International Journal of Computer Science
and Engineering (IJCSE)
ISSN(P): 2278-9960; ISSN(E): 2278-9979
Vol. 3, Issue 4, July 2014, 175-188
© IASET

International Academy of Science,
Engineering and Technology
IASET Connecting Researchers; Nurturing Innovations

A RGBR PASS POINT GRAPHICAL PASSWORD SCHEMA RESISTANT TO SHOULDER-SURFING

R. SATYA PRASAD[1] & T. SRINIVASA RAVI KIRAN[2]

[1]Associate Professor, Department of Computer Science & Engineering, Acharya Nagarjuna University,
Nagarjuna, Andhra Pradesh, India

[2]Lecturer, Department of Computer Science, P.G Centre, P.B. Siddhartha College of Arts & Science,
Vijayawada, Andhara Pradesh, India

ABSTRACT

Alphanumeric passwords are widely used in computer and network authentication to protect user's privacy. However, it is well known that long, text based passwords are hard for people to remember, while shorter ones are susceptible to attack. Graphical password is a promising solution to this problem. According to human psychology, human can easily remember pictures. Further, a colored graphical password scheme is suggested which is inexpensive compared to biometrics and addresses some of the challenges of text-based passwords.

In this paper, the proposed scheme of authentication resistant to peeping attack starts with identifying triangle formed by clicking on the cells containing colors red, green, blue & red of the interface respectively. An analysis of security and usability aspects of the proposed scheme is presented.

KEYWORDS: Graphical Password, Authentication, Peeping Attack, Security, Attack

INTRODUCTION

Security system plays an important role in the control of people in or out of protected areas, such as physical buildings, information systems, and our national borders. In order to that computer systems and the information associated to them should also be protected. Computer security systems should consider the human factors such as ease of a use and accessibility, in this context, Current secure systems suffer because they mostly ignore the importance of human factors in security. An ideal security system considers all four items such as security, reliability, usability, and human factors.

Traditionally, alphanumeric passwords have been used for authentication, but they are known to have security and usability problems. Today other methods, including graphical passwords, are possible alternatives [1], [2].

Graphical password has a lot of benefits when compared to alphanumeric passwords. It is more safe and easy to remember. Graphical passwords (GP) use pictures instead of textual passwords and are partially motivated by the fact that humans can remember pictures more easily than a string of characters [3]. Human beings have the ability to remember faces of people, places they visit and things they have seen for a longer duration. Thus, graphical passwords provide a means for making more user-friendly passwords while increasing the level of security.

If a password is not frequently used it will be even more susceptible to forgetting. To resist brute force search and dictionary attacks, users are required to use long and random passwords. Unfortunately, such passwords are hard to remember [4]. Besides these advantages, the most common problem with graphical passwords is the shoulder surfing problem: an onlooker can steal user's graphical password by watching in the user's area. Many researchers have attempted to solve this problem by providing different techniques [6].

Graphical passwords serve the same purpose as textual passwords differing in consisting of handwritten designs (drawing), possibly in addition to text. If the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text based schemes and thus presumably offer better resistance to dictionary attacks. Because of these advantages, there is a growing interest in graphical password. In addition, the possible password space of a graphical password scheme may exceed that of text based schemes and thus most probably offer higher level of security. It is also difficult to devise automated attacks for graphical passwords. As a result, graphical password schemes provide a way of making more human-friendly passwords while increasing the level of security. Due to these advantages, there is a growing interest in graphical password. However, existing graphical passwords are far from perfect. Typically, system requirements and cost of communication for graphical passwords are significantly higher than text-based passwords.

RELATED WORK

Textual alpha-numeric passwords were first introduced in the 1960s as a solution to security issues that became evident as the first multi-user operating systems were being developed.

Abdullah et al [10] further note that colored pictures are able to produce or generate many clickable points compared to pictures that are presented in black and white. Color increases the usability of graphical passwords. According to studies conducted by Abdullah et al, a total of 89% of the respondents chose the picture in color mode.

Blonder [5] designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, a user must click on the approximate areas of those locations. The image can assist users to recall their passwords and therefore this method is considered more convenient than textual passwords.

The "Pass Point" system extended Blonder's idea by eliminating the predefined boundaries and allowing arbitrary images to be used [7, 8, 9]. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of the chosen pixels.

A complete review of graphical passwords is available elsewhere [11]. Of interest herein are cued-recall click-based graphical passwords (also known as locimetric [12]). In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues [13] to aid recall. Example systems include Pass Points [14] and Cued Click-Points (CCP) [15].

In Pass Points, a password consists of a sequence of five click-points on a given image. Users may select any pixels in the image as click-points for their password. To log in, they repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points. The usability and security of this scheme was evaluated by the original authors [18, 19] and subsequently by others [1, 16, 17]. It was found that although relatively usable, security concerns remain. The primary security problem is hotspots: different users tend to select similar click-points as part of their passwords. Attackers who gain knowledge of these hotspots through harvesting sample passwords or through automated image processing techniques can build attack dictionaries and more successfully guess PassPoints passwords [17].

T. S. Ravi Kiran and Y. Rama Krihna [22] suggest a hybrid user authentication approach combining CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) and graphical passwords to provide increased security.

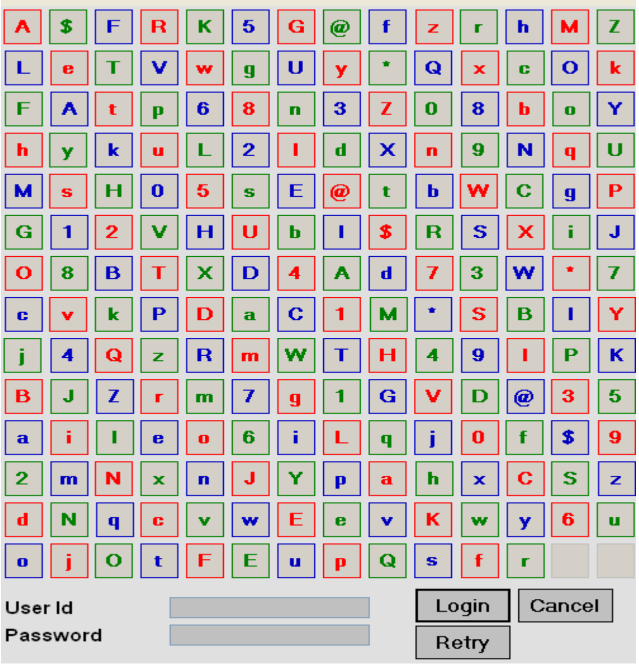
T. Srinivasa Ravi Kiran, Dr. K. V. Samabasiva Rao, M.Kameswara Rao [24] proposed schema starts with identifying quadruplets formed from the user password starting with the first character and sliding to the right one character at a time wrapping around if necessary until the last character in the password appears as the first character in a quadruplet.

T. Srinivasa Ravi Kiran, Dr. K. V. Samabasiva Rao, Dr. M. Kameswara Rao, A. Srisaila [24] proposed scheme we use 5 x 5 grid formed using 25 blocks. Each block consists of a symbol. The symbol contains a set of four characters. The characters may numbers between 0 to 9, A to Z (Uppercase), a to z (Lowercase), Spaces and some special characters totally 95 character and 5 blank spaces are represented as shown in the Figure 1. Passwords are input by typing or by mouse clicks.

