Research Journal of Computer and Information Technology Sciences _____ISSN 2320 – 6527
Vol. **1(4),** 5-14, May **(2013)** *Res. J. Computer and IT Sci.*

Common Biometric Authentication Techniques: Comparative Analysis, Usability and Possible Issues Evaluation

Narmeen Bawany, Rabia Ahmed and Qanita Zakir
Department of Computer Science and Information Technology, Jinnah University for Woman, Karachi, PAKISTAN

Available online at: www.isca.in
Received 1st May 2013, revised 13th May 2013, accepted 17th May 2013

Abstract

Although the usage of biometric devices has tremendously increased but still the traditional authentication techniques are still used by majority of average users. The concept behind biometric authentication technique is that users will not have to remember intricate passwords. Even if the people use biometric authentication mechanisms in their personal devices, they are still expected to remember the passwords and they are asked to input their passwords every now and then. This paper presents different biometric authentication techniques with reference to the past research work and focuses on common authentication techniques (fingerprint recognition, face recognition, pattern recognition, hand pointing device gesture recognition and passwords and personal identification numbers) that people use in their everyday life especially in their personal devices for instance laptops and cell phones. Furthermore, it presents the issues face by the users and what can be done to minimize the issues and increase the usability of biometric authentication techniques. The methods used to determine usability and security issues include experiments, questionnaires and interviews. Experiment session presents comparative analysis on how much time users from different age groups spend on enrolling biometrics and then authenticating with the provided sample. Body language of users and common errors are discussed. Survey session determines users' perceptions, preferences and evaluates authentication mechanisms using usability heuristics. The most important interview session with users determines users' expectations and needs as well as problems that they have faced using different authentication techniques under evaluation. In the end, authors conclude with feasible solutions of the problems discussed.

Keywords: Biometric devices, biometric authentication, comparative analysis, contactless biometrics, contact biometrics, human computer interaction.

Introduction

Typically, authentication is done based on information about one or more of the following: i. Knowledge of the subject, such as password or secret information. ii. Possession of the user, such as smart card, passport, driver's license, etc. iii. Biometric traits of the client, such as fingerprint, voice, iris, etc[1].

Traditional authentication systems requires the user perform the cumbersome task of memorizing numerous passwords, personal identification numbers (PIN), pass-phrase, and/or answers to secret questions like "what is your mother's maiden name?", etc. in order to access various systems[1]. Majority users choose some important dates, names, phone numbers, different combinations of some unique words and symbols or numbers etc. The arising need of keeping strong and complex passwords leads the users to write their passwords in their files or save them in their mobile phones which violates security. If users are restricted in their choice of password and are provided with random auto generated passwords then there appears a loss in efficiency of the system and users will have to spend more time in resetting the passwords again and again. This is where biometric authentication comes and make the lives of people a great deal easier. People believe that biometric devices enhance security. This is true to some extent. The biometric devices have some security issues too. Biometric devices are susceptible to spoofing. For example, a gelatin copy of user's fingerprint data on the glass, user's photograph etc. can be used[2] to trick the biometric authentication system[2] and the theft of biometric data is much more serious. Users can change their passwords but they cannot change their biometrics. Similarly, biometric authentication techniques have usability issues too. For example, traditional ink fingerprinting expected users to place the thumb or any finger and wait few seconds for enrollment whereas fingerprint scanners in personal computers expect users to swipe their fingers on the scanner. This inconsistency is one of usability issues. Face scanning by visible light has high false rejection rate and consumes a lot of time in enrollment. This frustrates users but steps can be taken to overcome this issue. People generally draw letters in mouse gesture recognition authentication but there will always be some difference between saved gesture sample and gesture drawn to authenticate. In this research paper, strengths and weaknesses of contactless and contact biometric technologies are discussed with respect to the previous research work and then usability and user acceptance of some common biometric authentication in different age groups will be evaluated. The authors also have discussed the possible solutions to existing problems. This paper focuses on: What authentication mechanisms users from different age groups prefer and why? Does using biometrics in personal devices

really saves time when users generally choose passwords with high memorability? How users perceive and why do they perceive so? Is single authentication technique is enough? Does the time spent on enrollment has any effect on user's perception about the authentication mechanism?

Background and related work: A biometric system is essentially a pattern recognition system that operates by acquiring physiological and/or behavioral characteristics from individual (such as fingerprint, iris scan, retina scan, hand geometry, etc.), extracting a set of features from the acquired data, and comparing this feature set against the set of templates pre-stored in the database[1].

Fingerprint is probably the most used for biometric authentication. It is also likely to be the oldest biometric in use. Till date, beside improvements of fingerprint recognition, many other biometrics have been revealed namely, face recognition, voice recognition, hand geometry, iris recognition, retinal pattern recognition, etc. The basis of every biometric based authentication system[1] is the fact that the biometric characteristic used to identify and/or verify users is unique for each user. There are also other factors such as universality, permanence, etc., which relate to security concerns of biometric authentication[2].

While the main focus of this research paper is on authentication for access to computer systems, occasional reference will be made to authentication in other contexts[1].

All authentication systems suffer from two kinds of errors, false acceptance of impostors and false rejection of authorized users[1].

False rejection rate (FRR): The false rejection rate (FRR) of a biometric authentication system is the fraction of authorized user authentication attempts that result in rejection. Impostors may happen to have biometric characteristics very similar to those of the authorized user, or may obtain a copy of the user's biometric feature, such as a photograph of a user's face, that can be used for spoofing the biometric authentication system[2].

False Acceptance Rate (FAR): The fraction of authentication attempts by impostors that succeed is known as the false acceptance rate (FAR). If the system requires a very close match, FAR will be low, but FRR will be high, and vice versa. Therefore, testing of a biometric authentication system must determine both the FAR and FRR of the system[2].

Contactless biometric technologies

Facial recognition: The face recognition process normally consists of four phases:

Detecting a face: It is not difficult for people to differentiate one person from another just look at his/her face. This task is more difficult for computer. The task of the computer is to decide what the part of the image is and what is not. The task is easier with the photos with white background, but it becomes more difficult if there are some other colors, things on the background[3].

Normalization: When the face is found it should be normalized, it should be standardize in terms of position, size relative to the image in the database. The system locates the facial landmarks. With the help of these landmarks the system can create a slight variation of the image. Using the facial landmarks is the key to all systems. If facial landmarks cannot be located, the recognition process cannot take place and fail[3].

