DOI 10.12694/scpe.v20i1.1460
Scalable Computing: Practice and Experience ISSN 1895-1767
Volume 20, Number 1, pp. 101–112. http://www.scpe.org © 2019 SCPE

A PATTERN-BASED MULTI-FACTOR AUTHENTICATION SYSTEM

PANKHURI[*], AKASH SINHA[†], GULSHAN SHRIVASTAVA[‡], AND PRABHAT KUMAR[§]

Abstract. User authentication is an indispensable part of a secure system. The traditional authentication methods have been proved to be vulnerable to different types of security attacks. Artificial intelligence is being applied to crack textual passwords and even CAPTCHAs are being dismantled within few attempts. The use of graphical password as an alternate to the textual passwords for user authentication can be an efficient strategy. However, they have been proved to be susceptible to shoulder surfing like attacks. Advanced authentication systems such as biometrics are secure but require additional infrastructure for efficient implementation. This paper proposes a novel pattern-based multi-factor authentication scheme that uses a combination of text and images resulting for identifying the legitimate users. The proposed system has been mathematically analyzed and has been found to provide much larger password space as compared to simple text based passwords. This renders the proposed system secure against brute force and other dictionary based attacks. Moreover, the use of text along with the images also mitigates the risk of shoulder surfing.

Key words: Security, Password, User authentication, Multi-factor, Pattern-based

AMS subject classifications. 68M12

1. Introduction. Recent advances in the technology have resulted in the development of complex IT based systems for delivering value added services to the users. These systems may store users personal data with aim of providing personalized services to the users. The rapid growth in the demand for personalized services will eventual transform these systems into the storehouses of various types of personal information of the users. This urges for the requirement of having more robust and secure access mechanisms in order to mitigate the various security risks associated with the unauthorized access to these IT systems [1, 2, 3]. This makes the user authentication the most essential and indispensable component of such systems. There are three basic authentication methods which are based on token, biometric and knowledge [4]. Smart cards are token-based authentication system implementing knowledge-based techniques to enhance security as in case with ATM cards having a PIN number. Biometric based authentication techniques, such as fingerprints, iris scan or facial recognition provide highest level of security but are still expensive, slow, unreliable and hence, not yet widely adopted [5]. Knowledge based techniques are the most widely used authentication techniques which include both text and picture-based passwords [6].

The most basic mechanism for authenticating users is by the use of passwords [7]. The concept of using passwords is an efficient and cost effective solution for user authentication. The fundamental requirement for any password is that it should be easy to remember and must be secure enough. In other words, authentication process must be efficient and password must be tough to guess. Text based password continues to be the most widely used form of authentication methods owing to a number of factors such as easy to remember, tough to guess, and small time is required to finish the process. Studies have revealed that users often have a tendency of picking a short password so that it could be easily remembered but unfortunately, these passwords are easy to compromise. This can be attributed to the fact that textual passwords are just a series of characters (numeric, alphanumeric, and special characters) and are usually based on Latin or other well-known scripts supported by the input devices. This renders the textual passwords susceptible to various security attacks. It has been observed that 4.66% of accounts on rockyou.com have been compromised with the help of social engineering, dictionary and brute force attack [8]. As per Open Security Foundation, millions of credit card records has been compromised by the hackers from the big organizations like TRW, Sears Roebuck, Sony Corporation etc. [9]. According to a computer world news article, the security team at a large company ran a network password cracker and within 30 seconds and identified about 80% of the passwords [10].

In light of the above mentioned requirements, this paper proposes a novel pattern-based multi-factor recognition mechanism for user authentication. The proposed mechanism requires a user to enter textual key along

[*] Computer Science and Engineering Department, National Institute of Technology Patna, India (pankhuri.sai@gmail.com)
[†] Computer Science and Engineering Department, National Institute of Technology Patna, India (akash.cse15@nitp.ac.in)
[‡] Computer Science and Engineering Department, National Institute of Technology Patna, India (gulshanstv@gmail.com)
[§] Computer Science and Engineering Department, National Institute of Technology Patna, India (prabhat@nitp.ac.in)

with the clicks at specific areas on multiple graphical images. The combination of text and graphics increases the password space thereby making the authentication mechanism more robust and secure against various types of security threats. This paper further analyzes the storage requirements and the tolerance of the proposed password scheme with respect to different possible combinations of images and text in the proposed mechanism.

The rest of the paper is organized as follows: Section 2 provides the highlights of the existing literature related to the proposed work; Section 3 discusses the proposed system; Section 4 presents a mathematical analysis of the proposed system; and finally, Section 5 concludes the paper along with a brief discussion of the future works.

