Tri-Pass: a new graphical user authentication scheme

Elmira Yesseyeva, Kanat Yesseyev, Mustafa M. Abdulrazaq, Arash Habibi Lashkari, Mohammad Sadeghi

***Abstract*—**User authentication is one of the most significant issues in computer and information security. Currently, the most prevalent and well-established authentication approach is based on the use of alphanumeric passwords. The first text-based authentication scheme was introduced in the late 1960s, and so far the most computer systems, networks and applications use this technique to authenticate their users. With the growth of users and services, this approach became susceptible to several vulnerabilities and drawbacks. In contrast to text-based passwords, graphical authentication mechanisms promise greater security, memorability and usability. In this paper, we propose and evaluate a new graphical password scheme called Tri-Pass with the purpose of improving the user authentication in both security and usability.

***Keywords*—** Graphical password, recognition-based schemes, pure recall-based schemes, cued recall-based schemes

I. INTRODUCTION

In any organization, regardless the size and nature of the company, information security is a major concern. The protection of information and implementation of adequate security mechanisms with respect to confidentiality, integrity and authenticity are especially important in today's increasingly interconnected business environment [1]. Traditional textual passwords are perhaps the most prevalent and convenient authentication method because they are familiar to all users, easy to use, and cheap to implement.

The known weakness of traditional user authentication is a tendency to choose passwords with predictable characteristics, which in turn reduces password strength and makes it vulnerable to various attacks [2,6]. Sufficiently secure password should be at least eight characters or longer, random, without any semantic content, with mix of uppercase and lowercase letters, digits, and special symbols. Generally, users ignore any tips and recommendations for creating a secure password. Moreover, some users write down their passwords on a piece of paper, share passwords with others or use the same password for multiple accounts [3,8]. Most of the common attacks namely brute force search attack, dictionary attack, guessing attack, shoulder surfing attack, spyware attack, and social engineering attack can use these weaknesses for attacking to the system.

In attempt to overcome the weaknesses of traditional textual password, graphical password schemes have emerged as a possible security enhancement. Human's ability to better recognize visual information as opposed to verbal information makes the graphical passwords easier to remember [4]. The first graphical password based scheme was introduced by Greg Blonder in 1996. In his scheme the user is asked to click on several locations on the image to create a password. To login the user must click on previously selected locations on the image or close to those locations [5]. Today, there is a growing interest in graphical passwords but most of the graphical password authentication schemes have not been widely adopted.

II. LITERATURE REVIEW

Currently, user authentication mechanisms fall under three main categories: biometric authentication (something you are), token-based authentication (something you have), and knowledge-based authentication (something you know) [6,24].

Biometric authentication refers to the identification of some unique physical or behavioral characteristics of the user. Examples include fingerprint, iris scan, handwritten signature, voice recognition, and others. Even despite the fact that biometric passwords are very efficient, easy to manage and do not require memorizing, they are expensive solutions, which cannot be widely adopted [7,16].

Token-based authentication is a technique where in order to be authenticated the user is required to present a token. Unfortunately, the token can be easily stolen, forgotten or duplicated. Also token-based authentication scheme is not convenient for use because special additional hardware devices are needed [8,14].

This manuscript is part of the final projects of three students who worked in graphical passwords in, Limkokwing University of Creative Technology, Cyberjaya, Malaysia.

Elmira Yesseyeva, Kanat Yesseyev, and Mustafa M. Abdulrazaq, were students in the graphical passwords research group (itsmeelmira@hotmail.com, kana.ky6@gmail.com, sas.usmc@gmail.com).

Dr. Arash Habibi Lashkari was supervisor of this group and advisor of research projects in Postgraduate Centre of Study (PGC), Limkokwing University of Creative Technology (a_habibi_l@hotmail.com).

Mr. Mohammad Sadeghi is head of Postgraduate Centre of Study (PGC), Limkokwing University of Creative Technology (m.sadeghi@limkokwing.edu.my).