Feature extraction and recognition: Biometric template is generated with a help of recognition algorithms. These algorithms differ by the ways they transform or translate the face image to a simplified mathematical representation in order to perform a recognition task. This template is stored in the database and it is the basis of any recognition task. It is important that maximum of information should be retained for successful recognition. If this condition fails, the algorithm will not have ability for successful recognition and the task will failed[3].

Recognize face image: Here we can have different purposes, whether it is identification or verification. If verification takes place the image will match to only one image in data base. If it is identification the image will be compared with all images in the database[3].

Face scan can be carried out by visible or infrared light. Face scan with visible light suffers from a small number of features compared to other biometric authentication methods, and those features may be changed by disguise or by weight change. It is also subject to spoofing with a picture of an authorized user. Infrared face scan uses a thermal image to detect patterns due to blood flow beneath the surface of the face. The positions of the blood vessels are permanent, and provide much information for authentication. The main disadvantage is the high cost of a camera[2].

Voice Recognition: Voice is often compared with fingerprints, because like fingerprints, due to their unique form serve for biometric authentication, so the voice does. The uniqueness of the voice is achieved due to the different physical components of a human throat and mouth. To produce a sound, air leaves the body of a human being through resonators: larynx, the oral cavity (mouth), nasal cavity (nose). The form, tone of the sounds are dependent on the size of the stream, obstructions. Obstructions may include tongue, gums, teeth, lips, their position and size[3].

To identify the person with the help of voice print, a sample of speech should be taken. This sample is analyzed. Different multiple measurements are taken and the results are presented in the form of the algorithm. Common delusion is that the voice

itself is 47stored in the database. No, the output from the algorithm is stored in the database. For verification, another sample of the speech is taken. As in identification process the second sample is analyzed, and measured. If the results match, the identity can be verified[1].

Weakness of voice scan includes susceptibility to replay attacks, problems due to low-fidelity equipment and ambient noise, and large template size. Enrollment can be difficult and for authentication user has to speak in the same way as he speaks during enrollment[2].

Retinal scan: If Moore's law is correct in its hypothesis of exponential increases in computer processor speeds over time, retinal images could be compared between an individual and other people enrolled in the system similar to way fingerprints currently are[4].

Retina scan seems to be an extremely high security technology. In testing by Sandia National Lab there were no false acceptances, and a 1% FAR with three attempts. The distribution of impostor scores has a Gaussian distribution, and from the tail of the distribution a FAR of about 1 in 10 is predicted. Spoofing such a system would be difficult. Alignment would be difficult with a "fake eye." If further protection against spoofing was needed, Hill suggests that the System could display a random number in the alignment optics during scanning then the user would be required to enter it in order to authenticate. Retinal scan also has important disadvantages. Some users fear eye damage. The systems do not work well out of doors, or in areas with high light level, because bright light causes the pupil, to contract, lowering the signal in the retina scan. Also, medical changes, in particular pregnancy, may cause changes in the veins of the retina, causing false rejection[2].

Iris Scan: Iris is a part inside our eye, which is unique in every individual, it remains unchanged till end of life this is the most prominent technique that can be implemented. The capture of iris is very simple one even need not stand before the camera[5].

Iris recognition is the best of breed authentication process available today. Iris recognition takes a picture of the iris; this picture is used solely for authentication, it is different from retinal scan[5].

Iris recognition technology provides accurate identity authentication without PIN numbers, passwords or cards and the enrollment takes less than 2 minutes. Authentication takes less than 2 seconds. Producing a template to enroll has been made easy with the use of Video-Based technology[5].

An advantage of iris scan is that the iris features do not change of the course of a person's life. However, "training and attentiveness" are needed for good image acquisition, and perhaps for this reason the systems have a "propensity for false rejection". Spoofing of an iris scan system is relatively difficult, but still possible[2].

Contact biometric technologies

Palm Print: Palm print refers to an image required of the palm region of the hand. As a method of biometrics palm print is often mentioned with such methods as fingerprints and iris recognition. Palm print is also distinctive and can easily be captured with low resolution devices. The devices are not expensive. They are similar to those which are used for taking fingerprints but their size is bigger and this makes the limitation of use in mobile devices. Palm print is suitable for everyone and besides it has one big plus: it does not require personal information. The palm of each person consists of principle lines, wrinkles secondary lines and ridges. Palm also contains such information as texture, indents and marks which are used during the comparison of one palm with another. Classification of palm prints is based on the different principle lines and number of intersection. This classification was offered by X.Wu, D.Zhang, K.Wanfg and B.Huang in their book "Palm print classification using principle lines"[3].

Palm printing has its own advantages comparing with other methods of biometrics. Palm print is hardly affected by age (the problem of age is the main problem for face recognition). Palm prints contains more information and can use low resolution devices (in comparison with fingerprinting). Palm printing cannot make harm to the health of people, and many people prefer palm printing to iris recognition based on this very reason[3].

Palm printing is a rapidly developed method of biometrics. One of the variants of palm printing is the recognition based on the veins of palm. Infra-red camera makes the image of inner or external side of the hand. Hemoglobin absorbs infra-red light and veins can be seen as black lines. This method is contactless and reliable. The main minus of this method is that there should be no light near the scanner[3].

Hand/Finger Geometry: Hand geometry is the use of geometric shape of the hand for recognition purposes. This method was rather popular 10 years ago but nowadays it is seldom used. The method is based on the fact that the shape of the hand of one person differs from the shape of the hand of another person and does not change after certain age. But it is not unique. The main characteristics for this method are measuring and recording the height, length of the fingers, distance between joints, shape of the knuckles, and surface area of the hand. There are two kinds of principles that can be used for measurement of the hand: mechanical and optical[3].

Optical scanners can also be divided into two subcategories: devices that belong to the first subcategory create black and white bitmap image. These devices use 2D characteristics of the hand. The second subcategory offers a bit more complicated

devices. They have two (vertical and horizontal) sensors to measure the hand shape. These devices use 3D characteristics. There are scanners that produce the video signal with hand shape. Computer digitalizes and process the image[3].

For verification the person should enter his personal PIN code and place the hand to the platen. The system makes common procedures and compares the given template with the template stored in the database[3.]

