International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 9, September- 2014

3-Way Authentication for Virtual Locker

Tarun Mirani, Yogesh Motwani, Disha Gurnani
Thadomal Shahani Engineering College,
Department of Computer Engineering,
Mumbai University, Mumbai, Maharashtra, India

***Abstract*— In this modern digital world the authentication schemes like textual and graphical security systems alone do not suffice the need of higher security and confidentiality for a virtual locker. So in this paper, we are proposing a 3-way authentication scheme to user that can be deployed for providing higher security and confidentiality to passwords and essential document pins and ID's. In this authentication scheme, we are proposing the use of textual password, pass point and steganography process in a combined manner**.

***Keywords*—Authentication scheme, Pass Point, Steganography, Least Significant Bit.**

I.INTRODUCTION

In this Digital age, more and more people have started storing important documents online. These documents can be files belonging to any individual or organizations like government agencies, businesses, corporations, etc. These files are stored and managed in digital lockers.There are various ways in which digital files can be stored and accessed online. One of the such ways is using traditional user authentication technique in which each user has unique username and password. This approach is more vulnerable to cyber attacks, hackers, and cyberpunks and therefore makes this scheme less secure. Security of files stored in digital lockers is a matter of prime concern in this era where technology is not been utilized to its full potential for security purposes.

The other authentication technique used for security purpose is graphical authentication. The graphical authentication scheme is a proposed technique developed by researcher in order to overcome the bottleneck of traditional textual authentication. The graphical authentication exceeded the level of security as compared to traditional textual authentication. The graphical password is an authentication scheme that works by user selecting images in a specific order. The other possible graphical password can ask a user to identify the pattern or alphanumeric password depicted in image in a distorted form. But such graphical passwords are nowadays become vulnerable to pattern recognizing programs developed by attacker to recognize the depicted password. The graphical authentication is also vulnerable to shoulder surfing. When user enters there password in public or under surveillance area it can be captured by attacker by direct observation or by recording user's authentication session. Such attack is known as Shoulder surfing. And because of their graphic nature, nearly all password schemes are vulnerable to shoulder surfing.

The security level can be exceeded beyond the textual and graphical authentication by performing multilevel authentication scheme.

One way to increase security for digital files is by using various security techniques like PassPoint, Steganography, and Cryptography, etc. Passpoints technique is a technique in which user is presented with any arbitrary image that is rich enough so as to have several click points where user can click on few points in some particular sequence to create a password. This password is stored as tolerance which is calculated around each chosen pixel. This tolerance is given because it is nearly impossible to click at the same pixels every time you login. Tolerance allows user to click on adjacent pixels. For example, if tolerance is 10 X 10 then user is allowed to select any pixel that is within this tolerance range. At the time of logging in, the user is supposed to click points in the correct sequence and within the tolerance of chosen their chosen pixels. Steganography is a way in which a secret message can be hidden in any ordinary message or image in such a way that presence of hidden message is only known to its intended receiver. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, audio, text, HTML, or even floppy disks) with bits of discrete, invisible information. This hidden information can be plain text, cipher text, or even images[1].There are various techniques in which steganography can be used to hiding messages inside images.These are Least Significant Bit (LSB) modification, Masking,Filtering and Transformations via algorithms.

II. OUR PROPOSITION

A. PASSPOINT AUTHENTICATION

The PassPoint method is implemented by allowing random images to be used. User can click multiple times anywhere in the image in particular sequence generating password and select the area while registration to set the password. This is performed by calculating the tolerance around each selected pixel. And in order to pass the authentication the user has to click within the tolerance area of their selected pixel and also in the correct sequence.

The quality of authentication depends on how many times the system allows the user to select the pixels in proper sequence. We can assign an acceptable size of tolerance area around selected pixel to minimize the false positive and false negative limit. For an actual selected point (x,y), we can allow a user to click an point on X-coordinate anywhere between (x-4) to (x+4) and Y-coordinate anywhere between (y-4) to (y+4). This makes the length of tolerance area square around 8. [1]

Fig. 1.1. The image appears to user to select point

Fig. 1.2. PassPoint Password

Above images shows the example of point selection. The user has to select the 3 points in sequence that he had selected while process of registration. As in this case, the password is an eye, teeth and mike. If these areas are selected in correct order in 3 attempts, this completes the PassPoint authentication level.

B. STEGANOGRAPHY

The origin of steganography came from Greek word it means to write something secretly. steganography is art of science which hides the secret messages into a medium. it hides the messages in such a way that no one except the receiver knows how to expose the secret message. Steganography takes cryptography a level more by hiding an encoded message.

The steganography is art or practice to hide a message, image or file within another image, file or message. In our paper the image steganography is proposed with LSB technique.

