INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2774 - 2784
RECEIVED : 05.02.2018 PUBLISHED : 02.03.2018
March 02, 2018

# SMART CARD BASED BIOMETRIC SECURITY INNOVATIONS

[1]S.Girija, P.G.Scholar, Department of MCA, Ganadipathy Tulsi's Jain Engineering College, Vellore, Tamilnadu, India.

[2]J.Kaviya, P.G.Scholar,Department of MCA,Ganadipathy Tulsi's Jain Engineering College,Vellore,Tamilnadu,India.

[3]A.Appandairaj, Asst.Prof,Department of MCA, Ganadipathy Tulsi's Jain Engineering College,Vellore,Tamilnadu,India.

**Abstract**

This paper presents biometric authentication techniques and actual deployment potential, together with an independent testing of various biometric authentication products and technologies. Security is the critical issue in a customary life. Different surprising state industry utilizes biometric security for confirmation of their workers, for example, iris, thumb, confront and so forth.

**Index terms:** biometrics, fingerprint technologies, iris, retina, hand geometry, signature dynamics, face recognition.

## 1. INTRODUCTION

Individuals see each different as demonstrated by their distinctive characteristics for quite a while. We recollect that others by their face when we meet them and by their voice as we address them. Character check (approval) in PC systems has been usually in perspective of something that one has (scratch, alluring or chip card) or one knows (PIN, watchword). Things like keys or cards, nevertheless, tend to get stolen or lost and passwords are routinely ignored or revealed. To achieve more strong affirmation or recognizing verification we ought to use something that really depicts the given person. Biometrics offer motorized methodologies for identity affirmation or ID on the rule of quantifiable physiological or behavioral properties, for instance, a one of a kind finger impression or a voice test. The traits are quantifiable and stand-out. These characteristics should not be duplicable, but instead it is disastrously frequently possible to make a copy that is recognized by the biometric structure as a bonafide case. This is basic where the level of security gave is given as the measure of money the impostor needs to get an unapproved get to.For this circumstance the customer's biometric data is facilitated against each one of the records in the database as the customer can be anywhere in the database or he/she actually does not have to be there at all. It is evident that identification is technically more challenging and costly. Identification accuracy generally decreases as the size of the database grows. For this reason records in large databases are categorized according to a sufficiently discriminating characteristic in the biometric data.Subsequent searches for a particular record are searched within a small subset only. This lowers the number of relevant records per search and increases the accuracy (if the discriminating characteristic was properly chosen). Before the user can be successfully verified or identified by the system, he/she must be

registered with the biometric system. User's biometric data is captured, processed and stored. As the quality of this stored biometric data is crucial for further authentications, there are often several (usually 3 or 5) biometric samples used to create user's master template. The process of the user's registration with the biometric system is called **enrollment.**

***What to quantify?***

Most critical distinction amongst biometric and conventional advances lies in the appropriate response of the biometric framework to a confirmation/recognizable proof demand. Biometric frameworks don't give basic yes/no answers. While the secret key either is 'abcd' or not and the card PIN 1234 either is substantial or not, no biometric framework can check the character or recognize a man completely. The individual's mark never is totally indistinguishable and the position of the finger on the unique mark peruser will differ also. Rather, we are told how comparative the current biometric information is to the record put away in the database. Along these lines the biometric framework really says what is the likelihood that these two biometric tests originate from a similar individual. Biometric advances can be separated into 2 noteworthy classes as indicated by what they measure:

*Devices in light of physiological attributes of a man, (for example, the unique mark or hand geometry).

*Systems in light of behavioral attributes of a man, (for example, signature progression).

