Comparison of different Authentication Techniques

Manish Giri [1] and Pooja Ahuja[2]
Dept. of CSE, UIT, BU, Bhopal (M.P.), India[1, 2]
goswami.manishgiri@gmail.com[1] , samayra.ahuja@gmail.com[2]

Abstract: *Cyber-attacks has increased at a tremendous rate in the last decade. Due to this sensitive data are not safe. Thus to counter this we need a robust authentication method. Effective user authentication techniques are used to protect information and system safety In recent years different types of fast authentication systems are already being developed such as token based, biometrics system, captcha etc. Each of the existing methods have their own merits and demerits discuss in this paper.*

Keywords: *graphical password, authentication, security, token, biometric.*

1. INTRODUCTION

Secure operations , Authentication and development of secure system; these are the most important areas for human computer interaction [1]. In today's fast changing hi- tech environment where systems are converted into Smart phones, the probability of attack on the sensitive data stored in the system are very high. Today peoples are making transaction on their Smart phones using Apps, checking mails and doing many online activities. This results in movement of large data from system to the outside world, and there are more chances of the attack on this data. Attackers tries to get the login details such as password. The password is a very common and widely used authentication method[21] but due to its excessive use in many applications like data transfer, emails login, validating accounts ,online transactions etc., drawbacks of normal password appears(such as stealing of password, forgetting the password, providing a weak password, etc.). So it is required to have a strong authentication method to secure all our applications. In the paper, our main focus is on different types of authentication systems and their authentication problems. In the text based password technique passwords are mostly simple name of any person, place, lovable thing or any dictionary word that can be easy to memorize, but these passwords can be easy to guess or crack by a hacker by dictionary attack and brute force attacks within 30 seconds [2]. Another password is combination of alphabets, number and special symbols, but this type of passwords are difficult to memorize. Remembering different passwords for different accounts are also very difficult.

2. AUTHENTICATION TECHNIQUES

There are four types of techniques here we are categorizing

1. Text based authentication technique.
2. Token based authentication technique.
3. Biometric based authentication technique.
4. Graphical password authentication techniques.

2.1. Text based authentication technique

This is simplest and mostly used technique. User simply enters their user name and password. User name should be some unique name or any email-id and password may be any combination of alphabets, digits and special symbols.

LOGIN

Username : ******

Password : ******

forgot your password ?

Fig 1 Text based authentication

Here User name is unique according to the user or a unique email id. There are different levels of password can be selected according to the user. Simplest password is the combination of alphabets or lovable name of any person, place or things. But it can be easily cracked be hackers easily. To provide difficulty to it, user can make any combination of alphabet, digits and special symbols that is very difficult to gauss by any person. But is hard to memorize but these passwords can easy to guess or break, a cracker can break these passwords by dictionary attack and brute force attacks within 30 seconds [2].

Table 1. advantages and disadvantages of text based password technique.

Advantages	Disadvantages
1. Least expensive authentication method to use.	1.Weak and susceptible to numerous attacks.
2. No need to carry any extra hardware device.	2.Security depends on users ability to maintain the users ID and password secret
3. No need to install extra software.	3. Not fully reliable when used for making financial transaction remotely, such as fund transfers and bill payments through an internet banking channel.
4. User ID and password can be changed to the user's choice.	4.Cost of support increases with user ID and password complexity (i.e. help support or IT staff may need to extra time dealing with authentication problems, such as helping staff reset passwords that are locked after a certain number of failed entry attempts).
5. Most users know how to use this technique.	

2.2. Token based authentication technique

These days Token based techniques are widely used. Smart cards, ATM card and key cards are the main examples of the token based technique. These token based authentications techniques also use the knowledge based techniques. For example ATM cards use a PIN number.