The method of hand geometry has its own advantages and disadvantages. The main advantages of this method are its simplicity, easiness of use. Scanners are not expensive. Also it is easy to collect hand geometry data that differs this method from fingerprinting. Environmental factors (dry skin) cannot influence on the results. Among disadvantages of the method it should be mentioned that hand geometry cannot be used in identification system. Hand geometry is ideal for adults but not for growing children as their hand characteristics can change in time. And data size is too large[3].

Dynamic Signature Verification: Dynamic signature verification measures both the shape of the signature, and also dynamic factors such as speed and pressure. Inconsistent signatures may cause increased error rates. Advantages attributed to dynamic signature verification are resistance to impostors, the ability of users to change their signature if it is "stolen" by an impostor, and the perception by users that it is not invasive. However, inconsistent signatures are said to lead to increased error rates[2.]

Keystroke dynamics: Keystrokes dynamics is the process of analyzing the way a user types at a terminal by monitoring the keyboard input thousands of time per second, and attempt to identify them based on habitual rhythm patterns in the way they type. We present our data selection and extraction methods as well as our classification and identification strategies. Moreover, unlike other biometric systems which may be expensive to implement, keystroke dynamics is almost free-the only hardware required in the keyboard[6.]

Personal device authentication techniques evaluation: We have evaluated fingerprint, face, patter and hand pointing device gesture recognition and password and pins authentication techniques in personal devices that is cell phones and laptops.

Methodologies Used: For evaluating the aforementioned techniques, we have used three methodologies: experiment, questionnaire and interviews. Observations will be discussed in all three methods.

Participants: Participants in this usability study were recruited according to age groups to analyze and distinguished results between older adults and youth. Age groups were divided as follows: i. Individuals above 40, ii. Individuals above 30 and below 40, iii. Individuals above 20 and below 30, iv. Individuals below 20

Materials: We used HP Protect Tool Security Manager for testing of password, fingerprint and face recognition on laptop and Android Security Locker Application for testing mouse gesture, pin and pattern recognition in smart phones.

A post-study system usability questionnaire was used to assess participant's level of satisfaction, ease of use, functionality, learnability and error and system reliability. We used most widely utilized approach "likert scale" for measuring the responses in survey questionnaire. In experiment, users were asked to perform following tasks: i. Provide authentication sample, ii. Logging in or authenticate with the given sample, iii. Reset or remove the given sample

Experiment: Users were invited to participate in the research and experiment with different authentication techniques. Statistical data was observed as how long it takes each user to provide authentication sample (password, fingerprint biometric), login and then removing or resetting the provided sample. It was also observed what mistakes or slips users make and with what age group they belong.

Providing Authentication Sample: It was observed that although it takes almost same time in providing pins, passwords, patterns, and mouse gestures but people felt frustrated in providing gestures.

Older adults has problems in their face scan by visible light. They felt extremely uncomfortable. It was also observed that older adults perceive fingerprint reader

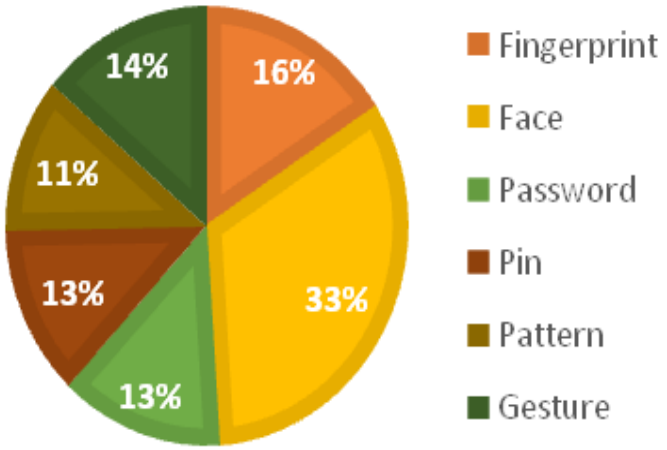

Figure-1
Time taken by individuals above 40

Young generation tends to have high typing speed and are always in hurry. They lack patience. It took almost same time in providing authentication sample for fingerprint and face scan. Most of them had correct mental model about how biometric authentication techniques under evaluation work and general slips like "don't swipe the finger so fast" or "don't move your face while saving" were observed.

