ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Secured Hybrid Authentication Schemes using Session Password and Steganography

Priti S. Katkade [1], Dr. Shubhas K. Shinde [2]

P.G. Student, Dept. of Computer Engineering, Lokmanya Tilak College of Engineering, Navi Mumbai, Maharashtra, India[1]

Professor, Dept. of Computer Engineering, Lokmanya Tilak College of Engineering, Navi Mumbai, Maharashtra, India[2]

ABSTRACT: The most common method is textual passwords that were used for authentication. Unfortunately, these passwords can be easily guessed or cracked. The next best techniques are graphical passwords**.** Since, there are many graphical password schemes that are proposed in the last decade, But most of them suffer from shoulder surfing which is also a big problem. Also, there are few graphical passwords schemes that have been proposed which are resistant to various attacks. In this paper two new authentication schemes are proposed with steganography algorithm for any transaction**.** Any authentication process gets very secure when two or three techniques used together for a system. For every login process, user input different passwords. We proposed two different shoulder surfing resistance graphical password authentication scheme methods one is AS3PAS and second is hybrid textual scheme using color code also Advanced LSB which removes the drawback of simple LSB that it supports all image format.

KEYWORDS: Advanced Scalable Shoulder-Surfing Resistant Graphical Password Authentication Scheme (AS3PAS), Hybrid Textual Authentication Scheme (using color code), Advanced Least significant Beat (LSB).

I. Introduction

Text passwords remain popular because they have several advantages. They are easy to learn to use, easy to implement, can be easily changed if they are forgotten. As Simple password and short password is easy to remember but it can be easily hacked, while random and lengthy passwords are secured but hard to remember.

To overcome these problem graphical schemes were used. In graphical password there is also problem for shoulder surfing. But here user is authenticated using session to enter the different password. Its not possible that any one technique is very strong and fully secured. We need to make transaction very strong when we used two –three techniques simultaneously. Now when literature survey was done we come to know session passwords are more secure. When the session is over then that password is of no use for next session and current session gets terminated. Session password provides more security as every time the session starts a new password is created. Also steagnography is the technique that can be implemented so that we can secure our secret data while transaction. But LSB had some limitations like not supporting all file formats also not supporting 24-bit color images.

In this paper we have removed this drawback and implemented ALSB algorithm. So, here AS3PAS scheme, hybrid color code scheme and ALSB is explained in detail how does it work. So we use hybrid authentication schemes to make the transaction very strong.

II. LITERATURE SURVEY

Sr.no	Authors Name	Method /Techniques Used	Advantages	Disadvantages
1	Dhamija and Perrig	Proposed a graphical authentication scheme where the user has to identify the pre-defined images to prove user's authenticity. In this system, the user selects a certain number of images from a set of random pictures during registration. Later, during login the user has to identify the pre selected images for authentication from a set of images[1][3]	The system is more secure than text based authentication scheme.	This system is vulnerable to shoulder-surfing
2	Jermyn	Proposed a new technique called "Draw-a-Secret" (DAS) where the user is required to re-draw the pre-defined picture on a 2D grid. If the drawing touches the same grids in the same sequence, then the user is authenticated. [2]	This system is more secure than then simple graphical authentication process.	This authentication scheme is vulnerable to shoulder surfing
3v	Syukri	Developed a technique where authentication is done by drawing user signature using a mouse. At the time of registration stage the user draws his signature with a mouse, after that the system extracts the signature area. In the verification stage it takes the user signature as input and does the normalization and then extracts the parameters of the signature.[5][6]	Drawing with mouse is not Familiar to many people, it is difficult to draw the signature in the same perimeters making it more secure.	The disadvantage of this technique is the forgery of signatures.
4	Haichang	Proposed a new shoulder-surfing resistant scheme where the user is required to draw a curve across their password images orderly rather than clicking on them directly.[7] This graphical scheme combines DAS and Story schemes to provide authenticity to the user	This authentication process is more secure because its shoulder-surfing resistant scheme	This scheme is complicated for the user of the system.
5	Wiedenback	Describes a graphical password entry scheme using convex hull method towards Shoulder Surfing attacks. A user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects.[4]	In order to make the password hard to guess large number of objects can be used making it indistinguishable objects to be more secure.	If fewer objects used it may lead to a smaller password space, since the resulting convex hull can be large.
6	Zhao and Li	Proposed a shoulder-surfing resistant	It has high level	It takes long time for

