Webology (ISSN: 1735-188X)
Volume 18, Number 4, 2021

A Modern Image Authentication Algorithm Using Image Click Points To Resist Shoulder Surfing Attack

Devidas S. Thosar* and Dr. Dhanraj Verma

Department of Computer Science & Engineering, Dr. A. P. J. Abdul Kalam University, Indore (M.P) -452016

Corresponding Author Email: Devidas S. Thosar

Abstract:
This research presents a security scheme with the help of Graphical Password which uses images. The primary objective of this algorithm is to support the users in selecting better and safe passwords. The user will click on already selected Click point at the time of registration of the image to confirm the authentication. The persuasive cued clicked points will provide a series of images so that security increases as it will give a workload for the intruders. The user will select multiple images along with selecting the at least 3-4 click points on every image. The psychological study reveals that except remembering alpha-numeric characters, a person can easily remembers a visual image. So remembering the points on the images for a user will be easy and will be difficult for an intruder to get access. The persuasive cued clicks help the users to choose more random positions for the increase of security. The major advantage of this Graphical Authentication Algorithm is to provide the easy usability and greater security to the user in authentication process.

Keywords: Security, Graphical passwords, Authentication, Image Rotation, Image Click Points.

1. INTRODUCTION

The technology is been developing at a rapid rate in the past three centuries. We are getting modernized by making everything digitalized by the growth of technology. So the digital data is been growing in an exponential manner which leads to a major concern for the security [2]. While the predictability problem can be solved by reject by user choice and assigning passwords to users, this usually leads to usability issues since users cannot easily remember such unmethodical passwords. Number of graphical password systems has been developed; Study shows that words-based passwords suffer with both security and usability problems

Images that can operate on digital cameras or Smartphone's. Proposes a method for fusing multiexposed. The proposed method consists of an automatic exposure bracketing algorithm that determines which exposures to capture and a newly proposed multi-exposure image fusion algorithm. This fusion algorithm attempts to improve the fusion performance on the basis of the recently proposed no-reference image quality metrics and also change the affects the change noting that the change affects on image is in the local details of the image like contrast and color density of a pixel. The poor lighting condition and limited dynamic range of digital imaging device in smart phones and cameras, the recorded images are often under-/over-exposed and with low contrast.. The various Subjective experiments were conducted to screen the best quality of the image as the reference image by changing each scene. During the survey , total thirteen representative multi-exposure was done using image fusion in various Smartphone and using various stack-based high dynamic range based authentication imaging algorithms are used to generate the color density enhanced images for each sequence of images and Most of previous single image contrast enhancement (SICE) methods in Smartphone’s to adjust the tone curve to correct the contrast of an input image to capture the snap. These methods, often failed in changing the old details of the image because of the insufficient information of the any single image.

This algorithm presents a security scheme with the help of Graphical Password which uses images for authentication purpose. The main objective of using this algorithm is to help the users in selecting multiple images by selecting different click points for every image as password to provide better and secure passwords. The persuasive cued click points will provide a series of images so that security issue increases at a level and user will have to click on the correct pixels of the image to be authenticated. The series of images as well as selection of clicks points for every image is totally depends on the user. Because the psychological study reveals that a person better way remember the images / graphical part more than the traditional passwords like series of alpha-numeric characters. This will help the user to remember the pixels to be clicked on the image and it will be difficult for an intruder to get access over the user. The advantages of the Graphical Password Scheme are easy usable and greater security

2. BACKGROUND OF INVENTION

Initially a survey to find the existing authentication system was conducted where many of the existing different and similar systems were revealed. But the existing systems have the disadvantages of their own such as some systems needs more time for authentication, while need more space, while some are targeted by shoulder surfing attack. To overcome all these disadvantages I proposed an algorithm which will be reliable to use and provide security and appropriate authentication to the user.

The first existing similar authentication system was working in such a way that it was displaying a 3/3 grid and 9 images were displayed on that grid and user needs to select the same category of images as described to be authenticated. If the user is not able to select the appropriate images, then another grid with different images were displayed and user again needs to select the images with same category again and if the user fails this time then the user is not authenticated[2].