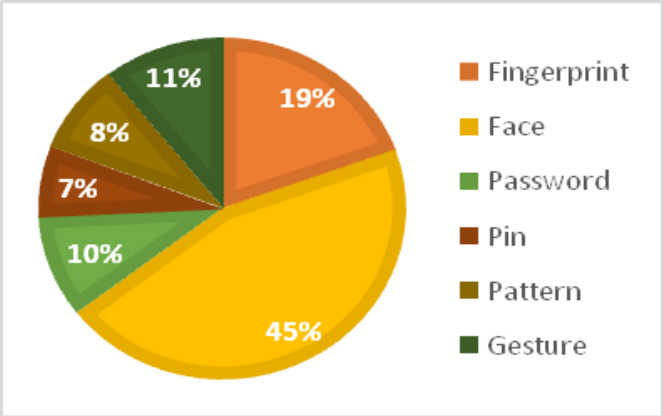

Figure-2
Time taken by individuals above 30 below 40

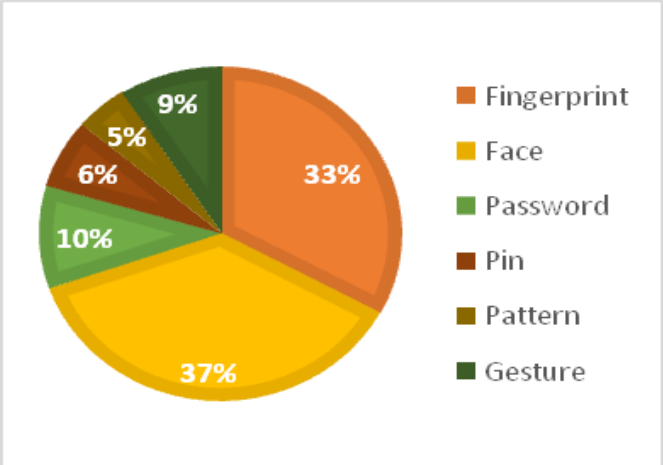

Figure-3
Time taken by individuals above 20 below 30

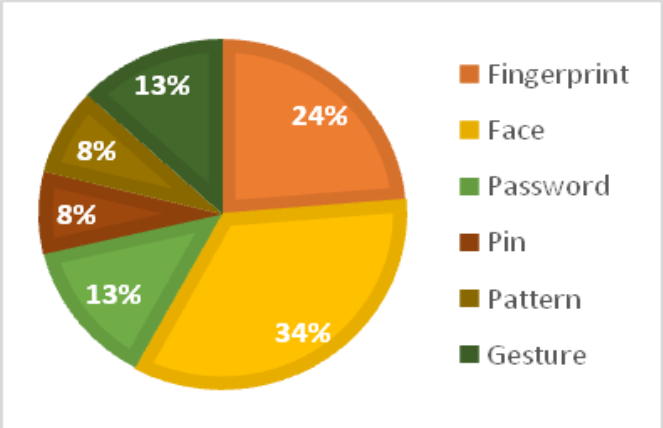

Figure-4
Time taken by youth below 20

Login Using Authentication Sample: It was observed that few older adults were unable to login with face recognition. And they prefer using passwords and pins to authenticate themselves.

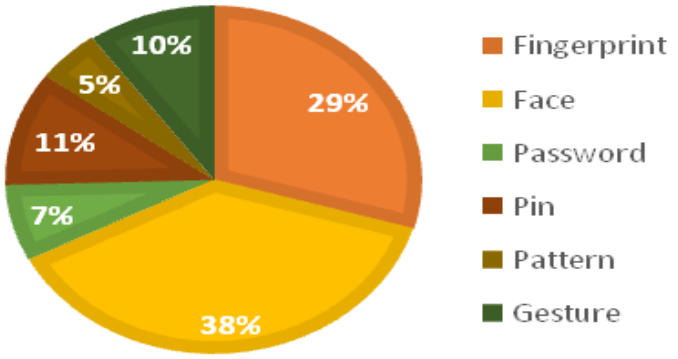

Figure-5
Time taken by individuals above 40

It was observed that biometric authentication takes less time for individuals above 30 and below 40. But they prefer fingerprint scan to authenticate themselves.

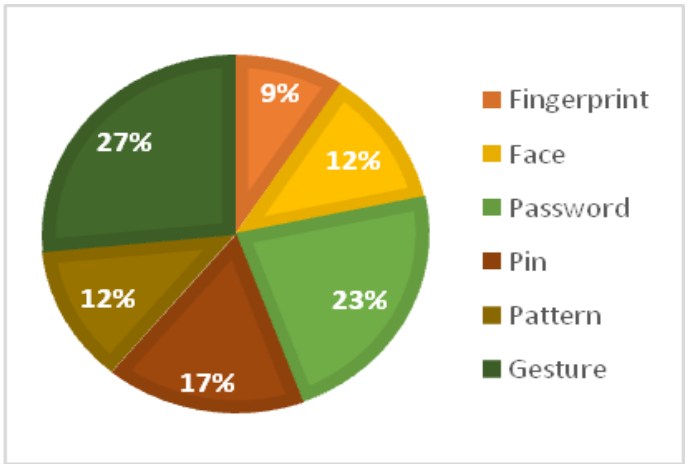

Figure-6
Time taken by individuals above 30 below 40

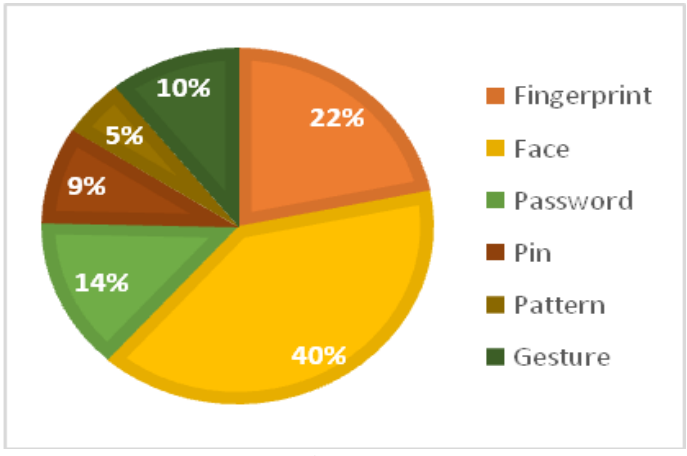

Figure-7
Time taken by individuals above 20 below 30

Most of the participating individuals below 20 prefer face scan by visible light as their first authentication technique in personal devices. It was also observed that young generation below 20 does not prefer fingerprint scans.

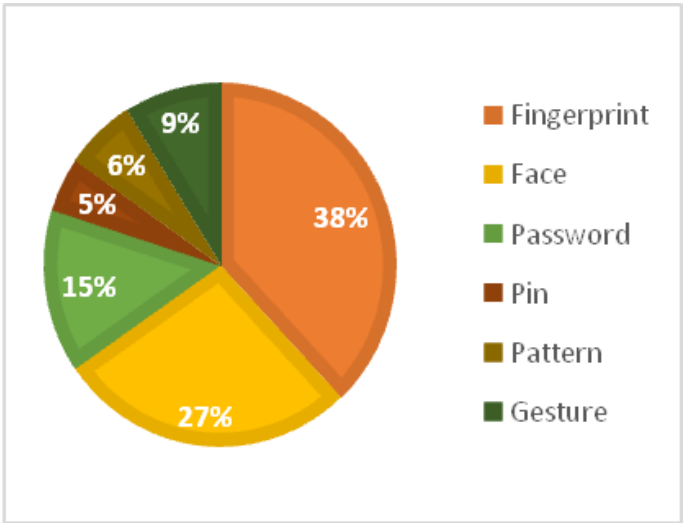

Figure-8
Time taken by youth below 20

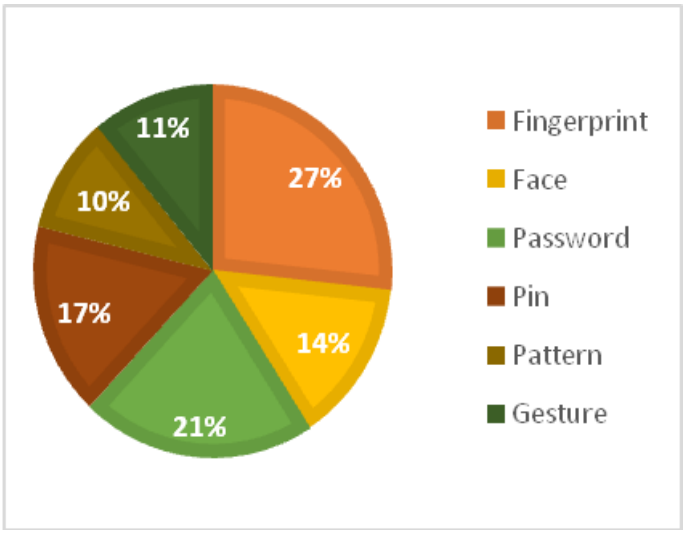

Figure-9
Time taken to remove or reset authentication sample

Post Study User Satisfaction

Ease of Use: Ease of use determines how much easy the system is to use, how much knowledge user is expected to have, visibility of the system status, level of affordance and how much consistent the system is.

