A Systematic approach towards enhancing of Security and usability of graphical password through cognitive computing and data mining

Norman Dias

Research Scholar, Dayananda Sagar University, Department of Computer Science & Engg., Bengaluru-India
norman.dbce@gmail.com

Dr. Mouleeswaran S. K

Assistant Professor, Dayananda Sagar University, Department of Computer Science & Engg, Bengaluru-India
mouleeswaran-cse@dsu.edu.in

Dr. Reeja S R

Professor, Vellore Institute of Technology, Department of Computer Science & Engineering, AP-India
reeja.sr@vitap.ac.in

Abstract

This In this modern era of online world, one requires to have an online account. It may be a social, transactional, online shopping or an e-mail account, with a heap of so many accounts and the burden of memorizing the difficult passwords, user tends to compromise on the password, thereby weakening the security aspect. Most of the passwords are prone to shoulder surfing attack. In this paper we propose a novel Graphical authentication system named Confusys. Cofusys system takes care of the shoulder surfing assault, as it deals with information from different images. The befog module does not provide any information to the attacker; above all it confuses the attacker more .The befog module differs for every user as it is purely based on the click point from the user. The slightest change in the click point from the user results in a massive change of data. A prototype of this system is implemented to check for various parameters of this system and the results proved the chances of breaking into the system is very less within the range of 7.63183 e^{-15} to 1.38936 e^{-17}, and also provides password entropy between 2^{58} to 2^{67}.

***Keywords*: Graphical Password, Password Space, Memorability, Saliency Mask**

1. Introduction

The issues with traditional password techniques are quite notable. A secret key verification framework ought to energize strong passwords while looking after memorability.

This paper suggests a verification and authentication method that permits client decision towards more grounded passwords. The paper discusses about framework, the existing method's in choosing powerless password is more dreary, debilitating users from settling on such decisions. Essentially, the proposed method makes picking a safer secret key.

As opposed to expanding the weight on clients, it is much simpler to follow the framework recommendation for a safe secret word. With the expanding number of gadgets and wide utilization of various applications, network protection of a user turns into an issue; also it turns out to be hard to recall various passwords for each extraordinary verification activity. The password strength additionally weakens after some time, corresponding to the absence of security episodes the client may have not experienced, and these results in a misguided feeling that all is well and they progressively become more careless towards protection of their passwords they use[Gao, *et al*(2013)]. An efficient way was proposed by camouflaging the cursor to prevent shoulder surfing [Sun, *et al*(2018)].

1.1. Background and related work

Graphical password can be ordered into three classifications [Ralph,(1970)] mainly the recognition, recall and cued recall systems. In the first method, the client needs to recall a graphical password and provide it during the validation phase. In the recognition framework the graphical data which is provided to the client in the verification phase from which the client have to make a proper choice that coordinates with the dataset that was previously retained by the database.

The recall based verification methods can be classified in two classes[Weidenbeck, et al(2006),Pegrum, et al(2013),Gao, et al(2013)],i.e. verification & confirmation. In the precise match, during verification, the client creates the same drawing as during the enlistment, Whereas the versatile methods provide some variation among enlistment and confirmation [Ralph,(1970),Lashkari, et al(2009)].

Graphical secret phase validation frameworks can be like wise separated into dynamic and static methods. Static or offline frameworks utilize the doodle picture for validation , whereas the while dynamic frameworks use time capacities removed from the doodle direction. Dynamic methods yield better check execution as compared to static frameworks in area of signature confirmation [Diaz, et al(2015)].

The DAS system was designed in such a way that the 5*5 cell grid helped in tracing of the secret phrase, the cell sequence itself was the secret phrase [Sree and Radha(2014)]. A further improvement to draw a secret was the Background Draw A Secret (BDAS), wherein an image in the background is served with much improved memorability .

A variation to draw a secret, was the Pass Go authentication where the secret phrase was defined based on the sequence of grid intersections [Weidenbeck, et al(2016),Pegrum, et al(2013)].

The doodle authentication used the trajectory coordinates and derivatives of first and second order were utilized as features to group the doodles mentioned [Diaz, et al(2015)].

The Levenshtein distance to compute the distance between two patterns in the static authentication procedure where the sketches in free form were preserved as a sequence of cell relative positions [Peeck,(1993)]. Using the support vector classification [Zaho, et al(2013),Aviv, et al(2014),Curran and Snodgrass (2015)] the method allowed the client to draw various gestures based on predefined symbols at the same time using all fingers.

The android pattern lock [Joshi, *et al*(2012),Patil, *et al*(2015)]found on the phones provides a grid of 3*3 points , client usually makes a pattern connecting the points, making some predefined symbols or some dynamic symbols, various drawbacks were found on this android locks. Also a smudge attack was quite possible on all this android locks, the 3*3 grid pattern was rearranged in various different patterns to study the behavior of clients in choosing strong passwords.[Dias and Reeja,(2018)]

The “shapes of shapes” graphical authentication method [Skinner, (2016)] is based on the concept of bring your own device configurations, as most of the users are unaware of the cyber security threats. This authorization technique is based for the younger demographic. This authorization system provided the user with a static grid of 4*4, with static labels, and a total of 6 geometric shapes in four different colors, providing in total 24 shapes (figure1.1.1). User randomly selects eight symbols (each symbol could be repeated more than once) and places them in the grid as shown in figure 1.1.2, the password generation is based on the label of the grid and the numerical number of the symbol, which provides close to 28 alphanumeric characters as compared to 8 characters of the traditional password.

