cisdi Journal

Computing, Information Systems & Development Informatics Journal
Vol. 10 No. 1, March, 2019 - www.cisdijournal.org

A Proposed Graphical Authentication Method for Preventing Shoulder-Surfing Attack

Adebimpe, Lateef Adekunle
Department of Computer Science
Emmanuel Alayande College of Education
Oyo, Oyo State, Nigeria.
E-mail: dradebimpela@yahoo.com

ABSTRACT

The adoption of Graphical password for authentication is increasing. Graphical passwords are widely used for authentication since human brain can easily recognize and recall visual images. Graphical password eliminates the difficulties involved in remembering random and complex passwords. In addition, graphical password discourages users from unsafe practices such as writing the password down. However, graphical password systems do encounter threats especially shoulder-surfing attack. Shoulder-surfing is the act of tactically obtaining useful information in order to legitimately gain access into a system. Overtime, many methods have been proposed to overcome shoulder-surfing attack. The outcome of the review indicated that most of these methods are still vulnerable to shoulder-surfing attack especially multiple observations and video-recorded shoulder-surfing attacks. It is against this backdrop that a new method is proposed to prevent shoulder-surfing attack, especially multiple observations and video-recorded shoulder-surfing.

Keywords: Graphical Password, Shoulder-Surfing, Biometric, Token, Authentication

CISDI Journal Reference Format
Adebimpe, Lateef Adekunle (2019): A Proposed Graphical Authentication Method for Preventing Shoulder-Surfing Attack. Computing, Information Systems & Development Informatics Journal. Vol 10 No 1. Pp 87-94. Available online at www.cisdijournal.org

1. INTRODUCTION

Information and communication technology (ICT) has become one of the basic necessities of modern society [1]. There are many systems and services using ICT and authentication is one of the methods that is used to authorize the legitimate users to access the secure systems and services [2-3]. Authentication can be classified into three: Token-Based, Biometric-Based and Knowledge-Based (see Figure 1). Token-based authentication depends on what the users have to perform authentication (e.g. ATM card). Biometric-based depends on users attributes to perform authentication (e.g. fingerprint). Knowledge-based depends on what the users know to perform authentication (e.g. secret password) [4]. Nowadays, graphical password systems are commonly being used for user authentication in many security systems [5].

The convenience of graphical password has reduced the difficulty often encountered in remembering complex alphanumeric passwords. Graphical passwords reduced memory burden, make passwords less predictable and discourage users from unsafe practices (such as writing down) [6]. However, graphical password systems do encounter threats especially shoulder-surfing attack. Shoulder-surfing is the act of tactically obtaining useful information in order to legitimately gain access into a system [7]).

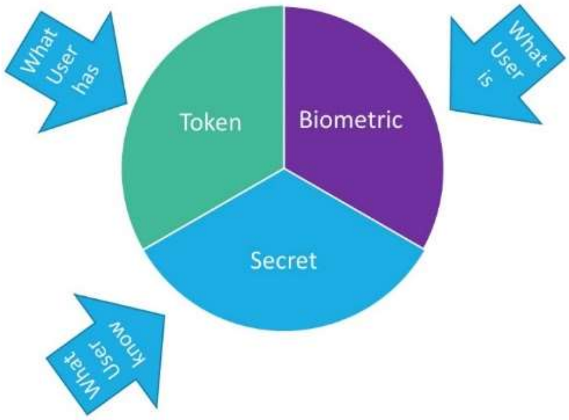


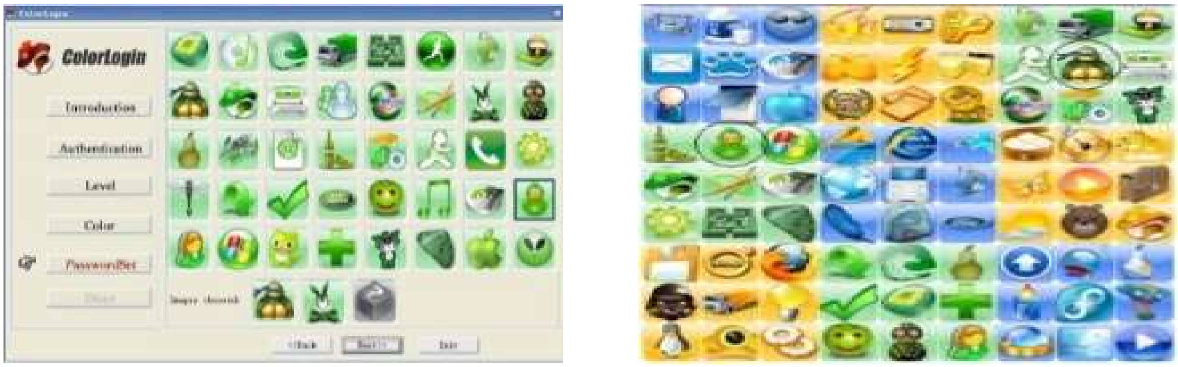
Figure 1: Basic forms of Authentication [4]