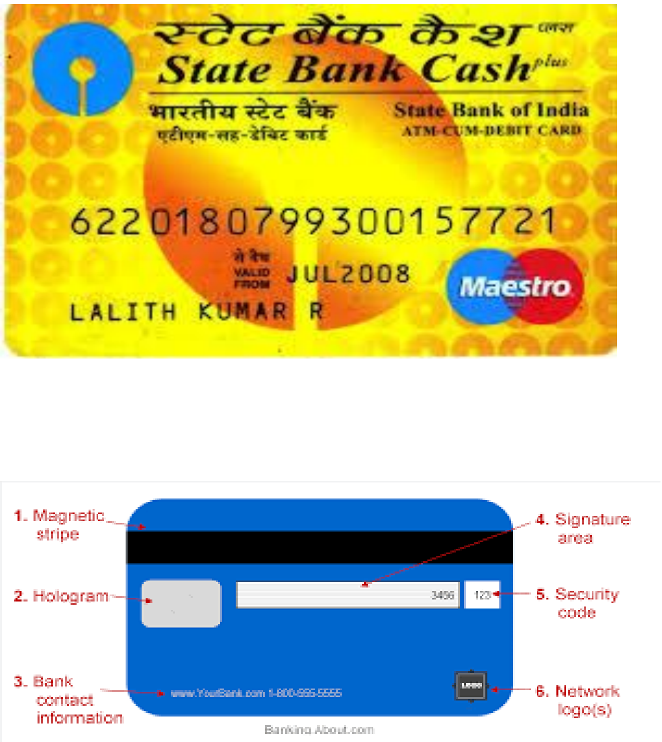


Fig 2 ATM card front and back side

In the above figure, mentions all the fields of ATM card front and back side both. In the front side of ATM card ATM transaction code, card holder name, validity date of atm card, and type of ATM card, bank name etc printed. At the back side of atm there is a black stripe called magnetic stripe that contain a secret encrypted code which is used at time of transaction and other operation performing time. There is a signature field and hologram and security code mention. Security code is used at the time of online transaction by ATM card.

But this techniques is also got unsecured because sometimes it happens that all the money of your account has been stolen form the ATM machine where you had got transition from ATM card.

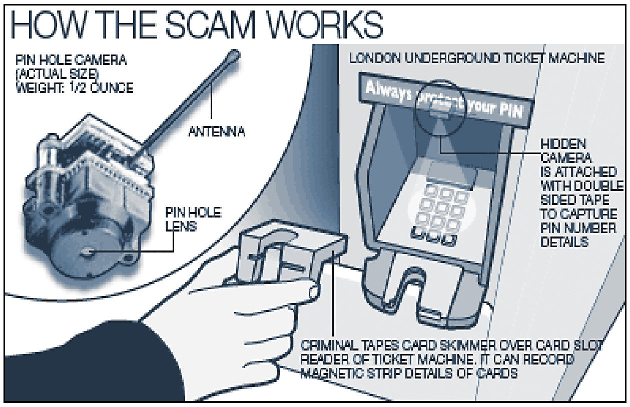

HOW THE SCAM WORKS
PIN HOLE CAMERA (ACTUAL SIZE) WEIGHT: 1/2 OUNCE
ANTENNA
PIN HOLE LENS
LONDON UNDERGROUND TICKET MACHINE
Always protect your PIN
HIDDEN CAMERA IS ATTACHED WITH DOUBLE SIDED TAPE TO CAPTURE PIN NUMBER DETAILS
CRIMINAL TAPES CARD SKIMMER OVER CARD SLOT READER OF TICKET MACHINE. IT CAN RECORD MAGNETIC STRIP DETAILS OF CARDS

Fig 3. SCAMING work in ATM

Hackers put a scanner where ATM inserted that scan and copy the ATM code which is encrypted in black magnetic part of ATM card and there is a hidden camera of size 0 and with a little weight about ½ OUNCE is fitted very secretly about the keyboard of ATM machine which copy the users secrete password and sent it through small but powerful antenna to the hackers system.

So customer should be very careful when he/she get transition from ATM. Customer should be aware that there is no camera putted in the ATM machine from where you are getting transition and whenever you are entering the password from the keyboard that should be hidden from the hand or fully covered from the body so nobody can watch it outsider.

