Wheel Authentication based Multi-level Scalable Color-Textual Graphical Password System

Muhammad Ilyas
Department of Computer Science and Information Technology
University of Sargodha
Sargodha, Pakistan
muhammad.ilyas@uos.edu.pk

Qaisar Abbas
Department of Computer Science and Information Technology
University of Sargodha
Sargodha, Pakistan
qaisar.abbas@uos.edu.pk

Saad Razzaq
Department of Computer Science and Information Technology
University of Sargodha
Sargodha, Pakistan
saad.razzaq@uos.edu.pk

Fahad Maqbool
Department of Computer Science and Information Technology
University of Sargodha
Sargodha, Pakistan
fahad.maqbool@uos.edu.pk

Wakeel Ahmed
Department of Computer Science
University of Engineering and Technology
Taxila, Pakistan
wakeel.ahmed@uettaxila.edu.pk

Syed M. Adnan
Department of Computer Science
University of Engineering and Technology
Taxila, Pakistan
syed.adnan@uettaxila.edu.pk

***Abstract*—Password is basically a word, or a string of characters used to gain admittance, or to login to a system or a network. Passwords are usually tending to be alphanumeric or based on some graphics, often have considerable drawbacks. Guessing attacks or shoulder surfing is a well-known threat in which authentication session is observed or record to guess the password. With the passage of time, modern technologies and mobile communications make this world a mobile society and causes significant threats to authentications. Now it's very risky to enter alphanumeric passwords in public places, so these typical schemes of validations are bethinking as defenseless against shoulder surfing risk. In this paper, we have introduced an improved scheme based on alphanumeric text to defense against shoulder surfing. The scheme based on random number generation that provide a better choice for the users. In addition, provision of color scheme strengthens the proposed password scheme. Moreover, placement of all data in multi circular randomized wheel pattern make it more secure, reliable, and usable.**

***Keywords*—alphanumeric, admittance, watchword, hallmark, graphical passwords, shoulder surfing, security, reliability**

I. INTRODUCTION

In a computer security system human factors are perceived as the Achilles 'heel. Human computer interaction is important in three major areas which are referred by Patrick, et al. [1]:

1. Security operations, where the condition of not being threatened make satisfied.

2. Authentication, something which confirms or validates the authenticity of someone.

3. Developing secure systems, which are protected and free from attack or danger.

Authentication problem are focused here, usually the user enter user name and password or some kind of pin code for authentication. In addition of these two requirements, it's common to have some personal details like date of birth etc. for authentication key information. We are familiar with the weaknesses of these methods. The need of the hour is to remember password which is quite difficult for the users.

User like to choose short passwords and familiar ones to remember easily. They commonly avoid to pick lengthy and hard to remember passwords. More likely, the user wants passwords which are suitable to their typing speed and of reasonable length that they can easily use to enter for authentication without being grasped by anyone else. People always try to select a password which is easy to remember for them. But to their misfortune one can easily guess or broke that password.

Recently a news article which is related to computer world is published. In that article it is mentioned that a network password cracker was tried by a security team at a huge organization that identifies 80% of passwords within 30 seconds [3]. It is conferred by studies that users can recall only a few passwords. It's a common observation that most of the users are habitual to use the identical password for all their accounts. [5].

Different methods [3] [7], are used to solve the complications with classic username-password authentication. One such technique is Biometric authentication. Combination of numbers, alphabets and colors as passwords is used as another reciprocal way on which we will focus on this project. This project is about wheel authentication technique use all the mention elements as its core. Rotation of wheel by pressing buttons either clockwise or anticlockwise provide login for the user. Attractive and charming look and feel of color wheel provides a user capturing interface.

II. BACKGROUP AND RELATED WORK

The traditional way to access an account is by entering the required data like account number or username etc. New research work has led to graphical password techniques. The alternative way to text base passwords is graphical password schemes. In those applications that support graphics [2] and in many of the touch screen products, graphical passwords are used. Mutually Text-based and picture-based passwords are extensively used authentication techniques.

Both type of passwords secured a territory in their times. Punched cards and wild cards had also been in use for login into systems. Picture based authentication on many of the systems provide different manners to facilitate users with security accuracy and reliability. The picture-based techniques have further two sub classes: one is recognition based and the other is recall-based graphical technique.

ISBN-978-969-23372-1-2

Recall based graphical techniques are sub divided into two: Cued and Pure techniques. In recognition-based techniques, a set of images is displayed to a user and he or she identify and recognize the images which were selected by him during the stage of registration, then he or she passes authentication of images. In recall-based techniques, a user is requested to reproduce something that was created or chosen by him prior in the stage of registration.

Dhamija and Perrig [4] suggested hash visualization based authentication scheme. This scheme is categorized as graphical authentication technique. A Random picture is generated in visualization authentication method. Specific number of images is selected by user from those pictures. A computer program is used to generate the picture set. Later on, the user again recognizes those preselected images.

