Global Scientific JOURNALS

GSJ: Volume MH, Issue y, !dzƎdzăű 202n, Online: ISSN 2320-9186
www.globalscientificjournal.com

Face-Based Graphical Authentication Systems: Comparison of Memorability between Models

[1*]Salihu Umar Suru. Department of Computer Science, University of Bakht-Alrudah, Sudan [1]surusalihu@yahoo.com
[2]Hassan Umar Suru. [2]Department of Computer Science, Kebbi State University of Science and Technology, Nigeria. [2]suruhassan@yahoo.com

Key Words
Authentication, Memorability, Hybrid Scheme, Graphical Password, Login time, Success rate, Usability, Security, Images, Mixed Model.

ABSTRACT

Due to the proliferation of human activities online, numerous computing applications and users compete for system resources, such as hardware, software and data. Hence access control is a fundamental issue in application design. Both system and resource access are important security challenges in computing systems and need to be addressed to maintain system integrity. In such applications, people often have to prove their identities through some means of authentication. Authentication is the process of granting resource and application access to legitimate users and denying such access to illegitimate users. This paper is aimed at comparing the memorability of a newly designed Face-Based hybrid authentication system with the simulated sports Faces Scheme. The novel Face-Based Hybrid Authentication System and the simulation of sport faces scheme were developed and implemented. A series of laboratory tests were conducted on the novel system and the simulated sports faces scheme to ascertain and compare their memorabilities. Users created accounts using the novel schemes in each category and were subsequently required to login to their accounts in order to measure the rates at which they could be able to memorize and subsequently remember their graphical passwords they had created initially. The study found out that the novel system has significantly higher memorability rates compared to the simulated sports faces scheme based on the average login times of the participants and their login success rates.

Introduction

Designing a usable and secure authentication system is one of the major concerns in system design. However, a good authentication system should possess all the usability and security features before it is being deployed for use by the end-users. Traditional text based password authentication is facing challenges as an authentication mechanism due to lack of good memorability and security. As such, usable authentication schemes need to be provided due to the proliferation of networks and personal accounts [1]. Several graphical password schemes have been developed to overcome the problems of alphanumeric passwords. Usability, security and memorability features of such graphical schemes need to be effectively tested. Usability and security are the major areas of concern in the development of new systems. However, many researches in usability and security have confirmed that systems can be either secure or usable but not both [2]. Researchers in [3] defined usability as the extent to which a product can be used by specified users to achieve specified goals within effectiveness, efficiency and satisfaction in a specific context of use. However, memorability has been defined as one of the major critical usability issues [4]. Graphical passwords have considerable advantages over text-based passwords or PINs due to their capacity and the capabilities of the visual system. The major advantage of graphical password is that they are highly resistant to guessing attacks, due to their larger password space. However, memorability of multiple graphical passwords is more effective than multiple PIN numbers [4]. This research paper is intended to compare the password memorability between our novel systems and the simulated sports faces scheme from the original scheme proposed in [15] . We designed and implimented a simulation of sports faces scheme and compared it with our new hybrid schemes based on login time and login success rate.

Literature review

Authentication using alphanumeric password is the most common authentication mechanism and has been shown to have so many drawbacks as well as being prone to several security attacks such as brute force attack, guessing attack, shoulder surfing attack and dictionary attack among others [1]. Most existing authentication schemes have either been usable but not secure or secure but not usable [2]. These two conflicting password system requirements have been the major area of concern in the systems design profession [1]. Generally, authentication techniques can be divided into three major categories as follows:

Token based and biometric based systems require a user to use a special hardware device recognized by the system while knowledge based rely completely on shared piece of information between the user and the system. The knowledge based authentication technique is also subdivided into text based authentication techniques and graphical authentication technique. Text based authentication techniques are the most widely used authentication techniques. However, it is faced with a number of security vulnerabilities such as being susceptible to dictionary attacks, guessing attacks and shoulder surfing attacks. To overcome the security flaws in text based passwords, graphical passwords were developed. These came in the three subcategories: Recognition based, Pure recall based and Cue recall based [5]. The first recognition based authentication scheme was proposed by Blonder in 1996. His scheme requires users to identify one or more points on an image as their password. Users were restricted to predefined areas within the image. Lack of choice of click points was one of the major drawbacks of Blonder's scheme. Several graphical schemes were proposed after blonder's suggested scheme, for example the passpoints scheme which was proposed in [16] in which a user is allowed to click on any point within the displayed image to create his password. Passpoints is better than blonder suggested scheme security wise but, there is difficulty in selecting and memorizing the passwords in passpoints scheme. Draw-A-Secret (DAS) was also proposed in [17]. In order to use DAS, users need to draw lines as a password into an N x N grid. A study conducted in [18] and [5] confirmed that DAS suffered from usability and security flaws.

