Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 14 (2019) pp. 067-077

An Evaluation Model for Recognition-based Graphical Password Schemes

Shah Zaman Nizamani[1], Syed Raheel Hassan[2], Riaz Ahmed Shaikh[3] and Sheikh Tahir Bakhsh [4]

[1]Department of Information Technology,
Quaid-e-Awam University, Pakistan
shahzaman@quest.edu.pk

[2]Department of Computer Science,
King Abdulaziz University, Saudi Arabia
rhassan1@kau.edu.sa

[3]Department of Computer Science,
King Abdulaziz University, Saudi Arabia
rashaikh@kau.edu.sa

[4]Department of Information Technology,
King Abdulaziz University, Saudi Arabia
stbakhsh@kau.edu.sa

Abstract: **User authentication is the basic need for information security and textual password scheme has been in use for authentication since a long time. In the textual password scheme, security issues increase when a user set easy to remember password, while secure passwords are difficult to remember. To overcome the deficiencies of textual password scheme, different graphical password (GP) schemes are developed. In textual password scheme, security and memorability are two prime concerns whereas in GP schemes, usability is another concern along with security and memorability. GP schemes are divided into three categories, which are recognition-based graphical password schemes (RGP), pure recall-based graphical password schemes (PRGP) and cued recalled-based schemes graphical password schemes (CRGP). Different models are proposed for evaluation of the authentication schemes but they are difficult to execute. In this research paper, an evaluation model is proposed for analyzing the RGP schemes. The model evaluates the schemes with the help of thirty heuristics or features. Furthermore, evaluation of Passface and Deja Vu schemes have been presented by using the proposed evaluation model.**

Keywords: Authentication, Security, Graphical passwords, Alphanumeric passwords.

I. Introduction

Textual password scheme is easy to use but strong or secure passwords are difficult to memorize [1]. Textual password scheme is also weak against spyware-based attacks. Graphical password (GP) schemes are used as an alternative to traditional textual passwords for user authentication. GP schemes have some security and memorability advantages over textual password scheme. In this category of user authentication, passwords consist of some pictures, points inside a picture or some lines. Graphical passwords are easier to remember than textual passwords, because pictures are easier to remember than random alphanumeric characters [2]. Some GP schemes are secure but require large amount of time for authentication while others are easy to use but have some security issues.
Many GP schemes have been proposed but the evaluation made by owner of the schemes, is often incomplete and optimistic. Researchers highlight superiority of their schemes and often ignore weaknesses. In order to give an impartial analysis of GP schemes, some evaluation models have been proposed [3] [4], but the models do not provide in-depth analysis of GP schemes and the evaluation process is often difficult to execute.
In this research paper, an evaluation model is developed which gives a detailed analysis of recognition-based graphical password (RGP) schemes. In the model, evaluation is done on the basis of different heuristics. The proposed model gives evaluation results in numerical format.
The remaining paper is divided into six sections. In section II, RGP schemes are explained along with different evaluation models for authentication schemes. Proposed evaluation model for RGP schemes is explained in section III. In section IV, two GP schemes are evaluated by using the proposed model. Complexity of the proposed model is discussed in section V. Finally, conclusion is given in section VI.

II. Literature review

Dhamija *et al.*[5] proposed an authentication scheme, known as Deja Vu. In this scheme, 25 abstract art pictures are used for authentication. In this scheme, a password consists of at-

least five pictures. For authentication, a user has to correctly select the password pictures. Educated guessing attack is difficult to apply due to abstract art pictures, but such pictures are difficult to remember. This scheme is also weak against shoulder surfing attacks because the password pictures can be recognized at the time of selection.

Brostoff *et al.* [6] proposed an authentication scheme known as PassFace. In this scheme, a password is created from forty five pictures of human faces. In the login screen, all the pictures are shown in five screens. Each screen contains 9 pictures in a 3 * 3 grid-based screen. Educated guessing attacks can be applied in the scheme because users generally select password pictures based upon gender, attraction, and race for better memorability. This information can be used for password guessing.

For improving memorability of picture-based passwords, Devis *et al.* [7] used different categories of pictures for password selection in an authentication scheme known as "story scheme". In this scheme, authentication is done by correctly selecting the password pictures. This scheme has memorability advantage over Deja Vu and PassFace scheme due to multiple categories of pictures but it is weak against shoulder surfing attacks because the password pictures can be viewed from the login screen.

Issue of shoulder surfing attack was tried to solve in the scheme suggested by Bilgi *et al.* [8]. This scheme also uses different categories of pictures in the password registration screen. However, in the login screen hybrid pictures are shown based upon the original pictures. Due to hybrid pictures, the passwords are difficult to view from the login screen. This scheme reduces the chances of shoulder surfing attack but it is weak against brute force attack because small number of pictures are used for the password creation.

Lopez *et al.* [9] suggested another shoulder surfing resistant RGP scheme. In this scheme, users are given a challenge to identify the number of password pictures in the login screen. For authentication, the users have to inform that whether password pictures are even or odd in each row of the login screen. Exact password is not selected for authentication, therefore this scheme is resilient to shoulder surfing attacks. But this scheme is weak against brute force attack due to small number of pictures used for authentication process.

A. Frameworks for evaluation of authentication schemes

Many evaluation frameworks or models are proposed for analyzing the authentication schemes. One of the evaluation model was proposed by Bonneau *et al.* [10]. In the model, different features of the authentication schemes are highlighted for evaluation. This model can be used for analysis of biometric, token-based or password-based authentication schemes, but the model does not show in-depth analysis of the schemes.