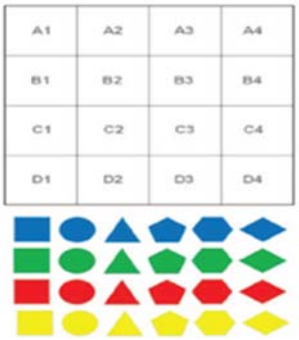

Figure 1.1.1: 4*4 grid with static labels

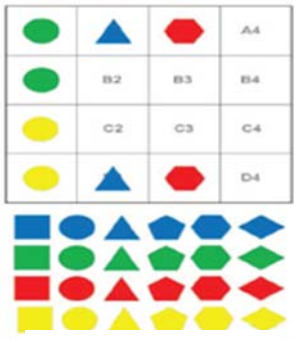

Figure 1.1.2: Random selection of symbols

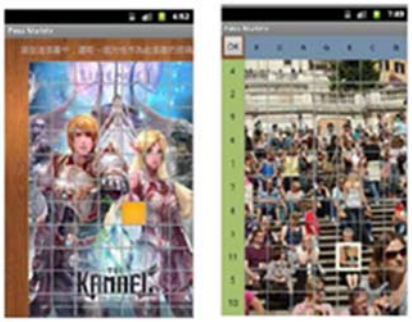

Figure 1.1.3 Shows grid selection point along with horizontal and vertical login indicator

Even though the password space appears to be large, the system does not provide any kind of security from shoulder surfing assault. Privacy can be achieved over Encrypted data [Zheng, *et al*(2020)].

Another graphical authentication scheme[Sun, *et al*(2018)] similar to cued click points[Chiasson, *et al* (2012)] proposed a very innovative technique for hand held devices known as Pass matrix in which the user had to go through a series of three rounds , each image would be discretized into cell or a kind of grid, the user had to select a cell in each image, the selected cell would be highlighted in orange shade(Figure 1.2.3), the login indicator module displays certain predefined characters indicating each row and column that are displayed on the horizontal and vertical direction of the image, a cell chosen by a user would be an intersection of the characters which would act as password, the experimental study shows acceptance by the user , also the system had a drawback as the

users for certain images had selected a common cell , which was very obvious to be a part of the password. This experiment revealed that there is a high probability to trespass in an account through a hot spot guessing attack.

2. Problem Statement

With the increase in the number of online accounts for web services, it becomes very tedious to memorize all the different passwords. When making use of this web services in public, there are chances of these passwords being exposed unknowingly to people with wrong intention. Once the passwords are compromised it is obvious that it will be of a great danger to one's asset. In the proposed method we try to overcome the problem of shoulder surfing assault.

The following problems are assessed in this study.

i. Can the System be easily attacked?
ii. Is there an improvement in the password space for the proposed model?
iii. Is there a significant difference in the time required to login ?
iv. Is there a significant difference in the memorability of the password?

2.1 Assumptions

In this paper we assume that

i. The attackers will not be able to eavesdrop or attack the packets during transmission as the communication between the participating devices is being protected by Secure socket layer.
ii. The devices participating in the communication are trustworthy.
iii. We make sure that the clients using this system for registration are done in a safe environment which is free from people with wrong intentions and surveillance cameras.

3. Proposed Methodology

We introduced "Confusys" which is a new graphical authentication system. This helps to overcome the disadvantages associated with the traditional password system, such as the security and the simplicity in guessing password by merely observing the client while logging into the system.

In confusys the client is allowed to choose a click point per image in a sequence of n images [Dias and Reeja(2020)]. As proposed by chiassion, et al., the CCP method helped the clients to memorize their password easily. In case the client click point is wrong then the client will be provided a different image indicating the client a wrong password. In the confusys system we do not use this approach as our aim is to avoid a shoulder surfing assault. The client is allowed a minimum of 3 attempts to login to the system, after which the system is being blocked for the next 24 hours. Figure 3.1.1 explains the registration process. The system proposed by [Shen,*et al*(2018)], will not be capable to identify the hand movements as each time, hand movements are bound to change.

3.1 Overview

The confusys is composed of the following modules

Registration module
i. Discretization of image,
ii. Region of Interest, iii.
iii. Data collection module

Login module
i. Befog module,
ii. Verification Module

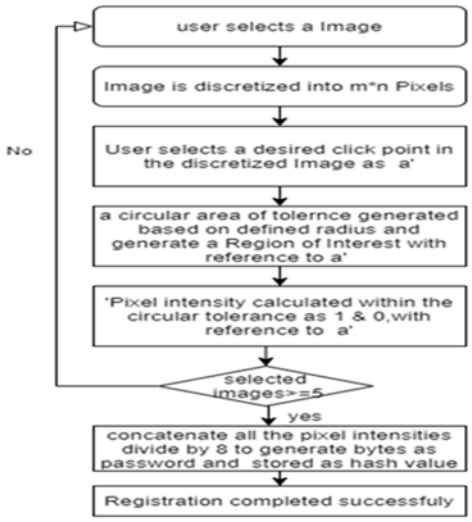

Figure 3.1.1 Confusys Registration Process

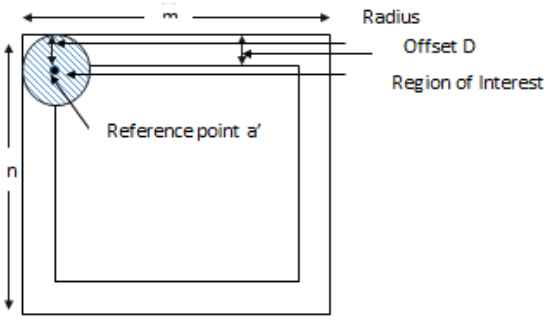

Figure 3.1.2: Image m*n, Indicating Reference point a', offset on all 4 direction, Region of Interest (Shaded Area)