Many systems have been proposed to prevent shoulder-surfing attacks. These systems include Déjà vu [5], PassfacesTM [8] and Story systems [9] but they were easily shoulder-surfed by attackers. Later, ColorLogin [10], and cuedRecognition [11] were proposed to prevent shoulder-surfing attacks. These systems can confuse attackers from obtaining the correct pass-objects via direct observation but are vulnerable to multiple and video-recording shoulder-surfing. Hence, it is imperative to propose new method to overcome this challenge.

2. RELATED WORKS

In Déjà Vu proposed by [5], a user is required to register several images from the displayed images during the registration process. During the authentication process, the registered images and the decoy images are shown in the grid. The user needs to select registered images to login. The system is vulnerable to shoulder-surfing attack because attackers can easily capture the clicked images. In PassfacesTM [8-9], a user is required to register four images (human faces) during registration. During authentication, the user is required to identify and click the registered images within a 3x3 grid for four consecutive rounds. Since the registered images are clicked during authentication, attackers can easily capture the clicked images and use the information to gain access as legitimate users. Davis et al. [9] improved on PassfacesTM by using human faces images together with other categories such as sceneries and animals. A user is required to register certain images during the registration and make a story based on chosen images. During authentication, the user needs to click on the registered images in one after another. This system is easy to use but vulnerable to shoulder-surfing attack.

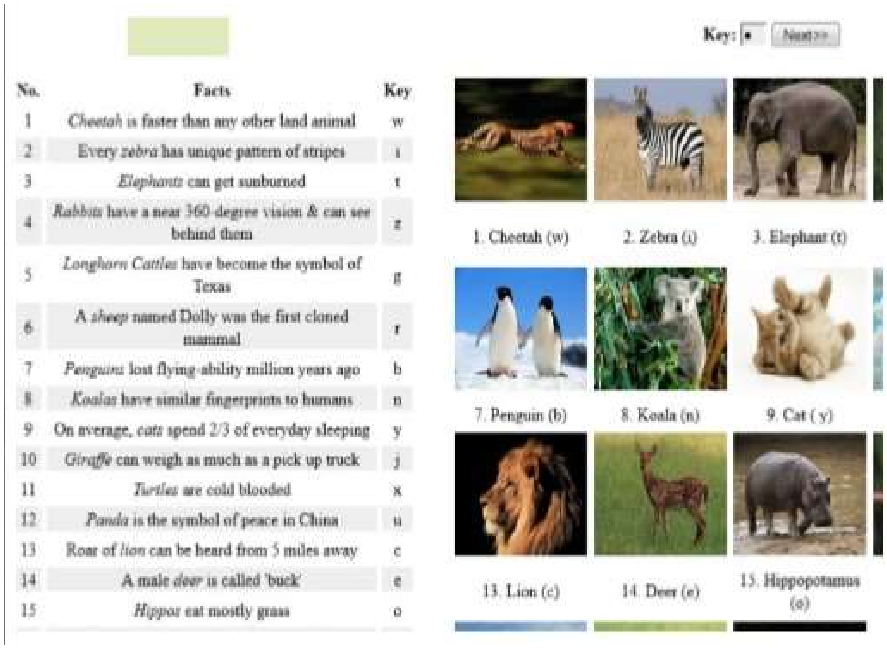
In the ColorLogin proposed by [10], users register icons from the given images during registration. Users selection would be based on background colors used to distinguish randomly displayed square icons. During the authentication procedure, users need to identify icons with registered color rather than all the icons displayed. Users would then click on the line where the pass-icon lies rather than the pass-icon itself. This will deny shoulder-surfing attackers from taking note of the icons that situate on that line especially when shoulder-surfers cannot remember the icons in a short time. According to the authors, this scheme can prevent shoulder-surfing. However, attackers can easily identify background color associated with a particular icon via multiple shoulder-surfer sessions. After that, attackers can shoulder-surf the icons that situate on the clicked line and login as a legitimate user.



