Biometrics Fingerprint Sensors: An Introduction

Nitin Sambharwal[1] Dr. Chander Kant[2]
[1]Research Scholar [2]Assistant Professor
[1,2]Department of Computer Science and Applications
[1,2]K.U, Kurukshetra, India

Abstract— Every human has distinct physiological as well as behavioral characteristics and to recognize each individual we need a biometric system that provides a wide variety of reliable personal recognition schemes either in form of confirmation or determination. The purpose of such schemes is to make sure that the services are only accessed by a genuine user, and no one else use of it. This includes fingerprint, voice, face, gait, iris, signature, hand geometry etc. Mainly the biometric system consists of four main modules i.e. sensor module, feature extraction module, matching module and decision module. In a biometric system, sensor module is the first module so it is very essential to have accurate acquisition of data over there. In this paper various type of fingerprint sensors are discussed in detail. There are some parameters like pixel density, resolution, SN ratio, motion blur, gray scale etc. of these sensors which are also included. Sensors also encounter some challenges like durability, dry & wet finger, noisy data, spoof attacks etc. Finally the list of most deployed sensors with their parameters.

Key words: Biometric System, Fingerprint Sensors, Ink Method, Multispectral, Optical, Solid State, Ultrasound

I. INTRODUCTION

A. *Biometric System:*

Biometrics system uses these unique characteristics (or identifiers) to identify or verify people's identity known as Identification or Verification respectively. Unique Identifiers include distinct features such as iris patterns, fingerprints, voice inflections in speech, signature, It also includes use of computer keyboard for typing and the way we walk i.e. gait recognition etc [1].

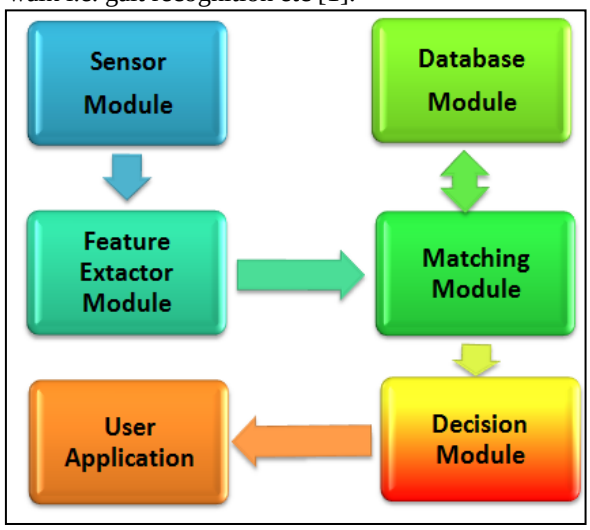

Fig. 1: Biometric System Modules

There are total four different types of modules in a biometric system and these are shown in Fig. 1 and there descriptions about modules are given below:

1) Sensor Module:
It is responsible for capturing the data from user.

2) Quality Assessment and Feature Extraction Module:
This module helps to extract the salient feature from the captured biometric data that is taken by sensor module.

3) Matcher Module:
The extracted features are compared against the stored template in the data base to generate match scores.

4) Decision Module:
It takes the decision based on comparing match score or threshold value [2].

B. *Biometric Sensor:*

A sensor is a transducer which is responsible for sense (that is, to observe or to detect) some characteristic of its environs. Basically it detects actions or changes in quantity and then provides corresponding output.

In Biometric System a sensor is a device liable for capturing the data from the user i.e. capturing the sample of physical traits (like fingerprint, iris, retina, face etc) or behavioral traits (like voice, signature, gait etc). If the quality of taken sample is not so good then definitely processing at all other levels will be affected [3].

1.1) Features of good biometric sensors are explained below [4]:

- Input data correctly converted from analog data to digital data for processing smoothly.
- Sensor should be supposed to be easily to operate and use.
- It should be non-intrusive i.e. spoof attacks should not be possible over there.
- Error rates should be low.
- Sensor should be of reasonable cost.

1.2) Factor affecting biometric sensors: In generally, sensor module encounters with a numerous problems and these are explained below in fig. 2. [5][6].