Knowledge-based authentication can be classified into two categories: textual passwords and graphical passwords. Graphical passwords include recognition-based techniques and recall-based techniques. Using **recognition-based** techniques, in order to pass the authentication, user is required to recognize and identify a set of images selected earlier during the registration phase. Recall-based techniques categorized into: pure recall-based and cued recall-based. In **pure recall-based** category, the user is asked to recall and reproduce something created or selected earlier during the registration phase without being given any hint. In **cued recall-based** category, the technique proposes a hint that helps the user to recall and reproduce previously created or selected password more accurately [9,18].

A. RECOGNITION-BASED AUTHENTICATION SCHEMES

1) Déjà vu algorithm

In 2000 Dhamija and Perrig proposed a new graphical authentication scheme called Déjà vu algorithm, which is based on the perception of hash visualization technique. At registration phase the user is asked to choose a certain number of images from a collection of random non-describable abstract pictures generated by a system. Later, the user will be required to identify previously selected images in order to be authenticated [7]. The average registration and login time of this approach is much longer than in the traditional text-based approach. Also the server needs to store large number of pictures that may delay the authentication process while transferring over the network. Furthermore, the process of selecting and identifying a set of images from the picture database can be time consuming for the user [5].

Fig 1. An example of Déjà vu algorithm

2) Triangle algorithm

In 2002 Sobrado and Birget developed a new graphical password scheme called Triangle algorithm that is aimed to deal with shoulder surfing problem. At registration phase user is asked to choose a certain number of pass objects from 1000 proposed objects. Later, to authenticate, the system displays a variety of objects on the screen and the user is asked to click inside the area that the previously selected objects form. The action repeats for several times but every time the icons on the screen will shuffle and appear in different place [7]. Major disadvantage of this scheme refers to a very crowded display, so the user cannot distinguish the objects on the screen. Also the average registration and login time is much longer than in the traditional text-based approach. On the other hand, using fewer objects may lead to a smaller password space [5].

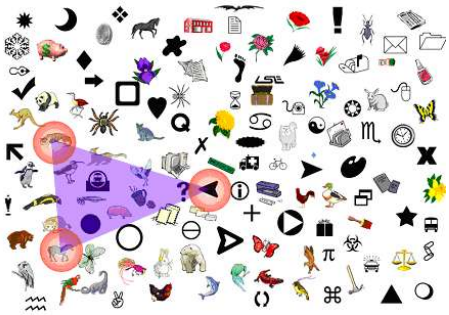


Fig 2. An example of Triangle algorithm

3) Passface algorithm

In 2000 Brostoff and Sasse from Real User Corporation proposed a new graphical authentication scheme that is called Passface algorithm. To create a password the user will be asked to choose a certain number of images of human faces from the picture database. At authentication phase user will be required to identify previously chosen faces in order to be authenticated. The user recognizes and clicks on the known face, and then the procedure repeats for several times. This technique is very memorable over long time periods. However, majority of the users tend to choose faces of people based on the obvious behavioral pattern, which makes this authentication scheme kind of predictable and vulnerable to various attacks [9]. Also it takes longer for login and registration than in traditional text-based password scheme.

Fig 3. An example of Passface algorithm

B. PURE RECALL-BASED AUTHENTICATION SCHEMES

1) Draw-a-Secret (DAS) algorithm

In 1999 Jermyn, Mayer, Monrose, Reiter, and Rubin proposed a new graphical password scheme called Draw-a-Secret algorithm. This scheme allows user to draw a unique password on a 2D grid. At registration phase the coordinates of the grids occupied by the drawn patterns are stored in order of the drawing. During authentication phase, the user is asked to redraw the picture by touching the same grids and in the same sequence [6]. Unfortunately, most of the users over a certain period of time forget their drawing order. Another drawback is that the users tend to choose weak graphical passwords, which as a result makes this authentication scheme kind of predictable and vulnerable to various attacks [5].

