A SECURE GRAPHICAL AUTHENTICATION SYSTEM USING WATERMARK EMBEDDING

SREYA PRAKASH
M-TECH , DEPT OF CSE
Malabar Institute of Technology,
Anjarakandy.
sreyaprakash0@gmail.com

.

SREELAKSHMY M K
Asst.Proffesor, DEPT OF CSE
Malabar Institute Technology,
Anjarakandy.
mksreelakshmy@gmail.com

Abstract

Nowadays the most popular method for User Authentication is using Textual Password. This method has many drawbacks like dictionary attack, brute force attack etc. A secure text based password must be made using a combination of uppercase, lowercase, and special characters. Users have a tendency to choose weak text-based passwords, which are short and easy to remember. To overcome the drawbacks of text-based passwords, many picture-based passwords have been proposed. Picture based password systems often suffer from several problems, one of them is the shoulder surfing attack, ie ,images that users choose as password are both easy for an attacker to watch by snooping over shoulders or by using a camera to record input and also predictable. An authentication system called PassMatrix is used to overcome the shoulder surfing attack. User has to choose images as their password during the registration phase and choose a pass-square per image. To secure the pass-images from the attackers, Generic Visible Watermark Embedding technique is used to blend a cover image and a pass-image..This method can be extended to secure web applications by using QR code.

1. Introduction

User authentication based on passwords is used in many applications for security and privacy. Comprised of numbers and upper and lower case letters, textual passwords are strong enough to resist against brute force attacks. They are very easy to implement and use. Alphanumeric passwords are required to satisfy two requirements. They should be easy to memorize and at the same time they should be very hard to guess. Various graphical password authentication schemes were developed to overcome the problems and weaknesses associated with textual passwords. Humans have a better ability to memorize the images with long-term memory than verbal representations. However, most of these image based passwords are vulnerable to shoulder surfing attacks.

A secure graphical authentication system called Passmatrix [1] is used that safeguard the users from becoming the victims of shoulder surfing attacks,while inputting the passwords in public .A login indicator is randomly generated for each pass-image and will be useless after the session ends. The login indicator provides security against shoulder surfing attacks because users use a pointer to point to the position of their passwords rather than clicking on the password image directly .If the pass-image is faintly printed on a cover image, the legitimate user who is closer to the monitor screen can see the pass-image ,but someone who is far away from the screen cannot identify the pass-image. Generic Visible Watermark Embedding algorithm is used to blend a cover image with a pass-image. Moreover, because images with less independent objects usually suffer more on the hot-spot problem, carefully selecting images with rich objects can alleviate the hot-spot based random guess attacks.This method can also be extended to secure login of web applications in computers by using QR code.

2. RELATED WORK

Tsung-Yuan et al. [2] proposed a novel method for generic visible watermarking with a capability of lossless image recovery is proposed. The method is based on the use of deterministic one-to-one compound mappings of image pixel values for overlaying a variety of visible watermarks of arbitrary sizes on cover images. The compound mappings are proved to be reversible, which allows for lossless recovery of original images from watermarked images. The mappings may be adjusted to yield pixel values close to those of desired visible watermarks. Different types of visible watermarks, including opaque monochrome and translucent full color ones, are embedded as applications of the proposed generic approach. A two-fold monotonically increasing compound mapping is created and proved to yield more distinctive visible watermarks in the watermarked image.

Sarosh Umar et al. [3]proposed a a novel recognition-based image authentication system called Select-to- Spawn which is secure, robust and convenient to use.This system allows the user to create a graphical password by first selecting an initial image from a collection of available pictures.The selected image will be opened in a new window in which the picture is furthur dvided into 4x4 grid or 16 rectangular parts. The grid lines can be highlighted if one desires to facilitate ease of selection but as a default case they are rendered invisible. The user can then click on any one of the grid cell.This further spawns into a new image with invisible grid ines dividing it into 16 cells.Selecting any cell of the image spawns yet another picture with invisible grid lines. This process of selection may progress depending upon the user and each image selected by the user becomes the part of the password.

Susan Wiedenbeck et al. [4]proposed a Convex Hull Click Scheme (CHC). CHC is based on several rounds of challenge-response authentication.icons. The icons are displayed using only the image without text. To create a password the user chooses several icons from the portfolio to be his or her pass-icons.