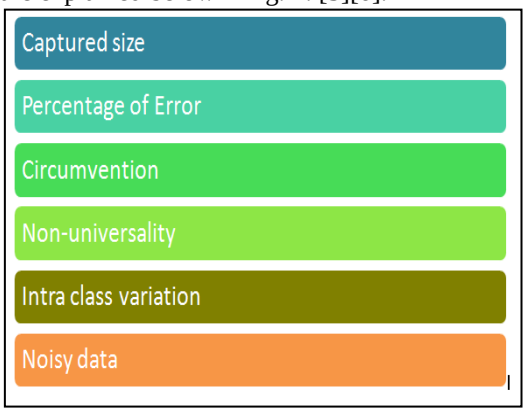

Fig. 2: Factor Affecting Biometric Sensors

1) Captured Size:
A reasonable size is required i.e. neither very big nor too small.

For example if the size of captured data is very large then it would be hardly manageable.

2) Percentage of Error:

For a better biometric system if error at sensor level would be lower in rate then it would have the maximum chances for an error free result taken by the biometric system. In generally sensor may encounter with various error rates and these are shown in Fig. 3.

3) Circumvention:

It means how easily to break the system security or spoof the system. This type of issue occurs only when there is submission of facsimile of a person's biometric to gain illicit advantage for access.

For example a gluey fingers or a fake finger can be easily made with wax. These sensors should have liveness detection to differentiate between the fake and a genuine finger.

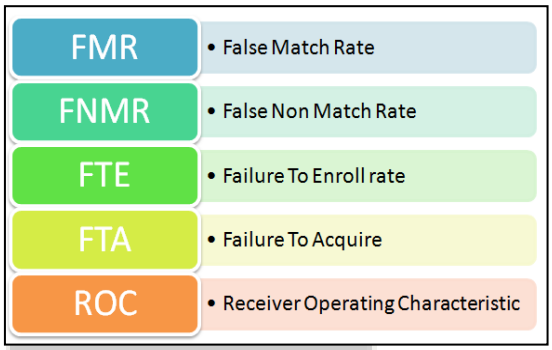

Fig. 3: Showing List of Error Rates

4) Non-Universality:

It means that the trait we required for capture by sensor is possess by everyone or not. i.e. universally present.

For example some people may not have fingers. Some people have burnt fingers, cut marks, dry or oily fingers which can resulting of the impression of Non-universality because their samples are of poor quality resulting in degrades poor performance of a system.

Non-universality leads to failure to enroll (FTE) and failure to capture (FTA) error rates, which again resulting in degrades the system performance.

5) Intra Class Variations:

This type of issue occurs when a user uses improper interactions with the sensor. If there are some rotational and translational movements then also there can occur variations.

For example if a user applies too much pressure on sensor surface or swiftly moving its finger on a sensor.

6) Noisy Data:

It occurs due to improper placement of finger on a sensor or it may be occur if the dust practical on a sensor surface are present.

For example in a fingerprint sensor there remain previous fingerprint impressions over there and dirt can produce noisy data.

Value of all these factors must be in lower for better performance or accurate acquisition of data.

II. FINGERPRINT SENSORS

Fingerprint sensors: The main task to perform by the fingerprint sensors are detect pattern of valleys and ridges. Uniqueness is determined by minutiae points (whorl, arch, loop), ridges, and furrows etc [2]. For this a user places its finger on the surface of sensor and sensor scans the unique information. Fingerprint sensors are basically categorized into two main categories offline and online fingerprint sensors [7]. This is shown in figure 4.

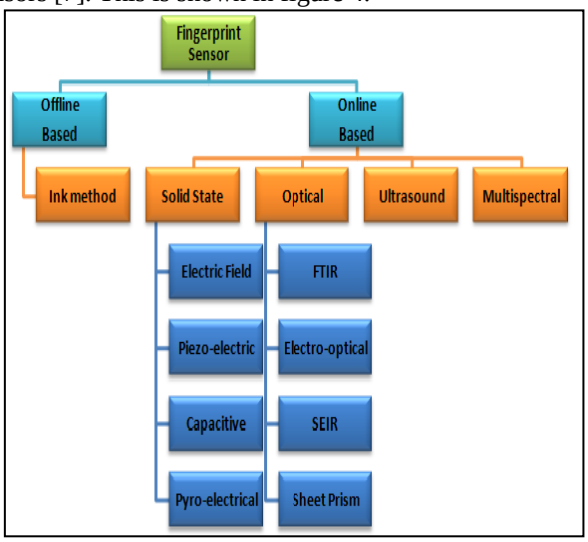

Fig. 4: Classification of Fingerprint Sensors

A. Offline Fingerprint Sensors:

It was the oldest among all technique. In this type of technique; sensors image acquisition and further processing is done separately.