DOI: 10.15680/IJIRCCE.2016. 0404225

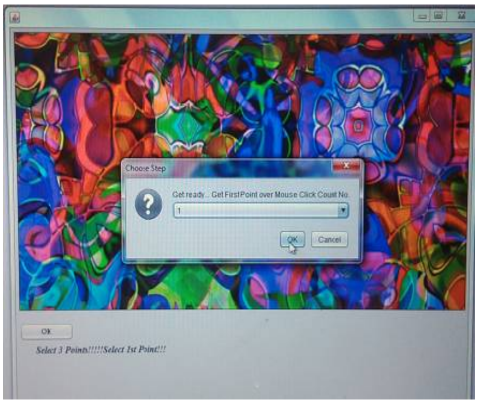
		scheme “S3PAS”. The main idea of the scheme is as follows. In the login stage, they must find their original text passwords in the login image and click inside the invisible triangle region.[2]	security since Protected by shoulder-surfing , hidden camera, and spyware attacks.	login process.
7	Zheng	Designed a hybrid password scheme based on shape and text. The basic concept is mapping shape to text with strokes of the shape and a grid with text.[5]	The scheme has salient features as a secure system for authentication immune to Shoulder-surfing, hidden camera and brute force attacks.	The shapes chosen by the user may have normal meaning, the attacker will have more chance to attack the password.

TABLE 1: DIFFERENT GRAPHICAL AUTHENTICATION TECHNIQUES.

III. PROPOSED SYSTEM

Graphical based password authentication systems are now more secure than text based. So, after literature survey on all graphical based schemes we decided to make s3pas scheme more advanced. So its future scope was to implement s3pas totally by graphical way instead of printable pass character and to implement hybrid authentication scheme using color code. Also advanced LSB algorithm is used in a system to provide more secure authentication. So for any transaction when all three schemes used together make a system more secure. So let’s discuss all the three (AS3PAS, hybrid textual and advanced LSB) authentication techniques briefly.

1. **Advanced Scalable Shoulder-Surfing Resistant Graphical Password Authentication Scheme (AS3PAS):** In the proposed system the user has to create its own region in AS3PAS. The smaller the region the security is more. Clicking on three times on a given complicated image. During registration process the user is provided with the complicated images. What user has to do is, he has to click on image three times creating a triangular region.

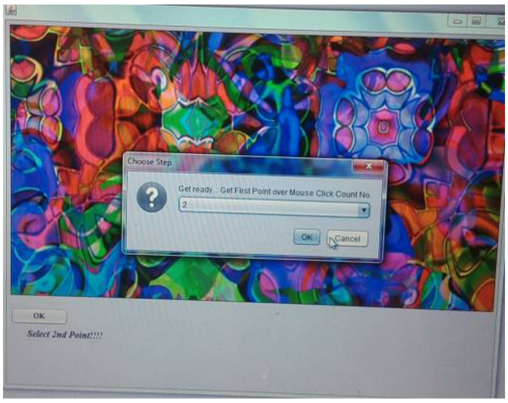


Get ready... Get FirstPoint over Mouse Click Count No

1

Select 3 Points!!!!!Select 1st Point!!!

Figure 1: user selects 1st point while registration.



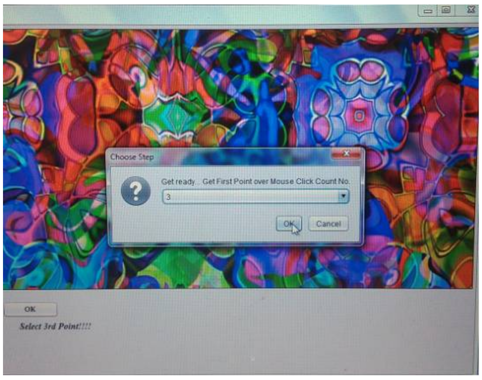
Get ready... Get First Point over Mouse Click Count No

2

Select 2nd Point!!!!