3.1.2 Discretization of Image

The image is presented to the user in a discretized form. 12 standard Images were used from the publicly available dataset of compcars [15]. We have considered three different standard Image sizes 451*221, 640*480 and 1024*768. User has to select a click point in the image; the click point in the image will generate a tolerance area around the chosen click point, based on the predefined radius which is of 6px, 7px, 8px or 9px. The number of points available to choose depends upon the radius of the tolerance area. An offset is considered in an Image on all the four edges. This offset is a non-clickable area which is defined based on the radius .The aim is to allow full circle tolerance. In Simple words: (figure 3.1.2)

- Consider a 2D discretized Image (m*n) Pixels.
- Assuming a random point selection (X,Y) in 2D Image called as the reference point a'.
- Let D be the offset in (m*n)image on all the four edges
- Tolerance area will be calculated based on the radius r and the reference point a', this region is called as the region of Interest (ROI)

3.1.3 Generation of ROI

By applying the midpoint technique, the ROI function is defined as stated below [Jia, *et al*(2011)]

$$ROI(x,y)= x^2+y^2-r^2 \quad (1)$$

The equation ROI(x, y) =0 will be satisfied for any point (x, y) on the circle boundary with radius r. The ROI function will be negative in case the point is interior of ROI, and will be positive if the point is outside the ROI.

$$ROI(x, y)= \begin{cases} <0 & \text{if(x,y) is inside ROI} \\ =0 & \text{if(x,y) is inside ROI} \\ >0 & \text{if(x,y) is outside ROI} \end{cases} \quad (2)$$

Figure 3.1.3 indicates the midpoint between two contesting pixels at location x_j+1.

We assume that after an initial plot of (x_j, y_j), we require to judge the next position of the pixel whether it will be at (x_j+1, y_j) or at $(x_j+1, y_j -1)$ which will be closer to the boundary of ROI.
Based on the ROI function Equ. (1)the midpoint will be calculated between the two contesting points

$$Pj=ROI\ (x_j+1, y_j-1/2)$$
$$=(x_j+1)^2 +(y_j-1/2)^2-r^2 \quad (3)$$

If $p_j<0$, the midpoint will be interior of ROI and the pixel on the line y_j will be closer to the ROI boundary else the location of this point will be on the exterior or on the ROI boundary, so the pixel on the line y_j-1 will be selected.
The successive calculations can be carried out using the ROI function at sampling positions

$$x_j+1 +1=x_j+2:$$
$$P_j+1=ROI\ (x_j+1 +1, y_j+1-1/2)$$
$$=[(x_k+1)+1]^2+(y_j+1-1/2)^2-r^2 \quad (4)$$

Depending on the sign of p_j , y_j+1 may be y_k-1 or y_k .
To obtain the further points p_j+1, it will be either $2x_j+1$(in case p_j is negative) else it will be :

$$2x_j+1+1-2y_j+1$$

The terms $2x_j +1$and $2y_j+1$ can be successively evaluated as

$$2x_j +1 = 2x_j +2$$
$$2y_j+1 = 2y_j- 2$$

Evaluating the ROI function Equ.(1) at the start position (x0,y0)=(0,r) the initial decision parameter can be obtained

$$p_0=ROI\ (1,r-1/2)$$
$$= 1+(r-1/2)^2-r^2$$

This can be also written as

$$p_0=(5/4)-r \text{ or } (1-r) \quad (5)$$

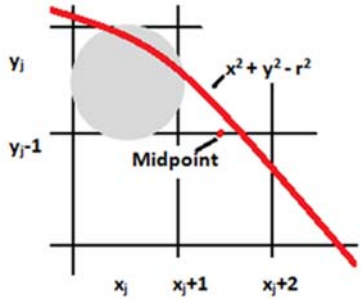

Figure 3.1.3: Midpoint between two contesting pixels at a sample position x_j+1

3.1.4 Data Collection module

The Data within the ROI boundary is retrieved based on the pixel intensity, by comparing each of the pixels with the reference pixel within the boundary. The ROI is applied in a concentric fashion such that the data within the boundary is computed. The intensity of each pixel is computed by converting it into gray scale.
I=Brightness of each pixel

f_r→ red channel intensity at (x, y)
f_g→ green channel intensity at(x, y)
f_b→ blue channel intensity at(x, y)

$$I=0.30\ f_r +0.59\ f_g+0.11\ f_b \quad (6)$$

Using the predefined values of red, green and blue channel, we obtain the intensity in grey scale.
We create a binary test f defined as follows, Where $f(a'; ci[i_0 \ldots i_{n-1}])$ is defined as:

$$f(a'; ci[i_0 \ldots i_{n-1}]) = \begin{cases} 1: & I(a'(x)) < c_i[i_0 \ldots i_{n-1}] \\ 0: & I(a'(x)) > c_i[i_0 \ldots i_{n-1}] \end{cases} \quad (7)$$

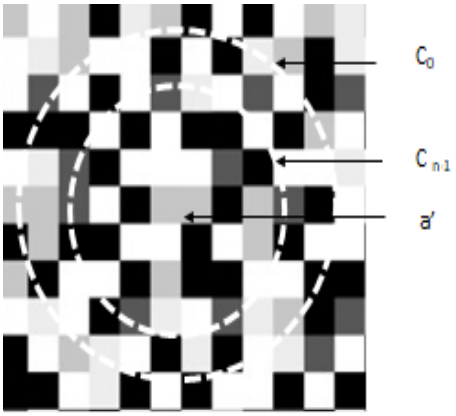

Figure 3.1.2: Pixelated Image data collected on c_0 to c_{n-1}, also shows reference Pixel a'

