Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

Integration of Image and Video Signature in Graphical Password Authentication System

Vaishali Ravi[1], Seema Khan P[1], Usha H Y[1], Yashashwini B N[1], Kanmani B S[1*]
[1]Department of Electronics and Communication Engineering,
School of Engineering, Dayananda Sagar University,
Bangalore, 560068, India

***Abstract*— In this study we are providing the security and authentication for the user. This paper includes two parts, Image processing using cued click point and video processing using clicked intervals, where the combination of both will generate a password for the user to login. To login its necessary that both the combination need to match. The user is allowed to select their choice of images and video for the process and it is stored in a private database so that they are not available to other users. The password generated by both image and video is hidden from both users and developers. This method is obtained for prevent unauthorized access to important and confidential data and to protect them.**

Keywords—Video signature; Image cue point, authentication.

I. INTRODUCTION

A method to provide an individual with access to the required details or object based on identity of the individual is called Authentication. We need verification at varies stages, as it is the right given to someone of any particular task depending on their designation. The traditional method used is text based password, which further has evolved to pass codes based on graphical using image, color and audio. The latest developed system is using graphical password authentication, which still have the drawback of shoulder surfing and mouse lagging. Also as few sites save password automatically like Google, or password can be traced in keypad using key logger software there is need to improve the security in the verification of the user and to ensure that any unofficial users cannot access or modify the data of another user. Each password is uniquely encrypted, which is hidden even from the developers.

II. PRESENT SYSTEM

In the present systems like text based the passwords were very hard to remember for the users so to make it easier color coded passwords came into existence. Where as in color coded authentication system there a number of colors in which user needs to select colors in some order of combination and remember it. Although it is easy to remember it is even easier for the unauthorized users to access other users because of the combinations can be tried and guessed. In the sound based graphical authentication system, a password consists of sequence of some images in which the user can select one click-point per image and a sound signature which is used to recall the password set by the user while Sign in.

III. PROPOSED SYSTEM

In this proposed system we are integrating graphical password and video signature. The password consists of sequence of some images in which user can select one click-point per image. In addition user is asked to select a Video signature corresponding to interval click point. The password for login is combination of image and video click point, user gets access to login only if it matches. When the click point doesn't match then the window closes. In this system a two level password authentication is present. It consists of an image recognition followed by a video recognition. The uniquely created password is encrypted and hidden even from the developers. Data Security and User Authentication is the basic factor for information security.

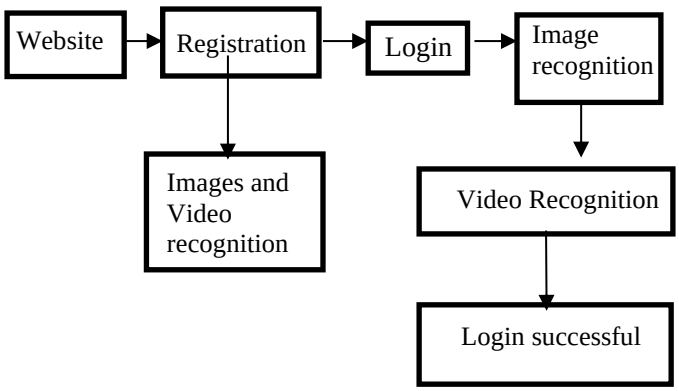

Figure 1: System block diagram

Firstly when the user wants to access the documents, they need to go to the website page. Secondly the user has to register by selecting cue points in those images according to their choice for logging in into the page. In login page they have to select the same cue points Selected during the registration process. If the points are matched then they can login successfully else the window shows a pop up saying invalid login.

IV. LITERATURE SURVEY

The observation we made from the papers we studied are mentioned below:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

"Authentication scheme for session passwords using color and images":- The scheme uses colors and user has to rate the colors in registration phase. During login phase four pair of colors and 8*8 matrixes will be displayed. As the color rating given by the user, the password will be generated. First color shows the row number and second shows column number of the grid. The drawback of this system is intersecting element is the first letter of the password. The user has to memorize the rating and order of the colors. So it is very stressful for the user. The benefit of this system is that it is flexible and simple to use. [1]

"A Graphical Password Based Authentication Based System for Mobile Devices":- A hybrid graphical password based method is directed, which is a mixture of recognition and recall based methods having many advantages as compared to existing systems and more suitable for the user. In the following paper the user draws the selected object which is then stored in the database with the specific username. Objects may be symbols, characters, shapes, simple objects etc. Then the user draws previously selected objects as his password on a touch sensitive screen with a mouse. This system performs some complicated actions like pre-processing, stroke merging. So it can be a fault of this system.[2]