(a) (b)

Figure 2: User interface of Gao et al (adopted from [10]). (a) Before Rotation (b) After Rotation

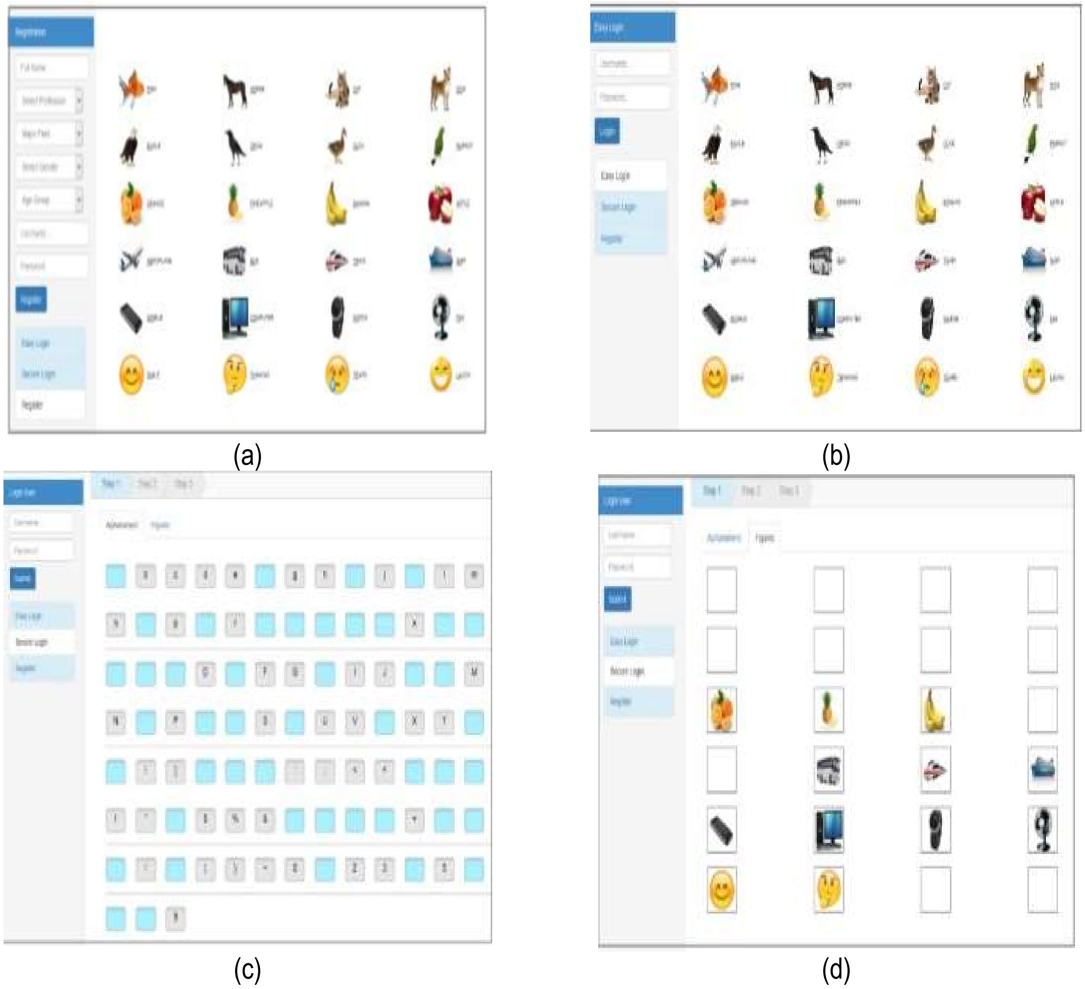
Al-Ameen et al. proposed cuedRecognition in 2015 [11]. During registration, a user needs to register a keyword and associate the keyword to a key. During the authentication procedure, the user needs to enter a key corresponding to the keyword using the keyboard rather than mouse. This key is associated with each keyword changes with every login to distract attackers. The author claimed that variant response property provides higher resilience to shoulder-surfing since it is difficult in practice to observe both keyboard and screen at the same time. Also, the key input is shown as an asterisk or dot (as with a regular password) to minimize the risk of shoulder-surfing attack. However, this system is vulnerable when the authentication process is video recorded because both screen and keystrokes can be captured at the same time. Thus, this system is vulnerable to video-recording shoulder-surfing attack.



