Date of publication MAR-31, 2025, date of current version DEC-15, 2024.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.24.1.3884

Effective Graphical Password Mechanism Using Two-Dimensional Shapes

KHALID MANSOUR[1,2], BILAL EID FAYYADH[1], YASER AL-LAHHAM[1], HAYEL KHAFAJEH[1]
[1]Faculty of Information Technology, Zarqa University, Zarqa, Jordan
[2]Faculty of Computer Studies, Arab Open University, Bahrain

Corresponding author: Yaser Al-Lahham (e-mail: yasirlhm@zu.edu.jo)

This research is funded by the Deanship of Scientific Research at Zarqa University, Jordan.

ABSTRACT Authentication systems are paramount to individuals and institutions. Several methods are proposed and used to grant access for legitimate users to systems. The most common way of authenticating users is textual passwords. However, textual passwords can be forgotten—especially if they are used infrequently—or easily guessed, as many users tend to choose simple passwords that are easy to remember. Furthermore, even though other authentication mechanisms can be used such as biometric passwords, these methods may require extra equipment and requirements. Graphical authentication methods were proposed because humans can remember pictures and shapes more than written text. This paper presents an empirical analysis of a password creation mechanism based on selecting several intersected 2D shapes. This mechanism of password creation enhances remembering passwords and protecting them from being attacked since it automatically transforms these shapes into long textual passwords. The experimental results show that users experience little difficulty in remembering the 2D passwords. On average, users require about two attempts or less to remember their passwords under all experimental results.

KEYWORDS Graphical passwords; Hardening Passwords; 2D shapes; Authentication systems.

I. INTRODUCTION

AUTHENTICATION systems are essential parts of any computer system and have received community interest since the invention of computer systems [8, 14]. With the introduction of computer networks and the Internet, authentication mechanisms and passwords have become increasingly crucial for preserving data privacy and integrity across multiple devices. Regarding authentication issues, security has always been a major worry because it can break the privacy of the users and enable unauthorized access to systems. Authentication procedures have been set out to preserve data from this unauthorized access. Authorized users are given passwords, as a text of their choice, to remember them when accessing the systems. Textual passwords are widely used since they are simple and cheap. These passwords should be chosen to be hard to predict by intruders, making them complex and easy to forget. Unfortunately, most users tend to use simple to-remember passwords; for example, in 2017, the Telegraph newspaper claimed that the majority of individuals used the password (”12345”) [10], which led to develop some tools to asses textual password creation, such as the proposal in [17], or to harden the password surfing by adding the pattern of keystroke as a part of the password, such as in [18]. Other authentication systems, such as biometric-based ones, are being utilized to solve some textual password problems [5]. However, biometric-based authentication methods are challenging when considering cost, privacy, and health issues. Graphical password schemes were proposed to enable users to remember passwords easily. This type of authentication depends on flash scenes that are simply remembered as many cognitive and psychological studies showed that one could remember pictures better than remembering texts [5]; that is because flash scenes are stored in the long-term memory of the human being, as reported by some researchers [13]. Moreover, some researchers reported that graphical passwords achieved a recall rate of 97%, and the password entropy was higher than short PINs [3]. Similarly, an authentication mechanism that formed a password using text and an image showed that the login success rate after a week was over 90% [9].

To this end, this paper extends a previous work [4] by incorporating the results of extensive empirical, experimental works that show that the proposed 2D-shapes graphical authentication system effectively remembers the drawn 2D-shape passwords. As an experiment, several users are asked to form a number of shapes by picking them from the predefined set of regular shapes, and the formed shapes should include an intersection of selected standard shapes. The experimental results section shows the details regarding the number of shapes and intersections. Each shape that corresponds to a particular user is automatically converted into a textual password, which is then fed to a hash function to give it a key with which it is stored in a database. The features of a 2D-shaped password include the types of shapes, the order of the drawn shapes, and the intersections between shapes, which gives a broader password space, making 2D-shaped passwords effective against brute force attacks, dictionary attacks, and key logger attacks [9]. This paper demonstrates the effectiveness of the 2D-shape-based authentication mechanism empirically.

The rest of the paper is organized as follows: Section 2 reviews the related work, while Section 3 shows the proposed authentication mechanism. Section 4 explains the experimental setups and the results. Finally, Section 5 concludes the paper and presents directions for future work.

II. RELATED WORKS

The authentication systems that use graphical patterns to represent passwords are commonly based on: (1) drawing metrics to produce and re-draw a pattern or recall-based methods, users should remember the pattern without being guided by the system and may be vulnerable in case of a dictionary attack [15]; (2) loci metrics, or cued-recall methods, which require the user to repeat pre-defined points in an image, this method suffers from the problem that images could be displayed using different contrast so the selected points could be different from the originally pre-defined ones [12], or hot-spot problem [15]; (3) search metrics, or recognition-based methods, authenticate users by selecting a number of pre-defined pictures from a list of random images. This method suffers from high communication cost problems [15]. In addition to the problems indicated with the above methods, these mechanisms also suffer from shoulder surfing problems [5, 7].

