International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Graphical Password Authentication Techniques: A Review

Aakansha Gokhale[1], Vijaya Waghmare[2]

[1] Sr. Lecturer, Dept. of Information Technology, Dr. .D. Y. Patil Polytechnic, Nerul, Navi Mumbai, Maharashtra, India

[2] Assistant Professor, Dept. of Computer Engineering, Saraswati College of Engineering, Kharghar, Navi Mumbai, Maharashtra, India

Abstract: ***In today's IT world, for the computer and information security the user authentication and authorization play a significant role. For this authentication a password is very important aspect. The conventional method of password is a strong textual password which is also called as alphanumeric password. But because of the problem of memorability, users writing them down on the pieces of papers or kept the password which can be easily memorable. Because of this it is vulnerable to various attacks like brute force, dictionary attack, social engineering, keylogger, spyware, guessing. So to overcome this limitation of textual password, a new password technique is developed which is a Graphical Password .In this as name indicates the images are used as a password. Also psychological study says that images can be easily remembered by human beings as compare to text. Generally password has two essential aspects: security and usability. In Graphical Password, the clicking and dragging activities are performed on the images rather than text. So it can be best alternative to the textual password. This paper will explore the strengths and limitations of various graphical password techniques on the basis of security and usability metrics.***

Keywords: Authentication, Graphical Password, Security, Usability.

1. Introduction

Today, authentication is the necessity to guarantee information security and the most convenient method is password authentication [1]. The traditional method is to use textual or alphanumeric password which consists of strings of alphabets, digits and special symbols. But there are several deficiencies in these alphanumeric passwords.

Due to the limitation of human memory most users tendency is to choose short and simple passwords which are easy to remember[2]. In this technique passwords are personal names of family members, birth-dates and dictionary words. Because of these simple passwords they are easy to guess.

Nowadays users require password for many accounts like personal computers, social networks, email, online transactions and more. So to remember easily sometimes users can use same password for all these accounts which reduces security [3, 4].

And also these passwords are vulnerable to guessing, dictionary attack, brute force attack, key-loggers, social engineering, shoulder-surfing, hidden-camera, spyware attack etc. In this way if textual passwords are kept difficult then they are difficult to remember and if they are kept easy then they are easy to guess.

So alternative to traditional method of textual password, a concept of graphical password is proposed. The main goal of graphical passwords is to use images or shapes to replace text, since people can remember pictures than words. This difference is the dual-coding theory [5], suggests that verbal and non-verbal memories are processed and represented differently in the mind. The way images are represented retains the perceptual features being observed and texts represented with symbols convey cognitive meaning. Thus it is easy for human being to remember faces of people, places they visit and things they have seen for a lengthy duration. In this way graphical passwords are easy to remember and difficult to guess.

The remaining paper is organized as follows: Background and Related work is presented in Section II .The Section III comprises the five recent graphical password schemes with detailed explanation and example. The analysis of these schemes has been done on the basis of security and usability metrics in Section IV. We conclude the paper with Section V.

2. Background and Related Work

Since last one decade lots of research work has been done on the concept of graphical password. The first graphical password technique was introduced by Blonder. The balance is maintained between the security and usability metrics and the attacks are resisted to the maximum.

Graphical Password techniques are categorized as follows:

2.1 Recognition-based Techniques

In this, for registration the user has to select the certain number of images from a set of random images as a password, and for authentication the user has to identify (recognize) those images sequentially.

Some examples of this are:

2.1.1 Dhamija and Perrig Technique [6]: In this, during registration the user has to pick the several pictures according to choice from a set of random pictures as a password and during authentication the user has to identify those same pictures in a sequential manner.

2.1.2 Passface Technique [7]: Here, human faces are used

as a password. This is based on an assumption that human can remember the human faces easily. A grid of nine human faces is used. In these nine faces one is known to the user and others are decoys. The user has to identify that known face among the nine faces. And this is continued until all the four faces are identified that are registered during the registration stage.

2.1.3 Sobrado and Birget Technique [8]: In this, during registration numerous icons (pass-objects) are displayed to the user and user has to select some icons. During authentication user has to identify those preselected icons and has to click inside the convex hull bounded by pass-objects.

2.2 Recall-Based Techniques

In these techniques, a user is asked to reproduce (recall) something that he/she created or selected earlier during the registration stage.