The second existing similar authentication system was nearly same to the first one but some new features were added to it. It was also displaying a 3/3 grid and images was partitioned into 8 parts. User needs to arrange these partitioned parts into such a manner that it forms a meaningful image. This system has some time to arrange the images to form a meaningful image. Also the user can change the image if user is not able to guess the image. If user fails to arrange these parts into a well manner, then the user is not authenticated.

In the previously available systems, there is a huge probability of shoulder surfing attack and in the second system the storage needed is too large. So to overcome all of these disadvantages I proposed an algorithm with this new invention, in which I provide recommendations based on the image based graphical password to address the weakness of textual password graphical passwords are proposed. As now days, the Click based or pattern based approaches are commonly used techniques for mobile authentication system. Such textual and graphical passwords a scheme suffers from shoulder surfing attacks. Attacker can directly observe or can use video recorder or webcam to collect password credentials. To overcome the problem, shoulder surfing attack resistant technique is proposed. This technique contains pass-matrix. More than one image is used to set the password. For every login session, user needs to scroll circulative horizontal and vertical bars. A password hint is provided to the user to select desired image password grid. For password selection, password hint to set covering the entire scope of pass-images. The proposed technique is implemented on android platform. The system performance is measured using memorability and usability of a password scheme with respect to the existing technique [5].

This algorithm relates to the field of Computer Engineering. This invention is related to the security that is must while authenticating user. This invention will use graphical passwords instead of text-based passwords. This invention helps the users to register for a series of images and every image has some pixels clicked by the user which will be used for authentication of user in future. Number of images can be increased to the security issue. In this algorithm any image from the registered images are displayed in front of the user where the user needs to select pixels to get authenticated. Every time any random image is selected from the registered images. In addition to this also some more features are added for security purpose such as image fusion, image flipping, image rotation, image discrimination and these features will also avoid the chances of shoulder surfing [1].

Initially a survey to find the existing authentication system was conducted where many of the existing different and similar systems were revealed. But the existing systems have the disadvantages of their own such as some systems needs more time for authentication, while need more space, while some are targeted by shoulder surfing attack. To overcome all these disadvantages this algorithm is been proposed which will be reliable to use and provide security and appropriate authentication to the user [2].

The first existing similar authentication system was working in such a way that it was displaying a 3/3 grid and 9 images were displayed on that grid and user needs to select the same category of images as described to be authenticated [7] If the user is not able to select the appropriate images, then another grid with different images were displayed and user again needs to select the images with same category again and if the user fails this time then the user is not authenticated.

The second existing similar authentication system was nearly same to the first one but some new features were added to it. It was also displaying a 3/3 grid and images was partitioned into 8 parts. User needs to arrange these partitioned parts into such a manner that it forms a meaningful image. This system has some time to arrange the images to form a meaningful image. Also the user can change the image if user is not able to guess the image. If user fails to arrange these parts into a well manner, then the user is not authenticated [5].

In the first system there is a huge probability of shoulder surfing attack and in the second system the storage needed is too large. So to overcome all of these disadvantages we are coming up with this new algorithm.

3. OBJECTIVES AND MOTIVATION

The major objectives of this research work are as follows:

1. Graphical authentication schemes provide a way of making more human-friendly passwords.
2. Ease of addition of new images in the system.
3. To reduce the shoulder surfing attack.
4. To concern the security of the user.

4. SCOPE OF THE WORK

The scope of this work is as follows:

This algorithm will help the user in been authenticated with the security. The application will reduce the shoulder surfing attack and will keep the intruders far away from our system. This algorithm will take some more time to authenticate than that of text based authentication. In the initial stage the user needs to register with their pre-defined images or also with some selected images that user wants to include. As the user tries to login the next time the images will be displayed and user needs to click the correct pixels for authentication. The more images selected by the user helps in more security. As the application is virtual the user can change the password by forgetting password by using forgot password option and can select new pixels on the existing images already selected by the user. This application will also contain some features such as image rotation, image flipping, image perspective changing to provide a better security.

5. LITERATURE SURVEY

The following problems were identified during the time of the review and analysis. This was annotated based on the analysis and the observations of the complete study. It also covers the periodical data from the 2017 to 2020 reviews. It shows the analytical and explorative way of exploration of the purpose and the study scenarios.

