ISSN 2047-3338

A Novel Approach for Script Based Password Generation by using Image Partitioning

Saba Khan[1], Dr. Deepak Arora[1] and Mohd. Zeeshan[1]

[1]Department of Computer Science and Engineering, ASET, Amity University, Lucknow, India

***Abstract*— With increasing demand of security, ample of security measures and techniques have been proposed in the literature. Text or password based authentication can be easily compromised with few finger strokes or attacks. Image-based-authentication (I.B.A.) is a good alternative since images are easier to recall than alphanumeric passwords. Therefore, in this paper a novel approach has been proposed which supports script provided by its user to generate password by using image partitioning. It increases the extent of security and provides a user-friendly environment. It displays a set of image blocks that are randomly arranged. The user has to rearrange the image set by moving some blocks at their correct place according to his script, in order to get successful access.**

***Index Terms*— Partitioning, I.B.A, Security, Techniques and Image**

I. Introduction

SECURITY plays a vital role in protecting resources against unauthorized access. There are numerous ways of authenticating a person. Authentication systems based on text passwords are widely used but they can be easily compromised. Moreover they are difficult to remember. On contrary, images are easier to remember and secondly the image based authentication system is less vulnerable to attacks. For over a century, psychology studies have recognized that human brain's have superior memory for recognizing and recalling visual information as compared to verbal or textual information [10]. Hence, this has been proved by psychologists that pictures are easier to remember than words or numbers [9]. Numerous authentication processes has been proposed in the literature. Some of them failed to provide high security while others are not user friendly.

In this paper a secure as well as user friendly authentication method i.e., a script based password generation by using image partitioning has been proposed. At the login time, the user will be presented with set of randomly arranged image blocks. He has to move few image blocks to their correct location according to his script, as he has set the image grid at the Password generation phase, after which he is allowed to get access. The proposed approach can also be deployed in real-time systems such as bank lockers, secret door entry, confidential systems etc.

II. Literature Survey

Several Image Based Authentication systems have been proposed in literature. Dhamija and Perrig proposed a system D´ej`a Vu through which a person authenticates himself through her ability to recognize images which he has seen before i.e. at registration time. It requires identification of '*p*' random-art images, out of image set containing *n* images [1]. Takada et al. proposed a scheme Awase-E in which he introduced user's secret personal pictures as their pass images, the authentication process contains several verification stages including a stage with 'no pass image' [2]. Richard E Newman et al. presents the basic Image Based Authentication System and analyzes the technique in which user has to select his set of pass images in several rounds. He also worked on tempest and other forms of attack and suggested measures to mitigate them [3].

Surabhi Anand et al. proposed a 3-level security approach, involves text based password authentication at Level 1, Image Based Authentication at Level 2 (which contains several difficulty levels), and automatically generated one-time password (which will be received through email to the authentic user) at Level 3 [4]. Nitin et al. Presents Image Based Authentication system which is encapsulated in Kerberos Protocol, Version 5, and hence provides secure authentication tool to work on [5]. Md. Asraful Haque et al. suggested a hybrid authentication scheme combining graphical i.e., image and text passwords into a unit.

User authentication employed two steps to increase the security. In this approach, firstly the user has to authenticate himself by selecting his set of predefined pass-images, then in second round he will be presented with pre-selected image on that image he has to click on predefined P.O.I. (Point of Interest) and enter the text password [6]. Himika Parmar et al. invented an authentication system that is image based and which eliminates the need for textual passwords. Using the instant messaging service (e-mail) available in the Internet, user will obtain the One Time Password (OTP) after image based authentication. This OTP then can be used by the authentic user to access their accounts or data [7]. Pramod Verma gave an approach, in which the user not only chooses image as a password or key during the registration process, but also clicks on various different regions on the image to generate an additional key or password. This additional key is in the form of a sequence of colors that corresponds to the clicked areas. In essence, the user chooses a color sequence after selecting his image as a password [8].

III. Proposed work

In this paper a novel image-based-authentication framework has been proposed that exploits high security. Since images are easier to remember than the text based passwords, this approach is user-friendly as well. In this paper at the time of login, a matrix of randomly generated image blocks is presented to the user, which has to be arranged correctly according to user's script(which he invents in his mind) to gain access.