Some research efforts used hybrid graphical and textual representations for the sake of strengthening textual passwords; for example, in [1], the researchers proposed a hybrid authentication system in which the user selects a number of images at the registration time and at the login time a grid of images is displayed where the user must remember the location (the row and column numbers) of his/her images, then a grid of alpha-numeric symbols is displayed, where the symbols at the row and column of the remembered images should be entered as a session password. In this case, each session would have a different password depending on the location of the user's images.

In [12], an image-based graphical authentication was proposed based on image encoding, where the selected image is encoded and encrypted by a selected key. The input image is decoded and decrypted by the same key the user provided at the authentication time. Authentication succeeds if the decrypted image and the decoded data are the same as the original image. The proposed method was tested against differences that could be encountered when displaying images at the generation phase and at the authentication phase. This method shows the high accuracy of image determination. However, the user should keep the encryption key, which, if lost, makes it impossible to decrypt the image. Moreover, the method was not tested in a real authentication environment.

An XML transform method was proposed in [6], in which a user is required to select an image and draw some pattern on that image. The system stores multiple instances of geometric statistics of the endpoints of the pattern in an XML database. At the login, the user has to regenerate the pattern (without any guided points) on the same image; then server matches the entered pattern with the stored ones. If the stored pattern matches, then the user has successfully logged in. However, it is clear that it is hard for the user to regenerate the pattern by hand without a guide, and the hand could make some deviations that makes an incorrect pattern.

Some other works proposed a graphical password for mobile devices; for example, [16] proposed the EvoPass, where a user is asked to select several different pass images, and the server adds a set of challenge list of images to them, making some modifications on the images to generate some sketches, and sends them back to the client. The client allows the user to try to recognize the sketch of his/her images. At the login, the system presents all sketches of images, and the user must correctly identify the sketches of his/her images. However, it could be challenging to select sketches of all images since it is difficult to remember them in case many images are used, especially for infrequent logins. A similar system of graphical authentication for mobile devices using JavaScript has been recently proposed by Jha, Anand, et al. in [19].

In [20], the authors proposed a graphical authentication based on a secret question, which is linked to an image (selected during the registration phase), and the secret image is embedded into a bigger (less important) image using the steganography method. The user must remember the secret question, and a hot spot within the "stego image" to restore the embedded image, to be authenticated by the system.

In [11], a map generating graphical passwords was considered. Due to it, a user is asked to draw a route (a straight line) between two locations on the map. In addition, they added some options to help the users remember their passwords, such as sight as a background. Finally, they added a guide for users to remember their passwords.

In [2], the researchers tried to overcome the problem of shoulder surfing against the picture-based graphical passwords by enabling the user to select six pictures as his/her password, a flag picture, and a skipping picture. The system presents twelve pictures at the login, and the user is asked to select his/her password among them. If the skipping or the flag picture is given, the user selects this image. The flag and the skipping images are given randomly at each login. The proposed method could solve the shoulder surfing attack, but the user still needs to remember eight pictures, which could be challenging for many users.

Recently, the authors in [21] presented a graphical password scheme (called Bu-Dash) that uses four shapes and a dash to build the password, such that a 3×3 shape grid is built to represent the password, at least two different shapes should be used. The proposed scheme was tested by two groups of users; survey and pilot groups. This method needs the user to remember the shapes and its location in the grid.

In [22], authors proposed a combined password; textual and graphical passwords. The user is prompted to draw an image of each digit, they use deep learning to classify the images, to predict the drawn figure, the system sends the index of the selected color of both the drawn digit and the background to the server, and they called it the "selected pixel", during the authentication phase the server sends back the uncolored images to the user to select the right color.

The authors of [23] proposed GamePass, where users can create their passwords by drawing three gestures on a background image with three hidden hotspots. The background is a game field, the system gives more scores to closer gestures to the hotspots. The hotspots are randomly selected, and three zones surround each. It is just like a guessing game, the users should have time to train them building their passwords.

In [24], three image frames are used to present 27 images uploaded by the user, each frame contains nine images, and each image has a two-digit number. During registration, a user is prompted to select an image from each frame, the numbers of the selected images form the password, and a hash function is applied to the selected images, and the hash results are XORed and submitted to the server. The user has to upload so many images, which could be hard for a user to follow.

In [25] a gesture was combined with an image to generate the graphical password. It is similar to the proposal of [23], but without the hotspot on the background image.

