International Journal of Innovative Research in Electronics and Communications (IJIREC)
Volume 1, Issue 6, September 2014, PP 20-30
ISSN 2349-4042 (Print) & ISSN 2349-4050 (Online)
www.arcjournals.org

Implementation and Design of Graphical Password System Using Image Fusion

[1]G. Madhavi, [2]N. Ramakrishna, [3]N.Moorthy Muthukrishnan

[1]Dept. of ECE, [2,3]Dept.of ETM
G.Narayanamma Institute of Technology and Science
Hyderabad, INDIA.
[1]gmadhavi54@gmail.com,[2]ramakn@gmail.com, [3]nmoorthy2001@yahoo.com

Abstract: *User authentication is a fundamental component in most computer security contexts. It provides the basis for access control and user accountability. While there are various types of user authentication systems, alphanumerical passwords are most widely used user authentication. Users are known to choose easily guessable and short text passwords, which are easy targets of dictionary and brute-forced attacks. Enforcing a strong password policy sometimes leads to an opposite effect, as a user may resort to writing his or her difficult-to-remember passwords on sticky notes or back of the debit card exposing them to direct theft.The graphical passwords are preferable authentication systems where users click on images to authenticate themselves. Graphical password schemes have been proposed as possible alternatives to text-based schemes, motivated partially by the fact that humans can remember pictures better than text [1].This paper aims at implementing the simple Graphical Password Authentication System using fusion algorithm. The proposed work includes three phases- Registration, Training and Authentication.*

Keywords: *Graphical password, Alphanumeric password, passpoints, Authentication, passwordsecurity.*

1. INTRODUCTION

Nowadays, the most widely used authentication mechanism is the textual passwords. However, it is well known, that most users are frustrated by their experiences with these traditional passwords in general. Even if they want to behave securely, they often do not understand what constitutes a "secure" password since guidelines for the creation of secure passwords are seldom adequate. Even with good guidelines in place, human nature will lead users to prefer the least resistance path e.g. choosing easy passwords, storing them in plain text on their mobile phones or reusing those [2]. Traditional way of user authentication is by prompting the user to key in their username and password. This method is widely used in many authentication systems. However, the approach has many drawbacks; such as passwords can easily be guessed, vulnerable to key-logger and spyware. Alphanumerical passwords are required to satisfy two requirements. One is the password should be easily remembered by a user, while they have to be hard to guess by attackers.

Many problems that users have with alphanumeric passwords are related to memorability of secure passwords. In an attempt to create more memorable passwords, graphicalpasswordsystems came into existence. In these systems authentication is based on clicking on images rather thantyping alphanumeric strings. Graphical passwords which use pictures as passwords instead of using alphanumeric characters.

The main motivation for graphical passwords is that people are better at remembering images than alphanumeric. For example we can recognize the people we know from thousands of faces; this fact was used to implement an authentication system. This is the basis for the graphical passwords [3]. A survey of numerous graphical password schemes have been developed which classifies the password systems as recognition-based systems, pure recall based systems, and cued recall based systems.

In recognition-based systems, users would choose pictures, icons from a collection of images. In authentication process, the users need to recognize their registration choice among a set of candidates. The research shows that 90% of users can remember their passwords after one or two month [4]. In pure recall-based graphical password schemes, users need to reproduce their

password without being given any hints or cues. Jeremyn et al. described a graphical password scheme Draw a Secret" (DAS), where the user has to draw a something shape or pictures on a grid. Users need to draw approximately the same shape in order to authenticate themselves. The graphicalpassword schemes based on pure recall are quick and convenient to use, but they have the same disadvantage as alphanumeric password: They are hard to remember [5] [6].In cued recall, the users have to recall a password, but the system offers a framework of hints, context, and cues, that help the users reproduce their password or help them make the reproduction more accurate. Here, the user is shown an image on the screen, and the password consists of a few points that the user chooses in the image (by clicking or pointing). Authentication is performed by clicking near the previously determined points. Cued recall is intermediate between recognition and pure recall.

2. METHODOLOGY

Our proposed work implements the two simple graphical password schemes to provide more security. They are click-based image fusion and connectivity-based image fusion technique.