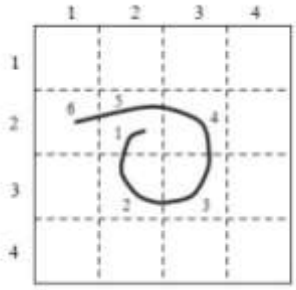


Fig 4: An example of Draw-a-Secret (DAS) algorithm

2) Grid selection algorithm

In 2004 Thorpe and Oorschot proposed a new graphical authentication scheme that is called Grid selection algorithm. Firstly, within a large selection grid user chooses a smaller grid for drawing. This adds an extra degree of complexity to the password. Then the user zooms in this piece of grid and creates a drawing like in original Draw-a-Secret (DAS) scheme. This technique of authentication dramatically increases the password space. However, it introduces additional job to memorize and time to input the password. In other words, the security enhancement is achieved by sacrificing password usability and memorability [7].

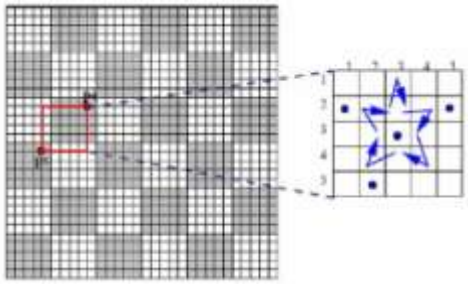


Fig 5. An example of Grid selection algorithm

3) Syukri et al. algorithm

In 2005 Syukri, Okamoto, and Mambo proposed a new graphical authentication scheme called Syukri et al. algorithm. During the registration phase user will be asked to draw the signature with an input device. At verification phase the system extracts the parameters of the signature that are stored in the database. The biggest advantage of this approach is that signatures are hard to fake [16]. Also there is no extra job to memorize the password. The main drawback is that drawing signature with a mouse is not an easy task. The obvious solution to this problem would be usage of a pen-like input device instead of mouse. However, such devices are not widely used and adding new hardware can be expensive [14].

Fig 6: An example of Syukri et al. algorithm

C. CUED RECALL-BASED AUTHENTICATION SCHEMES

1) Blonder algorithm

In 1996 Blonder proposed a new graphical authentication scheme that is called Blonder algorithm. During the registration the user is asked to click on several locations on an image to create a password. At authentication phase the user has to click on previously selected locations on the image or close to those locations. The image acts as a hint for the user to recall graphical passwords and therefore this method of authentication is considered more convenient than unassisted pure recall-based schemes [6]. Major problem this scheme faced with is that the number of predefined click areas is relatively small so the password had to be quite long to be secure. Also, the usage of predefined click areas required simple and plain images, instead of complex, real-world and crowded scenes [14].

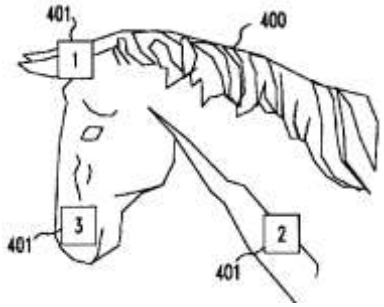


Fig 7. An example of Blonder algorithm

2) Passlogix v-Go algorithm

In 2002 Passlogix Inc. Company developed a new graphical authentication scheme called Passlogix v-Go algorithm. At registration phase the password is created by a chronological situation with repeating a sequence of actions. In this method user is asked to click on various items on the image in the correct sequence in order to be authenticated [3]. One drawback is that this technique provides only a limited password space, therefore causing the password to be kind of guessable or predictable [14].