Déjà vu is one of the popular graphical password schemes developed in [9] that implements the harsh visualization method to generate abstract images with the help of computer algorithm. Each image is unique and has no definite form in the déjà vu scheme. The seed for each of the images generated in déjà vu is stored by the system in order to generate the image accurately for feature use. It is believed that the déjà vu scheme provided better memorability than alphanumeric passwords. However, its drawback is that the system is required to store the seeds for all images in order to generate such images in the feature [6].

A number of graphical password schemes were also proposed in [19] using picture, object and pseudo word or language recognition with large number of images. These schemes however, are known to have good memorability and the picture based implementation is also known to have better usability than the others. No security experiments were performed with these schemes [6].

A number of shoulder surfing resistance schemes were also proposed in [20]. Shoulder surfing is the ability to observe a user's identity by looking over their shoulders [7]. Their schemes were an extension of the Convex Hull Scheme developed in [21]. A user needed to locate any three of his chosen password images in their first scheme and then click inside the convex hull formed by those images. In their second method, the user is required to position one of his chosen images in a movable frame before he then moves the frame to align with any other two of his chosen images to authenticate. The third method was also introduced in which the user is required to focus on any four of his chosen images before he then click on the point of intersection of invisible lines joining the images placed at the opposite vertices of the quadrilateral formed by the four images. No experimental details with these schemes have been reported [7].

SmudgeSafe authentication scheme was proposed in [4] which uses graphical transformations to the image on which password points are selected. This scheme provides a better enhancement to resistance against smudge attacks and researches have rated the memorability of this approach to be very high [4].

A number of studies were conducted on the security and usability of click-based graphical authentication schemes in [22]. In click-based graphical password, users had to select one point per image but for a sequence of several images. Researchers reported that click-based approach is better in terms of usability and users preferred this approach than passpoints approach. However, the choice of images in click-based approach significantly influenced the login success rates [4].

Persuasive cued click points are an enhancement to cued click points by adding persuasive features. This scheme allows users to select less predictable passwords, and creates difficulty in selecting passwords where all click-points are hotspots. A hotspot is an area on an image with higher likelihood of being selected by users as password click point. The drawback of this approach is that it consists of sequence of images which may create burden on user memory to remember more click points [8].

Passfaces is one of the promising authentication systems developed and commercialized by the Real User Corporation in [6]. The idea of this scheme came due to the belief that humans remembered faces easier than other pictures even after a long period of time. In passfaces scheme, a user is required to choose four images of human faces as his password after which a grid of nine images of human faces including one of the faces he had chosen previously, and eight decoy faces is displayed. The user then identifies and clicks on his preselected faces. This procedure is repeated for several rounds until the user identifies his correct preselected faces. However this scheme is vulnerable to shoulder surfing attack and also predictable because users can possibly chooses the faces that are attractive to them [1].

Another promising authentication scheme was developed by Passlogix Inc [9] which allows users to create their passwords by simply clicking on objects in a graphical window, for example by dialing a phone number, hiding an object in a room. This scheme simply remembers user names and passwords and then automatically allows users to logon to the system. This scheme however is not secured and the scheme required the user to precisely recall the authentication task instead of relying on recognition [9].

Another authentication scheme that allows a user to simply protect his secrete key using the personal entropy in his whole life is a promising scheme developed [9]. In this scheme, a user can protect his secrete key by encrypting the passphrase using the answers to several personal questions. A user can simply recover his secrete key even if he forget the answers to a subset of the questions but, an attacker must learn the answer to a large subset of the questions in order to learn the key.