1) Ink Technique:

In this finger area is spread with dark black ink and then pushed against paper. This will stamp the pattern of ridges and valleys on a paper which is then scan by the digital scanner to convert the document into digital format. This conversion is done with the help of paper scanner or high quality CCD camera [7].

a) Advantages:

- It a simple technique.

b) Problem:

- It lies with smudge and ink stains on paper also.
- It is slow technique.

B. Online Fingerprint Sensors:

Unlike the offline technique these sensors directly sense the finger without the requirement of ink and paper. Online fingerprint sensors are divided into four main categories i.e. solid state, optical, ultrasound and multispectral sensors.

1) Solid State Sensors:

Solid state sensors permit these devices to be easily implanted in various applications such as cell phones, PDAs, laptops etc. These are well-known by silicon sensors. These sensors implement DC capacitance. This category includes four main types of and these are shown in Fig. 5[8].

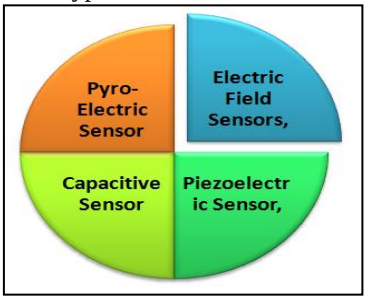

Fig. 5: Various Types of Solid State Sensors

a) Electric Field Sensor:

This type of sensors consists of two parts, one is a sensor that is consists of drive ring and other is matrix of active antenna. These sensors would produce a radio frequency (RF) signals. The skin of finger modulates these signals and then RF signals are received by active sensors. The finger must be lie between the both sensor and the drive rings. Magnitude of RF signals is used to generate fingerprint image [7].

Advantages:

- Less vulnerable to damaged fingerprints.
- Dry fingers do not create any problem.

Problems:

- Large post image processing is required

b) Piezoelectric Sensors:

These sensors are also known as pressure sensitive sensors i.e. current is produced when mechanical stress is applied on surface of sensor. This mechanism is well-known as piezoelectric effect. The sensor surface is prepared by non-conducting dielectric material. Ridges and valleys are present apart from each other so they apply different amount of pressure on the surface of sensor. The amount of current generated that will depend upon pressure applied resulting in different amount of current produced by ridges and valleys as shown in Fig 6. below [8] [9] [11][14].

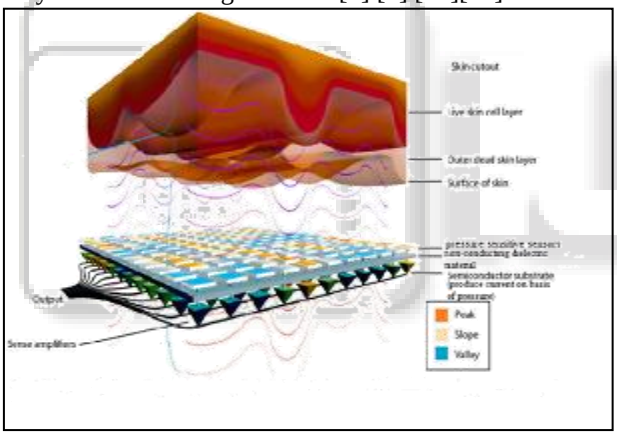

Fig. 6: Piezoelectric Sensor

c) Advantages:

- Less in cost.
- Easily to incorporate with other devices.

d) Problems:

- Do not capture fingerprints relief precisely.
- High in FMR (false match rate) and FNMR (false non match rate).
- Coating on sensor is less long-lasting.

e) Capacitive Sensors:

Capacitive sensors are two dimensional (2-D) arrays of ten to thousands of capacitance plates embedded on a chip. Finger area acts as another plate for capacitance. When a user's finger is placed on sensing area then a small amount of electrical charge is generated between the two plates that is finger area and plate area. The amount of this charge is different for the valleys and ridges, since that will depend on distance between the capacitors. Resulting in different pattern of fingerprints is produced by valleys and ridges [12] [13]. As shown in Fig 7.