Huanyu Zhao and Xiaolin Li proposed S3PAS System. To login, the user must find all his/her original pass characters in the login image and then make some clicks inside the invisible triangles which are called “pass-triangles” created by 3 original pass-characters following a certain click-rule.

PROPOSED SCHEMA

In the proposed scheme, we use a 14 x 14 grid formed using the cell colors red, green & blue respectively. 167 printable character set added with two spaces as shown in Figure 4.



A	$	F	R	K	5	G	@	f	z	r	h	M	Z
L	e	T	V	w	g	U	y	*	Q	x	c	O	k
F	A	t	p	6	8	n	3	Z	0	8	b	o	Y
h	y	k	u	L	2	I	d	X	n	9	N	q	U
M	s	H	0	5	s	E	@	t	b	W	C	g	P
G	1	2	V	H	U	b	I	$	R	S	X	i	J
O	8	B	T	X	D	4	A	d	7	3	W	*	7
c	v	k	P	D	a	C	1	M	*	S	B	I	Y
j	4	Q	z	R	m	W	T	H	4	9	I	P	K
B	J	Z	r	m	7	g	1	G	V	D	@	3	5
a	i	I	e	o	6	i	L	q	j	0	f	$	9
2	m	N	x	n	J	Y	p	a	h	x	C	S	z
d	N	q	c	v	w	E	e	v	K	w	y	6	u
o	j	O	t	F	E	u	p	Q	s	f	r		

User Id

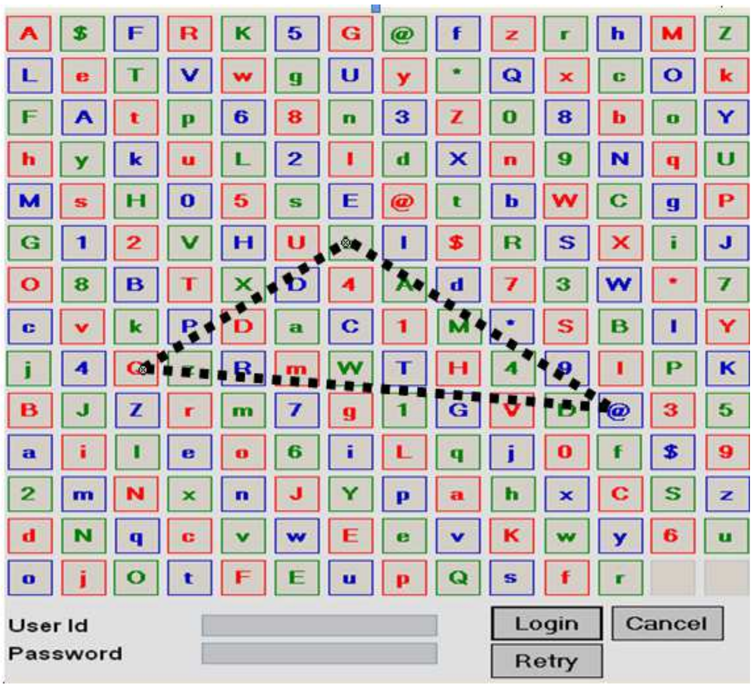
Password

Figure 1: Proposed Schema

The proposed scheme starts with identifying triangle formed by clicking on the cells containing colors red, green, blue & red respectively. If the triangle is not formed that combination can be ignored. The selection of specified triangle takes the user to the next level.

Passwords are input by typing four characters or by mouse clicks. For example, if the password selected at registration time is “Q b @ 3” then the possible triangles formed by clicking on the cells red, green, blue and red respectively are “Qb@Q”,”b@3b” ,“@3Q@”,”3Qb3” . At least one combination considered from the password definitely form the triangle and the first character and last character is same.

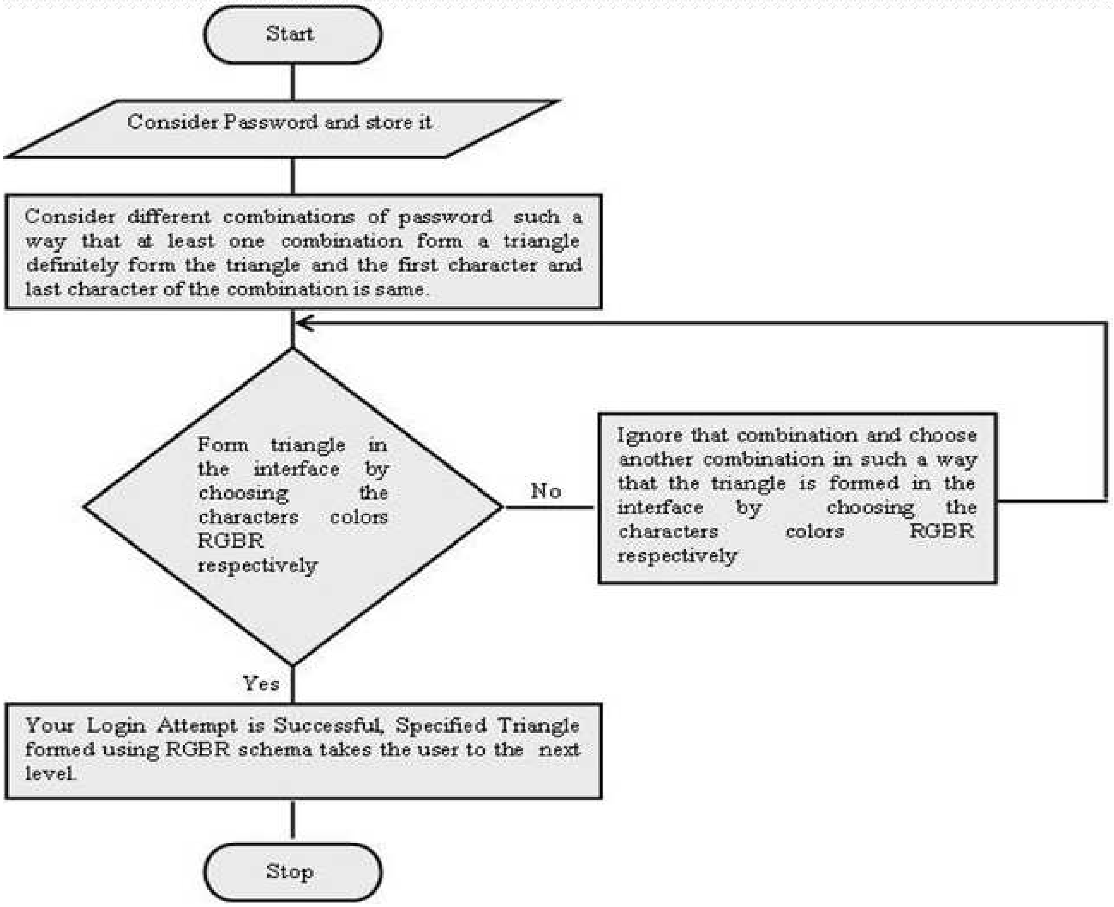
If the combination of characters is such that a triangle cannot be formed, that combination can be ignored. For instance, if the combination selected is such that the first character is not also the last character, a triangle cannot be formed to arrive at the sequence Red, Green, Blue and Red as Red is required both at the beginning and the end. All cells that are even touched by any side of the triangle are also considered valid along with the cells that lie entirely within the region inside the triangle itself.

