JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Recent Survey of Different Techniques Used in Image Authentication Schemes

Zeeshan I. Khan, Vijaya K. Shandilya

Assistant Professor, Professor
Dept. of CSE
P. R. Pote Patil COE&M, Amravati, Maharashtra, Sipna COET, Amravati, Maharashtra

Abstract : Authentication is the action or a process to check the identity of the user to use or access any system, profile, database, etc. Today, in the era of advanced technologies, user strongly needs a flexible, easy to remember and secured authentication scheme to protect the privacy of user's data. The main problem faced by a user is password remembrance because textual password becomes more complex nowadays since it contains alphabets, numbers and symbols. So, now it's the time to move on with image passwords which can be easily remembered by the user. But the implementation of an image password is not an easy job since it consumes a large amount of memory and time. This paper focuses on the well-known techniques that are used in image authentication schemes. It also explains the architecture and workflow of all those schemes which makes the image authentication scheme advantageous as well as acceptable in today's digital era.

IndexTerms **- Alphabets, Images, Non Sequential, Numbers, Recognition Based, Sequential, Symbols**

I. INTRODUCTION

Computers, Mobile Phones, Tablets, TV's, ATM's, etc. are electronic devices which communicate with user individually. Authentication is the action or a process to check the identity of the user to use or access the above-mentioned systems. The systems which are capable of doing authentication are called as Authenticators. A secret code remembered by the user and processed by authenticators including text, images, graphics, body prints, etc. for accessing the system is called as a Password.

Nowadays, every system needs a strong authentication scheme to check the authenticity of the user. There are various authentication schemes developed & suggested by researchers & developers till date. The primary aim of this paper is to explain in detail about the architecture, workflow and the abilities of various image authentication schemes which are suggested and developed by researchers and developers and it should be taken into use because of its strengths and advantages.

Image Passwords: It is the modern type of passwords that uses images as the primary data. It is easy for the user to remember the images as compared to the string of characters, numbers or symbols. In Image Passwords, there are two categories of authentication,

1. Recall Based:

This category of image password allows the user to create an image, graphics or drawing as a password and always used it for verification. For Example: Pattern drawing, a well-known authentication system used in the Android operating system is recall based. [1]

2. Recognition Based:

This category of image password allows the user to select the images, graphics, from the list of given examples on the screen and recognize it at the time of verification.

For Example: Image selection from a given set of images are recognition-based. [1]

Now, in the following section, the different image authentication techniques (Recall Based & Recognition Based) category has been described with architecture and work flow.

II. TECHNIQUES USED IN IMAGE AUTHENTICATION SCHEMES

Technique 1 (2003):

Visual Login Technique for Mobile Devices (Category: Recognition Based)

Wayne Jansen, Serban Gavrila, Vlad Korolev, Rick Ayers and Ryan Swanstrom [2] proposed an authentication scheme in which image thumbnails are given to the user for image selection. When the user selects an image, a randomly generated text (attached with the image cell) is stored in the database as a password. This technique saves the memory at the front end and back ends both.

At the front end, due to image thumbnail, memory is saved and at the back end, due to randomly generated text, memory is saved. It is shown in the Fig. 1. [2]

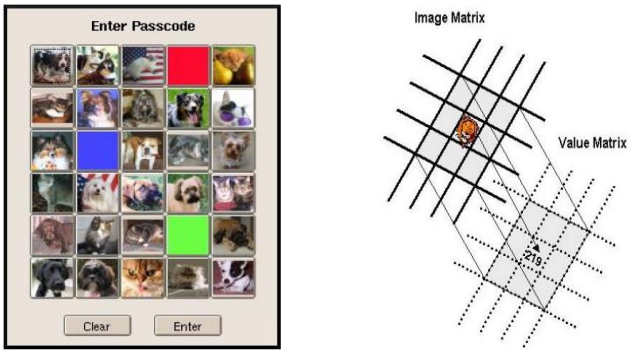

Fig. 1. Image to Random Number Generation Method

Technique 2 (2012):

Time Interval and Pressure Scheme (Category: Recognition Based)

Ting-Yi Changa, Cheng-Jung Tsaib and Jyun-Hao Lina [3] proposed a graphical authentication scheme for touch screen devices. In this system, users have to select images by click on the touch screen. It stores the time interval and pressure at the time of image selection which acts as a password. It is shown in the Fig. 2. [3]