No.	Facts	Key
1	*Cheetah* is faster than any other land animal	w
2	Every *zebra* has unique pattern of stripes	i
3	*Elephants* can get sunburned	t
4	*Rabbits* have a near 360-degree vision & can see behind them	z
5	*Longhorn Cattles* have become the symbol of Texas	g
6	A *sheep* named Dolly was the first cloned mammal	r
7	*Penguins* lost flying-ability million years ago	b
8	*Koalas* have similar fingerprints to humans	n
9	On average, *cats* spend 2/3 of everyday sleeping	y
10	*Giraffe* can weigh as much as a pick up truck	j
11	*Turtles* are cold blooded	x
12	*Panda* is the symbol of peace in China	u
13	Roar of *lion* can be heard from 5 miles away	c
14	A male *deer* is called 'buck'	e
15	*Hippos* eat mostly grass	o

Figure 3: User interface of Al-Ameen et al's system (adopted from [11])

Nizamani et al. proposed an authentication method in 2018 [7]. During the registration procedure, a user is required to register four images from the twenty four images displayed on the 6x4 grid. After that, the user is required to register alphanumeric password using key. The user is also required to register pass-image using "Control" + "Alt" + "<any_letter_for_the_image>". During authentication, the user is required to login in either of the two ways – "easy login" or "secure login". As for the "easy login", the user is required to use the key to enter alphanumeric password and shortcut key for the image. For the secure login, a user is required to click on the "Step" button. The system generates password which the user needs to compare with the registered one and click the correct one. According to the authors, this scheme can prevent shoulder-surfing. However, if attackers know the underlying algorithm, they can easily trace the clicked number and obtained the information about the registered password via multiple shoulder-surfer sessions