Picture password scheme was developed in [10] in 2003. This scheme was specially designed for handheld devices like Personal Digital Assistants (PDAs). This scheme also allows a user to select a theme that identifies the thumbnail photos to be applied and then registers a sequence of thumbnail images that are used for future password during enrollment. The current enrolled image sequence for verification must be entered by the user whenever the PDA is switched on in order to gain access to the device. Initially the numbers of thumbnail photos were limited to thirty (30) making the size of the password very small. To overcome the problem of smaller password size, the second method of selecting thumbnail images was introduced leading to an expansion from 30 thumbnail photos to 930. However, the expansion of thumbnail photos will make the memorability of password complex and difficult. Another drawback of this scheme is that the addition of shift key makes the algorithm more complex and difficult [10].

A new method of graphical password that is resistant to shoulder surfing attack was also proposed by Man et al in[10]. In their scheme, a unique code was assigned to all pictures. The user is challenged with a number of scenes containing several password objects and many decoy objects, during the authentication process. Due to the unique code for each picture, the user will input the string of code for his password. The drawback of this method is that the user is required to memorize the code for each password object variant. For example, supposing there are 5 pictures each with 5 variants, then each user has to memorize 25 codes [10]

A usable hybrid graphical password scheme known as Jetafida scheme was proposed in 2008 in [15]. The aim of this method was to implement all the usability features in a single algorithm. During registration, the user is required to select three pictures as his/her password and then sort them according to the way he/she wants to see them in the login phase. The user password images are mixed with seventeen color pictures in login phase. According to the article, all the usability features in the scheme were implemented successfully. The research article did not, however, investigate any of the security issues of the system.

Several hybrid authentication schemes have been developed and tested. Hybrid authentication schemes refer to authentication mechanisms that involve the combination of more than one authentication scheme. For example, a combination of text and graphical authentication schemes in order to improve both the usability and the security of the system. An authentication scheme of this kind was proposed by M. Sreelatha et al. in [11]. This scheme was also extended by M. S. Tidke et al. in [12]. They proposed a hybrid scheme which combines text and graphical authentication method for the generation of session based passwords. During registration, a user is required to select text based and graphical passwords. In order to authenticate, the user must correctly enter both graphical and text based passwords. At the initial implementation, a user will be presented with a text grid from which he chooses his password from an intersection of rows and columns of the grid and this represents his password. The ranking of colours which needs to be remembered accurately was suggested in the second implementation. Combining upper case letters, lower case letters and augmentation with special characters was also suggested for the text based password. This scheme is believed to be resistant to security attacks. However, there is likelihood that it will suffer from usability issues. No study was conducted on its usability evaluation [11, 12].

A hybrid system that combines shape and text is also proposed in [13]. This scheme combines text based password with a shape drawn on a grid as in the DAS scheme. This system is found to be resistant to shoulder surfing and brute force attacks. However, it suffers from serious usability flaws. Another hybrid method that combines the traditional text based and the recognition based graphical authentication systems was proposed in [14]. In this scheme, a user is required to enter his text based password containing alphanumeric and special characters after which he selects a number of images from an image grid during registration phase. The user also enters his alphanumeric password and then selects his chosen images from an image grid provided during authentication. Below each image is assigned a unique number in the image grid for this system. This unique number is randomly assigned and changes at each authentication round. A user does not need to click directly on an image to select it, but to click on the digit that represents it in the selection panel. This scheme is believed to be resistant to shoulder surfing attack. However, further study to investigate and analyze its security and usability potentials, have not been conducted.

THE NOVEL SYSTEM

In the cause of this research, four Novel systems prototypes were developed and experiment was conducted for each prototype. The first three models were designed and compressed in a single interface for ease of use. This single interface contained Sport Model, Non Sport Model and Mixed Model. These models were designed using the Faces of Celeberities from different region to reduce the problem of usability and security which remained the bottleneck in the previous authentication mechanisms. Our three novel systems are better than Sports Faces scheme interms of usability and ability of users to remember their chosen images for authentication because, the study in Sports Faces is limited to only two category of Sports. In the Sports Faces, users are only allowed to choose their images from either Football or Cricket in order to get themselves authenticated. In this novel scheme, users are not limited to only two categories of sports due to the belief that some users may not be familiar with Cricket or Football or may not have interest in such sports categories coupled with a perception of the long period of time taken to create password in Sports Faces scheme. This meant that Sports Faces system suffered serious usability flaws. Face-Based Hybrid Authentication System is the name given to our Novel System in this study. Figure 1 below explained the design process and how the three models works.