Biometric frameworks from the primary class are typically more dependable and precise as the physiological attributes are less demanding to rehash and frequently are not influenced by current (mental) conditions, for example, push or sickness. One could construct a framework that requires a 100% match each time. However such a framework would be for all intents and purposes pointless, as just not very many clients (assuming any) could utilize it. The majority of the clients would be dismissed constantly, in light of the fact that the estimation comes about never are the same. We need to take into account some fluctuation of the biometric information all together not to dismiss an excessive number of approved clients. Notwithstanding, the more noteworthy changeability we permit the more prominent is the likelihood that an impostor with a comparative biometric information will be acknowledged as an approved client. The fluctuation is as a rule called a (security) edge or a (security) level. In the event that the fluctuation permitted is little then the security edge or the security level is called high and on the off chance that we take into account more noteworthy inconstancy then the security edge or the security level is called low.

## 2. BIOMETRIC TECHNIQUES

There are loads of biometric systems open nowadays. Several them are in the period of the investigation just (e.g. the scent examination), yet a basic number of advancements is starting at now create and modernly open (no under ten one of a kind sorts of biometrics are monetarily available nowadays: exceptional check, finger geometry, hand geometry, palm print, iris outline, retina plan, facial affirmation, voice relationship, signature stream and composing musicality).

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2774 - 2784
RECEIVED : 05.02.2018 PUBLISHED : 02.03.2018
March 02, 2018

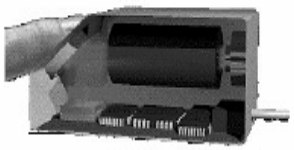
*A. Interesting imprint developments*

Interesting imprint ID is possibly the most settled of all the biometric strategies. Fingerprints were used starting at now in the Old China as a techniques for vehemently recognizing a man as a maker of the report. Their use in law usage since the latest century is striking and truly let to an alliance one of a kind check =crime. This caused a couple of worries over the customer affirmation of special check based systems. The condition upgrades as these systems spread around and end up being more run of the mill.

***Interesting imprint perusers***

Before we can proceed with any further we need to get the digitalized interesting imprint. The standard procedure uses the ink to get the one of a kind stamp onto a touch of paper. This bit of paper is then inspected using a customary scanner. This strategy is used just sometimes today when an old paper-based database is being digitalized, a one of a kind check found on a scene of a bad behavior is being readied or in law necessity AFIS systems.

For the most part show day live one of a kind finger impression perusers are used. They don't require the ink any more. These live exceptional finger impression perusers are most typically in light of optical, warm, silicon or ultrasonic gauges. Optical special stamp perusers are the most understood at present. They rely upon reflection changes at the spots where the finger papilar lines touch the perusers surface. The measure of the optical one of a kind check perusers frequently is around 10X10X5 centimeters. It is difficult to confine them significantly more as the peruser needs to incorporate the wellspring of light, reflection surface and the light sensor.



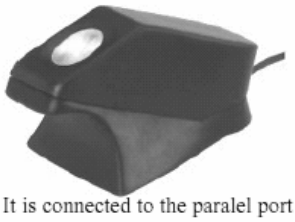
Source: I/O Software [6]
All the optical fingerprint readers comprise of the source of light, the light sensor and a special reflection surface that changes the reflection according to the preassure. Some of the readers are fitted out with the processing and memory chips as well.

The optical one of a kind stamp perusers work typically reliably, however generally have issues with clean if strongly used and not cleaned. The clean may cause latent fingerprints, which may be recognized by the peruser as a honest to goodness one of a kind finger impression. Optical one of a kind stamp perusers can't be deceived by an essential photograph of a finger impression, however any 3D remarkable stamp exhibit makes an immense issue, all the peruser checks is the weight. Two or three perusers are in this way equipped with additional locators of finger liveness.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2774 - 2784
RECEIVED : 05.02.2018 PUBLISHED : 02.03.2018
March 02, 2018

This is a fingerprint bitmap obtained by an optical fingerprint reader (Securetouch 99 manufactured by the Biometric Access Corporation)

Optical perusers are for the most part decrepit and are created by a great number of creators. The field of optical advances attracts various as of late settled firms (e.g., American Biometric Company, Propelled Persona) and what's more two or three huge and clearly comprehended associations, (for instance, HP, Philips or Sony). Optical exceptional finger impression perusers are also much of the time introduced in consoles, mice or screens. Both optical and silicon extraordinary stamp perusers rush to catch and demonstrate the one of a kind check persistently. The conventional assurance is around 500 DPI.