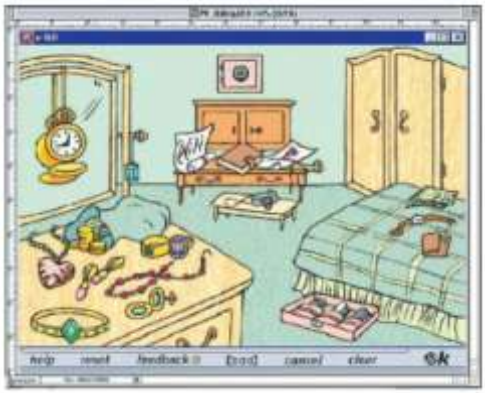


Fig 8. An example of Passlogix v-Go algorithm

3) PassPoint algorithm

In 2005 Wiedenbeck, Waters, Birget, Brodskiy, and Memon proposed a new graphical authentication scheme that is called PassPoint algorithm. During the registration the user is asked to click on several locations on an image. At authentication phase the user has to click on previously selected locations on the image or close to those locations. This method covers the limitations of Blonder algorithm because the images that are used for this method should be rich enough, complex and crowded. Any pixel in the image is a candidate for a click point so there are thousands of possible memorable points and combinations [6]. One drawback is that it takes more time to input the password than text-based password users spend [5].

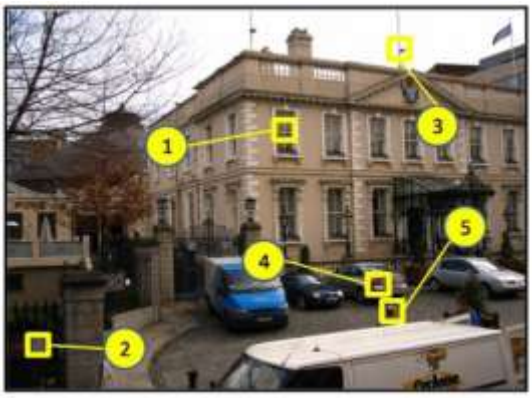


Fig 9. An example of PassPoint algorithm

III. SECURITY

Security is a primary goal and the main requirement for any user authentication mechanism. A lot of strategies exist for attacking to the system. Unfortunately, none system offers the perfect security, therefore schemes must be evaluated according to their vulnerabilities and susceptibility to different attacks [11].

Brute force search attack attempts to decipher the password by searching and testing for all possible combinations of alphanumeric characters until finding the correct key. For some graphical password schemes the most effective way against brute force search attack is to enlarge the password space by increasing the capacity of the picture library. In general, graphical passwords are less vulnerable to brute force search attacks than traditional text-based approach. However, recall-based methods of authentication tend to have bigger password space unlike recognition-based technique.

Dictionary attack attempts to reveal the password by running through a possible series of dictionary words that are compiled based on knowledge or assumptions considering the user's typical behavior. In general, graphical passwords are less vulnerable to dictionary attacks than traditional text-based approach. Users of recognition-based methods usually use a mouse for input, so it has no purpose to carry out the dictionary attacks against this kind of graphical authentication. Employment of a dictionary attack for recall-based methods is much more complex than in text-based dictionary attack but the speed of retrieving will slow down.

Shoulder surfing attack refers to obtaining the password of a particular user during login through direct observation or external recording devices. Text-based passwords like most of the graphical password schemes are vulnerable to shoulder surfing attack. Only a few of recognition-based techniques are designed to resist shoulder surfing and none of the recall-based techniques are considered resistant to shoulder surfing.

Guessing attack is a very common problem for both textual and graphical authentication approaches because users usually create short and simple passwords that give a convenience for guesswork. Users of text-based approach and the users of some graphical password schemes tend to choose weak passwords with predictable characteristics.

Spyware attack refers to any unauthorized software installed without the user's permission that collects information about user's computational behavior by tracking the keyboard input. In general, graphical passwords are less vulnerable to spyware attacks than traditional text-based approach. Since for inputting the graphical password users exploit the mouse, through the mouse motion alone is not enough to break graphical passwords.

Social engineering attack includes any method used to gain access to the system under false pretenses by exploiting human psychology. In general, graphical passwords are less vulnerable to social engineering attacks than traditional text-based approach. Also it reduces the possible password revealing because the explanation of graphical password to another person by verbal interpretation is much more difficult [14, 26, 27, 28].

Table 1: Types of common attacks

Attacks	Brute force search
	Dictionary
	Guessing
	Shoulder surfing
	Spyware
	Social engineering

Regarding the common attacks in graphical passwords and based on our research we can conclude the comparison among different schemes in the table below [26, 27, 28].