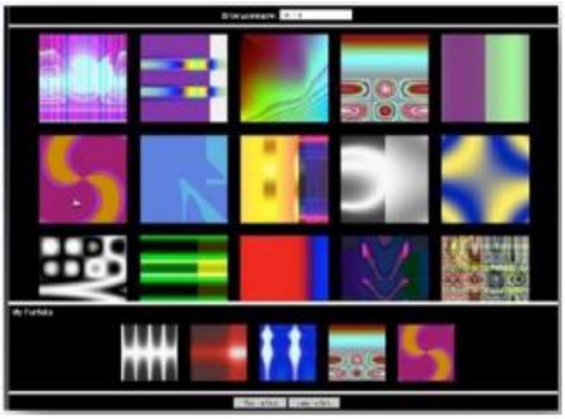

Fig. 1. Random Images used by Dhamija and Perrig [4]

Another graphical based technique which has some similarity with that of Dhamija and Perrig [4]. Is proposed by Akula and Devisetty's algorithm [9] their technique is using Secure Hash Algorithm 1 (SHA-l), that generates a 20-byte output making it different from the technique of Dhamija and Perrig. The specialty of their technique is that it is more secure and require less memory. Later, both Akula and Devisetty proceed with their work to make their technique more persistent in use. Persistent storage is suggested by the author for possible further improvement and so their proposed technique could be deployed on PDA’s, mobile phones and internet.

Inshall and Kirkpatrick [10] worked on a number of authentication schemes, such as object recognition, pseudo word recognition and picture recognition. They conducted a lot of user studies. Their brilliant work in the field of security and information field pay a special heed to facilitate the users with a number of sketched scheme through which user authentication method become more efficient. A database of images is provided to users, which are trained to recognize the selected images in picture recognition techniques.

In the field study of Security and information technology, shoulder-surfing is meant to be a known threat. A new graphical password technique is presented by Sobrado and Birget [11]. In their proposed scheme, first the pass objects previously selected by the user are displayed along with many other pass objects. For the authentication criteria, a user needs to recognize his previously selected pass-objects and click inside the convex hull made by all the pass objects. The user’s first priority is that his/her password is hard to guess by others and should be easy to remember by himself. IN order to make it difficult to guess the password, Sobrado and Birget propose a scheme. A total of 1000 objects are used which makes them nearly indistinguishable and creates a very packed display. In their second algorithm, the object is moved by user within a frame until the pass-object on the frame lines up with the other two pass-objects.

Man, et al. [14] sketched an alternative technique to avoid shoulder surfing. In his algorithm, the user is requested to choose a specific number of images as its pass-objects. Every pass-object has several alternatives and each alternative is assigned a special code. This diversity adds a high resistance. During authentication, several scenes challenge the user. There are number of pass-objects and decoy-objects in every scene. These decoy-objects are meant to lure some other person to grab the actual password. The person intends to enter, have a special code and have to type in a string according to the pass-object diversities presented by the screen. In addition to a pin or a code point outs the comparative position of the pass objects with respect to the pair of eyes. The statement used was that these kind of passwords are tough to guess and it’s really hard to crack the security envelope by such authentication technique even if the whole login session is recorded because there are no mouse events which give any clue. However, this kind of technique still requires a high capability of memorizing. Later Hong, et al. [15] enhanced this approach by allowing the user to give his own codes to pass-object variants. This technique was also very hard. It forces the user to remember pass codes of object variants which causes a sufficient load on user’s memory. That’s why it contains many drawbacks of text-based passwords and suffers users from memory loads. The memory load often makes authentication hard to grab and hard to recall. Especially in the cases if you want the immediate login and can’t wait, but these kind of techniques are good in resisting accidental login.

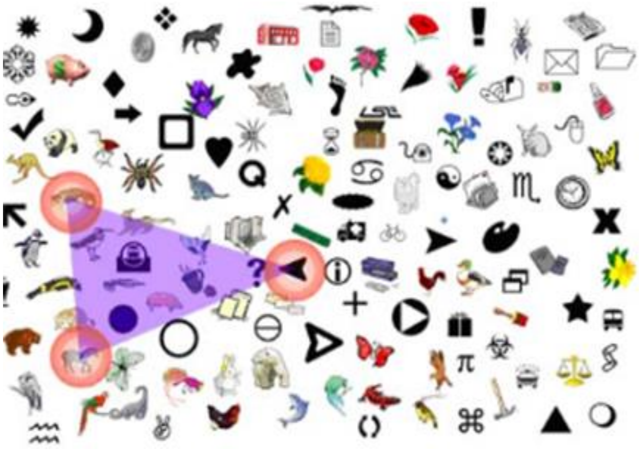

Fig. 2. Sobrado and Birget log shoulder-surfing resistant [11]

Another era in the field of computer security was of Passface. By Real User Corporation, a technique of “Passface” was developed [16]. In this technique a database of the human faces was maintained. Among those faces user selected four human face images. The selected images will be uses as user’s future password. The user will be presented with a grid of 3*3 during the phase of login. That grid contains one of the selected images and all the rest images will be decoy images. The user recognizes and clicks the known face. The same procedure will repeat for a number of stages. On correctly identifying all the preselected images, user will authenticate