Figure 3.1.2 shows enlarged view of a pixelated image where a´ is the click point selected by the user. The concentric dotted circles c0 indicate the boundary of ROI, data is collected in the form of bits with respect to each pixel from c_0 to c_{n-1}

For example

C_0= [11010……000111]
C_1= [00100……010100]
C_2= [10101……101001]
C_{n-1}=[01010……111001]

Further these set of bits c0 to cn-1 are concatenated divide by 8 which gives us the total number of bytes in the ROI, a hash of these bytes is calculated and stored in the database using hashing techniques [Andrade, et al(2016)] Now $(c_0||c_1||c_2||\ldots\ldots||c_{n-1})/8$→ number of bytes/ROI considering only integer values. $b_0 \ldots b_{n-1}$ indicates the bytes. H indicates the hash value

$$P=(H(b_0),H(b_1),H(b_2),\ldots\ldots\ldots,H(b_{n-1}))$$

Where p is the final hashed password.

3.2 Authentication phase

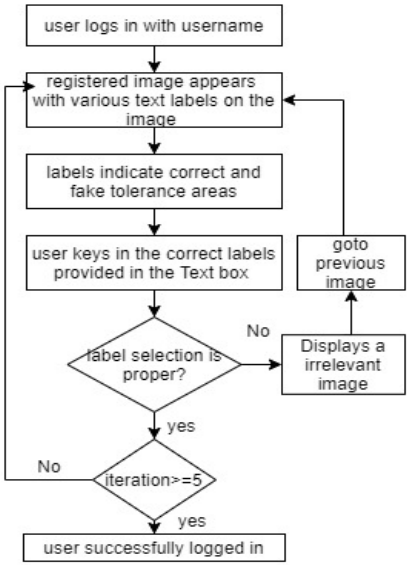

Figure 3.2: shows the flow chart for authentication of the users

3.2.1 Befog Module

The user once logged into the system with the username and password will be provided with the initial image that was chosen as the user. This module acts as a confusion module for an attacker, who is trying to perform a shoulder surfing assault on the system.

The initial image is displayed to the user with the actual ROI as shown in the figure, along with other dummy ROI, to perplex the attacker similar ROI is display on the entire image. Only the actual user will know the correct ROI. These ROI are displayed with a character or two. (Figure 3.2.1)

In the befog module, translation of ROI is performed in all the neighboring directions covering the entire image i.e. (m*n)

Let

- coordinates of the Initial ROI a' =(X_{old}, Y_{old})
- After Translation, coordinates of the object a' will be = (X_{new}, Y_{new})
- Shift Vector= (T_x, T_y)

Given the translation vector

The distance by which the X_{old} coordinate has to be moved is defined by T_x

The distance by which Y_{old} coordinate has to be moved is defined by T_y

The New translation will be obtained by summing up the new translation coordinates to the old coordinates of the object as

$$X_{new}= T_x+ X_{old} \quad (8)$$

(Denotes the Translation towards X axis)

$$Y_{new}= T_y+ Y_{old} \quad (9)$$

(Denotes the translation towards y axis)

The labels with respect to each ROI are produced based on combination of alphanumeric characters and letters. For a combination of only alphanumeric characters may be calculated as $(26+10)^2 = 1296$ combinations. If capital letters are also included, then the result will be $(10+26+26)^2 = 3844$. If only letters are used then it gives a combination of $(26)^2= 676$ combinations [Balen and wang,(2015)].

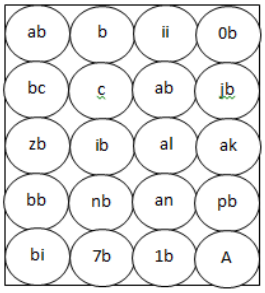

Figure 3.2.1: befog module, indicating Dummy ROI

3.2.2 Verification Module

A label represents a subset of bytes[D_0,D_1,D_2……,D_{m-1}] from superset [C_0,C_1,C_2,C_3……,C_{n-1}] per ROI

If the similarity of the label is 100% then the user will be granted access.

A Correct label represents random bytes from ROI base on [C_0, C_1, C_2, C_3……, C_{n-1}]

Using Jacard similarity coefficient, we measure the diversity and similarity of the finite sample set which is defined as the intersection and union of the sample set.

$J(C_1,D_2)=|C_1 \cap D_2|/ |C_1 \cup D_2|$

$= |C_1 \cap D_2|/ |C_1|+ |D_2| - |C_1 \cap D_2|$

Both the objects sets C and D with n binary attributes. The Jaccard Similarity coefficient is a useful measure on the overlap that C & D share with their attributes.

The total number of each combination of attributes for both C & D are as follows.

P11 Indicates total number of attributes where C & D contain the same value as 1.

P01 Indicates total number of attributes where C is 0 & D contains a value of 1.

P10 Indicates total number of attributes where C is 1 & D contains a value of 0.

P00 Indicates total number of attributes where C & D both contain a value of 0.

The entire Pattern must fall into one of these categories

P11+P01+P10+P00=n

The similarity coefficient will be calculated

$$J= P11/ (P01+P10+P11) \quad (10)$$

Every time the user logs into the system there will always be a variation in the objects of set D that try to map with the objects in set C, along with this , the percentage required for the objects to map also varies randomly across all the images. If the user logs into the system for the first time the system will automatically set a percentage across each image to compute the similarity coefficient
If the mapping across all the five images i.e. If the similarity coefficient is 100% the user will be granted access to the system

4. Design of the Experimental Procedure

To carry out the experiment at total of 60 candidates participated in the study, the candidates were in the age group of 16 to 35 years old (m=23.5 ,sd=5.2). The group consisted of 40 undergraduate students and 20 staff all of them were well versed with use of internet. None of the participants had any kind of relation with the research carried out, so as to avoid any kind of biasing done to the final result. The groups were divided into two . The 1st group were provided with the full image and the second group were provided with the same set of images but these images were provided with saliency masks [Mikusz,(2016)] .

