International Journal of Information & Network Security (IJINS)
Vol.1, No.3, August 2012, pp. 163~170
ISSN: 2089-3299

Novel Shoulder-Surfing Resistant Authentication Schemes using Text-Graphical Passwords

M.Kameswara Rao*, Sushma Yalamanchili **
* Department of Computer Science, P.G.Centre, P.B.Siddhartha College of Arts& Science.
** Department of CSE, NRI Institute of Technology, Agiripalli.

Article Info

Article history:

Received Jun 06th, 2012
Revised July 07th, 2012
Accepted July 22th, 2012

Keyword:

Authentication
Text-graphical-Passwords
Shoulder- surfing
Spyware attacks
Usability

ABSTRACT

There are many applications which require the user to be authenticated before being permitted to perform certain tasks. Text password-based authentication is a popularly used authentication mechanism. Despite having greater security, text-passwords are characterized by selection of a weak and easy to remember passwords. Users also tend to write them down and share them with friends, family members and colleagues defeating the security provided by text-passwords. Graphical passwords offer an alternative to text passwords as the password space is typically higher, less prone to dictionary attacks and easier to remember visually. However, they suffer from shoulder-surfing attacks. In this paper, we propose two authentication schemes that support keyboard as well as graphical mouse-based input that map password characters to other regions of the password space. This shields the user's password from being known to the adversary thus deflecting shoulder-surfing and spyware attacks. The schemes include both single and multi color input images consisting of printable characters. An analysis of security, usability, memorability and social engineering aspects of the proposed schemes is presented. Future research directions are also presented.

Corresponding Author:

First Author,
Department of Computer Science, P.G.Centre,
P.B.Siddhartha College of Arts& Science, India
Email: kamesh.manchiraju@gmail.com

1. INTRODUCTION

Authentication determines whether a user should be allowed access to a particular system or resource. Conventional passwords are used widely for authentication, but they are known to have security, memorability and social engineering problems. Drawbacks of conventional passwords include password theft, forgetting passwords and choice of weak passwords. Researchers have designed advanced password-based authentication systems relying on graphical passwords which have improved password space and can be better remembered by humans as psychological studies have shown that people can remember pictures better than text [1] and suggest that humans are better at recognizing visual information than recalling meaningless text-based strings.

Graphical password-based authentication schemes are commonly vulnerable to shoulder-surfing attacks wherein an adversary observes the password being input by the user. Graphical password schemes are also vulnerable to spyware attacks which monitor keyboard input or mouse clicks. These attacks can be avoided by mapping the characters in a password to other regions in the password space based on a set of rules. Inputting characters or clicking with mouse in the mapped password regions is the equivalent of the pass-characters being input and results in the user getting authenticated without revealing the actual characters in the password string.

2. RELATED WORK

Studies of graphical password schemes have been taken up and are presented in [2, 3, 4, 5, 6, 7]. Recognition-based graphical password schemes are those where a user is presented with a set of images and the user gets authenticated by recognizing and identifying the images that were selected during registration. R.Dhamija et al. [8] proposed a graphical authentication scheme in which the user needs to identify a sequence of images from among a set of random pictures. Jansen et al. [9] proposed a graphical password mechanism for mobile devices where image thumbnails need to be selected in sequence that match the graphical password images related to a theme.

Takada and Koike [10] discuss a scheme for mobile devices where at every round the user either selects a pass-image among several decoy-images or chooses nothing if no pass-image is present. In Passface scheme [11] the user needs to identify four human faces from among decoy faces. In recall-based techniques, a user is asked to reproduce something that was selected earlier during the registration. Reproduce-a-drawing and Repeat-a-selection are the basic types of recall-based password techniques. Reproduce-a-drawing authentication methods include Draw-a-secret (DAS) scheme proposed by Jermyn et al. [2], Passdoodle scheme proposed by Goldberg et al. [12] and signature drawing scheme proposed by Syukri [13]. In Repeat-a-Sequence authentication algorithms, a user is asked to repeat sequences of actions performed by the user during password registration. Methods under this category include Blonder method [14], Passpoint method [15] and Passlogix method [16].