Table 2: The attacks resistance in graphical user authentication algorithms

Algorithms		Attacks					
		Brute force	Dictionary	Shoulder surfing	Guessing	Spyware	Social engineering
Recognition -based	1.1 Déjà vu	👎	👎	👎	👎	👍	👍
	1.2 Triangle	👎	👍	👍	👎	👍	👍
	1.3 Passface	👎	👎	👎	👎	👍	👍
Pure recall -based	2.1 DAS	👍	👎	👎	👎	👍	👍
	2.2 Grid selection	-	-	👎	-	-	-
	2.3 Syukri et al.	👍	👎	👎	👎	👍	👍
Cued recall -based	3.1 Blonder	👎	👍	👎	👎	👍	👍
	3.2 Passlogix v-Go	👎	-	👎	👎	-	-
	3.3 PassPoint	👎	👍	👎	👎	👍	👍

IV. USABILITY

In order to develop an effective authentication mechanism that can satisfy the user needs and requirements, not only security should be on the agenda. Usability of authentication scheme as well as its security should be of a prime importance. It includes factors such as learnability, efficiency of use, memorability, nice interface and overall user satisfaction with the product [7]. It is obvious, that graphical authentication schemes need more steps to execute and much more time to spend during the registration and login phases than traditional text-based approach. For the recall-based schemes the tolerance of an error has to be set carefully because the major issue is the accuracy of user's input and its recognition during verification phase. Besides, the hundreds of pictures for graphical authentication require more storage space and centralized database management as opposed to text-based passwords [3].

Table 3: The usability features and attributes

Usability features	Attributes
Effectiveness	Reliability and Accuracy
Efficiency	Applicable
Satisfaction	Easy to use Easy to create Easy to memorize Easy to execute Nice interface Easy to understand Pleasant picture

Regarding these usability attributes in graphical passwords and based on our research we can conclude the comparison among different schemes in the table below.

Table 4: The usability features in graphical user authentication algorithms

Algorithm		Effectiveness	Efficiency	Satisfaction						
		Reliable , Accurate	Applicable	Easy to use	Easy to create	Easy to memorize	Easy to execute	Nice interface	Easy to understand	Pleasant picture
Recognition -based	1.1 Déjà vu	👎	👍	👎	👎	👍	👍	👎	👍	👍
	1.2 Triangle	👍	👍	👍	👍	👍	👍	👎	👍	👍
	1.3 Passface	👍	👍	👍	👍	👍	👍	👍	👍	👍
Pure recall -based	2.1 DAS	👍	👍	👍	👎	👍	👍	👎	👍	👎
	2.2 Grid selection	👍	👍	👍	👎	👍	👍	👎	👍	👎
	2.3 Syukri et al.	👍	👍	👍	👍	👍	👍	👍	👍	👎
Cued recall -based	3.1 Blonder	👎	👍	👍	👍	👍	👍	👎	👍	👎
	3.2 Passlogix v-Go	👍	👍	👍	👎	👍	👎	👍	👎	👎
	3.3 PassPoint	👍	👍	👍	👍	👍	👍	👍	👍	👍

V. TRI-PASS: OUR PROPOSED ALGORITHM

The objective of this paper is to propose a new algorithm based on two previously discussed techniques namely PassPoint and Triangle algorithms. In our proposed algorithm we want to focus on the features and advantages of these two algorithms and join them together to get as much as possible security and usability.

Registration phase: To create a password the user should choose one image from the library of pictures and then choose any three points as his future password by clicking on the image. For better perception we will call these points "password points".

Fig 10. Registration phase of Tri-Pass algorithm

Login phase: The process of verification is based on our newly proposed scheme called Tri-Pass algorithm. In Tri-Pass algorithm to authenticate, the user has to imagine an invisible triangle around the area of the first "password point" and click on any three points that will form a triangle around this "password point". It means that in order to be authenticated the "password point" should be inside the area of invisible triangle. Then the user should do the same for the second "password point" and third "password point". So total there

are nine clicks during the login phase, by three clicks for each "password point".