Halunen *et al.* [11] mentioned thirty attributes for analyzing the authentication schemes. An evaluator needs to highlight implementation level of each of the attribute in an authentication scheme. The suggested implementation process is difficult to execute because it is not easy to find out the implementation level of the attributes.

English and Ron [4] suggested a model for analyzing security of RGP schemes. In the model, evaluation is done by assigning scores or ratings to different security attacks with the help of flowcharts. Advantage of this model is that, it provides quantitative mechanism for assigning score to each of the security attack. However, flowcharts of some security attacks are missing from the model. This model also does not give flowcharts for analyzing usability and memorability areas of the schemes.

Khodadadi *et al.* [12] presented attributes for analyzing RGP schemes. The evaluation is done by highlighting whether each of the attribute is implemented or not inside an RGP scheme. By using this model, a clear picture of the performance of the schemes is difficult to get because of the two level of ratings (implemented or not implemented).

The suggested evaluation models have different issues, some of them have vague evaluation process while others do not contain complete set of features for analysis. Additionally, in-depth analysis of the authentication schemes is missing from some models i.e. it is difficult to understand, against which features an authentication scheme performs better and what are the weak areas of the authentication schemes.

The proposed model is designed for evaluation of the RGP schemes. In the model evaluation is done through thirty heuristics, which gives a complete and clear process of evaluation. Each of the heuristic is separately analyzed and presented in the final result, so that in-depth analysis of the RGP schemes can be made.

III. Proposed evaluation model

In the proposed evaluation model, heuristics are related to security, memorability, and usability of the RGP schemes as shown in figure 1. The heuristics which evaluate security of the RGP schemes are the well-known security attacks. While, heuristics of memorability and usability are derived from the field of information memorization and human computer interaction. In the proposed model, evaluation is done by assigning scores or ratings to all the heuristics. Proposed model uses 30 heuristics for evaluation, out of which 10 heuristics belong to security, 8 for memorability and 12 heuristics for usability.

Overall quality of the RGP schemes can be derived from the equation 1.

$$Q = \alpha S + \beta M + \gamma U \tag{1}$$

In the equation 1, Alpha shows how much an RGP scheme is secure, while Beta and Gamma shows the level of memorability and usability. *S, M* and *U* represents heuristics of security, memorability, and usability respectively. *Q* is the total quality of an RGP scheme, which can be concluded by adding all the rating scores.

Detailed evaluation is given in equations 2-4. In the equations αi, βj and γk represents the ratings of all the heuristics belong to security, memorability and usability respectively.

$$\alpha S = \sum_{i=1}^{10} \alpha i \tag{2}$$

$$\beta M = \sum_{j=1}^{8} \beta j \tag{3}$$

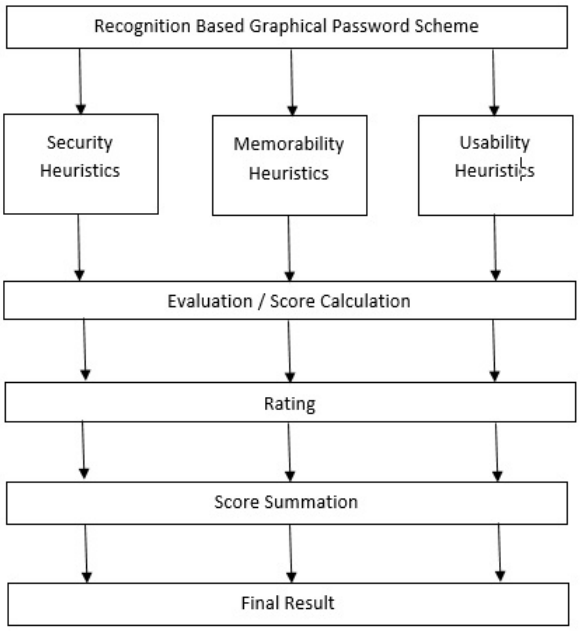

Figure. 1: Proposed model

Table 1: 3 Points Scale

Rating	Meaning
0	Feature is not implemented
1	Feature is implemented with mid-level efficiency
2	Feature is very efficiently implemented

$$\gamma U = \sum_{k=1}^{12} \gamma k \tag{4}$$

Equation 5 shows that, overall quality is the summation of rating points given to all the heuristics.

$$Q = \sum_{i=1}^{10} \alpha i + \sum_{j=1}^{8} \beta j + \sum_{k=1}^{12} \gamma k \tag{5}$$

In the model, ratings are given through 3 point (0 to 2) or 5 point (0 to 4) Likert scale. The definitions of 3 point and 5 point Likert scales are defined in tables 1 & 2. The rating scales are assigned to all the heuristics, as mentioned in the "Rating scale" column of table 3 - 5. The rating scale is given on the basis of range of options available for assigning a score. Value of each rating depends upon the performance of an RGP scheme with respect to a particular heuristic.

A. Security heuristics of the model

Authentication schemes need to provide maximum resistance from different password security attacks. In the proposed model, the password security attacks are considered as security heuristics as shown in table 3. For the security heuristics, a scale (3-point or 5-point) is given for assigning evaluation scores as shown in table 3. The evaluation is done by assigning scores and (optionally) comments to all the security heuristics, according to performance of an RGP scheme.