The idea behind providing saliency mask to the images was to find out the probable hotspots which was carried out using saliency maps and saliency filters. Both the groups were initially trained on object detection methods, so that the prominent locations on the images could be avoided. The entire user study was carried out in two phases, In Phase one, the participants were explained how to create a graphical password, similarly in phase two, the same group was again asked to create graphical password, on the same set of images which were processed using saliency filters.

We analyzed on the following research objectives

RO1- What is the probability of attacking the system successfully.
RO2- Is there a improvement in the password space for the proposed model
RO3- Is there a significant difference in the time required to login
RO4- Is there a significant difference in the memorability of the password

Also further we calculated the image complexity in terms of bits for both the masked and unmasked images. Table 4.1 below summarizes the complexity of the images used for both the groups.

Image Id	1	2	3	4	5	6	7	8	9	10
Complexity for group 1 Images	7.62	7.57	7.49	7.32	7.54	7.66	7.64	7.44	7.56	7.59
Complexity for group 2 Images	7.45	7.54	7.40	7.39	7.43	7.58	7.67	7.49	7.55	7.54

Table 4.1 Complexity of Images

RO1- What is the probability of attacking the system successfully.(Answering this question will help us to understand how difficult it is to attack the proposed system)

4.1 Security Analysis

This section deals with the security of the proposed confusys authentication method .here we discuss about the random guessing attack.
In order to do a random attack , the attacker will have to randomly select the ROI appearing on the Image until a successful login is indicated
We define A_ij_k be the event that the i^{th} chosen ROI in the image is correct in the j^{th} attempt (i=1,2,…,5; $1<=j_k<=3$)
Such that

$$1 <= \sum_{k=1}^{5}(j_k \leq 3) \quad (11)$$

Than it can be easily seen that the chances of attacking the system i.e. the probability of a successful attack on the system can be given as:

$$P[A]= n(A)/n(S) \quad (12)$$

Where A is the attack, n(A) is the number of attack can occur, n(S) is the number of ways in which the attacker can proceed with the experiments
The advantage of this method is that it is not an approximation but an accurate description of the frequency with which the event A will occur, the chances of a successful attack is with a probability of only **0.36**, which is very less.

A further analysis on the various ROI with different dimension is stated in the table 4.1.1below:

Image Size	R.O.I in Px.	Chances of successfully cracking the system
451*221	6	7.63183 e^{-15}
	7	3.92459 e^{-14}
	8	1.56492 e^{-13}
	9	4.11523 e^{-13}
640*480	6	2.65032 e^{-17}
	7	1.19273 e^{-16}
	8	5.40365 e^{-16}
	9	1.60248 e^{-15}
1024*768	6	2.27092 e^{-19}
	7	1.05055 e^{-18}
	8	4.39347 e^{-18}
	9	1.38936 e^{-17}

Table 4.1.1: Probability of attacking the system

The table 4.1.1 above shows how weak are the chances for a successful attack with different image dimension with different ROI, which clearly indicates that the chances of successful attack is very less.

RO2- Is there a significant difference in the password space for the proposed model.(Answering this question will help us to understand what is the password space as compared to traditional authentication methods)

4.2 Implementation and Calculation of password space

The confusys prototype is built using Visual studio Community 2019. Once the user is connected to the internet, client can get registered to use the system. The client side for this prototype uses HTML5, CSS 3 and JavaScript to build the user interface and also to implement the functions like Discretization of image, Region of Interest, Data collection module, Befog module. C# and MYSQL are used on the server side for the Verification Module which helps in storing and retrieving registered accounts from the database

As mentioned earlier our proposed system is designed to work with three different standard image sizes of 451*221, 640*480 and 1024*768, with a ROI,radius of 6px, 7px, 8px and 9px.

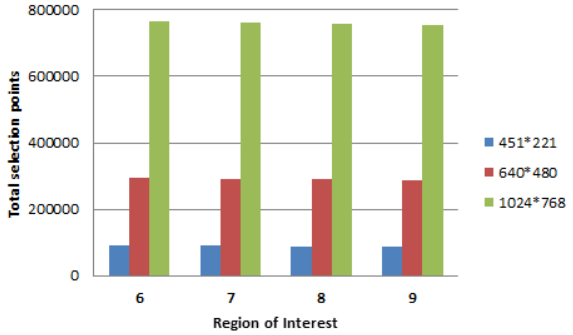

Figure 4.2.1: Number of clickable points on Images with different Dimensions

Figure 4.2.1 shows the number of clickable points in a single image of all three dimensions which were calculated for radius of 6px, 7px, 8px and 9px respectively, these points were are excluding the offset area, Similarly figure 4.2.2 is a comparison graph with single image and five images which indicate a very high rise in the selection points the x-axis indicate the radius any the y-axis indicate the number of possible password.

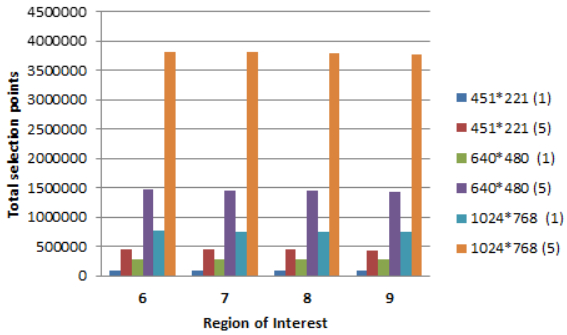

Figure 4.2.2: Comparison with number of clickable points with one and five images

A study was also conducted on the number of available Region of interest for the different radius excluding the offset area. The following graphs represent the number of ROI in single dimension on X and Y axis. These ROI on X and Y axis when multiplied will provide the number of ROI per Image, so also when multiplied by 5 it will provide the total number of ROI for the entire authentication process Figure (4.2.3 to 4.2..6) to indicate the ROI for radius 6px, 7px, 8px and 9px.