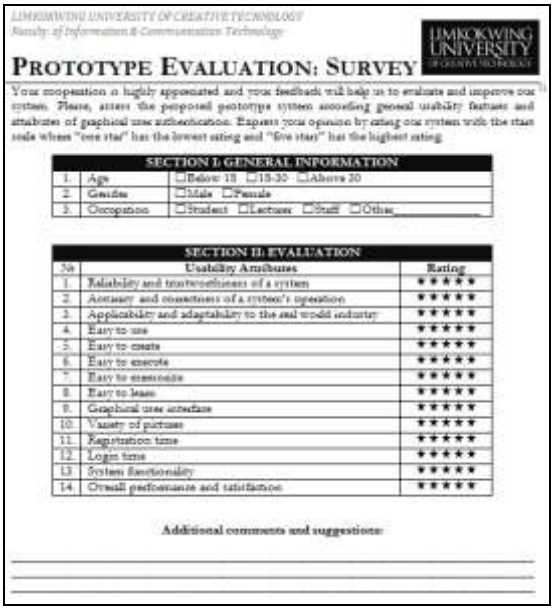
- Sequence. The process of inputting points that will create an invisible triangle around the "password points" should be done in a sequence, which you followed at registration phase.
- Overlapping. There is no overlapping of triangles is allowed.
- Size. The maximum size of each triangle should be not more than 300 pixels.
- Shape. The shapes of triangles can vary.

Fig 11. Login phase of Tri-Pass algorithm

VI. Data Collection and Evaluation

The method we used to collect data was a survey. Questionnaire was distributed to the lecturers and students from Limkokwing University of Creative Technology, Faculty of Information and Communication Technology, Cyberjaya campus, to get user perceptions on satisfaction and usability attributes based on 14 questions. The first section of the questionnaire involved the participants' general information from the point view of the age, gender and occupation. The second section of the questionnaire involved the participants' opinions and feelings about our prototype system.

Reliability attribute is important because it shows whether the users trust the system or not. Accuracy and correctness attributes are those that determine the flow of system's operation process. By rating the applicability attribute the users express their opinions about adaptability of a system to the real world industry. Easy to use feature of the graphical password prototype is one to see the feedback of our participants about the usage and manipulation process of a system. Easy to execute feature of the graphical password prototype is one to see the feedback of our participants about the execution process of a system. Easy to create feature of the graphical password prototype is one to see the feedback of our participants about the creation process of the password. Easy to memorize feature of the graphical password prototype which is important in the usability features in our questionnaire to see the feedback of our participants about the memorization process of the pictures chosen to be the password. Easy to learn feature of the graphical password prototype which is important in the usability features in our questionnaire to see the feedback of our participants about the learning process and understandable instructions. Graphical user interface feature is not about the usability but just to get the participants' feedback about the prototype design. Variety of pictures is also not about usability but just to get participants' feedback about the library of pictures. The registration time and login time for the prototype gives an idea how long time it takes to register and to login and whether it is short or long time. In the last question the users are asked to evaluate the overall performance and satisfaction with the system.


LIMKOKWING UNIVERSITY OF CREATIVE TECHNOLOGY
Faculty of Information & Communication Technology

PROTOTYPE EVALUATION: SURVEY

Your cooperation is highly appreciated and your feedback will help us to evaluate and improve our system. Please, assess the proposed prototype system according general usability features and attributes of graphical user authentication. Express your opinion by rating our system with the stars scale where "one star" has the lowest rating and "five stars" has the highest rating.