Advantages:

- Compact in size.
- Easily to implant.
- Do not generate any type of geometric distortions.

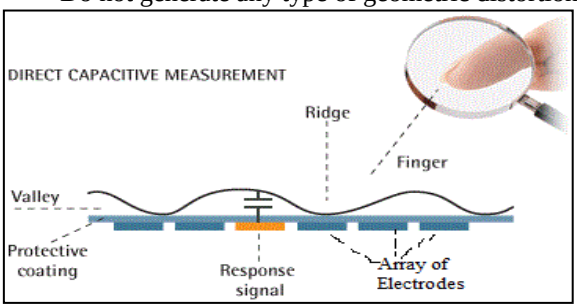

Fig. 7: Capacitive Sensor

Problems:

- Mostly the sensor affected by Electrostatic discharge available at the tip of the finger.
- Sensor can be affected from 60 Hz power line.

f) Pyro-Electric Sensor:

Pyro-electric sensors are also well-known as temperature differential sensors or thermal sensors. As the name implies these sensors are mainly constructed of pyro-electrical material. Whenever two surfaces are bought in contact that will generates electric signals based on variation in temperature. When a user place his finger over the sensor surface there is a electric signal will be generated by thermal sensors resulting in ridges are directly contact with the surface except valleys because they are away [8] [9] [11] [14].

Pyro-electric sensors are of sweeping type because image is generated by in contact with sensor and it will disappear quickly as equilibrium is reached. Therefore sweeping sensors are providing relatively a stable image [4].

g) Advantages:

- Low in cost.
- Small in size.
- They do not produce geometric distortions.
- Fake fingerprints are easily to detected.

h) Problems:

- Susceptible to dry and humid conditions.
- Environmental temperature would create problems.
- It introduces distortions typical when a sensor is replaced.

2) Optical Sensors:

Mainly the optical fingerprint sensors are of four types as shown below in fig. 8.

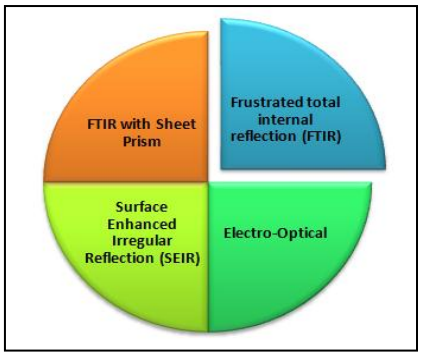

Fig. 8: Various Types of Optical Sensors

a) Frustrated Total Internal Reflection (FTIR):

The basic principle of these sensors are Total Internal Reflection (TIR) [8]. These sensors require a glass prism, a lens, a light source, a charged coupled device (CCD camera) and frame grabber.

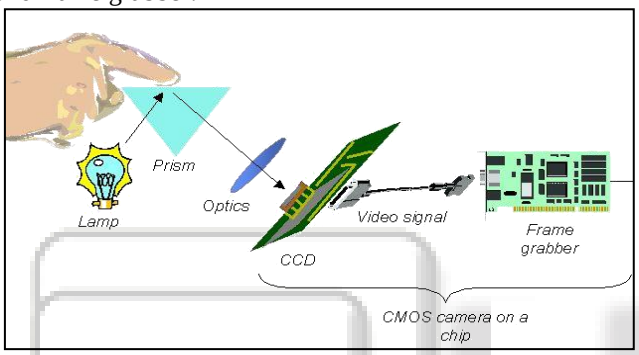

Fig. 9: Frustrated Total Internal Reflection

In Fig. 9 Initially the finger is placed over the surface i.e. upper side of glass prism. Usually ridges are contact with surface while valleys do not contact with it. Then a laser light source is used whose aim is to reflect the light toward the glass prism. Then the light scatters at ridges and valley both. As a resulting of the light which is scattering ridges looks dark and due to total internal reflection valleys seems bright. Finally the light will exit from the another side of glass prism and then lens will focus the light toward the Charged Coupled Device camera it will produce video signal and then sent these signals to frame grabber (a frame grabber is a device that captures individual, digital still frame from the analog video signal or a digital video stream. And also it would provide the interface between a device and computer) [9].

b) Electro-Optical Sensors:

Its main working principle is to convert the light signals into electrical signals. These sensors consist of two layers one is for light emitting polymer and other is for photodiode array.