Andrew Lim et al. [5] proposed a new method which is resistant to shouldersurfing attack by using a false image in authentication step. Like other authentication
methods, the graphical password consisted of two steps, registration and authentication. In the registration step, users select some images from different categories or produce a graphical image as his password. Later on, in the authentication step, he needs to select the correct images or re-draw the graphical password which is used by him.

3. EXISTING SYSTEM

In PassMatrix, the password consists of one pass-square per pass-image for a sequence of n images. The number of images is user-defined. A login indicator will be randomly generated for each pass-image and it will be useless after the session terminates. To protect against the shoulder surfing attack, the indicator is not shown until the hand touches the screen and will vanish immediately when the hand of the user leaves the screen. There are two scroll bars: a horizontal bar with a sequence of letters and a vertical bar with a sequence of numbers. Users can fling either bar using their fingers to shift one character at a time.They are used to align the one-time indicator with the pass-square in each passimage during the authentication phase.In order to obfuscate and thus hide the alignment patterns from observers, randomly shuffled the elements on both bars in each pass-image and let users shift them to the right position.

4. PROBLEM DEFINITION

The graphical passwords are mostly vulnerable to shoulder surfing attcks. In Passmatrix, the pass-image is displayed on the screen and the user can easily identify their password image. PassMatrix is vulnerable to random guess attacks based on hot-spot analyzing.This method is only implemented in mobile devices for screenlocking.

5. PROPOSED SYSTEM

5.1 Registration

Proposed system allows the user to create a graphical password by selecting an image as their password from a collection of shown pictures.After selecting the password image , the user need to choose one grid as the password. The choosen image by the user is watermarked on a cover image using Generic Visible Watermark Embedding technique. The method is based on the use of one-to-one compound mappings of pixel values of the image for overlaying different types of visible watermarks of arbitrary sizes on cover images.

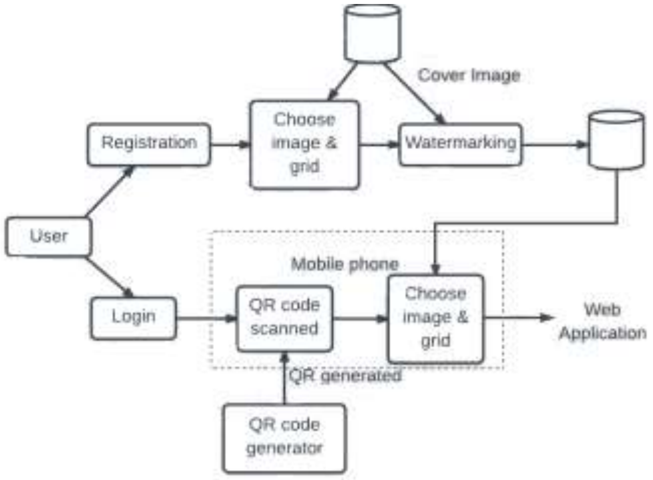


Fig: System Architecture

5.2 Login

At the time of login by the user, after entering the user deatils a QR Code will be generated on the computer screen. User has to scan that generated QR code using his QR scanner embedded mobile phone. After successfulr scanning, a collection of images will be appeared in the screen of the registered mobile phone of the user. User has to select the image that he had choosen as the password image. After choosing correct password image ,the watermarked image that are divided into multiple grids will be appeared on the screen of the mobile phone of the user. User has to choose the correct grid that he has already registered in the watermarked image during the registration phase.