Several shoulder-surfing resistant schemes have been proposed in literature [17]. Man et al. [18] proposed a scheme where the user gets authenticated by inputting unique codes corresponding to the chosen pass-objects from amongst a set which includes decoy-objects. Wiedenbeck and Birget [19] developed a shoulder-surfing resistant graphical password technique in which the system will display a number of graphical icons. To be authenticated, a user needs to recognize the chosen icons and click inside the convex hull formed by them. Malek et al propose a personal entropy-based system that relies on binary pressure when a user draws a secret [20] while Kumar et al propose a scheme that uses the orientation of the human pupil for selection of password, personal identification number [21] making both schemes resistant to shoulder surfing. Zhao and Li [22] proposed S3PAS that is a scalable shoulder-surfing resistant password authentication scheme (PAS). Forget et al propose a cued-recall eye gaze authentication system that facilitates memorizing of multiple distinct passwords. In the scheme proposed by Gao [24], users draw a curve along their images in order with some variations such as degraded images and starting and ending with randomly designated images which is shoulder-surfing resistant.

3. PROPOSED WORK

We put forth two authentication schemes using graphical passwords and discuss key aspects of authentication for each of these schemes. The proposed schemes are PairPassChar (PPC) and TricolorPairPassChar (TPPC). Each of these schemes supports two modes of input, namely, keyboard entry and mouse clicks. We refer to the former mode as the text mode and the latter as the graphical mode. The input image consists of a 10x10 grid of cells each of which represent the characters A-Z, a-z, 0-9 and other printable characters which are padded with spaces in a single color and randomly spaced on the grid. In this paper, we refer to this as the basic character set and is used in the PPC scheme. The same character set in three colors randomly spaced and padded with spaces in a 17x17 grid is the color character set and is used as the input image in the TPPC scheme.

The pass-characters in the password string are mapped to other portions of the password space and therefore avoid shoulder surfing and spyware attacks. The password is changed after a specified number of logins or failed attempts. This feature is a deterrent to brute force attack. In following discussion, we refer to the characters in the password string as the pass-characters and a pair of pass characters under consideration as a pass-character pair. Let n represent the length of the password and $p_1p_2 \ldots p_n$ represent the password. In both schemes, we process one pass-character pair at a time sliding to the right one character at a time and wrapping around until the last pass-character forms the first character in the pass-character pair. To login, users have to give input by entering in a character or by clicking on a character for each of the pass-character pairs $\{p_1,p_2\}$, $\{p_2,p_3\}$,… $\{p_{n-1},p_n\}$, $\{p_n, p_1\}$ pairs in the login image.

3.1. PairPasswordChar (PPC) scheme

In this scheme, the image consists of the basic 10x10 character set. We propose the rules that govern the allowable input corresponding to each pass-character pair. At the end of the statement of rules, we demonstrate how a user may offer input corresponding to a specific password.