Figure 2: user selects 2nd point while registration.

DOI: 10.15680/IJIRCCE.2016. 0404225

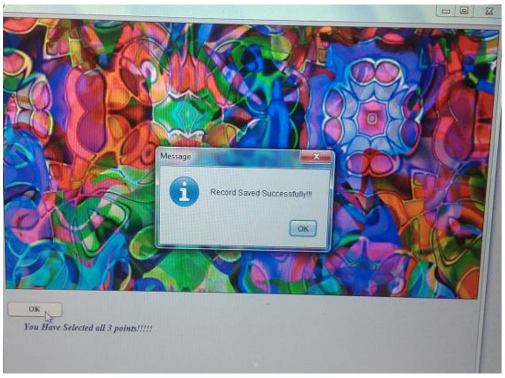


Choose Step

Get ready... Get First Point over Mouse Click Count No.

3

Select 3rd Point!!!!



Message

Record Saved Successfully!!!

You Have Selected all 3 points!!!!!

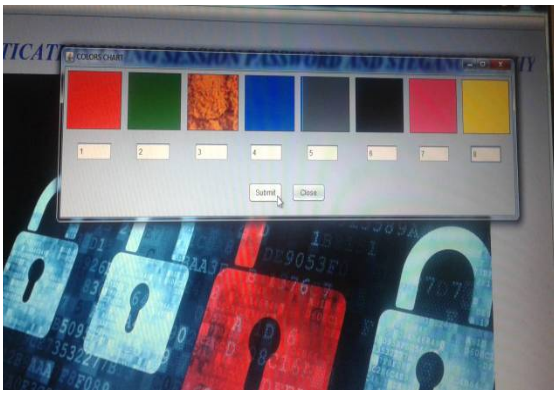
Figure 3: user selects 3^{rd} point while registrations

Figure 4: user's record saved successfully

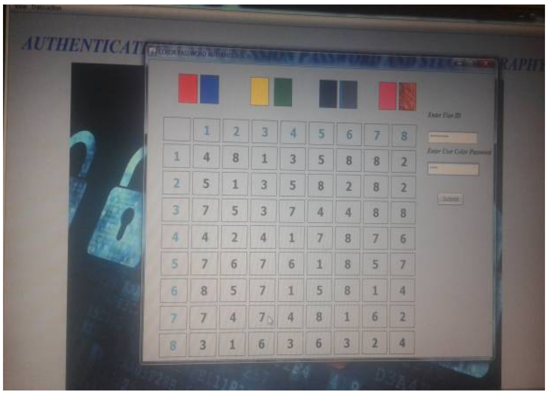
Now during logging process the valid user will click inside that region all the three times to get authenticate successfully. Cracker or invalid user will try to click on image but probability of clicking inside the region three times is very low and exits from the system if attempts exceed making system more secure. AS3PAS generates the login image locally and transmits the image specification i.e. coordinates of image instead of the entire image pixel-by-pixel from clients to servers, which greatly reduces communication overheads and authentication time. AS3PAS can be used in a high capability system to provide high level security by "Change image" technology. In that image will be changed if a user fails in clicking the correct areas, or inputs wrong session passwords for more than a certain no. of times.

2. Hybrid Textual Authentication Scheme (using color code)

During registration, user should rate colors as shown in figure 5. The User should rate colors from 1 to 8 and he can remember it in any sequence. During the login phase, when the user enters his username an interface is displayed. The login interface consists of grid of size 8×8. This grid contains digits 1-8 placed randomly in grid cells. The interface also contains strips of color as shown in figure 6. The color grid consists of 4 pairs of colors. Each pair of color represents the row and the column of the grid.