A. Architecture

It consists of two phases namely Password Generation phase and login Phase. Password generation phase requires user to register his details such as username, e-mail id etc., and generation of password through his script while login phase requires user to authenticate him by clearing Image Based Authentication level. The basic working within these two phases is shown in figure 1 given below with the help of a flow-diagram:

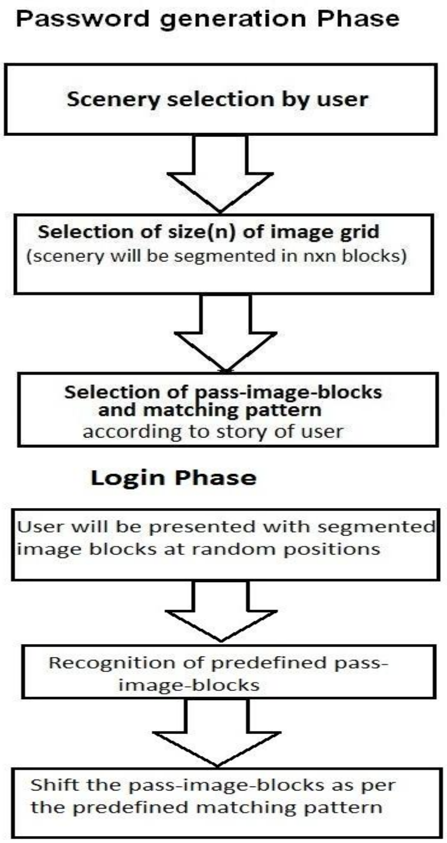

Password generation Phase
Scenery selection by user
Selection of size(n) of image grid
(scenery will be segmented in nxn blocks)
Selection of pass-image-blocks and matching pattern according to story of user
Login Phase
User will be presented with segmented image blocks at random positions
Recognition of predefined pass-image-blocks
Shift the pass-image-blocks as per the predefined matching pattern

Fig. 1: flow-diagram that shows working done by user in Password generation phase & Login phase

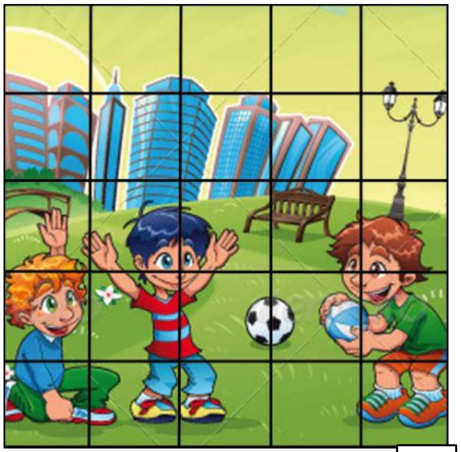
B. Two Phases

The adopted approach is described below:

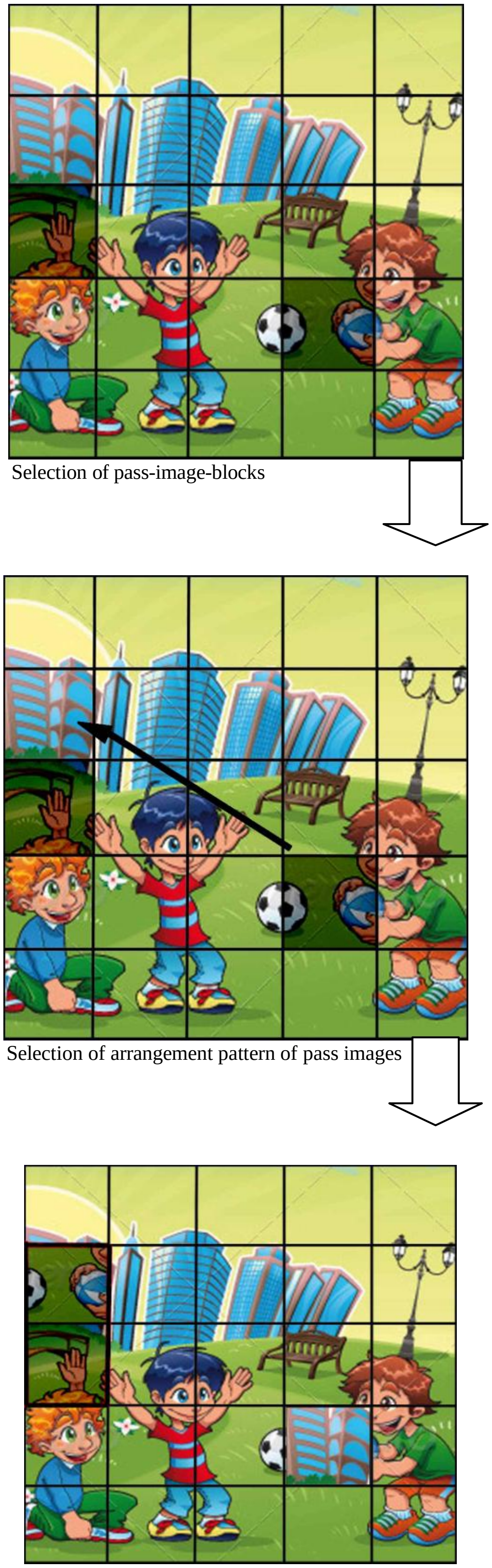
1) Password generation phase

In the Password generation phase, after registering personal details, the user has to select scenery which contains various different objects (like ball, tree, hut, boy, sun, bird etc.), then the user should chose the size (*nxn)* in which he has to partition the original scenery into the image-grid. Keeping the script in his mind; the size will be chosen by the user that perfectly fits the objects in the scenery into separate image-blocks. Now, the scenery will get divided in form of image grid or matrix (of size *nxn*), as shown in figure 2. Higher the size of matrix more will be the number of image-blocks, hence higher will be the security. In the next-step, the user has to select his pass images and the pattern in which he want the images to be matched according to his script, in order to form a password. For e.g.: suppose he makes a script that "a boy kicks a ball and the ball reached at the head of another boy", now he selects the image block of a ball to be placed at the top of the boy's head. Hence, the ball and the boy's head will serve as his pass image blocks and their top-bottom alignment will be the original pattern.

Original Scenery selected by user



Segmented image after selection of size nxn (here 5x5) by user



Selection of pass-image-blocks

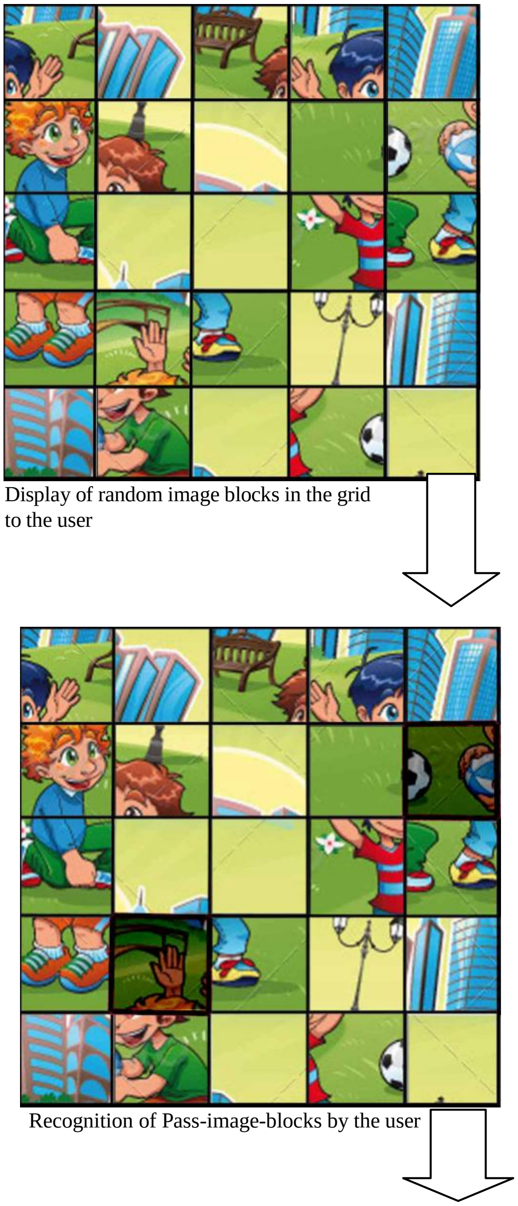
Selection of arrangement pattern of pass images