It has two categories:
- Pure Recall Based Techniques
- Cued Recall Based Techniques

2.2.1 Pure Recall Based Techniques: In this user is not provided a clue to recall a password.

Some examples are:

(a) Passdoodle Technique [9]: It is a handwritten design or text, usually drawn with stylus onto touch sensitive screen.

(b) Draw-A-Secret (DAS) Technique [10]: Here, user will draw a picture on 2D grid. The coordinates of a grid occupied by the picture are stored in the order of the drawing. During authentication, the user will be re-drawing the same picture. If the drawing touches the same sequence of coordinates on 2D grid, then the user is authenticated.

(c) Signature Technique [11]: Here, during registration user will record his/her signature as a password and authentication is conducted by having the user will re-drawing the same signature using mouse.

2.2.2 Cued Recall Based Techniques: In these techniques, user is provided a clue to recall a password registered earlier. Cued based provides more hints to user to memorize the passwords and hence easier than pure recall based techniques.

Some examples of these are:

(a) Blonder technique [12]: The graphical passwords were originally described by Blonder. In this, a user is presented with a predetermined image with predetermined areas (tap regions). To create a password user has to click those tap regions in a particular order. For authentication, user has to click the approximate areas of those tap regions in the predefined sequence.

(b) Pass-point technique [13]: To cover the limitation of Blonder technique this technique was proposed. Here a picture could be any natural picture or painting but at the same time should be rich enough in order to have many possible click points. The role of image here is also helping the user to remember the click points. Here no need of predefined click points like Blonder technique. The user can click on any place on the image to create a password. The tolerance around each chosen pixel is calculated. For authentication, user has to click within the tolerances of chosen click points in a correct order.

(c) Background DAS (BDAS) technique [14]: Here, the background image is added to original DAS as an improvement. So background image is a clue here. Password is a free form drawing that a user creates on a grid under laid with a background image of their choice. The background image is used to draw a password. People can be able to make their drawing passwords more complex and less predictable. For authentication user has to recreate a same drawing on the grid with background image.

3. Recent Graphical Password Techniques

There are various limitations of all those earlier graphical password authentication techniques like they are not resistant to shoulder surfing, brute force attack or guessing attack. So in this section the recent graphical password techniques have been studied which are resistant to all above attacks to some extent.

3.1 Pair-Based Authentication Technique

This technique [15] consists of 3 phases: registration, login and verification phase. In registration phase, the user has to enter a username and a password with minimum length 8. It is called as secret pass. It should contain even number of characters. The session password is based on this secret pass. During login phase, the user has to enter the correct username and after this a grid (login interface) is displayed. This grid is of 6 x 6 size and it contains alphabets and numbers randomly placed on the grid. Here user has to form the pairs of secret pass. Afterwards by using these secret pass pairs and interface the session password is generated.

The first letter in the secret pass pair is used to select the row and the second letter is used to select the column. The intersection letter is a part of the session password and this is repeated for all pairs of secret pass. Figure1 shows intersection letter ‘L’ for the pair “AN”. After this the server verifies the password to authenticate the user. If the password is correct, the user is an authorized user to enter into a system.

Here, at every login the interface changes and so session password changes accordingly. So resistant to brute force, shoulder surfing, guessing attack.

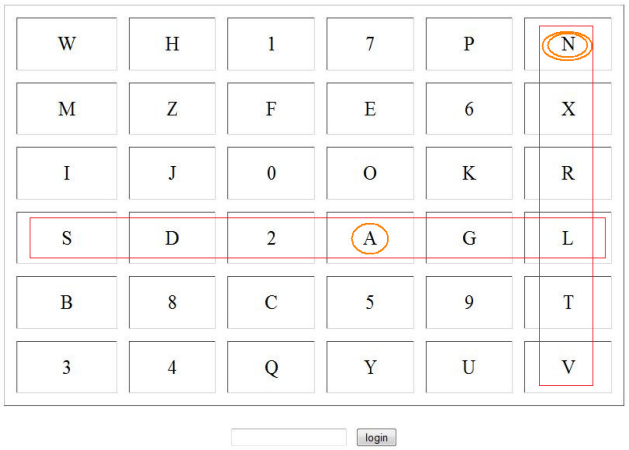

Figure 1: Login Phase

3.2 Hybrid Textual Authentication Technique

This also consists of registration, login and verification phases [15]. In registration phase, user has to first enter a username and afterwards has to rate colors from 1 to 8 randomly as shown in Figure2 and can remember it as "RLYOBGIP".