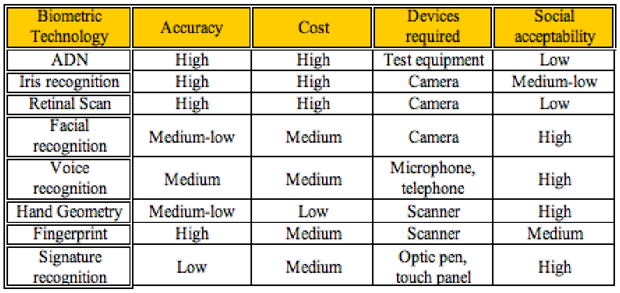
Table 2 advantages and disadvantages of token based authentication technique

Advantages	Disadvantages
1.More secure to use than user ID and password	1.Involves additional costs, such as the cost of token and any replacement fees.
2.inhance the image of organization by securing user credentials more effectively.	2.Users always need to carry the token with them.
3.Users don’t need to remember complex password.	3.Users need multiple tokens for multiple web sites and devices.
4. Can be used for login and transaction authentication.	4.Does not protect fully from man-in-the middle attacks(i.e. attacks where an intruder intercepts a user’s Session and steals the user’s credentials by acting as proxy between the user and the authentication Device without the users knowledge).

2.3. Biometric based Authentication Technique

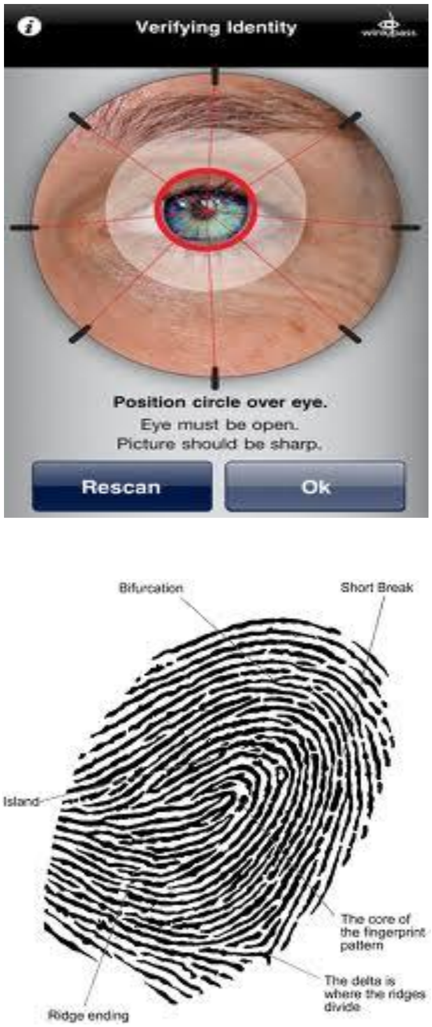
Biometrics authentication systems recognizes individual based upon one or more physical or behavioral traits. Biometrics systems authorizes the users by asking questions who he or she is? According to Zhu [19] biometrics provides the highest level of security among all other techniques. One characteristics of this method is physiological, related to the shape of the human body. Physiological characteristics includes fingerprints, iris recognition, face recognition and DNA [20]. It provides the best level of security, but still cannot be used because of its high costs. This cutting edge technology involves cost of device, cost of deployment and cost of support. There are some environmental issues which make the usage of biometrics difficult. For example, it is not reliable to use a sound recognition based technique in a noisy environment. The major drawback of this technique is that such systems improvement becomes very expensive [3]. However, this type of approach provides the highest level of security.

Table 3. comparison of different biometric technologies



Biometric Technology	Accuracy	Cost	Devices required	Social acceptability
ADN	High	High	Test equipment	Low
Iris recognition	High	High	Camera	Medium-low
Retinal Scan	High	High	Camera	Low
Facial recognition	Medium-low	Medium	Camera	High
Voice recognition	Medium	Medium	Microphone, telephone	High
Hand Geometry	Medium-low	Low	Scanner	High
Fingerprint	High	Medium	Scanner	Medium
Signature recognition	Low	Medium	Optic pen, touch panel	High

The above table compares some of the biometric systems used lately, from the point of view of accuracy, cost, devices required and social acceptability.