Source: ABC [1]
This is an example of the optical fingerprint reader. The "Biomouse Plus" integrated with a smart card reader is able to capture the fingerprint at 500 DPI. It is connected to the paralel port of a computer and costs between $100 and $200.

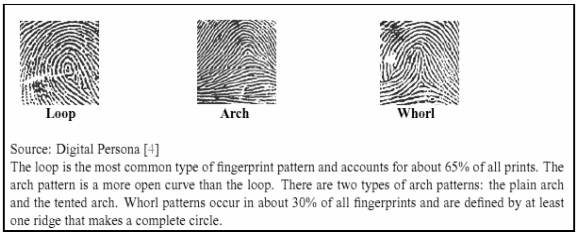
Ultrasonic exceptional stamp perusers are the most present and smallest typical. They use ultrasound to screen the finger surface. The customer puts the finger on a touch of glass and the ultrasonic sensor moves and examines whole the one of a kind stamp. This technique takes perhaps a few seconds. Ultrasound isn't annoyed by the dirt on the fingers so the idea of the bitmap obtained is regularly sensible. Ultrasonic remarkable check perusers are made by a single association nowadays.

Source: UltraScan [17]
This is an example of a fingerprint bitmap image obtained by an ultrasonic fingerprint reader. This image was obtained using the Model 703 ID Station at 250 DPI.

***Fingerprint processing***

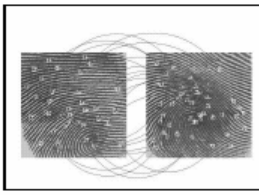
Novel stamp dealing with Fingerprints are not taken a gander at and generally also not set away as bitmaps. One of a kind check organizing methodology can be put into two classes: particulars based and relationship based. Particulars based strategies find the points of interest concentrates first and after that guide their relative circumstance on the finger. Particulars are solitary stand-out characteristics inside the one of a kind stamp case, for instance, edge endings, bifurcations, divergences, spots or islands (see the photograph on the going with page). In the present years electronic one of a kind stamp relationships have been routinely in light of points of interest. The issue with particulars is that it is difficult to remove the

subtle elements concentrates unequivocally when the one of a kind finger impression is of low quality. This procedure in like manner does not think about the overall case of edges and wrinkles. The association based system can vanquish a bit of the inconveniences of the particulars based approach. In any case, it has some of its own deficiencies. Relationship based techniques require the correct region of an enlistment point and are impacted by picture translation and insurgency. The clarity of a remarkable finger impression depends upon a combination of work and normal components. These join age, sex, occupation and race. A young, female, Asian digger is seen as the most troublesome subject. A shockingly high degree of the masses have missing fingers, with the left pointer having the most hoisted rate at 0.62%.




Source: Digital Persona [4]
The loop is the most common type of fingerprint pattern and accounts for about 65% of all prints. The arch pattern is a more open curve than the loop. There are two types of arch patterns: the plain arch and the tented arch. Whorl patterns occur in about 30% of all fingerprints and are defined by at least one ridge that makes a complete circle.

There are around 30 points of interest inside an ordinary one of a kind check picture obtained by a live novel stamp peruser. The FBI has shown that no two individuals can have more than 8 essential particulars. The U.S. Court structure has allowed affirmation in light of 12 organizing particulars. The number and spatial spread of particulars moves as demonstrated by the idea of the one of a kind finger impression picture, finger weight, moistness and course of action. In the decision technique, the biometric structure tries to find a particulars change between the present scattering and the set away configuration. The organizing decision is then in perspective of the probability and multifaceted nature of the key change. The decision generally takes from 5 milliseconds to 2 seconds. The speed of the decision all over depends upon the security level and the negative answer consistently take longer time than the positive one (as a less than dependable rule even 10 times more). There is no prompt dependence between the speed and precision of the organizing figuring as demonstrated by our experience. We have seen speedy and correct and likewise direct and less exact organizing estimations.