B.1 Image Steganography

In this data is first encrypted and then inserted, using a special algorithm, into redundant (that is, provided but unneeded) data that is part of a particular file format such as a JPEG image.

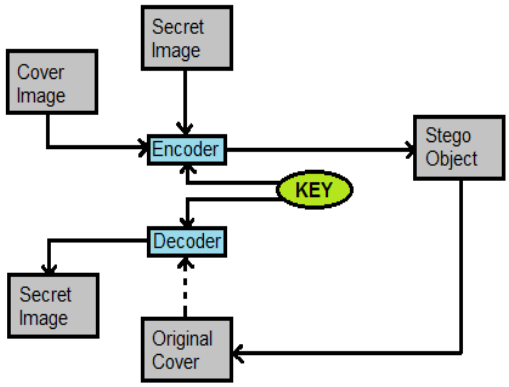

Fig. 2. Steganography Process

B.2 Least Significant Bit Technique

LSB technique will replace the least significant bits with the message to be encrypted. it tends to embed secret message into image. We have used the bmp images as it does lossless compression so LSB can be resourceful while using bmp.

We are using least significant bit because of following reason. [2]

a) After hiding the message, the intensity of image is change by 1 or 0.
b) Change of intensity is either 0 or 1 because it changes your last bit .e.g.

1010110 ----> 1010111

The only change is 1 bit so that its intensity should not be affected.

For example, suppose you want to hide a message in image (24-bit colors i.e., RGB). Suppose the original 3 pixels are:

00101101 00011101 11011100

10100110 11000101 00001100

11010011 10101101 01100011

Now if we insert 'A' in image. Binary equivalent for A is 10000001, it will change 3 bits

00101101**0**0011100 11011100

10100110**1**1000100 00001100

1101001**0** 10101100 01100011

In this way, the binary equivalent or secret message 'A' is embedded into image (24bit).

B.2.1 PROCUDURE: [3]

1. Secret Message Insertion

- Obtain cover image pixels.
- Obtain secret message characters.
- Obtain steganography key characters.
- Take first pixel and any characters from steganography key and keep them at first part of pixel.
- Now take any terminating symbols like 0 to indicate that key has been terminated.
- Now insert each character of secret message in each of first part of next pixels.
- Replace each characters of secret message with first part of next pixels.
- Repeat step 6 and step 7 untill all the characters from secret message are been encoded.

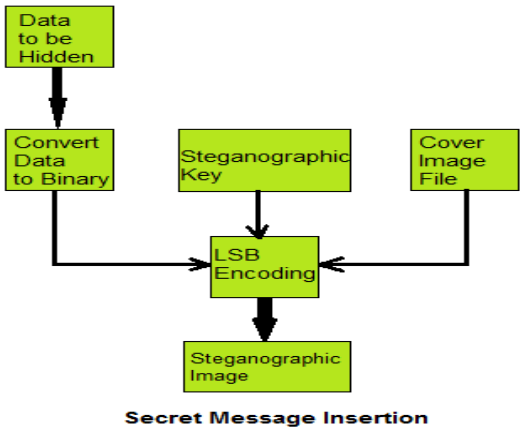

Fig. 3. Secret Message Insertion Proces

2. Secret Message Extraction

- Obtain steganographic image pixels.
- Now take first pixel and obtain steganography key characters from first part
- If the steganography key matches with the key entered by user while insertion then go to next pixels and obtain your secret message characters, follow this until you obtain 0 (terminating symbol) or obtain secret message.
- If key does not matches with the key entered by user while insertion, and then terminate the program.

In this way both the procedures are used to insert as well as extract the secret message.

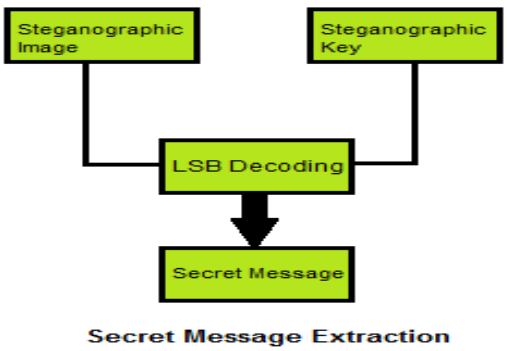

Fig. 3. Secret Message Extraction Process

III. PROPOSED SYSTEM

A. Registration Phase:

- Initially the user creates his/her profile by creating username and password.
- The username and password provided by user is checked for availability. If it is unique then user will be allowed to create a profile where user is asked for all details and his/her own ID picture of which will be used in process of pass point authentication.
- After the user profile is created, the user has to set three points on provided ID picture which will be used while pass point authentication.
- As soon as PassPoint authentication process is completed by user another stage of authentication that user needs to complete is steganohraphy. In steganography, the information you want to hide is hidden in an image and to unlock it a key is generated. This key is used by user while login to access and manage the data in virtual locker. In registration process, Steganography is last phase.