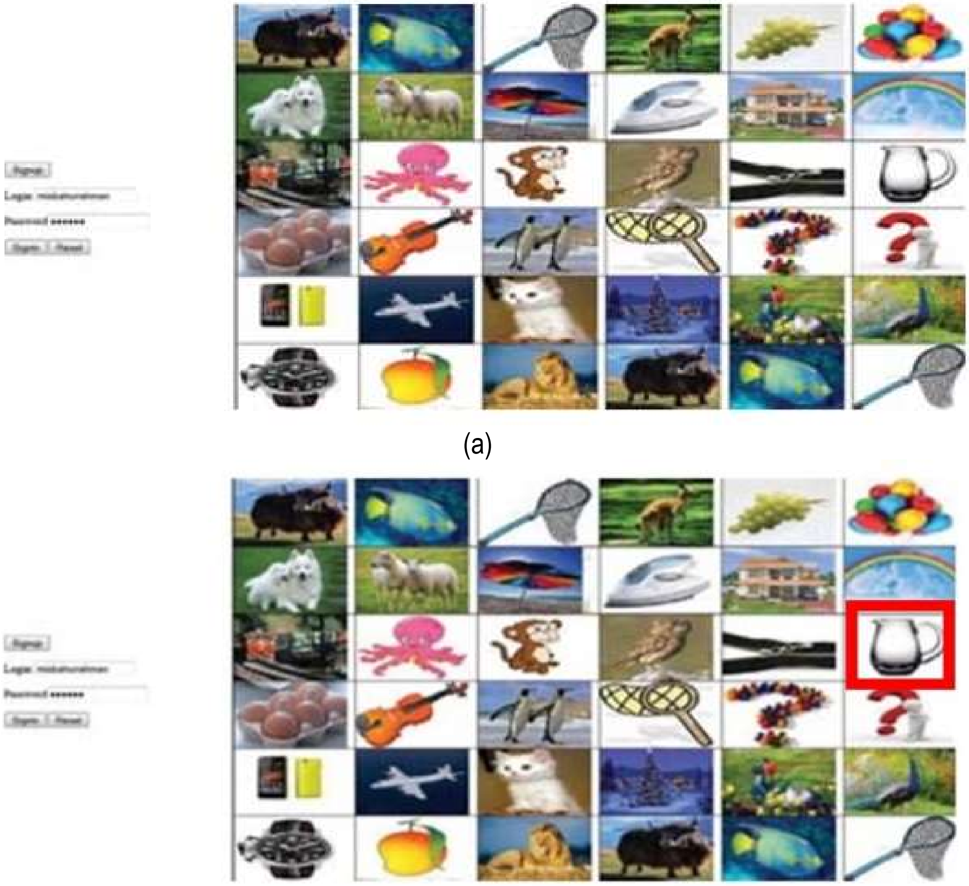


(a) (b)

(c) (d)

Figure 4: User interface of Nizamani et al's system (adopted from [7]).
(a) Registration (b) Easy Login (c) Alphanumeric Secure Login (d) Image Secure Login

Siddiqui et al. proposed a graphical authentication scheme in 2018 (Siddiqui et al., 2018). During registration, a user is required to register several images within 6x6 grid (see Figure 5(a)). The user is required to remember the name of the registered images. Each image represents the first character of its name. During the authentication procedure, a challenge set consists of 6x6 grid is shown. To login, the user needs to identify and click on the correct pass-image based on the first character of the names of the images shown in the challenge set. The image that has first character similar to the first character of the registered image is the pass-image. The user is required to repeat this for all the registered images. According to the author, this method can prevent shoulder-surfing attack since the challenge set will always be filled with a new random set of images. However, this method has a weakness whereby attackers can easily use the name of the clicked image to determine the first character of the registered image. For example, if the name of the clicked image is “cup” as highlighted in red (see Figure 5(b)), an attacker that knows the underlying algorithm, can easily identify the first alphabet of the registered image to be “c” and use the obtained information to login as legitimate users.



(a)

(b)

Figure 5. User interface of Siddiqui et al’s system (adopted from Siddiqui et al, 2018).
(a) Registration; (b) Authentication

The following section discusses the problem statement of this research work.

3. Problem Statement

Over the years, many systems have been proposed to prevent shoulder-surfing attacks. Though some of these systems can prevent attackers from obtaining the correct pass-images via direct observation, however, they can be easily shoulder-surfed using multiple and video-recording shoulder-surfing attack. This challenge has established a research gap that require further study. Therefore, this research is being conducted to propose a method that can resist the activities of shoulder-surfing attackers.

4. Scope of the Research

This research mainly focuses on resisting shoulder-surfing attacks. In the light of this, the research has proposed a recognition-based method capable of preventing shoulder-surfing attacks. The research only considered shoulder-surfing attacks via direct observation, multiple observations and video-recorded way.

5. Research Questions

It is imperative to ask these research questions while finding solution to the identified gap

i. What method can be proposed to prevent shoulder-surfing attacks?
ii. How can the proposed method be developed and implemented?
iii. How can the proposed method be evaluated in terms of preventing shoulder-surfing attacks?

6. Proposed System

Figure 6 depicts the proposed system

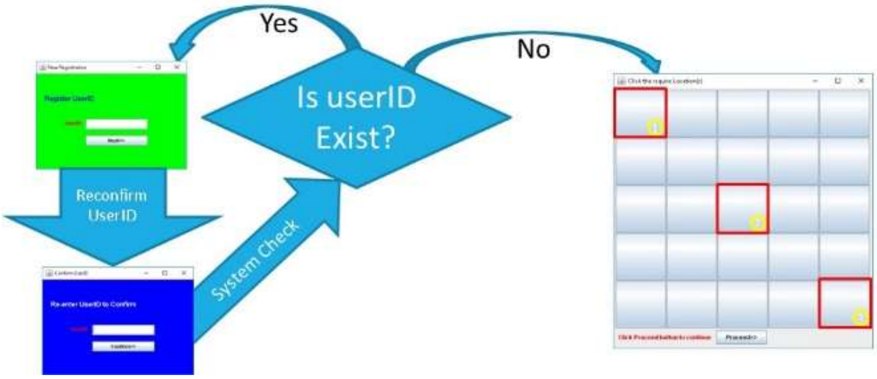


Figure 6: Proposed System

The proposed system is divided into registration process and authentication process

6.1 Registration Process

During the registration process, a user is required to register userID and password. The essence is to give the user unique identification. After that, the user is required to register three locations from the given grid. The user is required to note the sequence of registration of these locations. The user is required to confirm the registered locations. The registration is saved into the database after clicking the confirm button.