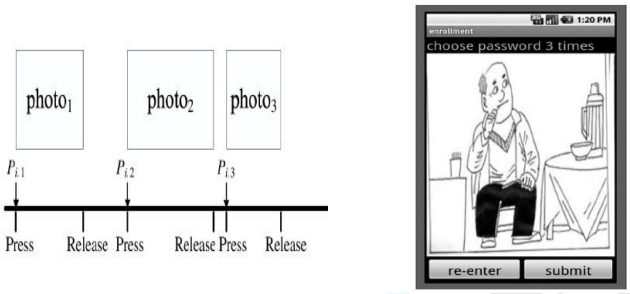

Fig. 2. Time Interval and Pressure Scheme

Technique 3 (2012):

Select to Spawn (Category: Recognition Based)

Mohammad Sarosh Umar and Mohammad Qasim Rafiq [4] developed a novel system "Select-to-Spawn" which is also a recognition based image authentication scheme. In this scheme, there are two levels of password selection. In the first level, the user has to select an image from the given 16 images. In the second level, the selected image is divided into 16 cells through 4 × 4 grids. From that, the user has to select a grid. At the time of verification, users have to select the image first and then the grid which increases the level of security. It is shown in the Fig. 3. [4]

Fig. 3. Select to Spawn

Technique 4 (2013):

Three Dimensional Password (Category: Recall Based)

Ronak B. Singh, Zeeshan I. Khan [5] proposed a three dimensional password scheme in which a virtual environment is provided with a choice to the user. The choices are Carom, Draw, Radio, etc. From those choices, user has to select an environment. For example, if user selects a carom, then a carom board appears on screen and user has to select a carom shots from the predefined 7 shots on the screen. That shot will be stored in the form of corresponding text and acts as a password . It is shown in the Fig. 4. [5]

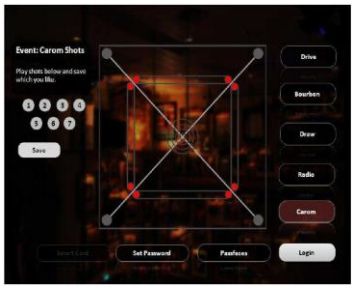

Fig. 4. Three Dimensional Password

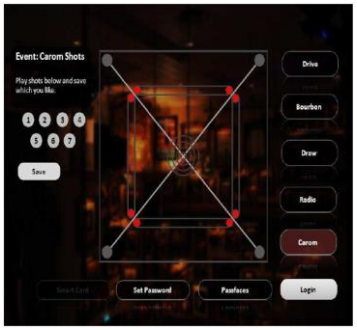

Fig. 4. 3D Password

Technique 5 (2013):
Android Pattern Lock (Category: Recall Based)
In the Android Operating System, the pattern lock is a very well-known authentication scheme that belongs to recall based type. In this scheme, the user has to draw a pattern with the help of 3×3 dots. The password will be stored in the form of pixel coordinates . It is shown in the Fig. 5. [6]

Fig. 5. Pattern Making in Android OS

Technique 6 (2015):
Click and Session Based Captcha – Graphical Password (Category: Recognition Based & Recall Based)
Vikas K. Kolhekar and Milindkumar B. Vaidya [7] proposed a click and session-based scheme for smartphones and the web. This scheme contains 2 methods using the concept of captcha as a graphical password . It is shown in the Fig.6. [7]

Fig. 6. Text and Image Captcha as a Password

Technique 7 (2015):
Five Cued Click Points Technique (Category: Recognition Based)
Amol Bhand, Vaibhav Desale, Swati Shirke and Suvarna Pansambal (Shirke) [8] proposed a system in which user has to upload any image of his/her choice or can select an image from the existing database. After selecting the image, the user has to select some cued click points on that image. Based on the RGB values of the selected image, a textual password is generated and sent on the email of the user. At the time of verification, the user has to select the cued points on the image and also enters the textual password which is generated earlier.

