ICIC Express Letters
Volume **12**, Number **8**, August **2018**

ICIC International ©2018 ISSN 1881-803X
pp. **775–783**

AN IMPROVED AUTHENTICATION SCHEME BASED ON GRAPHICAL PASSWORDS

Mohammad Ahmad Alia, Adnan Ahmad Hnaif, Ayman Mahmoud Abdalla and Eman Mohammad Abu Maria

Faculty of Science and Information Technology
Al-Zaytoonah University of Jordan
P.O. Box 130, Amman 11733, Jordan
{ dr.m.alia; adnan_hnaif; ayman; eman.maria }@zuj.edu.jo

Received January 2018; accepted April 2018

Abstract. *This paper presents a new password scheme that employs graphical user interface for password entry. The password consists of multiple graphical objects that are integrated to form one picture. The main advantage of this approach is making user authentication more user-friendly where it is often easier to remember a scene than an alphanumeric password. The user creates the password scene by selecting from the available shapes where the selection process is combined with the selected objects to create the actual password. The scene created by the user is transformed into an alphanumeric password where the number of combinations used in creating this alphanumeric password from the given objects of the scene prevents brute-force attacks. These combinations include the choice of objects to use, the number of times each object is selected, the order of object selection, and object sizes. Other factors, such as colors and object location within the scene, could be added. Compared to entering alphanumeric passwords, these factors increase the security against shoulder-surfing attacks where an attacker tries to obtain the password either by directly looking over the victim's shoulder or by recording the whole login process. The alphanumeric password generated from the graphical password is not displayed and it is encrypted to prevent attacks on it. Implementation results and analysis of this scheme showed it to be secure and easy to use.*
Keywords: Graphical password, Identification, Authentication, Access control

1. **Introduction.** The field of information security is dedicated to preventing unauthorized use of information, including unwanted disclosure and modification. Information security services include identification and authentication (validating users), confidentiality (restrict access to information), integrity (preserving information from loss and corruption), non-repudiation (ensuring proper dissemination of information), and accessibility (providing access to information).

The first line of defense against unauthorized access to a computerized system is system access control through identification and authentication. Identification is the process of determining the identity of the user requesting access to the system, and authentication is the process of determining if the access request is genuine.

One of the most common methods of identification is giving each legitimate user a unique valid username. After the user is identified, authentication is performed using secret information stored in the system and associated with this user. Surveys of cryptography-based authentication methods are available [1,2]. Common authentication methods may be classified into four main categories: something you know, something you have, something you are (biometrics), and somewhere you are (location).

When authentication is based on something you know, it requires using a memorized password. These passwords are generally classified into two types: alphanumeric and

DOI: 10.24507/icicel.12.08.775

graphical. An alphanumeric password may use a combination of characters or may be simple such as an integer used as a personal identification number. More secure methods for alphanumeric passwords include symmetric key cryptosystems and public-key authentication with Diffie-Hellman key exchange. A graphical password is an image created by the user and encoded by the system for user authentication.

An authentication based on something you have requires using a tangible access object such as a token or an access card. A username may be included in the access object for low security systems such as hotel rooms. For more secure systems, as in banks, the user is normally required to use additional authentication methods such as a numeric password.

Biometrics recognition is a science that uses unique physical or behavioral characteristics for the purpose of identification and authentication. A survey with comparisons between biometric modalities, such as fingerprints, iris, retina, voice, and gait was performed by [2]. These natural characteristics of the user are captured by proper machines.

The physical location of the user or the user proximity to a specific object may be used in authentication. This method, however, is not sufficient by itself and it is often combined with other methods of user identification and authentication.

Graphical password authentication methods are not invasive like most biometric methods. They do not require special authentication hardware, and they do not require the user to carry an access object. In addition, graphical passwords are more secure and easier to use than alphanumeric passwords, but they require longer authentication time [3]. A graphical password is easier for the user to remember than an alphanumeric password, but the sequence of entering the components is not easily determined by looking at the password. This is because the components of a graphical password do not appear as a left-to-right sequence in the same order they are entered. Other password information, such as the attributes of the graphical password components, may not be easily noticed by observation.

