Songklanakarin J. Sci. Technol.
35 (5), 589-597, Sep. - Oct. 2013

SJST SONGKLANAKARIN JOURNAL OF SCIENCE AND TECHNOLOGY
http://www.sjst.psu.ac.th

Review Article

A review of data acquisition and difficulties in sensor module of biometric systems

Sunil Kumar Singla and Santosh Kumar*

Department of Electrical & Instrumentation Engineering,
Thapar University, Patiala, Punjab, India.

Received 10 February 2012; Accepted 7 June 2013

Abstract

Biometrics refers to the recognition of individuals based on their physiological and/or behavioral characteristics. The biometric traits which may be considered for the authentication of a person are face, hand geometry, finger print, vein, iris, etc. A competent selection of a sensor, its mechanism and adaptability is required, as the absence of these will leave the biometric sensor deceptive to information sensing. Selecting a sensor for a biometric application from the large number of available sensors with different technologies always brought the issue of performance and accuracy. Therefore, various error rates and sensibility contention differentiate the available biometric sensors. This paper presents the difficulties faced in the sensor module of the biometric system and the incomparable alternatives on the basis of availability of information at sensor module of the various systems.

Keywords: biometrics, authentication, sensors, error rates, sensibility contention

1. Introduction

Biometric is one of the hyped technologies that set in motion for identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. One of the applications which most people associate with biometrics is security. Some of the physiological and/or behavioral characteristics that are being used for the biometric recognition include face, retina, palm print, DNA, hand-geometry, ear, voice, finger print, gait, signature, key-stroke dynamics, and iris (Jain *et al.*, 2004). Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions (Zhan *et al.*, 2008). As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. In recent years, biometric authentication has seen considerable improvements in reliability and accuracy, with some of the traits offering good performances. However, even the best biometric traits till date are facing numerous problems; some of them are inherent to the technology itself. In particular, biometric authentication systems generally suffer from enrollment problems due to non-universality of biometric traits, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data acquisition (sensor module) in certain environments (Sutcu *et al.*, 2008).

Challenges of providing security to a genuine user and easy access to the information are achieved through identity management system. A typical identity management system is one that renders its services to a legitimate user and stops the imposter to access the security. Conventionally the security issues in the domestic and commercial organizations dealt with personal identities. Here, identity management achieved through hard-coded passwords and badge-based appliances (driver licenses, and passports) (O'Gorman, 2003). This introduces numerous problems because sometimes it is very easy for application programmer to crack the password.

* Corresponding author.
Email address: santu.thoughts@gmail.com

Also risk of stolen identity and the risk of compromising the template are some of the most publicized issues and frequently cited in relation to the security of conventional identity management systems. Biometrics offers a better and reliable approach to the identity management by recognizing individual based on their physiological and behavioral characteristics that are inherent to the person. An orthodox biometric system inherits five main modules. The sensor module, preprocessing module, feature extraction module, matching module and decision module (Ross *et al.*, 2004). The sensor module is responsible for acquiring (collecting) the biometric information from the subject. Acquiring data at the very first stage of the biometric system is a very big-league since it becomes extremely difficult to extract features from the fingerprint, iris, face images, etc., if the quality and amount of information collected by the sensor is not accurate and efficient. For example, extracting the minutiae from the fingers of aged persons as well as manual worker are major problems in fingerprint based biometric system (Mordini *et al.*, 2009). If the sensor is of good quality which can capture fine details then these problems can be minimized in fingerprint based system. Likewise, in face recognition system and iris recognition system the choice of good sensor can eliminate or minimize the need of preprocessing for background area, coordination etc. Therefore the choice of sensor is very critical for making the system more accurate and stable. In this paper, we briefly explore this problem and present a case study describing its impact on biometric systems.

2. Sensor and Data Acquisition

The adroitness of a biometric system to adapt the raw data is the essential task. This ability of the biometric systems for the data acquisition and providing the high quality information at the very first stage of the sensors, determines the sensor incisiveness. The acquisition module interprets the biometric data into digital form.

Finger print biometric sensors are the integrated circuits with embedded principles and algorithms that are required for user authentication. When one places his/her finger on the chip they produce the electrical signal for the finger print images. Number of tiny electrodes and analog-to-digital converter that are present in the sensor, convert the information in digital form. The varying capacitive values across the sensor array are then converted into an image of the fingerprint. The thermal energy flux is also used to capture the fingerprints. This is done when a ridge comes in contact with a sensor surface and heat flow between the ridges. The differential temperature due to heat between the ridge and sensor surface forms the cavity. Therefore the obtained images are then stored as template to create the database. Other components of the biometric access control system then compare the image to a stored template to achieve the genuine user authentication (Modi, 2008).