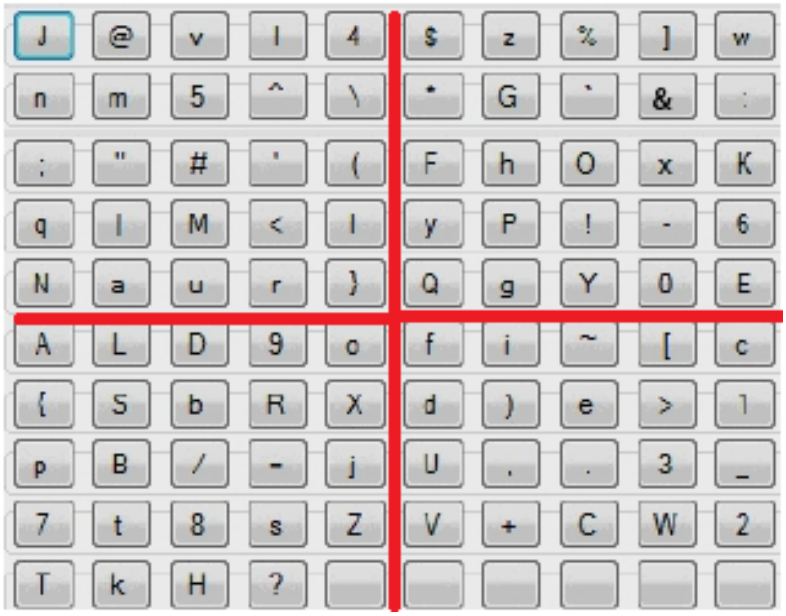

Figure 1. Basic 94-character set

Rule 1 : If both pass-characters in the current pass-character pair form a vertical line, the rectangle formed by the pass-characters and their corresponding mirror characters with respect to Y axis is identified. In graphical mode, the user can click anywhere within a rectangle for a successful click. In text mode, typing in any of the characters that lies on the border of the rectangle is considered to be successful.
Example: If the pair is 'a', 't' then the rectangle is 'a', '0', 'W', 't'. For the graphical mode, clicking anywhere in the rectangle is a successful click. In the text mode, any of the characters successful click can be any of the cells 'a', 'u', 'r', '}', 'Q', 'g', 'Y', '0', '[', '>', '3', 'W', 'C', '+', 'V', 'Z', 's', '8', 't', 'B', 'S', 'L'.

Rule 2 : If both pass-characters in the current pass-character pair form a horizontal line then the rectangle formed by the pass-characters and their corresponding mirror characters with respect to X axis is identified. In graphical mode, clicking anywhere in the rectangle is a successful click. In text mode, typing in any character that corresponds to the cells that form the border of the rectangle is successful.
Example: If the pair is 'u', 'g' then the rectangle is 'u', 'g', 'i', 'D'. In graphical mode, clicking anywhere in the rectangle is a successful click. In text mode, successful click can be any of the cells 'a', 'u', 'r', '}', 'Q', 'g', 'i', 'f', 'o', '9', 'D'.

Rule 3 : If the pass-characters in the current pair appear on different rows and columns then the rectangle formed by pass-character pair and their corresponding diagonal rectangle vertices is identified. In the graphical mode, clicking anywhere in the rectangle is a successful click. In the text mode, typing in any character that lies on the cells that lie on the border of the rectangle is successful.
Example: If the pass characters in the current pair are 'M', 'd'. Rectangle will be formed with 'M', 'd' as diagonal rectangle vertices. Thus the rectangle is 'M', 'y', 'd', 'b'. For graphical mode, clicking anywhere in this rectangle is a successful click. For text mode, typing in any of the characters from the outline cells ie. 'M', '<', '|', 'y', 'Q', 'f', 'd', 'X', 'H', 'b' is considered to be successful.

Rule 4: If the two pass-characters in the current pass-character pair are the same, the rectangle formed by the pass-character with its mirror character in the diagonal quadrant as diagonal rectangular vertex is identified. For graphical mode, clicking anywhere in the rectangle is a successful click. In text mode, typing in any of the characters on the outline cells of the rectangular border is considered to be successful.
Example: If pass characters are the same ie. pair is '>','>'. Thus '>' forms one vertex of the rectangle while its mirror character in the diagonal quadrant, namely, '|' forms the diagonal rectangular vertex. Thus the rectangle is '>', 'S', '|', '-'. In the graphical mode, successful click is anywhere in the rectangle is a successful click. In the text mode, typing in any of the characters that lie on the border of the rectangle, namely, '>', 'e', '}','d', 'X', 'R', 'b', 'S', 'L', 'a', '|', 'M', 'l', 'y', '{', '-', '0', '['.