It was found that password and pin authentication techniques have greater ease of use as compared to other techniques but no greater difference was observed. Mouse gesture authentication technique is less easy to use than any other technique.

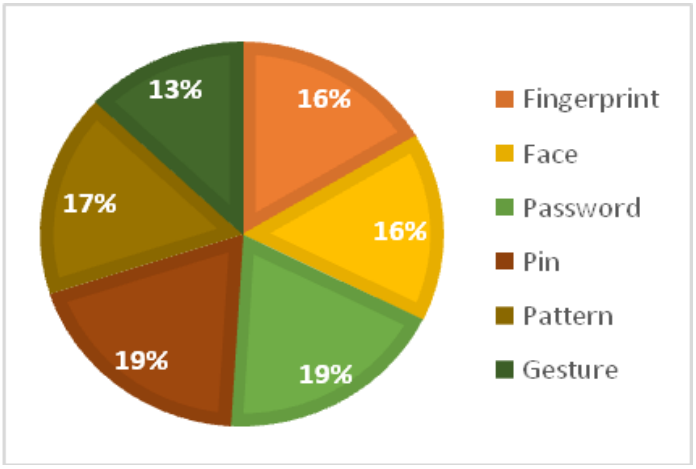

Figure-10
Ease of Use for Authentication Techniques under Evaluation

Functionality: It is researchers' observation that logging in personal devices with passwords and pins takes less time than logging in using biometric devices because users choose easy passwords with high memorability. The password is usually on their fingertips. In figure 11, some common password choosing strategies are mentioned.

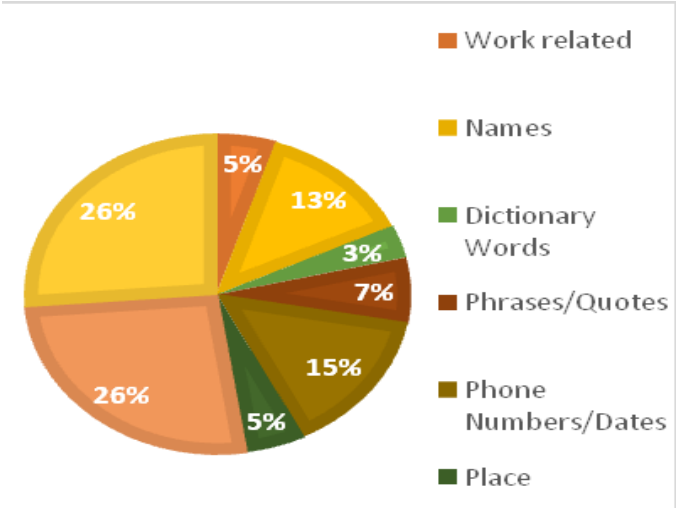

Figure-11
Password choosing strategies

Here in figure 12 users' perception about the level of concentration expected in each authentication technique is explained in comparison with other techniques.

Authentication techniques require the least level of concentration. There is little difference among perceived concentration level required in other techniques excluding hand pointing device gesture recognition. The major problem that we observed in gesture recognition is that it has least memorability and users cannot draw same gestures every time they try to authenticate. There will always be some difference which

increases the false rejection rate and as a result requires more concentration from users.

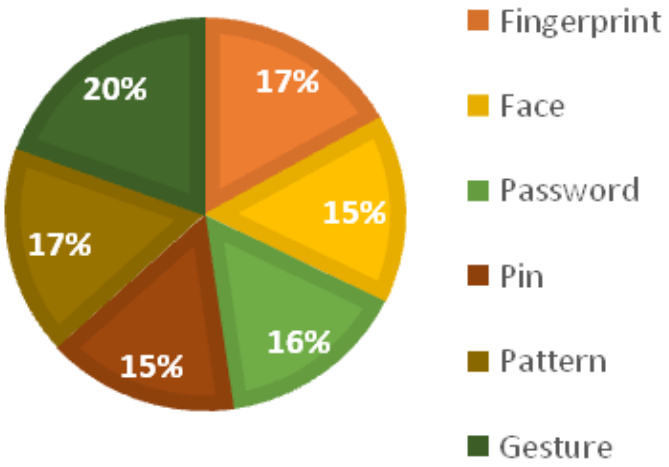

Figure-12
Level of concentration required for authentication techniques under evaluation

According to the perceived mental model of users, face and pin. in figure 13 the comparison is presented about failure to authenticate in first attempt using different authentication techniques. Passwords when chosen by users have 0% failure rate.

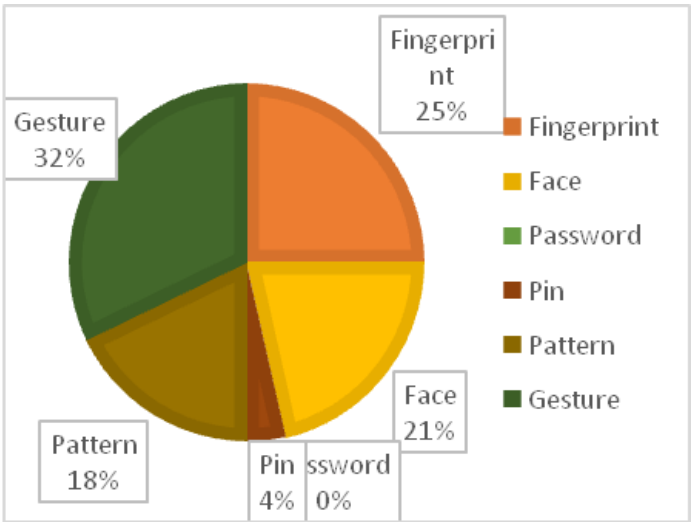

Figure-13
Failure to authenticate in first attempt

Learnability: Fingerprint scan is observed to have a greater learnability and gesture has the least. By learnability, we mean users can figure out features on their own and once learned they can work on those features in future too. It was observed that providing authentication sample for second finger took approx. 40% less time than providing the sample for first finger.