Construction of the data base for the face image is developed by acquiring information through the evidences obtained from face recognition sensors. 3-D laser scanner, which employs an optical triangulation method, is one of the most popular devices for acquiring the face images. The most meticulous 3-D face data can be obtained through this laser scanner. It analyzes the face of a person and collects the data on its shape and possibly its appearance (i.e., color). The data which is collected from the face can then be used to construct digital, three dimensional models. However, the system is very expensive and acquisition time is more (Cyberware, 2011). Sometimes using a stereo vision system for reconstruction of the 3-D image form the data which is obtained from the two images of same person is helpful. This technology requires only two cameras to reconstruct 3-D face data, but accuracy and reconstruction performance is hard to find (Ohta *et al.*, 1985).

The elementary step in the iris recognition is the iris image acquisition, but capturing high-resolution iris images is very difficult. In real time, most of the system which has small capture volume requires user concentration with machines, which is the biggest barrier in iris image acquisition and recognition. Most of the products available in the market are non-contacting and acquire iris images at a distance. So, to capture the unique feature of the iris, a high-quality (resolution) image of the eye in the near-infrared range (700-900 nm) is required to be captured. The image consists of its own source of infrared illumination to the eye. The infrared illumination reveals patterns even for dark eyes. Hence for capturing the eye image at a distance, systems require users to machinate with the machine actively in good amount of visible light, e.g. as staring in camera. To overcome the disturbance due to movement of user, a tilt-and-pan camera can be used. Because of the cost of tilt-and-pan cameras, most current applications involve manual alignment of the eye with the camera (Yoon *et al.*, 2002).

At present, hand geometry is another biometric trait which is taken in to action to verify identicalness of an individual. The available hand geometry scanners (electro-mechanical) and devices (solid state electronic devices) use infrared optics and microprocessor technology for fast and efficient database creation and template matching. Selection of an affordable system is made on the basis of parameters such as low cost hardware, fast processing unit and solid state electronics which made it best suitable for commercial applications. In contrast to this, every individual has a unique hand. Parameters which are the basis of the hand geometry recognition are length of the finger, axes, finger shapes, height and angle, thickness, curvatures, and width of the hand. In hand geometry scanner, images of the human hand are projected on a background with the help of charge coupled device camera and an infrared light generating device. There is one side mirror and a reflector is also assembled in the system which helps in generating two distinct images of the hand. In addition to this, the projected images on the background give the information of hand's shape, which is then read by the scanner for the template creation.

Vein recognition system captures the radiated vein pattern when they are exposed to infrared rays. These system glances over the veins within the hand when placed few inches above the hand. When infrared rays projected over the hand they illuminate the veins pattern in such a way that the diffusion inside the vein can be captured easily. The process includes the deoxidization of the hemoglobin in the vein vessels so that they can absorb a high amount of the infrared rays. When it happens it reduces the reflection rate of the infrared rays thereby stimulating the veins to come out as a black pattern. These black patterns then are used to produce a digital template that constitutes a soul's unparalleled vein pattern. Furthermore, these sensors distinguish the patterns of different users if the deoxidized hemoglobin is flowing in an active manner inside the user's veins and helps in enabling a highly secure network.

The identification of any person on the basis of retinal scan is done with minimal human intervention which provides genuine recognition of the individual by evolving a choroid image with the cooperation of the user. Along with iris recognition systems, retinal identification has also found the act of bringing high security in various confidential areas, such as atomic research center, communication center and airbase, etc. In the process of feature extraction from choroid image of the retina the unique pattern of the blood vessels are checked. In a subsequent study of the feature extraction, have contributed. Though the subsequent study in the field of retinal recognition, there is not much exposed literature covering the systematic investigation issues underlying retina recognition based identity authentication; one of the literature presented by C. Simon and I. Goldstein (Simon *et al.*, 1935) is on the use of retinal images for identifying individual based on blood vessel patterns.

International Biometric Group (IBG) has conducted a test program to evaluate the market trend and share of all existing biometric technologies (Modi, 2008). This analysis presents the revenue of adoption of biometric technologies and applications from 2007-2012, which is illustrated in the Table 1.

Market size of the biometric technology is being incorporated by government and private organizations are growing inextricably. It is believed that till the end of 2012 the biometric market to grow from $3012 million USD in 2007 to $7407 million USD in 2012 (Figure 1, Modi, 2008).