Table 2: 5 Points Scale

Rating	Meaning
0	Feature is not implemented
1	Feature is slightly implemented
2	Feature is implemented with mid-level efficiency
3	Feature is implemented with enough efficiency
4	Feature is very efficiently implemented

Table 3: Security heuristics

SNo.	Heuristics	Rating scale
01	Brute force attack	5
02	Dictionary attack	5
03	Shoulder surfing attack	3
04	Malware attack	5
05	Online guessing attack	5
06	Intersection attack	5
07	Social engineering attack	5
08	Phishing attack	3
09	Network interception attack	3
10	Recordability attack	5

Following information is important for assigning ratings to the security heuristics.

1) Brute force attack

In brute force attack, blind guesses are made on the passwords stored in a database. If an authentication scheme has a small number of possible passwords then password cracking become easy through brute force attack. Traditional textual password scheme contains 94 alphanumeric characters (excluding space key) based on Standard American keyboard, for password creation. In RGP schemes, different pictures are used for password creation. Large number of pictures are important for improving security of the RGP schemes. Passwords of larger length and stored with salt based hashing technique [13] also increase effort to break a password. In order to speed-up the process of breaking the passwords with brute force attack, parallel processing is used [14]. The rating for this heuristic depends upon number of available pictures and the password storage technique.

2) Dictionary attack

For dictionary attack a list of possible passwords are created. The list contains passwords which have high chances of being set by the users. There are some specialized forms of dictionary attacks used for increasing efficiency of dictionary attacks such as rainbow table attack [15]. In order to counter dictionary attacks, high password entropy is required. In textual password scheme, entropy level is increased by restricting users to create the passwords from different combinations of character, numbers, and symbols or in some applications password meters are used to motivate users for creating strong or high entropy passwords [16][17]. In RGP schemes, high entropy can be achieved by restricting users to set passwords from different categories of pictures and setting minimum length of the passwords.
Password storage technique also affect the success ratio of the dictionary attack. The passwords need to be encrypted with a secure hashing hashing [18][19] for improving security against brute force and dictionary attack.

3) Shoulder surfing attack

In this attack, password of a user is identified by observing password entry process through naked eyes or a camera recording. The level of difficulty in observing and identifying passwords, decides the rating of this heuristic. The RGP schemes where password images can not be identified after observing or recording a login session, will be given full rating for this heuristic.

4) Malware attack

Malware programs send authentication information to attackers without getting permission from actual users. Higher rating will be given to those schemes where passwords can not be fetched from the information provided by the malware programs.

5) Online guessing attack

For better memorability, users select password pictures based on culture, interest, and gender. This approach of selecting the password pictures, increases the chance of online guessing attack because the attackers can use profile information for password guessing. For reducing chances of online guessing attack probability of selecting the password pictures, need to be equal among all pictures of an RGP scheme.

6) Intersection attack

In this attack, a password is recognized after observing multiple logging sessions. This attack is used in the situation where exact password elements are not selected in the login screens. Rating for this heuristic depends upon the number of recordings required for recognizing the password elements.

7) Social engineering attack

In social engineering attack, users mistakenly reveal their password information to attackers. Although core responsibility lies to the users for preventing from social engineering attacks. The pictures which are difficult to describe, can reduce the chances of password break in RGP schemes. The rating for this heuristic depends upon the level of difficulty in describing the password pictures.

8) Phishing attack

In phishing attack, users are redirected to a fraudulent login screen, which is specially created for capturing the password elements of the users. From the login screen, password elements of the users are collected by the attackers. Chances of successful phishing attack can be reduced if password pictures are not exactly selected in the RGP schemes.

9) Network interception attack

In this attack all communication between a user and legitimate server is governed by an attacker. From the communication, attacker gets the login credentials, which are later used for authentication. Chances of this attack can be reduced, if a scheme changes login credentials on every login session.

Table 4: Memorability heuristics

SNo.	Heuristics	Rating scale
01	Password scalability	3
02	Minimum password size	5
03	Selection of pictures	5
04	Picture relate stories	5
05	Freedom of choice	5
06	Meaningfulness	5
07	Memory recall clues	5
08	Pictures upload facility	3

10) Recordability attack

In recordability attack, login credentials (username & password) are recorded from a login screen. The attackers use different type of spyware applications for recording the information. The information may be consist of screen recordings, keys pressed while entering authentication credentials or mouse click position. One time password (OTP) [20] approach can be used to minimize the recordability attacks. High ratings will be given to those schemes where the recorded login credentials do not show any clue of original password.

B. Memorability heuristics of the model

Password memorability is another important area of user authentication. Different pictures are used as a password for RGP schemes. An evaluator can examine how much easy it is to remember a picture-based password through the heuristics listed in table 4.

1) Password scalability

Users mostly set similar passwords in different applications because such passwords are easier to remember than completely different passwords. In an RGP scheme, password scalability can be achieved if a scheme is standardized and same pictures are used in different deployments.

2) Minimum password size

Length of the password is important for both security and memorability of the schemes. In textual password scheme minimum length of six to eight alphanumeric characters is followed. In RGP schemes it is difficult to remember eight pictures in sequence. Therefore, minimum password size is required to be such that password pictures can be easily remembered by users. Minimum password size can vary depending upon the type of pictures used in by the schemes.

3) Selection of pictures

In RGP schemes, passwords consist of different pictures, therefore selection of the pictures is very important for success of the schemes. The pictures which contain culturally familiar and singular objects such as pictures of famous animals and birds are easy to remember [21]. Rating depends upon the memorability level contains by the pictures selected for an RGP scheme.