This paper will present a new graphical password scheme that is secure and user-friendly. The new scheme is implemented and tested under different conditions to verify its convenience for different users. Results are analyzed theoretically and statistically to verify its security. The next section will discuss the previous work and Section 3 will present the new scheme. Sections 4 and 5 will discuss the implementation results and present analysis of the scheme and its effectiveness, respectively. Finally, the conclusion will be presented.

2. **Previous Work.**

A variety of schemes for using graphical passwords have been previously developed and implemented. The schemes varied in techniques, where they employed different factors to enhance their effectiveness.

In [4,5], a graphical-password authentication scheme for mobile devices was introduced. In this scheme, the user creates a graphical password by selecting from the available components, and authentication is performed by making the same selections. The selected sequence is represented in the authentication system by a sequence of corresponding numerical values. This scheme may not be well suited for non-mobile devices.

A scheme comprised of two authentication techniques was introduced by [6] for mobile devices. Their scheme used a grid that combines text and color properties for password generation, where the generated password changes with every login. This scheme requires long training and it may not be effective with general devices and average users.

The scheme in [7] uses a grid of random images with the correct password image included. A selection process is performed multiple times with different random images where the user is required to select the column containing the password image every time. This scheme appears to reduce the possibility of shoulder-surfing attacks, where the attacker attempts to obtain the password either by directly looking over the victim's shoulder or by recording the whole login process, since the user identifies columns rather

than single images. However, the authors did not provide sufficient experimental results and analysis to show the effectiveness of their scheme.

The scheme by [8] combined the ideas from two previous schemes: Draw a Secret (DAS) [9] and Story [10], and it focused on resistance to shoulder-surfing attacks. Their scheme used a grid of images where the user draws a curve through the password images and non-relevant images in the grid to produce the password. The pattern of the curve and its beginning and end points are variable to increase the randomness of the password and the difficulty of visually recognizing it. However, placement of password images close to each other in the grid reduces security, whereas scattering them reduces usability.

[11] increased the security of graphical passwords by image segmentation. In this system, the user selects an image as a password, and the image is automatically segmented with a grid. Authentication is performed by randomly rearranging the segments and asking the user to arrange them correctly. This increases usability at the cost of reducing security.

The scheme by [12] combined shape and text properties for password authentication in different mobile and non-mobile systems. This scheme employs a grid of points to allow the user to enter the password by drawing the required shapes, one by one. Each shape is mapped to a set of points on the grid. The user may use any combination of drawings, including letters, to create the graphical password. This scheme makes the password easier to remember. However, it requires longer entry time compared to other graphical password schemes, and users may need training before using it. In addition, users may compromise the security of the scheme when they create their passwords easier to draw and remember.

[13] used cued click points for user authentication, as part of a graphical password authentication system. This system requires the user to enter a username and a text password. Then, the user must choose an image and select three or more points on it. The user repeats the process of image and click-point selection with more images if desired. In addition, the user may choose a video sequence and specify a frame number with an object name. Although this method increased security against different types of attacks, it also increased difficulty for the users to remember password entry sequences. Furthermore, this method did not provide effective means to prevent guessing attacks based on hotspots – the click locations on pictures that are most likely chosen by users.

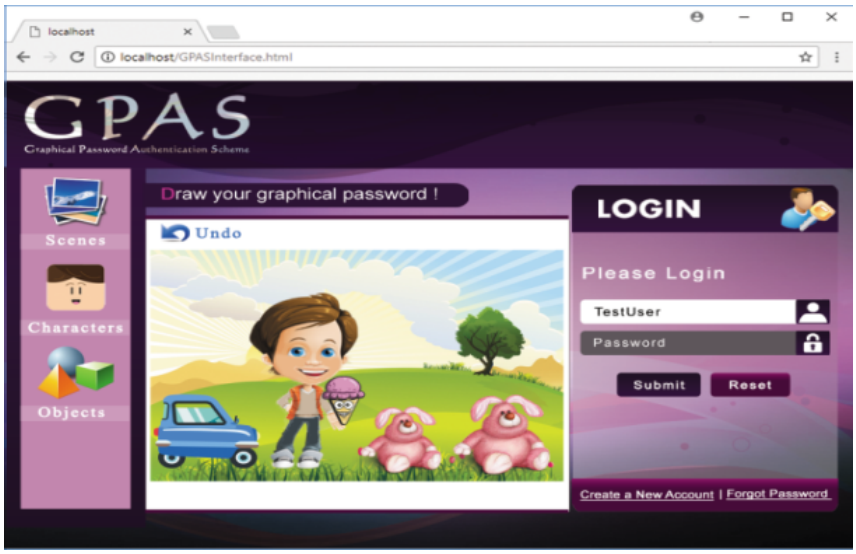
The problem of hotspots in general was addressed by [14] using saliency masks. Their study showed that masking hotspots increased security against guessing attacks at the expense of increasing difficulty for users to remember the click points, especially with images of simple details. Alternatively, [15,16] reduced the hotspot problem by using CAPTCHA as graphical passwords (CaRP), where CAPTCHA is the commonly used authentication system (Completely Automated Public Turing tests to tell Computers and Humans Apart). CaRP systems employ click-based graphical passwords, where multiple ordered clicks on an image are used to derive a password. Unlike other click-based graphical passwords, images used in CaRP are CAPTCHA challenges, and a new CaRP image is generated for every login attempt. However, this caused some difficulty for users.

