Cumulative Security of Maze Based Folder Locking: Combination of Image Analysis, Cued Click and Pass-Point Based Approach

Monika Kadam[1] Madhuri Nanaware[2] Shweta Pote[3] Payal Solanki[4] W.P. Rahane[5]
[1,2,3,4,5]Department of Information Technology
[1,2,3,4,5]NBNSSOE, Pune, India

Abstract— The paper introduces a novel technique of security for folder locking over the traditional alphanumeric passwords. This paper mainly converges on securing the information prevailing in the folder. One can acquire an image as a password by clicking the block of meticulous image. Only authorized people would have admitted to the confidential files is the main endeavor of Graphical password .Folder locking software is inserted by us who enables security with the help of image Password. The user will have to fall into place on the block which consists of pixels which is strung-out on the pecking order of pictures. The pecking order of images and their subsequent blocks enables to lock and unlock the folder. This software gives authentication for desktop application.

Key words: Alphanumeric, Graphical Password, Authentication

I. INTRODUCTION

The surety is the degree of resistance to/ or protection from an impairment. Information processing system includes all the security procedures and mechanisms by which information and services are protected from unintended access, diversity or fatal, and are of growing importance due to increasing reliance on computer systems in most companies. A password is a word or a string of characters which enables the user to prove its identity to acquire admittance to a resource for authentication, which is not revealed to the unauthorized users. Most organizations claim password to be alphanumeric which include a combination of 26 alphabets, 10 numbers and some special symbols.

The most common computer authentication method is to use an alphanumeric username and password. This technique has been proven to have eloquent drawbacks. Most users tend to set passwords which are small, as long passwords are difficult to be remembered, but its main drawback is that such passwords are easily hacked.

Biometric authentication refers to passwords that are human based. It is oftentimes categorized as physiological versus behavioral characteristics. It includes fingerprints, palm prints, DNA, facial expression recognition, retina scans, and so on. It may also include behavioral characteristics like voice recognition of a person. Traditional ways also include token based password, such as personal identification number, passport or driving permit. Biometrics is more reliable than token based passwords as they are unique to the person.

But there are pros and cons for every scheme, out of which littlies discussedinfra. Very small terms like light, truncated precision, age, camera effect, illness, and so along. May easily disturb the biometrics machines. The point that machines are expensive and intrusive should also be brought into thoughtfulness. To conquer this drawback researcher have come up with the image password technique which enables the user to set an image as their password.

Graphical Password is an image based scheme which is an alternative to text based scheme as it is propped up by psychological assumptions that on a normal human remember images faster than text.

Generally, there are two looms to password: Recall and Recognition. There is a gigantic modification between recall and recognition. Recall is troublesome because it calls for fewer numbers of pool sticks, whereas recognition is apparent. Recall is the action of remembering something learned from an experience. Recognition is the process of identification of images from previous encounters or knowledge.

Recognition looms is being talked about in this paper. This paper engrosses entering the username as alphanumeric string and password as pecking order of images with their respective blocks.

II. LITERATURE SURVEY

The main motto of graphical password was first portrayed by Greg Blonder in 1996; the user needs to elect meticulous sections in particular image that materialize on the screen. To sign in, the user has to click on the same pieces again.

The login phase used to embrace to fill the necessary information such as Username; the recorded data field is it can be satiated. Subsequently the user has selected the environment and user is required to choose the random color pictures, that it chose at the time of registration, if the selected color images at the login time is equal to the selected images at the time of registration then the certification is valid otherwise authentication is broken. The text password field shows where the user is asked to present the text word. It also observed that the text password field is likewise very significant because this field is too contained in the database, i.e. Text password at the time of enrollment and the text password at the time of login. If the username and the text password are matched with respect to Registration time and that the user entered at the login time then and then only the authentication is valid. [1]

And so the new technique has been proposed which consists pecking order of click point. It is defined as Pass Points graphical password scheme, a password consists of a pecking order of click points (say 5 to 8) that the user elects in an image. The system arbitrary displays an image on the screen. The image is covert and has no purpose other than assisting the user to evoke the click stops. To log in, the user needs to flick on the same points which have been selected while registrations, in the elected pecking order. [3]