If the user enters or selects the wrong point in the image, an alert message will be sent on the user email. It is shown in the Fig. 7. [8]

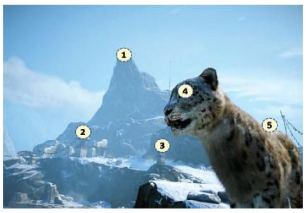

Fig. 7. Five Points Cued Click Technique

Technique 8 (2015):
Invisible Triangle Technique (Category: Recognition Based)
Roshni Rajavat, Bhavna Gala and Asmita Redekar [9] developed an authentication scheme to remove shoulder surfing attacks. In this system a combination of images and texts are used. Initially the user has to type the textual password which is stored in the database. At the time of verification, an image containing alphabets, symbols and numbers at random places. The user has to draw an invisible triangle with the help of any 3 characters (3 points) from the password. If the 3 characters are correct, then the password is accepted. It is shown in the Fig. 8. [9]

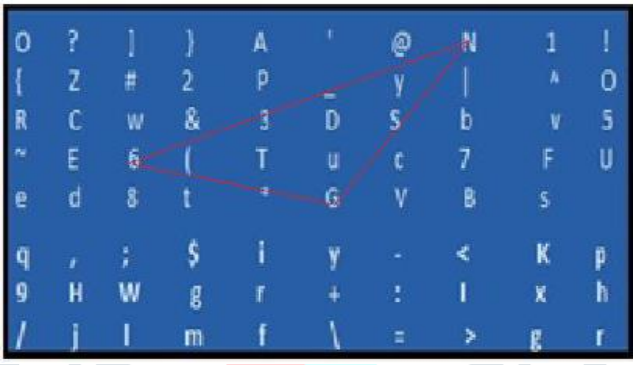

Fig. 8. Invisible Triangle Method

Technique 9 (2015):
Shoulder Surfing Resistant using Falsification (Category: Recognition Based)
Andrew Lim Chee Yeung, Bryan Lee Weng Wai, Cheng Hao Fung, Fiza Mughal and Vahab Iranmanesh [10] developed a graphical password system to remove shoulder surfing attack. In the system, the user has to select some images from the given set. The images will be selected when the user will enter the respective alphabet, number or symbols that are generated randomly along with the images. At the time of authentication, the user will put the randomly generated text along with the images and can prevent shoulder surfing attacks. It is shown in the Fig. 9. [10]

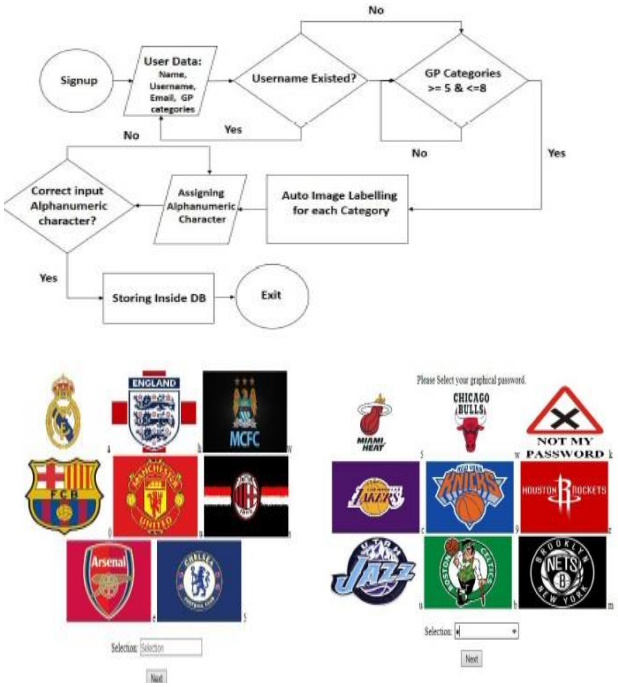

Fig. 9. Image Falsification Method

Technique 10 (2015):

Hybrid Graphical Authentication Scheme (Category: Recognition Based)

Swaleha Saeed and M. Sarosh Umar [11] implemented an authentication scheme in which the user has to select an image from the given set of 16 images by entering a three-digit code written on the image. At the time of password verification, the images are displayed on the screen and below the images the balls of different colors are also given. The color of the balls goes on changing randomly at runtime. The user has to remember the ball color which is present exactly below his/her selected image. Now that ball color has to be selected in the second login phase to complete the authentication process. It is shown in the Fig. 10. [11]