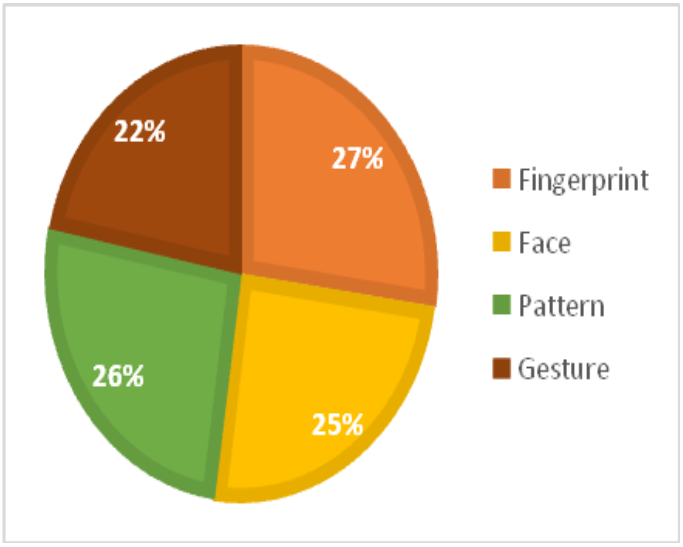

Figure-14
Learnability of Fingerprint, Face Pattern and Mouse gesture Authentication Techniques

Satisfaction: Level of satisfaction varies for each age group. Youth enjoy face recognition, adults above 30 and below 40 enjoy fingerprint recognition more. In Figure 14, level of enjoyment for all age groups is presented in general. Users enjoy face scan more because they just have to smile to authenticate themselves. Fingerprint scan and pattern recognition has almost same degree of enjoyment.

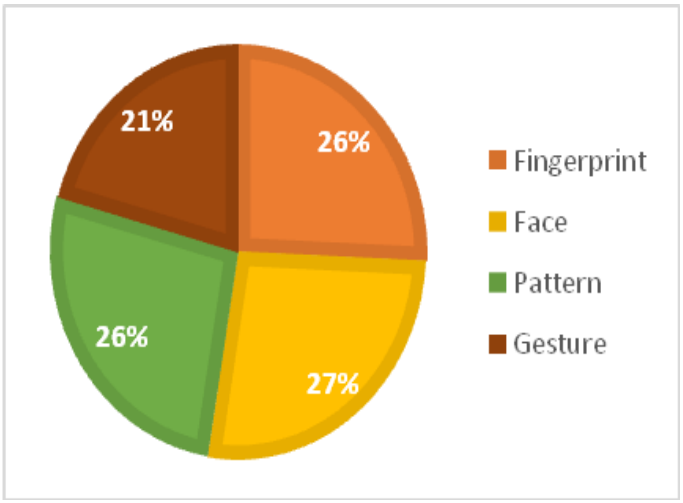

Figure-15
Level of enjoyment user feels for each biometric technique under evaluation

In the evaluation, researchers also observed that older adults have greater fear of using the biometrics because they think they may get locked up. The possibility is far less than the fear. To overcome this fear, users prefer to have multiple authentication techniques available with traditional password or pin as one of them.

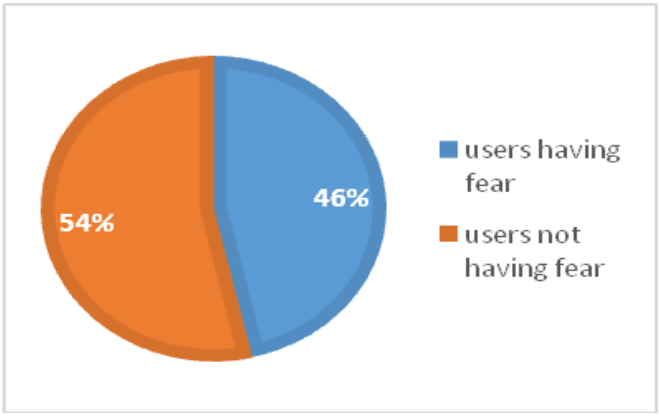

Figure-16
Fear of having or getting a locked device in case of using biometrics

In Figure 17, a comparison is presented as how much each authentication technique is used.

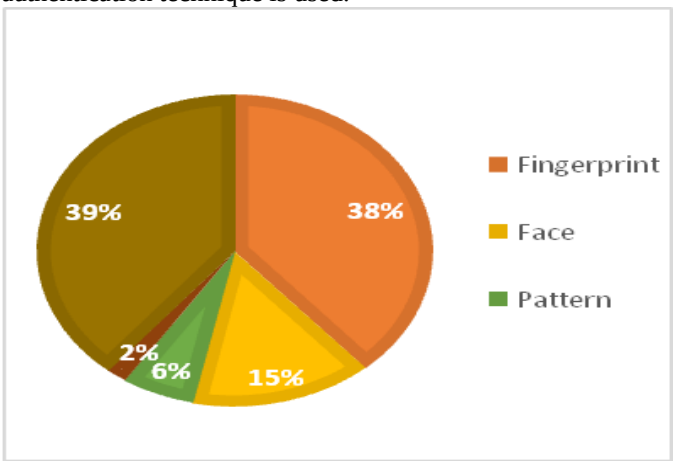

Figure-17
Use of authentication techniques in users' everyday life

The figure below compares how much biometric authentication techniques under evaluation are disliked by users.