2.1 Click-based Image fusion Technique

The click-based image fusion technique was designed to improve the security and to reduce the dictionary attacks. In order to improve the security the image fusion algorithm has been introduced in click-based image fusion technique. In this method the password constitutes a single click point on the source image. In click-based image fusion user has to select a pixel and fusion is performed. In registration phase standard deviation of the fused image is calculated and image space is created in training phase. Authentication is done by comparing standard deviation of the image with image space.The proposed method includes two phases. One is registration phase and second one is verification phase.

2.1.1 Registration Phase:

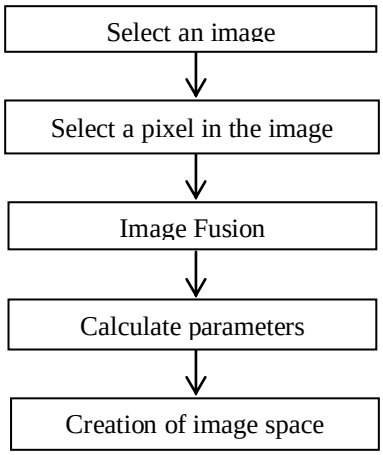

Figure 2.1. *Flowchart for click-based image fusion technique in registration phase*

2.1.2 Verification Phase:

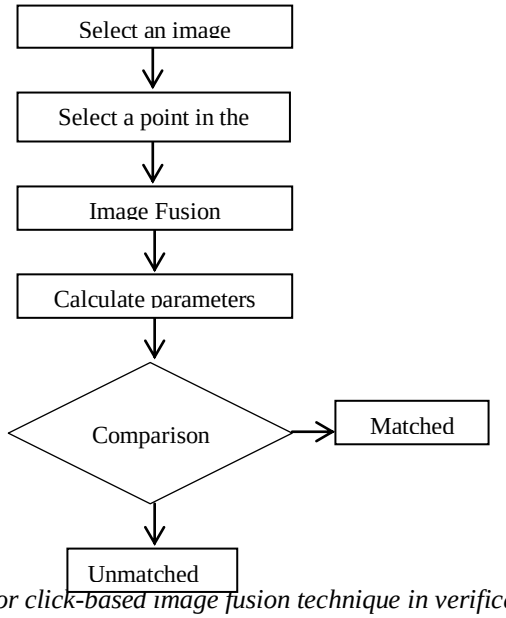

Figure 2.2. *Flowchart for click-based image fusion technique in verification phase*

The following steps give the detailed description about the registration and verification phase.

Step 1: Select an image

In this step user need to select an image from the available list of images provided by the system database.

Step 2: Select a pixel in the image

In step-2 user has to select a pixel from the selected image by using user interaction with the mouse pointer.

Step 3: Image fusion

Image Fusion is a process of combining the relevant information from a set of images, into a single image, wherein the resultant fused image will be more informative and complete than any of the input images [7]. The image fusion is performed on the user selected image. This will provide high security because the user selected image is fused with the second image that is randomly generated by the system.

In this paper the pixel-level image fusion was done in this method;it assumes that the input images are to be of equal size and spatial resolution.

The sequence of operations carried out in pixel-level image fusion is as explained below[8][9] [10]:

A)Read the set of images i.e. here in this algorithm we have considered two images which are of same size.

B)Fusion factor can be varied to vary the proportion of mixing of each image.

- With Fusion factor = 0.5, the two images are mixed equally.
- With Fusion factor< 0.5, the contribution of background image will be more.
- With Fusion factor> 0.5, the contribution of foreground image will be more.

In this method we have consider fusion factor= 0.5.here the selected pixel in step2 is considered as fusion factor(x)

C)The image fusion is done by this formula

Fused image = x*first image + (1-x)second image

Where x is fusion factor and choose x<1.

Step 4: Calculating the statistical parameters for the fused image.

Step 5: image space is created by using fusion parameters.

In the verification phase, in step1, the user has to choose an image that he/she selected during the registration phase. In step2 user need to choose a pixel from the chosen image and fusion is performed. The statisticalparameters of the fused image is compared is compared with Image space created in registration phase. If it matches any one value of Image space then image matching will be done.