Illustration : To illustrate the login process, let us follow an example where the user's password is "L9sL". The four pass-character pairs for this password are "L9", "9s", "sL" and "LL". The login procedure consists of the following four steps and is also shown below.

1)The user's first pass-character pair is 'L','9' and then identifies the rectangle formed by 'L' ,'9' as rectangular vertices and their mirror characters with respect to X –axis, namely, 'a' ,'r' as the other rectangular vertices. Thus in graphical mode, the user can click on any of the cells that are part of the rectangle. In text mode, the border of the rectangle namely, 'L','9','r','a' can be entered.. Figure 2 represents the rectangle for this pair of pass-characters.

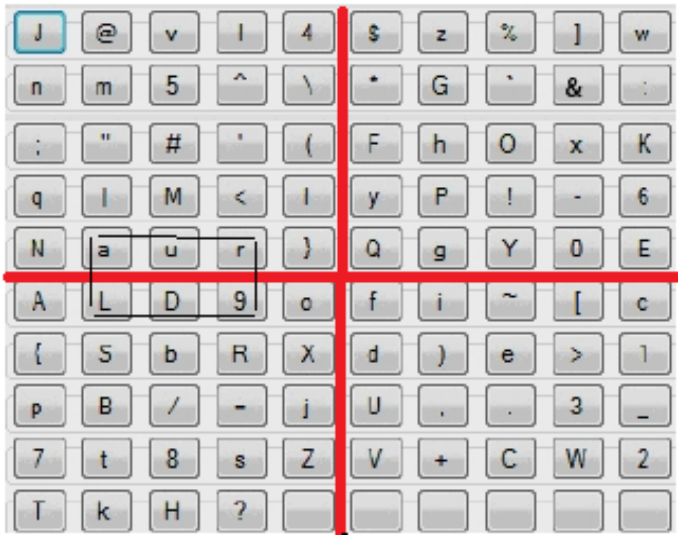

Figure 2 Pass-characters form horizontal line

2) The user's second pass-character pair is '9','s' and identifies the rectangle formed by vertices '9','s' and their mirror characters wth respect to Y-axis, namely, 'i','+' as the other rectangle vertices. The user can click anywhere within that rectangle or type in any of the characters '9', 'o', 'f', 'I', ')', ',', '+', 'V', 'Z', 's', '-', 'R'. Figure 3 highlights the cells that represent the clickable area for this pair of pass-characters.

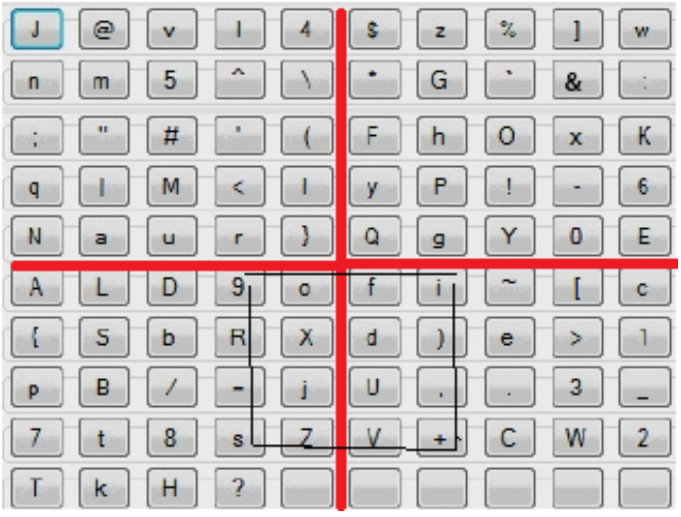

Figure 3 Pass characters form vertical line

3) The third pass-character pair is 's','L' and then clicks on any of the cells in the rectangle grid formed by 's' ,'L' and their diagonal rectangular vertices are 't' ,'9'. Thus the user can click anywhere in the indicated rectangle in Figure 4. The user can also type in any of the characters 'L', 'D', '9', 'R','-', 's', '8', 't', 'B' and 'S'.