Two algorithms in [17] used free-form sketches as graphical passwords and they were shown to have reasonable security and usability in different situations. However, they require large storage space and long computational time because they store each password as a different image and require complex feature-extraction and recognition operations.

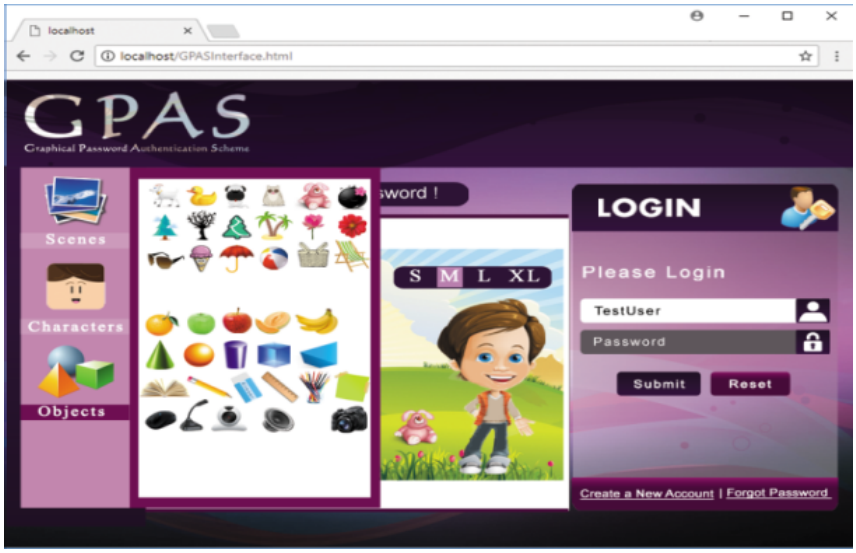
The authentication system presented by [18] performs authentication using a click-based graphical password combined with a sound sequence. They claimed their system is resistant to several types of attacks and provided a comparison with other systems to show that their system is more secure. Nevertheless, they did not provide sufficient experiments, convincing arguments, or detailed analysis to support their claim.

3. **The Graphical Password Authentication Scheme.** The proposed system, called Graphical Password Authentication Scheme (GPAS), provides a user-friendly graphical interface where the user selects different components to create and enter a graphical password. It provides access control in two phases: registration and authentication. In the registration phase, the system creates a username and a temporary alphanumeric password for identifying the new user. The user must log in using these username and password and change the password at the first login by creating a new graphical password that follows some given specifications dependent on the implementation. The registration is concluded by encrypting and storing the accepted password in the system. Then, the authentication phase allows the registered user to access the system using the valid username and password. The password components must be selected in the same order during registration and authentication.

3.1. **Password entry.** The GPAS entry screen, shown in Figure 1, provides the user with the option of entering a graphical password or an alphanumeric password. The alphanumeric password entry option provides a method for using a temporary password supplied by the system at first login or for password reset.



(a) A sample password



(b) Object selection in GPAS entry screen

FIGURE 1. Examples of graphical password entry screens in GPAS

The graphical password in GPAS is composed of three elements: one scene, one human character, and some objects. The scenes, characters, and objects may be chosen from pull-down menus. Each object may have multiple attributes, such as size, color, and rotation angle. The order of selecting the objects is significant, and objects may be repeated. However, the total number of objects, including repeated objects, must be within a given range. This range depends on the security level required by the system.