2. Literature Review. It is well established fact that humans can remember pictures better than text which makes graphical password schemes better alternative to text-based schemes [11]. Moreover, if the number of images is sufficiently large, the possible password space of a graphical password scheme exceeds than that of text-based schemes thereby, offering better resistance to dictionary attacks. In pattern-based recognition techniques, a user is being presented with a set of images and authenticated by recognizing the images he or she selected during the registration stage but in recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Password retention was measured longitudinally three times: at the end of the first session (R1), one week later (R2) and four weeks later (R3), which revealed the following statistics presented in Table 2.1 [12].

Table 2.1
Response towards textual and graphical password scheme [12]

	Mode	**Mean R1**	**Mean R2**	**Mean R3**
No. of incorrect submission	Alphanumeric	1.61	2.82	1.43
	Graphical	0.28	2.44	1.20
Time of correct submission(sec)	Alphanumeric	9.01	22.53	20.76
	Graphical	5.28	9.87	8.99

Table 2.1 clearly depicts that graphical passwords are easy and efficient to implement, and therefore, the chance of incorrect submission and time taken for correct submission is always less than that of alphanumeric passwords. In contrast to graphical passwords, alphanumeric passwords require more effort to remember but their implementation for secure system is simpler. Table 2.2 and 2.3 lists few important statistics related to textual passwords.

Table 2.2
Most common textual passwords [13]

Top 10 Passwords	**Number of users**	**Percentage of use**
123456	1666	0.38
Password	780	0.18
Welcome	436	0.1
Ninja	333	0.08
abc123	250	0.06
123456789	222	0.05
12345678	208	0.05
sunshine	205	0.05
princes	202	0.05
Qwerty	172	0.04

From Table 2.2 and 2.3, it can be inferred that dictionary and brute force attack may decode alphanumeric passwords easily. Graphical password has been employed for implementing the users personal handheld device as

Table 2.3
Most popular structure of textual passwords [14]

Prevalent password	Number of users	Percentage of use
One to six characters	88164	19.91
One to eight character	272885	61.63
More than eight characters	169888	38.37
Only lowercase alpha	146486	38.37
Only uppercase alpha	1778	0.4
Only alpha	148264	33.49
Only numeric	26077	5.89
First capital last symbol	1259	0.28
First capital last number	17464	3.94

the password decoder and the user is being challenged with an image password with few hints [15][7]. Humans have exceptional ability to recognize image, therefore, PassFace Scheme has been implemented with cogno metric or search metric systems requiring user to remember a set of images both during password creation and authentication phase [16][17]. Figure 2.1 depicts the PassFaces grid scheme.

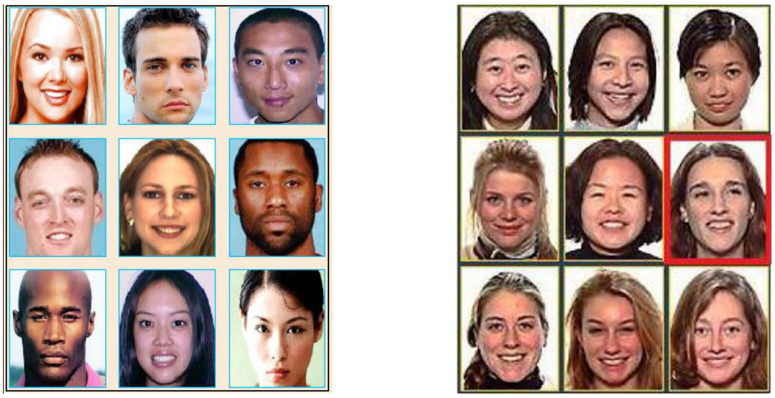

Fig. 2.1. *PassFaces grid [18]*

Hollingworth et al. [19] revealed that people may retain accurate, detailed, visual memories of objects which they attended previously. They suggested that user may remember specific parts of an image more accurately as their password if they are focused upon as shown in Figure 2.2.

In an ideal design, the cue is always helpful for legitimate user during authentication. Cued-recall system requires users to remember particular locations within image which is easier than that of pure recall. These systems may also be called as locimetric due to their reliance on identifying specific location. Sobrado et al.[20] developed a graphical password technique that deals with shoulder surfing problem in which user needs to identify his pre-selected pass objects among objects. User authenticates himself by clicking inside convex hull formed by these objects 2.3.