Fig. 10. Hybrid Scheme Using Color Balls

Technique 11 (2015):

Microsoft Windows 10 Picture Password (Category: Recognition & Recall Based)

In Windows 10 Operating System, a picture password authentication scheme is available. In this scheme, the user has to draw a circle, a line and a tab on a given image. Those 3 activities will be acting as a password. It is shown in the Fig. 11. [12]

Fig. 11. Picture Password In Windows 10

Technique 12 (2016):

Scheme to resist shoulder surfing attack (Recall based & Text Based)

Aakansha S. Gokhale & Vijaya S.Waghmare [13] proposed a system which can resist the shoulder surfing attack. It is a two-step process in which user has to select minimum 6 images from the set of 25 images in the first phase. And in the second phase, user has to select some questions and answers. The combination of images and questions can resist the attack at higher extent. [13]

Technique 13 (2017):

Two Way Authentication (Category: Token Based & Knowledge Based)

Subhradeep Biswas and Sudipa Biswas [14] proposed a system in which the user has to upload an image on the system. The system derives the password from that uploaded image and stored it in memory. At the time of verification, the user has to upload the same image again and the system checks the derived password from that uploaded image with the stored one. If both are the same, then the password is verified. They also suggest the two-way authentication i.e. along with image user has to enter secret text also to increase the security level. [14]

Technique 14 (2017):

Pass Positions (Category: Recall Based)

Gi-Chul Yang [15] proposed a system containing pass positions in which the user has to draw a curve, a line, etc. on an image and it stores the coordinates of the same in the database. With the help of pass position concepts, if the user forgets the actual position and draws the same type of pattern anywhere in the image, the password will be accepted because the pass positions also store the relative point of the pattern drawn by the user.

It is shown in the Fig. 12. [15]

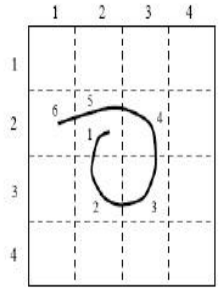

Fig. 12. Pass Positions Scheme

Technique 15 (2017):
Captcha as Graphical Passwords (CaRP) (Category: Recognition Based)
P. Sahaya Suganya, Dr. J. Andrews [16] introduced CaRP (Captcha as Graphical Passwords) that contains the two different methods of authentication using images. In the first method, the password is identified on the set of CaRP images after clicking the right character sequence. In the second method, the user is allowed to enter the correct pixel position of the corresponding image during authentication. It is shown in the Fig. 13. [16]

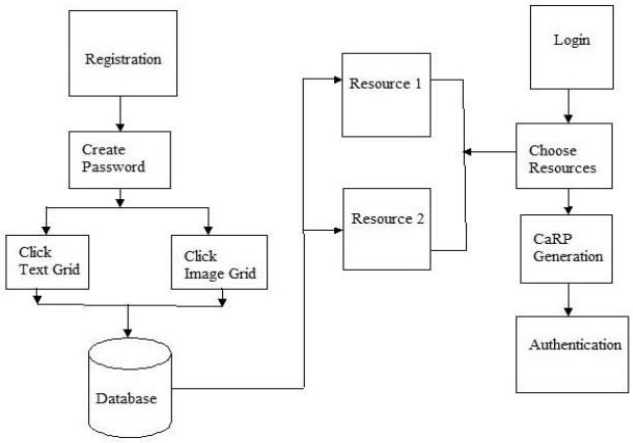

Fig. 13. CaRP Scheme Architecture

Technique 16 (2017):
Combination of Textual and Graphical password through Virtual Environment (Category: Recall Based & Text Based)
Deepika Gupta, Dr. Vishal Gaur, Akhand Pratap Singh and Shikha Mathur [17] proposed a system in which the user has to move the object in a virtual given environment with the help of mouse keystrokes. That movement done by the user is acting as a password. [17]

Technique 17 (2017):
Persuasive Cued Click Points (Category: Recall Based)
Sachin Kaja and Divya Gupta [18] implemented an authentication scheme using persuasive cued click points in which an image is displayed on the screen and the user has to click at any portion of an image and set that portion as a password. In this authentication scheme, there are various positions in a single image a user can choose. [18]