6.2 Authentication Process

During the authentication process, the user is required to enter correct userID and password. If a wrong userID is supplied an error message is displayed, otherwise a challenge set that consists of 5x5 grid is displayed. The user is expected to identify the images displayed on registered locations within the 5x5 grid. These images will be used to obtain the pass-image to login after applying the proposed algorithm.

7. EVALUATION

Participants would be invited to evaluate the feasibility of the proposed method in preventing shoulder-surfing attacks. The participants would be given tutorial to gain knowledge of the workability of proposed system. After that, the participants would be given unlimited trials to perform the shoulder-surfing attack.

8. CONCLUSION

The study began by analyzing the existing methods for preventing shoulder-surfing attacks. To achieve this, different search engines (such as Web-of-science, Springer, Science Direct, IEEE etc.) were used to obtain relevant journal and conference papers. The outcome of the review indicated that the challenge of shoulder-surfing attacks has not been conquered. Hence, it is imperative to explore more methods to prevent shoulder-surfing attacks. This research when completed will contribute significantly to the mechanisms available for preventing shoulder-surfing attacks especially via multiple and video-recording ways.

REFERENCES

[1] Adebimpe, L.A. (2011). Problems and Prospects of Utilizing ICT Tools in Science Education. Journal of Computing, Information Systems, Development Informatics & Allied Research, 2(2), 1-8.

[2] Abbasi, K., Zin, A.M., & Mokhtar, M. (2016). Graphical Passwords: Requisite for Secure Information Systems. Advanced Science Letters, 22(10), 2809-2813.

[3] Sun, H.M., Chen, S.T., Yeh, J.H., & Cheng, C.Y. (2018). A shoulder surfing resistant graphical authentication system. IEEE Transactions on Dependable and Secure Computing. 15(2), 180-193.

[4] Por, L.Y., Ku, C.S., Islam, A., & Ang, T.F. (2017). Graphical password: prevent shoulder-surfing attack using digraph substitution rules. Frontiers of Computer Science. 11(6), 1098-1108.

[5] Dhamija, R., & Perrig, A. (2000, August). Deja Vu-A User Study: Using Images for Authentication. In USENIX Security Symposium. 9, 1-14.

[6] Biddle, R., Chiasson, S., & Van Oorschot, P.C. (2012). Graphical passwords: Learning from the first twelve years. ACM Computing Surveys (CSUR). 44(4), 1-41.

[7] Nizamani, Shah Zaman, Waqas Ali Sahito, and Shafique Awan. (2018). "Divide and Conquer Approach for Solving Security and Usability Conflict in User Authentication. International Journal of Advanced Computer Science and Applications 9(5) 489-495.

[8] Passfaces: Two Factor Authentication for the Enterprise. (2019, January 4). Retrieved from http://www.realuser.com/

[9] Davis, D., Monrose, F., & Reiter, M.K. (2004, August). On User Choice in Graphical Password Schemes. In USENIX Security Symposium. 13, 11-11.

[10] Gao, H., Liu, X., Wang, S., Liu, H., & Dai, R. (2009, December). Design and analysis of a graphical password scheme. In Innovative Computing, Information and Control (ICICIC), 2009 Fourth International Conference on (pp. 675-678). IEEE.

[11] Al-Ameen, M.N., Wright, M., & Scielzo, S. (2015, April). Towards Making Random Passwords Memorable: Leveraging Users' Cognitive Ability Through Multiple Cues. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. 2315-2324.

[12] Anwar, M., & Imran, A. (2015). A Comparative Study of Graphical and Alphanumeric Passwords for Mobile Device Authentication. In MAICS. 13-18.

[13] Siddiqui, M. U., Umar, M. S., & Siddiqui, M. (2018, December). A Novel Shoulder-Surfing Resistant Graphical Authentication Scheme. In 2018 4th International Conference on Computing Communication and Automation (ICCCA) (pp. 1-5). IEEE..