In [26] a graphical password construction was proposed that depends on drawing a graph of cells, which can be selected from a panel of dimension N× M, each cell has a color randomly selected from a predefined set of colors. The user should build a graph of P nodes. This method aimed to solve the shoulder surfing problem. The users should remember the positions of the graph nodes on the panel, and the color of each node, which could be hard to achieve for many users, especially for infrequent use of their passwords.

Estimation of Your Encodable Distorted Images (EYEDi) was considered in [27] to prevent over-shoulder attacks. A user has to register five images, which are distorted and saved on the server. At the authentication stage, the system presents a grid of the registered images beside a set of dummy images on a grid, the user has to click on the distorted images that he registered. The system prevents attacks by displaying different dummy images at each user logon. The user should remember the distortion of all of the registered images.

III. THE PROPOSED AUTHENTICATION SYSTEM

This part introduces the proposed verification approach using (2D) forms and how it could be used to overcome specific vulnerabilities in other graphical password structures, such as brute force and dictionary attachments. The proposed method includes a registration phase in which the user can select shapes, scale, and intersect them. Afterward, the system maps it into textual passwords. The other phase consists of a sign-in and verification phase.

A. REGISTRATION PHASE

In this phase, the system registers the user's data, and he/she enters a username and specifies a password by drawing a number of shapes, as illustrated in Figure 1. In our experiments, the user must draw at least two shapes using the shapes provided by the system (as shown in the left side of Figure 1). Provided 2D shapes are sorted into two categories. Different sizes of shapes are used to widen the space of alternative shapes, and these shapes should be intersected (at least one intersection) to give a more significant number of options as well. After the user generates his/her drawing, the system automatically generates a textual password according to the type and the layout of the selected shapes, as explained in the password encoding next in this section.

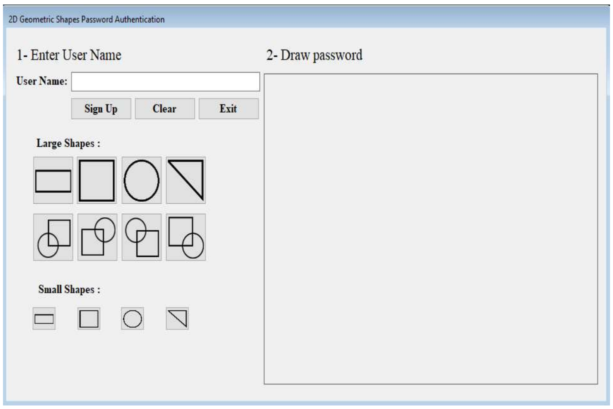

Figure 1. Interface for drawing shapes

B. PASSWORD ENCODING

Encoding a password involves assigning a different symbol for each shape, and these symbols are used to create the corresponding textual password. An example is illustrated in Figure 2, where a number is used as a symbol to represent each shape. The shapes are given the following symbols: (1→ Brec, 2→Bsq, 3→Bci, 4→ Btr, 5→ LBCS, 6→RTCS, 7→LTCS, 8→RBCS, 9→Srec, 10→Ssq, 11→ Sci, 12→Str). As mentioned in the previous phase, the textual password is generated by considering (1) the order of shapes drawn, (2) the type of shape, and (3) the intersections between shapes. Moreover, ready-made intersected shapes could be used to harden imitating a password since it is more difficult for an attacker to differentiate between a ready-made intersected and a user-intersected shape.

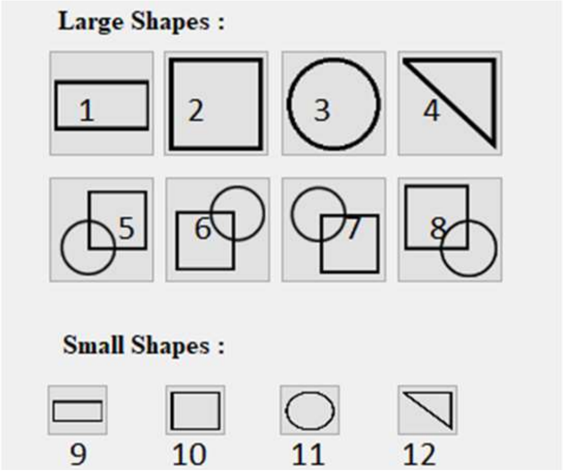

Figure 2. Shapes with designated numbers

Intersections created by users are encoded as follows: a shape is divided into four parts according to the position of intersection (as shown in Figure 3), and each part is given a code as follows: 1→LT, 2→TC, 3→RT, 4→LC, 5→RC, 6→LB, 7→BC, 8→RB, 9→UH (upper half of a large circle), 10→LH (lower half of a large circle). For example, if a user draws an intersection between a Bsq shape and another Bsq where the intersection position between (x-axis + 25) and (y-axis + 25), then the intersection code will be LT, see Figure 3. A circle shape is divided into two halves, where the top half area is considered separately in the calculation procedure.