2.2 Connectivity-based Image fusion Technique

The technique is broadly classified in to two phases i.e., registration phase and verification phase.

In click-based image fusion technique, in order to log in, the user has to select pixel by clicking on particular pixel; within the image .The tolerance is needed because the user's click point literally is a single pixel, which is too precise for a user to click on successfully. In order to overcome this drawback, we are proposing the connectivity based image fusion technique.

In connectivity-based image fusion user has to select series of images and connected components and fusion is performed. Fusion parameters are calculated in registration phase. Training phase

creates image spaceusing fusion parameters. *K*-NN classifier is used for authenticationin verification phase.

2.2.1 Registration phase:

The following steps give detailed explanation of operations involved in registration phase.

Step 1: Select an image

In the registration and verification phase the user has to select two input images from the list of images provided in the database.

Step 2: Specify connectivity

Here the user has to specify connectivity by entering the number for 4 or 8 connectivity.

The following sequences of operations are performed to get connected components

A) The selected inputs itself is taken as input images.

B) The pre-processing method uses the median filtering and the output thus formed is free from noise and can be used in the next step for edge detection.

Median filtering is a nonlinear process useful in reducing impulsive noise. It is also useful in preserving edges in an image while reducing random noise. In a median filter, a window slides along the image, and the median intensity values of the pixels in the window becomes the output intensity of the pixel being processed. For example, suppose the pixel values in a window are 5, 6,

55, 10 and 15 and the pixel being processed has a value of 55. The output of the median filter and the current pixel location is 10 which is the median of five values. The median filtering smoothens the image and it can preserve discontinuities in a step function and can smooth a few pixels whose values differ significantly from their surroundings without effecting other pixels. An important parameter in using the median filter is the window size. If it is less than 5, the two pixels with impulsive values will not be significantly affected. For large window, they will be. Thus this choice depends on the context because it is difficult to choose the optimum window size in advance.

C) In the edge detection, the Sobel Operator is used to detect edges.

The Sobel operator find edges using the Sobel approximation to the derivative. It precedes the edges at those points where the gradient is highest. The Sobel technique performs a 2-D spatial gradient quantity on an image and highlights regions of high spatial frequency that correspond to edges. In general it is used to find the estimated absolute gradient magnitude at each point in n input gray scale image. In conjecture at least the operator consists of a pair of 3x3 complication kernels as given away in below figure. One kernel is simply the other rotated by 90^{o}.

-1	-2	-1
0	0	0
+1	+2	+1

-1	0	+1
-2	0	+2
-1	0	+1

Figure 2.3: Sobel Operators with $G_{x\ and} G_{y}$respectively

D) The image with the detected edges has connected components and here the number of connected components has to be reduced to extract the required data of pixels. The reduction of connected components is done by using 4 components.

E) After reducing the connected components we identify the number of connected components and extract the desired values.

The following algorithm shows the different operations involved in the connectivity.

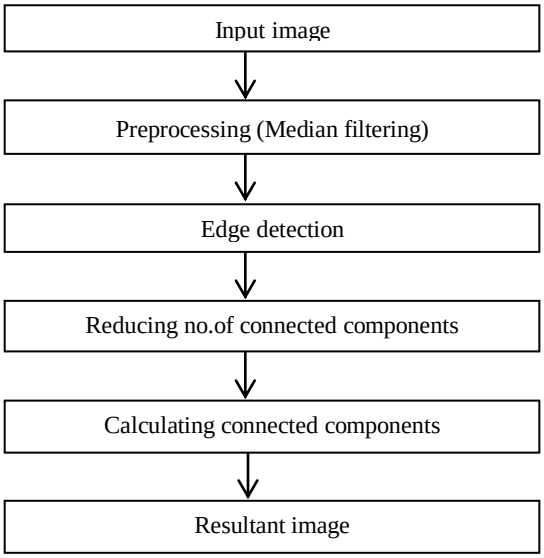

Figure 2.4. *Algorithm for connectivity*

Step 3: Image Averaging

In image averaging the resultant image is obtained by simple averaging corresponding pixels in each input image as:

$$\mathrm{I}(m,n) = \sum\sum G(i,j) \; (1)$$

Where i: 1 to m and j: 1 to n

Step 4: Image fusion

The pixel based image fusion algorithm is performed on the averaging image. The Steps for the image fusion is as discussed earlier in step3 of the first technique.