Sabzevar and Stavrou [15] proposed a methodology in which users need to move a frame along with objects until the pass object in this frame lines up with the other two pass objects. This process may be repeated to reduce the likelihood of getting authenticated randomly but this makes the entire process slow. Jansen et al. [6] proposed a graphical password mechanism for mobile devices in which user enrolls himself by selecting a theme consisting of thumbnail images and then registers a sequence of images as a password. During authentication, the user must enter the registered images in the correct sequence. The basic drawback of this technique is the number of thumbnail images is limited to 30 and hence, the password space is small.Figure 2.4 shows an instance of their second algorithm, where the user is required to move a frame until pass objects line up with

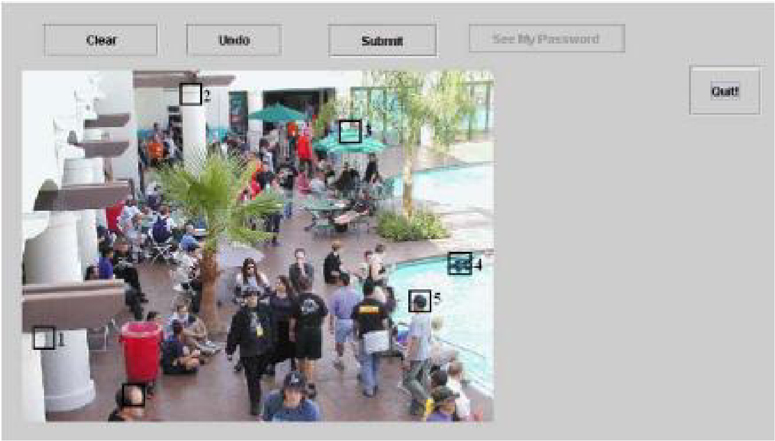

Fig. 2.2. *Cued Recall System [12]*

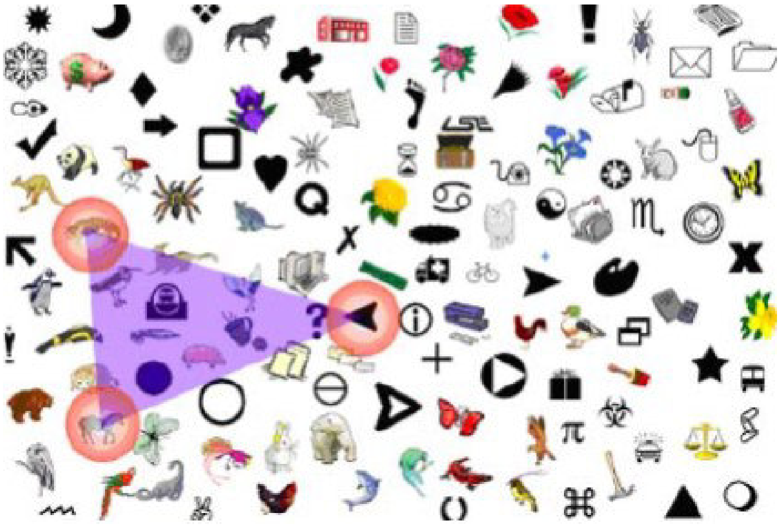

Fig. 2.3. *Convex hull formed with pre-selected objects [20]*

the other two pass objects. The main disadvantage of this is the slow authentication process.

Jansen et. al [6] proposed a graphical password mechanism for mobile devices. In enrollment stage, a user selects a theme which consists of thumbnail images and then registers a sequence of images as a password. During authentication, the user must enter the registered images in the correct sequence. One weak point with this technique is number of thumbnail images are limited to 30 as shown in Figure 2.5. This leads to a smaller password space.

3. Proposed Methodology. This paper implements a pattern-based multi-factor authentication scheme in which a number of images are displayed for a fixed time interval. The user has to click within a predefined area on a particular image for authentication. As the number of clicks increases, the security of the system also increases but at the same time it becomes more complex, therefore, the number of clicks required for authentication may vary as per the requirement of the system. The proposed system also requires a user to enter a key along with the click at specific areas on respective images in the slide show to enhance the level of security. The images considered in the proposed system are of 1360 x 660 pixels, each of which is displayed for an interval of 2.5 seconds during the slide show. Images selected for the authentication are preferably gray scale images to reduce the storage space and to make the process fast. During authentication, user has to input