Whenever a user placed its finger over the sensor resulting in the ridges contact with polymer surface and valleys do not. Therefore different intensity of light gets emitted. Then the difference in light intensity are sense by photodiode array as shown in Fig. 10 [5][9].

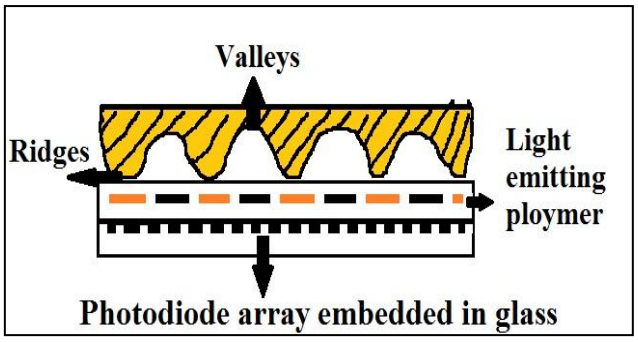

Fig. 10: Electro-Optical Sensor

c) Advantages:

- Less expensive.
- Most widely used.
- Not susceptible to electrostatic discharge.

d) Problems:

- Difficult to manage the sensor.
- Latent prints can create problems.
- Sensor's coating is not durable.

e) Surface Enhanced Irregular Reflection (SEIR):

Surface Enhanced Irregular Reflection sensor is work on the principle of scattering fused through optical design. In this type of sensor when a user places its finger over the sensor the light is scattered from ridges but there is no light scattered through valleys. Now the scattered light is collected by the camera so valleys appear dark and ridges seems highly bright [10].

f) FTIR with Sheet Prism:

In this type of sensors glass prism as in normal FTIR sensor would be replaced by sheet prism. Sheet prisms are made up of number of adjacent 'prismlets'. As shown in fig. 11.[8]
Advantage:

- Cost effective.
- Sizes of sheet prism sensors are smaller than glass prism.
- Reduced mechanical assembly.

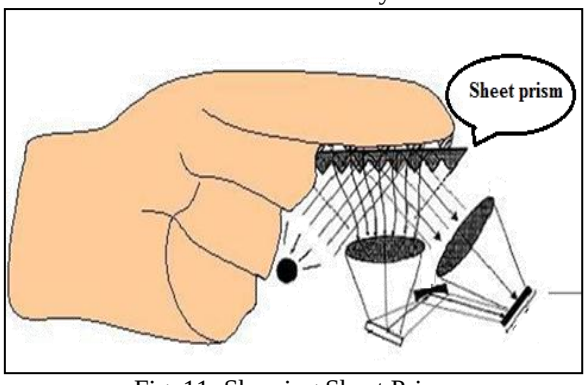

Fig. 11: Showing Sheet Prism

C. Ultrasound Sensors:

Ultrasound sensors are works on the principle of acoustic signals. There are two components of ultrasound sensor that is sender and receiver known as transducer. Sender sends the acoustic signals toward the fingertip over the sensor surface and receiver detect the echo when the signals get

reflect back by finger. So there is no skin contact is necessary. Echo signals are used to analysis the image of finger on behalf of echo analysis the structure of ridges and valleys can be differentiated. Basically it calculates the distance based on the impedance of finger [7][9][15]. As shown in Fig. 12.

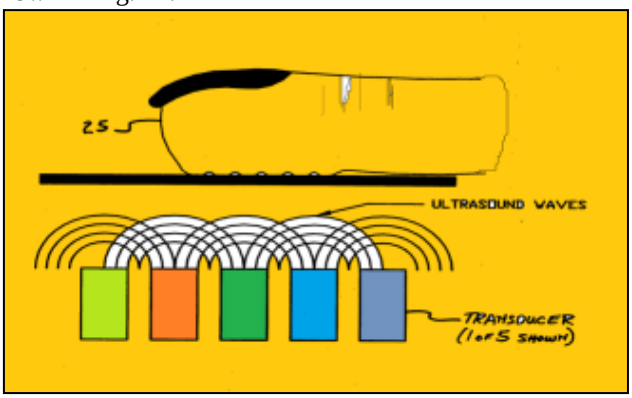

Fig. 12: Ultrasound Sensor

a) Advantages:

- High quality image is generated.
- Not affected by oil and dirt.
- Highly accurate.

b) Problems:

- Not suitable for large scale productions.
- Scanner consists of large number of mechanical small parts.
- Expensive in cost.

