World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:12, No:2, 2018

Hybrid Authentication Scheme for Graphical Password Using QR Code and Integrated Sound Signature

SalimIstyaq, Mohammad Sarosh Umar

***Abstract*—**Today, the mankind is in the stage of development, every day comes with new proposal of technology, in order to secure these types of technology, we also prepare high yielding security modules to conserve these resources. The capacity of human brain to recognize anything is far more than any species; this is all due to our developing cycle of curiosity. In this paper, we proposed a scheme based on graphical password using QR Code which provides more security to the recent online system. It also contains a supportive sound signature. In this system, authentication is done using sequence of images in QR code form. Users select one click-point per image with the help of QR scanner or recognizer. The encoded phrase in a QR code emphasizes the minimum probability of attacking via shoulder surfing or other attacks.

***Keywords*—**Graphical password, QR code, sound signature, image authentication, cued click point.

I. Introduction

THE concept of introducing password is to protect the information from malicious activity, and to conserve from illegal access. Passwords are used to:

(a) Access Control: Restriction of access includes authentication & authorization.
(b) Authorization: The process used to decide if the authenticated person is allowed to access specific information
(c) Authentication

Sometimes hackers predict the passwords set by users if it is alphanumeric based. Users tend to choose memorable password. Unfortunately, it means that passwords follow some easily recalling patterns that can be predicted easily. Random strings are generated as password [1] to provide authentication. Users cannot easily recall such passwords.

A. Security Analysis of GUA

Here, we briefly examine some of the possible techniques for breaking graphical passwords and try to do a comparison with text-based passwords.

Brute force attack [8]: The textual passwords are mostly affected by this attack. On the other hand, it is a bit difficult to impose these attacks easily on graphical based passwords. It also proved that recall based password schemes are more secure than recognition based ones, when it comes to the resistivity towards brute force attack. Draw-a-secret (DAS) is only the Graphical Password Scheme which is completely resistant to brute force attack.

Spyware attacks are generally not applicable to graphical system but sometimes screen capturing is possible, but in modern graphical based systems, the background or reflexives are invisible. These attacks are venomous for text based passwords as many types of key loggers are available.

Shoulder surfing attacks [8] are like text based passwords. Most of the graphical authentication methods are vulnerable to shoulder surfing. Up till now, only a few recognition based methods claim to resist shoulder surfing. None of the recall based methods are considered for shoulder-surfing resistant.

Social engineering attacks are useless on the Graphical User Authentication (GUA).

Guessing attacks [8]: This type of attack is not working in any manner of capturing graphical passwords because for a human species the combination of trillions of pixels will be impossible to recognize.

Due to recent attacks like hacking passwords, confidential information etc., it is important for all organizations to protect their resources from such malware by providing the robust security system. As per [7], currently the authentication methods can be broadly divided into three main areas as Token based, Biometric based, and Knowledge based, as shown in Fig. 1.

B. Classification of Current Authentication Methods

Token based technique [7] includes authentication through plastic cards, RFID chips, Magnetic Cards in which a unique id is encoded through electronic writers which is used as password key in the specific modules. Biometric based [9], [10] authentication system includes finger scan, palm scan, facial scan and iris scan. Here we use the biological factors of the body in authentication. But system cost is very high. Knowledge based technique [7], [8] includes both textual and graphical password. The authentication technique in these systems is totally dependent on users' logic [2].

II. Related Work

There are several researches done in this area, the best of the work done is based on Passface [4], [7]. Brostoff and Sasse took some research on Passface [17] which show some analysis on graphical passwords. They concluded that there are problems for handling in operating such schemes. On the

Salim Istyaq is with the Computer Engineering, University Polytechnic, Faculty of Engineering & Technology, Aligarh Muslim University, Aligarh-India (e-mail: salim.ubp@ amu.ac.in).
Mohammad Sarosh Umar is with Department of Computer Engineering, A.M.U. Aligarh-India (email: saroshumar@zhcet.ac.in).

other hand Blonder schemes [8] are truly based on cued recall, in which a user selects many points on single image to login.

Fig. 1 Classification of Authentication Methods

The main disadvantage of preceding method is that there are less number of password spaces and also password predefined region is easily distinguishable [5], [6]. Our system is the composition of PCCP authentication. In this authentication scheme the users have to make selection by five times on five different QR Codes instead of making impression five times on single QR set. It also provides compatibility for the user to start from the point where they do wrong selection instead of initial start.