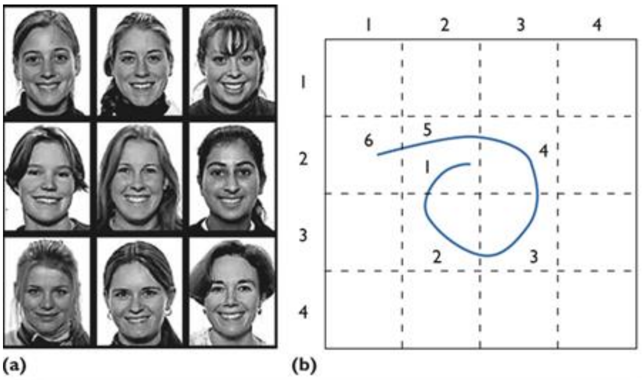

Fig. 3. (a) The Passfaces authentication system 7 uses a face grid for user authentication, whereas (b) another technique uses a pencil drawing as input [16-18]

Ziran Zheng et al. [16] presented a textual scheme based on strokes. The technique uses the shapes and patterns of strokes on the screen displays the grid. The scheme included traditional way to enter the password with the use of input devices. The technique was proved a high resistant technique against recording sessions and guessing attacks. Their study also showed that these types of passwords were used less frequent by users because they took longer the text passwords. Davis, et al. [19] investigated the graphical passwords that were generated using the Passface technique. He found a number of same patterns among these passwords. For example, having faces of similar features of people are chosen by the users. This marks the Passface password technique to a little bit predictable.

Jansen et al. [21] [22] developed a technique of graphical passwords for mobile devices. A user chooses a theme (e.g. cat, sea, etc.) during the entry phase which is a set of thumbnail photos. A sequence of images is then registered by him as his password. The user must enter the registered images in the correct sequence in authentication stage. A major drawback of this technique is the smaller password space (in case the thumbnail images are restricted to thirty). Each thumbnail image is assigned a numerical value; therefore, a particular numerical password will be produced by a specific sequence selection. Here a problem arises; the image sequence length was usually lesser as compared to the textual password length. To cope with this problem, image alphabet size was expanded by combining two pictures.

As shown in the studies by Davis [19], the picture passwords selected by users are often predictable. Most of the users use their own pictures. It makes the password predictability even more easier, especially if the attacker is familiar to the user.

Next, we discuss some important techniques that have developed to create powerful passwords. Token based techniques are considered as very simple techniques. . User is required to enter user name and password in order to get a token. That obtained token helps to fetch the required resources, without entering user name and password. The token will give access to user to a specific resource. This technique is widely used in smart cards, bank cards and key cards. Many knowledge based techniques are used by token based authentication techniques to improve security. For example, Bank ATM (Automatic Teller Machine) cards are commonly used along with a PIN number.

Takada and Koike [23] discussed the idea of same single graphical password for mobile devices. The main idea behind the technique is that users were allowed to use their preferred image for authentication [23]. Users must first register their preferred passport photos with the server. In the authentication phase, the verification requires several cycles. In each round there are several false images from which the user has to select the passport photo or choose nothing if there is no passport photo. If all exams are passed, the program authorizes a user. Allowing users to save their own pictures makes it easier for them to remember their password pictures. A notification mechanism is implemented to notify users when new images are recorded. The reason is to prevent unauthorized image capture. This is not a better method of authentication over text-based passwords.

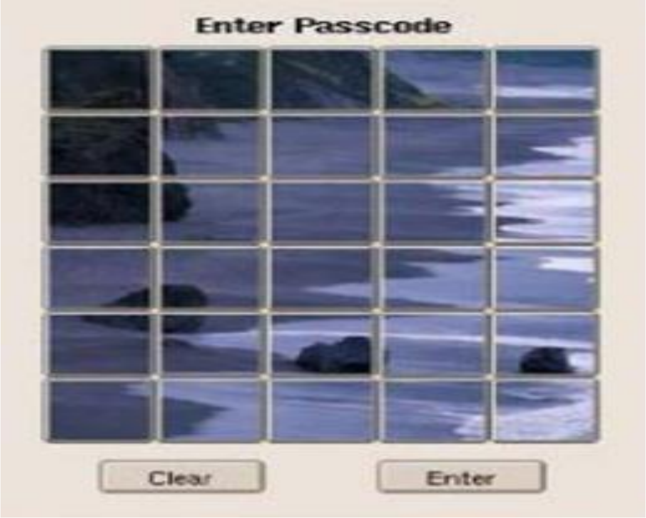

Fig. 4.A graphical password scheme [21]

Biometrics is the measurement and recording of the physical characteristics and distinctive of a person for use in afterwards personal identification. In this technique, such as traces of finger tips, facial traits recognition is still not highly adopted. This approach has been proved as expensive, unreliable and slow. Yet, a biometric authentication scheme provides a maximum level of security. Knowledge based technique is based on recalling. A user is presented with a prearranged collection of pictures from he/she have to select the images. In authentication stage he/she have to recall the image. So knowledge based techniques are meant to recognize and identified preselected images. In these techniques users will asked to create or identified something he/she already selected in registration phase. Jensen et al. worked on proposing a techniques based on pictures for mobile, PDA's. User was demanded to choose a theme from the grid of 5*6 matrix of images. Images was of size 40*40 and each image was displayed in thumbnail size.