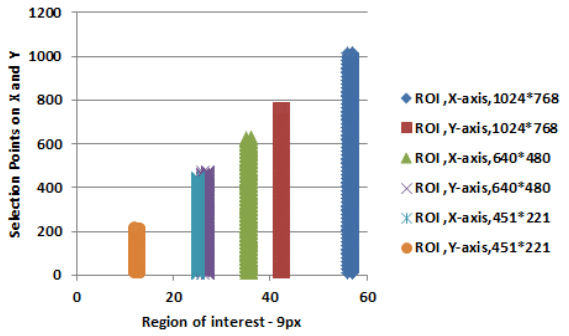

Figure 4.2.3: Region of Interest r=9px- Single dimension

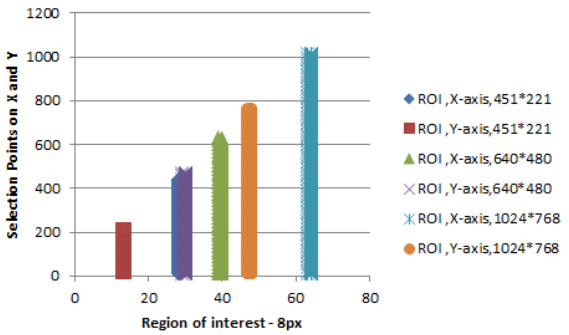

Figure 4.2.4: Region of Interest r=8px- Single dimension

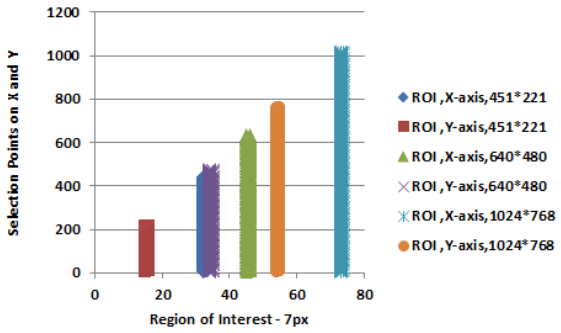

Figure 4.2.5 Region of Interest r=7px- Single dimension

The above Figures (4.2.3-4.2.6) is a scatter graph with markers indicating a clear rise in the number of ROI as we move from radius 6-9.figure 4.7 indicate the Region of interest that will be generated for the entire authentication system

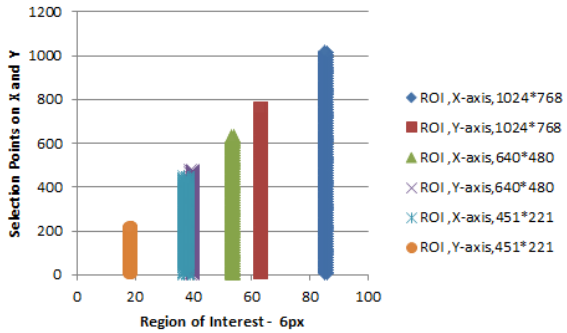

Figure 4.2.6: Region of Interest r=6px- Single dimension

This figure indicates the ROI that can be generated for a combination of all the four radius, the highest number of ROI that can be generated is when the all the five images are of the 1024*768 dimension and of the same radius i.e. 6px which generates about approx. 26775 ROI. This system gives the user, freedom to choose any one of the 54 combinations to set the user password which is illustrated in Figure 4.2.7.

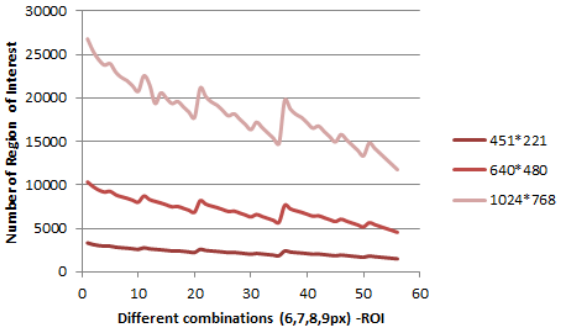

Figure 4.2.7: comparison with a combination of different ROI

4.3 Password Strength

To determine the measure of the password strength, we evaluate how strong a password will be against the adversaries, so we calculate the password entropy, in simple terms greater the entropy , the stronger will be the password. Table 4.3.1 below shows the password entropy, calculates in terms of bits . The formula to calculate the password entropy is

$$PE=Length*\log_2(Pool)$$

Where PE is the password entropy, length refers to the length of password and Pool, refers to the size from which unique ROI will be selected.

Image Size	ROI- (with Radius # Px)	Password Entropy(in bits)
451*221	6	58.50
	7	56.14
	8	54.14
	9	52.75
640*480	6	66.67
	7	64.50
	8	62.32
	9	60.75
1024*768	6	73.54
	7	71.33
	8	69.26
	9	67.60

Table 4.3.1 Depicts Password entropy in Bits

RO3- Is there a significant difference in the memorability of the password

To analyse this research question we performed independent sample t-test, Images without saliency mask v/s images with saliency mask considering this as independent variable and memory time as the dependent variable. The experiment revealed that the memory time among both the groups was not significantly different (t(45)=-1.056, p=.287; memory time of group1 was 212.21 +/-21.20, whereas with that of the second group was 235.01 +/-18.29 h. Figure 4.3.1 below shows a sample images used with group1 and group 2 i.e with and without saliency mask.