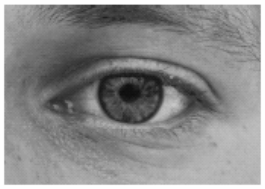
Source: PRIP MSU [11]
The minutiae matching is a process where two sets of minutiae are compared to decide whether they represent the same finger or not.

The particulars found in the one of a kind check picture are moreover used to store the interesting imprint for future connections. The particulars are encoded¶and every now and again furthermore stuffed. The measure of such an ace format generally is between 24 bytes and one kilobyte. Fingerprints contain a considerable measure of data. By virtue of the irregular condition of data display in the photo, it is possible to execute false matches and lessening the amount of possible matches to a little segment. This suggests the extraordinary finger impression advancement can be used for recognizing evidence even inside tremendous databases.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2774 - 2784
RECEIVED : 05.02.2018 PUBLISHED : 02.03.2018
March 02, 2018

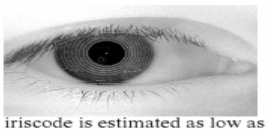
*B. Iris*

The iris is the hued ring of finished tissue that encompasses the understudy of the eye. Indeed, even twins have diverse iris examples and everybody's left and right iris is extraordinary, as well. Research demonstrates that the coordinating precision of iris recognizable proof is
more noteworthy than of the DNA testing.

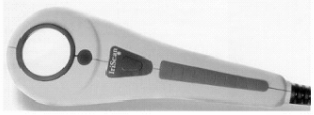


Each iris is a unique structure featuring a complex pattern. This can be a combination of specific characteristics known as corona, crypts, filaments, freckles, pits, furrows, striations. and rings.

The iris design is taken by a unique dim scale camera out yonder of 10– 40 cm from the camera (prior models of iris scanners required nearer eye situating). The camera is taken cover behind a mirror, the client investigates the mirror so he/she can see his/her own particular eye, at that point additionally the camera can "see" the eye. Once the eye is steady (not moving too quick) and the camera has concentrated legitimately, the picture of the eye is caught (there exist additionally less complex adaptations without self-adjust and with a catch).



Source: Iridian Technologies [7]
The iriscode is computed very fast and takes 256 bytes. The probability that 2 different irises could produce the same iriscode is estimated as low as $1 : 10^{78}$ The probability of two persons with the same iris is very low ($1 : 10^{52}$).



Source: Iridian Technologies [7]
The PC iris uses a hand-held personal iris imager that functions as a computer peripheral. The user holds the imager in his hand, looks into the camera lens from a distance of 10 cm and presses a button to initiate the identification process. The Iris Access is more advanced. It is auto-focus and has a sensor that checks whether an individual has stepped in front of the camera. It is also able to guide the person audily into the correct position.

The iris scanner does not require any extraordinary lighting conditions or any uncommon sort of light (not at all like the infrared light required for the retina filtering). On the off chance that the 7 foundation is excessively dull any customary lighting can be utilized. Some iris scanners additionally incorporate a wellspring of light that is consequently turned on when fundamental. The iris examining innovation isn't meddling and in this way is regarded satisfactory by generally clients. The iris design stays stable over a man's life, being just influenced by a few sicknesses. Once the dark scale picture of the eye is acquired then the product tries to find the iris inside the picture. On the off chance that an iris is discovered then the product makes a net of bends covering the iris. In light of the murkiness of the focuses along the lines the product makes the iris code, which portrays the iris. When registering the iris code two impacts must be considered. To start with, the general obscurity of the picture is impacted by the lighting conditions so the dimness edge used to choose whether a given point is dim or brilliant can't be static, it must be