Setting of the password

Fig. 2: Sequence of activities done during Password generation phase

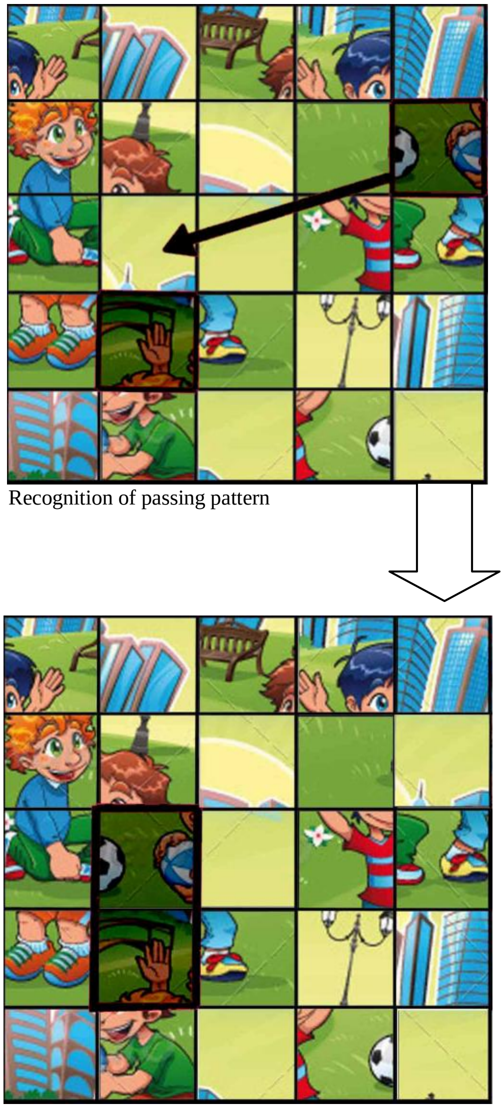
2) Login Phase

At the login Phase, the system displays a set of block-wise randomly arranged pieces of scenery in the size as defined by the user at Password generation phase. The user has to firstly observe where his pass-image-blocks are and how to arrange them in correct pattern (i.e. which image block is to be moved at which location), now the user must select and arrange his pass-image-blocks in predefined pattern i.e. according to the script in his mind as shown in figure 3. If the pass-image-blocks and their selected pattern are matched correct, the user can successfully login or access his secret information or account; otherwise his access will be denied. It provides high security as it will be too complex for an intruder to guess the pass-images and their pattern right away.



Display of random image blocks in the grid to the user

Recognition of Pass-image-blocks by the user



Recognition of passing pattern

Matching of pass-image-blocks in their predefined pattern

Fig. 3: Sequence of activities done during the login phase

IV. Security Issues

The prime objective of our proposal is to provide a highly secure and user-friendly approach which can be employed in real-world. The sole authentication criterion in our proposal depends on the image grid which consists of piece of images of the selected scenery. Now, the whole security depends on the question that which block is moved and replaced so that the two or more pass-images form a required pattern. So the pass-images and the pattern together form a password. Greater the size of image-grid, stronger will be the password.

A. *Attacker's Complexity Analysis*

Every image grid of size '*nxn*' will

- Consists of 4 corner image blocks and every corner block has 3 adjacent blocks.
- Consists of 4(*n*-2) blocks each with 5 adjacent blocks.
- Consists of (*n*-2)(*n*-2) blocks each with 8 adjacent blocks.

If an attacker randomly selects one block and try all possible combination of this block with other blocks in all possible ways(5,3,8), similarly he continues the process with other blocks as well so it form a series like:

$$8(n^2-1) + 5(n^2-2) + 8(n^2-3) + 3(n^2-4) + 5(n^2-5) +\ldots \qquad (1)$$

Hence a function with order O(n^2) is generated.

Therefore, If an attacker randomly selects an image block and tries to place it with other blocks at different location then a series or a polynomial function of degree 2 will be generated, i.e. the complexity of the function will be O(n^2). Hence the proposed approach is strong because n^2 grows faster in comparison to *n*, therefore for large values of n the system is so complex for an attacker that he can't get the pass-image and their associated pattern right away.

V. Attacks and Countermeasures

Image Based Authentication is a valid alternative to text based password schemes. The proposed approach is made so that it can be prevented from various attacks. Below we discuss some attack scenarios and their counter measures.