In Fig. 3, each click results in displaying a next-QR code which affects user down a path as they click on their queued points. For any malfunctioning on the system regarding to illegal attempts for password, here we secure this system by approaching no warning exit for those types of users. The users also have tendency to create or select any QR code by their own.

Passface [11] includes technique that recognizes face as the password. The users are provided by some images of faces, in which they have to select some faces as their passwords. At the time of login, these images are displayed as random grid of images, now the users have to select the right image for their authentication. Passfaces can be predicted as these are affected by race, gender and attractiveness.

Syukri et al. [12] proposed a system where authentication was conducted by having the users draw their signature using mouse. These techniques include drawing of signature and their verification, because it is hard to copy signature of any user and there is no condition of memorizing the password again and again. Sometimes the user faces many problems in making passwords through mouse or by stylus.

Dhamija and Perrig [13] proposed a method which is based on "Hash Visualization" in which user first selects the combination of images from the random set. For a user to be authenticated, he or she would have to identify the preselected images. The main problem in their scheme is that server has to create the records of each selected image in text. Also, it is a bit time consuming and tedious for the users to select images from the database [13].

Umar and Rafiq [3] proposed a graphical interface for User Authentication [15] in which the user draws some geometrical objects to authenticate him. In this scheme there are mxn grids and each grid is further divided into four parts by diagonal lines as shown in Fig. 2 formed by joining adjacent points horizontally and vertically. That gives 4x6=24 horizontal and 5x5=25 vertical lines which makes a total of 24 +25 = 49 (horizontal and vertical) lines. Thus there are a total of

$$P(5,4) \Rightarrow 80 + 80 + 49 = 209 \text{ objects} \quad (1)$$

As per [3], these 209 objects, i.e. lines and triangles, can be chosen to select a password by drawing some of these objects in an easy and efficient manner as shown in Fig. 2. The scheme is quite suitable for hand held devices.

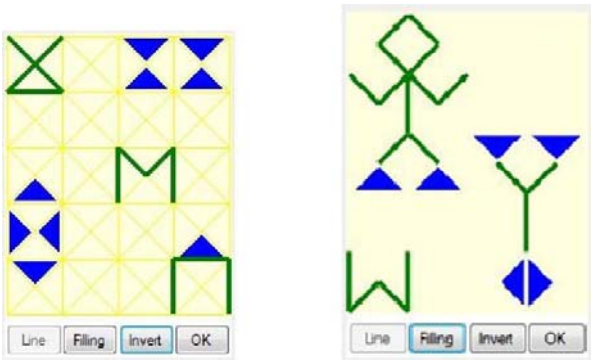


Fig. 2 Graphical interface proposed by [3]

Istyaq [14] defines a way of protecting the information from shoulder surfing attack that is combining QR Code based graphical authentication [16] with One Time Password scheme.