Cued Click Points (CCP) is a proposed substitute to Pass Points. In CCP, users click one point on images rather than five periods on one picture. It offers cued-recall and announces visual cues that instantly alert valid users if they have caused a mistake when recording their current click-stop. It also makes spasms based on hotspot analysis more inspiring. Each click results in showing a next-image, in

effect leading others down a "path" as they click on their pecking order of periods. A wrong click indicates down an invalid path, with an explicit suggestion of authentication failure only after the last click. Subsequently snapping on a meticulous pixel the next image will be enabled. If their aversion the resulting pictures, they could create a new password comprising different click-stops to contain various pictures. [2]

Since it is nearly unacceptable for human users to click repeatedly on exactly the same level, the scheme allows for an error acceptance at the click locations. This is done by discretizing the click locations, employing three different square grids. Each portion has width 6r between grids. Each one of the three grids is staggered with respect to the previous grid by a distance 2r vertically and horizontally. If there is only a quantization grid, then a selected clack point could be close to a grid line and small variations in the user's clicking could lead to a click in a different block, this may cause erroneous results. On the other hand, one can prove that with the three staggered portions every point in a two dimensional image is at a distance at least from the grid lines of at least one of the three grids; we suppose that the spot is "secure" in that grid. [3]

III. PROPOSED SYSTEM

Taking into account all the problems and limitations of graphical based systems, we have projected seek which springs authentication to the corresponding user.

Our proposed system is a methodology headed for more consistent, protected, user-friendly, and robust authentication. We have likewise cut the shoulder surfing problem to some extent.

The admin login is provided which enables the user to register, lock and unlock the folder. The admin receives the right to add and delete the users.

The First phase consists of Registrations where user needs to register. If the user has already registered then the particular user can immediately change to login phase and then go forward in the subsequent stages.

The Second phase consists of locking where the user has the authority to lock the folder using image password. The user needs to select an image as per their choice and click on the respective block per image after doing so the user needs to select the folder to be locked. Multiple folders can be locked using the same lock or different locks to multiple folders.

The last stage consists of unlocking the folder where the user asks to take the same image and the respective block which the user has previously applied for shutting up the folder.

A. Working of Proposed System:

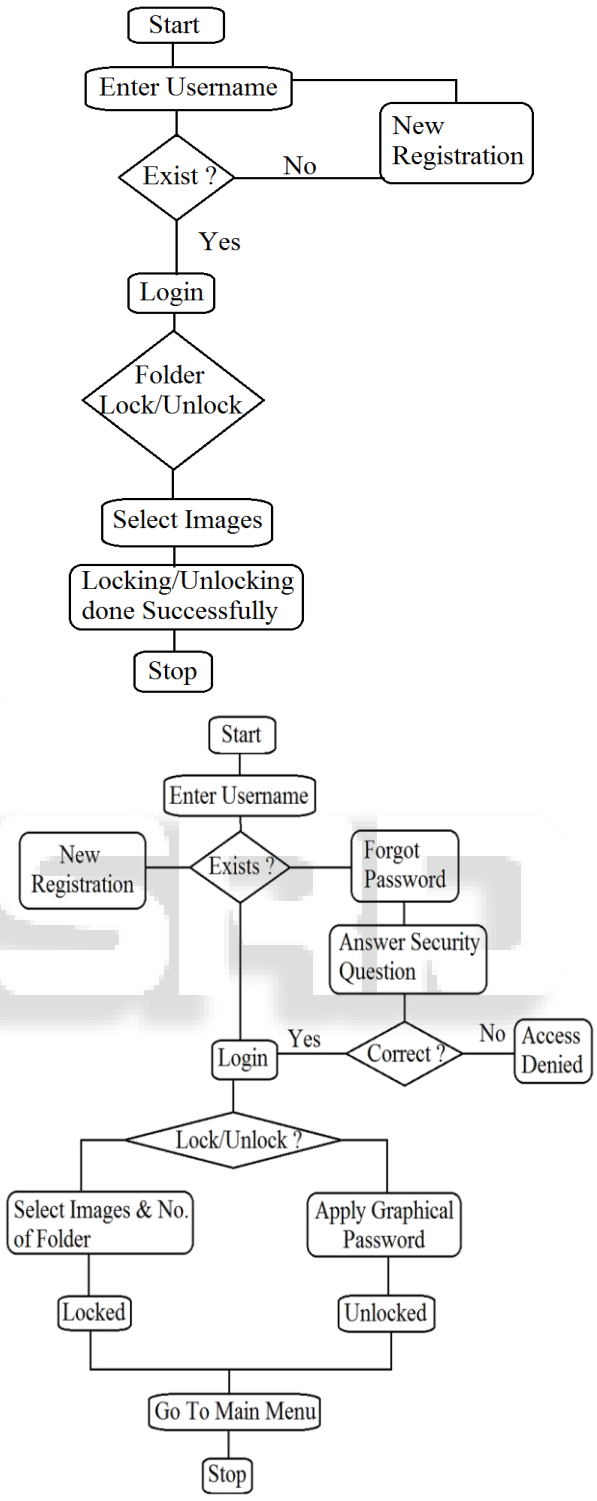

Fig. 1: Working of Proposed System

IV. IMPLEMENTATION

In this part, we will explain how the system works. The organization is split into 3 main modules: namely Registration phase, Lock phase and Unlock phase. And at that place are various Sub Modules like Forgot Passwords, Login, etc.