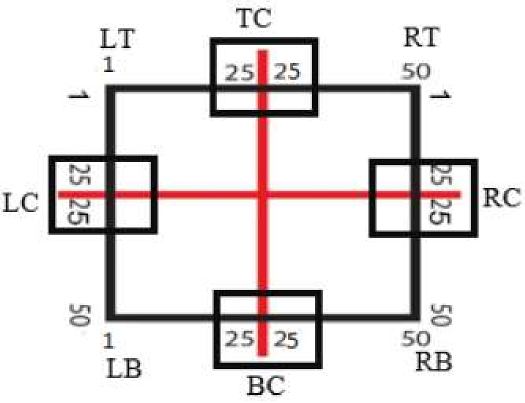

Figure 3. Possible intersections

Algorithm 1 represents the procedure of generating a textual representation of a graphical password. The first encoding step starts by determining the code for each shape drawn and concatenating its order to the overall code (line 7). For more clarification, if a user starts by drawing a square first, then the system concatenates the codec (Bsq) to (1), i.e., Bsq1, and stores it in an array, see line 8. Next, intersections between shapes are encoded as in line 10, and the type of the intersection is iteratively created by concatenating its appropriate code, see line 14. The algorithm generates a textual password of the graphical password shown in Figure 4 as follows: Brec1Bci2Brec3RTBrec1UHBci2, where the numbers shown in Figure 4 refer to the drawing order of the shapes. Finally, the MD5 hashing algorithm is used to hash the resulting textual password.

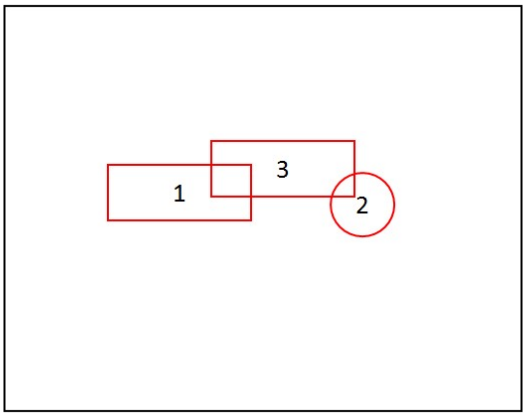

Figure 4. Example shape password

```
    Algorithm 1 generatePassowrd()
1:  password = null
2:  sha peNum = 0
3:  int ersect Num = 0
4:  ob ject = null
5:  for i = 1 t o numSha pes do
6:      sha peNum = get Sha peNum(i)
7:      encode = get E ncode(Sha peNum) + i
8:      array[i] = encode
9:      password = password + encode
10:     if i > 1 then
11:         for j = 1 t o numInt ersect s do
12:             if get Int ersect ion( j) <> null then
13:             object = get Int ersect ion( j) + array[j]
14:                 password = password + ob ject
15:             end if
16:             next j
17:         end for
18:     end if
19:     next i
20: end for
21: return  password
```

The proposed method generates longer textual passwords; for example, the graphical password shown in Figure 4 is formed using only three shapes and one intersection, where the length of the generated textual password is 27 characters. Consequently, a longer text-based password is more effective against brute force attacks than shorter ones. Moreover, the resulting textual password is rarely found in any dictionary.

Regarding shoulder surfing attacks, our proposed system is partially immune since an attacker who observes a 2D graphical password does not know the order in which shapes were drawn. Therefore, an attacker needs to try, for example, 120 different layouts in case a user drew a diagram using five different shapes.

Compared to the traditional textual password schemes, which enable users to select a sequence out of ASCII characters (94 printed symbols), our proposed mechanism may have more than 94 symbols, making the password space more significant than the password space of traditional text-based password schemes. Moreover, the entropy per symbol in our prototype is 3.58 - considering only 12 different shapes - bits, whereas traditional textual ones have 6.55 bits.

Consequently, the proposed authentication mechanism is effective against brute force attacks, dictionary attacks, shoulder surfing attacks, and keylogger attacks.

IV. EXPERIMENTAL RESULTS

The experiments shown in this section test the ability of users to remember the drawn shapes representing their passwords. This section presents the experimental settings and the experimental results and analysis.

A. EXPERIMENTAL SETTINGS

In our empirical experiments, thirty-one college students participated in the experiments. The experimental settings include three main phases, as shown in Table 2. The first phase allows users to draw passwords with one intersection and various shapes. The second phase allows for two intersections and various shapes, while the last phase allows for three intersections and various shapes. The first and second phases have four parts each, while the third has three, as shown in Table 2. In the first part of phases 1 and 2, the participants were asked to limit their password to three shapes, and in the second part, they used four shapes, etc., see Table 2. On the other hand, the first part of phase 3 starts with four shapes since one needs at least four to have three intersections. The participants were trained to use our prototype before starting the experiments. The participants were asked to draw their 2D-shaped passwords with concentration since they were not allowed to draw them on paper after saving the password. The following procedure is applied to each part of each phase:

Each participant selects a number of 2D shapes according to the instructions, which determine only the number of the allowed shapes and intersections between shapes.