III. Proposed Work

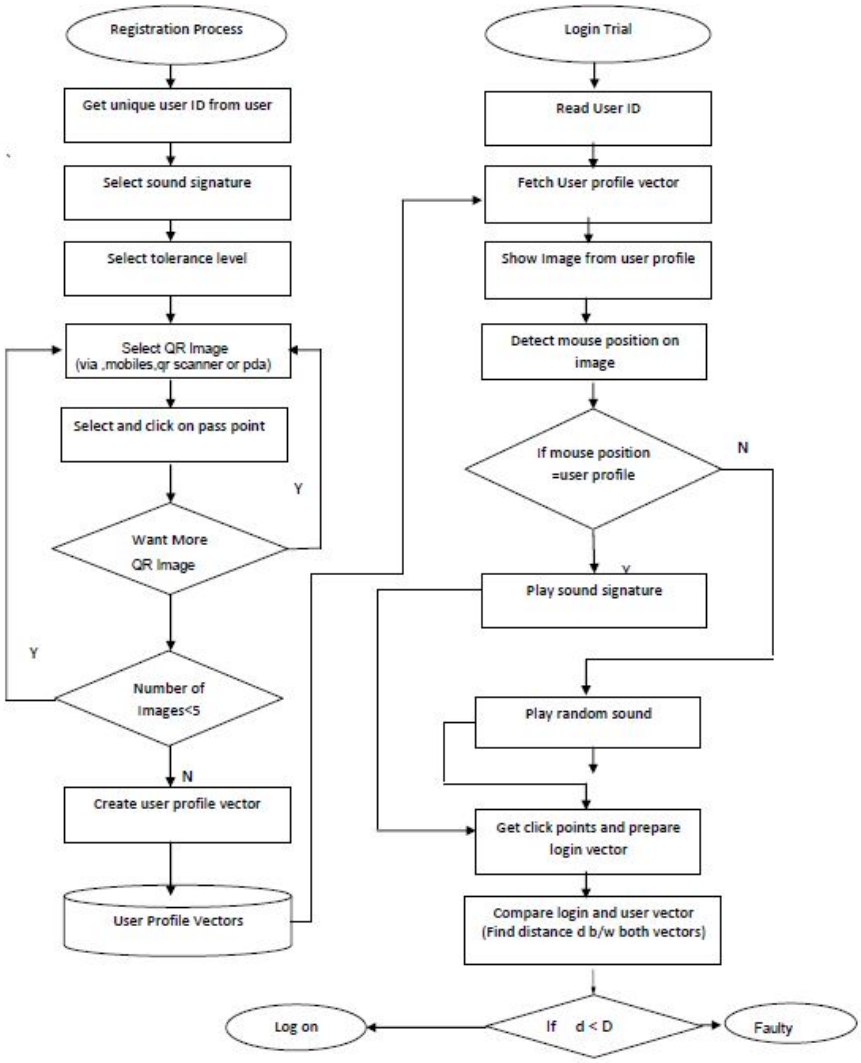
The GUA techniques are not widely introduced due to the problems of shoulder surfing and many other vulnerabilities. But here, we introduced the GUA system which is resistant to shoulder surfing and provide a robust authentication. Our system is the combination of recognition and pure recall based technique that uses two way authentication systems including extra multimedia content like audio as a password string.

A. User Profile Vector

In the first run a user has to make his impression in terms of profile vector, these are composed of (user id, sound frequency, tolerance) and detailed vector (QR image, Click points).

It is mandatory to select a voice signature in parallel within the selection of images. It is also important to adjust tolerance level which will decide whether the user is faulty or legal. To create detailed vector, the user first scans the QR codes via scanner or mobile devices respectively with the choice. Then user has to select the sequence of QR codes images and click on each code at the click points of his/her choice in order to

make profile vector.



STEP 1: REGISTRATION PHASE STEP 2: LOGIN PHASE

Fig. 3 Flowchart

TABLE I
INVALID USER OR ILLEGAL (5 ATTEMPTS PER LOGIN)

QR Image	Click points
i1	(113, 989)
i2	(411,569)
i3	(311,986)
i4	(711,548)
i5	(166,589)

Fig. 4 Bar Code to Image Name

B. Tolerance of System

After formation of login vector, the system will calculate the Euclidian distance between both vectors that are formed at the initial and final stage (login vector and profile vector). Euclidian distance between both the vectors p and q are given by:

$$d(j, k)^2=(j1-q1)^2 +(j2-q2)^2+…….(jn, qn)^2$$

$$\text{Or}\sqrt{\sum_{i=1}^{n}(ji-ki)^2}$$

TABLE II
LEGAL OR VERIFIED USER (5 ATTEMPTS PER LOGIN)

S.No.	User Login	Trails	Accepted times	Rejection times
1	N1	5	5	0
2	N2	5	4	1
3	N3	5	5	0
4	N4	5	5	0
5	N5	5	5	0

IV. Result Analysis

We just take an experimental approach in order to take survey. Five students are asked to register through the proposed system. Each person is given five login trails i.e. five times as legal user and five times for illegal access or not valid user. Table II shows the analysis result conducted by the legal user and Table III shows the result from the illegal activity.

TABLE III
Invalid User or Illegal (5 Attempts Per Login)

S. No.	User Login	Trails	Accepted times	Rejection times
1	u1	5	0	5
2	u2	5	0	5
3	u3	5	2	3
4	u4	5	1	4
5	u5	5	1	4

V. Security and Usability

As this system is hybrid that uses more than one technique for authentication, therefore it created a complex path for the corrupt or illegal users to bypass the system modules like scanning QR Code, accessing OTP. There are different types of system as shown in Fig. 5. Our proposed system is much secure as compared with others as shown in Fig. 6.

The possibilities of passwords generated in this system are very complex and depends on the random generated right QR code with other codes and finally a onetime password is to be sent on the users' Email id/Mobile No.