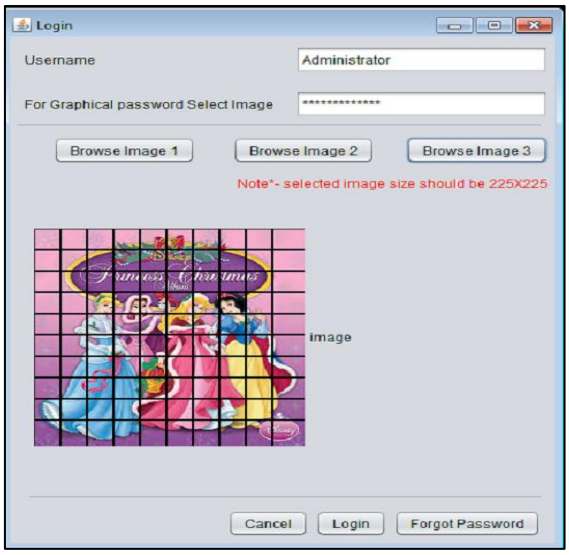

Fig. 2: Administrator Login

Initially we will discuss about the admin page which consist of admin name field and password field, which is disabled. In this text field, the user or admin is not admitted to enter anything; instead they demand to browse 3 images which are already stored in the database. These pictures are carved up into blocks and pixel point is compared with the one in the database. You will then be granted access to our site.

Admin can have access to the details of users those who are registered. This also includes forgot password button, which is explained further. If admin fails to remember the password, then he/she can opt for forgetting password where admin needs to provide 2 accurate images with their respective click/point.

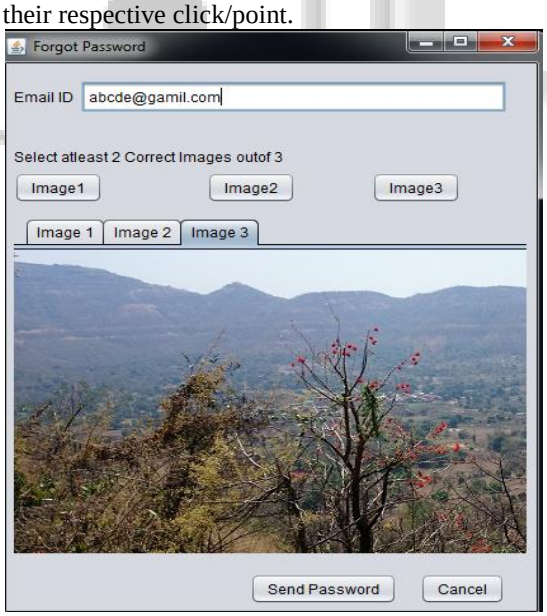

Fig. 3: Forgot Password

In this module, if the user forgets the password, user needs to furnish his/her email id which he/she has mentioned during the registration phase. The user needs to select at least 2 correct images out of 3 images, selected during registration, with its respective point; if the click points match with the one in the database then he/she will be granted to access.

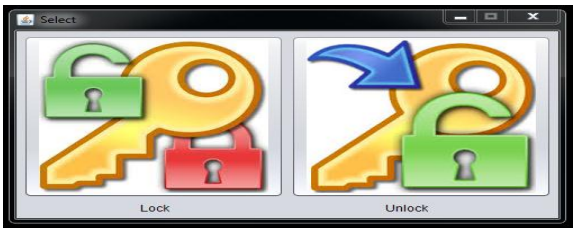

Fig. 4: Main Frame

The mainframe sub-module consist of frame with lock and unlock facilities to the user, while locking or unlocking phase the user goes through the mainframe.