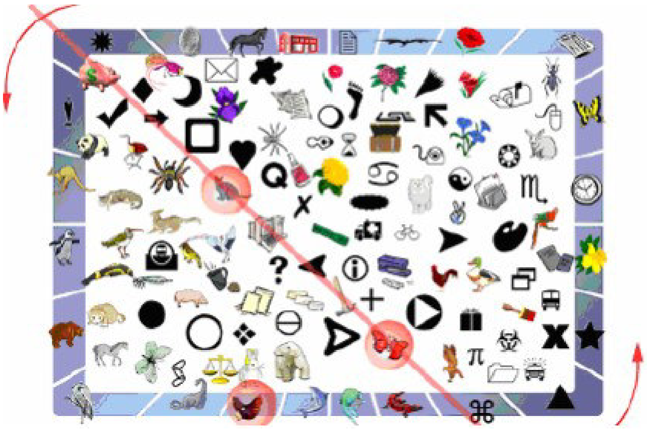

FIG. 2.4. *Alignment of pass object across line [20]*

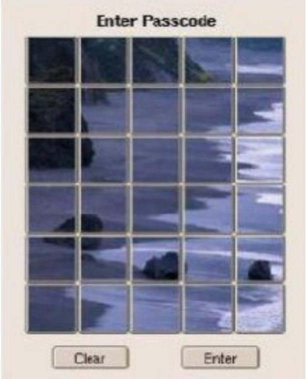

FIG. 2.5. *Grid of 30 thumbnail images [6]*

a key along with the click within a region of size 30 x 30 pixels around particular points in the corresponding images. If the region is too small, it will be more secure but at the same time, false rejection will be high for a genuine user. If this region is too large then it will be easier for the attackers to guess the clickable region. Graphical passwords are easy to remember, however, it is also prone to shoulder surfing, therefore, user has to input some keystroke along with the mouse click which would be difficult for the attacker to notice. The time duration for which each image is being displayed is another crucial factor. Longer the time interval of display, it will be easier for the user to authenticate. But, the authentication process will be much time-consuming and at the same time, attacker will get more time to guess the password. The basic working of the proposed system is as shown in Figure 3.1.

Studies on the Passface technique have shown that people often choose weak and predictable graphical passwords [21]. More research efforts are needed to understand the nature of graphical passwords created by real world users. Passface scheme has a shorter password-space than that of the system discussed in this paper. Davis et al. implemented Passface technique and discovered some obvious patterns among passwords [21]. For example, most users tend to choose faces of people from the same race which makes the Passface password predictable. This is not the case with this system, as different people select different click points in the same image containing many objects. Except for a few exceptions and mouse tracking spywares, it is very difficult for key logging or key listening spywares to crack graphical passwords. Mouse motion co-related with window position, size and timing has to be managed to compromise the graphical password system.

Like text based passwords, most of the graphical passwords including this system, are vulnerable to shoulder surfing [21]. However, adding the input keys in this system may help in preventing it. Recall-based password

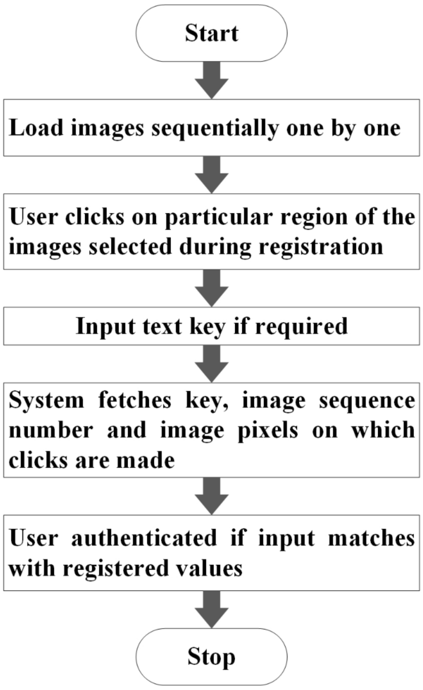
Start
Load images sequentially one by one
User clicks on particular region of the images selected during registration
Input text key if required
System fetches key, image sequence number and image pixels on which clicks are made
User authenticated if input matches with registered values
Stop

Fig. 3.1. *Flow Diagram for the Proposed system*

system is more prone to shoulder surfing than graphical password system. As drawing is being entered on the screen, an attacker needs to see the login process just once for getting the password and recall is not always a difficult task depending on memory prompts or cues. Passwords based on recognition-based techniques are remembered over a longer period of time. The system discussed in this paper provides more resistant to shoulder surfing and efficient than Jansen et. al algorithm [6] which is based on the correct sequence of clicks on the thumbnail images. The proposed system introduces a key, which would be difficult for an attacker to notice along with the correct click. The system discussed here is less confusing than the system used by Sobrado and Brdget for avoiding shoulder surfing as it contains thousands of pass-objects on the screen, out of which user had to select some objects which is being selected during the registration phase [6]. Therefore, introduction of key stroke along with click provide better protection against shoulder-surfing as compared with other algorithms. The formal specification regarding the working of the proposed system has been shown in Algorithm 1. The algorithm considers that the user has to click on *5* images (image1, image2, image3, image4 and image7) out of n images. Moreover, the user also enters an additional textual key along with the click on *image1*.