1. There is a need of secured password authentication system which overcomes the drawbacks of existing text and image based password schemes [1].
2. In today’s world of quick growing technologies there is the need of providing better Security which play’s a prominent role in the protection of people’s vital information from varied system attacks [6].

3. There is a need of providing graphical authentication system which should be designed in such a way that it must be able to restrict shoulder Surfing attack [7].
4. To resist shoulder Surfing attack there is a need of providing session password technique [8].
5. There is a need of Pass-matrix technique which uses pass-point clicking & also uses more than one image as a password [9].

6. PROBLEM IDENTIFICATION IN GRAPHICAL AUTHENTICATION

Existing approach for secure password like text-based password, OTP based password, PIN type of passwords does not provide very smart solutions for shoulder surfing attacks. Biometrical password scheme is very secured and safe. Whereas in biometric authentication system users voice, retina, thumbprint, face likewise different things are used as a passwords. There are various types of biometric sensors which as able to authenticate user. But costly hardware and sensors are required for this type of approach. Hence there must be smart system which provides flow and logic using which user can logged in to his mobile in the crowd without any heavy external hardware and other resources. Hence this need to fight against shoulder surfing attack motivates to design proposed system [9].

In this proposal I am going to provide a new graphical password authentication system algorithm named as **PASSIMAGE**. This is android based system. Multiple images are used to define password. Every time while login with system, the user needs to scroll the horizontal and vertical bars in Pass matrix. Also password hint is provided by the system to the user to select desired image password grid. For password selection, password hint to set covering the entire scope of pass-images [4].

7. ALGORITHMS DETAILS

In this Secured Graphical Authentication system, the study was performed on the basisof different authentication techniques currently available. On the basis of the limitations of literature review I proposed the advanced graphical authentication algorithm named as **PASSIMAGE Algorithm**:

1. PASSIMAGE Algorithm:

Step 1: Initially Complete the User Registration Process with User name & images used forverifying user with by selecting image object or Part of image.

Step 2: For every Login provides pass images by matching respective user name.

Step 3: Generate a random alphabet/ number or combination of both as a hint and provide it to the user using Audio message / Text Message if required.

Step 4: Repeat step 2 for every login pass image/Selected images.

Step 5: Discretize image in 6 *6 blocks by rotating image & apply image fusion algorithm on input images provided for authentication.

Step 6: Generate horizontal and vertical scroll bars for each image having 6 *6 block.

Step 7: Accept user input as per the hint provided in Step 2.
Step 8: Check if user input matches to the registration details & hint input correctly.
Step 9: Display next image and low steps from 4.
Step 10: Else display incorrect input image to the user as a warning.
Step 11: If all clicks matches notify user with success message.
Step 12: If login attempts >3 then lock the system for next 5 min.

Following is the proposed function which will useful for calculating the new pixel values after applying rotation / translation of the image.

```
defnew_pixel(x,y,θ,X,Y):
sin = math.sin(θ)
cos = math.cos(θ)
x_new = (x-X/2)*cos + (y-X/2)*sin + X/2
y_new = -(x-X/2)*sin + (y-Y/2)*cos + Y/2
returnint(x_new),int(y_new)
```

While applying some transform operations on images stored in pass-square, the rotation is one of operation that can be applied on an Image. By applying the Image rotation**,** the image is rotated from its center or from its origin by specified number of degrees i.e. **θ**. Image rotation is a specialization of commonly used transformation technique.Also Rotation is a geometric transformation which can be done through many ways like forward mapping or inverse mapping.

The transformation function for forward mapping is **x,y = T(v, w)** - x, y is the output pixel position and v, w is the input pixel position.

After applying any transformation operation on image, we required to determine the output pixel values by applying any one of the interpolation techniques on the neighborhood pixel values of the input pixel. The transformation matrix for the affine transformation in case of the rotate operation is given by:

$$\begin{bmatrix} cos\theta & sin\theta & 0 \\ -sin\theta & cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Where, **θ represents the angle of rotation**.