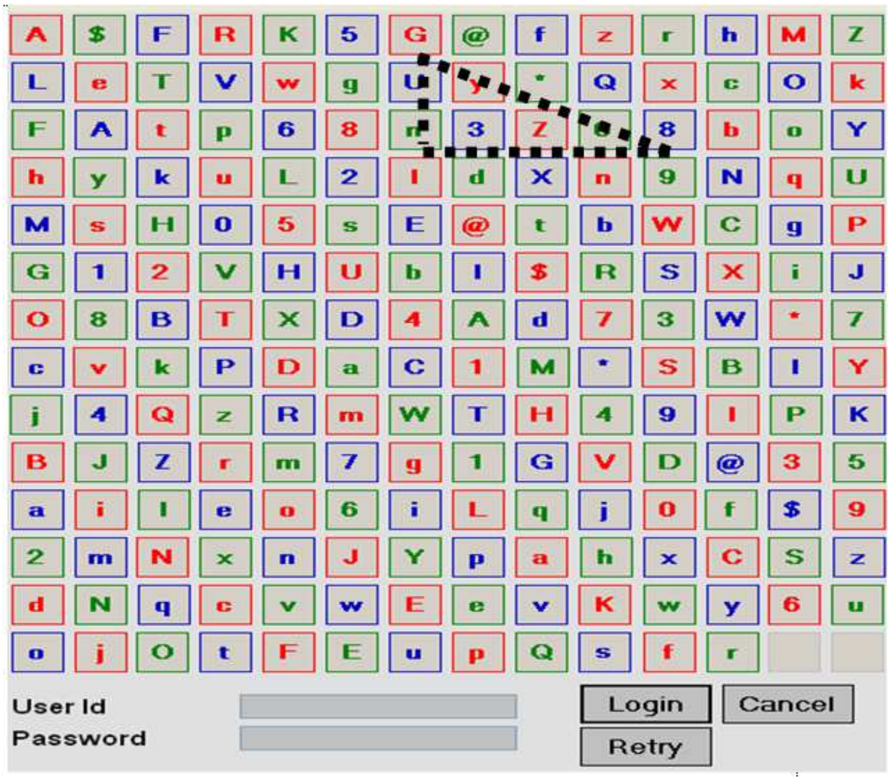


A	$	F	R	K	5	G	@	f	z	r	h	M	Z
L	e	T	V	w	g	U	y	*	Q	x	c	O	k
F	A	t	p	6	8	n	3	Z	0	8	b	o	Y
h	y	k	u	L	2	I	d	X	n	9	N	q	U
M	s	H	0	5	s	E	@	t	b	W	C	g	P
G	1	2	V	H	U	[illegible]	I	$	R	S	X	i	J
O	8	B	T	X	D	4	A	d	7	3	W	*	7
c	v	k	P	D	a	C	1	M	*	S	B	I	Y
j	4	Q	r	R	m	W	T	H	4	9	I	P	K
B	J	Z	r	m	7	g	1	G	V	b	@	3	5
a	i	l	e	o	6	i	L	q	j	0	f	$	9
2	m	N	x	n	J	Y	p	a	h	x	C	S	z
d	N	q	c	v	w	E	e	v	K	w	y	6	u
o	j	O	t	F	E	u	p	Q	s	f	r		

Figure 2: Triangle Formed by Clicking on the Cells “Qb@Q” Containing the Color Red, Green, Blue and Red Respectively for First Login Attempt

The user chooses the combinations in the same order cyclically per each login attempt. For example at first login the user chooses the combination “Qb@Q”, for second login the user chooses the combination ”b@3b”, for third login the user chooses the combination “@3Q@”, for fourth login the user chooses the combination “3Qb3”, again for fifth login the user chooses the combination “Qb@Q” and so on.

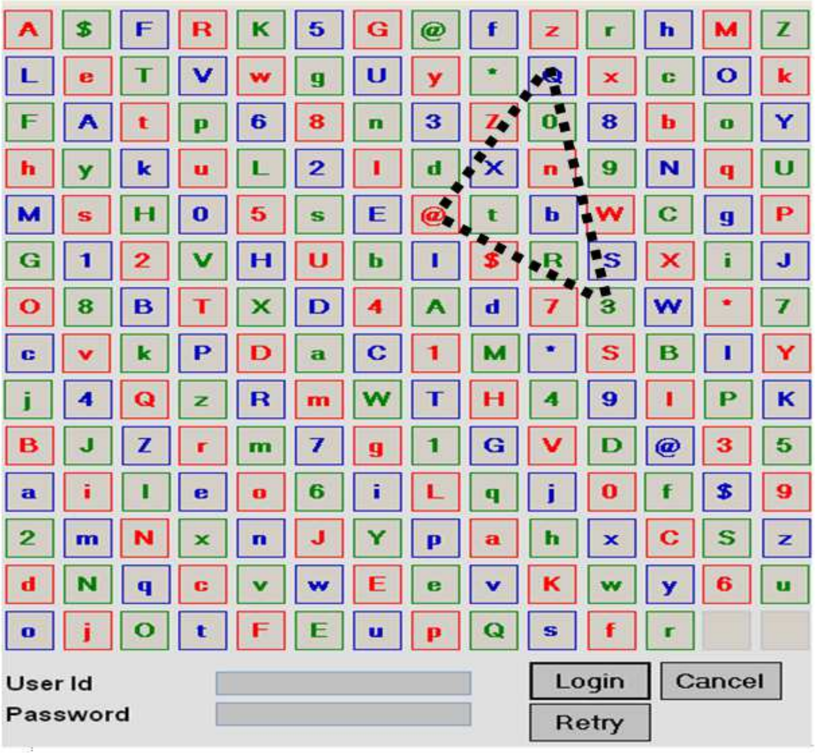

Start
Consider Password and store it
Consider different combinations of password such a way that at least one combination form a triangle definitely form the triangle and the first character and last character of the combination is same.
Form triangle in the interface by choosing the characters colors RGBR respectively
No
Ignore that combination and choose another combination in such a way that the triangle is formed in the interface by choosing the characters colors RGBR respectively
Yes
Your Login Attempt is Successful, Specified Triangle formed using RGBR schema takes the user to the next level.
Stop



A	$	F	R	K	5	G	@	f	z	r	h	M	Z
L	e	T	V	w	g	U	y	*	Q	x	c	O	k
F	A	t	p	6	8	n	3	Z	[illegible]	8	b	o	Y
h	y	k	u	L	2	I	d	X	n	9	N	q	U
M	s	H	0	5	s	E	@	t	b	W	C	g	P
G	1	2	V	H	U	b	I	$	R	S	X	i	J
O	8	B	T	X	D	4	A	d	7	3	W	*	7
c	v	k	P	D	a	C	1	M	*	S	B	I	Y
j	4	Q	z	R	m	W	T	H	4	9	I	P	K
B	J	Z	r	m	7	g	1	G	V	D	@	3	5
a	i	I	e	o	6	i	L	q	j	0	f	$	9
2	m	N	x	n	J	Y	p	a	h	x	C	S	z
d	N	q	c	v	w	E	e	v	K	w	y	6	u
o	j	O	t	F	E	u	p	Q	s	f	r		

