Journal of Statistics & Management Systems
ISSN 0972-0510 (Print), ISSN 2169-0014 (Online)
Vol. 27 (2024), No. 2, pp. 295–302
DOI : 10.47974/JSMS-1255

A secured image based three factor user authentication system

Priti Golar *
Rika Sharma †
Department of Computer Science & Engineering
Amity University Raipur
Chhattisgarh
India

Abstract

Graphical User Authentication (GUA) is an image-based password system that leverages the human tendency to remember visuals more effectively. This methodology enables users to effortlessly generate and recall passwords. The three important parameters for any graphical based password system are Usability, Randomness and Security. Usability deals with the system adaptability, memorability, flexibility, User satisfaction etc. On the other side randomness is about Hotspot Coverage, Click Point Clustering, Spatial Patterns, J-statistics etc. This paper is an attempt to initially develop an image-based authentication system that is usable, venerable in terms of randomness. In addition, it is necessary to build a strong security authentication process where the attackers are unable to access the system. The past research study claims the diversity between the usability and security aspect. The focus of this research study is to analyze the impact of various security attacks on the proposed system and the possible solution to avoid them.

Subject Classification: *68P30, 68P25.*

Keywords: *Graphical user authentication, Usability, Randomness, Security attacks.*

1. Introduction

The basic requirement of security in Information is achieved by authentication system. The findings of the past studies in this domain states that the GUA systems are better than any textual based authentication system. GUA supports memorization and higher usability, difficult to crack, easy to remember, random and hard to guess [1]. In addition, it has been noted that the advancement of the GUA system has parallel

* *E-mail:* priticgolar@gmail.com (Corresponding Author)
† *E-mail:* rsharma1@rpr.amity.edu

challenged in increasing the venerable security attacks. Thus, to minimize the intensity of cybercrimes it is necessary to build the strong GUA system which can optimally serve in its usability, more random as well as strongly secured [2].

The walk through of this research study starts with the available literature in the domain of information security and previous GUA system. This section also covers the various types of security attacks and their solutions. The section of initial lab study determines the proposed authentication systems with on the basis of the usability, randomness and security [3]. The next section of analysis of various security attacks provides the information as well as the optimum solution for the security measures applicable to the proposed system. The objective of this study is to make the proposed GUA system a robust one which can handle any complex security attack.

2. Existing Approach towards Usability Aspect

2.1 *Success Rate and Average Duration of Login*

Table 1

Success Rate AAnd Average Duration Of Login Time

PassMap [11]	Origin	Verification
Login-Rate (the first Attempt)	72/95(75.78%)	82/95(86.31%)
Average duration of completion (in seconds)	37.8	20.3
Standard-Deviation (in Sec.)	9.3	8.4
A Password Authentication Scheme that Combines both Text and Image Elements [17]	Login Success Rate (after a week)	Login Success Rate (after a month)
	90.38%(47/52)	75%(39/52)

2.2 Usability -Explorative Statistics for User Satisfaction

- On the basis of Excellent and Very good responses for the first four parameters as shown in Table 1, there is an increase in the system adaptability in terms of password remembrance in due course of time.
- For next four parameters the positive trends in terms of excellent and very good reflect almost 50% of the share.
- The user wants more flexibility for click point selection criterion.
- The system innovative in terms of excellent shares the highest contribution. Figure 1, and Table 2, 3 and 4 shows the overall analysis of the literature.