4) Pictures relate stories

The password pictures can be easily memorized when some stories are related with the pictures. Stories can be easily created from pictures which represent events of human life. For example, if a user's birth date is on 10th of October, then pictures like birthday cake and candle are helpful in creating a story. Rating depends upon how easy it is to create stories from a list of pictures provided by an RGP scheme.

5) Freedom of choice

Different users have different choices for password pictures. Some users love pets, so they want pets to be their password pictures. The users who like electronic devices, want pictures of electronic devices for password creation. An RGP scheme needs to cover the choices of majority of the users.

6) Meaningfulness

Objects inside a picture can represent an event or mood such as birth date or happy. Meaningfulness provides further clues for memorization of a picture. Those pictures which do not draw any meaning or concept are difficult to memorize such as abstract art pictures. Stories depend upon a combination of pictures, while meaningfulness relates with an individual picture. Rating for this heuristic depends upon the meaningfulness of each picture provided for password creation.

7) Memory recall clues

Information can be easily recalled if memorization clues are remembered by a user. Colours and shape of objects inside a picture can provide additional clues for the password memorization. Rating depends upon memory recall clues available in the pictures of the RGP schemes.

8) User can upload pictures

System generated pictures are generally difficult to remember than user uploaded pictures. Therefore, allowing users to upload their pictures for password creation, is helpful for better memorability. Although this feature has memorability advantage but it can negatively affect the security of "online guessing attack". Therefore, this feature needs to be carefully used.

C. Usability heuristics of the model

In the proposed model 12 usability heuristics are given for analyzing the usability of the RGP schemes. All the usability heuristics are listed in table 5.

1) Efficiency

Efficiency is the time required to complete different authentication activities. Registration and login time varies from few seconds to a couple of minutes in RGP schemes. High ratings will be given to those schemes where short amount of time is required for completing the tasks of authentication.

Table 5: Usability heuristics

SNo.	Heuristics	Rating scale
01	Efficiency	5
02	Input reliability	3
03	Applicability	3
04	Easy of use	5
05	Design flexibility	5
06	Presentation of pictures	5
07	Click ratio	5
08	Page loading time	5
09	Understandability	5
10	Physical effort	5
11	Look and feel or design	5
12	Deployment	5

2) Input reliability

Password pictures need to be accurately selected in the RPG schemes. When size and space among pictures becomes small, then the users can click on pictures which are not related to their passwords. In order to achieve high reliability, size and space among pictures is required to be such that users can easily click on required password pictures.

3) Applicability

There are many types of computing devices and each category of the device has its own limitations. For example, smartphones have touchscreen support but have limited size, while desktop computers contain bigger screen with mouse and keyboard support. Rating of applicability depends upon the number of the device categories where an RGP scheme can smoothly execute.

4) Ease of use

A simple and pleasant user interface is important for performing the authentication tasks. Process for entering login credentials need to be smooth and less error prone, so that users can easily authenticate. The rating for this heuristic depends upon the overall satisfaction of users about the user interface of an RGP scheme.

5) Design flexibility

Computing devices come with different screen sizes, therefore an authentication scheme needs to adjust efficiently according to the screen sizes. Flexibility in RGP schemes can be achieved by auto re-sizing and re-positioning of the pictures. Rating of this heuristic depends upon the effect of screen adjustments over other features of usability.

6) Presentation of pictures

Many pictures are used in the RGP schemes, therefore proper arrangement of the pictures is important for usability of a scheme i.e. searching time increases when pictures do not have a constant location. Rating depends upon how effectively pictures are presented in the schemes.

7) Click ratio

In an RGP scheme, the password is inserted by clicking on different pictures. It is better to have one to one click ratio for a password picture selection. For example, if a user's

password consists of five password pictures then five times clicking will be required for password selection. Scrolling and pagination increases the number of clicks, therefore high ratings will be given to those schemes where small number of clicks are required for selecting the password pictures.

8) Page loading time

Pictures take time to load inside a web-page and RGP schemes use many pictures for authentication. Page loading time can be decreased if less number of pictures and other asset files are used in a scheme. For better ratings, less number of pictures need to be used and each pictures should have small size.

9) Understandability

New authentication schemes are generally difficult to understand because of unknown processes used for authentication. Therefore, it is better to use most commonly used processes inside an authentication scheme. A high rating will be giving to those schemes where well known and easy to understand processes are used for authentication.

10) Physical effort

In RGP schemes, physical effort is required for searching and clicking on password pictures. Searching becomes difficult when a large number of pictures are used in the schemes. Small size and space among the pictures can also increase the physical effort for authentication. For better ratings the number and size of pictures needs to be carefully selected.

11) Look & feel or design

Overall look and feel of an RGP scheme sneeds to be pleasant. Rating depends upon quality, size, and space among password pictures along with quality of overall theme of a scheme. Human computer interaction (HCI) rules when properly followed, can improve the look and feel of the schemes.

12) Deployment

Authentication schemes become difficult to deploy when they need some hardware or software for execution. It is desirable to deploy an authentication scheme with default configurations of hardware and software. High ratings will be given to those schemes, which can be smoothly deployed without any requirement.

IV. Test Case

For testing purpose, two RGP schemes are selected for evaluation by using the proposed model. The schemes are Passface [6] and Deja Vu [5]. Graphical interface of both the schemes are shown in figure 2 and figure 3.

A. Evaluation of Passface Scheme

Evaluation results of the Passface scheme is given in table 6-8. Justification of the ratings are given in the “Comments” column of the tables.