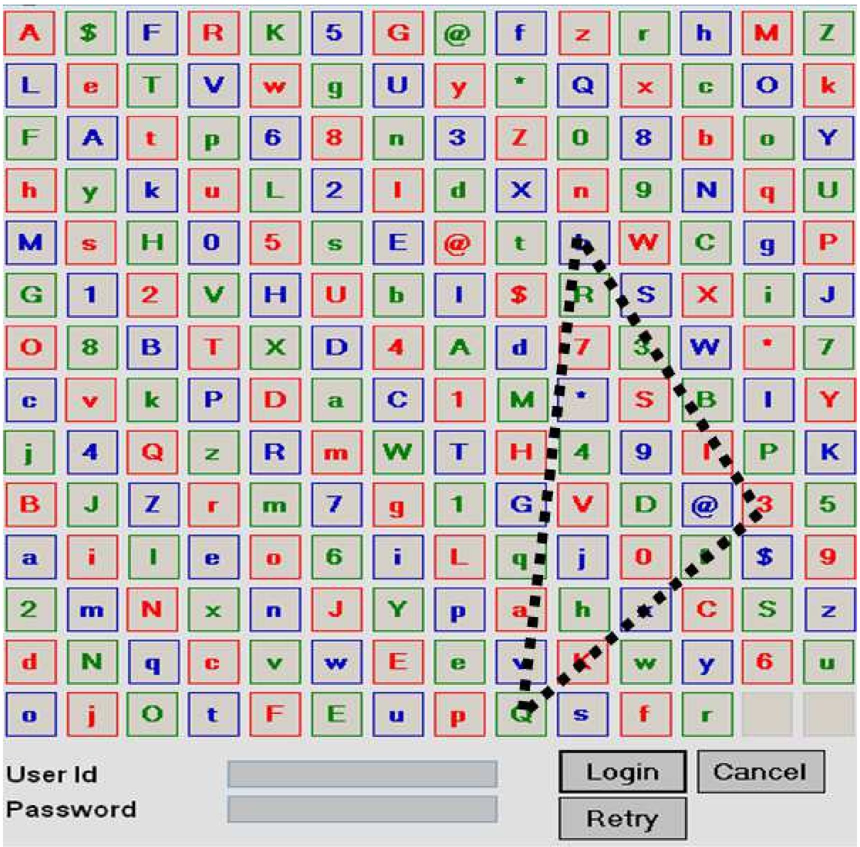
User Id
Password

Figure 3: Triangle Formed by Clicking on the Cells "b@3b" Containing the Color Red, Green, Blue and Red Respectively for Second Login Attempt



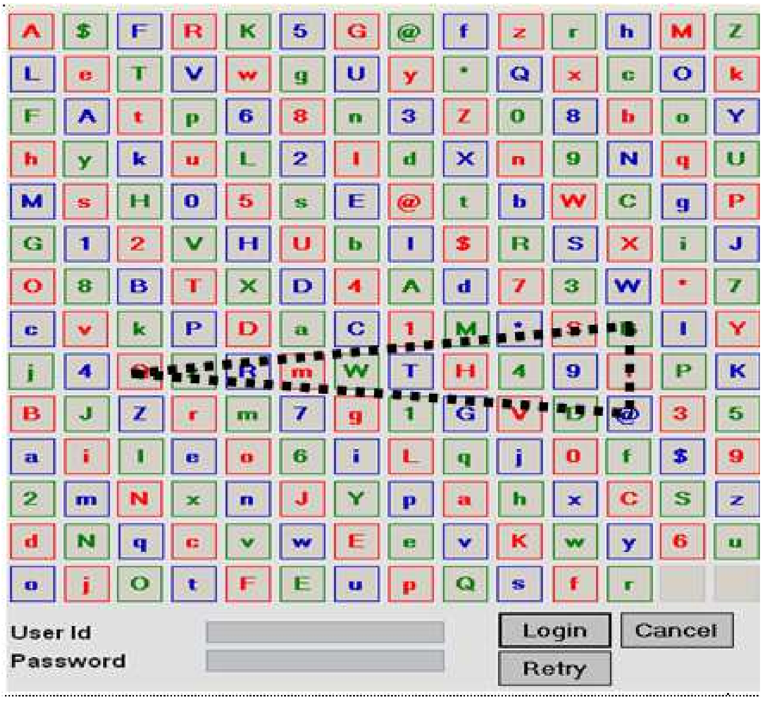
A	$	F	R	K	5	G	@	f	z	r	h	M	Z
L	e	T	V	w	g	U	y	*	Q	x	c	O	k
F	A	t	p	6	8	n	3	Z	0	8	b	o	Y
h	y	k	u	L	2	I	d	X	n	9	N	q	U
M	s	H	0	5	s	E	@	t	b	W	C	g	P
G	1	2	V	H	U	b	I	$	R	S	X	i	J
O	8	B	T	X	D	4	A	d	7	3	W	*	7
c	v	k	P	D	a	C	1	M	*	S	B	I	Y
j	4	Q	z	R	m	W	T	H	4	9	I	P	K
B	J	Z	r	m	7	g	1	G	V	D	@	3	5
a	i	I	e	o	6	i	L	q	j	0	f	$	9
2	m	N	x	n	J	Y	p	a	h	x	C	S	z
d	N	q	c	v	w	E	e	v	K	w	y	6	u
o	j	O	t	F	E	u	p	Q	s	f	r		

Figure 4: Triangle Formed by Clicking on the Cells "@3Q@" Containing the Color Red, Green, Blue and Red Respectively for Third Login Attempt



A	$	F	R	K	5	G	@	f	z	r	h	M	Z
L	e	T	V	w	g	U	y	*	Q	x	c	O	k
F	A	t	p	6	8	n	3	Z	0	8	b	o	Y
h	y	k	u	L	2	I	d	X	n	9	N	q	U
M	s	H	0	5	s	E	@	t	b	W	C	g	P
G	1	2	V	H	U	b	I	$	R	S	X	i	J
O	8	B	T	X	D	4	A	d	7	3	W	*	7
c	v	k	P	D	a	C	1	M	*	S	B	I	Y
j	4	Q	z	R	m	W	T	H	4	9	I	P	K
B	J	Z	r	m	7	g	1	G	V	D	@	3	5
a	i	I	e	o	6	i	L	q	j	0	f	$	9
2	m	N	x	n	J	Y	p	a	h	x	C	S	z
d	N	q	c	v	w	E	e	v	K	w	y	6	u
o	j	O	t	F	E	u	p	Q	s	f	r		

Figure 5: Triangle Formed by Clicking on the Cells "3Qb3" Containing the Color Red, Green, Blue and Red Respectively for Fourth Login Attempt