3. Data Accretion Issues and Sensor Abrents

The recognition of multiple emotions, patterns and evidences in real-time, expressed spontaneously in an uncontrolled environment using biometric sensors, is not an easy task to achieve. Thus, it is always expected to get the motion artifacts when the sensor is not effective enough to detect emotions and evidences that may be expressed more subtly. Biometric reliability also varies among different technologies and manufacturers. The range is broad from low to high reliability and ultimately the biometric reliability is made up of accuracy and availability aspects. Due to the uniqueness, these embedded and specific biometric sensors are restrained from using the information generated by the other unique biometric sensors. These restriction stops the user to annex the raw information from the number of biometric sensor with different characteristics in a single machine. Thus, it is obvious that the need today is to develop such mechanism that is ingenious to operate on information generated from different sensor (Ross *et al.*, 2004).

In addition to data acquisition concern this is to realize that sensor module is also an antecedent component of the biometric enrollment system and the reliability of the sensor module depends upon the enrollment success rate. Hence, a biometric system that originates higher score for failure to acquire (FTA), failure to enroll (FTE), false acceptance rates (FAR) and false rejection rates (FRR), is not reliable (Bhattacharyya, 2009). Failure to enroll occurs due to invalid and indigent quality of the information or image. Therefore, a certain amount of the data input to the system is considered to be invalid. On the other hand the vulnerability of the system to detect the biometric characteristic refers to the FTA. FAR and FRR reveals the system performance and efficiency in terms of system's ability of identifying the genuine and neglecting the imposter. Along with these aberrant,

Table 1. Different biometric technologies and their market share.

Sr. No.	Technologies	Market share
1	AFIS/Live scan	33.60%
2	Vein recognition	3.00%
3	Voice recognition	3.20%
4	Middleware	5.40%
5	Face recognition	12.90%
6	Hand geometry	4.70%
7	Iris recognition	5.10%
8	Fingerprint (off-line)	25.30%
9	Other modalities	4.00%
10	Multiple traits	2.90%

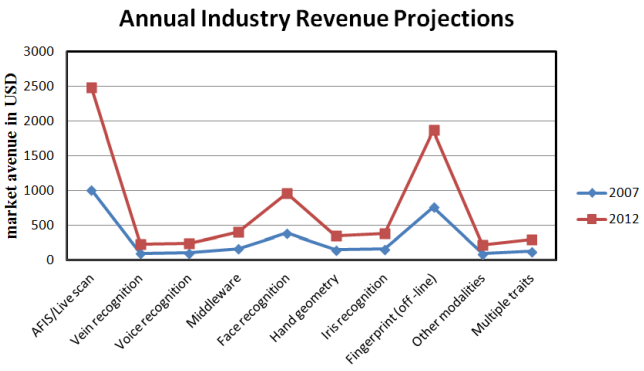

Figure 1. Annual industry revenue projections 2007-2012.

there are some other league issues which affect the sensor module.

3.1 Noisy data acquisition

While collecting the raw data from sensor, noise can occur in the acquired data mainly due to defective or improper placement of sensor. In finger print sensor if the residual of the previous scrutiny remains or there is an accumulation of the dirt on sensor, it can result in the noisy finger print image. Similarly, the unfavorable focus of the camera can lead to blurring the face and iris image. However authentication accuracy of the biometric sensor is highly dependent on the performance of the sensor and the quality of the evidences obtained from the sensor. The noisy data can result in a significant reduction in the accuracy of the biometric sensor (Chen *et al.*, 2005).

3.2 Non-universality

It is very rare to develop a system in which every person is able to present his biometric trait. If everyone in the target population is able to do this, then the trait is said to be universal. Truly not all the biometric traits are truly universal. According to a report presented by the National Institute of Standard and Technology (NSIT), it is difficult to obtain the good quality fingerprint, iris and face biometric trait from approximately 2-4% of the total population. People with very oily or dry finger, suffering from cataract, Entropion, etc. cannot provide good quality of images for automatic recognition (News BBC, 2011). Non-universality leads to the failure to enroll (FTE) and/or failure to capture (FTA) error in the system.

3.3 Lack of indistinctive representation

The generation of the biometric data during template creation and the data during verification may not be similar from the same person and same biometric system. This is known as "intra class variation". These changes in the data may occur due to the improper interaction of the user before the sensor. Due to some rotational and translational movement, the evidences obtained from face and iris may not be good enough for the recognition. The problem also occurs when user places his finger on the fingerprint sensor and applies extra pressure (Mordini *et al.*, 2009).