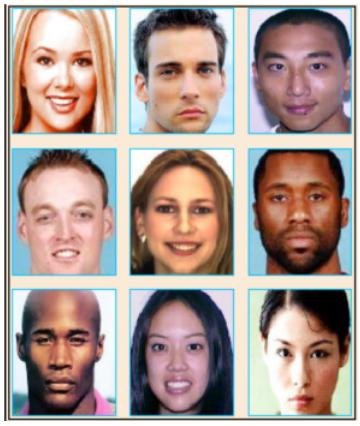

Figure. 2: Passface scheme [6]

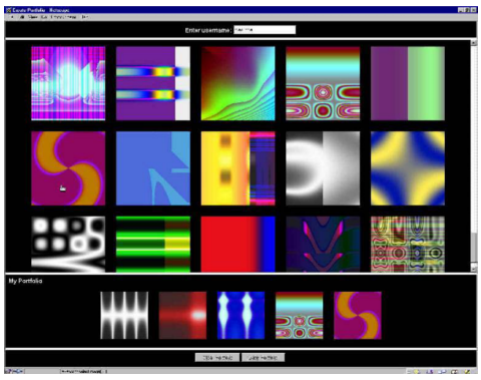

Figure. 3: Deja Vu scheme [5]

Table 6: Security evaluation of Passface Scheme

SNo.	Heuristics	Ratings	Comments
01	Brute force attack	2	The Passface scheme users 45 pictures on default configuration, which is quite low for brute force attack.
02	Dictionary attack	2	Users generally select password pictures based upon race, gender and attractiveness of human faces. This information can be used to create a password dictionary.
03	Shoulder surfing attack	0	This scheme is not resilient to shoulder surfing attacks.
04	Malware attack	2	Some effort is required for recognizing the password pictures after getting the information from the Malware programs.
05	Online guessing attack	2	It is very difficult to guess the passwords from a live application.
06	Intersection attack	0	The password pictures can be recognized from a recording of login session.
07	Social engineering attack	3	Password pictures of this scheme are difficult to describe, therefore social engineering attacks are difficult to apply.
08	Phishing attack	0	The password pictures can be easily recognized after applying a phishing attack.
09	Network interception attack	2	Pictures are shuffled in every login session, therefore attackers can not use recorded mouse coordinates for authentication.
10	Recordability Attack	2	Some effort is required to recognize the password pictures from recordings of mouse click positions and screen shots of login sessions.

Table 7: Memorability evaluation of Passface Scheme

SNo.	Heuristics	Ratings	Comments
01	Password scalability	2	Pictures are standardized for the scheme, therefore a user can use same password pictures among different accounts.
02	Minimum password size	3	The users have to remember five pictures of human faces, which is not difficult to memorize.
03	Selection of pictures	2	In the scheme only single category of pictures are used, therefore some effort will be required for memorization of the password pictures.
04	Picture relate stories	1	Stories can be easily created when multiple categories of pictures are used, but in this scheme pictures of single category is used, therefore it is difficult to create stories for password memorization.
05	Freedom of choice	0	Users are restricted to select pictures of human faces, which prevents the freedom of choice.
06	Meaningfulness	1	Very difficult to draw meaning from pictures of human faces.
07	Memory recall clues	1	Very minor clues are available such as gender and race.
08	Pictures upload facility	0	Users can not upload the password pictures.

Table 8: Usability evaluation of Passface Scheme

SNo.	Heuristics	Ratings	Comments
01	Efficiency	2	Passface scheme on average requires 3 to 5 minutes for registration and 20 seconds for login [22]. Therefore, the Passface scheme is little bit slow with respect to efficiency.
02	Input reliability	2	The pictures are separately presented along with border, therefore chances of input errors are low.
03	Applicability	1	Passface scheme can execute smoothly in majority of the devices.
04	Ease of use	4	Users can easily click on password pictures from the login screen.
05	Design flexibility	4	The pictures can be easily re-sized to adjust on different devices, hence the Passface scheme provides sufficient design flexibility.
06	Presentation of pictures	4	The pictures are presented in different screens, which improves usability of the scheme.
07	Click ratio	3	A user has to click on password picture along with pagination link, therefore one to one ratio is not maintained.
08	Page loading time	3	Forty five pictures are presented in the scheme, which does not take much time to load.
09	Understandability	3	The authentication process is very easy, the users just need to click password pictures on different screens the scheme.
10	Physical effort	3	Searching and clicking the password pictures is not difficult, as only nine pictures are shown on each screen of the scheme.
11	Look & Feel or design	3	The pictures are presented in grid-based arrangement, which improves look & feel of the scheme.
12	Deployment	3	The scheme can be deployed on different computing devices with basic configurations.

B. Evaluation of Deja Vu Scheme

Results of security analysis is given in table 9, while results of memorability and usability analysis are given in table 10 & 11 respectively.

C. Comparison between Passface and Deja Vu scheme

Comparison of both the schemes is shown in figure 4. The comparison results show that performance of Passface scheme is slightly better than Deja Vu scheme because total evaluation points of Passface scheme are 60, while Deja Vu scheme has got 58 points. The Passface scheme is better in memorability and usability but it is weak with respect to security.