"Graphical Password as an OTP":- The text based password system is a popular authentication system since olden times. It has many advantages but at the same time it has a few disadvantages too. Hence, the present graphical password techniques, is classified into four techniques as recognition based, pure recall-based, cued-recall based and hybrid based. The Hybrid system is a combination of two or more password schemes. It is used to overcome the drawbacks of single system, such as hotspot problem. The advantage of this system is it provides high authentication process. Disadvantage of this system is it's a complex and long term process.[3]

"Color Shuffling Password Based Authentication":- Authors proposed a scheme which focuses on shoulder surfing. In their system, they proposed a new click based color password scheme called Color Click Points (CCP). A password consists of a click-point per color for a sequence of colors. The next color displayed is constructed on the previous click-point. In this scheme, an improved text-based shoulder surfing resistant graphical password scheme by using colors. The benefit of this system is that it reduces the login time & it is an efficient system.[4]

"Video Authentication Using Spatio-temporal signature for surveillance System":-Authors proposed video authentication that could protect the modification to eventually increase the confidence and allow the authenticated videos as evidences in law court. The signature based video authentication system uses the histogram of oriented gradient of the selected DCT coefficients found in the frequency domain of video frames. The efficiency of our technique depends on an optimal threshold that need to use high threshold to reject all tampered and need to improve to allow compression. [5]

"Video Authentication with Self Recovery":-The authors proposed here a block-based method, the watermark payload of a block is composed of two parts: Authentication and recovery packets. The authentication packet is a digital signature with a special structure and carries the spatio-temporal position of the block. The digital signature guarantees the authenticity and integrity of the block as well as the recovery packet. On the other hand, the recovery packet contains a highly compressed version of a spatio-temporally distant block. This information enables the recovery of the distant block, upon detection of tampering by its authentication packet. A spatio-temporal interleaving scheme and a simple multiple description coding mechanism increase the probability of self-recovery by diffusing recovery information throughout the sequence. Finally, watermark payload is embedded by least significant bit modulation. [6]

"Video Authentication overview":-With the innovations and development in sophisticated video editing technology and a widespread of video information and services in our society, it is becoming increasingly significant to assure the trustworthiness of video information. Therefore in surveillance, medical and various other fields, video contents must be protected against attempt to manipulate them. Such malicious alterations could affect the decisions based on these videos. A lot of techniques are proposed by various researchers in the literature that assure the authenticity of video information in their own way. In this paper we present a brief survey on video authentication techniques with their classification. These authentication techniques are broadly classified into four categories: digital signature based techniques, watermark based techniques, intelligent techniques and other techniques. [7]

V. SOFTWARE REQUIREMENT

IDE : Visual Studio
Storage : SQL Server Database
Programming Language: C# with HTML
Supporting Application: Microsoft Silverlight