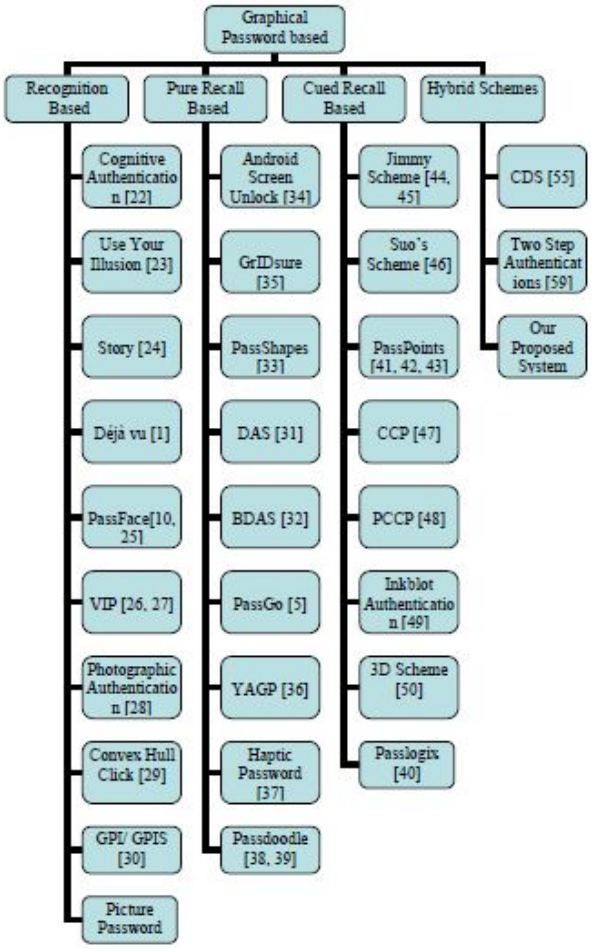


Fig. 5 Different types of system

Graphical Password Schemes/ Systems	Type of Scheme	Resistant to Possible Attacks					
		Brute Force Attack	Dictionary Attack	Guessing Attack	Spy-ware or Naïve Key logging	Shoulder Surfing Attack	Phishing Attack or Social Engineering
Blonder's Scheme	Recognition Based	Y	N	Y	N	Y	N
DAS	Pure Recall Based	N	Y	Y	N	Y	N
BDAS	Pure Recall Based	N	-	-	-	-	-
Qualitative DAS	Pure recall Based	N	-	-	-	-	-
Syukri Algorithm	Pure recall Based	N	Y	Y	N	Y	N
PassPoints	Cued Recall Based	Y	N	Y	N	Y	N
PassFace	Recognition Based	Y	Y	Y	N	Y	N
PassGo	Pure Recall Based	Y	-	-	-	-	-
Passlogix	Cued Recall Based	Y	N	Y	N	Y	N
PassMap	Pure Recall Based	Y	N	-	N	Y	N
Passdoodle	Pure Recall Based	N	-	-	-	-	-
Viskey SFR	Pure Recall Based	Y	N	Y	N	Y	N
Perrig and Song	Recognition Based	Y	N	Y	N	Y	N
Sobrado and Birget	Recognition Based	Y	N	Y	N	N	N
Man et al Scheme	Recognition Based	Y	N	N	Y	Y	N
Picture Password Scheme	Recognition Based	Y	N	Y	N	Y	N
CDS	Hybrid	-	-	-	-	Y	-
WIW	Recognition Based	-	-	-	-	Y	-
Association based scheme	Recognition Based	-	-	-	-	Y	-
Déjà Vu	Recognition Based	Y	-	Y	-	-	-
Haptic Password Scheme	Pure Recall Based	-	-	-	-	Y	-
YAGP	Pure Recall Based	Y	-	Y	-	Y	-
Photographic Authentication	Recognition Based	-	Y	-	-	-	-
Two Step Authentication	Hybrid	-	-	-	Y	N	Y
Our Proposed System	Hybrid	Y	Y	Y	Y	Y	Y
Note: Y= Yes resistant to attack N=No not resistant to attack							

Fig. 6 Comparison of our system

VI. CONCLUSION

In order to protect the information from all the attacks, our aim is to provide a complex strength which overcomes the attacks. We have proposed a hybrid technology in the graphical password scheme correlated with QR codes also uses sound signature in order to enhance the stability of the system. This system is helpful when logging after a long while. In future, other pattern may be used for recalling purpose like animation, touch, videos. Study shows that these patterns are very useful in recognizing the objects which in terms provide a good era of this system.