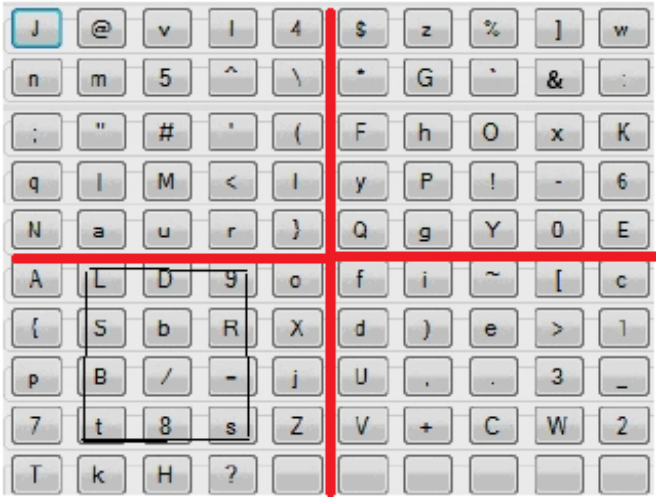

Figure 4 Pass characters form diagonal rectangular vertices

4) The user's fourth pass-character pair is 'L','L''. The rectangle is formed by the diagonal vertices 'L' and its mirror character in the diagonal quadrant '0'. The user can click anywhere in the rectangle 'L', 'a', '0', '[' as indicated in Figure 5. The user could also type in any of the characters 'a', 'u', 'r', '}', 'Q', 'g', 'Y', '0', '[', '~', 'I', 'f', 'o', '9', D', 'L' in text mode.

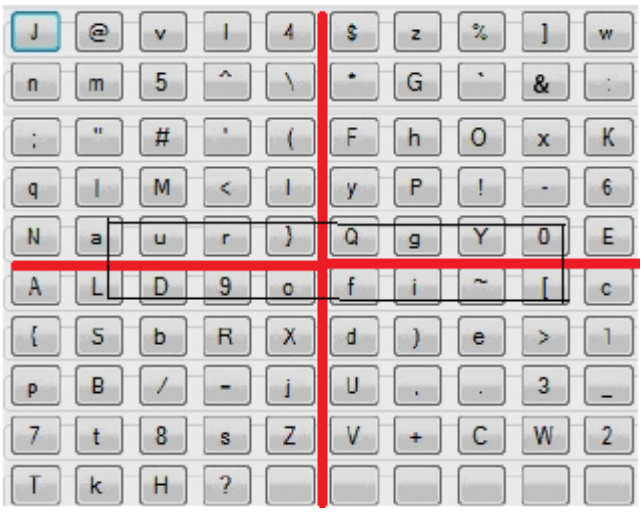

Figure 5 Same character Pass-character pair

3.2. TricolourPairPasswordChar(TPPC) scheme

TPPC scheme use the tricolour version of the basic character set where each character appears in three colors: red, green and blue randomly spaced in a 17x17 grid. As in the PPC scheme, the pass-characters are examined one pair at a time, starting with the first pass-character and shifting to the right until the last pass-character in the password becomes the first pass- character in a pass-character pair. Each pass-character pair is first converted into the mapped character pair and the rules of the PPC scheme and the special case rules of TPPC are applied to which results in the rectangle.