Table 2. The experimental settings

Phase number	Number of intersections	Number of shapes			
1	1	3	4	5	6
2	2	3	4	5	6
3	3	–	4	5	6

On the following day, each user was asked to access our prototype system using the password that was drawn a day ago.

If the participant forgets his/her password, the password is given to him/her, and the number of trials becomes 2 for this participant.

Data was collected from the system after all participants completed their access trials.

At the end of the experiments, 11 datasets were collected, see Table 2. The following section shows the results of the experiments and analysis.

B. EXPERIMENTAL RESULTS AND DISCUSSION

This section presents and discusses the results of the experiments, which study the effect of the number of shapes and intersections on the 2D password remembrance.

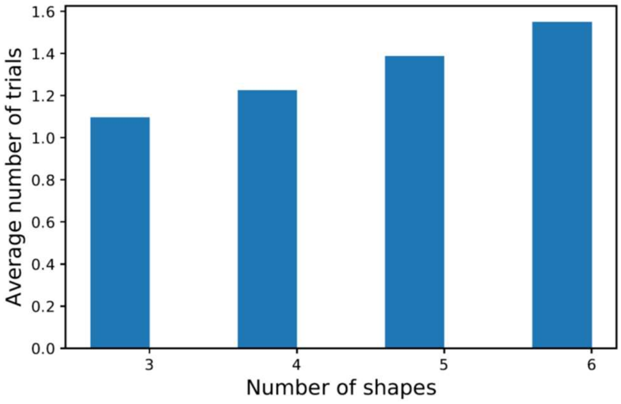

Figure 5. Users have one intersection between shapes

The results of using a different number of shapes with one intersection are shown in Figure 5. The results show that the number of trials needed for a participant increases as the number of shapes increases. However, the average number of trials for all shapes with one intersection is 1.31 times.

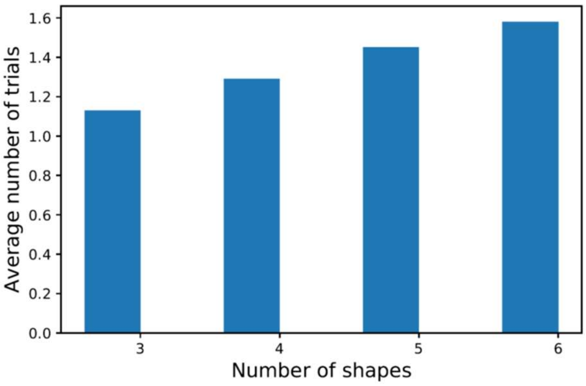

Figure 6. Users have two intersections between shapes

When two intersections are used, the average number of trials is slightly larger (1.36) than using a password with one intersection, see Figure 6. However, t-test result shows that there is no statistically significant difference between using one intersection or two intersections. The results shown in Figure 6 are consistent with those shown in Figure 5 regarding the number of shapes used, i.e., the number of trials needed to memorize the password is proportional to the number of shapes. When the number of intersections increased to 3, the average number of trials increased. The t-test results show that there is a statistically significant difference in the number of trials between using three intersections and one intersection.

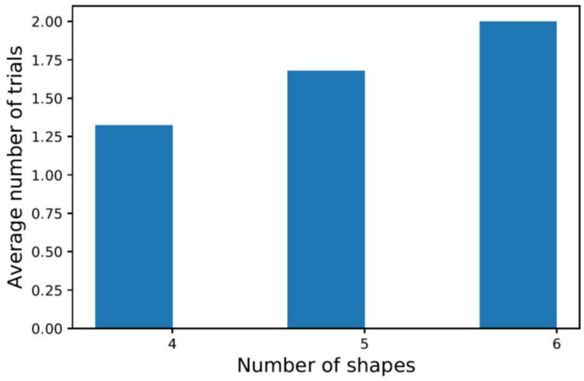

Figure 7. Users have three intersections between shapes.

Figure 8 shows the average number of trials against the number of intersections. The average number of trials for using 4, 5, and 6 shapes are 1.31, 1.36, and 1.67 for 1, 2, and 3 intersections, respectively. The results shown in Figure 8 indicate that when the number of intersections becomes three or more, the password remembrance ability decreases. However, even with three intersections, the average number of trials is less than 2.

The second set of figures shows the effect of using different shape numbers with 1, 2, and 3 intersections on password memorization. Figure 9 shows the results of using four shapes to construct the password. The figure does not show a significant effect between using 1, 2, or 3 intersections when the number of shapes is 4.