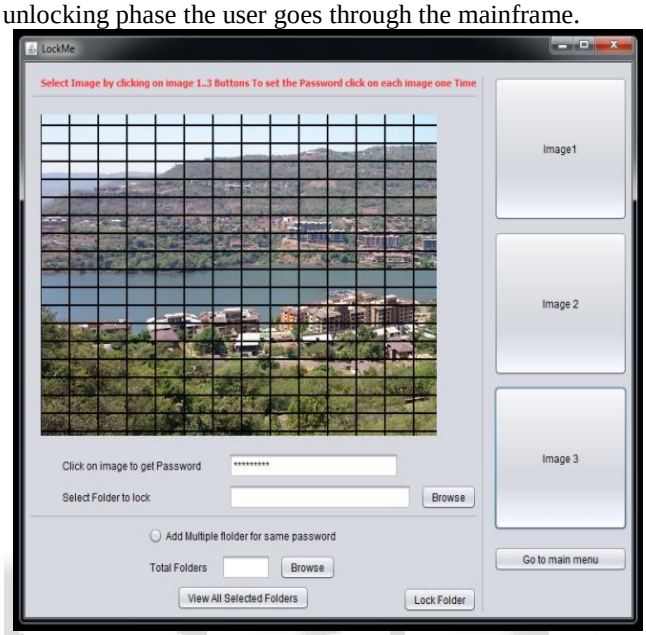

Fig. 5: Lock Screen

The lock is the core section of our application. At this stage the user is free to elect three images with its respective stages. While snapping the dots per image the password is generated. Further user has a selection of locking single or multiple folders. This can be executed by selecting the radio button; if it is selected, then the user is asked to put down the number of folders he/she desires to lock. The user is capable to keep different locks in different folders as well as same lock for multiple folders, depending on the user's selection.

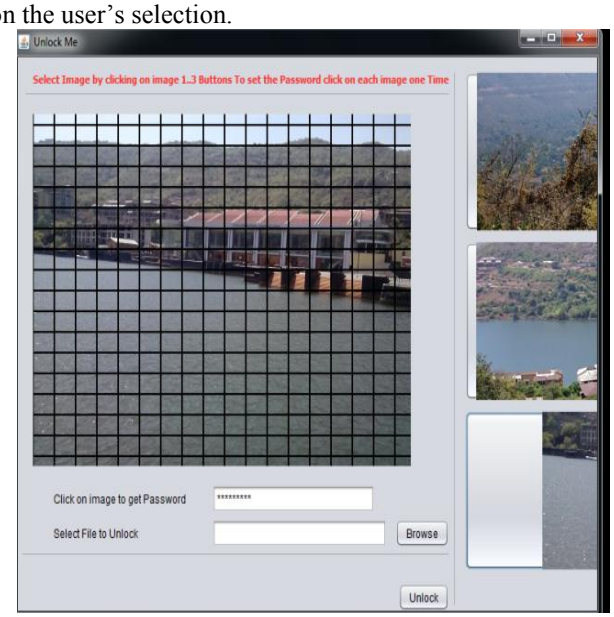

Fig. 6: Unlock Screen

In this module, to access the locked folder we need to apply graphical password which has been applied or provided previously for locking the folder. In unlock phase, we are heading towards the recognition methodology which means picking out the pictures from previous encounters. Here, we require browsing three images which we have selected for locking the same folder, each with their respective click points.

The folder we have locked initially should be browsed from the system. When the password presented by the user, is verified by the system software, then the folder gets unlocked.

In the registration phase, the user is required to register i.e. it requires to fill all the necessary information such as general details, contact details, credentials. General details consist of full name, address and gender. Contact details include mobile number and Email id; both are visible to the admin when they check the details.