4. Sensor Endorsement and Spoof Attacks

Acceptance of the biometric technology is evaluated by usability and overall system performance. However cost, size, resolution and various error rates are the extraneous factor which plays a vital role while selecting a biometric sensor. In fact, sensors for numerous biometric traits have recently dropped under the $10-$1,000. So at the enterprise level due to the competition, cost is no war in the selection of the system, but the accuracy. Figure 2 shows the usability of different type of fingerprint sensor on the basis of the error rates (FTA and FTE) (Ohta *et al.*, 1985; Mansfield *et al.*, 2001).

Among all the types of fingerprint sensors shown in the Figure 2, thermal and piezoelectric sensors are considered to be low cost fingerprint sensors. On the other hand, optical sensors and ultrasound fingerprint sensors have a high degree of stability and reliability which ultimately results in a very precise and fraud-free result. The usability of the fingerprint sensor has been examined on the basis of FTE and FTA error rates. It is clearly shown in the Figure 2 that the piezoelectric sensors has around 2.6% FTE and 2.75% FTA, while on the other hand thermal sensors have around 1.7% of FTE and 1% FTA, which are highest in the category. The capacitive fingerprint sensor has 1.5% FTE and around 0.4% FTA, which distinctly explains the accuracy and preciseness of this type of sensors. The optical sensors are one of the most widely used sensors since they have a negligible amount of FTE and FTA as examined around 1% and 0.75% respectively. Furthermore, ultrasonic sensors have nearly same percentage of FTE and FTA of around 1% and are widely used in many commercial applications.

With fast and accurate results, face recognition biometric enjoy a more eminent rate of recognition and with a short processing speed which make these systems an effective authentication option. The ability to recognize human faces irrespective of changes of facial expression such as the gaining of a beard, mustache and glasses. Furthermore, these systems also can precisely recognize faces even if the face images are taken from various distances and under various lighting condition. Facial recognition biometrics has found a diverse field of applications, including access control, information security, law-break fighting, and more. All these benefits help in achieving low FTE and FTA, FAR of 0.0001 and an FRR of 0.001 or below it.

In order to record and compare the hand attributes, many electro-mechanical devices and solid state electronic scanners sensors uses the infrared optics and microprocessor technologies. Hand-geometry sensors can be used to greatest advantage over most of the target population,

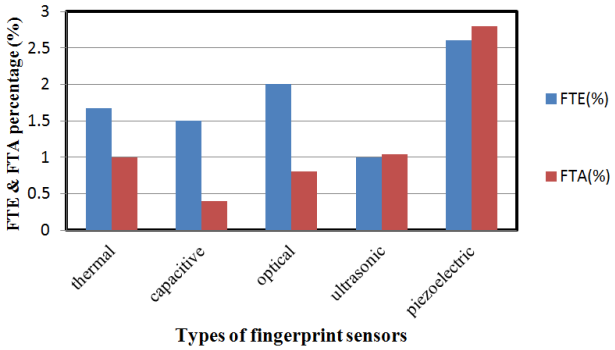

Figure 2. Usability of fingerprint sensors on the basis of FTA and FTE.

leaving some of the human being that endure from intense arthritic conditions. Therefore, hand-geometry devices exhibit relatively low FTE and FTA rates, when compared to other biometric devices. A novel report which studied the hand-geometry pattern of around 200 user demonstrated (Mansfield *et al.*, 2001) that the hand-geometry devices were having the lowest FTE and FTA rates among all the examined sensors (i.e., vein, voice, face, iris, fingerprint scanners and hand-geometry). But, when it comes to the security the false-acceptance rates (FAR) and false-rejection (FRR) rates for hand-geometry-based security systems are typically higher than those of face recognition, palmprint, retina or iris-based systems, which make hand-geometry devices suitable only for low/medium security applications. Various autonomous analyses (e.g., Holmes *et al.*, 1991; Kukula *et al.*, 2006; Mansfield *et al.*, 2001) presented that commercial hand-geometry sensors accomplish FAR and FRR rates in the range 0.1%-1.0% at the equal-error operating point.

The authentication solution which uses the vein pattern of a person offers an optimum level of security. Palmprint sensor observes the complex vein entity of the palm of the human hand with the extreme precision. These vein patters are registered by the sensing element and is lay aside for future use in a database, on an identity based badge or on a smart card. Furthermore, the identity of a person who is registered in implied time is identified on the basis of detected vein pattern when compared with the pattern template stored in the database of the same person. With the fact that every person has a radically distinctive structure and placement of veins in the palm of the hand which remain unchanged in the whole extent of the person's life. Palm-vein technology is in frequent use due their higher degree of preciseness which provides false rejection rate (FRR) below 0.01% and false acceptance rate (FRR) below 0.00008%.