The results of using five shapes are presented in Figure 10. The results shown in Figure 10 indicate that having three intersections with five shapes significantly increases the number of trials needed. The results presented in Figure 11 are consistent with those in Figure 10, as three or more intersections require more trials to remember the password in both figures.

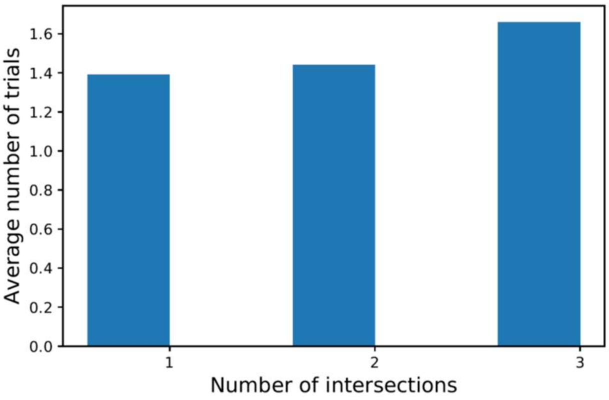

Figure 8. The average number of trials averages against a few intersections

It can be concluded that the effect of the number of shapes included in constructing the 2D shape password is more important than the number of intersections between the shapes in remembering the 2D password.

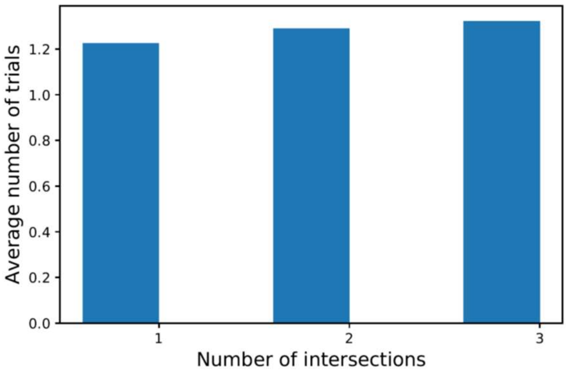

Figure 9. Users have four shapes with different intersections.

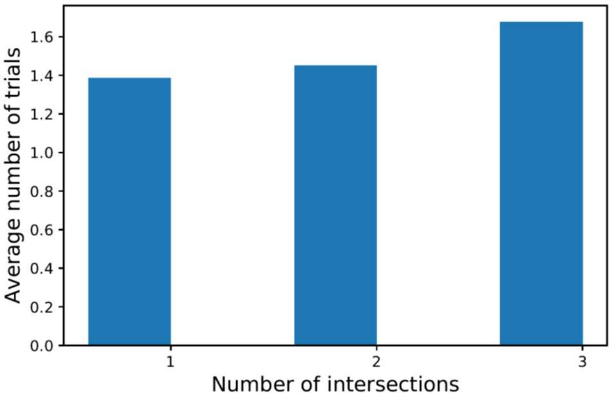

Figure 10. Users have five shapes with different intersections.

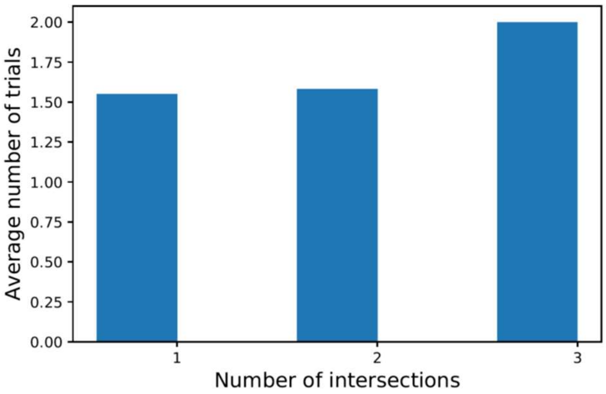

Figure 11. Users have six shapes with different intersections.

V. CONCLUSION AND FUTURE WORK

This paper develops a new graphical authentication mechanism based on using 2D shapes to construct a password. The proposed mechanism reduces the cognitive load associated with password remembrance and simultaneously makes the generated password more difficult to crack.

The application of the proposed authentication method on several users distributed over different categories shows that it is effective in terms of password remembrance since the overall results show that users, on average, needed about two trials or less to access the system.

The proposed authentication mechanism is effective against brute force attacks. It is also immune against dictionary attacks and keylogger attacks. It is also not easy for an attacker to guess the graphical password even if he/she sees the drawn diagram since the order in which shapes were selected is part of the password.

The proposed system has a mechanism to convert selected shapes and their intersections into long text passwords which can be hashed and stored.