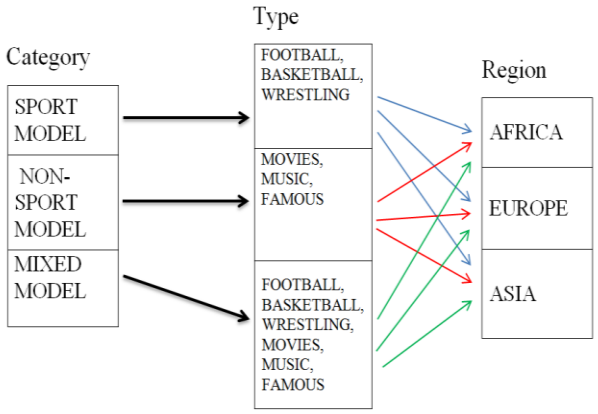

Figure 1: Design Process of the Novel System

The novel system uses a combination of text based user name and password as the first level entry point, the graphical password provides the second level security access point.

Image Based Registration Phase

After text based registration, a user is allowed to click on the model of his choice (i.e. Sports, Non Sports and Mixed Models.) and then select the region (i.e. Africa, Europe, Asia etc.) where each selected model type belongs to, and finally the images of celebrities from the selected region are displayed and selected for registration as shown in the last screen for image based registration window in figure 2 below.

Figure 2: Last screen for Image based registration phase

Image Based Login Phase

In login phase, a user is only required to enter his created id and password and then select the correct images from the sequence of nine images displayed by the system including the decoy images. Although the sequence of the chosen images is not important, but a user must select the exact number of images he had selected during password creation for successful authentication. The last screen for image based login phase is shown in figure 3 below.

Figure 3: Last screen for Image based login phase

Semulated Sports Faces Models

The fourth model is a simulation of sports faces model designed using the faces of all sports celebrities and the national flags of all countries that had participated in football and cricket in a particular FIFA world cup competition in [16]. In the Sports faces scheme, a user has to select twelve images from a particular category (i.e. football or cricket): one country's flag, three players belonging to that particular country and the process is repeated thrice during registration [16]. Sports faces offers security advantages such as resistance to shoulder surfing attack, exhaustive search and guessing attacks as multiple levels of challenges are involved during the registration phase.

Figure 4: Simulated Scheme Interface

Figure 5: Step 1 for registration Phase in Sports Faces Models

Registration

To register into the system, a user specifies his sport interest between football and cricket in order to select images that will make up his graphical password portfolio. The user registration interface then presents the user with an input field to specify a username. Based on the sports category selected, the registration interface presents the user with images of country flags of each of the participating team in the world cup of the selected sport category. Once a country flag is selected, the interface displays a catalog of Images of all the players for the particular team. There are 31 teams of football with 23 players in each team and 16 teams of cricket with 12 players in each team. For each selected flag, three (3) images must be selected from the team before moving to another step. This process is repeated thrice resulting in selecting nine (9) players in the graphical password portfolio with three players each selected from three different teams.

Figure 6: Step 2 for registration Phase in Sports Faces Models

Figure 7: Last screen for user registration in Sports Faces Models

Login Phase

Access to this system required a user to enter his registered user name and click the login button in figure 4 above to present a login challenge set for each image of the graphical password portfolio. The challenge set is generated in the order the images were selected. This means for the first image the challenge set will consist of eight (8) decoy images and the actual password image in random positions on a 3 x 3 image grid. A user is expected to click the password image for the next challenge set to be presented, and this goes on for all nine images in the password portfolio. If all images chosen in each challenge set correspond to password images in the portfolio, then a user is considered authenticated,otherwise the login is aborted.

Figure 8: Imagebased login window

Experimental Design and Procedure

A total of 40 students whome are both from post graduate and under graduate schools of Kebbi State University of Science and Technology, Aliero were participated in the experiment. We started from training the participants on how the Novel system and the Simulated Sports Faces models are being used to register a user and subsequently how a user can be authenticated through each scheme. The training was carried out using Hp laptop computer system connected to a projector in the ICT Mega lab but the experiment was conducted in the executive brousing lab which is limited to the staff of the department of computer science only. The choice of the executive brousing lab for this experiment is due to the fact that the memorability test required more time. The time intervals provided to test the memorability of these systems are two weeks after first trial, four weeks after second trial and two month after third trial. The experiment lasted for fourteen weeks. The participants were grouped into two groups and they were organized in form of Latin square to avoid being bias. Three high resolution hp laptop computers were used subsequently by the participants with each computer used to install one particular model. Participants were asked to authenticate themselves using the same login details they created their accounts during registration. The variables that were observed and recorded in this experiment are login success rates, login time and mean login time. The login success rates, login time and mean login time of each participant were recorded and used to assess the level of memorability for both the novel system and the simulated system using SPSS software.