Technique 18 (2017):
Improved Graphical Authentication Scheme using Login Indicator
R. Sudha and M. Shanmuganathan [19] implemented an authentication scheme in which a user has to upload an image of his choice given by the server and then the server breaks that image in the grid of 7 × 11. After breaking those images in pieces, all the pieces are displayed to the user and then the user has to select any one of those pieces as a password. [19]

Technique 19 (2017):
Pass-Matrix Authentication (Category: Recognition Based & Text Based)
Shums Tabrez and Jagadeesh Sai D [20] proposed a scheme in which the combination of OTP (one-time-password) and the row, column number from an image gives a password.
The whole process is done by giving an image containing gridlines on the screen. [20]

Technique 20 (2019):
Advanced Android Pattern Lock (Category: Recall Based)
Some advancement is proposed by Suliman A. Alsuhibany [21] to make this scheme resistant to shoulder surfing attack by using camouflage patterns having activation and deactivation nodes. [21]

Technique 21 (2019):
Graphical Pin Entry System (Text Based and Recognition Based)
Muhammad Salman, Yang Li & Jian Wang [22] proposed a system to resist Shoulder Surfing Attack by using a different way of Pin Entering System. It is a two-step process. In first step, user has to select any location from the given sets of location. The selected location has a random number. User has to move the correct digits of the registered pin at the place of random number. It is shown in the Fig. 14. [22]

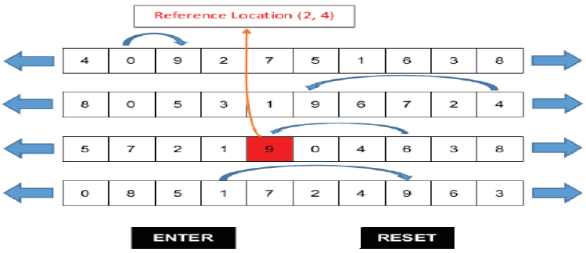

Fig. 14. Graphical Pin Entry System

Technique 22 (2019):
PIN Authentication Scheme using Tactile Feedback (Text Based & Recall Based)
Wei-Chi Ku & Hao-Jun Xu [23] proposed a method to resist shoulder surfing attack which will be completely based on Pin and Tactile feedback. At the time of entering the Pin, user has to observe the vibrations on the screen and follow accordingly [23].

Technique 23 (2020):
Integration of Image and Video Signature (Category: Recognition Based)
Vaishali Ravi, Seema Khan P, Usha H Y, Yashashwini B N, Kanmani B S [24] proposed a system which includes the combination of Image and Video Signature as a password. In Image Authentication, it includes cued clicked points. In Video Authentication, it includes clicked intervals. It is shown in the Fig. 15. [24]

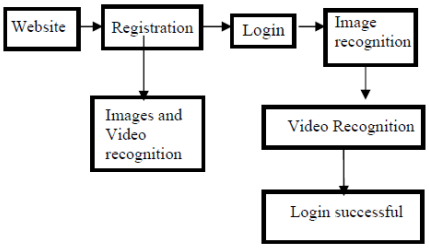

Fig. 15. Integration of Image and Video Signature

III. CURRENT ISSUES AND CHALLENGES

Recognition Based Image Passwords:
The main drawback is higher system storage and response time resulting in slow output and it is time-consuming for the user, process is difficult to understand, password sequence is difficult to remember.

Recall Based Image Passwords:
It is difficult to remember the graphics or drawing.
Approximate pixel taking algorithms are used and that algorithm also weakens the security.

The limitations of all the techniques which are mentioned in the paper are given in the following table,