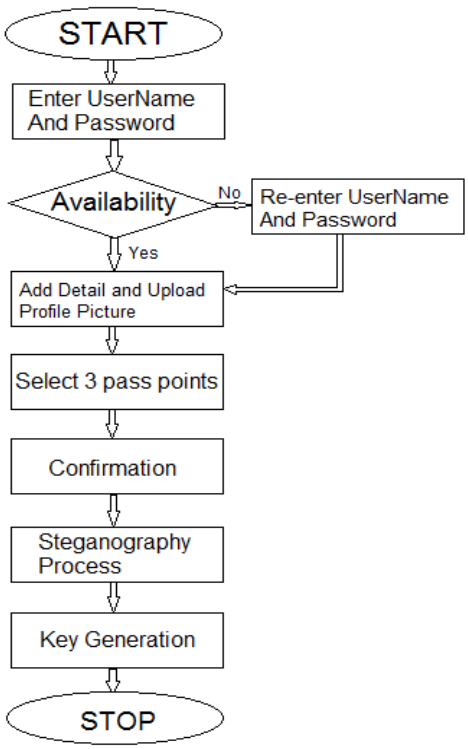

Fig. 4. Flowchart for Registration Process

B. Login Phase:

- Initially at start of the login process, the user has to enter the ID and password.
- In this Step, while login the user will be asked to select the 3 points that the user had selected while registration process.
- Once the correct 3 points are selected on picture, the user will be provided with steganography window. The user has to type the key to end the authentication process and access the information.

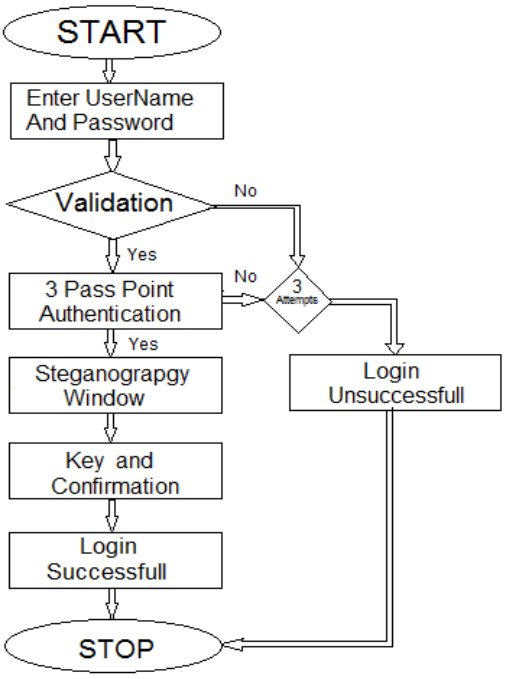

Fig. 1. Flowchart for Login Process

IV. FUTURE SCOPE

The future advancements with our proposed system will be to store all images used for authentication in a manner that they require very less space as compared to what they require in current scenario. This will provide more space for storing data than space allocated for authentication purpose. Another important advancement of our proposed system is to overcome the drawback in cases where graphical passwords are difficult to share as compared to text based passwords making it difficult for individuals or teams to work together when they have to share the data stored in digital lockers.

V. CONCLUSION

Our proposed system that is based on recall and recognition authentication scheme has various advantages over traditional authentication which supports only Username and password as means of security. Graphical passwords created using passpoint scheme are not only easier to remember as compared to alphanumeric passwords but they also provide larger password spaces. Password spaces is nothing but a set that comprises of all passwords that are possible for a given passwords scheme. The most common and popular method of modern day steganography is to make use of the LSB of an image's pixel information. Thus the distortion of overall image is kept minimal, while the information is spaced out over the pixels in the image [4]. Using graphical authentication technique like passpoints and steganography technique along with textual password in digital lockers can increase the security exponentially. Thus, making this authentication scheme more reliable and secure.

REFERENCES

[1] World Academy of Science, Engineering and Technology. International Journal of Computer, Information, Systems and Control Engineering Vol:8 No:2, 2014. Md. Asraful Haque, Babbar Imam.
[2] Cambridge, UK, May30-June1 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson (Ed.), pp.1-7 Benderr, D.Gruhl, N.Morimoto and A.Lu, "Techniques for Data Hiding", IBM System's Journal, Volume 35, Issue 3 and 4, 1996, p.p., 313-336.
[3] http://ethesis.nitrkl.ac.in/4626/1/109CS0608.pdf
[4] http://www.slideshare.net/vikasksharma140/steganography-ppt