Result Analysis

Memorability comparisons were made between the novel systems and simulated sports faces scheme based on the data collected from the experiment. The data was analysed using the One-way ANOVA analysis and the resulting descriptive statistics are henceforth used to interpret the results of the comparisons between the three models of the novel system and the simulated sports face scheme based on average login time and success rates.

Login Time

The time it takes for an individual to log into the novel system is primarily affected by the level at which the individual can easily identify the right password image from the set of decoy images. Another factor that affects our results in this experiment is the number of images presented in the challenge set and the speed at which the underlying platform renders it. This experiment eliminated such obstacles by imple-

menting the same number of images in the challenge set (3 x 3) and used computers of equal specification to carry out all experiments.

Descriptives

		N	Mean	Std. Deviation	Std. Error
MeanLoginTime	Sports	8	11.4125	1.87040	.66129
	Non Sports	17	11.5906	1.62034	.39299
	Mixed	5	19.5200	1.76409	.78892
	SportsFaces	10	36.5610	4.12492	1.30442

Figure 9: Descriptive statistic table showing the mean login time

Based on the descriptive statistics above, the novel systems shows similar average login times of 11.4 and 11.5 seconds respectively. The average login time of the simulated sports Faces scheme was significantly higher than that of the novel systems with 36.5 seconds (Sig. 0.000 significant difference using Tukey One-way ANOVA). Comparing the passwords size of the novel systems which have 3 and 6 images with that of the simulated sports faces having 9 images, such difference will be further investigated.The minimum login time of the novel systems were found to be 9 and 8.3 seconds and the highest recorded login time were 15.4 and 14 seconds respectively. In the simulated sports faces scheme, the minimum and maximum recorded login times were 30.3 and 44.1 seconds, which is more than three times the minimum and maximum time of the novel systems. This shows that even though the password sizes are not equal, respondents in the novel systems took less time during authentication.

Dependent Variable	(I) Model	(J) Model	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
MeanLoginTime	Sports	Non Sports	-.17809	1.00546	1.000	-3.1487	2.7925
		Mixed	-8.10750*	1.33692	.000	-12.0574	-4.1576
		SportsFaces	-25.14850*	1.11239	.000	-28.4350	-21.8620

Figure 10: Comparison of mean difference between the novel systems and sports faces scheme

The ANOVA table above shows a comparison of mean differences between the novel systems and simulated sports faces scheme. A significant difference of 0.000 was observed between the sports faces scheme and the novel systems showing that there is statistical significant difference between the novel systems and simulated sports faces scheme. However, there was no statistical difference within the novel systems. The graph below illustrates the clear difference in mean login time between the novel systems and simulated sports faces scheme.

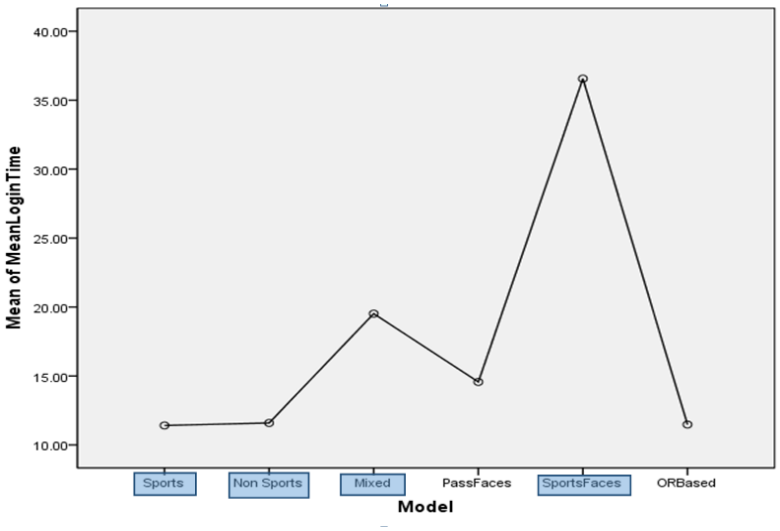

Figure 11: Mean difference of mean login time between the novel systems and sports faces scheme