1	2	3	4	5	6	7	8



	1	2	3	4	5	6	7	8
1	4	8	1	3	5	8	8	2
2	5	1	3	5	8	2	8	2
3	7	5	3	7	4	4	8	8
4	4	2	4	1	7	8	7	6
5	7	6	7	6	1	8	5	7
6	8	5	7	1	5	8	1	4
7	7	4	7	4	8	1	6	2
8	3	1	6	3	6	3	2	4

Enter User ID

Enter User Color Password

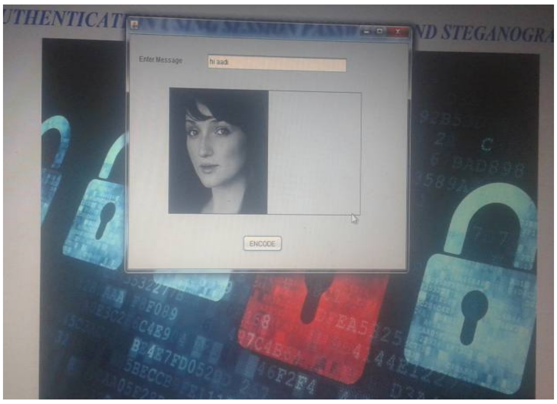
Figure 5: user rates the color while registration.

Figure 6: user enters his session password while logging.

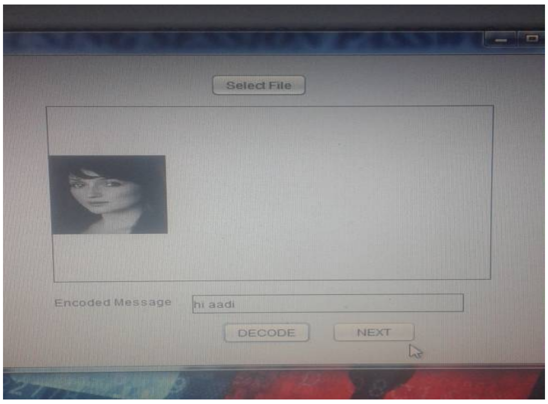
Figure 6 shows the login interface having the color grid and number grid of 8 x 8 having numbers 1 to 8 randomly placed in the grid. Session password is obtained depending on the ratings given by user. The first color represents row and second represents column of the number grid of every pair in color grid.[1] The number in the intersection of the row and column of the grid is part of the session password. Consider the figure ratings and figure login interface for demonstration. The first pair has red and Blue colors. The red color rating is 1 and blue color rating is 4. So the first letter of session password is 1st row and 4th column intersecting element i.e 3. The same method is followed for other pairs of colors. For every login, both the number grid and the color grid get randomizes so the session password changes for every session.[3]

3. Advanced Least significant Beat (LSB).

The word "Steganography" is of Greek origin and means "covered or hidden writing". Some algorithms are available for steganography purpose but they have some limitations like not supporting all the formats of file, not supporting to color image especially 24-bit etc. This proposed algorithm ALSB (Advance Least Significant Bit) is different from LSB algorithm and works especially for 24-bit color image and all image formats.



Enter Message: hi aadi



Encoded Message: hi aadi

Figure 7: sender enters his secret message & encodes in the image. Figure 8: valid receiver decodes it to get secret message.

As Shown in fig 7 here we used Advanced LSB so all types of image format can be used. In fig. Sender sends his secret message which is encoded in the image and the image is saved again by another name. Now, at the receiver side the only valid user knows by which name the image is saved since sender will let him know the saved image name. So user will decode that image and will receive secret message as shown in fig 8.

Working of proposed algorithm:

In this proposed algorithm,

Step 1: first remove last four bits of pixel's matrix of cover image (For R and G matrix) For Example: Let us consider given a row of m x n matrix. Now ANDing with 0XF0 we can remove last four bits (which contains negligible information) to store the data of secret file. After that obtain the matrix of secret message. The secret file can be a image file (.jpg,.jpeg,.bmp etc.) [8]which is to be converted into binary form. We can obtain 8 bit data which needs to be converted into nibble, so that we can store it in the lower nibble of the pixel[8]

Step 2: first take the matrix of secret message m1xn1 then by applying AND with 0XFO.