For first time users, the username is provided by the system along with a temporary alphanumeric password valid for one entry. Then, a graphical password must be entered and verified to be encoded and stored with the username for authentication of future logins.

3.2. **Password encoding.** The graphical password is represented by a binary number consisting of a code for each selected scene, character, object and object attribute. Note that changing the order of selecting these objects will produce a different collective binary number. For further security, the generated binary number should be encrypted, such as with a hash function, before it is stored.

If a user requires a temporary password, a new one is randomly generated and given to the user in the form of a hexadecimal number to be entered using the alphanumeric entry option. This alphanumeric password is compared only to the temporary passwords created by the system. The alphanumeric equivalent of a graphical password is not accessible by the user and may not be accessed with the alphanumeric password entry option.

4. **Implementation and Discussion.** GPAS has been implemented with the following available options. There are four scenes, representing the four seasons (Spring, Summer, Autumn, and Winter), four human characters (Man, Woman, Boy, and Girl), and 64 different objects. The scenes, characters, and objects may be chosen from pull-down menus as seen in Figure 1. Selected components of the graphical password are placed in the picture automatically. For this implementation, each object has only one attribute, which is the size (Small, Medium, Large, or Extra Large), chosen from a small menu as shown in Figure 1(b). Other attributes may be added in future implementations if needed. The total number of objects selected in the graphical password, including repetitions, has been limited to be in the range of four to 12 objects. The user may enter the components of the password in any order, but only the order of entering objects is significant. The scene and the character are encoded the same way regardless of the order they are entered. Undo and Reset buttons are available for correcting the current password entry, which is only allowed before the Submit button is selected. Links are provided for assistance in creating a new account and for resetting a forgotten password. The alphanumeric password entry option is only available for entering a system-generated password for new users and users who forgot their passwords. Such an alphanumeric password is valid only for one entry, and the user has to change it immediately after login.

The graphical password is represented by a binary number of 36 to 100 bits. The scene and the character are represented by two bits each. Each object is represented by eight bits, including six bits for selecting the object and two bits for its size. For example, the graphical password in Figure 1(a) is represented by the binary number shown in Figure 2, which is 24DA84E19 in hexadecimal. In this example, a Spring scene and a Boy character were selected. They are represented in this implementation by the binary numbers 00 and 10, respectively. The objects selected (with sizes) were, Medium Bunny, Small Car, Large Bunny, and Medium Ice Cream, in that order. These objects are represented by binary numbers, each followed by its size, in the same order of their selection. Therefore, their respective representations are 01001101, 10101000, 01001110, and 00011001. The binary password is the concatenation of these numbers, starting with the scene, and then the character, followed by the objects in the order they were selected, producing the binary

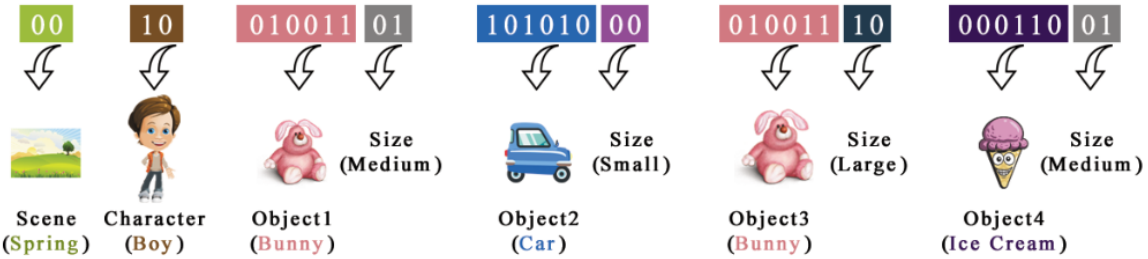


FIGURE 2. An example of binary number representation of a graphical password

TABLE 1. Timetable of login trials

Trial Number	Login Time	Login Platform	Number of Attempts
1	First Time at 10:00 am	Desktop Computer	5
2	After 1 Day at 05:00 pm	Tablet Computer	5
3	After 1 Week at 11:00 am	Desktop Computer	4
4	After 2 Weeks at 08:00 pm	Tablet Computer	3
5	After 1 Month at 10:00 pm	Desktop Computer	5