A. *Keystroke logging Attack*

In the proposed approach, keystroke logging attack can be prevented as user does not have to type the password. And at screen, just by logging the mouse coordinates will not be helpful for the intruder as the image blocks will get display at random location every-time the user log-in.

B. *Brute force Attack*

In our proposal, the brute force attack can also be prevented as there is no chance of guessing the pass images as there will be several objects in one scenery and that too will be divide into numerous pieces according to the choice of size of grid by user. If in extreme case, any intruder guesses the pass image, he has to try numerous combinations to select the next pass-image and right pattern in which they should be arranged.

C. *Shoulder Surfing Attack*

This is one of the most prominent forms of attack. If any attacker is peeping out the activity of user from his back then too he can't get the correct password because there will be numerous image blocks out of which only one or two image blocks will be moved, so the attacker will get confused and can't guess all pass-images and their corresponding pattern. Moreover, each time the user login, the image-blocks will be displayed randomly in the grid.

VI. Result and Analysis

The proposed concept of script based password generation by using image partitioning, undoubtedly provides secure and user friendly environment. There are some points which should be kept in mind while employing this in real-time systems:

- User should select the scenery with too many objects. Higher the no. of objects, higher the no. of stories that can be made and complex will be the image grid for an intruder.
- Higher the size of the grid higher will be the security, so user should select the grid with large size.
- User must remember the script to arrange the pass-images in right pattern.
- User must employ two or more than two pass-image-blocks to set the password.

Number of tests has been performed to determine the suitability of the given approach. In each case, the chances of pass-images and their corresponding pattern to be compromised comes out in power of *n* i.e., the complexity comes out in order of O(n^2) which is too high.

VII. Conclusion and Future Scope

In this paper a novel concept of script based password generation by using image partitioning, has been proposed. This technique of authentication adopted is completely unique and innovative. Moreover, it gives a secure and user friendly approach. In this paper, 2 pass-images are taken; user can involve more than 2 pass-images to increase the security. The proposed idea can be easily employed in real-time systems such as bank lockers, secret door entry, accessing confidential data etc. Many improvements can be made to enhance the security of given approach. In future, not only more features could be added but the system can also be made more customizable.

Acknowledgment

We would like to thank respected Mr. Aseem Chauhan, Chancellor, Amity University, Lucknow and Maj. Gen. K.K. Ohri AVSM (Retd.), Pro.Vice-Chancellor, Amity University, Lucknow for providing excellent facilities in university campus and their encouragement and advice. We would also like to pay regards to Prof. S.T.H. Abidi, Director and Brig. U. K. Chopra, Deputy Director, Amity University, Lucknow for their valuable feedback.

References

[1] Rachna Dhamija and Adrian Perrig, D´ej`a Vu: A User Study Using Images for Authentication, Proc. 9th Usenix Security Symposium, August 2000.

[2] Tetsuji TAKADA, Takehito ONUKI and Hideki KOIKE, Awase-E: Recognition-based Image Authentication Scheme Using Users' Personal Photographs, ©2006 IEEE.

[3] Richard E. Newman, Piyush Harsh, and Prashant Jayaraman, Security Analysis of and Proposal For Image-Based Authentication, ©2005 IEEE.

[4] Surabhi Anand, Priya Jain, Nitin and Ravi Rastogi, Security Analysis and Implementation of 3-Level Security System Using Image Based Authentication, ©2012 IEEE.

[5] Nitin, Durg Singh Chauhan, Vivek Kumar Sehgal, On a Software Architecture of JUIT–Image Based Authentication System, © 2008 IEEE.

[6] Md. Asraful Haque, Babbar Imam, Nesar Ahmad, 2-Round Hybrid Password Scheme, Volume 3, Issue 2, pp. 579-587, July- September (2012) IJCET © IAEME.

[7] Himika Parmar, Nancy Nainan and Sumaiya Thaseen, Generation of Secure One-Time Password Based on Image Authentication, © CS & IT-CSCP 2012.

[8] Pramod Verma, icAuth: Image Color Based Authentication System, IUI'12, February 2012, © ACM.

[9] Gordon H. Bower, Martin B. Karlin, and Alvin Dueck, Comprehension and memory for pictures, Memory & Cognition,*1975, Vol.* 3 (2)

[10] Kirkpatrick, B. 1894. An experimental study of memory. *Psychol. Rev. 1*, 602–609.