The various functionalities providing by this algorithm are:

1. Web-based application for user authentication.
2. Selected images and pixels stored in database.
3. Easily addition and deletion of new images and pixels.
4. Ease of adding external images as per user’s needs.
5. Number of wrong attempts displayed.
6. User is not able to login after 5 wrong attempts.
7. Also taking into consideration various factors like availability, security, database, etc.
8. Maintaining the accuracy of the model.

8. IMPLEMENTATION OF RESEARCH WORK

Basic Working Functionality of the Proposed Algorithm:

1. The user first logs in or signs up into the application. The pixels selected by the user are verified with the pixels stored in the database, if correct, the user is allowed to login.
2. On sign for first time the user needs to select images and pixels on it which are stored in the database.
3. The user can add pre-owned images from the system and select pixels on them, which eventually gets stored in the database.
4. The selected pixels are stored in the form of key-value pair in the database which will be needed for the authentication.
5. The user is able to login only if the correct pixels are selected.
6. Every time a random pair of images from the database will be displayed.
7. The user needs to select the correct pixels on both the images in defined order.
8. The user will also have 1 change to change the image if he/she forgets the pixels of the image.
9. If the user fails to select correct pixels for continuously 5 times then the user is not able to login and message is displayed as authentication unsuccessful.
10. The algorithm for the application is cued recall-based algorithm.
11. The selected pixels are stored in the form of key value pair and cued's are made of image which helps in authenticating fastly and accurately.
12. The algorithm will compare the pixels in the backend and will send the result to the system.
13. This will save the time as well as will provide the best security.

9. CONCLUSION

This algorithm is able to restrict shoulder surfing attack. To resist shoulder surfing attacks I proposed an algorithm to which use session password technique. During every session, new image fetched from pass-matrix to user at every login attempt. The fetched image is valid for only single login session. Pass-matrix technique is used in this work to kept images and pass-square is used to hold click points of every image. This technique uses more than one image as a password.

If user is not being able to select on correct click points as already available in pass-square then system displays a wrong image for next pass input. This wrong image is treated as a warning to the user. To define session password for pass square click, a hint is provided to the user. Based on the given hint user will select the password for that session.

REFERENCES

1. Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh, Chia-Yun Cheng, "A Shoulder Surfing Resistant Graphical Authentication System" in IEEE Transactions on Dependable and Secure Computing, Issue No. 02 - March-April (2018 vol. 15), Page 180-193.

2. R. Sudha, M. Shanmuganathan“An Improved Graphical Authentication System toResist the Shoulder Surfing Attack” in 2017 International Conference on Technical Advancements in Computers and Communications, IEEE, 2017.
3. Sreya Prakash, Sreelakshmy M K “A Secure Graphical Authentication System Using Watermark Embedding”, in International Conference on Intelligent Computing and Control Systems ICICCS, 2017.
4. Devidas S. Thosar, “A Review on Advanced Graphical Authentication to Resist Shoulder Surfing Attack”, published by IEEEXplore,978-1-5386-5367, IEEE, Dec-2019.
5. Devidas S. Thosar, “A Review On Modern Passimage Authentication System To Resist Surfing Attacks”, published by UGC Approved: Vidyawarta Interdisciplinary Multilingual Refereed Journal, Vol-04. Issue- 28, ISSN: 2319-9318, Dec-2018.
6. Devidas S. Thosar, “Graphical Authentication by taking profound single picture differentiate enhancer from multi-introduction pictures”,published by International Journal of Engineering Research and Management (IJERM), Vol-04. Issue- 01, ISSN: 2348-3415, 2018.
7. Devidas S.Thosar, “Review on Decentralized Access Control with Anonymous Authentication”, published by International Journal of Engineering Research and Management (IJERM), Vol-04. Issue- 01, ISSN: 2348-3415, 2018.
8. Z. Zheng, X. Liu, L. Yin, and Z. Liu, “A stroke-based textual password authentication scheme,” in Education Technology and Computer Science, 2009. ETCS’09. First International Workshop on, vol.3.IEEE, pp. 90–95,2009.
9. L. Wang, X. Chang, Z. Ren, H. Gao,X. Liu, and U. Aickelin, “Against spyware using captcha in graphical password scheme,” in 2010 24th IEEE International Conference on Advanced Information Networking and Applications. IEEE,pp.760–767, 2010.