TABLE 2. Overall averages when password object repetition was or was not allowed

Trial No.	*when repetition was not allowed*						*when repetition was allowed*					
	Entry Durations			Success Rate %			Entry Durations			Success Rate %		
	Min	Max	Ave	Min	Max	Ave	Min	Max	Ave	Min	Max	Ave
1	15.50	22.50	19.61	80	100	98	12.00	17.50	14.79	80	100	96
2	11.00	19.00	15.26	60	100	87	10.20	17.10	14.33	60	100	89
3	11.00	16.80	14.06	50	100	83	11.00	16.80	14.12	50	100	78
4	10.30	17.00	12.90	33	100	74	9.90	17.30	14.10	67	100	93
5	13.20	19.00	16.39	60	100	76	11.00	18.00	14.66	60	100	80

number shown in Figure 2. Note that these objects do not appear in the password image with the same order of their selection.

This implementation of GPAS was tested with 18 different users whose ages ranged from 18 to 51, and they included one color-blind person. The users were provided with different 7-inch computer tablets and desktop computers placed in a computer lab, with proper instructions. They were requested to log in multiple times in each trial where attempts were at least five minutes apart. Entering the graphical password was done by touching the screen of the tablet or using the mouse of the desktop computer. To study the effects of increasing the number of graphical password objects on users, nine users were asked to create passwords with a different number of objects for each user, where the number of objects ranged from four to 12, without repeating any objects. Another group of nine users was asked to do the same, except for allowing them to repeat objects. After creating the passwords, each of the 18 users made multiple login attempts over a period of one month, as outlined in Table 1. For the different login trials, each user alternated between a desktop computer with a mouse and a 7-inch tablet computer. Access times varied to include daytime and evening. The results for the color-blind person were close to the average, and there was no evidence that shows a relationship between age and performance with this implementation. Table 2 shows the overall average login time for each trial with the corresponding overall average login success rate.

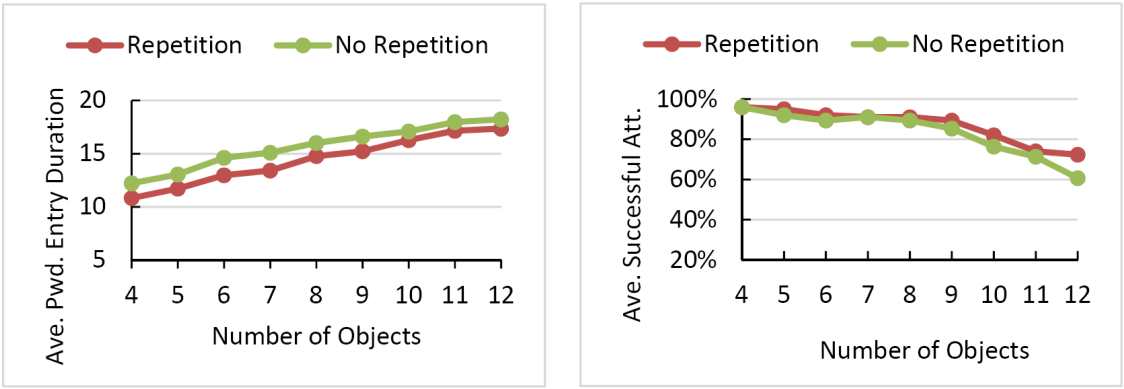
When repetition of objects in the password was not allowed, the duration required for entering a password for the first time ranged from 15.50 to 22.5 seconds with an overall average of 19.61 seconds. After one month, the overall average entry duration for

a password without repeated objects was down to 16.39 and ranged from 13.20 to 19.00 seconds. The overall average rate of success in login attempts was 98% with a range of 80% to 100% for first time login and an average of 76% with a range of 60% to 100% for login after one month. These results and the results for the other trials are listed in Table 2.

When object repetition was allowed, as seen in Table 2, the overall average duration required for entering the password for the first time was 14.79 seconds and ranged from 12.00 to 17.50 seconds. After one month, the overall average entry duration for a password with repeated objects was 14.66 and ranged from 11.00 to 18.00 seconds. The overall average rate of success in login attempts was 96% with a range of 80% to 100% for first time login and an average of 80% with a range of 60% to 100% for login after one month.