Verifying Identity
Rescan
Ok
Bifurcation
Short Break
Island
The core of the fingerprint pattern
The delta is where the ridges divide
Ridge ending

Position circle over eye.
Eye must be open.
Picture should be sharp.

Fig 4 Verifying identity and Thumb impression

Knowledge based techniques are the most widely used authentication techniques and include both text based and picture based passwords.

Facial recognition:

Table 4. Advantages and disadvantages of Facial recognition biometric technique

Advantages	Disadvantages
1. Non intrusive	1. 2D recognition is affected by changes in lighting, the person's hair, the age, and if the person wear glasses.
2. Cheap technology.	2. Requires camera equipment for user identification; thus, it is not likely to become popular until most PCs include cameras as standard equipment.

Voice recognition:

Table 5. Advantages and disadvantages of Voice recognition biometric technique

Advantages	Disadvantages
1. Non intrusive. High social acceptability.	1. A person's voice can be easily recorded and used for unauthorised PC or network.
2. Verification time is about five seconds.	2. Low accuracy.
3. Cheap technology.	3. An illness such as a cold can change a person's voice, making absolute identification difficult or impossible.

Signature recognition:

Table 6. Advantages and disadvantages of Signature recognition biometric technique

Advantages	Disadvantages
1. Non intrusive.	1. Signature verification is designed to verify subjects based on the traits of their unique signature. As a result,

	individuals who do not sign their names in a consistent manner may have difficulty enrolling and verifying in signature verification.
2. Little time of verification (about five seconds).	2. Error rate: 1 in 50.
3. Cheap technology.	

DNA:

Table 7. Advantages and disadvantages of DNA biometric technique

Advantages	Disadvantages
1. Very high accuracy.	1. Extremely intrusive.
2. It impossible that the system made mistakes.	2. Very expensive.
3. It is standardized.	

Retinal scanning:

Table 8. Advantages and disadvantages of Retinal scanning biometric technique

Advantages	Disadvantages
1. Very high accuracy.	1. Very intrusive.
2. There is no known way to replicate a retina.	2. It has the stigma of consumer's thinking it is potentially harmful to the eye.
3. The eye from a dead person would deteriorate too fast to be useful, so no extra precautions have to been taken with retinal scans to be sure the user is a living human being.	3. Comparisons of template records can take upwards of 10 seconds, depending on the size of the database.
	4. Very expensive.

Iris recognition:

Table 9. Advantages and disadvantages of Iris recognition biometric technique

Advantages	Disadvantages
1. Very high accuracy.	1. Intrusive.
2. Verification time is generally less than 5 seconds.	2. A lot of memory for the data to be stored.
3. The eye from a dead person would deteriorate too fast to be useful, so no extra precautions have to been taken with retinal scans to be sure the user is a living human being.	3. Very expensive

Fingerprint:

Table 10. Advantages and disadvantages of fingerprint biometric technique

Advantages	Disadvantages
1. Very high accuracy.	1. For some people it is very intrusive, because is still related to criminal identification.
2. Is the most economical biometric PC user authentication technique.	2. It can make mistakes with the dryness or dirty of the finger's skin, as well as with the age (is not appropriate with children, because the size of their fingerprint changes quickly).
3. it is one of the most developed biometrics	3. Image captured at 500 dots per inch (dpi). Resolution: 8 bits per pixel. A 500 dpi fingerprint image at 8 bits per pixel demands a large memory space, 240 Kbytes approximately → Compression required (a factor of 10 approximately).
4. Easy to use.	
5. Small storage space required for the biometric template, reducing the size of the database memory required	
6. It is standardized.	