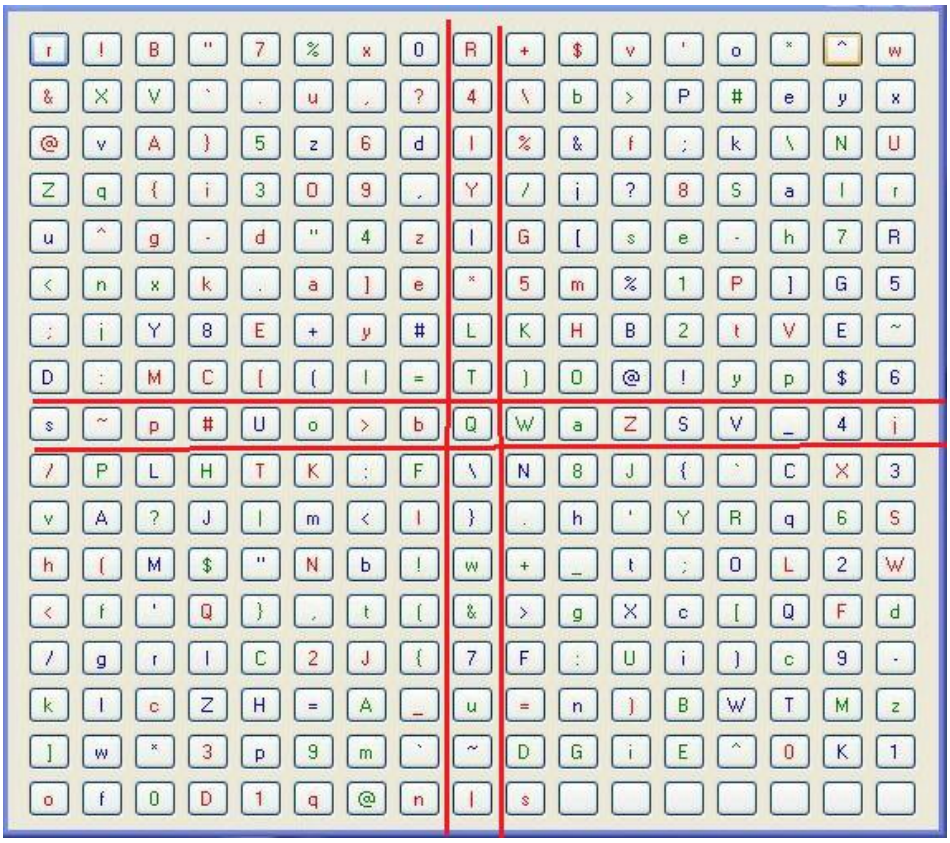

Figure 6 Tricolor character set

Rule:
The first pass-character in the pair is replaced with the same character in one of the other two possible colours. The second pass-character in the pair is unchanged. This results in two possible pairs that the user can select from. The rules of the original PPC scheme are applied to the mapped pair applying the special case rules where applicable. The clickable areas and characters that can be typed in are derived.

Special Cases:
Case 1: When the characters in the mapped pair form a vertical line on the 9th column, any of the characters including and in between the mapped characters can be clicked upon or typed in.
Case 2: When the mapped characters form a horizontal line on the 9th row, any of the characters including and in between the mapped characters can be clicked upon or typed in.
Case 3: When one of the characters in the mapped pair are diagonal vertices of a rectangle then Rule 3 of PPC scheme is applied.
Case 4 : When both pass–characters are same and lie at the center of the grid, any of the characters that lie on the cells that border the grid can be clicked or typed in.
Case 5: When both pass-characters are the same and lie on the 9th row/column then the mirror character with respect to Y axis / X axis is determined and the any of the characters that lie on or in between these two characters can be clicked on or typed in.

Illustration: Let us consider a scenario where Alice's password is $5_gR_r1_g<r$. We process the pass-characters pairwise as described below.

1) For the first pass-character pair 5_gR_r we replace '5' in green with '5' in red or blue and leave R_r unchanged. In other words, the user can select either of 5_rR_r or 5_bR_r. The user can then input in either text or graphical mode by applying the rules of the PPC scheme and special cases of TPPC scheme to the selected pair.

2) The second pair is R_r1_g and in this case the user can choose either R_g1_r or R_b1_r and input either text or graphical mode by applying the rules of PPC and special cases of TPPC scheme to the selected pair.