To create a password user has to choose the pictures in an order or a sequence. For authentication, user was required to touch his/her preselected images in the same sequence by a stylus. As the grid of images always contain 30 images so the password space of this technique is small. A number appointed for per image and a predefined order of selection will yield a numerical password. Sometimes the textual password was longer than Jensen's technique passwords. [20]. so to overcome this issue a single click allows to choose two images at once. But this leads to difficulty and complexity for the user. In Image Pass Technique, during registration user is provided with a rectangular array (grid) of 30 images. The user has to choose images as his/her password. During logon phase, the grid of 4*3 means 12 images matrix is presented to user. There are some real and other decoy images in the presented grid. For authentication

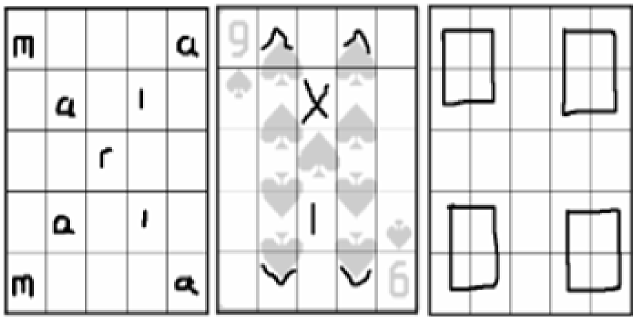

Fig. 5. Memorable complex secrets (a)Basketball and backboard, (b) Persian Name [23].

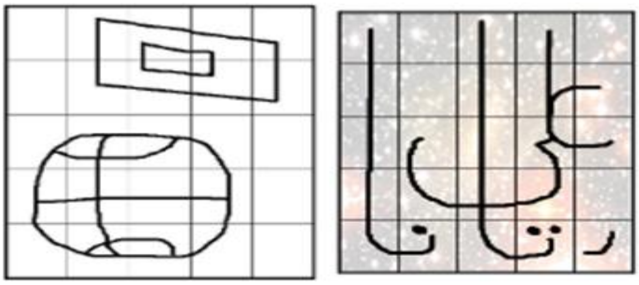

Fig. 6. Secrets created by participants claiming to be bad [23]

use have to pick the real images from the grid in right sequence [26]. The image location will change with time in every logon session. It is not strongly defensive to shoulder surfing as grid is only of size 4 x 3 and guessing attack can be also possible to occur, also the password images are stationary. So those can be easily seen, easily guess by striker. In Color Login technique, login time is decrease by the background color. Many colors are used to state conflict for the imposers, but easy to use for validate users. It is a nice technique to resist shoulder surfing attack, but the password space is less than text-based password and less password space leads to the risk probability.

With Recall Based Techniques, the person who is the user of the system must recall (re-create) whatever they have already created or selected during their recording session during the login phase. In the Pass Doodle technique, the main idea is based on the doodle coating. The user usually draws a picture with a pen on a sensitive screen. Users can easily remember the password they have drawn as a text password. The main drawback of the technique is observed as users sometimes forget the order in which they draw a doodle. The Draw-A-Secret (DAS) technique allows the user to draw an image on a 2D G x G array. This array can invoke a grid in such systems, and each cell in the array is considered a coordinate of an array denoted by a unique cell address versus coordinate values such as (x, y). The values of the touch grids are saved in the order of the drawing. To validate, the user must redraw the same pattern by touching the same coordinates on a grid. The length of the password does not make a short limit; the user can draw the password as long as he wants. The password space is much better than the text password [23]. Users can forget their stroke order, so sometimes it is easier to remember the text password than the DAS password.

TABLE 1THE ATTACKS PERUSE IN RECOGNITION-BASED TECHNIQUES [31]

Recognition Based Algorithm	Resistance	Non-Resistance
Pass Face	Brute Force, Guessing, Shoulder Surfing	Dictionary, Social Engineering
Dejavu	Brute Force, Guessing, Shoulder Surfing	Dictionary, Social Engineering
Triangle	Brute Force, Guessing,	Dictionary, Shoulder Surging Social Engineering

TABLE 2 ATTACK RESISTANCE IN PURE RECALL-BASED TECHNIQUES [31]

Pure Recall-Based Algorithm	Resistance	Non-Resistance
Blonder	Brute Force, Guessing, Shoulder Surfing	Dictionary, Spyware, Social Engineering
Passpoint	Brute Force, Guessing, Shoulder Surfing	Dictionary, Spyware, Social Engineering
Background DAS	Guessing,	Brute Force

TABLE 3 ATTACK RESISTANCE IN CUED RECALL-BASED TECHNIQUES [31]

Cued Recall-Based Algorithm	Resistance	Non-Resistance
Passdoodle	Dictionary	Brute Force
DAS	Dictionary, Guessing, Shoulder Surfing	Brute Force, Spyware, Social Engineering

Signature technique was smart because it was all about drawing signature with mouse and it’s difficult to make a replica of signature. They are difficult to fake, but it is a bit difficult for everyone to use mouse as a writing device. Most of the people usually do not have drawing or sketching skills and they do not prefer to make a password that includes any kind of sketching or drawing and make them insist to draw any pattern. Another problem is, there is usually less training for writing with mouse. So it’s hard to draw the same signature with same parameters as was in registration phase. One solution to this is to use pen like input device [24, 28]. But the disadvantages of adding new hardware is that they are not very common and also proves as expensive idea.