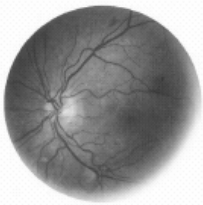
progressively figured by the general picture obscurity. What's more, second, the extent of the iris powerfully changes as the span of the understudy changes. Before processing the iris code, a legitimate change must be finished. In the choice procedure the coordinating programming given 2 iris codes figures the Hamming separation in light of the quantity of various bits. The Hamming separation is a score (inside the range 0 – 1, where 0 implies a similar iris codes), which is then contrasted with the security edge with settle on a ultimate conclusion. Processing the Hamming separation of two iris codes is quick (it is in speed truth just including the quantity of bits the restrictive OR of the two iris codes). Present day PCs can look at more than 4 000 iris codes in a single second. An iris filter creates a high information volume which suggests a high segregation (distinguishing proof) rate. For sure the iris frameworks are appropriate for recognizable proof since they are quick and precise. Our experience affirms all that. The iris acknowledgment was the speediest distinguishing proof out of all the biometric frameworks we could work with. We have never experienced a false acknowledgment (the database was not expansive, in any case) and the false dismissal rate was sensibly low. The maker cites the equivalent mistake rate of 0.00008%, however so low false dismissal rate isn't achievable with ordinary (non-proficient) clients. It is said that manufactured duplication of the iris is for all intents and purposes unthinkable as a result of the one of a kind properties. The iris is firmly associated with the human mind and it is said to be one of the initial segments of the body to rot after death. It ought to be along these lines extremely hard to make a manufactured iris or to utilize a dead iris to deceitfully sidestep the biometric framework if the discovery of the iris liveness is working appropriately. We were trying an iris examining framework that did not have any countermeasures actualized. We tricked such a framework with an extremely straightforward assault. The maker furnished us with a more up to date form of the framework following a while. We didn't prevail with our basic assaults at that point, yet we wish to take note of that we didn't have enough time to test further developed variants of our attack.A single organization (Iridian Technologies, Inc.) holds only all the overall licenses on the iris acknowledgment idea. The innovation was developed by J. Daugman of Cambridge University and the main iris filtering frameworks were propelled in 1995.


Source: Iridian Technologies [7]. Sensar used to be the only licensee, that used the iris recognition process in the financial sector. It signed agreements with ATM manufacturers and integrated its iris regognition products into ATMs. Such ATMs do not require bank cars anymore, the system identifies customers automatically. In 2000 Iriscan, Inc. merged with Sensar, Inc. and changed its name to Iridian Technologies, Inc.

*C. Retina*

Retina check depends on the vein design in the retina of the eye. Retina filter innovation is more seasoned than the iris examine innovation that additionally utilizes a piece of the eye. The primary retinal filtering frameworks were propelled by EyeDentify in 1985. The primary downside of the retina filter is its meddling. The technique for getting a retina examine is by and by intrusive. A laser light should be coordinated through the cornea of the eye. Additionally the activity of the retina scanner isn't simple. A talented administrator is required and the individual being examined needs to take after his/her headings.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2774 - 2784
RECEIVED : 05.02.2018 PUBLISHED : 02.03.2018
March 02, 2018



Source: EyeDentify [5]
Retina is not directly visible and so a coherent infrared light source is necessary to illuminate the retina. The infrared energy is absorbed faster by blood vessels in the retina than by the surrounding tissue. The image of the retina blood vessel pattern is then analyzed for characteristic points within the pattern. The retina scan is more susceptible to some diseases than the iris scan, but such diseases are relatively rare.