A	$	F	R	K	5	G	@	f	z	r	h	M	Z
L	e	T	V	w	g	U	y	*	Q	x	c	O	k
F	A	t	p	6	8	n	3	Z	0	8	b	o	Y
h	y	k	u	L	2	I	d	X	n	9	N	q	U
M	s	H	0	5	s	E	@	t	b	W	C	g	P
G	1	2	V	H	U	b	I	$	R	S	X	i	J
O	8	B	T	X	D	4	A	d	7	3	W	*	7
c	v	k	P	D	a	C	1	M	*	S	B	I	Y
j	4	Q	z	R	m	W	T	H	4	9	I	P	K
B	J	Z	r	m	7	g	1	G	V	D	@	3	5
a	i	I	e	o	6	i	L	q	j	0	f	$	9
2	m	N	x	n	J	Y	p	a	h	x	C	S	z
d	N	q	c	v	w	E	e	v	K	w	y	6	u
o	j	O	t	F	E	u	p	Q	s	f	r		

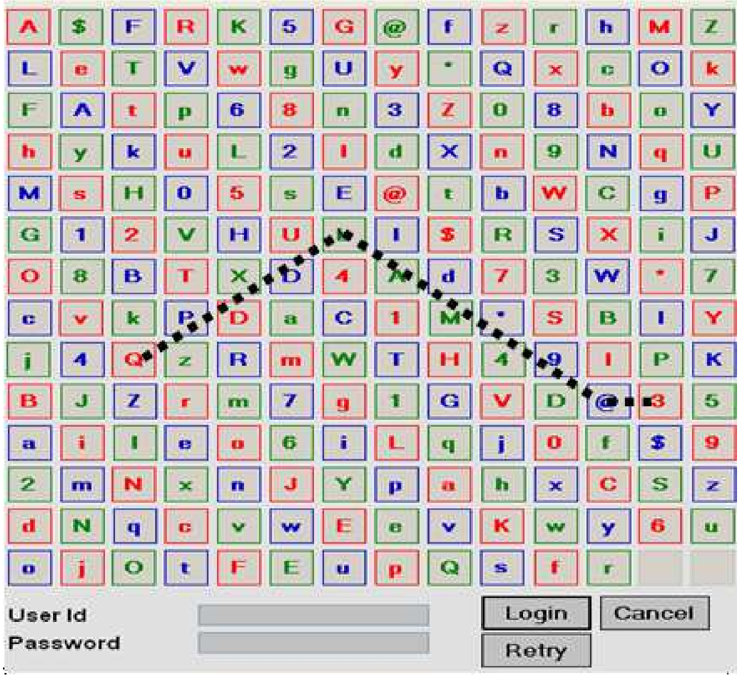
User Id

Password

Figure 6: Triangle Formed by Clicking on the Cells "Qb@Q" Containing the Color Red, Green, Blue and Red Respectively for Fifth Login Attempt

Rule 1: If the first character is not same as the last character then it is not possible to form the triangle in such case the combination can be ignored. Choose another combination of password such a way that the triangle is formed.

E.g. If user clicks on the cells containing the characters "Qb@3" containing the color red, green , blue and red respectively, the first character "Q" is not same as the last character "3" then it is not possible to form the triangle in such case the combination is ignored. Choose another combination of password such a way that the triangle is formed.



A	$	F	R	K	5	G	@	f	z	r	h	M	Z
L	e	T	V	w	g	U	y	*	Q	x	c	O	k
F	A	t	p	6	8	n	3	Z	0	8	b	o	Y
h	y	k	u	L	2	I	d	X	n	9	N	q	U
M	s	H	0	5	s	E	@	t	b	W	C	g	P
G	1	2	V	H	U	b	I	$	R	S	X	i	J
O	8	B	T	X	D	4	A	d	7	3	W	*	7
c	v	k	P	D	a	C	1	M	*	S	B	I	Y
j	4	Q	z	R	m	W	T	H	4	9	I	P	K
B	J	Z	r	m	7	g	1	G	V	D	@	3	5
a	i	I	e	o	6	i	L	q	j	0	f	$	9
2	m	N	x	n	J	Y	p	a	h	x	C	S	z
d	N	q	c	v	w	E	e	v	K	w	y	6	u
o	j	O	t	F	E	u	p	Q	s	f	r		

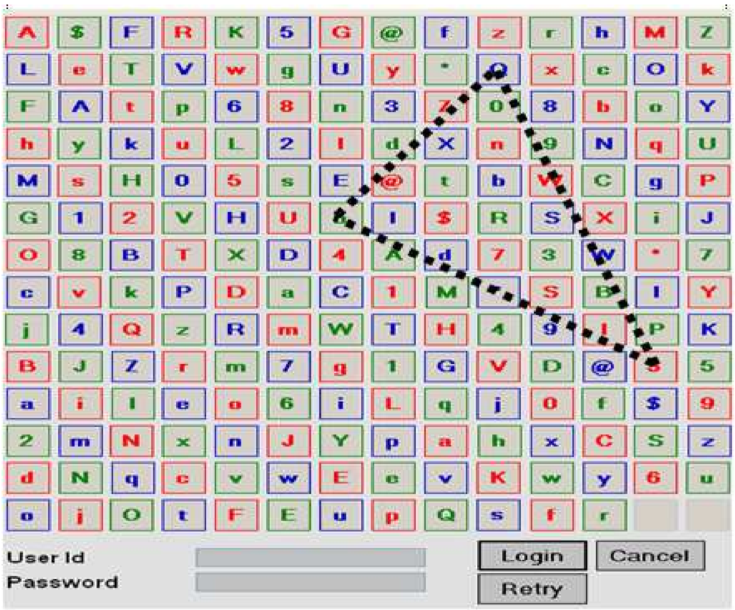
User Id

Password

Figure 7: Shape Formed by Clicking on the Cells "Qb@3" Containing the Color Red, Green, Blue and Red Respectively. Login Failed

Rule 2: If two characters in the password are same and other characters are distinct then form a triangle by clicking on the cells containing the colors red, green, blue and red respectively, then the login attempt is successful.

E.g. If user clicks on the cells containing the characters “3bQ3” containing the color red, green, blue and red respectively, then the login attempt is successful.