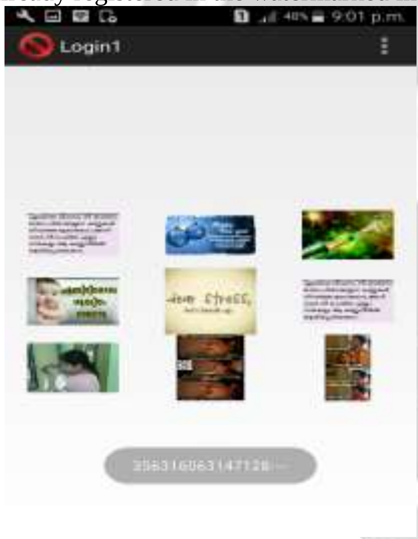
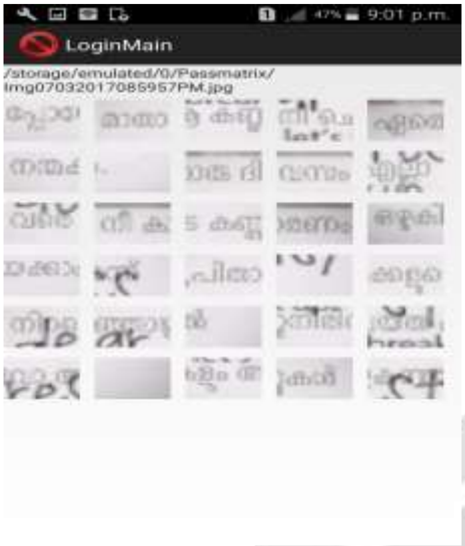


Fig: Password Image Selection Page



/storage/emulated/0/Passmatrix/
Img07032017085957PM.jpg

Fig: Password Grid Choosing Page

6. CONCLUSION

Graphical password authentication is the method that uses images as passwords rather than using alphanumeric characters. They are very attractive because humans have better ability to remember images better than words. In this project a secure graphical authentication system named PassMatrix is proposed that safeguards the users from becoming victims of shoulder surfing attacks when inputting passwords in public. User has to choose their password image that they already registered from a collection of shown pictures. To hide the pass-image from the attackers Generic Visible Watermark Embedding algorithm is used to blend a cover image and the password image. It is easy for legitimate users to recognize their password image in the watermarked image. On the other hand, it will be very diffcult for attackers to identify the password image.This method is extended to secure web applications by using QR Code.

References

[1] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh, and Chia-Yun Cheng. A shoulder surfing resistant graphical authentication system

[2] Tsung-Yuan Liu and Wen-Hsiang Tsai. Generic Lossless visible watermarking a new approach. IEEE transactions on image processing, 19(5):1224–1235, 2010.

[3] Pradyumn Nand, Prashast Kumar Singh, Joy Aneja, and Yash Dhingra. Prevention of shoulder surfing attack using randomized square matrix virtual keyboard.In Computer Engineering and Applications (ICACEA),2015 International Conference on Advances in, pages 916–920. IEEE, 2015.

[4]. Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, and Jean-Camille Birget. Design and evaluation of a shoulder-Surfing resistant graphical password scheme. In Proceedings of the working conference on Advanced visual interfaces, pages 177– 184. ACM, 2006.

[5] Andrew Lim Chee Yeung, Bryan Lee Weng Wai, Cheng Hao Fung, Fiza Mughal, and Vahab Iranmanesh. Graphical password: Shouldersurfing resistant using falsification. In 2015 9th Malaysian Software Engineering Conference (MySEC), pages 145–148. IEEE, 2015.

[6] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu,

And Uwe Aickelin. A new graphical password scheme resistant to shouldersurfing. In Cyberworlds (CW), 2010 International Conference on, pages 194–199. IEEE, 2010.

[7] Taiki Fukiage, Takeshi Oishi, and Katsushi Ikeuchi Visibility -based blending for real-time applications. In Mixed and Augmented Reality (ISMAR), 2014 IEEE International Symposium on, pages 63–72. IEEE, 2014.

[8] Yufeng Tang, Dongqing Zou, Feng Ding, Jianwei Li, and Xiaowu Chen. Lle coordinates for image blending. In Virtual Reality and Visualization (ICVRV), 2014 International Conference on, pages 278–283. IEEE, 2014.

[9] S Ramya and T Mercy Christial. Restoration of blurred images using blind deconvolution algorithm. In Emerging Trends in Electrical and Computer Technology (ICETECT), 2011 International Conference on, pages 496–499. IEEE, 2011.

[10] Tsung-Yuan Liu and Wen-Hsiang Tsai. Generic lossless visible watermarking a new approach. IEEE transactions on image processing, 19(5):1224–1235, 2010.

[11] Mohammad Sarosh Umar and Mohammad Qasim Rafiq. Select to- spawn: A novel recognition-based graphical user Authentication scheme. In Signal Processing, Computing and Control (ISPCC), 2012 IEEE International Conference on, pages 1–5. IEEE, 2012.