Cued Recall Techniques for authentication, the user is provided with a hint to retrieve a password that was recorded during the registration phase. These techniques provide advice for the user to remember the password and are therefore simpler than the techniques that are based on a callback only. Some examples are given in Table 3. Blonder originally described graphical passwords. In the Blonder technique, the user is presented with a predetermined image with predetermined detection areas [30]. When registering, the user must click on these take regions in a specific order in order to generate the password.

For authentication, the user must click on the approximate areas of these tap areas in the predefined order. The picture can help the user remember the password so that this pattern is marked as more appropriate than the text password. The disadvantage is a memorable password area. Due to the given grip areas, the user cannot click on the desired location. The background of the picture is also very simple.

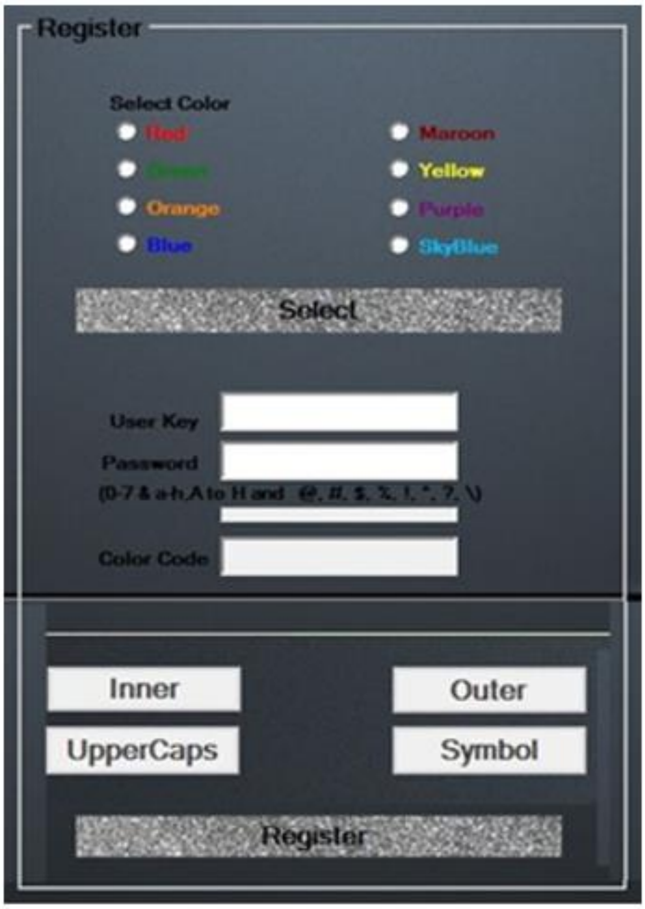

Fig. 7. GUI of Registration Process

To overcome the limitations of Blonder technique, pass points technique was proposed. In the technique user was helped by any natural photo or painting to remember his/her click. Here no need of predefined click points like Blonder technique. User can click on any of the place of picture to create his/her password in the registration phase [31]. The tolerance in every chosen point of click is calculated. The user has to click in correct tolerance to select his/her password clicks in correct sequence while authentication phase. In this, passwords can easily create but user have to face difficulty in recalling such passwords more than textual passwords. Also time for login is also longer than to login with textual passwords.

Another significant graphical password scheme is Background Draw a secret (BDAS). It is an innovative graphical password scheme. BDAS is the extension of Draw a Secret (DAS) scheme that was developed by researchers from New York University, AT&T Labs and Bell Labs. Its security and usability is much more enhanced as compared to that of DAS. In BDAS, a user draws a free-form drawing on a grid that has a background image chosen by him. This free-form drawing is then considered as his password. The users of this new system insist to draw any pattern. Maximum number of testers thought them easy to remember. Image at the background is main feature to success of this technique. It helps users in making their pattern or sketch passwords less predictable and more difficult and artistic. Users are also aided to re-produce them at the precise positions on the drawing grid. Another advantage of BDAS is its ease for people suffering from dyslexia or those who can't read or write well. It has also an increased complexity level as compared to DAS as it allows users to add more components to pattern they draw with a less cognitive load.

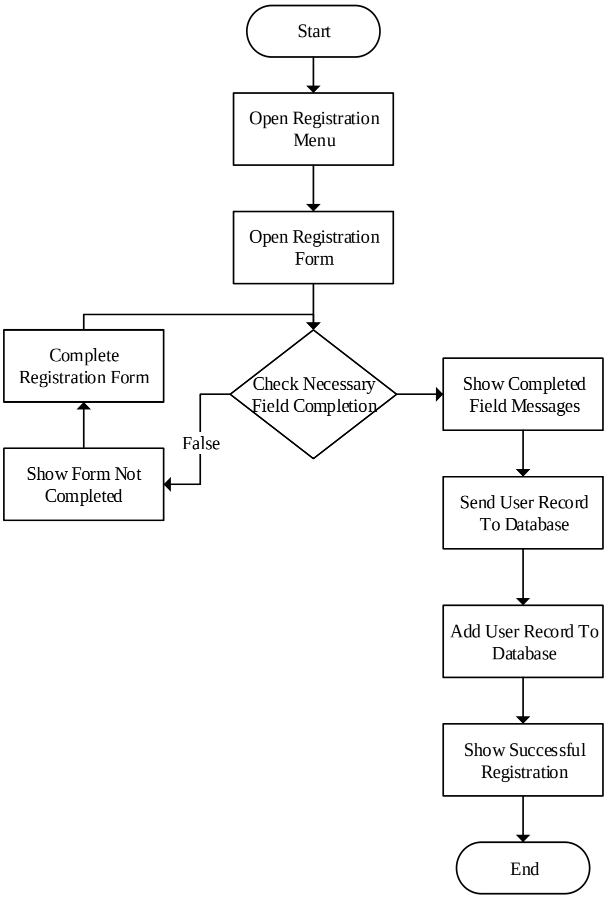
Start
Open Registration Menu
Open Registration Form
Complete Registration Form
Check Necessary Field Completion
Show Completed Field Messages
False
Show Form Not Completed
Send User Record To Database
Add User Record To Database
Show Successful Registration
End