SECTION I: GENERAL INFORMATION

1.	Age	☐Below 18 ☐18-30 ☐Above 30
2.	Gender	☐Male ☐Female
3.	Occupation	☐Student ☐Lecturer ☐Staff ☐Other_____

SECTION II: EVALUATION

№	Usability Attributes	Rating
1.	Reliability and trustworthiness of a system	★★★★★
2.	Accuracy and correctness of a system's operation	★★★★★
3.	Applicability and adaptability to the real world industry	★★★★★
4.	Easy to use	★★★★★
5.	Easy to create	★★★★★
6.	Easy to execute	★★★★★
7.	Easy to memorize	★★★★★
8.	Easy to learn	★★★★★
9.	Graphical user interface	★★★★★
10.	Variety of pictures	★★★★★
11.	Registration time	★★★★★
12.	Login time	★★★★★
13.	System functionality	★★★★★
14.	Overall performance and satisfaction	★★★★★

Additional comments and suggestions:

Fig 12. An example of questionnaire for prototype evaluation

VII. Results and Discussion

From the analyzing of the questionnaire results we can see that majority of the users are given us a good feedback about the whole prototype evaluation and usability features built in the prototype. More than 60% of the respondents valued our prototype system as reliable and trustworthy. Over 50% of the users are sure that our prototype system is applicable and adaptable to the real world industry. Furthermore, over 70% of the respondents think that prototype system is easy to use, create and execute. However, only the half of the users asserts that this type of authentication is easy to memorize and to learn. GUI and variety of pictures in the library are rated highly by more than 75% of the users who involved in the survey. Also most of the users are satisfied with registration time, but the login time of this graphical password scheme in comparison with text-based scheme is much longer. Overall, more than 80% of the respondents are satisfied with performance of our prototype system, which is a really good result.

VIII. Conclusion

Overall, we have reviewed nine different algorithms on recognition-based, pure recall-based and cued recall-based methods. As part of our discussion on previous works, we studied the security and usability issues of graphical authentication including six common attacks. As shown in Table 2, most of the graphical password schemes are

vulnerable to brute force search, shoulder surfing and guessing attacks. As we found, usability of an authentication scheme as well as its security should be of a prime importance. We proposed a new algorithm for graphical user authentication named Tri-Pass. Also, we focused on development and implementation of a usable graphical password system. The evaluation of the prototype has been done by questionnaire survey regarding the usability features and results were very good, which means that the new system is acceptable and usable.

Future work should be directed toward optimizing newly proposed Tri-Pass algorithm for more efficient graphical user authentication and include but not limited to:

- Enhancing the prototype by fixing errors and bugs
- Exploring more feasibility and usability features
- Designing more helpful referencing aids and instructions
- Looking for the better solutions against shoulder surfing problems
- More studies and research can be conducted.

ACKNOWLEDGEMENTS

We would like to thank Dr. Arash Habibi Lashkari for his encouragement, supervision, kind advice and great support he has given us. Also we would like to express our appreciation to all respondents who participated in our survey for their valuable contribution.

REFERENCES

[1] Meng, Y. (2012) Designing Click-Draw Based Graphical Password Scheme for Better Authentication, *IEEE Seventh International Conference on Networking, Architecture, and Storage*

[2] Hu, W., Wu, X. & Wei, G. (2010) The Security Analysis of Graphical Passwords, *International Conference on Communications and Intelligence Information Security, China*

[3] Ma, Y. & Feng, J. (2011) Evaluating Usability of Three Authentication Methods in Web-Based Application, *Ninth International Conference on Software Engineering Research, Management and Applications, USA*

[4] Eljetlawi, A. & Ithnin, N. (2008) Graphical Password: Comprehensive study of the usability features of the Recognition Base Graphical Password methods, *Third International Conference on Convergence and Hybrid Information Technology*

[5] Lashkari, A. H., Towhidi, F., Saleh, R. & Farmand, S. (2009) A complete comparison on Pure and Cued Recall-Based Graphical User Authentication Algorithms, *Second International Conference on Computer and Electrical Engineering*

[6] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A. & Memon, N. Authentication Using Graphical Passwords: Basic Results.

