Comparison of Iris, Finger, Voice Recognition Techniques – A Biometric Perspective

Vipul Vijigiri

Comparison of Iris, Finger, Voice Recognition Techniques – A Biometric Perspective

Venkata Praneeth Mareedu Bhargava Raviteja Chanduri Vipul Vijigiri
vema12@student.bth.se bhch12@student.bth.se vivi12@student.bth.se
Masters in Signal Processing, Dept. of Electrical Engineering
Blekinge Tekniska Högskola

***Abstract*— In the light of current lifestyle of humankind, there is a great need of high secure interfaces which apart from providing identification to the user, also enhances security. There are many biometric techniques and various new approaches that are being widely used in the fields of banking sector, security accesses, military, etc. But it is difficult to decide which of them is more feasible and secure. We tried to compare these Biometric Techniques and put forth the pros and cons of each of these methods while keeping a few major parameters as benchmarks. We believe this brief overview would help us to analyze the idea of the above approach, which would promote longevity and enable interoperability.**

***Index Terms*— Biometrics [1], Biometric Modalities [2], Feature Extraction, Template Matching.**

I. INTRODUCTION

There has been an enormous change in the use of science and security of which biometrics is one that is most widely discussed and experimented field. Biometrics has undergone drastic changes since its first inception as a Fingerprint recognizing method in China that dates back to 14th century Later on finger printing has become more standardized making it a gateway for other techniques like Finger, Iris, Voice Recognition etc. In the recent years, a number of recognition and authentication systems based on Biometric measurements have been proposed. There is no doubt in saying that Biometrics is going to be the most happening of all technologies in the field of Homeland Security.

II. SURVEY OF RELATED WORKS

There are many biometric techniques being used today and many new approaches are still in the early stages of development. Biometrics can, therefore, be grouped across a range of platforms based on their application and usage. Here we present literature survey for some of the biometrics of the specified categories. This survey is based on the previous study and considering certain characteristics and performances of the modalities. The focus is to build a state of art for the existing biometric method that have potential to take over the global market as the efficient yet secure method to protect ones classified or personal information. Larger research centers or commercial offices use these Biometric methods to either gain or grant access to targeted audience such that it prevents internet piracy, hacking and other potential dangers that could affect the privacy.

III. PROBLEM STATEMENT AND MAIN CONTRIBUTION

Today safety and security has become a primary objective in various sectors. So, in adapting a certain biometric modality there is a need for a certain comparison scheme which enhances the usage of biometric methods and to reduce their error rate. Our research questions deals with comparison of various biometric methods, and also try to predict the future of Biometrics. We hypothesize that there have been many unanswered questions regarding the quality assessment in any one of these biometric technologies. Hence it is our aim to try and compare all those methods and provide our understanding for those who want to have a better perception based on factors like accuracy, dependency, safety, user friendly etc.

IV. PROBLEM SOLUTION

This project is an analytical review carried out on various recognition techniques and hypothesized according to previous work done. Most of the techniques are either based on verification or identification [3]. All the existing methods in biometrics are accessed by certain criteria which are limited to few parameters. This paper puts focus on the Accuracy, Cost, User friendly, Safety, Universality and dependency on the standards of the methods. Each of the methods has its own set of advantages and disadvantages characterized by the technology and innovation that it incorporates in to. As in the 20^{th} century, everything is based on privacy and data integrity, the technology that manages it are prone to threats that could destroy once own integrity or of the country. Companies like Sony, Samsung, apple and networking sites like Facebook, twitter and many other invest millions to maintain the protection of data. Apple came up with finger print and facial recognition recently which seems to be challenging and efficient means of protecting information. Samsung developed Iris devices

to grant access to its own employees to get in and out of their work places. Biometrics can, therefore can't be justified in limited and be grouped across a range of platforms based on their application and usage. Here we present a brief analog of some of the biometrics.

1. BIOMETRIC MODALITIES

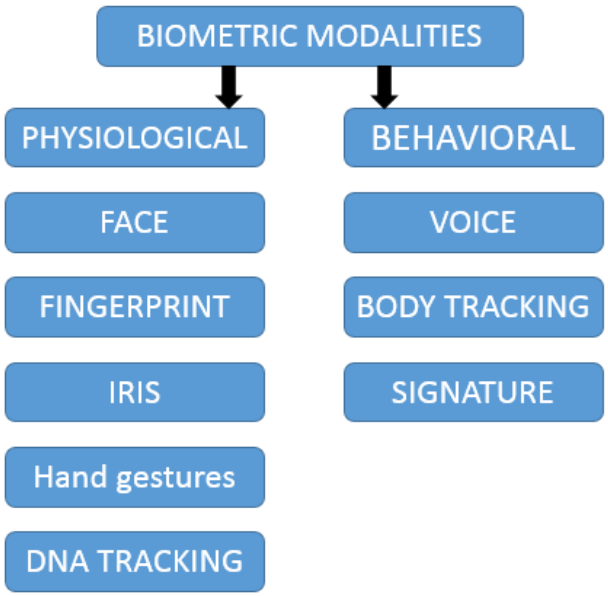

Fig 2: Classification of Biometric Methods.