Step 5: Finally calculates the parameters for the fused image.

Step 6: Image space is created using fusion parameters.

The flow of operations involved in registration phase is as shown below

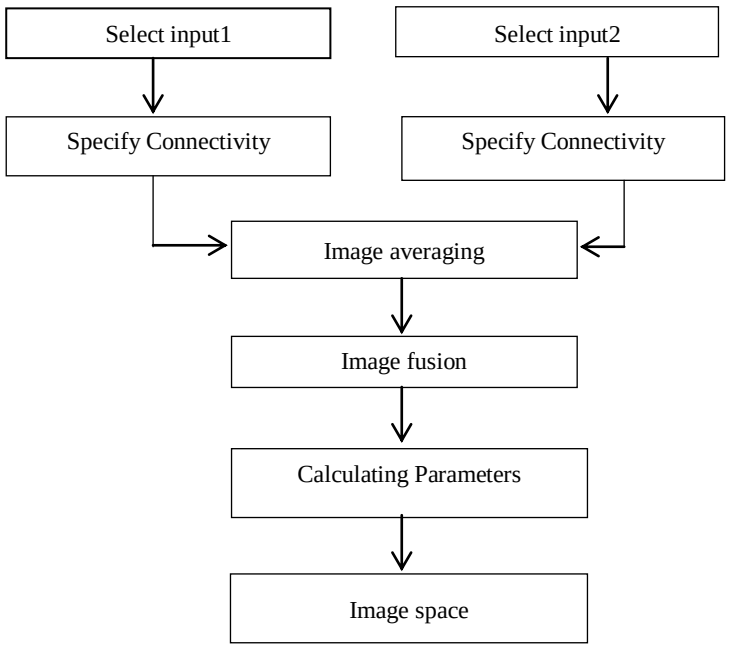

Figure 2.5. *Flowchart for connectivity-based Image fusion in registration phase*

2.2.2 Verification phase:

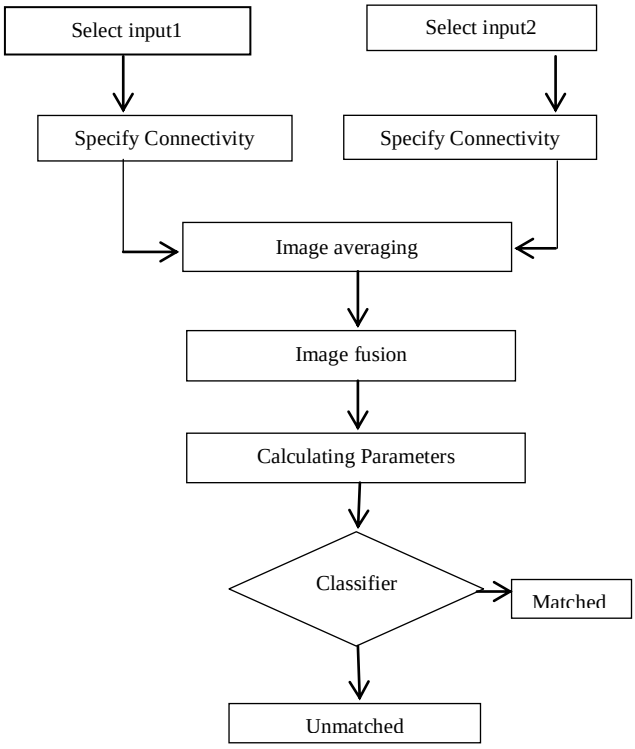

Figure 2.6. *Flowchart for connectivity-based Image fusion in verification phase*

In the verification phase the user has to repeat the same steps from step1 to step5 as registration phase. In step6 the *k*-NN classifier is used to compare the performance metrics of the verification phase with the registration phase and authentication is done for the user.