Sr. No.	Techniques	Limitations
1	Visual Login Technique	Shoulder Surfing Attack, Brute Force Attack
2	Time Interval and Pressure Scheme	Complicated Process, Maintaining time interval & Pressure is difficult, cannot be applicable on all platforms
3	Select to Spawn	Shoulder Surfing Attack, Time & Space consuming, Brute Force attack
4	Three Dimensional Password	Needs high processing power, Time & Space consuming, cannot be applicable on all platforms, multiple level of authentications
5	Android Pattern Lock	Shoulder Surfing Attack, Brute Force Attack, approximate pattern coordinates
6	Click and Session Based Captcha	Complicated Process, Time & Space consuming, Need more processing power
7	Five Cued Click Points Technique	Shoulder Surfing Attack, Time & Space consuming, multiple level of authentications
8	Invisible Triangle Technique	Not user friendly, triangle includes other characters also, Brute Force attack
9	Falsification Method	Shoulder Surfing Attack (if observed carefully), Time & Space consuming
10	Hybrid Scheme	Shoulder Surfing Attack (if observed carefully), Time & Space consuming
11	Microsoft Windows 10 Scheme	Shoulder Surfing Attack, Brute Force Attack , approximate pattern coordinates
12	Scheme to resist shoulder surfing attack	Time Consuming, Memory Consuming, multiple levels of authentications
13	Two Way Authentication	Complicated Process, User always carry image while authentication, multiple level of authentications, cannot be application at all platforms
14	Pass Positions	Shoulder Surfing Attack, Approximate pattern coordinates
15	CaRP	Complicated Process, Time consuming, Space consuming, cannot be applicable on all platforms, multiple level of authentications
16	Combination of Textual and Graphical password	Needs high processing power, Time consuming, Space consuming, cannot be applicable on all platforms, multiple level of authentication
17	Persuasive Cued Click Points	Shoulder Surfing Attack, Less User Friendly, Approximate pixel verification, Brute force attack (if multiple login chances allowed)
18	Improved Graphical Authentication Scheme using Login Indicator	Shoulder Surfing Attack if observed carefully, Less User Friendly, Time consuming, Space consuming, Brute Force attack (if multiple login chances allowed)
19	Pass-Matrix Authentication	Less User Friendly, Time consuming, Space consuming, needs an internet / network to check email containing OTP, multiple level of authentications
20	Advanced Android Pattern	Not user friendly, cannot be applicable on all platforms.
21	Graphical Pin Entry System	Complicated, Shoulder Surfing attack (if observed carefully), Time Consuming
22	PIN using Tactile Feedback	Complicated, applicable on Screen touch devices only
23	Integration of Image and Video Signature	Shoulder Surfing Attacks, Time Consuming, Memory Consuming System

IV. FUTURE TRENDS

Due to the problems faced by user and developers in textual password authentication schemes, the trend of image password authentication schemes is increasing. There are various ways suggested and developed by researchers or developers to implement image authentication schemes but somewhere it is not accepted as a full proof technique which can replace textual password authentication scheme completely. So the issues of image passwords including high consumption of memory and time, shoulder surfing attack, brute force attack, etc. will be resolved in the future making it as a successful authentication scheme.

V. CONCLUSION

The detailed survey of different techniques (23 techniques) mentioned in the paper which are proposed and implemented by researchers and developers give an idea and motivation to implement an image authentication scheme to replace the older traditional textual based approach so that the process of authentication becomes easy at users as well as developer side.

REFERENCES

[1] Reshma and G. Shivaprasad, "Research and Development of User Authentication using Graphical Passwords: A Prospective Methodology," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 8, no. 9S3, pp. 385-390, July 2019.

[2] Wayne Jansen , Serban Gavrila, Vlad Korolev, Rick Ayers, and Ryan Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices," National Insitute of Standards and Technology, Gaithersburg, USA, NISTIR 7030, 2003.

[3] Ting-Yi Chang, Cheng-Jung Tsai, and Jyun-Hao Lin, "A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices," *The Journal of Systems and Software, Science Direct*, vol. 85, no. 5, pp. 1157-1165, January 2012.

[4] Mohammad Sarosh Umar and Mohammad Qasim Rafiq , "Select to Spawn- A Novel Recognition-based Graphical User Authentication Scheme," in *International Conference on Signal Processing, Computing and Control, IEEE*, Waknaghat Solan, India, 2012.

[5] Ronak B. Singh and Zeeshan I. Khan, "Three-Dimensional Password System Implementation Technique," in *International Journal of Pure and Applied Research in Engineering and Technology*, Amravati, 2013, pp. 426-437.

[6] codedmin. (2018, July) CodingDemos. [Online]. https://www.codingdemos.com/android-pattern-lock-tutorial/

[7] Vikas K. Kolekar and Milindkumar B. Vaidya, "Click and Session Based- Captcha as Graphical Password Authentication Schemes for Smart Phone and Web," in International Conference on Information Processing (ICIP), IEEE, Pune, 2015, pp. 669-674.