During login phase, after entering a correct username the login interface based on colors selected by users is displayed as shown in Figure3. It consists of color grid (strip of colors) and number grid of size 8×8. The color grid consists of 4 pairs of colors. Each color pair represents the row and column for the number grid. It means first color represents the row and second color represents the column of the number grid. In number grid the numbers from 1-8 are randomly placed on the grid. According to color pair, the number in the intersection of the row and column of the number grid is the part of session password.

For example, consider the color ratings in Figure2 and login interface in Figure3.The first color pair has red and yellow colors. The red color rating is 1 and yellow color rating is 3. So the first number in session password is the intersection of 1st row and 3rd column that is 3. The same method is repeated for all other color pairs. So here for login interface shown in Figure3 the password is "3573". Here also authentication server verifies the password entered by user and if it is correct then user is allowed to enter into the system.

In this, also at every login both the color grid and number grid varies and so session password changes for every session. So it is also resistant to brute force, shoulder surfing and guessing attack.

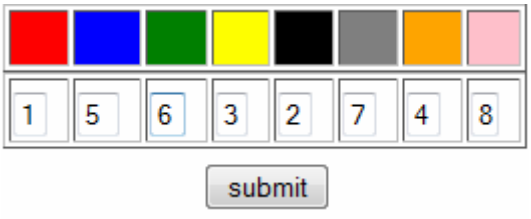

Figure 2: Color Ratings

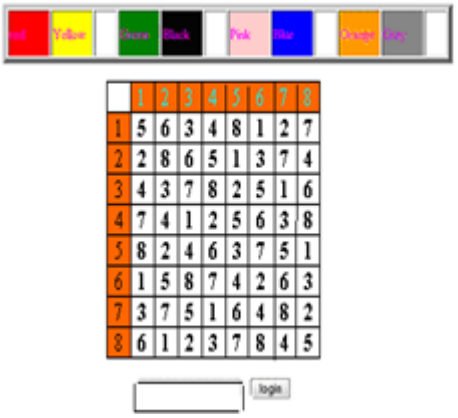

Figure 3: Login Interface

3.3 ImagePass Technique

It is recognition based graphical password technique [16].It has two phases, registration and login phase .During registration, user has to select a valid username and then he can select the particular number of images as a password from a set of 30 images as shown in Figure4. If user is not satisfied with a given set of images then he can click on "Load a new set of images" (Figure4). This is possible because ImagePass contains a large image database. Every image is a color image with size 90×90 pixels. The user can select x number of images in a particular sequence to set as a graphical password. The selected images are displayed on a selected password panel on top-right corner of image as shown in Figure4. The user can reset the selection of graphical password. Also if user wants to change or remove a particular image it can be done by clicking Remove image icon that appears in the top-right corner of Current Selection Panel as shown Figure5. After this user has to confirm the graphical password. The maximum number of images the graphical password contains is 12 because of the specificity of the system.

During authentication after entering a valid username, a grid of 4×3 is displayed as shown in Figure6. It is a combination of real and decoy images. Real images are the images selected by the user during registration and decoy images are the images randomly generated by the system during authentication. Total numbers of images are 12. It means if user selects 6 images during registration, then system randomly assigns 6 more decoy images. The image positions will change at every login. So for authentication user has to select the valid images in a correct sequence. If selection of images is done accurately in a sequence then user has a right to access the system. Here the authentication process is repeated for 5 unsuccessful attempts.

Because of the combination of real and decoy images and varying of the image positions this is also resistant to shoulder surfing, brute force, and guessing attack to some extent.