As a result of searching the scope in other biometric modalities, iris biometric trait provides an unmatched identification solution. Due to its underlying advantages iris based biometric identification systems is benefitting a lot of attention. Hence iris is an internal organ which is kept safe from danger or injury against harm which differentiates it from other modalities such as fingerprint, which may get damage due to certain types of manual labor in due course of time. This characteristic of the iris trait helps in achieving lower FTE and FTA for the iris biometric sensor among all other biometric sensor. These systems has been implemented and tested using different number of algorithms on number of images of iris data with different lightening conditions and have produced the FAR below 0.000083 and FRR below 0.00001.

It is possible that some of the biometric traits can be stolen or lifted to be employed for illegal purpose by re-producing the fraudulent samples which can eventually be used to attack biometric systems. For instance, an equivalent copy or fake fingerprints can be generated using gum and gelatins which was then accepted as legal user by the system in (Matsumoto *et al.*, 2007). Although, many literature on fake fingerprint detection (Kim *et al.*, 2009) and other biometric have been suggested to prevent the spoof attack, but no method is completely facilitated yet. A brief detail of vulnerability of various biometrics against spoof attack is listed below in Table 2.

5. Performance and Quality Parameters

The selection of the sensor to work efficiently is made under the influence of environmental as well as tradeoff factors such as temperature, humidity, power consumption, sensing area, resolution, image quality, scan time, cost, etc.

5.1 Fingerprint

Fingerprint recognition systems are the very first and most preferable choice for the commercial identification or verification applications since they provide an adequate and accurate platform for a medium-scale recognition system. However, a number of manufacturers use multiple fingerprints of a user to render further information for a versatile fingerprint recognition system consisting of a large user capability. The limitations of the present fingerprint technologies are that they need a prominent add up of computational resources for the identification purpose. However, manufacturers of the fingerprint recognition system are developing the best ever identification tools while taking care of the problems of aging, environmental effects, and finger artifacts. Table 3 has been created using different fingerprint sensor from different manufacturers and the study shows that the accuracy and features of the sensors varies with the cost factor as well as with the manufacturers.

Table 2. Vulnerability of various biometrics against spoof attack.

Biometrics	Vulnerability to spoof attack	Spoofing techniques
Fingerprint	Highly Vulnerable	Gummy finger
Face	Moderately Vulnerable	Direct print attacks to unimodal 2-D (visual spectra)
Hand geometry	Lower Vulnerability	Plaster made fake handSilhouette images based Fake hand
Vein	Lower Vulnerability	Hill climbing attack
Iris	Lower Vulnerability	High resolution imageMicrolithography Iris Spoofing Attack
Retina	Lower Vulnerability	Hill-climbing attack

Table 3. Performance parameters of the various fingerprint sensors.

Sensors/Parameters	Cost	Temp.	Sensing area	Resolution	Recognition speed	FAR%	FRR%
CMA S20	$10	20 to 55°C	18 mm x 20 mm	500 dpi	250 ms	0.0001	<=1
FPR-100	$15	25 to 85°C	9.6 mm x 0.4 mm	508 dpi	<100 ms	<0.0001	<0.1
ZJ12	$35	-20 to 25°C	18 mm x 22 mm	500 dpi	250 ms	0.001	0.01
U.ARE.U4500	$66	0 to 40°C	14.6 mm x 18.1 mm	512 dpi	140 ms	0.001	1
WG Reader208 Model	$80	-10 to 75°C	19 mm x 12.8 mm	450 dpi	<200 ms	< 0.0001	<0.01
UPEK Eikon 500	$100	0 to 40°C	12.8 mm x 18 mm	508 dpi	500 ms	0.001	1
AET65	$115	0 to 50°C	9.6 mm x 0.2 mm	508 dpi	<500 ms	d”0.001	d”0.001
Marks 175 bio	$600	-10 to 50°C	15 mm x 18.1 mm	500 dpi	100 ms	0.001	0.1
Rflogics FINGER006 Slave	$840	-10 to 40°C	13 mm x 15.2 mm	500 dpi	30 ms	0.001	0.1

Table 4. Performance parameters of the various facial recognition sensors.