The *k*-Nearest Neighbors algorithm (***k*-NN**) is a non-parametric method used for classification. In classification, the input consists of the *k* closest training examples in the feature space. In *k*-NN classification, the output is a class membership. An object is classified by a majority of its neighbors, with the object being assigned to the class most common among its *k*nearest neighbors (*k* is a positive integer, typically small). If *k* = 1, then the object is simply assigned to the class of that single nearest neighbor.

The advantages of *k*-NN classifier are it is easy to implement and debug, there are some noise reduction techniques that work only for *k*-NN that can be effective in improving the accuracy of the classifier.

3. PERFORMANCE METRICS

The statistical parameters have been calculated for the fused image. Standard deviation is ameasureofdispersioninafrequencydistribution obtainedbyextractingthe squareroot ofthe mean ofthesquares oftheobservedvaluesfromthearithmeticmeanofthedistribution. It should be maximum.

The standard deviation is given by

$$S = \left(\frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2\right)^{\frac{1}{2}} (2)$$

Where

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \, (3)$$

And n is the number of elements in the sample, $\bar{x}$ is the mean and x_i is ith element in the sample.

4. RESULTS AND DISCUSSIONS

The graphical password authentication systems have been developed by using the techniques as discussed earlier and the results are shown below.

4.1 Click-based Image fusion Technique

Figure 4.1. *GUI frame with list box and message box*

In figure 4.1, the GUI layout consists of listbox, read button and process button as shown below. Where the listbox contains collection of different images. After selecting the image from listbox in order to read the image the user has to click on read button. The process button is used to carry set of operations.

Figure 4.2 shows the matching process where it compares some performance metrics based on these results the authentication will be done, if it matches then the user will be successfully authenticated.

Figure 4.2. *GUI frame of verification phase*

The table 1 shows the matching process of the verification phase. Standard deviation (SD) of images is considered as image feature. In verification phase the standard deviation value of test image is calculated and compared with image space created during registration phase. In our proposed work, FAR or FRR considered as false detection. If there is a fractional change in mouse click point which results as false rejection (FR). If there is a same intensity click point on image other than desired one results in false acceptance ratio (FAR).

Table 1. *Shows training and recognition phases of click-based image fusion technique*

Registration phase	S.D	Test image in verification phase	Comparison	False detection
Capture1.jpg	68	Flwr1.jpg	Unmatched	No
Fabric200.jpg	82	Flwr1.jpg	Unmatched	No
Flwr1.jpg	51	Flwr1.jpg	Matched	No
Peppers.jpg	91	Flwr1.jpg	Unmatched	No
CT.jpg	37	Flwr1.jpg	Unmatched	No
B2jpg	41	Flwr1.jpg	Unmatched	No
T65a.jpg	12	Flwr1.jpg	Unmatched	No
T80a.jpg	46	Flwr1.jpg	Matched	yes
liftingbody.jpg	60	Flwr1.jpg	Unmatched	No
Images121.jpg	53	Flwr1.jpg	Matched	Yes

4.2 Connectivity-based Image fusion Technique

In Figure 4.3 the GUI window having listbox which consists of collection different natural images, edit text where the user can enter the number using keyboard and axes where it displays the user selected images and pushbutton is to perform some operations.