D. Multispectral sensor:

Multispectral sensor as the name implies multi means it takes multiple images of fingerprint under different conditions. When a user places his finger over the sensor surface then it would capture the multiple images at different condition. It may be different polarizing, illumination angles, and wavelengths conditions. These multiple images are merged together to produced single equivalent fingerprint image [14]. Here the image generated by these sensors is very accurate and high quality as well. Working diagram is shown below in Fig 13.

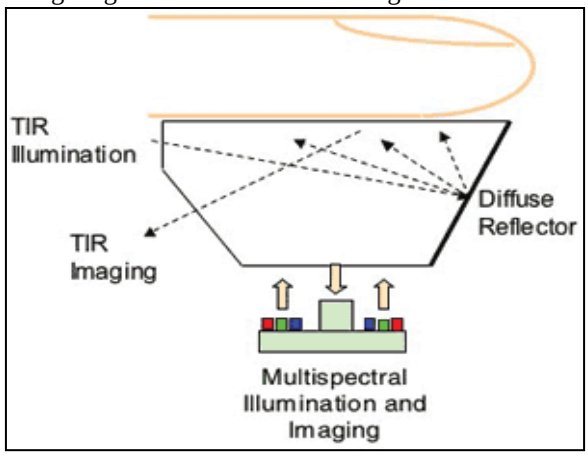

Fig. 13: Showing Multispectral Sensor

1) Advantages:

- More accurate images.
- Provide backward compatibility with all other fingerprint sensors.

2) Problems:

- Highly expensive.
- Complex background technology used.

III. List of Sensors Available in Market

There are lot of fingerprint sensor are available in market but the most commonly deployed sensors in market are shown in table 1 [2][4].

S. No.	Name of Sensor	Recognition Speed (in ms)	Cost (in $)	Resolution (in dpi)	Temp. (in °C)	Acquisition Area (in mm)	FAR %	FRR %
1	Rflogics FINGER006 Slave	30	840	500	-10 to 40	13 × 15.2	0.001	0.1
2	FPR-100	<100	15	508	25 to 85	9.6 × 0.4	<0.0001	<0.1
3	Marks 175 bio	100	600	500	-10 to 50	15 × 18.1	0.001	0.1
4	U.ARE.U4500	140	66	512	0 to 40	14.6 × 18.1	0.001	1
5	WG Reader 208	<200	80	450	-10 to 75	19 × 12.8	<0.0001	<0.01
6	CMA S20	250	10	500	25 to 55	18 × 20	0.001	<=1
7	ZJ12	250	35	500	-20 to 25	18 × 22	0.001	0.01
8	AET65	<500	115	508	0 to 50	9.6 × 0.2	d"0.001	d"0.001
9	UPEK Eikon 500	500	100	508	0 to 40	12.8 × 18	0.001	0.1

Table 1: Fingerprint Sensor Deployed In Market

A. Basic Parameters of Fingerprint Scanner:

It is not easily to define quality parameters somehow application requires some minimum quality need to specify some range of values. There are two standards for fingerprints i.e. EFTS (Electronic Fingerprint Transmission Specification) and PIV (Personal Identification) [8]. According to these values are given below or pictorial representation is shown in fig. 14. [7] [16].

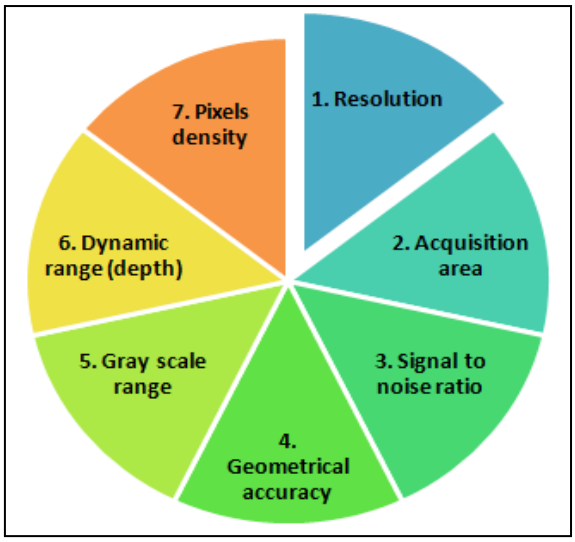

Fig. 14: Basic Parameter of Fingerprint Scanner

1) Resolution:

It is described as number of pixels per inch or dots per inch (dpi).maximum and minimum allowed resolution is 500dpi±10%.