*The considered password string is : $\{a, 001, (615, 335), (555, 320), (1052, 335), (115, 160), (327, 695), 1111001\}$. Here a is the key during the first click and (615, 335),(553, 320),(1052, 335),(115, 160), (327, 695) are the co-ordinate positions of the clicks in the first, second, third, fourth and up to seventh respective images during the enrollment stage. The user does not have much difficulty in remembering the click points as these are well-defined locations inside an image displayed on the screen.

Algorithm 1: Authenticating a user with graphical passwords

```
Input:
    1. mouseX=x-coordinate of mouse when it is being clicked
    2. mouseY=y-coordinate of mouse when it is being clicked
    3. ch=the key entered by the user
    4. mouseClick=boolean variable which returns 1 if mouse is clicked, else 0
Create an array img of $n$ images;
while all images not loaded do
    track status;
end
$i \leftarrow 1$
while $i <= n$ do
    display img[i] for 2.5 sec;
    if i=1 and mouseClick=yes and mouseX $\geq$ (615-15) and mouseX$\leq$(615+15) and mouseY$\geq$(335-15)
      and mouseY$\leq$(335+15) and ch=a then
        $click1 \leftarrow 1$
    end
    if i=2 and mouseClick=yes and click1=1 and mouseX$\geq$(555-15) and mouseX$\leq$(555+15) and
      mouseY$\geq$(320-15) and mouseY$\geq$(320+15) then
        $click2 \leftarrow 1$
    end
    if i=3 and mouseClick=yes and click2=1 and mouseX$\geq$(1052-15) and mouseX$\leq$(1052+15) and
      mouseY$\geq$(335-15) and mouseY$\leq$(335+15) then
        $click3 \leftarrow 1$
    end
    if i=4 and mouseClick=yes and click3=1 and mouseX$\geq$(115-15) and mouseX$\leq$(115+15) and
      mouseY$\geq$(160-15) and mouseY$\geq$(160+15) then
        $click4 \leftarrow 1$
    end
    if i=7 and mouseClick=yes and click4=1 and mouseX$\geq$(327-15) and mouseX$\leq$(327+15) and
      mouseY$\geq$(695-15) and mouseY$\leq$695+15 then
        print "USER AUTHENTICATED";
    end
    $i \leftarrow i + 1$
end
```

4. Discussion and Analysis. This section provides a mathematical analysis of the proposed system in terms of password space, storage requirement and tolerance level. The discussion is supported using a number of case studies in order to justify the efficiency of the proposed work.

Password Space

User needs to input an ASCII character as a key. Each key can take 2^7 different values.
Size of key = 1 Character
Password space for the keys= 2^7
Size of each image= 1360 x 660 pixels
Tolerance= 30 x 30 pixels
Hence, number of square grids for clicking = (1360 x 660) / (30 x 30) = 997

Consider the total number of images = 7
However, only 5 images have to be selected out of 7.

Number of possible ways in which this can be done is ${}^{7}C_5 = 21$
Total number of clicks required = 5
Password space for this = 21 x $(997)^5 = 2^{52.61}$

If key is input with the first click, password space of the system = (2^7) x $(2^{52.61})$ =$2^{59.61}$
However, the key can be input with any of the 5 clicks.
So, total Password space of the system = 5 x $(2^{59.61}) = 2^{61.93}$
This is greater than that of password space of an 8-character (ASCII) alphanumeric password, which is $(2^7)^8 = 2^{56}$.

A super computer may test 100 million passwords every second. Therefore, time required to test 10^7 passwords = 1s
Time required to test $2^{23.25}$ passwords = 1s
Time required to test $2^{61.93}$ passwords = $(2^{61.93})$ / $(2^{23.25})$ = $2^{38.68}$s = 13964.76 years = 14 thousand years (approx.)
Time required to test 2^{56} passwords = (2^{56}) / $(2^{23.25})$ = $2^{32.75}$ seconds = 229 years
Hence, it can be clearly deduced that it would be infeasible to use even a supercomputer for a brute force attack on the proposed system. Table 4.1 shows that there is no much difference in password space, however, the time required to brute force graphical password is 60 times greater than that of textual password system. Hence, graphical password with 7 images and key of length 1 byte is 60 times more secure than textual password.