Sensors/ Parameter	Cost	Temp	Resolution	Recognition Speed	FAR%	FRR%
Face IDF710	$807	0 to 40°C	320 x 240	<1 sec	<0.001	<1
Wiface 300	$507	0 to 45°C	320 x 240	<=2 sec	<=0.0001	<=1
iface201	$268	0 to 45°C	512 dpi	<2 sec	<0.0001	<1
Zks-f20	$127	-30 to 55°C	640 x 480	<=2 sec	<0.01	<1
HF-FR213	$ 359	-20 to 45°C	320 x 240	<=1 sec	0.01	<=1
Comet-face4000	$120	-20 to 55°C	640 x 480	<=1 sec	<=1	<=0.1
C-FK605	$220	0 to 40°C	800 x 600	<=1 sec	<0.0001	<=1

5.2 Face

The accuracy of face recognition systems may vary from one system to another, which may be declared on the basis of various parameters and algorithms used. Although, every face recognition system has its own degree of freedom of identifying the person, but the distinction between them can be made on the basis of accuracy and error rates. Furthermore, face recognition technologies are changing rapidly; hence a wide range of product is available in the market. In Table 4, we have collected the recent information about the various face recognition systems on the basis of cost, environment effects and few error rates and have checked company literature and industry reports.

5.3 Iris

Unparalleled attributes of the iris encourage the various manufacturers to design a highly robust and precise system. It is very beneficial for the manufacturers to know that contrived implementation of the iris is almost insufferable because the iris is directly associated with the brain and it is believed that iris is one of the parts of the body which decompose first after the death. The level of performance of all iris recognition systems is not same for every application. As the performance of iris recognition system depends on the kind of application, so it is very significant to acknowledge how the iris recognition system performs relatively. In the following Table 5, we have studied some comparison

Table 5. Performance parameters of the various iris recognition sensors.

Sensors/ Parameter	Cost	Temp	Resolution	Recognition Speed	FAR%	FRR%
IG-AD100	$1,945	0 to 40°C	800 x 600	<4 sec	0	0
Iris Pass-M	$3,000	0 to 40°C	300 dpi	<1 sec	0.000083	0.01
Iris ROU 2200	$316.25	0 to 40°C	800 x 600	1-2 sec	0	0.00001
BM-ET330	$2,137.5	0 to 40°C	1024 x 768	1.5 sec	0.001	0.01
Iris ID iCAM TD100	$2,699	0 to 50°C	1600 x 1200	<2 sec	<0.0001	<0.01
CLG7600	$135	-40 to 60°C	600 x 650	0.5-1.2 sec	0.001	0.01

results for various iris recognition systems on the basis of cost, environment effects and few error rates.

5.4 Hand geometry

A number of hand geometry recognition systems subsist and are in use for various applications. Each hand geometry recognition system has its effectiveness and weak points, and the alternative depends upon the application. Even the most desirable system cannot anticipate to accurately accomplishing the demands of all the applications. The comparison among various recognition systems is figured out on the basis of functional mode of the application and the properties of hand geometry. A brief comparative study of the commonly used hand geometry recognition systems on the basis of cost, environment effects and few error rates is given in Table 6.

5.5 Vein

The geometry of the veins depicts a pattern which is distinctive for most individuals. The vein geometry is still in the phase of research and development. Vein recognition biometrics is in particular, an impressive and assuring technology since it demands only a single-chip design, leading to the units that are comparatively small and cheap. The ID verification process in vein recognition is relatively fast and contact-less which encourages the manufacturers to develop the compact and robust designs. The vein pattern can be detected, captured and subsequently verified, using a light-transmission technique. Since the vein recognition has great potential, it may be the leading biometric technology in the world. In the Table 7 given below, we have a selection of sensors to make a comparative study for best suitable vein recognition system on the basis of cost, environment effects and few error rates.

5.6 Retina

The process of automatic feature extraction for biometric traits other than retina seems easy with the advent of numerous sensors. But the efforts that have been made for the feature extraction and recognition purposes have found their application more in software field than in hardware (sensors) due to abnormal structures of retinal images. However, few retinal scanners have been evolved in order to provide an incorporated platform that unwinds the complexity of authentication and abidance risk management for the dynamic enterprise. A brief detail of some of the work done in the field of retinal image analysis is shown in the Table 8.

6. Conclusion

Thanks to the current advancement in the biometric market which is providing the innovative, secure and highly precise sensor technologies with high acceptability among users. In fact, biometric systems can make the promising growth, if the technologies and ingress procedure of sensing the data are not restrained by the numerous errors as explained above. Therefore, the sensor management problem is directly related to the sensor mode selection, sensor's data acquiring ability and somehow on their cost tradeoffs. Since, variedness of these parameters for different vendor under different costs range is significant, and hence on one hand if they are very admirable, they also affect the accuracy. The objective of minimizing the error rates and increasing the accuracy depends upon the feedback and various conditions.

Table 6. Performance parameters of the various Hand geometry recognition sensors.