Hand Geometry:

Table 11. Advantages and disadvantages of Hand Geometry biometric technique

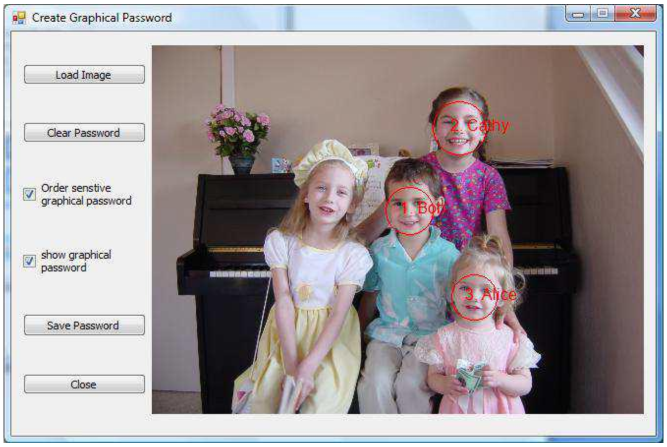
Advantages	Disadvantages
1. Though it requires special hardware to use, it can be easily integrated into other devices or systems.	1. Very expensive
2. It has no public attitude problems as it is associated most commonly with authorized access.	2. Considerable size.
3. The amount of data required to uniquely identify a user in a system is the smallest by far, allowing it to be used with Smartcard easily.	3. It is not valid for arthritic person, since they cannot put the hand on the scanner properly.

2.4. Graphical password authentication

Human can remember pictures better than the text based passwords or the combination of alphanumeric with symbolic passwords so the proposal is to graphical passwords are the alternative to the text based password schemes and it is more easy to use and more secure than text based password[5].
First technique is recognition based and second is recall based graphical authentication techniques.

i. Recognition based technique

In recognition based techniques, In this method user have to choose several figures form a pool of figures and to create a picture password [16,17], User have to memories this picture pattern also. During authentication phase user have to identify the correct images that they have selected earlier. Basically user have to select pixel position of each images that is used as a password

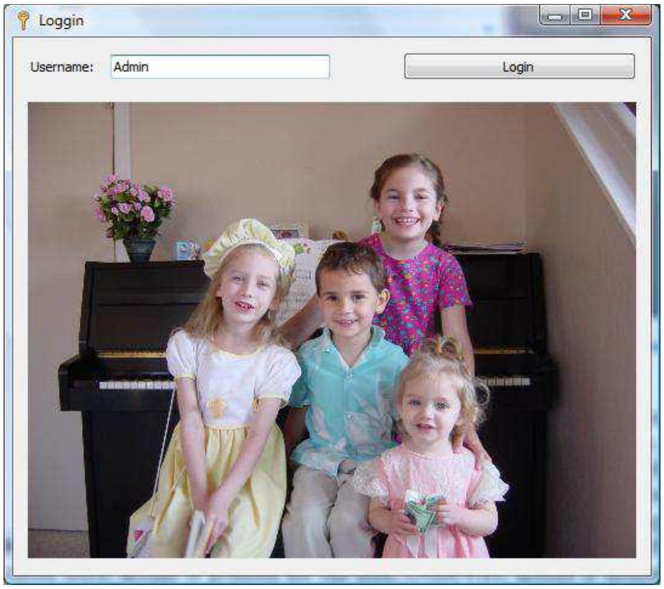


☑ Order senstive graphical password

☑ show graphical password

Figure 5. An example of creating a graphical password using the proposed system

In Figure 5, we show an example of a user creating a graphical password. In this example, the user chooses a picture of his or her kids by pressing “Load Image button”. Then the user clicks on the kids faces in the order of their ages (order is enforced). For each selected region, the user types the kid’s name or nickname.



Username: Admin

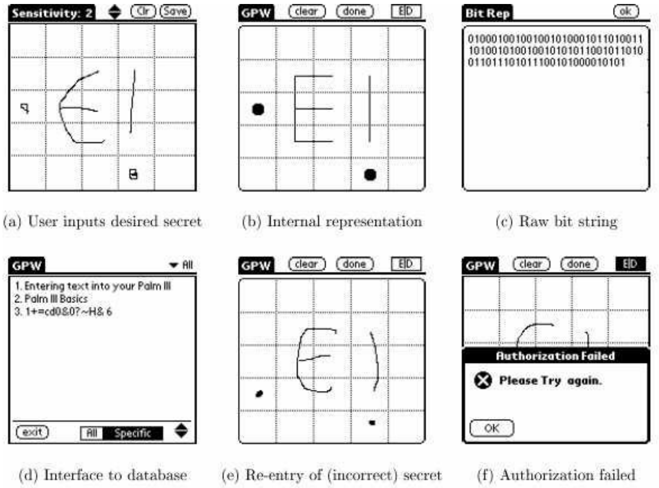
Figure 5. Login Screen

For authentication, the user first enters his or her username. The system, then, displays the registered picture.

