secondly, the eye retina sensor which are being used today are inefficient to scan eye retina from long distance and also takes very long. Our idea is to build an eye retina scanner which is capable of scanning the eye retina from a long distance in a very less time. Not only this it would also be capable of saving the scanned data at same time

IV. Issues in Current Technique

- The software being used today are slow and not so accurate. The technique of data packet storage is not secure, fast and reliable.
- The fingerprint sensors are slow in working and they are physically hackable i.e. they also scan the duplicate of fingerprint (plastic model of anyone being used by anyone else).
- Eye retina scanner are slow to scan the fingerprint and also have the limitation of distance (15-20 centimeters).

V. Methodology

Methodology used for this innovation will be comprising of the two parts (software and hardware) as follows;

5.1. Software

Basically, data base will be made of 30 to 50 individuals for the test run and abig data base such as the data base of Aadhar card data base or data base of criminals etc. after the successful trial period of the test run.

Received: 27 Feb 2019 | Revised: 20 Mar 2019 | Accepted: 30 Apr 2020

The data base will be made with the help of ORACLE which is a multi-model database management system. The non-biometric data will be manually stored and the biometric data will automatically be stored by the Oracle Biometric Manager which is NT based for PC

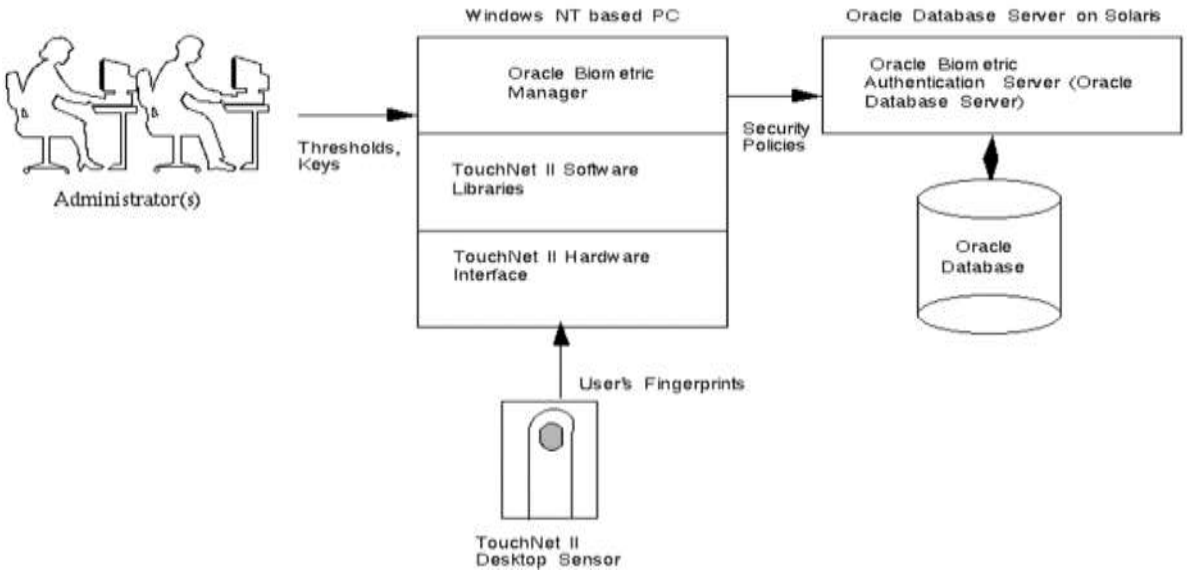
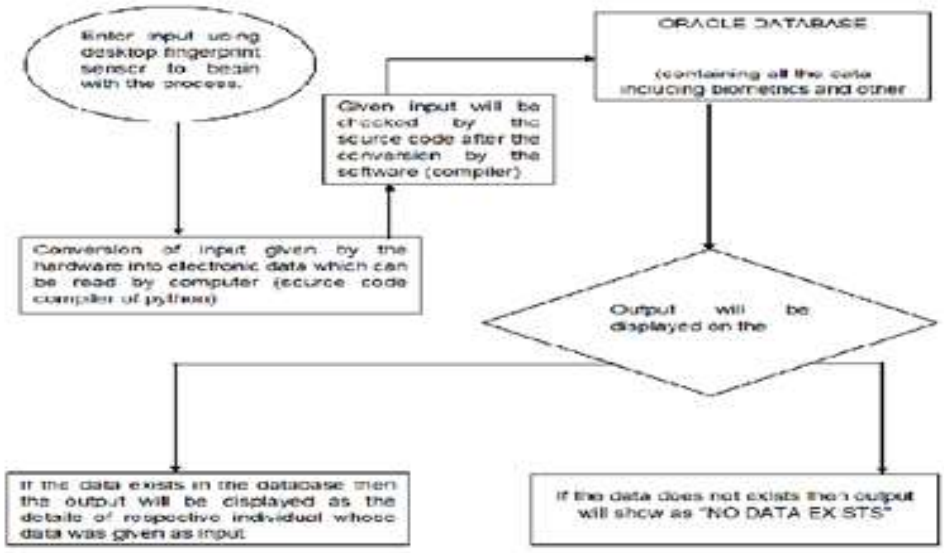


Figure1: How biometric data will be stored and processed by ORACLE Database Manager [IV]

Now, When the data base is ready the programs will be made to perform the task according to the needs of our software. The program will be made with the help of PYTHON which is a high-level programming language. The program will perform the task to take the input given by the user and will pick out the data whose data was given as input. It will also be capable of taking inputs of two or more different peoples and pick out both the individuals for e.g. input is given as fingerprint of person 'A' and eye retina of person 'B' then the output will be the details of 'A' and 'B' both separately.