Sensors/ Parameter	Cost	Temp	Resolution	Recognition Speed	FAR%	FRR%
Handkey CR HG4-PROX	$2,710.0	32 to 13°C	960 x 640	<1 sec	0.1	0.1
TW-ATH-1000	Approx. $1,300	-10 to 60°C	500 dpi	<1 sec	0.001	0.1
GT-400	$2,369	0 to70°C	240 x 400	<1 sec	<0.0001	<0.01
HP-4000	$1,365	0 to 45°C	1,200 dpi	<1 sec	<0.001	<0.1
Handkey-II	$1,799.9	-10 to 60°C	640 x 480	<1 sec	0.08	0.98

Table 7. Performance parameters of the various vein recognition sensors.

Sensors/ Parameter	Cost	Temp	Resolution	Recognition Speed	FAR%	FRR%
PV1000	$960	0 to 40°C	500 dpi	<1 sec	0.00008	0.01
K32lite	Approx. $700	0 to 50°C	1,024 x 768	2-4 sec	0.00008	0.01
XMP-TMC2801-PV	$560	-20 to 70°C	640 x 480	1.5 sec	0.00008	0.01
M2-PV	$499.9	-20 to 70°C	500 dpi	2 sec	<=0.00008	<=0.01
PVG102-C	$1,400	-15 to 60°C	500 dpi	2 sec	<=0.00008	<=0.01
Xceltech-101	$2,000-2,500	0 to 60°C	352 x 288	1 sec	<=0.0000008	<=0.00001

Table 8. Performance parameter of the various retina recognition sensors.

Sensors/ Parameter	Cost	Temp	Resolution	Recognition Speed	FAR%	FRR%
Retina Scan PCMCIA Card	$169.99	0 to 50°C	600 dpi	<1.5 sec	<0.000001	<0.00001
Eyedentification 7.5 scanner	$299	-10 to 35°C	1,040 dpi	2 sec	0.000001	0.00001
ICAM 2001	$170	0 to 45°C	640 x 480	<1.5 sec	0.0000001	0.00001
LLC Retinal	$50	0 to 40°C	320 x 240	2 sec	0.00001	0.00001
Canon Hybrid Mydriatic	App. $599	10 to 35°C	1,600 x 1,200	<1sec	<0.0000001	<0.00001

In order to predict users mind for the credence of new technologies and services, manufacturers are required to go through the market surveys and research studies. Systematic investigation of biometric sensors market distinctly evidences every biometrics device has its own set of quality of being able to provide good services, therefore we need to set up unfavorable environmental conditions for errors.

7. References

Bhattacharyya D., Ranjan,R., Alisherov, F.A. and Choi, M. 2009. Biometric Authentication: A Review. International Journal of u- and e- Service, Science and Technology. 2, 13-28.

Borgen, H., Bours, P. and Wolthusen,S.D. 2008. Visible-Spectrum Biometric Retina Recognition. In the Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, China, August 15-17, 2008, 1056-1062.

Chen, Y., Dass, S.C. and Jain, A.K. 2005. Fingerprint quality indices for predicting authenticating performance. In Proceedings of the fifth international conference on audio and video based biometric person Authentication (AVBPA), New York, USA, July 17, 2005, 160-170.

Cyberware 2011, http://www.cyberware.com/products/scanners/desktop.html. [November 25, 2011]

Etienne-Cummings, R., Spiegel, V.D.J., Donham, C., Fernando, S., Hathaway, R., Mueller, P., Van der S.J., Donham, C., Fernando, S., Hathaway, R., Mueller, P. and Blackman, D. 1993. A General Purpose Analog Neural Computer and a Silicon Retina for Real Time Target Acquisition, Recognition and Tracking. In proceedings of International Conference on Computer Architectures for Machine Perception. New Orleans, *Louisiana*, USA., December 15-17, 1993, 48-57.

Fingerchip. 2011. http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint_sensors_productsi.htm. [November 23, 2011].

Holmes, J.P., Wright, L.J. and Maxwell, R.L. 1991. A Performance Evaluation of Biometric Identification Devices. Sandia National Laboratories, Report, U.S.A., 1991, 1-27.

Islam, M. N., Siddiqui M. A. and Paul Samiron. 2009. An Efficient Retina Pattern Recognition Algorithm (RPRA) towards Human Identification. In the Proceedings of 2nd International Conference on Computer, Control and Communication, Khulna, Bangladesh, February 17-18, 2009, 1-6.

Jain, A.K., Ross, A. and Prabhakar, S. 2004. An introduction to biometric recognition. Institute of Electrical and Electronic Engineers Transaction on Circuits and Systems for Video Technology, 14, 4–20.