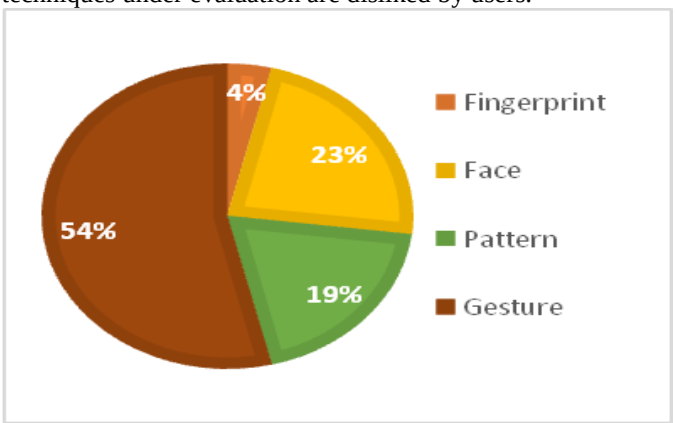

Figure-18
Level of dislike for biometric authentication techniques under evaluation

Some people prefer biometrics and some prefer traditional passwords and pins as their primary authentication mechanism. The reasons of their preference will be discussed in interview section but a brief presentation of the ratio of individuals' preferences is given below.

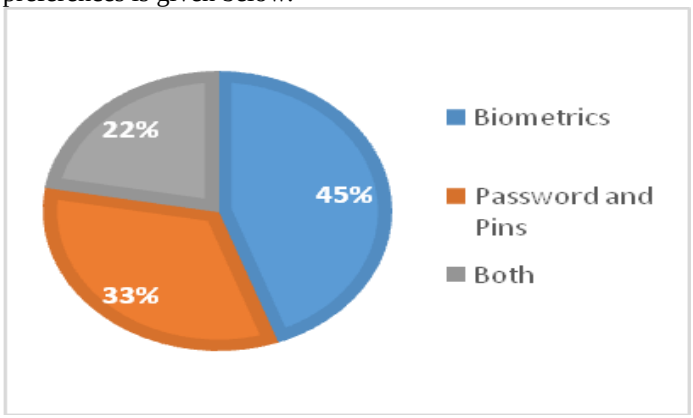

Figure-19
Participants' preference for biometrics and traditional authentication techniques

Error and System Reliability: The degree of error recovery and reliability is almost same in all biometric authentication techniques under evaluation excluding mouse gesture recognition. The users do not get any clue as to why they are unable to authenticate themselves although they perceive that they are making the right gesture.

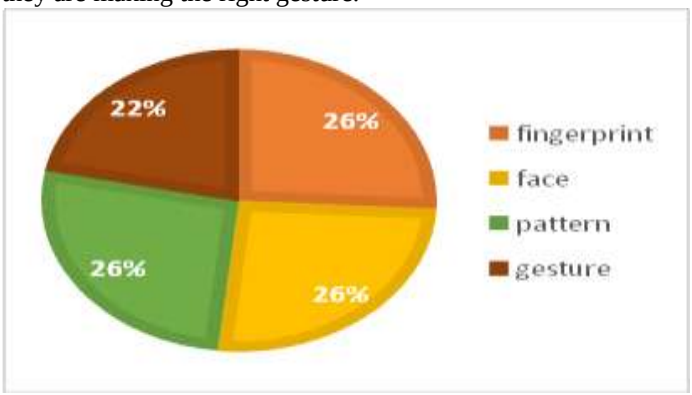

Figure-20
Error Recovery and System Reliability Comparison

Interviews and Discussion: In this session, we tried to instigate users about how they feel about using different authentication techniques, what should be done to make the existing system better and more reliable. Users were prompted to share their experiences, their preferences and the reasons behind preferences. It must be kept in mind that all the users interviewed were average computer users and this research is about authentication techniques in personal devices. It is a common observation that users who use biometric authentication prefer to have multiple authentication mechanisms available to them and they don't like the idea of getting their device locked because some imposter tried multiple false attempts. A participant shared his experience

of an Android phone. The user has turned on Google 2-Step verification system and he was using application specific password for Gmail on his Android. Due to multiple false attempts, the phone got locked and asked to input Google Account password that the system was using, that is, application specific password. Now the tragedy is that Google recommends against saving application specific passwords and these passwords are not even saved on the user's Google Account. The participant has the habit of writing passwords in his diary. If he hadn't saved that application password then his phone had definitely got locked. Issue like this can happen with anyone. The system should not make actual users suffer due to imposters.

Password and Pin: Every age group has different preferences. Individuals below 40 prefer biometric authentication whereas the older the individuals were the more they preferred pins and passwords as their primary authentication mechanism. A very interesting discovery was that users still prefer same passwords or combination of same phrases in their passwords. For example, some of the combinations may be jinnahUNI123, JINNAHuni123, 123jinnahUNI, 123JINNAHuni, Jinnah 123 UNI etc. When users were asked do they always remember which password they should use at what place? Majority of them shared that they make several attempts with different combinations and most of the time it works. Even if it doesn't then there are always an option to opt for forgotten password or pin techniques. It was also found that user above 25 and below 45 are more security conscious. Strategies like writing passwords in files or saving passwords in mobile and then encrypting those passwords with an added security are still very much common. In this experiment some users were asked to use a system generated random password for authentication. Then users were prompted to save biometric authentication sample. When they were done with biometric authentication experiment, users were then asked to login with the system generated password. Almost all of them had written it somewhere although it was expected to be used for very short term basis. And they were unable to recall the password. From this experiment, we deduced that the more complex and the more secure the password is, the more people tend to forget it and if users authenticate by biometrics then the memorability of complex passwords decreases drastically. It was also suggested by a user that if the passwords are expected to be remembered then the system should recall those passwords for users every time they access the system with biometric authentication. Some of the biometric scanning softwares prompt users to write their password when they try to alter the biometric sample. This appears frustrating to users. We have concluded from past research that fingerprint and face authentication samples can change with time. If the concept behind biometrics is that users don't have to remember passwords anymore but still the softwares ask users to type their passwords. This should be avoided. An issue was also found related to windows operating system from a web article that some of the pre-installed biometric authentication softwares save the passwords in windows registry which is a potential security threat. If the password is compromised then anybody having the password can alter or delete the biometric sample.