[8] Amol Bhand, Vaibhav Desale, Swati Shirke, and Suvarna Pansambal (Shirke), "Enhancement of Password Authentication System Using Graphical Images," in International Conference on Information Processing (ICIP), IEEE, Pune, 2015, pp. 217-219.

[9] Roshni Rajavat, Bhavna Gala, and Asmita Redekar, "Textual and Graphical Password Authentication Scheme Resistant to Shoulder Surfing," International Journal of Computer Applications, vol. 114 - No. 19, pp. 26-30, 2015.

[10] Andrew Lim Chee Yeung, Bryan Lee Weng Wai, Cheng Hao Fung, Fiza Mughal, and Vahab Iranmanesh, "Graphical Password: Shoulder-Surfing Resistant using Falsification," in 9th Malaysian Software Engineering Conference (MySEC), IEEE, Kuala Lumpur, Malaysia, 2015, pp. 145-148.

[11] Swaleha Saeed and M. Sarosh Umar, "A Hybrid Graphical User Authentication Scheme," in Communication, Control and Intelligent Systems (CCIS), IEEE, Mathura, 2015, pp. 411-415.

[12] Walter Glenn. (2017, January) How-to Geek. [Online]. https://www.howtogeek.com/135561/should-you-protect-your-windows-8-pc-with-a-picture-instead-of-a-password/

[13] Aakansha Gokhale and Vijaya Waghmare, "The Shoulder Surfing Resistant Graphical Password Authentication Technique," in 7th International Conference on Communication, Computing and Virtualization 2016, vol. 79, 2016, pp. 490-498.

[14] Subhradeep Biswas and Sudipa Biswas, "Password Security system with 2-way authentication," in Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), IEEE, Kolkata, India, 2017, pp. 349-353.

[15] Gi-Chul Yang, "Pass Positions: A Secure and User-Friendly Graphical Password Scheme," in 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), IEEE, Kuta Bali, Indonesia, 2017.

[16] P. Sahaya Suganya and Dr. J. Andrews, "Analysis of various Authentication Schemes for Passwords using Images to enhance Network Security through Online Services," in International Conference on Information, Communication & Embedded Systems (ICICES 2017), IEEE, Chennai, 2017.

[17] Deepika Gupta, Dr. Vishal Goar, Akhand Pratap Singh, and Shikha Mathur, "Combination of Textual And Graphical Based Authentication Scheme Through Virtual Environment," in 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA), IEEE, Dehradun, 2017.

[18] Sachin Kaja and Divya Gupta, "Graphical Password Scheme using Persuasive Cued Click Points," in International Conference On Smart Technology for Smart Nation, IEEE, Bangalore, 2017, pp. 639-643.

[19] R. Sudha and M. Shanmuganathan, "An Improved Graphical Authentication System to Resist the Shoulder Surfing Attack," in International Conference on Technical Advancements in Computers and Communications, IEEE, Melmaurvathur, 2017, pp. 53-55.

[20] Shums Tabrez and Jagdeesh D Sai, "Pass-Matrix authentication," in International Conference on Intelligent Computing and Control Systems, IEEE, Madurai, 2017, pp. 776-781.

[21] Suliman A. Alsuhibany, "Usability and shoulder surfing vulnerability of pattern passwords," Journal of Ambient Intelligence and Humanized Computing, March 2019.

[22] Mohammad Salman , Yang Li, and Jain Wang, "A Graphical PIN Entry System with Shoulder Surfing Resistance," in 4th International Conference on Signal and Image Processing, Wuxi, China, 2019, pp. 203-207.

[23] Wei-Chi Ku and Hao-Jun Xu, "Efficient Shoulder Surfing Resistant PIN Authentication Scheme Based on Localized Tactile Feedback," in International Conference on Cyber Security and Cloud Computing (CSCloud), Paris, France, 2019, pp. 151-156.

[24] Vaishali Ravi, Seema P Khan, Usha Y H, Yashashwini N B, and Kanmani S B, "Integration of Image and Video Signature in Graphical Password Authentication System," International Journal of Engineering Research & Technology (IJERT), vol. 9, no. 05, pp. 1314-1317, May 2020.