Success rates

One of the most important factors that determine the memorability of graphical authentication systems is the rate at which users are able to remember their passwords. Several graphical password schemes with impressive concepts have failed with regards to the issue of memorability thus making them less usable. However, to improve the applicability of the novel systems, celebrities from three regions were used and made available for users to create their passwords thus simplified the choice of images by user for authentication.The login success rates of the participants after three attempts were recorded and analyzed as shown in the figure 12 and 13 below. The result shows the mean value of success rates out of three (3) attempts from each authentication scheme. Individual record indicates the number of successful login recorded after three trials with valid values of 0, 1, 2 and 3. A success rate of 3 for an individual record meant a participant logged in successfully in all three attempts, and 0 indicated none.

		Minimum	Maximum
SuccessRate	Sports	1.00	3.00
	Non Sports	1.00	3.00
	Mixed	1.00	3.00
	SportsFaces	.00	2.00

Figure 12: Login success rates after three attempts

Descriptives

		N	Mean	Std. Deviation	Std. Error
SuccessRate	Sports	8	2.5000	.75593	.26726
	Non Sports	17	2.3529	.78591	.19061
	Mixed	5	1.8000	.83666	.37417
	SportsFaces	10	.9000	.73786	.23333

Figure 13: Mean of login success rates after three attempts

The novel systems obtained the highest average success rates of 2.5 and 2.3 successful logins out of 3 attempts and all with minimum of 1 successful login attempts out of 3 attempts and this shows that there were participants that were only successful with their first login. Both models also have a maximum of 3 success rates, meaning that participants were able to login successfully in all three attempts. The mixed model has an average success rate of 1.8 and Sports Faces obtained a mean success rate of 0.9 which is the lowest recorded success rate. The mean success rates graph shown in figure 14 below illustrates the sports Faces scheme having the lowest success rates in this experiment.

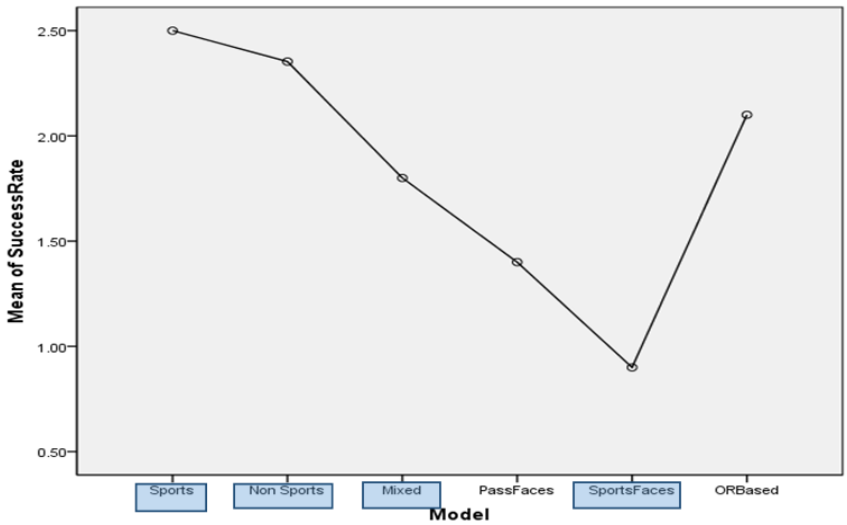

Figure 14: Mean of success rates between the novel systems and sports faces scheme

Dependent Variable	(I) Model	(J) Model	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
SuccessRate	Sports	Non Sports	.14706	.32423	.997	-.8109	1.1050
		Mixed	.70000	.43112	.587	-.5737	1.9737
		SportsFaces	1.60000*	.35872	.001	.5402	2.6598
	Non Sports	Sports	-.14706	.32423	.997	-1.1050	.8109
		Mixed	.55294	.38473	.704	-.5837	1.6896
		SportsFaces	1.45294*	.30138	.000	.5625	2.3434
	SportsFaces	Sports	-1.60000*	.35872	.001	-2.6598	-.5402
		Non Sports	-1.45294*	.30138	.000	-2.3434	-.5625
		Mixed	-.90000	.41421	.267	-2.1238	.3238

*. The mean difference is significant at the 0.05 level.