[7] Suo, X., Zhu, Y. & Owen, G.S. Graphical Passwords: A Survey

[8] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A. & Memon, N. Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice

[9] Gao, H., Liu, X., Dai, R., Wang, S. & Liu, H. (2009) Design and Analysis of a Graphical Password Scheme, *Fourth International Conference on Innovative Computing, Information and Control*

[10] Almulhem, A. A Graphical Password Authentication System, Saudi Arabia

[11] Sabzevar, A. & Stavrou, A. (2008) Universal Multi-Factor Authentication Using Graphical Passwords, *IEEE International Conference on Signal Image Technology and Internet Based Systems.*

[12] Qureshi, M., Younus, A. & Khan, A. (2009) Philosophical Survey of Passwords, *IJCSI International Journal of Computer Science Issues, Vol. 2, Pakistan*

[13] Eljetlawi, A. (2008) Study and Develop a New Graphical Password System

[14] Lashkari, A. & Towhidi, F. (2010) Graphical User Authentication (GUA), *LAP LAMBERT Academic Publishing, Germany*

[15] Tao, H. (2006) Pass-Go, a New Graphical Password Scheme

[16] [16] Biddle, R., Chiasson, S. & Oorschot, P. (2011) Graphical Passwords: Learning from the First Twelve Years

[17] Chiasson, S. (2008) Usable Authentication and Click-Based Graphical Passwords

[18] Thorpe, J. & Oorschot, P. (2004) Towards Secure Design Choices for Implementing Graphical Passwords, *20th Annual Computer Security Applications Conference, IEEE*

[19] Lasarus, R. (2006) Pass-Color: Generating Password with Colored Graphical Assistance

[20] Li, Z., Sun, Q., Lian, Y. & Giusto, D. (2005) An Association-Based Graphical Password Design Resistant To Shoulder-Surfing Attack, *IEEE*

[21] English, R. & Poet, R. (2012) The Effectiveness of Intersection Attack Countermeasures for Graphical Passwords, *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*

[22] Dunphy, P., Heiner, A. & Asokan, N. (2010) A closer look at recognition-based graphical passwords on mobile devices, *Sixth Symposium on Usable Privacy and Security*

[23] Joshi, A., Kumar, S. & Goudar, R. (2012) A more Multifactor Secure Authentication Scheme based on graphical Authentication, *International Conference on Advances in Computing and Communications*

[24] Khandelwal, A., Singh, S. & Satnalika, N. User Authentication by Secured Graphical Password Implementation.

[25] Seng, W., Khuen, Y. & Shing, N. (2011) Enhanced Graphical Password by using Dynamic Block-style Scheme, *International Conference on Information and Intelligent Computing*, Singapore

[26] Lashkari A.H. and Farmand S. (2009) A survey on usability and security features in graphical user authentication algorithms, *International Journal of Computer Science and Network Security (IJCSNS)*, VOL.9 No.9, Singapore

[27] Masrom M., Towhidi F., Lashkari A.H. (2009) Pure and cued recall-based graphical user authentication, *Application of Information and Communication Technologies (AICT)*

[28] Lashkari A.H., Saleh R., Farmand F., Zakaria O.B. (2009) A Wide range Survey on Recall Based Graphical User Authentications Algorithms Based on ISO and Attack Patterns", *International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 6, No. 3

Dr. A. H. Lashkari received his B.E. degree in Software Engineering from the IAU in IRAN (1995), also he received his Master of Science in computer Science and Data communication from University Malaya (UM) in Malaysia (2010). Now, he has PhD of computer science (Network Security) from University Technology Malaysia (UTM) (2013). He has a mixture of academia and industry experience. His industry experience includes working as a programmer and systems analyst in three companies namely Rahgostar Naft Co., Bonavar Co., Norahan Co. in IRAN (5 years), and after join to the MCSE professional team worked as network designer and administrator in more than five companies in IRAN and Malaysia such as NBB Group, RADAAN Co., and Elecomp Co. (6 years).

Since January 2008, his academic experience has started as a research assistance in university Malaysia (UM), and university technology Malaysia (UTM). He is editorial and technical committee member in many journals and conferences around the world. Also, he serves as supervisor, Advisor, and senior lecturer in computer networks and security departments and handling two research centers in Malaysia. His research interests include Network Security, Authentication process, Graphical Passwords, Attacks and Anti-attacks.