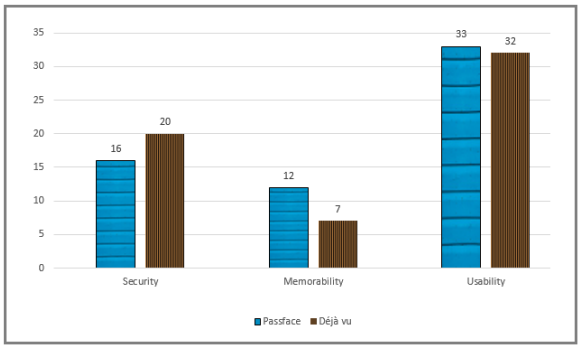

Figure. 4: Comparison of Passface Vs Deja Vu scheme

Comparison between Passface and Deja Vu scheme against all the heuristics of the proposed model are given in figure 5 - 7.

V. Discussion

The proposed model analysis the RGP schemes with the help of different heuristics. Performance of the schemes can be recognized with the total evaluation score. If an evaluator gives slightly different rating to any of the heuristic, the final result may not be effected. For example, if an evaluator gives rating "4" to scheme "A" and "3" to scheme "B" for the heuristic "efficiency", when the correct ratings are "3" and "2" for the scheme "A" and "B" respectively. There will be no effect in the final evaluation results because both the results show that scheme "A" is better than scheme "B" with respect to the heuristic "efficiency".
There are some heuristics which have conflicting nature. For example, in memorization point of view minimum size of a password needs to be as low as possible, while with respect to security higher length is better. In order to adjust this conflict, a mid-point needs to be identified to fulfill the requirements of both memorability and security.

VI. Conclusion

Current evaluation models provide complex methods of analyzing the schemes. In the proposed model, evaluation is done by different heuristics, which are individually analyzed, as a result detailed level of analysis can be made. In the proposed approach a simple process has been introduced to evaluate different authentication schemes.
The proposed model can be easily enhanced to cover pure and cued recall-based GP schemes. For that purpose missing usability and memorability heuristics need to be identified. While, security heuristics of the proposed model can be used in all the three categories of GP schemes.

References

[1] A. Anne and S. M. Angela, "Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures," *Commun. ACM*, vol. 42, 1999.

[2] R. N. Shepard, "Recognition memory for words, sentences, and pictures," *Journal of verbal Learning and verbal Behavior*, vol. 6, no. 1, pp. 156–163, 1967.

[3] M. Mihajlov, B. Jerman-Blazič, and S. Josimovski, "A conceptual framework for evaluating usable security in authentication mechanisms-usability perspectives," in *5th International Conference on Network and System Security (NSS)*, pp. 332–336, IEEE, 2011.

[4] R. English and R. Poet, "Towards a metric for recognition-based graphical password security," in *5th International Conference on Network and System Security (NSS)*, pp. 239–243, IEEE, 2011.

[5] A. Perrig and R. Dhamija, "Deja vu: A user study using images for authentication," in *Proc. 9th USENIX Security Symposium*, 2000.

[6] P. Dunphy, J. Nicholson, and P. Olivier, "Securing passfaces for description," in *Proceedings of the 4th symposium on Usable privacy and security*, pp. 24–35, ACM, 2008.

[7] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes.," in *In Proc. 13th USENIX Security Symposium*, 2004.

[8] B. Bilgi and B. Tugrul, "A shoulder-surfing resistant graphical authentication method," in *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*, pp. 1–4, IEEE, 2018.

[9] N. Lopez, M. Rodriguez, C. Fellegi, D. Long, and T. Schwarz, "Even or odd: A simple graphical authentication system," *IEEE Latin America Transactions*, vol. 13, no. 3, pp. 804–809, 2015.

[10] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *Security and Privacy (SP), 2012 IEEE Symposium on*, pp. 553–567, IEEE, 2012.

[11] K. Halunen, J. Häikiö, and V. Vallivaara, "Evaluation of user authentication methods in the gadget-free world," *Pervasive and Mobile Computing*, vol. 40, pp. 220–241, 2017.