3) Next the pair 1_g<r is considered and Alice can choose one among the two possible pairs of 1_r<$_r$ and 1_b<$_r$ as the selected pair. The PPC rules and special cases of TPPC are applied to the selected pair.

4) The pair <$_r5_g$ is processed and Alice can choose between <$_g5_g$ and <$_b5_g$. The rules of PPC and the special cases of TPPC are applied to the selected pair.

4. ANALYSIS OF PROPOSED SCHEMES

An experiment was conducted involving 20 Computer Science graduate students to study memorability, usability and login times for PPC and TPPC schemes. It was found that the average login times for the PPC scheme consisting of 4 character passwords, 5 character passwords and 6 character passwords were 28.4, 39.6 and 47.3 respectively. The average login times for the TPPC scheme for the same lengths of passwords were 30.4, 44.1 and 54.3 respectively. This clearly demonstrates that the average login times increase as the password length increases in both schemes. Further, the login times for the TPPC scheme are higher than the PPC scheme for the same password length. It was also found that 64% of the participants in the study found the rules for the TPPC scheme to be difficult to apply than the PPC scheme. Memorability of the passwords in TPPC scheme decreased with increase in password length. Observers of the password being input could not guess the text-graphical password in each case.

The traditional text-based password scheme and the proposed PPC and TPPC schemes are analyzed with respect to security, usability, memorability and social engineering aspects and a summary is presented in Table 1.

Table 1. Comparison of authentication schemes.

Scheme	Usability	Memorability	Security
Traditional Textbased	User familiarity with the interface.	Hard to remember multiple and strong passwords.	Reduced security due to weak passwords and password sharing. Prone to Dictionary, Brute force, Shoulder surfing, and Spyware attacks. Password space 94^n (n=Password length).
PPC	User familiarity with text interface. User training required for graphical interface. Longer login time than above scheme	Advantages of graphical passwords	Resistant to Shoulder surfing and Spyware attacks. Brute force and Random click attacks are avoided due to login screen reset. Password space 94^n .
TPPC	User familiarity with text interface. User training required for graphical interface. Longer training and login times than above two schemes	Users have to remember coloured password combinations. Rules more complex than above schemes.	Resistant to Shoulder surfing and Spyware attacks. Brute force and Random click attacks are difficult due to increased password space and login screen reset. Password space 282^n .

5. CONCLUSIONS

In the present work, we have proposed two text-graphical authentication schemes that are shoulder-surfing and spyware resistant as the pass-characters are mapped into password regions that do not indicate a relation between the pass-characters and the input characters. The password space provided by the PPC scheme is as much as that offered by conventional password systems while it is greatly enhanced in the TPPC scheme due to the use of the same 96-character set in three colours. In the two schemes, when the number of login attempts exceeds a certain threshold, say 3, the login screen is reset and no indication is given to the user if some of the characters are correctly input thereby deterring Brute force and Random click attacks. Brute force attack in TPPC scheme is significantly more difficult due to the increased password space. Based on the experimental work, it can be concluded that the TPPC scheme rules are complex and therefore harder to remember than the PPC scheme even though Brute force attack was more difficult in TPPC scheme due to the increased password space. The login times were longer for the TPPC scheme. TPPC scheme is more secure than the traditional textual password scheme and the PPC scheme which use only 96 character set. Observers could not determine any relationship between the password being input and the actual password

therefore it can be concluded that shoulder-surfing and spyware attacks are deflected in both schemes. The password space may be increased further by using more than three colour character sets based upon user choice. The larger grid in multi-color pairwise schemes would require scrolling on mobile phones and personal digital assistants. The extension of the proposed schemes to hand-held mobile devices can be explored as future work. Automated guided training and password validation of the schemes can be taken up. The above PPC scheme can be modified to represent the same character rotated by 90, 180 and 270 degrees respectively in place of the original orientation of the character as future work.