Step 3: .Now apply right shift 4 times to the resultant Nibble.

Step 4: To obtain Stego image the new row of m x n matrix of R or G is ORed with a row of m1 x n1 matrix of the Secret file.

Step 5: In Resultant matrix 4-bits of cover image and 4-bits of secret message are stored.

IV. Analysis And Discussion On Proposed System

1 Shoulder Surfing Resistant

After an attacker observes or records one click on the screen from the user, the attacker cannot gain enough information of the user's password. That is it's not impossible to click within same region of valid user. This shows that a shoulder-surfing attack is mostly not possible.

2 Brute Forces Search Resistant

The primary reason is that we adopt "change image" technology. If a user fails in clicking in the correct region, or a user inputs wrong passwords for 3 times, the system automatically changes the complicated login image. By doing this, there is no way for attackers to adopt brute-force search to break the password because the password will change after changing the image.

So, all the attempts toward the previous complicated login image become useless. The attacker has to start a new search in the new image. Therefore, we argue that "change image" technique makes AS3PAS immune to the brute-force search. [2]

3. Social engineering

Graphical passwords are not easy way to share the passwords with each other For example; it is very difficult to give away graphical passwords over the phone. Setting up a phishing web site to obtain graphical passwords would be more time consuming.

4. Dictionary attacks

Since graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords

V. CONCLUSION

Thus after literature survey we decided to use AS3PAS, color code and advanced LSB algorithm to provide a user more secure authenticated transaction. This Advanced all three techniques are implemented and results are obtained which is shown in above figures.This Scheme can also be used to develop as windows application folder locker or as an external gateway authentication to connect the application to a database or an external embedded device.

References

1. Priyanka S. Kedar and Vrunda Bhusari., "Using PBKDF2 Pair & Hybrid technique for Authentication", International Journal of Emerging Research in Management &Technology, Volume-3, Issue-5, May 2014.
2. H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme", in 21st International Conference on Advanced Information Networking and Applications Workshops, vol. 2. pp. 467-472, Canada, May-2007.
3. D. Aruna Kumari, "Implementation of Network Based Authentication Mechanisms", Advances in Information Technology and Management, volume-1, Issue-.2, April- 2012.
4. S.Balaji, Lakshmi.A, V.Revanth, M.Saragini, V.Venkateswara Reddy., "Authentication Techniques For Engendering Session Passwords With Colors And Text", Advances in Information Technology and Management, Vol. 1, Issue- 02, May-2012.
5. Vaishnavi panchal, Chandan p. patil " Authentication schemes for session password", International Journal of Scientific & Engineering Research, Volume 4, Issue3, March-2013
6. Z. Zheng, X. Liu, L. Yin, Z. Liu., "A Hybrid password authentication scheme based on shape and text" Journal of Computers, vol.5, Issue-5 May 2010.
7. V. Bhusari., "Graphical Authentication Based Techniques", International Journal of Scientific and Research Publications, Volume 3, Issue 7, July 2013.
8. Chintan M. Mahant, Samip A. Patel, Makhduma F. Saiyad, Krunal N. Patel, "A New Perspective in Steganography Technique", International Journal of Computer Science and Information Technologies, Vol. 5 , Issue-1, May2014,

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

BIOGRAPHY

	Priti S. Katkade is a PG student in Dept. of Computer Engineering at Lokmanya Tilak College of Engineering, Navi Mumbai, India. Her area of interest is networking and security. Also participated in AVISHKAR Research convention 2016 at district Level.
	Dr. Subhash K. Shinde is working as professor in Dept. of Computer Engineering at Lokmanya Tilak College of Engineering, Navi Mumbai, India. He is having academic experience of 16 years at UG and PG level courses of University of Mumbai. He has guided many projects at UG and PG level. His areas of interest are Data Mining, Database, Computer Network

DOI: 10.15680/IJIRCCE.2016. 0404225