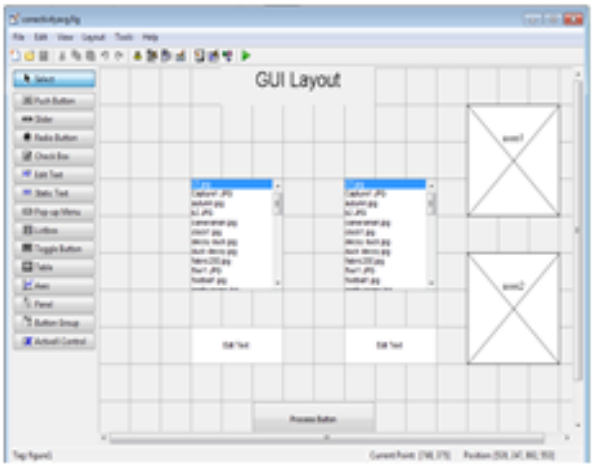

Figure 4.3. *GUI Layout with listbox, axes and push buttons*

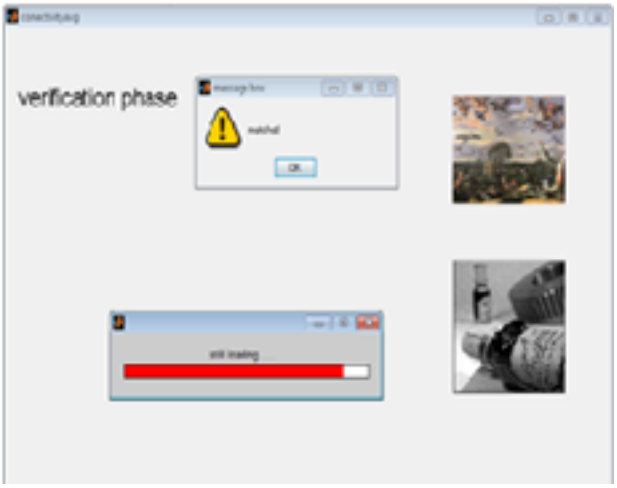

Figure 4.4. *GUI results of verification phase*

The figure 4.4 shows the matching process where it compares some performance metrics based on these results the authentication will be done, if it matches then the user will be successfully authenticated.

Table 2. *Shows training and recognition phases of connectivity- based image fusion technique*

Registration phase		SD	Test images in verification phase		k-NN Classifier
Input1	Input2		Input1	Input2	
B2	flwr	20	T75b	T9b	Unmatched
T70a	flwr	16	T75b	T9b	Unmatched
T71a	T86a	14	T75b	T9b	Matched
T75b	T9b	15	T75b	T9b	Matched
Images121	Capture1	25	T75b	T9b	Unmatched
football	Peppers	26	T75b	T9b	Unmatched
P30b	Westcord	22	T75b	T9b	Unmatched
T4a	T65a	18	T75b	T9b	Unmatched

In table-2 two input images are selected from data set and average of the connected components are fused, the standard deviation of fused image is calculated.The two test images in verification phase are compared with the registration phase by using k-NN classifier and give the result as matched or unmatched. As there is no click point is required in connectivity- based image fusion the false detection can be avoided.

Figure 4.5 shows the standard deviation of the images in the dataset. This standard deviation is consideredas image feature in our proposed algorithm.

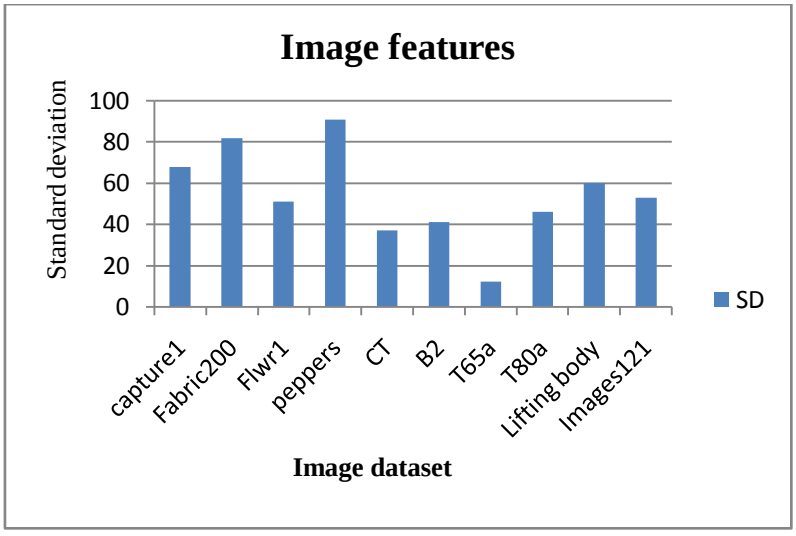

Figure 4.5. *Image dataset with SD values*

Table 3. *Comparison of graphical password systems*

Techniques	Image size	No. of Click points	Connected components	False detection	User interaction
Passpoint Technique[3]	421x342 676x598	3	Not Considered	Yes	Mouse click point
Cued click point technique[11]	804x566 676x470	3	Not Considered	Yes	Mouse click point