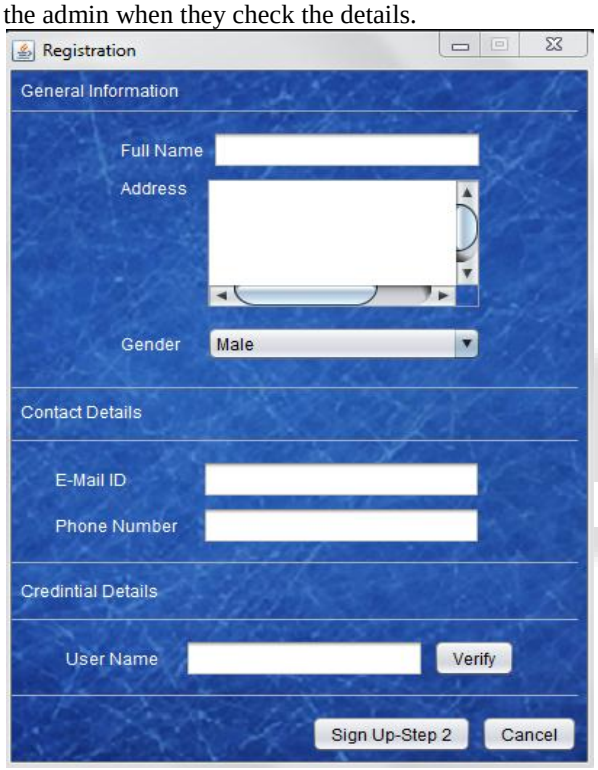

Fig. 7: Registration Screen

Credential details consist of a username and password, where user needs to browse three images as his/her password with per click on respective image, this will be used when the user will login to lock or unlock a folder i.e. the master module. The security question is being provided so that if the user forgets the password, it may facilitate the user to log in.

The locking and unlocking consists of browsing three images and picking out their blocks as a ringlet. Then, if the radio button is clicked, the textbox must be filled with the number of folders to be locked, multiple folders can be locked. After clicking on the browse button it will browse the number of folders specified in the text box. Now clicking on the lock button the folders will be locked. A standardized process is followed for unlocking the folder.

V. RESULTS

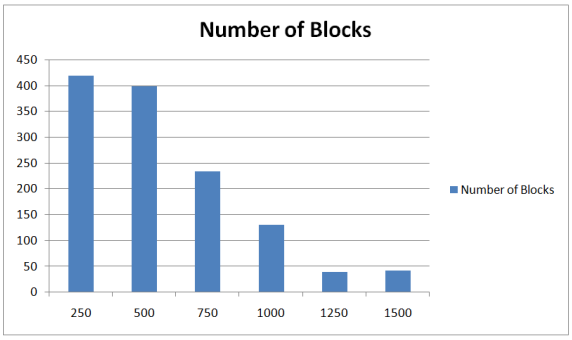

Fig. 8: Number of Blocks

After implementation of an application the next stage is its working. Working of an application gives various results as per the input from the user. Here we use the maze to split picture into small portions i.e. blocks. These blocks depend on the size of an picture. Image size is inversely proportional to the number of blocks.

As the image size increases the number of blocks decrease and vice versa. For example if images size is 250*140 then it is divided into 21*20 blocks, and total is 420 blocks. And if picture size is 1000*562 then it is split into 10*13 portion, and total is 130 blocks. From above two examples it is easily recognized that if picture size is increased, block size is decreased.

VI. FUTURE SCOPE

In the current system we are using 2D images as an input to graphical password and in the future one may use 3D images as an input to image password.

Lately, the image is kept in original form but the image can be carved up into multiple blocks where the picture is developed down into blocks, so that while locking and unlocking the image are scattered and the point is to be identified where it is being snapped.

VII. CONCLUSION

Therefore, we have produced the folder locking application using graphical password with many techniques, i.e. color image, exit point and cued click point. This arrangement enables the user to keep their folder inaccessible to intruders using images as a watchword. It provides strict security and authentication to the user.

REFERENCE

[1] Sonkar S.K., Paikrao R.L., Awadesh Kumar, "Graphical Password Authentication Scheme Based on color image Gallery", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 4, October 2012.

[2] Sonia Chiasson1, 2, P.C. Van Oorschot1, and Robert Biddle2, "Graphical Password Authentication Using Cued Click Points"

[3] Ahmet Emir Dirik, NasirMemon, Jean-Camille Birget,"Modeling user choice in the PassPoints graphical password scheme".

[4] G. Agarwal1, S. Singh and R.S. Shukla "Security Analysis of Graphical Password Over the Alphanumeric Password", International Journal of

Pure and Applied Sciences and Technology ISSN 2229-6170, 2010, pp. 60-66.

[5] XiaoyuanSuo, Ying Zhu, G. Scott. Owen "Graphical Password: A Survey".

[6] Kailas I Patil, JaiprakashShimpi, "A Graphical Password using Token, Biometric, Knowledge Based Authentication System for Mobile Devices", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-4, March 2013

[7] MD. AsrafulHaque, Babbar Imam, "A New Graphical Password: Combination of Recall & Recognition Based Approach", World Academy of Science, Engineering and Technology International Journal of Computer, Control, Quantum and Information Engineering Vol: 8 No: 2, 2014

[8] Iranna A M1, Pankaja Patil2, "Graphical Password Authentication using Persuasive Cued Click Point", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, July 2013