2) Acquisition area:

Rectangular area that the fingerprint senses and it is given as height*width.

More the sensing area more good quality sensor it is because more ridges and valleys are captured. But more sensing area poses problem of incorporation in small devices and also increases cost of sensor. Typical area for correct capturing is 1*1 square inches.

3) Signal to Noise Ratio:

It is defined as ratio between signal power to noise power. Usually Signal to Noise ratio is 500±2%.

4) Geometrical accuracy:

Most of geometric distortions produced by acquisition device that is known as geometrical accuracy. It is better expressed in the form of percentage with respect to x and y direction. It's typical value is max (0.0007'', 0.01'').

3.1.5)

5) Gray Scale Range:

Value of gray scale range is be >=128.

6) Dynamic Range (Depth):

Defined as the no of bits used to encode the intensity value of each and every pixel. In generally its value is taken as 8.

7) Pixels Density:

No of pixel are derived from the value of acquisition area and resolution. Let us assume resolution is denoted by R dpi and area as height (H)*width (W) then the number of pixels is given by RH*RW pixels.

B. Challenges in Design of Fingerprint Sensors:

There are various challenges encounter in designing of fingerprint sensors and some of these are shown in Fig. 15.

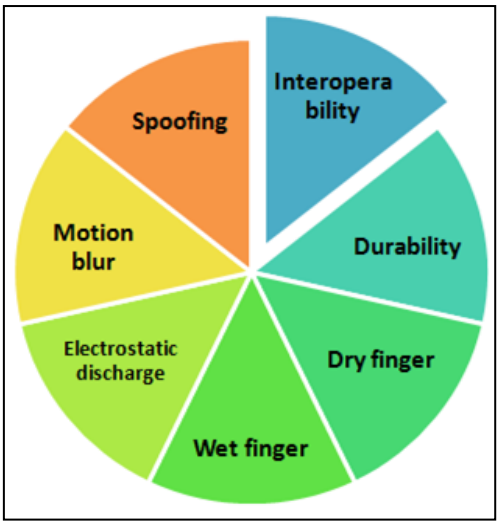

Fig. 15: Challenges in Fingerprint Sensor Design

1) Interoperability:

This may arise due to different sensors used at the time of enrollment and verification may cause problem.

- Solution: To solve these problems calibration of sensor can be used also some new matching algorithms are to be designed.

2) Durability:

It means the time duration over which the fingerprint sensor work fine. Here the main difficulty is durability that lies with the sensing surface area because it gets wear with time.

- Solution: Optical sensors have glass or plastic surface is reasonably durable but silicon sensors are less durable

3) Dry finger:

In a biometric system if a finger is extremely dry then it will not formulate properly contact with the sensor surface. Hence the exact finger image of ridges and valleys cannot be obtained as in resulting of poor quality fingerprint image.

- Solution: Use moisturizer to remove dryness of finger and other alternate is to heating the surface, it can produce sweat on fingers but it increases power consumption.

4) Wet finger:

It is also a biggest challenge for a fingerprint sensor if there is some amount of water content over a finger then whenever user apply its finger on sensing area water gets filled into the valleys also. So a sensor can't distinguish ridges and valleys separately.

- Solution: Use towel or cloth to remove excess moisture. And also some temperature can be applied on sensors to maintain dryness.

5) Electrostatic discharge:

If there is some electrostatic charge is present over a finger resulting in a good quality image can't be obtained. This problem is mostly happen with solid state sensors rather than optical sensors.

Solution: This problem can be solved by using surface coating, grounding etc. to discharge the electrostatic charge.

6) Motion Blur:

Whenever a finger is scanned in moving position of fingerprint then a clear image can't be formed this problem is known as motion blur.

- Solution: When a finger is scanned then doesn't try to move your finger until the scan is not complete.

7) Spoofing:

Spoofing is a technique by which we can fool system easily with artificial fingers which is easily made up of gelatin and wax compound etc.