Face Recognition by Visible Light: Young participants enjoy authenticating themselves with face scanning by visible light. So emotionally it is always a pleasant experience for those who are in suitable surroundings and who are authenticated within seconds in one or two attempts. But the experience becomes frustrating to users with less light or when users are not in the same position as when they were at the time of enrollment. We experimented with a participant to enroll with the hand on her head. When she tried to authenticate herself without having her hand on her head, the system was unable to recognize her. It was a funny experience but give us an insight to an important issue. One of the user pointed out that not everyone has same facial bone structure. Some have round big faces and some have small faces. The system should allow users to set the facial scan contours so that only that part of the face is scanned when users try to authenticate leaving the surrounding. Users were asked if they feel that their time was saved using face logon. Most of them think that their time is saved a great deal but this is not the case according to the statistics. We found that for personal devices when users have their passwords on their fingertips and when users don't have to recall the passwords or pin, it takes less time to authenticate using passwords or pins than face logon. We deduced that users think so because they don't have anything to work for instance they don't have to type and users don't have to recall anything like password. Their mind is free so they can think of other important things and therefore they perceive that it takes less time to authenticate via face scanning than with passwords or pins. But same is not the case with older adults. When they switch on the system, the only thing they have in their mind is the system and the work for which they want to access the system and they feel that it takes less time to authenticate via password. They get impatient and move their body which increase the false rejection rate and hence consumes more time than it should. Another worth mentioning fact is that older adults have very low acceptance rate and very low learnability. This is the reason that older adults perceive that they can only be comfortable in using traditional authentication mechanisms. It was also suggested by participants that face recognition should only be used for personal devices because it has very high false acceptance rate and it will be easier for the family members with similar faces to be authenticated in some urgent situation.

Fingerprint Recognition: In experiment we found one mistake and two slips that users most of the time commit. But all the problem have one solution. Some users had incorrect mental model as to how fingerprint scanning works. They expect their fingerprint to be scanned when they place their finger on scanner. But that's now how the scanner in laptops work. Users are expected to swipe their finger on the scanner. We observed two slips. Either the users swiped their finger too fast/slow or users did not vertically swipe their finger in center or tried horizontal swiping. All these issues can be solved if there is a big size scanner which expects users to place their finger and wait for the scanning to be completed. The fingerprint scanners like this exist

in the market. Integrating them in personal devices will decrease the FRR and increase the usability of fingerprint authentication.

Pointing Device Gesture Recognition: It was observed to be the least accepted authentication mechanism. Fear of having a locked device was dramatic in this technique. For mouse gestures, we also found that people generally keep a letter as their authentication gesture. It is suggested that hand pointing device gesture recognition should be able to recognize letters. This technique appears to have greater FRR and FAR.

Pattern Recognition: The few usability issues that were discussed with participants are: the system does not inform users how many dots should be used to create the pattern and if the user is expected to create complete pattern without leaving the cursor. Users also suggested that they should be allowed to customize the number of dots on the screen. This will enhance security and will make shoulder surfing difficult.

Results: It was observed that few older adults were unable to login with face recognition. And they prefer using passwords and pins to authenticate themselves Most of the individuals below 40 and above 20 prefer fingerprint scan to authenticate themselves and individuals below 20 prefer face scanning the most. The older adults above 40 face difficulties in using biometric devices and perceive that they can only be comfortable in using traditional authentication mechanisms while young participants enjoy authenticating themselves using biometric authentication. The studies show that using biometrics does not save time but users believe so because using biometrics requires less concentration and attention from the users and they feel that the time they spend on typing is saved. Hence they perceive that biometric authentication is less time consuming.

The primary reason as to why some people prefer traditional password and pin authentication mechanism is that they feel frustrated or perceive that they will be uncomfortable using biometric authentication. The feeling may be due to word of mouth, personal experience etc. It was observed that those users who faced little or no problem in providing or setting up biometric authentication sample felt more comfortable using it and those who faced problems initially got their mind set and did not prefer that authentication mechanism. Users also feel hesitation when they are informed about the consequences. For example, telling the users that you may not be able to log in using face unlock scares the users. Users can be informed that they should enroll themselves in the similar environment with proper lights. User can be asked to smile for enrollment. Technically they will always use same gesture every time they log in but for users it will be a good experience as the system is expecting them to smile to authenticate them.

Another issue is that all users are expected to choose a password for their personal devices even if they intend to use biometric authentication. If the users who intend to use biometric authentication choose some intricate password then they eventually forget it because they don't use it at all. But the biometric authentication soft wares expect the users to remember their passwords. If the users have chosen easy-to-remember or easy-to-guess passwords then there lies a security threat too. Anybody having the password can alter or delete the biometric enrolled sample. The best way to enhance security would be to disable the use of passwords for biometric users and they must identify themselves using biometrics to alter or delete the authentication data. Now what if the hardware is damaged? To address this issue, there should be more than one biometric authentication techniques made available to users. Face scanning is highly susceptible to spoofing so iris recognition can be used for personal device authentication.

Conclusion

The more complex and the more secure the password is, the more people tend to forget it and if individuals use biometric authentication then the memorability of complex passwords further decreases drastically. It is better to disable the use of passwords and make use of biometric authentication if security is a major concern and users are recommended to keep strong passwords. It is also concluded from this studies that logging into personal devices with passwords and pins takes less time than logging in using biometric devices because users choose easy passwords with high memorability.

Error recovery rate of all biometric authentication mechanisms under evaluation was found to be same except mouse gesture recognition. Users perceived that they were giving the right input and they were unable to figure out where they had gone wrong. It appeared to be very frustrating to users. 54% of participants strongly dislike mouse gesture recognition. With respect to accuracy and susceptibility to spoofing, iris and fingerprint scans are better as compared to hand pointing device gesture, voice, face or palm print recognition. With respect to learnability, users who once had set up the fingerprint scanning took approx. 40% less time when providing the sample for second finger.

References

1. Minhaz Fahim Jibran, Biometric Authentication: The Security Issues, *University of Saskatchewan* **(2012)**
2. David C., Hitchcock, Evaluation and Combination of Biometric Authentication Systems, *University of Florida Digital Collections* **(2003)**
3. Aleksandra Babich, Biometric Authentication. Types of biometric identifiers, *Theseus.fi* **(2012)**
4. Stephen Hoffman, Biometrics, Retinal Scanning, and the Right to Privacy in the 21st Century, *Social Science Research Network*, **22,** 38-52 **(2010)**
5. Chandrakant D. Patel, Sanket Trivedi, Sanjay Patel, Biometrics, in IRIS Technology, *International Journal of Scientific and Research Publication,* **2(1) (2012)**
6. Fabian Monrosea, Aviel D. Rubinb, Keystroke dynamics as a biometric for authentication, Future Generation Computer Systems, **16(2000)**, 351-359 **(1999)**