A retina examine creates in any event an indistinguishable volume of information from a unique finger impression picture. Subsequently its separation rate is adequate for check, as well as for distinguishing proof. In the training, in any case, the retina 8 checking is utilized for the most part for confirmation. The measure of the eye signature layout is 96 bytes. The retinal checking frameworks are said to be extremely precise. For instance the EyeDentify's retinal filtering framework has reputedly never erroneously confirmed an unapproved client up until now. The false dismissal rate, on the opposite side, is moderately high as it isn't generally simple to catch an ideal picture of the retina. Retinal examining is utilized just once in a while today since it isn't easy to use and still stays extremely costly. Retina filter is reasonable for applications where the high security is required and the client's acknowledgment isn't a noteworthy viewpoint. Retina check frameworks are utilized as a part of numerous U.S. penitentiaries to confirm the detainees previously they are discharged. The check of the eye liveness is normally not of a critical worry as the strategy for acquiring the retina vein design is fairly confused and requires an administrator.

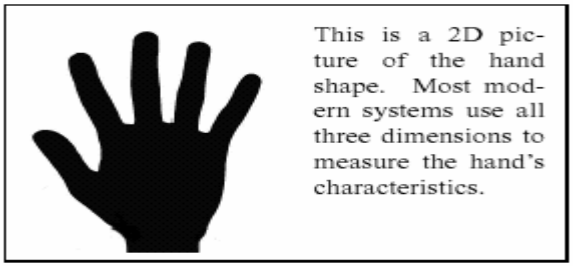
Source:
EyeDentify [5]
The company EyeDentify is the only producer of the retinal eye scanners. It has been founded in the late seventies and since then has developped a number of retina scanners. The current model 2001 is equipped with the memory for 3300 templates and (after the image has been captured) is able to verify an individual in 1.5 seconds or run an identification (withing the stored 3000 templates) in less than 5 seconds.

*D. Hand Geometry*

Hand geometry depends on the way that almost every individual's hand is molded contrastingly and that the state of a man's hand does not change after specific age. Hand geometry frameworks create appraisals of specific estimations of the hand, for example, the length and the width of fingers. Different techniques are utilized to quantify the hand. These techniques are most ordinarily construct either in light of mechanical or optical guideline. The last ones are significantly more typical today. Optical hand geometry scanners catch the picture of the hand and utilizing the picture edge identification calculation figure the hand's attributes. There are fundamentally 2 subcategories of optical scanners. Gadgets from the primary class make a highly contrasting bitmap picture of the hand's shape. This s effectively done

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2774 - 2784
RECEIVED : 05.02.2018 PUBLISHED : 02.03.2018
March 02, 2018

utilizing a wellspring of light and a high contrast camera. The bitmap picture is then handled by the PC programming. Just 2D qualities of the hand can be utilized as a part of the case. Hand geometry frameworks from the other class are more modern. They utilizes uncommon guide markings to position the hand better and have two (both vertical and level) sensors for the hand shape estimations. Along these lines, sensors from this class handle information from all the three measurements.




Hand geometry scanners are anything but difficult to utilize. Where the hand must be set precisely, direct markings have been fused and the units are mounted with the goal that they are at an agreeable tallness for larger part of the populace. The clamor factors, for example, soil and oil don't represent a difficult issue, as just the outline of the hand shape is essential. The main issue with hand geometry scanners is in the nations where people in general don't care to put their hand down level on a surface where another person's hand has been set. A couple of hand geometry scanners create just the video motion with the hand shape. Picture digitalization and handling is then done in the PC. On the opposite side there exist exceptionally modern and computerized scanners that do everything without anyone else including the enlistment, information stockpiling, confirmation and even basic systems administration with a ace gadget and numerous slave scanners. The span of a run of the mill hand geometry scanner is impressively huge (30 ∨ 30 ∨ 50 cm). This is generally not an issue as the hand geometry scanners are ordinarily utilized for physical access control (e.g. at an entryway), where the size isn't a urgent parameter.