Fig. 8. Flow Diagram of Registration Process

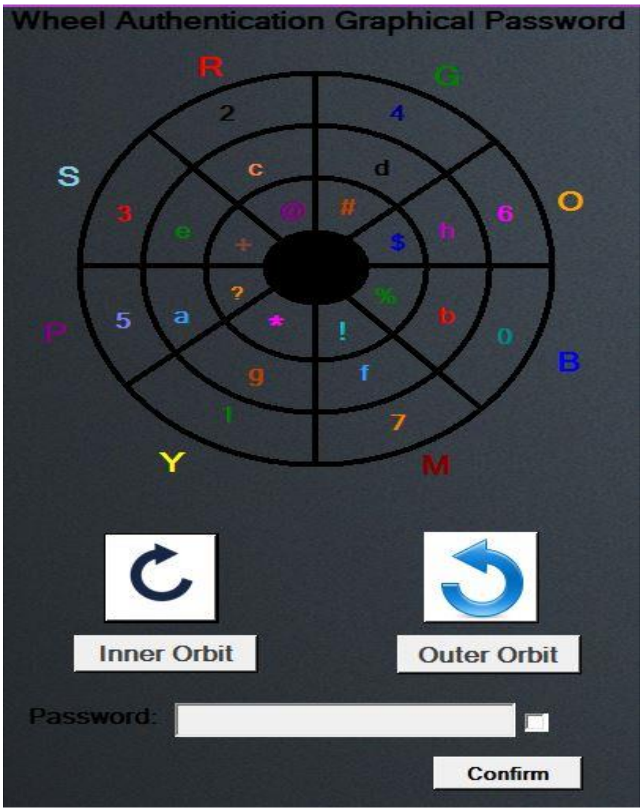

Fig. 9. Login Form

III. PURPOSE

Wheel authentication method is meant to provide an efficient and user friendly interface for login purposes, to establish an easy and quick graphical password through registration. This is about achieving Security for authentication and validation of systems in an efficient way to avoid shoulder surfing. Shoulder surfing is a known risk for security events and a permanent threat for key information needs to be hide from unauthorized persons. Main objective is about achieving safe and efficient confirmation with resistance against being grab by a surfer to a nice extent. The strength about this technique is generating random numbers each time the authentication session undergoes, no external keyboard, dependency on active and decoy color codes, with reliability, accuracy and usability of the data provided by user. The key advantage of graphical passwords over text-based passwords is that people are better at memorizing them. The wheel authentication technique is also meant to give a criterion to login with such memorizing passwords.

IV. METHODS

The main strategy is to develop the usability and security elements of the new technique name as Wheel Authentication Graphical Passwords. It is rather significant to outline the entire plan in order to make sure that the progress of project will not deviate from its core objective and the result can be achieved in an anticipated way. Prototyping will be applied; an initial prototype will be created that will be then gradually shifted to the final prototype. Prototype testing is required to check the usability and security features. The security testing will be done by calculating the "password entropy" and by "observation". Two sessions/phases are implicated by the forth put scheme:

1. The registration phase
2. The login phase

The alphabet used in the presented wheel authentication system contains 16 characters, including 8 lower case alphabets from a to h, and 8 Upper caps from A to H, in addition to symbol set (@, #, $, %,!, *, ?, +) & 8 numbers from 0-7.The phases can be described as in the following:

Registration: User will set text password K of length L. Eight (8) color s will be given by the system and one color will be choosing as his pass color. After selecting one color as user active color, all the remaining seven color will act as decoy color s. System will immediately show the color code to the user with respect to selection criteria in the form of a popup message. User will then give his user key in the form of numbers and set his/her password. The system will store the text password in the user entries password table. For registration, User key and Password will be given to the system manually while the color code will be automatically generated by selecting one of the radio button of his/her desired color and click on the Selected button.

A. *Workflow of Registration Scenario*

The user is first intent to be on the registration page having essential elements to fill them up. Following is the Flow diagram of Registration process for registering password to login. It is must to fill up all the required fields to register the password. Afterwards, a completion message will be displayed and the data of the user will be saved in the database. Following is the Flow diagram of Registration process for registering password for login.

a) Login

The user demands to login the system by providing the system with User key. If User key is registered, the system shows the wheel authentication session form containing a colored circle composed of 3 circles of different radii and 8 equally distant sectors. The color codes of the arcs of the 8 sectors are different from each other. On the bases of User key provided by user, the color code with respect to that key will active for the current session. Each sector is identified by that code of its arc label, e.g., the Green sector is the sector of green code denotes with "G". Initially, 24 characters are placed averagely, arbitrarily and randomly among these sectors. All the displayed color codes can be simultaneously rotated either in clockwise or anti-clockwise direction. When user will click the "clockwise" button once, the adjacent color sector's codes will move in the clockwise direction or by clicking the "anti-clockwise" button, the adjacent color sector's codes will rotate in the anti-clockwise direction. Any of the character can be selected if it's laying in the scope of user color code.