REFERENCES

[1] E. Shephard, "Recognition memory for words,sentences, and pictures", *Journal of Verbal Learning and Verbal Behavior*, 6, pp. 156–163, 1967.

[2] A. Jermyn, et al., "The design and analysis of graphical passwords", *Proceedings of the 8th USENIX Security Symposium*, August, Washington, D.C., USA, 1999.

[3] X. Suo, et al., "Graphical passwords: A survey.", *Proceedings of 21st Annual Computer Security Applications Conference*., pp. 463–472, 2005.

[4] S. Chiasson, et al., "Graphical Password Authentication Using Cued Click Points", *ESORICS*, 24-27 September, Dresden,Germany, pp. 59–374, 2007.

[5] M. D. Hafiz, et al., "Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique", *Proceedings of second Asia International Conference on Modelling & Simulation, IEEE Computer Society*, pp. 396–403, 2009.

[6] A. H. Lashkari, "A Survey On Usability And Security Features In Graphical User Authentication Algorithms", *IJCSNS International Journal of Computer Science and Network Security*, 9, Korea,pp. 195–204, 2009.

[7] R. Biddle, et al., "Graphical Passwords: Learning from the First Twelve Years", *ACM Computing Survey*, issue 44(4), 2011.

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

[9] W. Jansen, "Authenticating Mobile Device Users Through Image Selection", *Data Security*, 2004.

[10] T. Takada and H. Koike, "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images", *Human-Computer Interaction with Mobile Devices and Services*, 2795, Springer-Verlag GmbH, pp. 347–351, 2003.

[11] Passfaces Corporation, "The science behind Passfaces", White paper, Available at http://www.passfaces.com/enterprise/resources/whitepapers.htm, July 2009.

[12] J. Goldberg, "Doodling Our Way to Better Authentication", *Proceedings of Human Factors in Computing Systems (CHI)*, Minneapolis, Minnesota, USA.

[13] A. F. Syukri, et al., "A User Identification System Using Signature Written With Mouse", *Third Australasian Conference on Information Security and Privacy (ACISP)*, Springer-Verlag Lecture Notes in Computer Science, pp. 403–441, 1998

[14] http://www.baychi.org/calendar/files/ISO-Standards-for-Usability/ISO-Standards-for-Usability.pdf.

[15] S. Wiedenbeck, et al.,"PassPoints: Design and longitudinal evaluation of a graphical password system", *International Journal of Human-Computer Studies*, 63, pp. 102–127, 2006.

[16] M. Boroditsky. Passlogix password schemes. http://www.passlogix.com.

[17] AH Lashkari, et al., "Shoulder Surfing attack in graphical password authentication", *International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 6, No. 2, 2009

[18] S. Man, et al,, "A shoulder-surfing resistant graphical password scheme – WIW", *Proceedings of International Conference on Security and Management*, Las Vegas, pp. 105–111, 2003.

[19] S. Wiedenbeck, et al.,"Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme, *Proceedings of AVI*, pp. 177–184, Venezia, Italy, ACM Press, 2006.

[20] B. Malek et al., "Novel shoulder-surfing resistant haptic-based graphical password". *EuroHaptics '06*, 2006.

[21] M. Kumar, et al., "Reducing Shoulder-surfing by Using Gaze-based Password Entry", in Symposium On Usable Privacy and Security (SOUPS). 2007: Pittsburgh, PA, USA, 2007.

[22] H. Zhao and X. Li., "S3PAS:A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme", *AINAW '07 Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops*, vol. 2, pp. 467-472, 2007.

[23] A. Forget, et al., "Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords", Proceedings of CHI 2010, Atlanta, Georgia, USA, April 10 – 15, 2010.

[24] H. Gao, et al., "A New Graphical Password Scheme Resistant to Shoulder-Surfing", *International Conference on Cyberworlds. 2010, IEEE*: Singapore pp. 194 – 199, 2010.