2. IRIS RECOGNITION

Iris Recognition [3] is an automated ocular based automated method of that recognizes patterns matching techniques used for retina scanning. Common iris recognition systems contain five different stages: Iris acquisition, iris localization and segmentation, normalization, encoding and pattern matching. When someone participates in an iris- recognition system; his or her eyes are scanned to create iris codes, which are in fact binary representations of the image that are stored for security reasons to counter the malfeasance. A basic scheme is as follows where 3 stages are used to evaluate the identification of the user from a prespecified database entry.

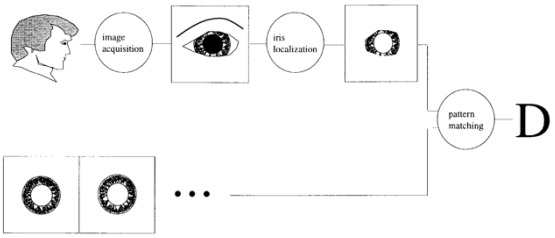

Fig3: Schematic Representation of Iris Method.

These techniques due to its uniqueness (i.e. does not change with age, time and emotional state) can secure/encrypt the data that are highly dependable marking highest levels of safety that protects these systems from counter attacks making it more accurate because of the illumination factor, providing universality to the user.

3. FINGERPRINT RECOGNITION

Fingerprint recognition [4] is one of the most widely used technologies today. Fingerprints are used for biometric recognition as they are quite unique and differ from person to person. Generally in every method, there are three basic steps: Capturing fingerprint by using various sensors, analyzing the data, and Template matching.

The main difference among all fingerprint recognition techniques is the analyzing of the data. The most used data technique is plotting of fingerprint ridges in a 2-d plane by converting ridges into pixels.

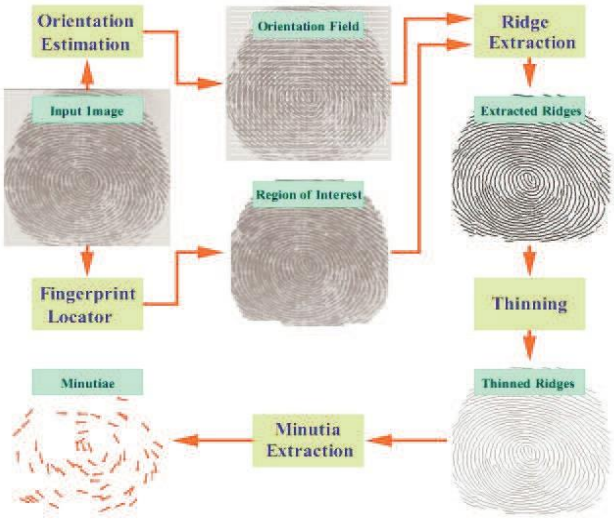

Fig4: Fingerprint Method Schematic Representation.

So using this method we can have high accuracies of about 99%. Fingerprint recognition technique is also quite dependent, user-friendly and cost effective.

3. VOICE RECOGNITION

Voice recognition [4] or speaker recognition uses voice for identifying or verifying a certain individual. It mainly uses the distinct features of speech found in them. It highlights the behavioral patterns like voice pitch, speaking style, voice tone, and frequency of the individual's voice. Generally, this type of recognition depends on either the text dependent or on the text independent formats. Schematic representation of the proposed biometric method is seen below.

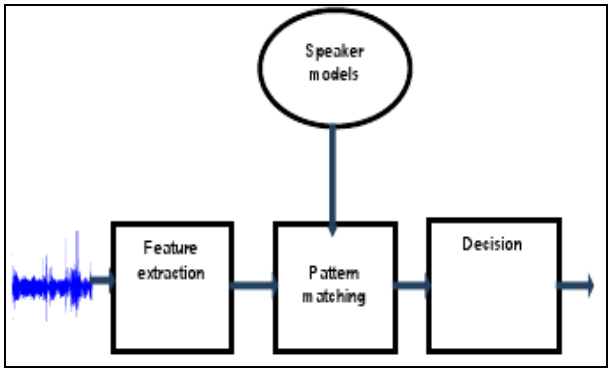

Fig5: Voice Biometric Schematic Representation

When the user speaks in front of the Voice Recognition System, it records the voice. The recorded voice is then analyzed and its key features such as tone, notes, pitch etc. are extracted. They are then compared with the template voice which is already registered within the system. The decision is taken based on the percentage of matching of those two voice features.