Figure 4.3.1: Image (a) without sailency mask;(b) with Sailency mask

RO4- Is there a significant difference in the time required to login
The time that was required to login in to the system were analyzed using R[Core Team,(2015)] and the lme4 package[Bates],which enabled to handle the variables under study. In total 600 login session were registered over a period of five weeks with a gap of one week between two weeks, to analyze the effect on memorability. We used ANNOVA statistical tool for the same since it can handle missing data. We considered failed events while logging in with a successful attempt. P-values were obtained, the analysis revealed that there was an impact on the time requires to login ($x^2(1)=1.002$,p=.29)the mean login time for the 1st duration was 18.11 +/- 2.04 s, whereas for the 2nd duration the mean login time was 10.06 +/- 3.2. Figure 4.3.2 represents the mean login time required during 1st and 2nd duration.

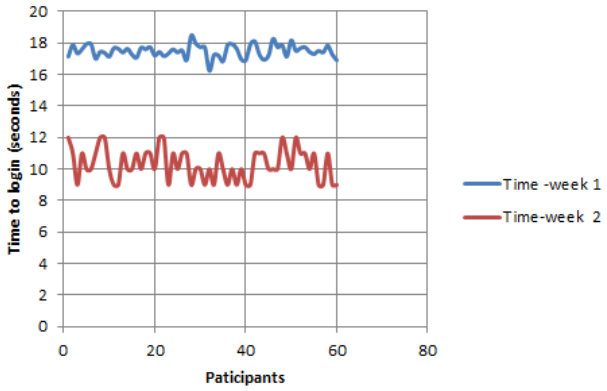

Figure 4.3.2: mean login time required by both the groups

5. Conclusion & Future Scope

We presented “confusys”, method, a graphical authentication system which helps to overcome the memorability issues and also improving the password space . The befog module plays a very important role in the system as it enhances the confusion rate of attack .we obtained a satisfactory result from all our research observation. The probability of attacking the system is very less, which lies in the range of (7.63183 e-15 to 4.11523 e-13), (2.65032 e-17 to 1.60248 e-15), (2.27092 e-19 to 1.38936 e-17) for 451*221, 640*480 and 1024*768respectively. Similarly, the second research objective where the password strength was calculated in terms of entropy in bits and it was in the range of(258 - 252),(266 -260), (273-267) for all the three image dimensions respectively.

The third research objective also proved that even though the images were provided to the user group with and without saliency mask, still the users were able to memorize their password with an ease.

Our last research objective was to check for the login duration aver a period of time, the average time taken by the users to login was 11 sec.The befog module helps evading the shoulder surfing attack as it keeps on modifying

the the characters entered by the user for every login, The befog module can provide ROI's with 3844 different unique combinations of characters per image.

The reliability of the system was checked by performing the usability experiment and a statistical analysis as to how it affects the memorability of the users. The usability test also helped to determine the accuracy of the system. A further enhancement to the system can be done by setting up cameras at certain angle in a closed environment trying to perform a guessing attack and also build a dictionary

Acknowledgement
The Research behind this paper would not have been possible without the continuous support of my Guide Dr. Mouleeswaran S.K. and Dr Reeja S.R, Their Knowledge in this area has kept my work on track, right from the inception of the idea till the implementation and to prepare the final draft of the paper. I am very grateful to the generosity and expertise of one and all who helped me in improving this study in a much better way and prevented from making many errors.