The user, then, has to correctly pick the POIs and type the associated words. At any time, typed words are either shown as asterisks (*) or hidden. In Figure 2, we show an example of the login screen.

ii. Recall based Authentication Techniques

In the recall based techniques user need to recall or remember the particular images or drawing which he or she has already generated in the phase of registration. There are lots of techniques provided for recall based scheme. Here we have selected a scheme proposed by Jemyn et.al[18] called Draw-A-Secret(DAS). Figure 3 for our analysis. In this scheme user need to design a picture signature on a 2D grid. The coordinate occupied by the picture drawn by user are stored in the order of drawing. In the authentication process user need to redraw the same picture. If the picture touches the same grid, then user is authenticated.



(a) User inputs desired secret (b) Internal representation (c) Raw bit string

010001001001001010001011010011
101001010010010101011001011010
0110111010111001010000010101

1. Entering text into your Palm III
2. Palm III Basics
3. 1+=cd0&0?~H& 6

Authorization Failed
Please Try again.

(d) Interface to database (e) Re-entry of (incorrect) secret (f) Authorization failed

Figure 7 Draw-A-Secret (recall based technique) proposed by Jemyn[18].

After applying these techniques the result are obtained that 90% of all users successfully authenticated with these techniques, while only 70% succeeded using text based passwords [4].

3. SECURITY FROM PASSWORD ATTACKS

3.1 Brute Force Attack

Brute force attack uses an algorithm that produces every possible combination of words to crack the password. Text based password contain 94^N number of space where 94 is the number of printable characters with space and N is the length. It has always proven successful against text based password because of its ability to check all possible combination of password [5]. That's why users are advised to select a stronger and complex password to prevent discovery from brute force attack. However, GUA proves more resistant to brute force attacks because attack software needs to produce all possible mouse motions to imitate passwords especially when trying to recognition and recall the graphical passwords [5].

3.2 Dictionary Attack

If any user uses a weak password that can be crack by dictionary attack after checking the word found in dictionary. Dictionary attack on GUA would be waste of time because graphical password is a method of using mouse input type recognition [6]. It is more difficult and complex to use the automated dictionary method to produce all possibility of a single user click of an image in recognition and recall based password attack than a text based attack [6-8].

3.3 Spyware Attack

This type of attack uses a small application which installed on a user's computer accidentally or secretly to record sensitive data during mouse movement or key press. This is a type of malware which secretly store this information and reports back to the attackers system. With a few exceptions, these key-loggers and listening spywares are unproven in identifying mouse movement to crack graphical passwords. Even if the movement is recorded, it is still not accurate in identifying the graphical password. Other information is needed for this type of attack namely window size and position as well as the timing [9].

3.4 Shoulder Surfing Attack

Password can be identified by looking over a person's shoulder. This type of attack is more frequent in crowded areas where it is not infrequent for people to stand behind another queuing at ATM machines. There are some cases in which key pin number can be record using ceiling and wall cameras placed near ATM machines. Properly shield the keypad when entering the pin number can be avoid pin numbers being recorded or remembered by attackers [10-12].

3.5 Physical Attack

When a user directly accesses to the data from the server then it is called physical attack. It makes a chance for attacker to bypass the authentication process and directly access to the resources [5]. There are two situation are created in text password and graphical password by physical attack is possible to access the image gallery and password database. In the first situation, if image gallery is accessed by attacker, it is possible to change the images and make a miss functioning for the system in next login and registration processes. If attacker access to the password database then it is possible to login to the system by any user name [13-15].