Voice recognition technique was dominant until early 2000's but lost its prominence due to lack of accuracy, dependency and safety.

V.RESULTS

After collecting/analyzing the data which were extracted from the papers (2007-2012) that was studied, observed six vital parameters that marks the accountability of the user to rely upon with, which provides a benchmark for these 3 biometric methods that are dominant in the field of advanced commercial applications. The realization of the parameters is as follows:

1. Accuracy: It depends on recognition rate and template matching rate. High matching rates results in better accuracy.

2. Dependability: It relies on FAR and FRR. FAR (False Acceptance rate) is the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs that are incorrectly accepted, for example: a potential intruder. FRR (False Rejection Rate) is this probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs that are incorrectly rejected, for example: an authorized person.

3. Safety: It secures the user data from malfeasance. It is generally related to encryption size of the biometric inputs. Higher encryption sizes are very difficult to be decoded and hence prove to be a very good safety criterion.

4. User-friendly: For a biometric method to be user friendly, it has to have easy accessibility and smooth user interface. The delay time or Extraction time (in biometric sense), is a key feature of interpreting user-friendliness. Extraction time is the time taken for an input to be analyzed and result given. Greater extraction time generally creates a sense of fear and frustration in the user.

5. Universality: Universality refers to ruggedness of the biometric system. Users require their system to be highly abrasive- resistant, good range of operational temperature and also how well can a biometric system work under various conditions.

6. Cost Effectiveness: Not all biometric users are Bill Gates or Warren buffet, so general population will look for cost effective biometric systems. Hence, cost plays a major role in a success of a biometric modality.

The above-discussed parameters are enlightened in the table as follows:

Table 1: Comparisons of Biometrics Methods Using Parameters

Biometric Methods	Iris	Fingerprint	Voice
Accuracy [6]	Recognition Rate>95% Matching rate>50,000Irises/sec	Recognition Rate (85-95%) Matching Rate<2000fingerprints/sec	Recognition rate-70-90%
Dependency [1],[7]	FAR=0.01% FRR=5%	FAR<0.0001% FRR<1%	FAR=0.01% FRR=0.28%
Safety [8]	Encryption Size=5000bits	Encryption Size=(2500-4000bits)	Encryption size=2000bits
User Friendly [9]	Extraction Time (0.1-0.2sec)	Extraction Time<0.4sec	Extraction Time=0.5sec
Universality [7],[8]	Resistant to abrasion	Change in light exposure effects accuracy	Change in voice patterns
Cost	High	Medium	Low

VI.CONCLUSION

Accordingly we have collected data in table1 and fig6 from few research centers (biometric research center, Hong Kong) and through few research papers and taking in to consideration previous work done we have come to the following conclusion. According to the results obtained while taking the parameters into consideration, it can be said that Iris recognition technique dominates qualitatively over its biometric counterparts.

Fingerprint technology currently has 46% and 34% share in the biometric markets for the years 2007 and 2012 respectively. Although fingerprint has a lion's share in the usage of biometrics, Fingerprint is gradually losing its hold. According to the International Biometric Group [9], the projected market study for the 2015 reveals that Iris and face recognition is going to be the leading biometric modality with 19% of the total market share.

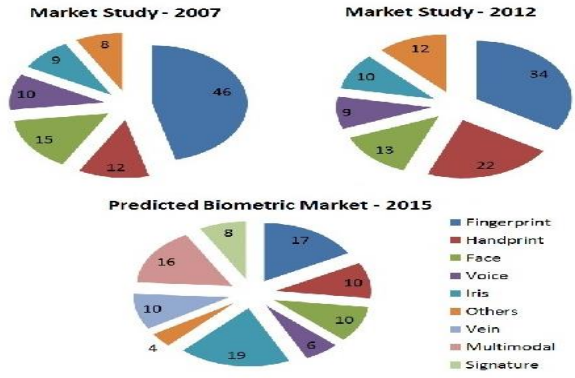

Fig6: Statistics of Various Biometrics Usages

Hence due to its predominant Positive traits, Iris Technique has wide scope of usage in application such as sub substituting for

passports in automated border crossing; expediting security screening at airports; controlling access to restricted areas.