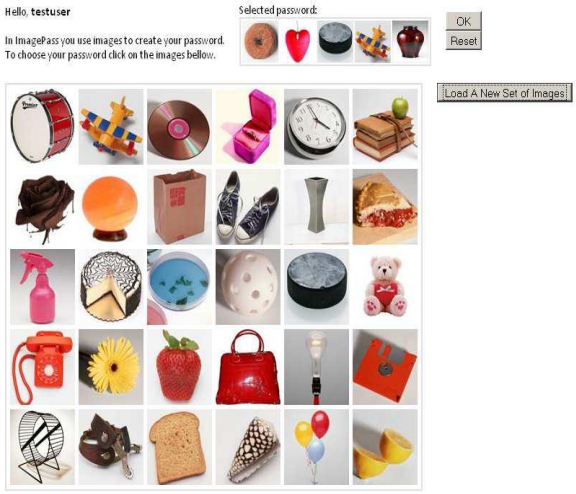

Figure 4: Graphical Password Selection

Figure 5: Current Selection Panel

Figure 6: Graphical Password Authentication

3.4 PairPassword Char (PPC) Technique

It has two modes of operation text mode and graphical mode [17]. In this, grid image consists of basic 94 characters set represents characters from (A-Z), a-z, 0-9 and other printable characters. All the characters are randomly spaced on cells of a grid of size 10×10 with single color as shown in Figure7. From the password string the pairs of pass characters are formed. If the size of the password is n then the pairs of password string are formed like $\{P_1, P_2\}$, $\{P_2, P_3\}$, ------ $\{P_{n-1}, P_n\}$, $\{P_n, P_1\}$. The pass-characters in the pair are mapped to the other portions of password space. Here processing is, starting from first character in a pair and going to the right one character at a time and wrapping around until last character forms the first character in the pass character pair.

Some rules are used here for how a user can offer input corresponding to a specific password:

Rule1: 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’,‘S’ then the rectangle is ‘a’, ‘0’, ‘>’, ‘S’. 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’, ‘[‘, ‘>’, ‘e’, ‘)’, ‘d’, ‘X’, ‘R’, ‘b’, ‘S’, ‘L’.

Rule2: 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 ‘r’, ‘Y’ then the rectangle is ‘r’, ‘Y’, ‘~’, ‘9’. In graphical mode, clicking anywhere in the rectangle is a successful click. In text mode, successful click can be any of the cells ‘r’, ‘}’, ‘Q ‘, ‘g’, ‘Y’, ‘~, ‘i’, ‘f’, ‘o’, ‘9’.

Rule3: 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 pair is ‘a’,‘R’. Rectangle will be formed with ‘a’,‘R’ as diagonal rectangle vertices. Thus the rectangle is ‘a’, ‘r’, ‘R’, ‘S’. 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 ‘a’, ‘u’, ‘r’, ‘9’, ‘R’, ‘b’, ‘S’, ‘L’.

Rule4: 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 i.e. pair is ‘A’, ‘A’. Thus ‘A’ forms one vertex of the rectangle while its mirror character in the diagonal quadrant, namely, E|’ forms the diagonal rectangular vertex. Thus the rectangle is ‘A’, ‘N’, ‘E’, ‘c’. In the graphical mode, successful click is anywhere in the rectangle is a successful. In the text mode, typing in any of the characters that lie on the border of the rectangle, namely, ‘A’, ‘N’, ‘a’, ‘u’, ‘r’, ‘}’, ‘Q’, ‘g’, ‘Y’, ‘0’, ‘E’, ‘c’, ‘[’,’~’, ‘i’, ‘f’, ‘o’ ‘9’, ‘D’, ‘L’.

In this technique, password is changed after a specified number of logins or failed attempts. So resistant to brute force and also pass-characters are mapped to password regions so strongly resistant to guessing, shoulder surfing and spyware attack.

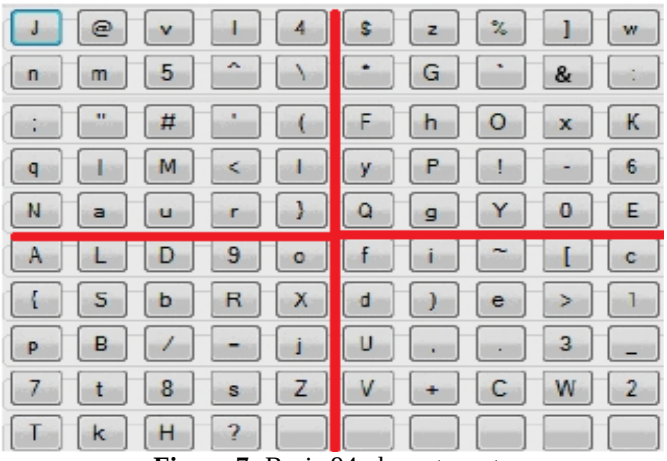

Figure 7: Basic 94-character set

3.5 TricolorPairPassword Char (TPPC) Technique

TPPC technique [17] uses the tricolor 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 as shown in Figure8.

Rules of TPPC technique:

The first pass-character in the pair is replaced with the same character in one of the other two possible colors. 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:

Case1: 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.