As the Wheel contains three circles of different radii, and each of them is further divided into 8 equal sectors, and each sector contain a character. Outermost circle's characters can be selected by button "Outer orbit", and the characters within circle just inside the outermost circle can be selected by button "Inner orbit". Innermost circle contains a set of 8 symbols that can be selected by button "Symbol". Another button "UpperCaps" works just like the functionality of "Caps Lock" button. Once a user writes down all his/her password characters by rotating and selecting the wheel characters, he/she can click on login button to authenticate his/her session. There exists a key, unless the user not remember his/her color code, he/she will not be able to login. Rotation of wheel either clockwise or anticlockwise give the user to pick his/her password character either it's a number, an alphabet or a symbol. There are no restrictions over rotation of wheel. User can rotate the wheel in his/her desired direction.

As the wheel authentication does not involve keyboard to enter the password, so the onscreen buttons are the key entities for this job.

B. *Workflow of Entering Password Scenario*

The first form that appears will ask the user to enter its user key. If the authentication is valid the wheel authentication form will appear next, otherwise valid user key have to be enter. On validation, the databases will be searched for the color code, if the user is already registered with entered user key than the color code for the respected user key will be activated. User can now enter his/her password by rotation of wheel either clockwise or anti clockwise and by using selection buttons. If color code is not activated for the entered user key, error will occur. The only way to access is to enter the registered user key and password correctly. Figure 10 shows the Flow diagram of entering password through wheel Authentication.