Kim, Y. Na, J. Yoon S. and Juneho Y. Masked Fake Face Detection using Radiance Measurements. Journal of Optical Society of America. 2009, 26 (4), 760-766.

Kukula, E. and Elliott, S. 2006. Implementation of Hand Geometry: An Analysis of User Perspectives and System Performance. Institute of Electrical and Electronic Engineers Aerospace and Electronic Systems Magazine. 21(3), 3–9.

Latha , L., Pabitha, M. and Thangasamy, S. 2010. A Novel Method for Person Authentication using Retinal Images. In the Proceedings of International Conference on Innovative Computing Technologies, Tamil nadu, India, February 12-13, 2010, 1-6.

Mansfield, T., Kelly, G., Chandler, D. and Kane, J. 2001. Biometric Product Final Report, CES contract X92A/4009309, Centre for Mathematics and Scientific Computing, National Physical Laboratory, 1, 1-22.

Matsumoto, T., Matsumoto H., Yamada, K. and Hoshino, S. Impact of Artificial Gummy Fingers on Fingerprint Systems. In Proceedings of the SPIE on Optical Security and Counterfeit Deterrence Tech. IV. Czech Republic December 21, 2007, 275-289.

Modi, S.K. 2008. Analysis of fingerprint sensor interoperability on system performance, Center for Education and Research in Information Assurance and Security, Purdue University, 1, 1-189.

Mordini, E., Wright, D., Hert, P.D., Mantovani, E., Wadhwa, K.R., Thestrup, J. and Steendam, G.V. 2009. Ethics, e-Inclusion and Ageing. Studies in Ethics, Law, and Technology, Mendeley publications, 11, 203-220.

News BBC 2011. BBC news long lashes thwart ID scan trial. http://news.bbc.co.uk/2/hi/uk_news/politics/3693375.stm [December 10, 2011].

O'Gorman, L. 2003. Comparing Passwords, Tokens, and Biometrics for User Authentication. In Proceedings of Institute of Electrical & Electronic Engineers, Avaya Labs., Basking Ridge, NJ, U.S.A., December 21-23, 2003, 2021–2040.

Ohta, Y. and Kanade, T. 1985. Stereo by intra and inter scan line search using dynamic programming. Institute of Electrical & Electronic Engineers Transaction on Pattern Analysis and Machine Intelligence, 7, 139-154.

Palomera-P´erez, M.A., Martinez-Perez, M.E., Ben´ýtez-P´erez, H. and Ortega-Arjona, J.L. 2009. Parallel Multi-scale Feature Extraction and Region Growing: Application in Retinal Blood Vessel Detection. Institute of Electrical and Electronic Engineers Transaction Transactions on Information Technology in Biomedicine.14, 500-506.

Pouyan, A.A., Naseri, A. and Kavian, N. 2010. An Image Processing Technique to Detecting Retina Layers. In the proceedings of the International conference on Signal and Image Processing (ICSIP). Chennai, India, December, 15-17, 2010, 7-10.

Ross, A. and Jain, A. 2004. Biometric Sensor Interoperability: A Case Study in Fingerprints. In Proceedings of International ECCV Workshop on Biometric Authentication (BioAW), Prague, May 2004, 134-145.

Simon, C. and Goldstein, I.1935. A New Scientific Method of Identification. New York State Journal of Medicine, 35, 901-906.

Sutcu, Y., Rane, S., Yedidia, J.S., Draper, S.C. and Vetro, A. 2008. Feature Transformation of Biometric Templates for Secure Biometric Systems based on Error Correcting Codes. In Proceedings of Institute of Electrical and Electronic Engineers Computer Society Conference on Computer Vision and Pattern Recognition, Cambridge, Massachusetts, U.S.A, October 31, 2008, 1-6.

Weiland, J.D. and Humayun, M.S. 2005. A biomimetic retinal stimulating array. Institute of Electrical and Electronic Engineers Transaction on Engineering in Medicine and Biology Magazine, 24, 14 - 21.

Yoon, S., Jung, H.G., Park, K.R. and Kim, J. 2009. Nonintrusive iris image acquisition system based on a pan-tilt-zoom camera and light stripe projection. International Journal of Image and Graphics, 48, 037202-1-037202-15.

Zhan, X., Meng, X., Yin, Y. and Yang, G. 2008. A Method Combined on Multi-Level Factors for Fingerprint Image Quality Estimation. In Proceedings of Fifth International Conference on Fuzzy Systems and Knowledge Discovery, Washington, DC, U.S.A., October 18-20, 2008, 31-36.