Case2: When mapped characters form horizontal line on the 9th row, any of the characters can be clicked upon or typed in.

Case3: When one of the characters in the mapped pair is diagonal vertices of a rectangle then Rule3 of PPC scheme is applied.

Case4: When both pass–characters are same and lie at the center of the grid, any of the characters that lay on the cells that border the grid can be clicked or typed in.

Case5: 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 the 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_g or R_b1_g 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 the user 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 the user can choose between $<_g5_g$ and $<_b5_g$. The rules of PPC and the special cases of TPPC are applied to the selected pair.

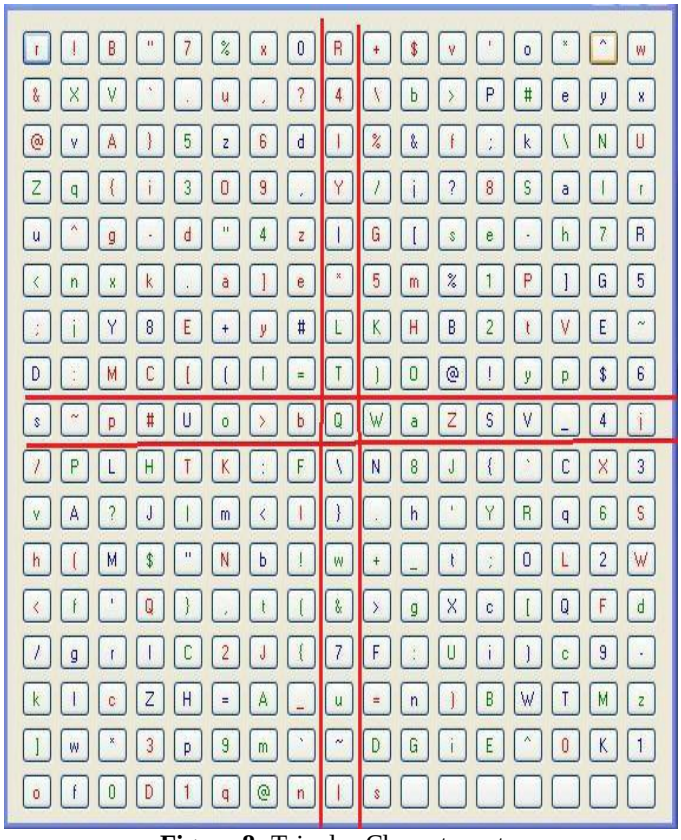

Figure 8: Tricolor Character set

4. Analysis On The Basis Of Security and Usability Metrics

4.1 Security analysis of the techniques

- Dictionary attack: In this attack, hacker uses the set of dictionary words and authenticate by trying one word after another.

But as all the techniques are graphical password authentication techniques, here instead of text, images are used as a password. Hence dictionary attack is not possible with any technique.

- Brute force attack: It means trying various possibilities to guess or crack a password. It depends upon password space of each scheme. Password space means number of possible values in a password. It can also be said as complexity of the password.

In Pair Based, a grid is of 6×6. Minimum length of password is 8. Hence password space is 36^8. It means complexity is large. So resistant to brute force attack.

In Hybrid Textual, it depends on colors and ratings. The complexity is 8! , if ratings are unique, else it is 8^8. Again here the complexity is large. Hence resistant to brute force attack.

In ImagePass, password space depends upon the number of images. The system assigns the temporary random numbers to images and when the password is entered correctly, these temporary numbers are erased. This effectively prevents brute force attack.

In PPC, it is 94^n and in TPPC it is 282^n. Here n is a password length. In both scheme complexity is large. So resistant to brute force attack.

- Shoulder surfing attack: It means watching over the shoulder of a person while entering a password.

In Pair Based, as the interface changes every time, the session password changes, so it is resistant to shoulder surfing.

In Hybrid Textual, the color ratings decide a session password. But with session password you can't find the color ratings. So resistant to shoulder surfing.

In ImagePass, during authentication as system uses decoy images with the real images and at every login attempt positions of all the images will change. So resistant to shoulder surfing to some extent.

In PPC and TPPC, the pass characters are mapped into password regions that do not indicate a relation between pass characters and input characters. So avoid shoulder surfing.

Also all the techniques are resistant to spyware, keylogger and social engineering attacks because of their graphics in nature.