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

VI. FLOWCHART

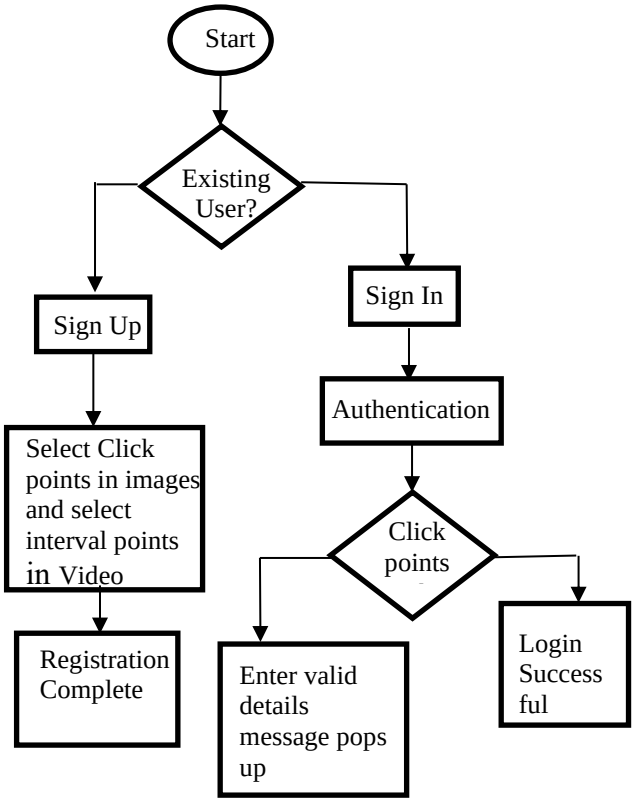

Figure 2: System Flow Chart

Firstly when the user wants to access the documents, they need to go to the website page. Secondly the user has to register by selecting cue points in those images and selecting cued intervals in video according to their Choice for logging in into the page. In login page they have to select the same cue points Selected during the registration process. If the points are matched then they can login successfully else the window shows a pop up saying invalid login. In Sign up Page the user has to register with full name, username, image cue click points and video cued intervals are saved in the data base when the user registers for the first time. If the user again tries to login then the user needs to select the same click points, then the login will be successful. If the cue points doesn't match with the cue points already saved while registering then a pop up message saying that 'invalid' valid details will be displayed. Then the user needs to again try logging in with the appropriate cue points. If the login is successful then the user gets the access to the authorized documents to download or upload for further uses. The flowchart above shows the flow of the system with image and video signature. The cue points in the image should be a picture image selected at the distinct point. The video selection should be reasonable so selection of interval is distinct and not confusing or very easy to hack. Here the combination of cue points of image and video interval points give an encrypted password for the user to login. If anyone cue selection either image or video is wrong then the user does not get an authenticated login.

VII. TEST RESULTS

The below table shows the success and failure rate for different login users.

User	Trial No	Success Rate	Failure Rate
User 1	5	10%	90%
User 2	5	70%	30%
User 3	5	40%	60%
User 4	5	90%	10%
User 5	5	50%	50%

Figure 3: Login Attempt by Various Users for image authentication

The table shows that 5 different users have tried login with 5 trials each. For User 1 the success rate was 10% while failure rate was 90%, as the user choose the cue points for the password which were random are not distinct point in the image and video hence the failure is more. While User 4 has more success rate then failure rate due to better selection of cue points in the image.

The table below shows the login for 5 different users with image and video authentication. The user 1 had a success of 10% and failure 90% with improvement and correction user 5 has a success of 80% and failure of 20% with the selection of proper cue point in image and a reasonable interval in video.

User	Trial No	Success Rate	Failure Rate
User 1	5	10%	90%
User 2	5	45%	55%
User 3	5	70%	30%
User 4	5	60%	40%
User 5	5	80%	20%

Figure 4: Login Attempt by Various Users for image and video authentication

The image should be selected such that cue point selection will be easier with distinct point in the image, and it should not be a plain or a solid color image. The video Selection Should be such that it has a reasonable interval and is not complicated to implement or remember while login.

Figure 5 shows the sign up page of the project during registration process.

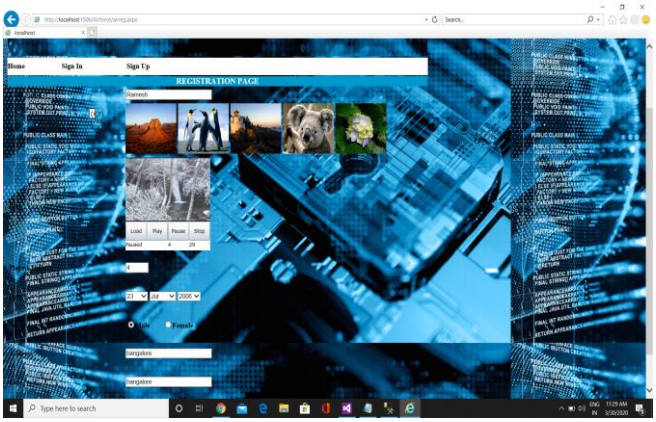

Figure 5: Sign Up page

Figure 6 shows the login page of the project consisting of image and video authentication.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

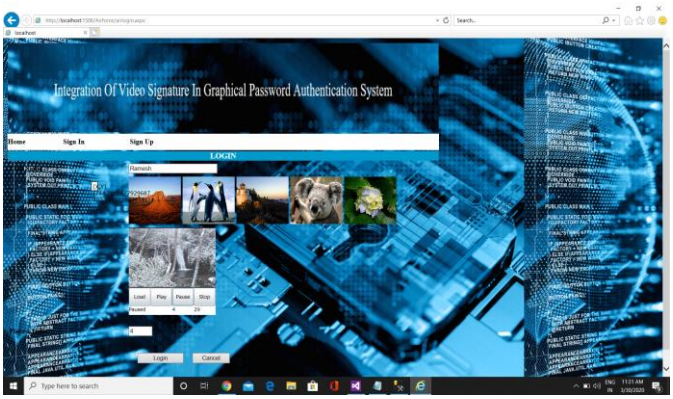

Figure 6: Login In page

Figure 7 shows the unauthorized login into the website.