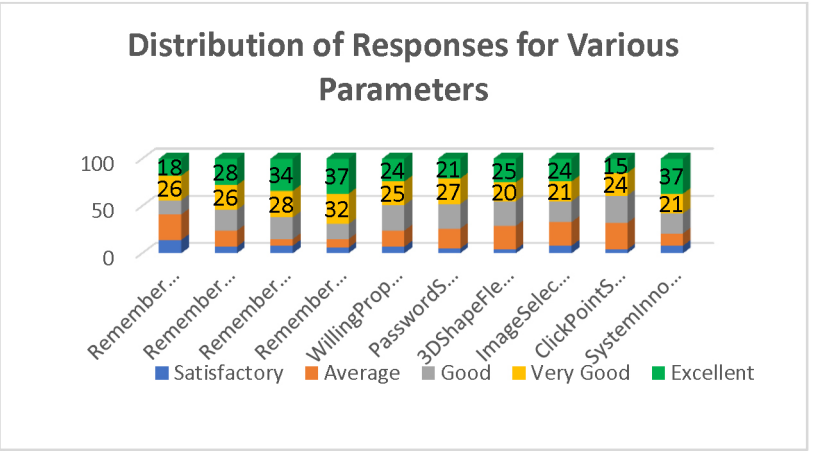

Figure 1

Explorative Statistics

2.3 *Descriptive Statistics for User Satisfaction*

2.3.1 ANOVA One Way

Table 2

Single Factor Scheme of ANOVA

Sets	**Values**	**Cumulative**	**Mean**	**Variance**	
RememberPass1	100	307	3.07	1.823333	
RememberPass2	100	351	3.51	1.585758	
RememberPass3	100	373	3.73	1.512222	
RememberPass4	100	385	3.85	1.421717	
ANOVA					
Selection	*S.S*	*d.f*	*M.S*	*F.*	*F .crit*
Inner Groups	35.4	3	11.8	7.441238	2.627441
Within Groups	627.96	396	1.585758		
Total	663.36	399			

2.3.2 Post Hypothesis Analysis

Table 3

Post Hypothesis Analysis

Parameters	Remember Pass1	Remember Pass2	Remember Pass3	Remember Pass4	Willing Proposed System	Password Secure	3D Shape Flexible	Image Selection	Click Point Selection	System Innovative
Mean	3.07	3.51	3.73	3.85	3.42	3.38	3.37	3.28	3.18	3.66
Standard Error	0.13	0.12	0.12	0.12	0.12	0.12	0.12	0.13	0.11	0.13
Median	3	4	4	4	3	3	3	3	3	4
Mode	2	5	5	5	3	4	3	2	3	5
Standard Deviation	1.35	1.26	1.23	1.19	1.22	1.18	1.22	1.29	1.12	1.31
Sample Variance	1.82	1.59	1.51	1.42	1.50	1.39	1.49	1.68	1.26	1.72

2.3.3 Correlation Analysis

Table 4

Correlation Analysis

Parameter	Willing Proposed System	Password Secure	3D Shape Flexible	Image Selection	Click Point Selection	System Innovative
Willing Proposed System	1					
Password Secure	0.16	1				
3DShapeFlexible	0.23	0.09	1			
Image Selection	0.14	0.245	0.20	1		
Click Point Selection	0.15	0.23	0.06	0.09	1	
System Innovative	0.37	0.26	0.09	0.41	0.09	1

3. Proposed Approach

3.1 *The Entropy Approach*

The most common measure of password quality is entropy, with Shannon entropy being the most popular[7]. The entropy is high for the images having more numbers of hits which indicates that the images having a greater number of clicks generates more randomness. Thereby degree of security is high. This avoids the attacker to guess the clickable points.

On the other hand, the images of low entropy can be guessed easily by attacker.

The entropy of password can be calculated with the expression as:

$$H(x) = N^* \log_2 (|L'| |^*O_1| |^*C_1|) \quad (1)$$

- N represents the length or number of runs or rounds.
- L denotes the collection of photos.
- O denotes the object set for hotspot points.
- C denotes the selection area, divides a picture into a total of 9 regions.

Table 5

Entropy of Existing and Proposed system

Technique Name	Entropy	N	L	O	C
Schemes based on text (With as long as 6 characters) [4]	39.36				
Pass face-like gnometric plans (4 runs, 9 shots)[4]	12.68				
Plans for locimetry that are like Passpoint (4 loci, 30 salient points) [4]	19.69				
3D GUA suggested a plan (4 chosen pictures) [4]	41.29	4	16	16	5
Hexagon Entropy [8]	35.56	2	150	150	10 to 36
Association-based graphical password [9]	35.63	4	30	4	4
Proposed System					
Cube	72.81	6	6	150	5
Cylinder	58.05	5	5	125	5
Hollow Cube	43.86	4	4	100	5
Sphere	30.41	3	3	75	5

3.2 *The Shoulder Surfing Attack*

Table 6

Comparative Analysis of Shoulder-Surfing Attack

Existing System					
Password length.	Two	Three	Four	Five	Six
Avg. No. of Observations. (M)	1.746	2.629	2.906	2.753	2.290
Remark.	Observation needs more than thrice as much				
Proposed System					
Password length.	2	3	4	5	6
Avg. No. of Observations. (M)	2.6432	3.1077	3.458	3.7356771	3.9647
Remark.	Observation needs more than thrice as much				