5.2. Hardware

In today's world of growing technology, it is important to prevent our important data and confidential places like your office etc. safe therefore, to prevent this and make our system and places we can use our biometrics with which we can have the assurance of our system and places to be fully secure.

5.2.1. Fingerprint Sensor

Before the Methodology of fingerprint sensor, we have to understand the concept of thermal imaging [V]. It is a technique to detect heat given off by an object and capturing it. The heat given by a human body is captured or read by a different color in this technique. Now, let's relate thermal imaging with fingerprint sensor. The idea is to build a fingerprint which detects human heat where the concept of thermal imaging would come in play, same way as it is used to capture human heat and display it to the user on the screen of thermal imaging camera system here, also the same task will be performed. The system has to change in such a way where the imaging detected by the thermal imaging system and then the program to read the fingerprint will execute. If under any circumstance human heat is not detected the sensor would not work at all and look as a dead system.

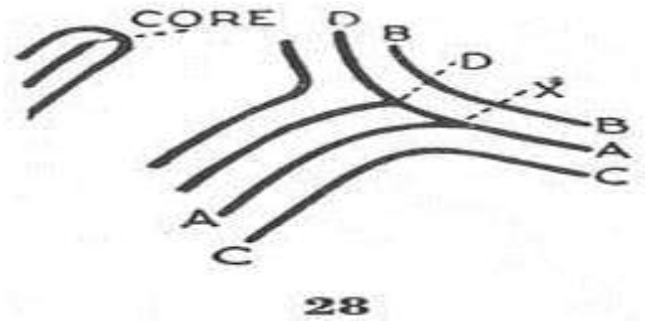


Figure 3; Study of fingerprints [VI]

Figure 4; main components to scan a fingerprint [VII]

5.2.2 Eye Retina Scanner

In the today's world where a new device or a new technology comes every next day and in such a world the technology used for eye retina is very old and not up-to-date for the today's fast world. A retinal scan is a biometric technique that uses unique patterns on a person's retina blood vessels.

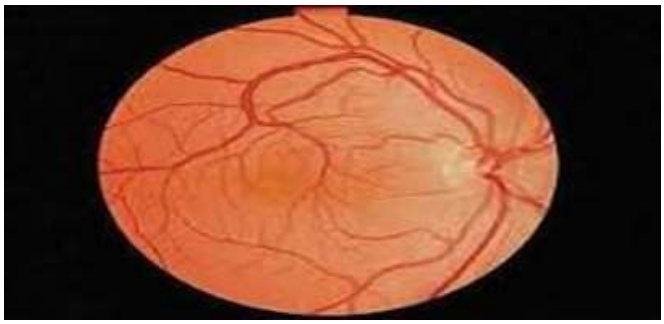


Figure 5; Eye retina of a human eye (VIII)

The scanner to be built would be capable of capturing eye retina from a long distance and also store the data at the desired database manger (ORACLE). It will also be compatible to capture the eye retina of more than one person at any instance of time and simultaneously store that data.

VI. Benefits and Applications

6.1. Benefits

The basic idea behind this paper is to develop new technology to make our systems more secure from getting misused. This technology can be used to protect our system, to make high security places safer by having all their data which can be used later in any type of crime scene or such kind of situation.

6.2. Application

6.2.1 Software

1. It will be of a great use for the defense organizations to have a data base of all the criminals and would be of a great help in catching the criminals.
2. It will also useful for the government to have a check on the fake identities and to manage them according to the law.
3. It will serve as a great source as, the data of the whole country with their biometric identities would be always a few clicks away.

6.2.2Hardware

1. The eye retina scanner and fingerprint sensor will increase the security of our system and places by many times.
2. The technology is made user friendly i.e. it will be fast and not a hectic a process.
3. It will be economically feasible and cost effective for the private as well as for the government organizations.

VII. Conclusion

ThisThe biometrics can play a vital role in keeping our data and places secure and can be of a great use with innovation and advancement in the technology. The software and the hardware would be making our system, our data and our places more secure. The use of data science and its practical use in day to day life by different authorities and organizations for the use of crime control, monitoring and surveillance purposes which will be

helpful in maintaining law and order. Private security organizations and local defense organizations will also be able to use this technology to as this is cost effective and economically feasible.

REFERENCES

1. https://ieeexplore.ieee.org/abstract/document/899930
2. https://www.igi-global.com/chapter/biometrics-past-present-future/7387
3. https://www.osapublishing.org/oe/abstract.cfm?uri=OE-14-2-487
4. Atul Kahate "Cryptography and Network Security", Tata McGraw-Hill Companies, 2008
5. A. Joseph Amalraj, Dr. J. John Raybin Jose, "A Survey Paper on Cryptography Techniques", International Journal on Computer Science and Mobile Computing (IJCSMC), Vol.5 August 2016
6. Sarita Kumari, "A Research Paper on Cryptography Encryption and Compression Techniques", International Journal of Engineering and Computer Science (IJECS), Vol 6 April 2017.
7. https://www.google.co.in/search?client=opera&q
8. https://en.wikipedia.org/wiki/Biometrics
9. https://blog.bioconnect.com/a-brief-history-of-biometrics
10. https://docs.oracle.com/cd/A57673_01/DOC/net/doc/NWANO233/ch8.htm
11. https://whatis.techtarget.com/thermal-imaging
12. https://www.crime-scene-investigator.net/fbiscienceoffingerprints.html
13. www.yourgenome.org/facts/what-is-a-DNA-fingreprint
14. www.biometricupdate.com