- Solution: The sensor should be capable to detect genuine and fake fingerprint by using liveness detection by sense the fingerprint temperature, blood flow, pulse etc.

IV. CONCLUSIONS

Biometrics is a technology that has very rapidly gone from being used like forensic, military security etc. Biometrics is technology that uses your individual and unique physical characteristics to identify an individual it may be fingerprint, hand geometry, iris, face, voice etc. and there are lots of different type of sensors are available in market. There are some parameters and standards to use them according to the system need these parameter include resolution, area, gray scale range, S-N ratio, pixels density etc. Which sensor is to be chosen that decision totally depends on various factors like user acceptance, type of application, cost, usability etc? The biggest challenge is of sensor interoperability In future this problem can be resolved successfully so that we can use any type sensor at any time i.e. there is no dependability on previous sensor used.

REFERENCES

[1] Ravi D., "An Introduction to biometric: A concise overview of the most important biometric technologies", Keesing Journal of Documents & Identity, 17, 2006.
[2] Anil K. Jain, Arun A. Ross, "An Introduction to Biometric Recognition", IEEE transaction on circuits and systems for video technology, vol.14, no.1, January 2004.
[3] Moridini E.,Wright D., Hert P.D., Mantovani E., Wadhwa K.R., Thestrup J. and Steendam G.V., "Ethics, e-Inclusion and Ageing. Studies in Ethics, Law,and technology", Mendeley publications. Vol 3, issue 1, article 5, 11,203-220, 2009.
[4] Gursimarpreet kaur, Dr. Sheetal Verma, Dr. Chander Kant Verma "Classification Of Fingerprint, Iris And Facial Sensors", IJSRD - International Journal for Scientific Research & Development| Vol. 2, Issue 03, ISSN (online): 2321-0613, 2014.
[5] Sunil kumar single, Santosh kumar, "A review of data acquisition and difficulties in sensor module of biometric systems", SJST,35950,589-597,sep-oct.2013.
[6] Sutcu, Y., Rane, S., Yedidia, J.S., Draper , S.C. and Vetro, A., "Feature Transformation of Biometric Templates for secure biometric systems based on error correction codes" , In Proceedings of Institute of Electrical and Electronic Engineers Computer Society Conference on computer vision and pattern recognition, Cambridge, massachusetts, U.S.A, ,1-6, October 31,2008.
[7] Jianjiang Feng, Anil K. Jain, and Arun Ross, "Fingerprint Alteration", J. Feng, A. K. Jain, A. Ross, "Fingerprint Alteration", MSU Technical Report, MSU-CSE-09-30, Dec. 2009.
[8] S. Prabhakar,Alexander Ivanisov, and Anil K. Jain,"Biometric Recognition: Sensor Characterstics and image quality", 2008.
[9] A. Ross and A. Jain, "Biometric sensor interoperability: A case study in fingerprints", in Proc. of International ECCV Workshop on Biometric Authentication (BioAW), LNCS, pp. 134–145, May 2004.
[10] Secugen Biometric Solutions, "SEIR optic technology", White Paper, Secugen, 2004.
[11] Modi.S.K., "Analysis of fingerprint sensor interoperatability on system performance", Center for Education and Research in Information Assurance and Security,Purdue University,1,1-189,2008.
[12] Tsikos, "C.: Capacitive fingerprint sensor", US Patent 4353056 (1982).
[13] Young N.D., Harkin G., Bunn R.M., McCulloch D.J., Wilks R.W., Knapp A.G.:" Novel fingerprint scanning arrays using polysilicon TFT's on glass and polymer substrates", IEEE Electron Device Letters 18 , 19–20, 1997.
[14] A. Ross and R. Nadgir, "thin-plate spline calibration model for fingerprint sensor interoperability", IEEE Transactions on. Knowledge and Data Engineering, 20(8):1097–1110, 2008.
[15] Bicz W., Gumienny Z., Kosz D., Pluta M.: "Ultrasonic setup for fingerprint patterns detection and evaluation", Acoustical Imaging 22(1996).
[16] Davide Maltoni and Matteo Ferrara," On the Operational Quality ofFingerprint Scanners", BioLab - Biometric System Lab Biometric System Lab University of Bologna University of Bologna – ITALY, November 7, 2007.