Table 4.1
Comparison of textual and graphical password system

Password system	**Password space**	**Time required to brute force**
Textual password of length 8 characters	2^{56}	229 years
Graphical password with 7 images in slide show and key of length 1 byte	$2^{61.93}$	13964 years (almost 14 thousand years)

4.1. Case Study.

The following sub-section presents different case studies with respect to the size of input key, number of images and other crucial parameters of the proposed system.

Case 1.
Size of input key = 4 characters
Number of images = 5
Number of input keys required = 5
Password space for keys = $(2^7)^4 = 2^{28}$
Password space for the clicks = ${}^{7}C_5$ x $(997)^5 = 2^{52.61}$
Total Password space of the system = 2^{28} x $2^{52.61} = 2^{80.61}$
Time required to test $2^{85.78}$ passwords = $(2^{80.61})/(2^{23.25}) = 2^{57.36}$ s = $5.86 * 10^9$ years = $5.86 * 10^3$ million years (approx.)

Case 2. Number of images in slide show = 10
Size of input key = 4 Characters
Number of input keys required = 5
Password space for clicks = $({}^{10}C_5)$ x $(997)^5 = 2^{57.78}$
Total password space of the system = 2^{28} x $2^{57.78} = 2^{85.78}$
Time required to test $2^{85.78}$ passwords = $(2^{85.78})/(2^{23.25}) = 2^{62.53}$ s = $2.11 * 10^{11}$ years = $2.11 * 10^5$ million years (approx.)

Case 3.
Size of input key = 1 Character

Number of images = 6
Total number of clicks required = 5
Password space for the clicks = ${}^{6}C_{5}$ x $(997)^{5} = 2^{52.39}$
The key can be with any of the 5 clicks.
Total password space of the system = $5x(2^{7})$ x $(2^{52.39}) = 2^{61.71}$
Time required to test $2^{61.71}$ passwords = $(2^{61.71})/(2^{23.25})$ s = $2^{38.46}$ s = 11989 years

Memory space is still greater than that of an 8-character long textual ASCII password but it may be reduced if 8-bit gray scale image is being displayed. Hence, total space required to store the slideshow = 6 x 1360 x 660 x 8 bits = 5.14 MB

Case 4.
Let the number of images = 5 Total number of clicks required = 5 Therefore, password space for the clicks = $(997)^{5} = 2^{49.8}$
The key can be input with any of the 5 clicks. Therefore, total password space of the system = 5 x (2^{7}) x $(2^{49.8})$ = $2^{59.12}$
Total space required to store the slide show with gray scale image = 5 x 1360 x 660 x 8 bits = 4.28 MB
Time required to test $2^{59.12}$ passwords = $(2^{59.12})$ / $(2^{23.25})$s = $2^{35.87}$s = 1991 years
Table 4.2 depicts that even if memory storage required for graphical password is much higher than that of textual password but still graphical password is more secure than textual password.

Table 4.2
Comparison of textual and graphical password system with respect of storage memory and time required to brute force

Password system	**Storage memory required**	**Time required to brute force**
Textual password of length 8 characters	56 bits	229 years
Graphical password with 8-bit 6 gray scale images	5.14 MB	12 thousand years
Graphical password with 8-bit 5 gray scale images	4.28 MB	2 thousand years

Case 5.
Let the number of images = 4
Number of clicks required = 4
Password space for clicks = $(997)^{4}$
Total password space of the system = 4 x 2^{7} x $997^{4} = 2^{48}$
Time required to test $2^{29.4}$ passwords = $(2^{48})/(2^{23.25})$s = $2^{24.75}$s = 326 days

Table 4.3
Impact of images and size of key on password space and time required to brute force

Number of images in slide show	**Size of keys in characters**	**Image selected**	**Password space**	**Time required to brute force**
7	1	5	$2^{61.93}$	14 thousand years
5	4	5	$2^{80.61}$	5.86 x 10^{3} million years
10	4	5	$2^{85.78}$	2.11 x 10^{5} million years
6	1	5	$2^{61.71}$	11989 years
5	1	5	$2^{59.21}$	1991 years
4	1	4	2^{48}	326 days

From Table 4.3, it may be concluded that even if the size of textual key is kept same but the number of images during slide show are being doubled then time required to brute force also gets doubled. Increase in size of keys is not as influential as increase in number of images during slide show. If we reduce the number of images to 4, the password space will be less than that of an 8-bit ASCII password (textual). Hence, this case is the optimal case with minimum password space.