The above results indicate that users become more familiar with the system over time, requiring less password entry duration. However, users appeared to forget their passwords when they did not use them frequently, as demonstrated by the login success rates that decreased over time. In addition, overall results show that allowing users to repeat objects in passwords increased login success rate and reduced password entry duration.

The effect of increasing the number of objects in the password on users was observed. As seen in Figure 3(a), average password entry duration increased as the number of objects increased, whether object repetition was allowed or not, where passwords without repeated objects required slightly more login duration than passwords without repeated objects. The rate of average successful login attempts decreased as the number of objects increased, whether object repetition was allowed or not, where success rate with passwords containing repeated objects was slightly better than the rate when repetition was not allowed. This is illustrated in Figure 3(b).



(a) Ave. password entry duration (Seconds) (b) Ave. number of successful login attempts

FIGURE 3. Averages for password entry duration and percentage of successful login attempts

5. **Analysis.** Test results of GPAS implementation showed that it could be used easily with reasonable entry duration. In the implementation, the graphical password was represented by a binary number of at least 36 bits, providing a minimum of 2^{36} different possible passwords. If repetition of objects in the password is not allowed, the minimum number of allowed passwords decreases slightly, to become approximately $2^{35.966}$. The maximum number of 12 objects requires a password length of 100 bits, with 2^{100} different possible passwords if repetition is allowed.

One way to increase security against different types of attacks would be to increase the range (i.e., the minimum and maximum number) of the objects to be selected. However, this may increase the difficulty for some users, and reduce login success rate, as seen in

the experimental results of the previous section. A better alternative may be to increase the number of scenes and characters and to add more attributes to objects. For example, providing 16 scenes, 32 characters, and 64 objects, each with size and color, will increase the number of bits in the equivalent alphanumeric password to four bits for the scene, five bits for the character, and ten bits for each object with its attributes. In that case, a graphical password with four objects will require 49 bits and provide 2^{49} different possible passwords. Note that changing any element of the graphical password or changing the order of selecting objects produces different alphanumeric passwords. Conversely, changing one bit in the alphanumeric password will make it equivalent to a different graphical password.

Due to the exponential number of possible passwords, a brute-force attack on the system is impossible regardless of allowing object repetition. Allowing passwords to contain repeated objects increases the password space slightly and makes passwords easier to remember, but it may increase the risk of guessing attacks. Therefore, as with any other type of user-generated passwords, users should be discouraged from creating passwords that are too simple, easy to guess, or based on commonly known personal details.

Even though a graphical password is easier for the user to remember, it contains several components with different attributes that are not easily observed and remembered by looking at the entry screen in shoulder-surfing attacks. In addition, the implementation may perform automatic placement of objects, so that the order of object selection may not be determined from a view of the graphical password. Furthermore, limiting alphanumeric password entry to special temporary cases makes keyboard-entry attacks improbable. When it is convenient for the user, the number of objects in the password may be increased to make it more resistant to different attacks such as shoulder-surfing and guessing attacks.

A comparison of GPAS with other schemes is presented in Table 3. Due to the lack of availability of exact data for these schemes, the comparison is presented in general terms.

Table 3. Comparison of GPAS with other schemes

Scheme	Brute-force Attack	Shoulder Surfing	Guessing Attack	Training Required	Login Duration	Login Success	Hardware Required
GPAS	resistant	resistant	moderate	minimal	small	high	general
[4,5]	resistant	resistant	moderate	minimal	small	high	mobile
[6]	resistant	resistant	resistant	extensive	small	medium	mobile
[7,8,18]	resistant	resistant	moderate	minimal	small	high	general
[11]	moderate	moderate	moderate	minimal	small	high	general
[12,13]	resistant	resistant	moderate	moderate	long	medium	general
[14]	resistant	resistant	resistant	minimal	small	medium	general
[15,16]	resistant	resistant	resistant	moderate	small	medium	general
[17]	resistant	resistant	resistant	moderate	small	medium	advanced

6. **Conclusions.** This paper presented a graphical password authentication scheme, GPAS, which provides a convenient secure password authentication system. It includes a user-friendly interface for entering a graphical password consisting of a scene, a character, and multiple objects with attributes. The graphical password is translated by the system into a long alphanumeric password, which is then encoded and stored in the system where it may not be used directly for login. The exponential number of possible combinations for creating the graphical password makes it protected from brute force attacks and resistant to other types of attacks. Further resistance to shoulder-surfing attacks is caused by using attributes that are not easily observed by viewers, in addition to automatic object placement in the scene that is unrelated to the order of object selection. Implementation

results of GPAS demonstrated its easiness and reliability, where results showed that increasing the length of the graphical password caused an increase in entry duration and a decrease in login success rate. Future work could provide features such as choosing components through voice commands and using sound recordings to describe options and selections.