As the number of shapes and their intersection involved in password, creations, the number of needed trials increases. However, the proposed mechanism is more effective in terms of creating, remembering and protecting password than text-based password.

As a future work, the system needs to be used on a broader scale to test its effectiveness further. In addition, a 3D shape-based password is worth investigating, as it can expand the password space and enhances its strength.

References

[1] S. Agrawal, A. Z. Ansari, and M. S. Umar,"Multimedia graphical grid-based text password authentication: For advanced users," *Proceedings of the 2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN)*, 2016, pp. 1–5. https://doi.org/10.1109/WOCN.2016.7759884.

[2] G. W. Bin, S. Safdar, R. Akbar, and S. Subramanian, "Graphical authentication based on anti- shoulder surfing mechanism," *Proceedings of the 2nd ACM International Conference on Future Works and Distributed Systems, ICFNDS'18*, New York, NY, USA, 2018, Article no. 20, pp. 1-6. https://doi.org/10.1145/3231053.3231073.

[3] N. Carter, C. Li, Q. Li, J. A. Stevens, E. Novak, Z. Qin, and J. Yu, "Graphical passwords for older computer users," *Proceedings of the Fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies, HotWeb'17*, 2017, pp. 7:1–7:7. https://doi.org/10.1145/3132465.3132472.

[4] B. E. Fayyadh, K. Mansour, and K. W. Mahmoud, "A new password authentication mechanism using 2d shapes," *Proceedings of the 2018 8th International Conference on Computer Science and Information Technology (CSIT)*, 2018, pp. 113–118. https://doi.org/10.1109/CSIT.2018.8486188.

[5] Z.M. Saadi, A.T. Sadiq, O.Z. Akif, A.K. Farhan, "A survey: Security vulnerabilities and protective strategies for graphical passwords," *Electronics*, vol. 13, issue 15, 3042, 2024. https://doi.org/10.3390/electronics13153042.

[6] K. Juneja. An xml transformed method to improve the effectiveness of graphical password authentication. Journal of King Saud University – Computer and Information Sciences, vol. 32, issue 1, pp. 11–23, 2020. https://doi.org/10.1016/j.jksuci.2017.07.002.

[7] S. Kumar, R. Ramya, R. Rashika, and R. Renu, "A survey on graphical authentication system resisting shoulder surfing attack," In: Chiplunkar, N.N., Fukao, T. (eds) Advances in Artificial Intelligence and Data Engineering. AIDE 2019. Advances in Intelligent Systems and Computing, vol 1133, pp 761–770, 2020. Springer, Singapore. https://doi.org/10.1007/978-981-15-3514-7_57.

[8] Gowtham M., M. K. Banga, and M. Patil, "Secured authentication systems for the Internet of things," *EAI Endorsed Transactions on Smart Cities*, vol. 4, issue 11, 4, 2020.

[9] I. Mackie and M. Yildirim, "A novel hybrid password authentication scheme based on text and image," In: Kerschbaum, F., Paraboschi, S. (eds) *Data and Applications Security and Privacy XXXII. DBSec 2018. Lecture Notes in Computer Science*, vol 10980. Springer, Cham. https://doi.org/10.1007/978-3-319-95729-6_12.

[10] C. McGoogan, "The world's most common passwords revealed: Are you using them?" The Telegraph, Jan 2017, [Online]. Available at: https://www.telegraph.co.uk/technology/2017/01/16/worlds-common-passwords-revealed-using/.

[11] W. Meng, L. Zhu, W. Li, J. Han, and Y. Li, "Enhancing the security of fintech applications with map-based graphical password authentication," Future Generation Computer Systems, vol. 101, pp. 1018-1027, 2019. https://doi.org/10.1016/j.future.2019.07.038.

[12] U. Singh, S. Chouhan, and S. Jain, "Images as graphical password: verification and analysis using non-regular low-density parity check coding," *International Journal of Information Technology*, 2020. https://doi.org/10.1007/s41870-020-00477-x.

[13] A. Delorme, M. Poncet, M. Fabre-Thorpe, "Briefly flashed scenes can be stored in long-term memory," *Frontiers in Neuroscience*, vol. 12, article 688, 2018. https://doi.org/10.3389/fnins.2018.00688.

[14] M. Xue, C. He, J. Wang, and W. Liu, "Lopa: A linear offset based poisoning attack method against adaptive fingerprint authentication system," *Computers and Security*, vol. 99, 102046, 2020. https://doi.org/10.1016/j.cose.2020.102046.

[15] G.-C. Yang, "Development status and prospects of graphical password authentication system in Korea," *KSII Transactions on Internet and Information Systems*, vol. 10, issue 11, 2019.

[16] X. Yu, Z. Wang, Y. Li, L. Li, W. T. Zhu, and L. Song, "Evopass: Evolvable graphical password against shoulder-surfing attacks," *Computers and Security*, vol. 70, pp. 179–198, 2017. https://doi.org/10.1016/j.cose.2017.05.006.