4. CONCLUSION

This paper represents the comparison between different types of authentication process and their merits and demerits. Text based password technique is widely used but it is very unsecured. So it is very rarely used where high level of security needed. Token based techniques are widely used at this time but there are some drawbacks of this technique. Biometric techniques are not widely used due to there initial development cost and there maintenance cost, but it is very secure. Now a days developer working on the graphical password to overcome the drawbacks of the all above techniques.

REFERENCES

[1] A.S. Patrick,A. C. Long and S. Flinn, "HCL and Security System" presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA. 2003.

[2] K. Gilhooly, "Biometrics: Getting Back to Business", in Computerworld, May 09, 2005.

[3] Lin, P. L. and Huang, L. W. (2008), Graphical Passwords using Images With random Tracks of Geometric Shapes, 2008 Congress on Image and Signal Processing, IEEE 2008, pp 27-31.

[4] Gaurav Agrawal, Saurabh Singh, Ajay Indian, "Analysis of Knowledge based graphical password authenticaiton" SuperStar Virgo, Singapore, August 3-5, 2011.

[5] Arash Habibi Lashkari, Azizah Abdul Manaf, Masin Masroom, "A Secure Recognition Based Graphical Password By Watermarking" in 11th IEEE International Conference on Computer and Information Technology, 2011.

[6] Chiasson, S., et. al., "Multiple Password Interference in Text Password and Click-Based Graphical Passwords", ACM, 2009.

[7] Wiedenbeck, S., J.-C. Birget, And A. Brodskiy, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choce, in Symposium On Usable Privacy and Security(SOUPS)", 2005.

[8] Dhamija, R. and A. Perrrig, D'ej'a Vu; "A User Study. Using Images for Authentication, in The proceeding of the 9th USENIX security Symposium", 2000, USENIX.

[9] Man S., et al., "A password scheme strongly resistant to spyware, in Int. Conf. on Security and Management" 2004: Las Vegas.

[10] Forget, A., S. Chiasson, and R. Biddle, Shoulder-Surfing Resistance with Eye –Gaze Entry in Cued-Recall Graphical Passwords. ACM, 2010.

[11] Lashkari A.H., S.F., Omar Bin Zakaria and Rosli Saleh, Shoulder Surfing attack in graphical password authentication. 2009, International Journal of Computer Science and Information Security (IJCSIS).

[12] Man, S., D. Hong, and M. Mathews, A Shoulder-Surfing Resistant Graphical Password Scheme – WIW, in International conference on security and management. 2003: Las Vegas.

[13] CAPEC, Standard Abstraction Attack Pattern List (Release 1.6). 2011, Common Attack Patterns Enumeration and Classification (CAPEC): USA.

[14] Todorov, D., Mechanics of User Identification and Authentication. 2007: Auerbach Publications.

[15] Gordon, P., Data Leakage- Threats and Mitigation, in InfoSec Reading Room. 2007, SANS Institute.

[16] Birget, J.C., D. Hong, and N. Memon."Graphical Passwords Based on Robust Discretization". IEEE Trans. Info. Forensics and Security, 1(3), September 2006.

[17] Suo X., Zhu Y., Own G. S., "Graphical Password: ASurvey", Computer Security Applications Conference IEEE, 21st Annual, Tucson AZ: Dec 2005, pp. 472.

[18] I Jermyn, A. Mayer, F. Monrose, M. K. Reiter and A. D. Rubin, "The Design and Analysis of Graphical Password" in proceedings of the 8 th USENIX Security Symposium, 1999.

[19] Suo X., Zhu Y., Own G. S., "Graphical Password: A Survey", Computer Security Applications Conference IEEE, 21st Annual, Tucson AZ: Dec 2005, pp. 472.

[20] Ratha, N.K., Thomas J., Bolle, R.M "Enhancing security and privacy in biometrics-based authentication systems", IBM Systems Journal, 2001.

[21] Akula S., Devisetty V.,"Image Based Registration and Authentication System"Midwest Instruction and Computing Symposium, 2004.