Reference

[1] Andrade E, Simplicio M, Barreto P, Santos P,2016, Efficient Password Hashing Techniques with High Security against Time –Memory trade Offs, IEEE Transactions on computers,DOi:10.1109/TC.2016.2516011
[2] Aviv A, Fichter D,2014, Understanding visual perceptions of usability and security on android graphical password pattern, Proceedings of the 30th Annual computer security applications conference ACM 2014, pg.286-295, DOI:10.1145/2664243.2664253
[3] Balen V N , Wang H, GridMap: Enhanced Security in Cued-Recall Graphical Passwords, International Conference on Security and Privacy in Communication Systems, November 2015,DOI:10.1007/978-3-319-23829-6_6
[4] Bates, D , Machler B, and Walker. Fitting Linear mixed-effects models using lme4
[5] Chiasson S, Stobert E, Forget A, Biddle R,2012, Persuasive Cued Click points: Design and Implementation , and evaluation of Knowledge based authentication Mechanism, IEEE Transaction on Dependable and secure Computing, DOI:10.1109/TDSC.2011.55
[6] Curran K, Snodgrass A, 2015,A novel cue based picture word shape character password creation scheme, International Journal of Digital Crimes and Forensics DOI:10.4018/IJDCF.2015070103
[7] Dias N, Reeja S R,2020,An Improvement of Compelling Graphical Confirmation plan and cryptography for upgrading the information security and preventing Shoulder Surfing Assault, Advances in Intelligent Systems and Computing Pp:435-453 (AISC Volume 1070) Springer Nature Switzerland DOI:10.1007/978-3-030-32523-7_30
[8] Dias N, Reeja S R,2018, A quantitative report on the present strategies of Graphical authentication, International Journal of Computer Sciences and Engineering, Vol.6, Special Issue.10, Nov 2018 E-ISSN: 2347-2693, https://doi.org/10.26438/ijcse/v6si10.6473
[9] Diaz M M, Fierrez J, Galbally J 2015, Graphical Password based user authentication with free from doodles,IEEE Transaction on Human Machine systems,DOI;10.1109/THMS.2015.2504101
[10] Gao H, Wei Jia, Fei Ye, Licheng Ma, 2013, A survey on use of graphical Password, Security, Journal of software, DOI:10.4304/JSW.8.7.1678-1698
[11] Zheng Y, Lu R, Guan Y, Shao J, Zhu H, 2020, Achieving efficient and Privacy Exact set Similarity search over Encrypted data, IEEE Transactions on Dependable and secure computing , DOI:10.1109/TDSC.2020.3004442
[12] Jia L, Peng C, Liu H, Wang Z,2011,A fast randomized circle detection algorithm,4th international congress and Image processing IEEE Xplore, DOI:10.1109/CISP.2011.6100372s
[13] Joshi A, Kumar S, Goudar R,2012,"A more multifactor secure authentication scheme based on graphical authentication " Advances in computing and communication IEEE, International conference DOI: 10.1109/ICACC.2012.43
[14] Lashkari,A, Farmand S, Zakaria O, Saleh R,2009 November ,Shoulder surfing attack in graphical password authentication, International Journal of Computer science and Information Security, Vol 6, No2, pp.145-154
[15] Mikusz M, Florian Alt ,Schneegass S, Bulling A, 2016, Memorability of Cued-Recall Graphical Passswords with Sailency Masks
[16] Ralph H N,1970, ,How we remember what we see", Scientific American, Volume 222,Number 5,pg:104-112, DOI:10.1038/scientificamerican0570-104
[17] Patil A, Patil K, Shah Z, Devendra, Godeshwar A, 2015,Towards an efficient method for graphical Password authentication, International Journal of Research in Applied Science & Engineering Technology vol.3,Issue II, ISSN:2321-9653
[18] Peeck J,1993,Increasing Picture effects in learning from illustrated Text learning and instructions, Learning and Instructions, Vol. 3,Issue 3, Pg. 227-238, DOI:10.1016/0959-4752(93)90006-L
[19] Pegrum M, Oakley G, Faulkner R,2013, A study on the adoption of mobile handheld technologies in western Australian independent schools, Australian Journal of Educational technology DOI:10.14742/ajet.64
[20] Shen C, Chen Y, Liu Y, Guan X,2018,Adaptive Human Machine Interactive behavior analysis with Wrist worn Devices for Password Inference, IEEE Transactions on Neural Network and Learning System, DOI:10.1109/TNNLS.2018.2829223
[21] Skinner G , 2016 ,cyber security for younger demographic, A graphic based authentication and authorization framework, IEEE Proceeding of International Conference ,DOI: 10.1109/TENCON.2016.7848481
[22] Sree SR, N. Radha,2014, A Survey on different graphical password Authentication technique, International Journal of Innovative Research in Computer and Communication Engineering , Vol 2 , Issue 12, December ,ISSN:2320-9801
[23] Sun H-M, Chen S, Yeh J, Cheng C,2018,A Shoulder Surfing resistant graphical Authentication System, IEEE Transaction on Dependable and secure computing vol. 5, No 2, DOI:10.1109/TDSC.2016.2539942
[24] Weidenbeck S, Waters J, Sobrado L, Birget J,2006,Design and evaluation of shoulder surfing resistant graphical password scheme, Proceedings of the working conference on Advanced visual interfaces, DOI:10.1145/1133265.1133303
[25] Yang L, Luo P, Loy C, Tang X,2015,A large scale car dataset for fine Grained categorization and verification, IEEE Conference on Computer Vision and Pattern Recognition, DOI: 10.1109/CVPR.2015.7299023
[26] Zhao Xi, Feng T, Shi W, 2013,Continuous mobile authentication using a novel graphic touch gesture feature, Biometrics Theory, Applications and system' IEEE, Sixth International Conference DOI: 10.1109/BTAS.2013.6712747
[27] R: A language and Environment for statistical Computing, Core Team,2015

Authors

Mr Norman Dias is a research scholar at Dayananda Sagar University Bengaluru, he pursued Bachelor of Computer Engineering from Goa University and Master of Computer Science in year 2013. He also pursued PG Diploma in Embedded Systen and Design at Centre of Development and Advanced Computing C-DAC, Kolkata. He is currently working as Assistant Professor in Department of Computer Engineering, at Don Bosco College of Engineering, Goa University since 2014.. His main research work focuses on Human Computer Interaction. . He has 9 years of teaching experience.

Dr. S.K Mouleeswaran working as Assistant Professor in the department of Computer Engineering at Dayananda Sagar University. He earned his doctorate from Anna University Chennai, Masters (M.E) from Anna University Chennai and B.E (CSE) from Bharadidasan University Trichy. He has more than 14 years of Teaching, 2 years of Industry and 8 years of Research experience. He has many publications in reputed journals, conferences and guided both UG and PG thesis.
His research interests are in the areas of Cloud computing, IoT, Computer Networks, Software Engineering, Network security and Mobile Computing.

Dr Reeja S R a Professor in the Department of Computer Science and Engineering,at VIT AP. She earned her Ph.D in Computer Science & Engineering from Visvesvaraya Technological University (VTU), Govt. of Karnataka for her thesis Real Time Video Denoising. She has nearly 12 years of teaching experience in various engineering colleges and 5 years of research experience in the concerned field. She has worked in VSSC/ISRO as a Research Assistant in QRSG (Quality Assurance & Reliability Software & mission Group) for 1 year. She has published 8 international Journal, 1 national journal, 5 international conferences and 3 national conferences. She was also a Programme committee member for the first international conference on bioinformatics and bioscience (ICBB) held in Pune, first international conference on Computer science and information technology (CoSIT) held in Royal orchid centre Bangalore, the second international conference on Artificial intelligence and Application(ARIR) in Switzerland and the fourth international conference on Natural Language Processing (NLP) in Australia and Editorial Board member of an international journal Signal and image processing(SIPIJ).