[17] Y. Al-Slais and W. El-Medany, "User-centric adaptive password policies to combat password fatigue," *International Arab Journal of Information Technology*, vol. 19, no. 1, pp. 55-62, 2022, https://doi.org/10.34028/iajit/19/1/7.

[18] K. Mansour and K. Mahmoud, "A new approach for textual password hardening using keystroke latency times," *The International Arab Journal of Information Technology*, vol. 18, no. 3, pp. 336-346, 2021, https://doi.org/10.34028/iajit/18/3/10.

[19] A. Jha, et al., "Graphical password authentication system for web and mobile applications in JavaScript," Cybersecurity Issues, Challenges, and Solutions in the Business World, edited by Suhasini Verma, et al., *IGI Global*, 2023, pp. 160-185. https://doi.org/10.4018/978-1-6684-5827-3.ch011.

[20] K. H. A. Al-Shqeerat, "An enhanced graphical authentication scheme using multiple-image steganography," *Computer Systems Science & Engineering (CSSE)*, vol. 44, no. 3, pp. 2095-2107, 2023. https://doi.org/10.32604/csse.2023.028975.

[21] P. Andriotis, M. Kirby, & A. Takasu, "Bu-Dash: a universal and dynamic graphical password scheme (extended version)," *Int. J. Inf. Secur.*, vol. 22, pp. 381–401, 2023. https://doi.org/10.1007/s10207-022-00642-2.

[22] A.F. Rasheed, M. Zarkoosh, & F.R. Elia, "Enhancing graphical password authentication system with deep learning-based Arabic digit recognition," *Int. J. Inf. Tecnol.*, vol. 16, pp. 1419–1427, 2024. https://doi.org/10.1007/s41870-023-01561-8.

[23] G. E. Raptis, C. Katsini, A. Jian-Lan Cen, N. A. Gamagedara Arachchilage, and L. E. Nacke, "Better, funner, stronger: A gameful approach to nudge people into making less predictable graphical password choices," In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI'21)*, 2021, Article 112, pp. 1–17. https://doi.org/10.1145/3411764.3445658.

[24] K. M. Quadry, A. Govardhan, M. Misbahuddin, "Design, analysis, and implementation of a two-factor authentication scheme using graphical password," *International Journal of Computer Network and Information Security*, vol. 14, issue 3, pp.39-51, 2021. https://doi.org/10.5815/ijcnis.2021.03.04.

[25] N. Patil, G. Bhutkar, P. Patil, P. Pishte, A. Popalghat, "Graphical-based password authentication," In: Fong, S., Dey, N., Joshi, A. (eds) *ICT Analysis and Applications. ICT4SD 2023. Lecture Notes in Networks and Systems*, vol. 782, 2023. Springer, Singapore. https://doi.org/10.1007/978-981-99-6568-7_38.

[26] H. Bostan, A. Bostan, "Shoulder surfing resistant graphical password schema: Randomized Pass Points (RPP)," *Multimed Tools Appl*, vol. 82, pp. 43517–43541, 2023. https://doi.org/10.1007/s11042-023-15227-x.

[27] T. Kawamura, T. Ebihara, N. Wakatsuki and K. Zempo, "EYEDi: graphical authentication scheme of estimating your encodable distorted images to prevent screenshot attacks," *IEEE Access*, vol. 10, pp. 2256-2268, 2022. https://doi.org/10.1109/ACCESS.2021.3138093.

KHALID MANSOUR received his Ph.D. in Computer Science from Swinburne University of Technology, Melbourne, in 2014. Currently, he is an Associate Professor of Computer Science at the Arab Open University in Bahrain. His research interests include machine learning, information security, and multi-agent systems.

BILAL EID FAYYADH received his M.S. degree in Computer Science from Zarqa University in Jordan. His research interest lies in information security.

Yaser A. Al-Lahham received a B.S. degree from the University of Jordan in 1985, an M.S. degree from Arab Academy (Jordan) in 2004, and a PhD in Computer science from Bradford University (UK) in 2009. He is currently an associate professor in the Department of Computer Science at Zarqa University in Jordan. His research interests include P2P information retrieval systems, text clustering, Natural Language Processing, and Databases.
Email: yasirlhm@zu.edu.jo

HAYEL KHAFAJEH obtained his Ph.D. in Computer Information Systems in 2008 in Jordan. He joined Zarqa University, Jordan in 2009. In 2010, he served as Head of the CIS Department for two years. Since the academic year 2014/2015, he has served and he still as the Vice Dean of the IT faculty. He has published many educational computer books for the Ministry of Education in Jordan. His research interests include information retrieval, AI and E-learning.