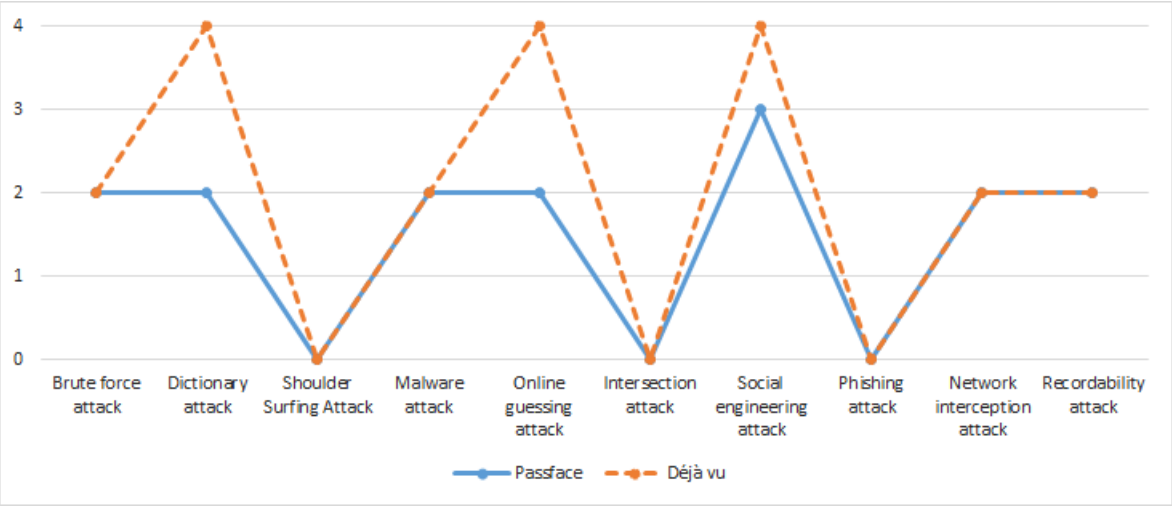

Figure. 5: Security comparison between Passface vs Deja Vu scheme

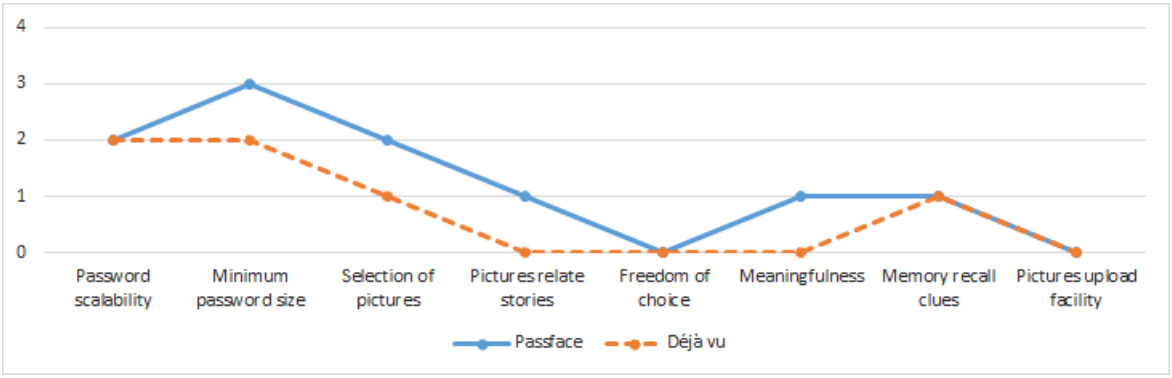

Figure. 6: Memorability comparison between Passface vs Deja Vu scheme

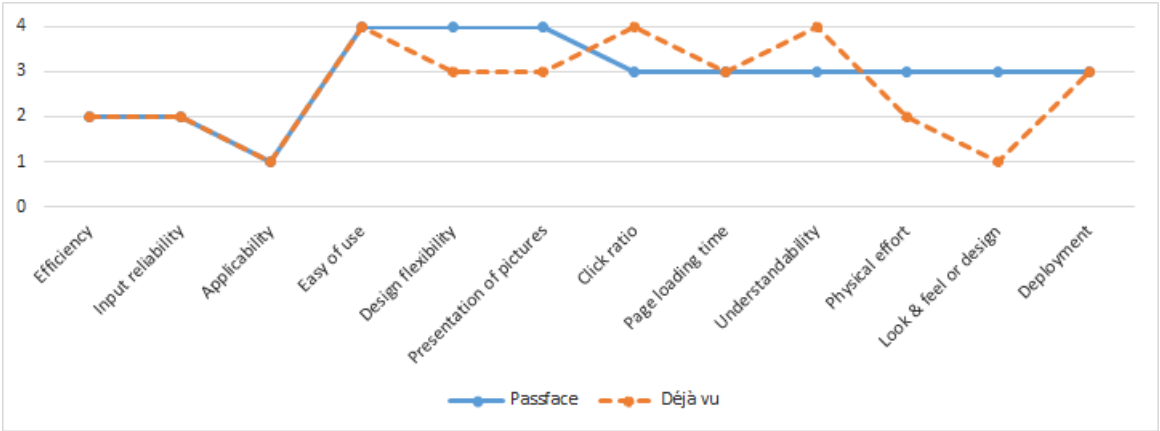

Figure. 7: Usability comparison between Passface vs Deja Vu scheme

Table 9: Security evaluation of Deja Vu Scheme

SNo.	Heuristics	Ratings	Comments
01	Brute force attack	2	Deja Vu scheme uses twenty five pictures for password creation, therefore moderate level effort is required for brute force attack.
02	Dictionary attack	4	Very difficult to create a password dictionary from the pictures used in the Deja Vu scheme.
03	Shoulder surfing attack	0	This scheme is not resilient to shoulder surfing attacks.
04	Malware attack	2	Some effort is required for recognizing the password pictures after getting the screen shots of the login screen and coordinates of mouse click.
05	Online guessing attack	4	The pictures used in the scheme, do not give any clue of the passwords.
06	Intersection attack	0	The password pictures can be recognized with the intersection attack.
07	Social engineering attack	4	The abstract art pictures are very difficult to describe.
08	Phishing attack	0	The scheme is not resilient to the phishing attack.
09	Network interception attack	2	Recorded login credentials can not be used for new login session.
10	Recordability attack	2	Password pictures can be recognized after analyzing multiple recordings of mouse click positions and screen shots of the login screen.

Table 10: Memorability evaluation of Deja Vu Scheme

SNo.	Heuristics	Ratings	Comments
01	Password scalability	2	Password pictures are not standardized i.e. different abstract pictures can be used in different implementations.
02	Minimum password size	2	Minimum password size is five in Deja Vu scheme. Five abstract art pictures are difficult to remember.
03	Selection of pictures	1	Memorability point of view, Deja Vu pictures are difficult to memorize.
04	Pictures relate stories	0	Almost impossible to create stories from abstract art pictures.
05	Freedom of choice	0	There is no freedom of choice, users are restricted to select from the provided pictures.
06	Meaningfulness	0	Very hard to draw meanings from abstract art pictures.
07	Memory recall clues	1	Very difficult to remember the pictures from the color combinations.
08	Pictures upload facility	0	Users can not upload the password pictures.