4. Results

Table 7

Comparative Analysis with attempts and Duration

Duration	No. of users	new	Attempts	1st Attempts	2nd Attempts	Success Attempts	Success Rate	Avg Login Time
Week 1	69	0	54	1	9	44	81.48 %	2:37
Week 2	164	0	124	4	15	105	84.68 %	2:15
Week 3	164	0	292	4	22	266	91.10 %	2:04
Week 4	164	0	456	5	30	421	92.32%	2:02
Fortnight 1	164	0	655	14	37	604	92.21%	2:01
Fortnight 2	164	0	823	19	44	760	92.35%	2:00
One Month	164	0	1178	25	51	1102	93.55%	1:59

In proposed system, we have provided 3 level security, so we are getting enhanced successful registration 91.10% as shown in Table 3. we have compared our work with this author paper [2]. Table 5, 6, 7 and 8 shows the analysis of the proposed system based on various parameters.

Table 8
Successful Authentication

Systems	Successful Authentication
Proposed System- (3-factor authentication system)	91.10%
Existing System- (2-factor authentication system) An Innovative Two-Factor Authentication System That Uses Image Recognition and Pre-Existing Relationships Between Users (2)	70.35%

5. Conclusions

The variations in the existing GUA systems have provide the scope of the proposed system. As in design phase of this proposed system, the security parameter has been also analysed to make it most robust and even more convincing to the end users.The major highlights of this study include password entropy and the crucial shoulder surfing attack. The study provides a better comparative result in terms of high entropy value for the images having maximum numbers of hits, that ultimately helps in reducing the guessability of the attacker. The entropy value of the proposed system when compared to the existing systems reflect the hike by 9% more and hence proves it is more secure. In terms of the Shoulder surfing attack, pre-assumptions related to the comprehensive proposed GUA system are stated for the fair calculations. The end results strengthen the security of the proposed system. It can be observed that with increase in the password length also provide the scopes of increase in the number of observations which stands the more impossible case for the attacker. In case of other graphical attacks, the proposed system also provides a much better scope of the security.

References

[1] Biddle R, Chiasson S, Stobert E, Paul C, Oorschot V, Forget A. "Graphical Passwords: Learning from the First Twelve Years." ACM Computing Survey (2012).

[2] Carrillo D, Arturo J, "A Novel Multi-Factor Authentication Algorithm Based on Image Recognition and User Established Relations." Applied Sciences (2023).

[3] Kumar Sarohi H, Ullah Khan F. "Graphical Password Authentication Schemes: Current Status and Key issues." IJCSI, Vol. 10(2), No. 1, March (2013).

[4] Saeed S, Sarosh Umar M. "A Hybrid Graphical User Authentication Scheme." International conference on Communication, Control and Intelligent Systems. IEEE (2015).

[5] Zhen Yu, HesanmiOlade, Hai-Ning Liang, Charles. Usable Authentication Mechanisms for Mobile Devices: An, Exploration of 3D Graphical Passwords. Xi'an Jiaotong-Liverpool University Suzhou China., IEEE (2016).

[6] Ansari S, Rokade J, Khan I, Shaikh A., Graphical Password Scheme Using Cued Click Point and Persuasion with Multiple Images. *International Journal on Recent and Innovation Trends in Computing and Communication*, Vol. 6(4) : 2321-8169 (2018).

[7] Yazdi, S.H. Analyzing Password Strength & Efficient Password Cracking. Master Thesis, Florida State University, Tallahassee, FL, USA, 2011. Available online: http://diginole.lib.fsu.edu/islandora/object/fsu% 3A181989 (accessed on 22 February 2018).

[8] L. Zhi, S. Qubin, L. Yong. An Association Based Graphical Password Design Resistant to Shoulder Surfing Attack. IEEE (2005).

[9] Chiasson S, Stobert E, Paul C, Oorschot V, Forget A "Persuasive Cued Click- Points: Design, Implementation and Evaluation of a Knowledge-Based Authentication Mechanism." IEEE Transactions on Dependable and Secure Computing, Vol. 9(2) : 1545-5971/12/831.00., 2012.

[10] Meng W, Jiang L., CPMap: Design of Click-Points Map-Based Graphical Password Authentication. HAL, Open science (2018).

[11] Mackie I, Yildirim M., A Novel Hybrid Password Authentication Scheme Based on Text and Image. HAL, Open science (2018).