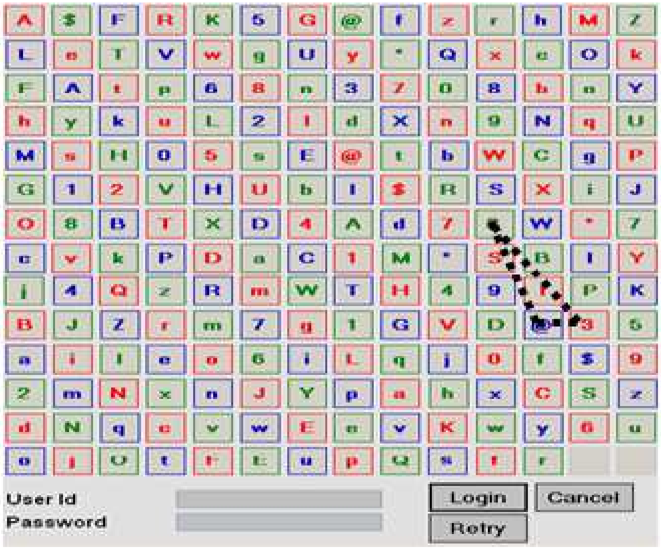


A	$	F	R	K	5	G	@	f	z	r	h	M	Z
L	e	T	V	w	g	U	y	*	Q	x	c	O	k
F	A	t	p	6	8	n	3	Z	0	8	b	o	Y
h	y	k	u	L	2	I	d	X	n	9	N	q	U
M	s	H	0	5	s	E	@	t	b	W	C	g	P
G	1	2	V	H	U	b	I	$	R	S	X	i	J
O	8	B	T	X	D	4	A	d	7	3	W	*	7
c	v	k	P	D	a	C	1	M	[illegible]	S	B	I	Y
j	4	Q	z	R	m	W	T	H	4	9	!	P	K
B	J	Z	r	m	7	g	1	G	V	D	@	3	5
a	i	I	e	o	6	i	L	q	j	0	f	$	9
2	m	N	x	n	J	Y	p	a	h	x	C	S	z
d	N	q	c	v	w	E	e	v	K	w	y	6	u
o	j	O	t	F	E	u	p	Q	s	f	r		

Figure 8: Triangle Formed by Clicking on the Cells “3bQ3” Containing the Color Red, Green, Blue and Red Respectively for First Login Attempt

Rule 3: If three characters in the password are same and other character is distinct then form a triangle by clicking on the cells containing the colors red, green, blue and red respectively, the user would click on any of the cells inside the triangle.

E.g. If user clicks on the cells containing the characters “bb@b” containing the color red, green, blue and red respectively, then the login attempt is successful.

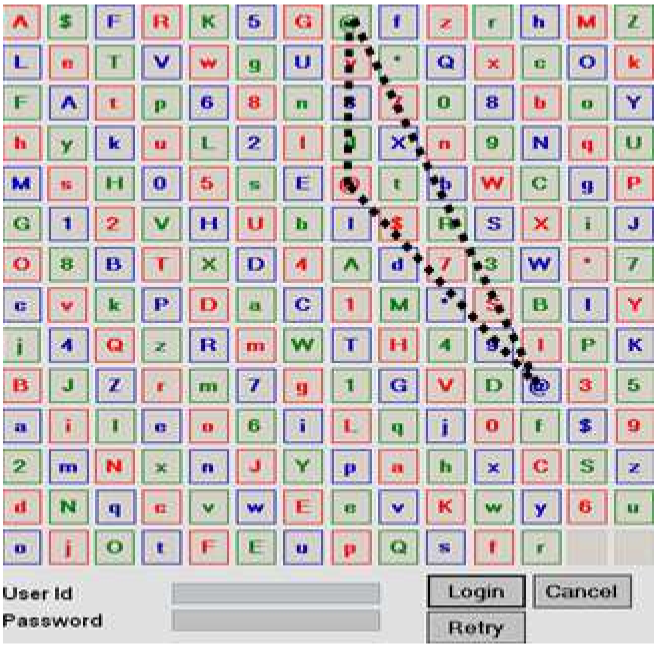


A	$	F	R	K	5	G	@	f	z	r	h	M	Z
L	e	T	V	w	g	U	y	*	Q	x	c	O	k
F	A	t	p	6	8	n	3	Z	0	8	b	o	Y
h	y	k	u	L	2	I	d	X	n	9	N	q	U
M	s	H	0	5	s	E	@	t	b	W	C	g	P
G	1	2	V	H	U	b	I	$	R	S	X	i	J
O	8	B	T	X	D	4	A	d	7	[illegible]	W	*	7
c	v	k	P	D	a	C	1	M	*	S	B	I	Y
j	4	Q	z	R	m	W	T	H	4	9	!	P	K
B	J	Z	r	m	7	g	1	G	V	D	@	3	5
a	i	I	e	o	6	i	L	q	j	0	f	$	9
2	m	N	x	n	J	Y	p	a	h	x	C	S	z
d	N	q	c	v	w	E	e	v	K	w	y	6	u
o	j	O	t	F	E	u	p	Q	s	f	r		

Figure 9: Triangle Formed by Clicking on the Cells “bb@b” Containing the Color Red, Green, Blue and Red Respectively for Login Attempt

Rule 4: If four characters in the password are same then form a triangle by clicking on the cells containing the colors red, green, blue and red respectively, the user would click on any of the cells inside the triangle.

E.g. If user clicks on the cells containing the characters "@@@@" containing the color red, green , blue and red respectively, the user would click on specified cells inside the triangle.



A	$	F	R	K	5	G	@	f	z	r	h	M	Z
L	e	T	V	w	g	U	y	*	Q	x	c	O	k
F	A	t	p	6	8	n	$	z	0	8	b	o	Y
h	y	k	u	L	2	l	J	X	n	9	N	q	U
M	s	H	0	5	s	E	@	t	b	W	C	g	P
G	1	2	V	H	U	b	I	$	R	S	X	i	J
O	8	B	T	X	D	4	A	d	7	3	W	*	7
c	v	k	P	D	a	C	1	M	*	S	B	I	Y
j	4	Q	z	R	m	W	T	H	4	9	I	P	K
B	J	Z	r	m	7	g	1	G	V	D	@	3	5
a	i	I	e	o	6	i	L	q	j	0	f	$	9
2	m	N	x	n	J	Y	p	a	h	x	C	S	z
d	N	q	c	v	w	E	e	v	K	w	y	6	u
o	j	O	t	F	E	u	p	Q	s	f	r		

Figure 10: Triangle Formed by Clicking on the Cells "@@@@" Containing the Color Red, Green, Blue and Red Respectively for Login Attempt

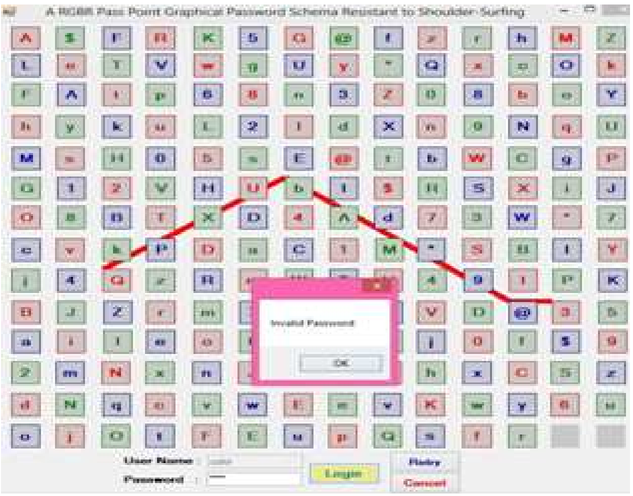
USABILITY STUDY & SECURITY ANALYSIS

We conducted case study in lab with 32 participants out of which 15 were male and 17 were female. All the participants were post graduate students with their ages ranging from 22 to 25 years. A learning phase was conducted for practicing proposed graphical password scheme. They are given training initially explaining the concept of how to identify their password based on the rules proposed through the interface.