Acknowledgment. The authors would like to thank volunteers and lab assistants who performed the testing and Al-Zaytoonah University of Jordan for providing the equipment.

REFERENCES

[1] M. A. Alia, A. A. Tamimi and O. N. A. Al-Allaf, Cryptography based authentication methods, *Proc. of World Congress on Engineering & Computer Science*, San Francisco, CA, USA, vol.1, 2014.

[2] D. R. Ibrahim, A. A. Tamimi and A. M. Abdalla, Performance analysis of biometric recognition modalities, *The 8th International Conference on Information Technology*, Amman, Jordan, 2017.

[3] G. Agarwal, S. Singh and R. S. Shukla, Security analysis of graphical passwords over the alphanumeric passwords, *International Journal of Pure and Applied Sciences and Technology*, vol.1, no.2, pp.60-66, 2010.

[4] W. Jansen, S. Gavrila, V. Korolev, R. Ayers and R. Swanstrom, A visual login technique for mobile devices, *National Institute of Standards and Technology Interagency Report NISTIR 7030*, 2003.

[5] W. Jansen, Authenticating mobile device user through image selection, *Data Security*, 2004.

[6] M. Sreelatha, M. Shashi, M. Anirudh, M. S. Ahamer and V. M. Kumar, Authentication schemes for session passwords using color and images, *International Journal of Network Security & Its Applications (IJNSA)*, vol.3, no.3, pp.111-119, 2011.

[7] R. S. Yenape and A. Waghmare, Three way graphical password authentication, *International Advanced Research Journal in Science, Engineering and Technology*, vol.4, no.4, pp.155-157, 2017.

[8] H. Gao, Z. Ren, X. Chang, X. Liu and U. Aickelin, A new graphical password scheme resistant to shoulder-surfing, *International Conference on CyberWorlds*, Singapore, 2010.

[9] I. Jermyn, A. Mayer, F. Monrose, M. Reiter and A. Rubin, The design and analysis of graphical passwords, *Proc. of the 8th USENIX Security Symposium*, 1999.

[10] D. Davis, F. Monrose and M. K. Reiter, On user choice in graphical password schemes, *Proc. of the 13th Usenix Security Symposium*, San Diego, CA, USA, 2004.

[11] K. Chand and A. Anand, Graphical password system using image segmentation, *International Journal of Current Trends in Engineering & Research*, vol.2, no.5, pp.487-492, 2016.

[12] Z. Zheng, X. Liu, L. Yin and Z. Liu, A hybrid password authentication scheme based on shape and text, *Journal of Computers*, vol.5, no.5, 2010.

[13] S. B. Sahu and A. Singh, Secure user authentication and graphical password using cued click-points, *International Journal of Computer Trends and Technology*, vol.18, no.4, pp.156-160, 2014.

[14] F. Alt, M. A. Mikusz, S. Schneegass and A. Bulling, Memorability of cued-recall graphical passwords with saliency masks, *Proc. of the 15th International Conference on Mobile and Ubiquitous Multimedia*, New York, pp.191-200, 2016.

[15] A. D. Pavitwar, A. S. Qureshi and S. A. Gaikwad, Login authentication using CaRP, *Imperial Journal of Interdisciplinary Research*, vol.2, no.6, pp.669-672, 2016.

[16] A. U and B. Wilson, Security through CAPTCHA using graphical password, *International Journal of Innovative Research in Computer and Communication Engineering*, vol.5, no.4, pp.7238-7243, 2017.

[17] M. Martinez-Diaz, J. Fierrez and J. Galbally, Graphical password-based user authentication with free-form doodles, *IEEE Trans. Human-Machine Systems*, vol.46, no.4, pp.607-614, 2016.

[18] S. Sayed, A. Mohid, M. Pal and M. Haji, Graphical password based authentication system with sound sequence, *International Journal of Computer Applications*, vol.138, no.12, pp.38-43, 2016.