REFERENCES

[1] William Stallings and Lawrie Brown. "Computer Security: Principle and Practices." Pearson Education, 2008.
[2] Authentication: http://www.objs.com/survey/authent.htm.
[3] Mohd. Sarosh Umar and Mohd Qasim Rafiq, "A Graphical Interface for User Authentication on Mobile Phones", in ACHI 2011: The Fourth International Conference on Advances in Computer-Human Interactions, Guadeloupe, France, February 23-28, 2011.
[4] L. Sobrado and J.C. Birget, "Graphical Passwords", The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol 4, 2002,http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm.
[5] Patric Elftmann, Diploma Thesis, "Secure Alternatives to Password-Based Authentication Mechanisms" Aachen, Germany October 2006.
[6] Xiayuan Suo, Ying Zhu, and G. Scott. Owen, *"Graphical Passwords: A Survey"*, In Proceedings of Annual Computer Security Applications Conference, 2005.
[7] Mr. Pratik, A Vanjara and Dr. Kishor Atkotiya, Analysis &Design 'Graphical Password Authentication Using Cryptography Algorithms' Volume: 1 | Issue: 9 | September 2012 ISSN - 2250-1991.
[8] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.
[9] W. Jansen, "Authenticating Mobile Device User through Image Selection," in Data Security, 2004.
[10] W. Jansen, "Authenticating Users on Handheld Devices "in Proceedings of Canadian Information Technology Security Symposium, 2003.
[11] Passfaces Corporation. The science behind Passfaces, White paper, http://www.passfaces.com/enterprise/resources/white_papers.htm.
[12] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse", In Third Australasian Conference on Information Security and Privacy (ACISP): Springer Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.
[13] Rachna Dhamija and Adrian Perrig, "Deja Vu: A User Study. Using Images for Authentication" in Proceedings of the 9th USENIX Security Symposium, August 2000.
[14] Salim Istyaq, "Hybrid Authentication System Using QR Code with OTP", in International Journal of Computer, Electrical, Automation, Control and Information Engineering (World Academy of Science, Engineering and Technology), Vol: 10, No:6, 2016, PP. 1194-1197.
[15] Mohammad Sarosh Umar and Mohammad Qasim Rafiq, "*A Novel Graphical Interface for User Authentication on Mobile Phones and Handheld Devices"*, International Journal On Advances in Intelligent Systems, volume 4, numbers 3 and 4, pp 380 to 387, 2011 (IARIA Journals) Publication Date April 30, 2012.
[16] Salim Istyaq and M. Sarosh Umar, "Encoding Passwords Using QR Image for Authentication", 2nd International Conference on Next Generation Computing Technologies(NGCT-2016), Dehradun, India, 14-16 October, 2016, 978-1-5090-3256-3/16/$31.00 ©2016 IEEE.
[17] Brostoff, S., Sasse, M.A., 2000. Are Passfaces more usable than passwords: a field trial investigation? In:

Mr. Salim Istyaq (M 2016) became Member of **World Academy of Science, Engineering and Technology** in May 2016.The place of birth is Aligarh, U.P. India. The Author has B.Sc. Engineering in Computer, M,Tech. in Communication & Information Systems. Currently pursuing Ph.d. in Computer Engineering from Aligarh Muslim University, Aligarh, U.P. India. Presently, working as an Assistant Professor in Computer Engineering, University Polytechnic, Faculty of Engineering & Technology, A.M.U., Aligarh-202002, U.P.-India since 2004 to till date. Earlier, worked as Guest Faculty in ECE Department, Jamia Millia Islamia, New Delhi-110025. Also worked in Computer Engineering, Al-Mergheb University, Alkhoms, Libya. Author has been published 16 Papers in International Journals (02 in **World Academy of Science, Engineering and Technology**) and International (04 in IEEE) Conferences. Review Committee Member in Editorial Board of various International Journals (**World Academy of Science, Engineering and Technology**, OMICS, ARSEAM, IJETAE).

Dr. Mohammad Sarosh Umar is working as Professor and Chairman in Department of Computer Engineering, A.M.U. Aligarh-India. He has published several papers in international journals & Conferences and also has patents.