V. FUTURE WORKS

1. Next Generation Identification by FBI [10]:

FBI took an initiative in this next generation identification. This is intended to "cut down terroristic and "culpable activities" by improving the biometric technology to the next level. According to which following modalities are considered to make it a successful project.

- Adaptability
- Capacity
- Certainty
- Response Time
- Functionality
- Interoperability
- Availability

NGI is collaboration between CJIS advisory policy board (WASHINGTON D.C) and Members of compact council. Its main goals are national security, public safety, leadership in biometrics etc and to enable smooth transition in public.

2. Leon, a city in Mexico [11] uses Iris scanners systems to run the entire city. It is still in its early stages but it won't be much longer before the whole cities will be administrated by Biometrics

VI. REFERENCES

[1].EncyclopediaArticle/(2012/09/12/http://en.wikipedia.org/w/index.php?title=Biometrics&oldi d=519553294

[2].The biometric consortium. (2012/09/19). Retrieved from http://www.biometrics.org/research.php

[3].(2012/10/04)Wildes, R.P.; "Iris recognition: an emerging biometric technology," Proceedings of the IEEE , vol.85,no.9,pp.13481363,Sep 1997 doi: 10.1109/5.628669 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=628669&isnumber=13673.

[4].(2012/10/04)Arun Ross, Rohan Nadgir: A Thin-Plate Spline Calibration Model For Fingerprint Sensor Interoperability. IEEE Trans. Knowl. Data Eng. 20(8): 1097-1110 (2008)

[5].Baumann, J. (n.d.). Voice recognition. (2012/10/08) Retrieved from http://www.hitl.washington.edu/scivw/EVE/I.D.2.d.VoiceRecognition.html.

[6].GRUSOFT (2009). *Grus iris tool* .(2012/10/13) Retrieved from http://www.grusoft.com/girist.htm

[7]TS&Tm04(L)(2012/10/13).pdf/http://www.autostar.com.sg/images/pdf/TS&Tm04(L).pdf

[8].bergdata fingerprint biometrics: FlySDKu100.pdf /http://www.bergdata.com/uploads/media/flySDKu100.pdf

[9].search-releases=biometrics/http://www.prweb.com

[10]. (n.d.).(2012/10/17) retrieved from http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi

[11]. (n.d.).(2012/10/21)retrieved from http://singularityhub.com/2010/09/26/iris-scanning-set-to-secure-city-in-mexico-then-the-world-video/

[12]. (2012/10/21) retrieved from http://researchweb.iiit.ac.in/~vandana/PAPERS/BASIC/biometric_challenges.pdf/

[13]. Biometric Cryptosystems:Web. 22 Oct. 2012. Retrived from http://biometrics.cse.msu.edu/Publications/SecureBiometrics/Uludagetal_BioCryptoSystems_ProcIEEE04.pdf

[14]. sulochana sonkamble, 2dr. ravindra thool, 3balwant sonkamble 22 oct 2012.retrived from http://www.jatit.org/volumes/research-papers/Vol11No1/6Vol11No1.pdf.

Venkata Praneeth Mareedu was born in Vijayawada, India in 1989. He did his schooling in Hyderabad. In 2011, he completed his Bachelors in Electronics & Instrumentation from Dr.MGR University, Chennai. Currently he is doing his Dual Degree Masters [2011-2013] from JNTU Hyderabad and Blekinge Institute of Technology.

Bhargava Raviteja Chanduri was born in 1989 and raised in Hyderabad, India. He did his schooling in Hyderabad. In 2010, he completed his B.E (Hons.) in Electronics & Instrumentation from BITS, Pilani-Dubai Campus, Dubai. Currently he is pursuing his Dual Degree Master's Program [2011-2013] from JNTU Hyderabad in compliance with Blekinge Institute of Technology.

Vipul Vijigiri was born in Andhra Pradesh, India in 1988.he completed his bachelor's degree in Electronics and Communication Engineering from Jawaharlal Nehru technological university, Hyderabad-India (JNTUH) .now he is pursuing his masters in electrical engineering [2011-2013] from Blekinge Tekniska Hogskola, Sweden. His current research includes neural networks and radio communication.

Jenny Lundberg received her PhD in Computer Science in April 2011 from Blekinge institute of technology. Her main research focus is Engineering Information and Communication Technology (ICT) for robust information sharing. Presently she is working as a professor in Blekinge institute of technology.