The result was encouraging that novice users were able to identify the triangle e formed by clicking on the cells containing the color red, green , blue and red respectively. It took about 35 seconds on average to log in. Peeping attack is the attack where an attacker gets the secret information through direct observation when the user is entering his or her password. Alphanumeric systems are susceptible to peeping attack. In these attacks, typically the attacker gets a chance to observe the password entry for a short duration of time. As alphanumeric passwords are typically small, the attacker may see the secret by looking just for a while. On the other hand, peeping attack is not feasible against our proposed scheme as the user types or clicks on non password characters

CONCLUSIONS & FUTURE WORK

We proposed a scalable shoulder-surfing resistant password authentication system. The outputs of proposed schema demonstrates desirable features of a secure authentication system being immune to shoulder-surfing, hidden-camera, and spy ware attacks.



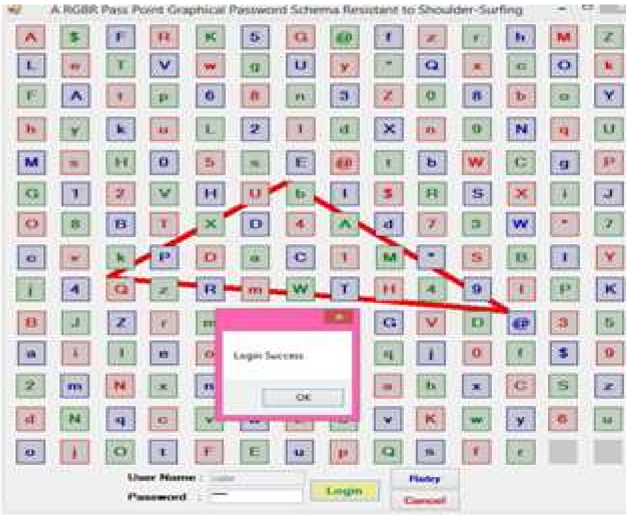
A RGBR Pass Point Graphical Password Schema Resistant to Shoulder-Surfing

Invalid Password

User Name : color

Password : ***

Figure 11: Shape Formed By Clicking on the Cells “Qb@3” Containing the Color Red, Green, Blue and Red Respectively for Login Attempt



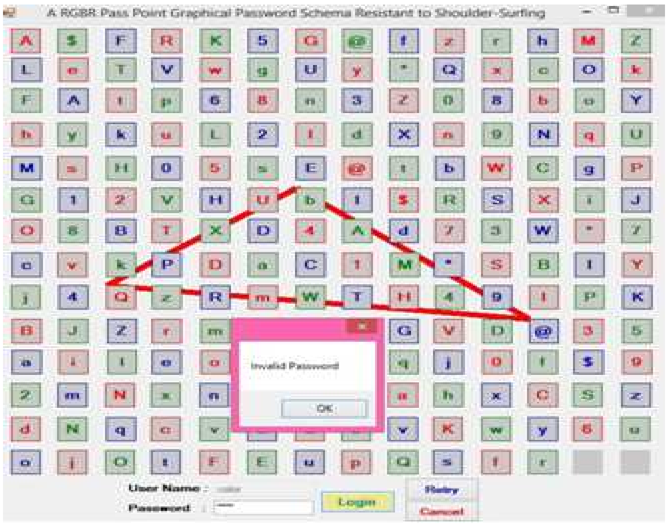
A RGBR Pass Point Graphical Password Schema Resistant to Shoulder-Surfing

Login Success

User Name : color

Password : ***

Figure 12: Triangle Formed by Clicking on the Cells “Qb@Q” Containing the Color Red, Green, Blue and Red Respectively for First Login Attempt



A RGBR Pass Point Graphical Password Schema Resistant to Shoulder-Surfing

Invalid Password

User Name : color

Password : ***

Figure 13: Triangle Formed by Clicking on the Cells “Qb@Q” Containing the Color Red, Green, Blue and Red Respectively for First Login Attempt Repeated Successively. Login Failed

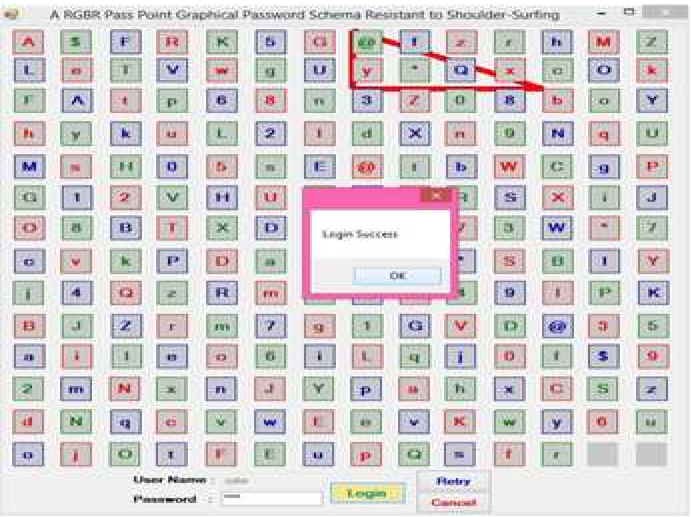

A RGBR Pass Point Graphical Password Schema Resistant to Shoulder-Surfing
Login Success
OK
User Name :
Password :
Login
Retry
Cancel

Figure 14: Triangle Formed by Clicking on the Cells “b@3b” Containing the Color Red, Green, Blue and Red Respectively for Second Login Attempt

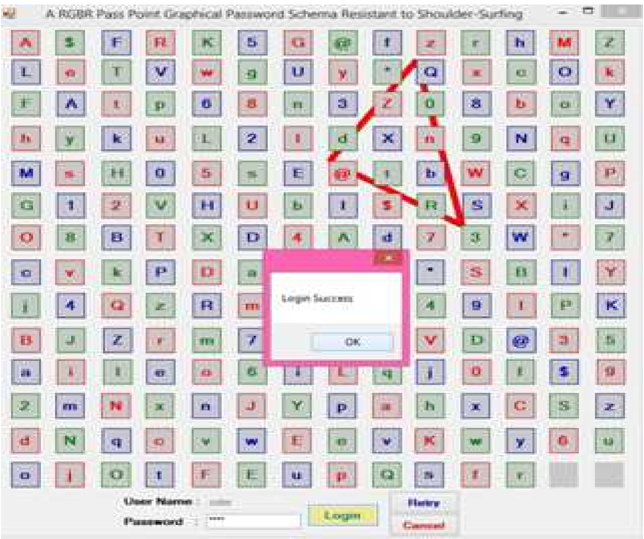

A RGBR Pass Point Graphical Password Schema Resistant to Shoulder-Surfing
Login Success
OK
User Name :
Password :
Login
Retry
Cancel

Figure 15: Triangle Formed by Clicking on the Cells “@3Q@” Containing the Color Red, Green, Blue and Red Respectively for Third Login Attempt