4.2 Usability analysis of the techniques

- Memorability: It is a extent to which user can remember a password after a period of time.

In Pair Based, easy as compare to other techniques. User has to remember only secret pass.

In Hybrid Textual, difficult to remember color ratings.

In ImagePass, user has to remember the sequence of images.

In PPC, difficult to remember mapping rules.

In TPPC, rules are more complex than PPC and user has to remember colored password pairs.

- Creation Time: The time taken to create a password using an authentication system.
- Login Time: The time taken to login using a particular authentication system.

For Pair Based both creation and login time are similar to existing authentication systems.

For Hybrid Textual, creation and login time are more than Pair Based but less than PPC and TPPC.

For ImagePass, both are less than all other techniques.

For PPC, creation and login time both are less than TPPC but more than others.

For TPPC, both are maximum.

5. Conclusion and Future Scope

Having studied different recent graphical password authentication techniques and subjecting them for usability features that is memorability, creation time and login time and comparing the security features of each of them by considering their password space (complexity), dictionary attack, shoulder surfing and brute force attack. Every method has good resistance to various password attacks, but not a single method is perfect with subject to usability.

The future work is to balance the trade-off between Usability and Security by considering the following factors:

How meaningful the image?
Can the scheme be used easily?
How understandable is the scheme?
Is the scheme easy to execute?
Memorability of the image.
Simplicity of the steps involved.
Simplicity of the training for user.
Simple and nice interface.
Password space.
Prevention against Social Engineering.
Prevention against Shoulder surfing.
Prevention against Brute force.
Prevention against Dictionary attack.
Prevention against Guessing.

In conclusion, if the above factors are considered for future then reliable, usable authentication scheme is possible to implement.

References

[1] K. Renaud. "Evaluating authentication mechanisms". In L. Cranor and S. Garnkel, editors, Security and Usability: Designing Secure Systems That People Can Use, chapter 6, pp.103-128. O'Reilly Media, 2005.
[2] A. Adams and M. A. Sasse. "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures". Communications of the ACM, 42:41-46, 1999.
[3] R. Morris and K. Thompson. "Password Security: A Case History". Communications of the ACM, 22(11):594-597, 1979.
[4] D. Florencio and C. Herley. "A large-scale study of WWW password habits". In 16th ACM International World Wide Web Conference (WWW), May 2007.
[5] B. Kirkpatrick "An experimental study of memory". Psychological Review, 1:602- 609, 1894.
[6] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9 USENIX Security Symposiums, 2000.
[7] Real User Corporation (2007) Passfaces T M, http//:www.realuser.com.
[8] L.Sobrado and J.C.Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.
[9] Christopher Varenhorst "Passdoodles; a Lightweight Authentication Method", Massachusetts Institute of Technology, Research Science Institute, July 27, 2004. Pocket Telephone, Inc.
[10] Jermyn Ian, A. Mayer, F. Monrose, M. K. Reiter and A. D. Rubin," The design and analysis of graphical passwords", Proceedings of the Eighth USENIX Security Symposium. August 23-26 1999. USENIX Association 1–14, 1999.
[11] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP):Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.
[12] G. E. Blonder. Graphical passwords. United States Patent 5559961, 1996.
[13] Susan Wiedenbeck, Jim Waters, Jean - Camille Birget and Alex Brodskiy, Nasir Memon.PassPoints,"Design and longitudinal evaluation of a graphical password system", International Journal of Human-Computer Studies, 63(1-2):102-127, July 2005.
[14] Paul Dunphy, Jeff Yan, "Do Background Images Improve "Draw a Secret" Graphical Passwords?" Proceedings of the 14th ACM conference on Computer and communications security. Alexandria, Virginia, USA. ACM. 36- 47; 2007.
[15] International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, 2011 "Authentication Schemes for Session Passwords using Color And Images" M Sreelatha, M Shashi , M Anirudh , MD Sultan Ahamer , V Manoj Kumar.
[16] "ImagePass - Designing Graphical Authentication for Security" Martin Mihajlov E-business Department Faculty of Economics Borka Jerman-Blazi Jožef Stefan Institute Ljubljana, Marko Ilievski Seavus Group 2011.
[17] International Journal of Information & Network Security (IJINS) "Novel Shoulder-Surfing Resistant Authentication Schemes using Text-Graphical Passwords" M.Kameswara Rao, Sushma Yalamanchili, 2012.