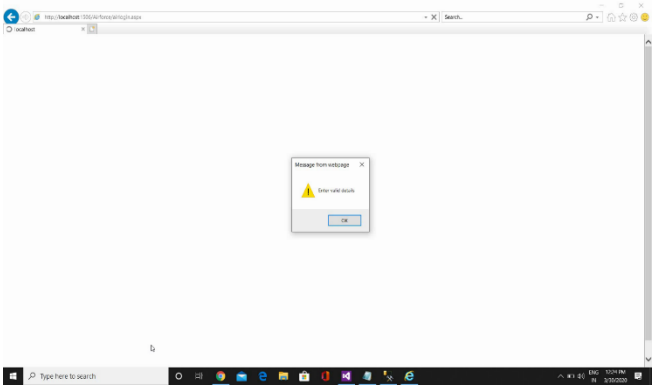

Figure 7: Unauthorized login

Figure 8 shows the authorized login into the website.

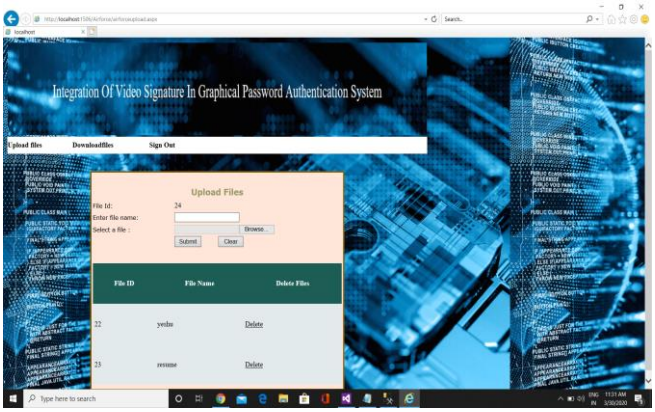

Figure 8: authorized access

VIII. CONCLUSION

We have proposed a method of password authentication which was not implemented before. The paper includes two step of authentication with image and video. The image recognition and authentication was successfully implemented and observed with overall success rate of 52% and failure rate of 48% for various users. The video authenticated was achieved partially only for few single frame.

We observed that the video authentication can be achieved by the usage of combination of software to support authentication. The dynamic nature of this project can be achieved using a more stable and supported software. Hence the complete success rate for the project so far is 64% while the failure rate is 36% for various users. The advantage of this system is that the security level is high especially for video. The video security for authentication is high and hard to crack. That makes the complete system strong against any threat. While one of the major limitations for the system is storage of data. The user here gets only two attempt to sign in using video authentication. When the user exceeds the maximum attempt the sign in page gets locked, which is an advantage and limitation as ones it locked only the authorized user can unlock after a random time. The other limitation which we observed was that the precision of cue point selection needs to be accurate even with tolerance during login.

IX. FUTURE SCOPE

The future plan for this project can be to achieve for multiframe, which can be achieved by using a combination of software to support authentication. This will improve the security and the dynamicity of the system. As most of the trends are in cloud this type of authentication can be used to protect it against cybercrime and other threat.

REFERENCES

[1] M SREELATHA, “Authentication scheme for session passwords using color and images”, proceedings of International Journal of Network Security & its applications (IJNSA), vol.3, No.3, May 2011.

[2] Er.Aman Kumar, “A Graphical Password Based Authentication Based System for Mobile Devices”, proceedings of International Journal of Computer Science and MobileComputing, Vol.3 Issue.4, April- 2014.

[3] Veena Rathanavel, “Graphical Password as an OTP”, proceedings of IJECS Volume 6Issue 1 Jan., 2017 Page No.20090-20095

[4] Aayush Dilipkumar Jain, “Color Shuffling Password Based Authentication”, proceedingsof International Journal of Engineering Science and Computing, April 2017.

[5] Teerasak Kroputaponchai, “Video Authentication Using Spatio-temporal signature for surveillance System”, *proceedings of* International Joint Conference on Computer Science and Software Engineering, July 2015.

[6] Mehmet U.Celik A, “Video Authentication with Self Recovery”, *proceedings of SPIE* Security and Watermarking of Multimedia Contents IV, Vol.4675, February 2003,pg. 531-541

[7] Saurabh Upadhyay, “Video Authentication Overview”, *proceedings of* International Journal of Computer Science & Engineering Survey (IJCSES) Vol 2, N0.4, November 2011. Pg. 75-96.

[8] Soumya K.N, “Video Authentication using Watermark and Digital Signature”, *proceedings of* International Conference on Computational Intelligence and Informatics, January 2017.