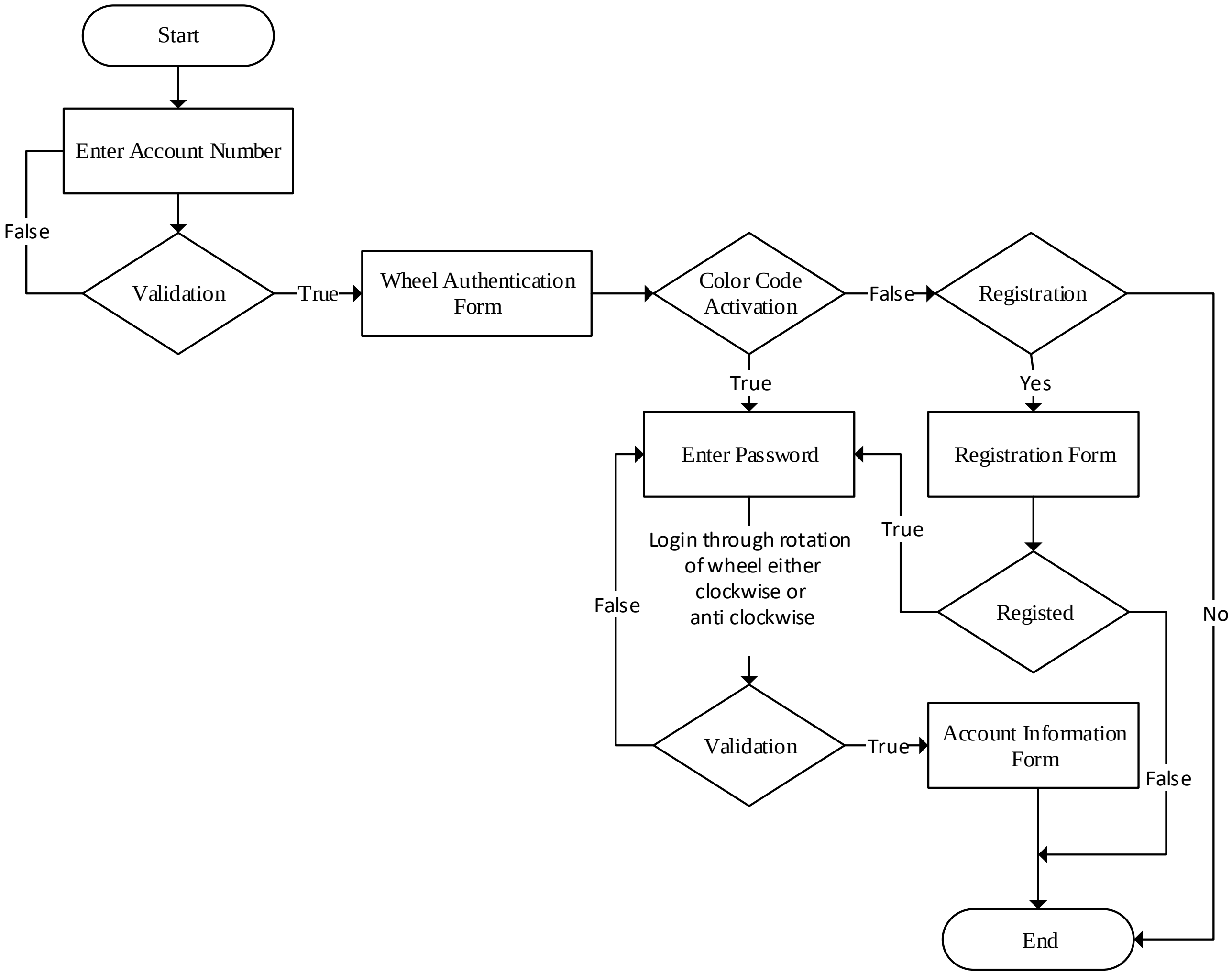

Fig. 10. Flow diagram of entering password through wheel Authentication

V. RESULTS

A. Result Analysis

Wheel authentication system will provide a number of password combination a user can make. The system proposed the security and the usability will be as follows:

a) Password Space

Suppose that the length password is L, i.e. $1 < L < 8$ so now there are $8*24^L$ password available for use.

So, the password space of the presented scheme is:

Total password space= $\sum_{L=0}^{7} 8 * 24^L$

b) Resistance to accidental login

The probability of entering password is 8/24, i.e., 1/3, so the probability of accidental login is, $(1/3)^L$.

VI. CONCLUSION

In this article, we've examined some work related to graphical password techniques. We had also proposed a system that uses a multi-circular wheels having color-based graphical text-based password that is helpful in reducing shoulder surfing attacks. With this authentication method, the user can log into the system without having to worry about shoulder navigation and can enter the password without using the physical keyboard. This method uses both a text password (number, upper and lower alphabets and some special characters) and a color-based graphical password. Placement of all data in multiple circles and continuously changing of position of all text on each click make this scheme more secure and reliable. The user can log into the system quickly, easily and efficiently. In future, more options to make password complex or enhance difficulty level will be incorporated. We can do this by swapping the position of different circles with one another (inner and outer bound). Moreover, a greater number of alphabets, number and special characters can be added to enhance the usability. In current prototype, color alphabets and other data could affect the performance if user have color blindness. So, for such user, shaded or patterned colored could be adopted in future work.

REFERENCES

[1] S. Patrick, A. C. Long, and S. Flinn, "HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA, 2003.

[2] A. Adams and A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp. 41-46, 1999.

[3] K. Gilhooly, "Biometrics: Getting Back to Business," in Computerworld, May 09, 2005.

[4] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.

[5] M. Kotadia, "Microsoft: Write down your passwords," in ZDNet Australia, May 23, 2005.

[6] M. Kotadia, "Microsoft: Write down your passwords," in ZDNet Australia, May 23, 2005.Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 33, pp. 168-176, 2000.

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

[8] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.

[9] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," Proceedings of Mid-west Instruction and Computing Symposium, 2004.

[10] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.

[11] L. Sobrado and J.C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[12] J. Thorpe and P. C. van Oorschot. Towards secure design choices for implementing graphical passwords. ACSAC, 2004. An extended version available at http://www.scs.carleton.ca/~jthorpe/extendedStrokes.pdf.

[13] Y. Mu and B. YAo, "Construction Of Topological Graphic Passwords By Hanzi-gpws," 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China, 2019, pp. 1957-1961, doi: 10.1109/ITNEC.2019.8729374.

[14] S. Man, D. Hong, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in Proceedings of International conference on security and management. Las Vergas, NV, 2004.

[15] D. Hong, S. Man, and M. Mathews, "A shoulder-surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.

[16] T. Valentine, "An evaluation of the Passface personal authentication system," Technical Report, Goldsmiths College, University of London 1998.

[17] T. Valentine, "Memory for Passfaces after a Long Delay," Technical Report, Goldsmiths College, University of London 1999.

[18] S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords: a field trial investigation," in People and Computers XIV - Usability or Else: Proceedings of HCI. Sunderland, UK: Springer-Verlag, 2000.

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

[20] W. Jansen, "Authenticating Mobile Device Users through Image Selection," in Data Security, 2004.

[21] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.

[22] W. A. Jansen, "Authenticating Users on Handheld Devices," in Proceedings of Canadian Information Technology Security Symposium, 2003.

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

[24] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.

[25] W. A. Jansen, "Authenticating Mobile Device Users through Image Selection," in Data Security, 2004.

[26] M. Mihajlov, "Image Pass - Designing Graphical Authentication for Security" E- business Department Faculty of Economics Borka Jerman-Blazi Jožef Stefan Institute Ljubljana, Marko Ilievski Seavus Group 2011.

[27] Haichang Gao, Xiyang Liu, Ruyi Dai, "Design and Analysis of a Graphical Password Scheme", International Conference on Innovative Computing, Information and Control (ICICIC), 2009, pp. 675 – 678.

[28] Christopher Varenhorst" Passdoodles; a Lightweight Authentication Method ", Massachusetts Institute of Technology, Research Science Institute, July 27, 2004.

[29] 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

[30] G. E. Blonder. Graphical passwords. United States Patent 5559961, 1996.

[31] R. Salleh, "A new Algorithm for graphical user authentication based on rotation and resizing" Arash Habibi Lashkari Faculty of Computer Science and Information Technology, University MALAYA (UM), May, 2010.