Click-based Imagefusion	256x256 166x167	1	Not Considered	Yes	Mouse click point
Connectivity -based Image fusion	250x202 239x242	0	Considered	No	Selection of connectivity

The table-3 shows comparison of different graphical password systems. In the image dataset different image sizes are considered for different methods as shown in table. The number of click points required in passpoint and cued-click point techniques is 3; where as in connectivity- based image fusion no click point is required. The connected components are considered for password generation in connectivity-based image fusion method. No false detection is observed in connectivity-based image fusion as it is depended on connectivity but not on click point.

5. CONCLUSIONS

The graphical password authentication system using fusion algorithms are discussed. The two methods namely click- based image fusion and connectivity-based graphical password authentication. Alphanumeric passwords lead to guessable password practices and lower overall security. It is found that the click based image fusion is giving 80% accuracy. The drawback of this method requires precise click point during authentication. However, click points seems to hold out the prospect of a much more secure system. First of all, it is easy to obtain large passwords spaces, based on user interaction, images with hundreds of potential click points. Second, this allows safe storage and protection during file back-up. Third, it appears from the small sample in our experiment that users did not too often chose points that were within a circle chosen by another individual. Moreover, the use image fusion using machine selected image and authentication based on statistical parameters reduces the possibility of users having the same click points even if they are attracted to a salient area of the image. This reduces the chance of an attacker being able to guess passwords. With respect to usability, which is the main focus of this paper, our results indicate first that users can quickly and easily create graphical password. Second, most users can quickly learn to input graphical passwords without error, and even those who do make repeated errors can input them successfully given enough practice .It is found that the connectivity based image fusion is giving 90% accuracy. This method avoids precise selection of click point for image authentication.

REFERENCES

[1] Bashier, H.K.; Lau Siong Hoe; Pang Ying Han, "Graphical password: Pass-images Edge detection," Signal Processing and its Applications (CSPA), 2013 IEEE 9th International Colloquium on , vol., no., pp.111,116, 8-10 March 2013.

[2] Renaud. K.; Mayer. P.; Volkamer, M.; Maguire, J., "Are graphical authentication mechanisms as strong as passwords?" Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on , vol., no., pp.837,844, 8-11 Sept. 2013.

[3] S.Wiedenbeck, J.Waters, J. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 102–127, 2005.

[4] English, R.; Poet, R., "Towards a metric for recognition-based graphical password security," Network and System Security (NSS), 2011 5th International Conference on, vol., no., pp.239,243, 6-8 Sept. 2011.

[5] Agarwal, G.; Singh, S.; Indian, A, "Analysis of knowledge based graphical password authentication," Computer Science & Education (ICCSE), 2011 6th International Conference on, vol., no., pp.588,591, 3-5 Aug. 2011.

[6] FarnazTowhidi, Maslin Masrom, "A Survey on Recognition-Based Graphical User Authentication Algorithms", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 2, 2009.

[7] Hasegawa, M.; Tanaka, Y.; Kato, S., "A study on an image synthesis method for graphical passwords," Intelligent Signal Processing and Communication Systems,ISPACS 2009. International Symposium on, vol., no., pp.643,646, 7-9 Jan. 2009.

[8] ShivsubramaniKrishnamoorthy, K P Soman,"Implementation and Comparative Study of Image Fusion Algorithms" International Journal of Computer Applications (0975 – 8887), Volume 9– No.2, November 2010.

[9] V.P.S. Naidu and J.R. Raol" Pixel-level Image Fusion using Wavelets and Principal Component Analysis" Defence Science Journal, Vol. 58, No. 3, May 2008, pp. 338-352, 2008.

[10] Chetan K. Solanki, Narendra M. Patel" Pixel based and Wavelet based Image fusion Methods with their Comparative Study" National Conference on Recent Trends in Engineering & Technology.

[11] Chiasson. S, van Oorschot. P, and Biddle. R, "Graphical password authentication using Cued Click Points," in European Symposium On Research In Computer Security (ESORICS), LNCS 4734, September 2007, pp. 359–374.