*E. Facial Recognition*

Facial acknowledgment is the most regular methods for biometric recognizable proof. The strategy for recognizing one individual from another is a capacity of for all intents and purposes each human. As of not long ago the facial acknowledgment has never been dealt with as a science. Any camera (with an adequate determination) can be utilized to acquire the picture of the face. Any filtered picture can be utilized too. As a rule the better the picture source (i.e. camera or scanner) the more exact outcomes we get. The facial acknowledgment frameworks for the most part utilize just the grayscale data. Hues (if accessible) are utilized as an assistance in finding the face in the picture as it were. The lighting conditions required are for the most part reliant on the nature of the camera utilized. In poor light condition, singular highlights may not be effortlessly noticeable. There exist even infrared cameras that can be utilized with facial acknowledgment frameworks. A large portion of facial acknowledgment frameworks require the client to stand a particular separation far from the camera and take a gander at the camera. This guarantees the caught picture of the face is inside a particular size resilience and keeps the highlights (e.g., the eyes) in as comparable position each time as could reasonably be expected. The

primary assignment of the preparing programming is to find the face (or faces) inside the picture. At that point the facial attributes are removed. Facial acknowledgment innovation has as of late formed into two territories: facial measurements and eigen faces. Facial measurements innovation depends on the estimation of the particular facial highlights (the frameworks normally search for the situating of the eyes, nose and mouth and the separations between these highlights).

After locating the face in the image the system locates eyes within the face region.

Another strategy for facial acknowledgment has been created in the previous three years. The strategy depends on classifying faces as per the level of fit with a settled arrangement of 150 ace eigenfaces. This procedure is in truth like the police technique for making a portrait,but the picture preparing is robotized and in light of a genuine picture here. Each face is relegated a level of fit to every one of the 150 ace eigenfaces, just the 40 format eigenfaces with the most noteworthy level of fit are important to recreate the face with the exactness of 99%.The picture handling and facial likeness choice process is finished by the PC programming right now, this preparing requires a considerable amount of figuring force thus it is difficult to collect a remain solitary gadget for confront acknowledgment.There are a few endeavors (by organizations like Siemens) to make an extraordinary reason chip with implanted face acknowledgment direction set.

The face region is rescaled to a fixed pre-defined size (e.g. 150 × 100 points). This normalized face image is called the *canonical image*. Then the facial metrics are computed and stored in a face template. The typical size of such a template is between 3 and 5 kB, but there exist systems with the size of the template as small as 96 bytes.

## CONCLUSIONS

Even if the accuracy of the biometric techniques is not perfect yet, there are many mature biometric systems available now. Proper design and implementation of the biometric system can indeed increase the overall security, especially the smartcard based solutions seem to be very promising. Making a secure biometric systems is, however, not as easy as it might appear. The word biometrics is very often used as a synonym for the perfect security. This is a misleading view. There are numerous conditions that must be taken in account when designing a secure biometric system. First, it is necessary to realize that biometrics are not secrets. This implies that biometric measurements cannot be used as capability tokens

and it is not secure to generate any cryptographic keys from them. Second, it is necessary to trust the input device and make the communication link secure. Third, the input device needs to check the liveness of the person being measured and the device itself should be verified for example by a challenge response protocol.

*Acknowledgment:*

We would like to thank our faculty Mentor for their support and encouragement in preparing this paper.

**REFERENCES**

[1]Tripathi, K P, International Journal of Computer Applications (0975 – 8887) Volume 14– No.5, January 2011

[2] Iridian Technologies, http://www.iriscan.com

[3] EyeDentify, http://www.eyedentify.com/

[4] Zdeneˇk R íhaVáclavMatyáš "Biometric Authentication Systems ", FI MU Report Series, November 2000.

[5] Bonsor, K. "How Facial Recognition Systems Work". Retrieved 2008-06-02.

[6] Vaclav Matyas, ZdenekRiha, "Biometric
Authentication Systems"

[7] Bhatia Renu, "Biometrics and Face Recognition Techniques", Pattern Analysis and Machine Intelligence, IEEE Transactions on Volume 3, Issue 5, May 2013.

[8] Introduction to biometrics page at www.biometrics.gov