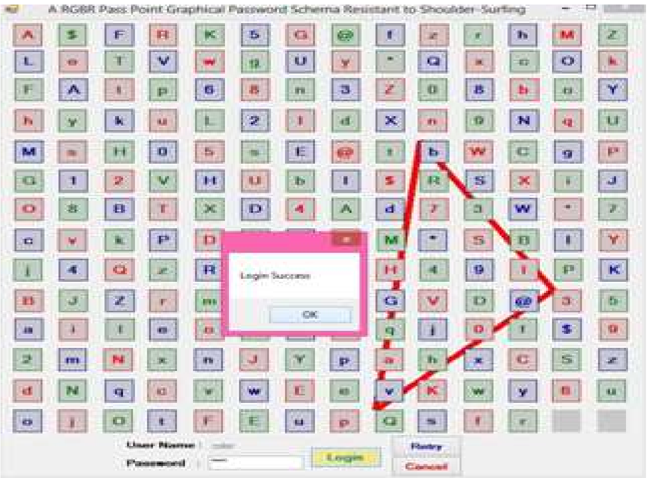
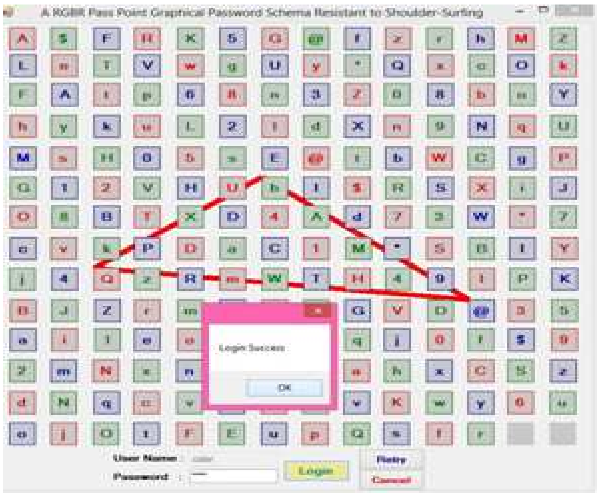

A RGBR Pass Point Graphical Password Schema Resistant to Shoulder-Surfing
Login Success
OK
User Name :
Password :
Login
Retry
Cancel

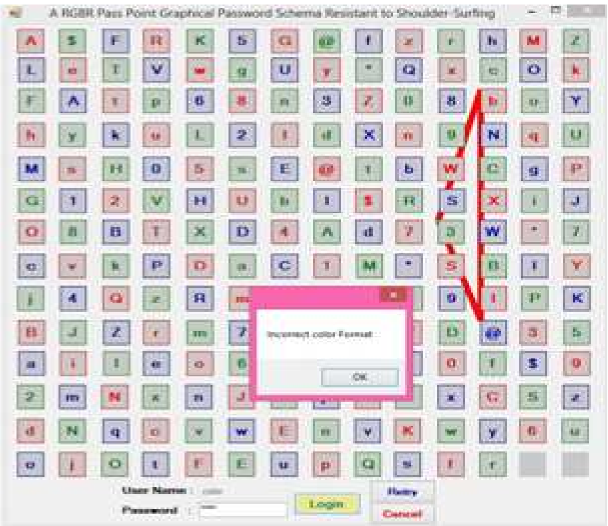
Figure 16: Triangle Formed by Clicking on the Cells “3Qb3” Containing the Color Red, Green, Blue and Red Respectively for Fourth Login Attempt



A RGBR Pass Point Graphical Password Schema Resistant to Shoulder-Surfing

Login Success

Figure 17: Triangle Formed by Clicking on the Cells "Qb@b" Containing the Color Red, Green, Blue and Red Respectively for Login Attempt



A RGBR Pass Point Graphical Password Schema Resistant to Shoulder-Surfing

Incorrect color Format

Figure 18: Triangle Formed by Clicking on the Cells "3@b3" Containing the Green, Blue, Red, and Green Respectively for Login Attempt. Incorrect Color Format

The scheme provides a potential solution for the current problems faced by the other graphical password schemes. The proposed scheme provides larger password space than traditional text based passwords. The extension of the proposed schemes is to identify the hexagon formed by clicking on the cells containing the color red, green , blue, red, green, blue and red respectively on the interface as future work.

REFERENCES

1. Standing, L.P., "Learning 10,000 pictures. Quarterly" Journal of Experimental Psychology vol. 25, pp. 207–222, 1973.
2. Paivio, A., Rogers, T.B., Smythe, P.C., Why are pictures easier to recall then words? Psychonomic Science 11 (4),137–138, 1968.
3. Patric Elftmann, Diploma Thesis, "Secure Alternatives to Password-Based Authentication Mechanisms" Aachen, Germany October 2006].

4. Abdullah et al (2008), Graphical Passwords: Users’ Affinity of Choice, AnAnalysis of Picture Attributes Selection,IEEE 2008.

5. G. E. Blonder. Graphical passwords. United States Patent 5559961, 1996.

6. Xiayuan Suo, YingZhu, G. Scott.Owen, “Graphical Passwords: A Survey”, In Proceedings of Annual Computer Security Applications Conference, 2005.

7. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon. Authentication using graphical passwords: Basic results. In Human-Computer Interaction International (HCII 2005), Las Vegas, NV, 2005.

8. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon. Authentication using graphical passwords: Effects of tolerance and image choice. In Symposium on Usable Privacy and Security (SOUPS), Carnegie Mellon University, Pittsburgh, 2005.

9. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon. Passpoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human Computer Studies, 63, 2005.

10. Abdullah et al (2008), Graphical Passwords: Users’ Affinity of Choice, An Analysis of Picture Attributes Selection, IEEE 2008.

11. R. Biddle, S. Chiasson, and P. van Oorschot, “Graphical Passwords: Learning from the First Twelve Years,” to be published in ACM Computing Surveys, vol. 44, no. 4, 2012.

12. De Angeli, L. Coventry, G. Johnson, and K. Renaud, “Is a Picture Really Worth a Thousand Words? Exploring the Feasibility of GraphicalAuthentication Systems,” Int‟l J. Human-Computer Studies, vol. 63, nos. 1/2, pp. 128-152, 2005.

13. E. Tulving and Z. Pearlstone, “Availability versus Accessibility of Information in Memory for Words,” J. Verbal Learning and Verbal Behavior, vol. 5, pp. 381-391, 1966.

14. S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, “PassPoints: Design and Longitudinal Evaluation of a Graphical Password System,” J. Human-Computer Studies, vol. 63, nos. 1/2, pp. 102-127, 2005.

15. S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, “Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice,” Proc. First Symp. Usable Privacy and Security (SOUPS), July 2005.

16. R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.

17. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.

18. S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwest Instruction and Computing Symposium, 2004.

19. Passlogix. http://www.passlogix.com, site accessed Feb. 2, 2007.

20. G. Blonder. Graphical Passwords. United States Patent 5559961, 1996.

21. L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

22. T.S Ravi Kiran and Y.RamaKrishna, "Combining Captcha And Graphical Passwords For User Authentication ", IJRIM Volume 2, Issue 4, April 2012

23. T.Srinivasa Ravi Kiran, Dr.K.V.Samabasiva Rao, M.Kameswara Rao," A Novel Graphical Password Scheme Resistant To Peeping Attack", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (5) , 2012, 5051-5054

24. T.Srinivasa Ravi Kiran, Dr. K. V. Samabasiva Rao, Dr.M.Kameswara Rao,A.Srisaila,"A Symbol Based Graphical Schema Resistant to Peeping Attack", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 5, No 1, September 2013