Figure 15: ANOVA table for multiple comparisons between mean difference of novel systems and sports faces scheme

The ANOVA tableshown in figure 15 aboveshows the levels of statistical significance difference in the success rates between the novel systems and sports faces scheme. In the multiple comparisons table above, significant differences of 0.001 and 0.000 respectively were observed between the sports Faces scheme and the novel systems, excluding the mixed model having 0.267 which is statistically not significant. This shows that success rates of the novel systems are higher than those of the sports Faces with a difference that is statistically significant.

Conclusion and future research

Memorability has been defined as one of the major critical usability issues in [4]. After the memorability studies were conducted between the novel systems and the simulated sports faces scheme, it is comfirmed that the novel systems are better than the simulated sports faces scheme interms of memorability and thus the novel systems are also usable. The result obtained in this research is based on the login success rates of the participants and their mean login time. Good authentication systems must be designed in such a way that endusers can be able to remember their passwords even after a long period of tme. Further research can be extended to investigate the security attacks against the novel systems and more sports and non sports categories can be added to improve the security of the systems. Another experiment should be conducted to compare the novel system with the existing graphical password schemes.

References

1 Ms Grinal Tuscanoet al "Graphical Password Authentication Using Pass Faces"*International Journal of Engineering Research and Applications Vol. 5, Issue 3, (Part -5) March 2015, pp.60-64*

2 Furkan Tari et al " A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords"*Symposium On Usable Privacyand Security (SOUPS) 2006, July 12-14, 2006, Pittsburgh, PA, USA*

3 Joel Mvungi &Titus Tossy "Usability Evaluation Methods and Principles for the Web"*(IJCSIS) International Journal of Computer Science and Information Security,Vol. 13, No. 7, July 2015*

4 Florian Alt et al "Memorability of cued-recall graphical passwords with saliency masks "*Conference Paper · December 2016, MUM '16, December 12 – 15, 2016, Rovaniemi, Finland*

5 Shah Zaman Nizamani et al "GPASS: A Graphical Password Scheme Using Alphanumeric Characters and Pictures"*International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 7, July 2016*

6 Hassan Umar Suruet al "A Review of Graphical, Hybrid and Multifactor Authentication Systems"*International Journal of Scientific & Engineering Research Volume 10, Issue1, January-2019 IJSER © 2019* http://www.ijser.org

7 Hassan Umar Suru and Pietro Murano" Security and User Interface Usability of Graphical Authentication Systems – A Review" *International Journal of Computer Trends and Technology (IJCTT) - Volume 67 Issue 2 – Feb 2019*

8 S.B. Nikam et al " Active Image Authentication System (AIAS): Design, Implementation and Analysis" *International Journal of Application, Innovation in Engineering & Management (IJAIEM) Volume 2, Issue 11, November, 2013*

9 Rachna Dhamija and Adrian Perrig "D´ej`a Vu: A User Study Using Images for Authentication" in USENIX Security Simposium. Volume 9, August, 2000. available at http//www.google.com

10 Farnaz Towhidi and Maslin Masrom " A Survey on Recognition-Based Graphical User Authentication Algorithms"*International Journal of Computer Science and Information Security", Vol. 6, No. 2, 2009.*

11 M. Sreelatha, et al. "Authentication schemes for session passwords using color and images." *In International Journal of Network Security & Its Applications, 3(3), 111-119. 2011.*

12 M. S. Tidke et al. "Password Authentication Using Text and Colors." *Computer Engneering, Rtm Nagpur University, Miet Bhandara. 2015.*

13 Z. Zheng, X. Liu, L. Yin and Z. Liu "A Hybrid Password Authentication Scheme Based on Shape and Text". *JCP, 5(5), 765-772. 2010*

14 P. C. Van Oorschot, and T. Wan "TwoStep: An Authentication Method Combining Text and Graphical Passwords". *MCETECH, 233-239. 2009.*

15 A. M. Eljetlawi and N. Ithnin " Graphical Password: Prototype Usability Survey" *International Conference on Advanced Computer Theory and Engineering 2008*

16 S. Kalsoom, S. Ziauddin and M. Tahir "SportsFaces: A Graphical Password System based on Images of Sports Celebrities" *In 11th International Conference on Innovative Internet Community Systems (I2CS 2011) Berlin, Germany June, 2011.*