Probability of Identifying the correct password by an attacker

Probability of identifying the correct key = $1/(2^7)$
Probability of identifying the correct click with which the key has to be input = 1/5
Probability of identifying the correct region of first click in an image = 1 / ((1360 x 660)px / (30 x 30)px) = 3/2992
Probability of choosing the correct 5 images on which to click out of the 7 images = $1/\ {}^{7}C_5 = 1/21$
Probability of identifying the correct password of the user = (1/5) x (1/128) x (1/21) x $(3/2992)^5$ = 7.54 x $(10)^{-20}$
This is too small. Hence, our graphical authentication system is very less vulnerable to password guessing.
It is clear from Table 4.4 that chances of guessing graphical password will always be less than that of alphanumeric password.

Table 4.4
Identification probability of different password systems

Password System	Identification probability
Alphanumeric password	1.3 x 10^{-17}
Graphical password	7.54 x 10^{-20}

Storage memory space

Graphical passwords require more storage space as compared with textual password but in this era of technological advancement, the storage space for enhancing the security may not be an issue.
Size of each image = 1360 x 660 px
Space taken to store 1 px = 32-bit in a 32-bit display
Total no. of images in our system = 7
Therefore, total space required = 7 x 1360 x 660 x 32 bits = 23.96 MB which is very large.

Case 1: Binary image

Space required to store each pixel = 1 bit
Total space required to store the slideshow = 7 x 1360 x 660 x 1 bits = 767 KB
This is much less than space required in a 32-bit display. Although the number of colors which can be displayed in the image does not effect the proposed system, however, some users might not prefer using binary images as these can cause some inconvenience to them.

Case 2: 8-bit gray scale images

Total space required to store the slideshow = 7 x 1360 x 660 x 8 bits = 6 MB

Table 4.5 depicts the storage requirements for different password systems.

Storage Space for the Proposed System

The password string consists of one key and coordinates (x,y) of each of the 5 clicks.
Space required to store 1 key character = 1 byte
Space required to store 5(click points) x 2(coordinates of each click), i.e. 10 integers = 10 x 2 bytes = 20 bytes
Number of bits required to store input key associated with one of the 7 image = 3 bits
(010 indicate the key has to be entered with 2nd image.) Number of bits required to represent the selected image = 7 bits
(1111001 indicates clicks in 1st, 2nd, 3rd, 4th and 7th images are required respectively)

Table 4.5
Total memory space of different password system

Password system	Storage space required
Textual password length = 8 characters	56 bits
Graphical password Binary image	767 KB
Graphical password 8-Bit gray scale image	6 MB
Graphical password Colored image	23.96 MB

Therefore, total memory space required to store the password string of each user = 3 bits + 1 byte + 20 bytes + 7 bits = 178 bits
The password string will be of the form: key, click, (X1, Y1), (X2, Y2), (X3, Y3), (X4, Y4), (X5, Y5), select
Here, click refers to the sequence number of the click with which key is being associated and select refers to the sequence number of images(in 7 bits) which have been selected by the user. Table 4.6 shows that single password string of length 8 character requires 56 bits of memory while proposed scheme for password requires 178 bits of memory.

Table 4.6
Comparison of memory space requirements

Password system	Space required to store password string
Textual password	56 bits
Proposed scheme of password	178 bits

5. Conclusions and Future Works. User authentication is one of the most important component of a secure system. Even after the development of advanced authentication mechanisms such as biometrics, the traditional concept of passwords still continues to be the most widely adopted means for user authentication. Owing to the limitations and weaknesses of text-based passwords such as smaller password space, susceptibility to brute force and shoulder surfing attacks, etc., this paper proposes a novel pattern-based multi-factor authentication scheme that involves the use of a combination of textual and graphical passwords. The proposed system has a larger password space and is secure against dictionary attacks since it involves additional mouse input along with keyboard input. Moreover, a brute force attack would require automatic generation of all possible mouse-click and text combination in order to crack the actual password. This renders the bruce force attack infeasible for the proposed system.

Traversing through multiple graphical images during the login process can be tedious and time taking process. This also requires maintaining tens of thousands of pictures in a centralized database and as such optimal storage space is also a matter of concern. Future research can be made regarding the storage of the images in an optimal manner in conjunction with minimization of network latency. Further, one of the major design challenge for the proposed system is regarding the accuracy and reliability of the user inputs. A high error tolerance may lead to many false positives while low tolerances may lead to many false negatives. This requires an optimal error tolerance strategy in order to enhance the accuracy of the system.