Table 11: Usability evaluation of Deja Vu Scheme

SNo.	Heuristics	Ratings	Comments
01	Efficiency	2	Deja Vu scheme requires 45 seconds on average for registration and 32 sec for login [5].
02	Input reliability	2	The pictures are separately presented in the scheme.
03	Applicability	1	Deja Vu scheme can be easily implemented in different kind of devices.
04	Easy of use	4	Users can easily click on password pictures.
05	Design flexibility	3	The pictures can be easily re-sized to adjust in different screen sizes but page scrolling will appear in small screen sizes.
06	Presentation of pictures	3	The pictures are presented in grid-based design which is good for usability.
07	Click ratio	4	A password picture is selected with single mouse click.
08	Page loading time	3	All the pictures are loaded in small amount of time in the login screen of Deja Vu scheme.
09	Understandability	4	Authentication process is very easy to understand, users just need to click on their password pictures in the login screen.
10	Physical effort	2	Searching requires some effort because the pictures are difficult to differentiate.
11	Look & feel or design	1	Design of the scheme is fine but overall look is not good due to the abstract art pictures.
12	Deployment	3	The scheme is easy to implement in majority of the computing devices.

[12] T. Khodadadi, A. M. Islam, S. Baharun, and S. Komaki, "Evaluation of recognition-based graphical password schemes in terms of usability and security attributes," *International Journal of Electrical and Computer Engineering*, vol. 6, pp. 2939–2948, Dec. 2016.

[13] D. Florêncio, C. Herley, and P. C. Van Oorschot, "An administrator's guide to internet password research.," in *LISA*, pp. 35–52, 2014.

[14] R. Lundin and S. Lindskog, "Changes in guesswork over time in multi-processor attacks," *Journal of Information Assurance and Security (JIAS)*, vol. 7, no. 4, pp. 241–251, 2012.

[15] C. Li and X. Zhang, "Password cracking based on rainbow tables with a dynamically coarse grain reconfigurable architecture," *Intelligent Automation & Soft Computing*, vol. 18, no. 7, pp. 923–935, 2012.

[16] B. Ur and P. Gage, "How does your password measure up? the effect of strength meters on password creation," in *21st USENIX Security Symposium*, 2012.

[17] M. Dupuis and F. Khan, "Effects of peer feedback on password strength," in *2018 APWG Symposium on Electronic Crime Research (eCrime)*, pp. 1–9, IEEE, 2018.

[18] R. Glabb, L. Imbert, G. Jullien, A. Tisserand, and N. Veyrat-Charvillon, "Multi-mode operator for sha-2 hash functions," *journal of systems architecture*, vol. 53, no. 3, pp. 127–138, 2007.

[19] W. Luo, Y. Hu, H. Jiang, and J. Wang, "Authentication by encrypted negative password," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 114–128, 2019.

[20] E. Erdem and M. T. Sandıkkaya, "Otpaas – one time password as a service," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 743–756, 2019.

[21] H. M. Aljahdali and R. Poet, "Challenge set designs and user guidelines for usable and secured recognition-based graphical passwords," in *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 973–982, IEEE, 2014.

[22] S. Brostoff and M. A. Sasse, "Are passfaces more usable than passwords? a field trial investigation," in *People and Computers XIVUsability or Else!*, pp. 405–424, Springer, 2000.

Author Biographies

Dr. Shah Zaman Nizamani has received the PhD degree from Quaid-e-Awam University of engineering Science and Technology, Pakistan. Currently working as an associate professor in Quaid-e-Awam University, in the department of information technology. He has around 13 years of experience both in teaching and software development. His research interest includes information security and software estimation.

Dr. Syed Raheel Hassan is working as an Assistant Professor in the Department of Computer Science at King Abdulaziz University, Saudi Arabia. He obtained his PhD in the Management of Security for Grid Computing Networks from Universite De Franche-Comte. He has worked in the industry and academia for more than 17 years. His research focused on IDSs, SIEMs, and Graphical Passwords.

Dr. Riaz Ahmed Shaikh is currently an Associate Professor at the Computer Science Department of the King Abdulaziz University, KSA. He received a Ph.D. degree from the Computer Engineering Department of Kyung Hee University, Korea in 2009. He wrote 50+ research articles published in peer-reviewed journals, and conferences. The two US and one Korean patents are issued to him. He served as a technical program committee member of 35+ international conferences. He was also an editor of the book entitled "Secure Cyber-Physical Systems for Smart Cities" published by IGI Global, USA. His research interests include privacy, security, trust management, risk estimation, sensor networks, Vehicular networks, and IoT. For more information please visit http://sites.google.com/site/riaz289

Sheikh Tahir Bakhsh has received the Ph.D. degree in Computer and Information Sciences from Universiti Teknologi PETRONAS, Malaysia in 2012. He joined the faculty of Computing and Information Technology, King Abdul Aziz University, Saudi Arabia as an Assistant professor in 2013. In the recent he has completed LTE HICI project with the collaboration of Stanford. He has also directed graduate and undergrad graduate projects. His areas of reach interests include Bluetooth network, Wireless sensor network (WSN), Mobile ad hoc network (MANET), and Computer networks. He works mainly on wireless network protocol designs optimizing the performance of networks. Recently, he has been involved in project related physical protocol design for Bluetooth scatternet. He has published more than 25 journal articles and referred conference papers in these area.