REFERENCES

[1] Hunt, H. C., & Shea, A. (2018). Enhanced user authentication. U.S. Patent Application No. 10/078,783.

[2] Khari, M., Shrivastava, G., Gupta, S., and Gupta, R. (2017). Role of Cyber Security in Today's Scenario. In R. Kumar, P. Pattnaik, and P. Pandey (Eds.), Detecting and Mitigating Robotic Cyber Security Risks (pp. 177-191). Hershey, PA: IGI Global.

[3] Saxena, A., Shrivastava, G., & Sharma, K. (2012). Forensic investigation in cloud computing environment. The International Journal of forensic computer science, 2, 64-74.

[4] Velsquez, I., Caro, A., & Rodrguez, A. (2018). Authentication schemes and methods. Information and Software Technology, 94(C), 30-37.

[5] Awad, A., & Liu, Y. (2019). Cognitive Biometrics for User Authentication. In Biometric-Based Physical and Cybersecurity Systems (pp. 387-399). Springer, Cham.

[6] Jansen, W., Gavrila, S. I., Korolev, V., Ayers, R. P., & Swanstrom, R. (2003). Picture password: a visual login technique for mobile devices. UMBC Student Collection.

[7] Abhishek, K., Roshan, S., Kumar, P., & Ranjan, R. (2013). A comprehensive study on multifactor authentication schemes. In Advances in Computing and Information Technology (pp. 561-568). Springer, Berlin, Heidelberg.

[8] Franchi, E., Poggi, A., & Tomaiuolo, M. (2015). Information and Password Attacks on Social Networks: An Argument for Cryptography. Journal of Information Technology Research (JITR), 8(1), 25-42.

[9] CNN Business (2013). 5 of the biggest-ever credit card hacks. https://money.cnn.com/gallery/technology/security/2013/12/19/biggest-credit-card-hacks [Accessed on Jan. 31, 2019]

[10] Gilhooly, K. (2005). Biometrics: Getting back to business. Computerworld, May, 9, 2005

[11] Amit, E., Rim, S., Halbeisen, G., Priva, U. C., Stephan, E., & Trope, Y. (2019). Distance-dependent memory for pictures and words. Journal of Memory and Language, 105, 119-130.

[12] Agarwal, G., Singh, S., & Shukla, R. S. (2010). Security analysis of graphical passwords over the alphanumeric passwords. International Journal of Pure and Applied Sciences and Technology, 1(2), 60-66.

[13] Emil Protalinski (2012). The top 10 passwords from the Yahoo hack: Is yours one of them?. https://www.zdnet.com/article/the-top-10-passwords-from-the-yahoo-hack-is-yours-one-of-them [Accessed on Jan. 31, 2019]

[14] Ahitagni (2012). 453,000 Yahoo voice, username and password leaked. http://www.ahitagni.com/?p=422 [Accessed on Jan. 31, 2019]

[15] Sabzevar, A. P., & Stavrou, A. (2008). Universal multi-factor authentication using graphical passwords. In Signal Image Technology and Internet Based Systems, 2008. SITIS'08. IEEE International Conference on (pp. 625-632). IEEE.

[16] De Angeli, A., Coventry, L., Johnson, G., & Renaud, K. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 63(1-2), 128-152.

[17] Renaud, K. V. (2009). Guidelines for designing graphical authentication mechanism interfaces. International Journal of Information and Computer Security, 3(1), 60-85.

[18] Passfaces: Two Factor Authentication for the Enterprise. http://www.passfaces.com/ [Accessed on Jan. 31, 2019]

[19] Hollingworth, A., & Henderson, J. M. (2002). Accurate visual memory for previously attended objects in natural scenes. Journal of Experimental Psychology: Human Perception and Performance, 28(1), 113-136.

[20] Sobrado, L., & Birget, J. (2002). Graphical passwords, The Rutgers Scholar, An electronic bulletin of undergraduate research. Rutgers University, Camden New Jersey, 4,12-18.

[21] Zheng, Z., Liu, X., Yin, L., & Liu, Z. (2010). A Hybrid Password Authentication Scheme Based on Shape and Text. Journal of Computers, 5(5), 765-772.

Edited by: Khaleel Ahmad
Received: Nov 15, 2018
Accepted: Feb 17, 2019