

1

2 **Graphical User Authentication System Resistant to Shoulder Surfing Attack**

3 **ABSTRACT**

4 User authentication is one of the most significant issues in the field of Information Security. The
5 most common and convenient authentication method used is the alphanumeric password which
6 has significant drawbacks. To overcome the vulnerabilities of traditional methods, graphical
7 password schemes have been developed as possible alternative solutions to text-based scheme. A
8 potential drawback of graphical password schemes is that they are more vulnerable to shoulder
9 surfing than conventional alphanumeric text passwords due to their visual interface. To
10 overcome the shortcoming of existing graphical password schemes this project focuses on
11 developing a graphical authentication system that is resistant to shoulder surfing attack.

12 **Keywords:** Graphical Password; Shoulder Surfing; Password Space; Password Entropy.

13 **1. INTRODUCTION**

14 User authentication is one of the most significant issues in computer and information security
15 (Yesseyeva, 2014). Currently, the most prevalent and well-established authentication approach is
16 based on the use of alphanumeric passwords. The known weakness of traditional user
17 authentication is a tendency to choose passwords with predictable characteristics, which in turn
18 reduces password strength and makes it vulnerable to various attacks (Hu et al., 2010). To
19 address the problems with traditional username-password authentication, alternative
20 authentication methods, such as token and biometrics, have been used. However, token based
21 systems such as smartcards or electronic-key can be lost, impersonated, stolen or misplaced.
22 Biometrics authentication offers conceptual advantages when compared to the traditional use of
23 passwords or PINs. But users tend to resist its usage because of their intrusiveness and the effect
24 on their privacy. Moreover, biometrics process is slow, expensive and cannot be revoked.
25 Graphical authentication has been proposed as a user-friendly alternative to password
26 authentication (Pering et al., 2003; Wiedenbeck et al., 2005). A graphical password is an
27 authentication system that works by having the user select from images, in a specific order,
28 presented in a graphical user interface (GUI). A potential drawback of graphical password
29 schemes is that most of the current graphical password schemes are more vulnerable to shoulder
30 surfing due to their visual interface (Dhamija et al., 2000; Davis et al., 2004; Wiedenbeck et al.,
31 2005).

32

33 **1.1 AIM AND OBJECTIVES**

34 The aim of this research is to design and implement an efficient graphical password resistant to
35 shoulder-surfing attack to improve security in user authentication.

36 The objectives are:

- 37 • To design and implement a new authentication mechanism with balanced security and
38 usability features.
39 • To test the developed system in an environment prone to shoulder surfing attack.
40 • To evaluate the developed authentication system against the existing authentication
41 techniques.

42 **2. LITERATURE REVIEW**

43 Graphical Password as defined by (Yokota et al., 2005) is: “an authentication system that works
44 by selecting or drawing images, by users in a specific order, presented in a graphical user
45 interface (GUI). Graphical Authentication Techniques are categorized into three groups:

- 46 • Pure recall based.
47 • Cued recall based.
48 • Recognition based.

49 **2.1 Pure Recall Based Techniques**

50 In pure recall-based techniques, a user is asked to reproduce something that he or she created or
51 selected earlier during the registration stage without any hint provided by the system. Examples
52 of pure recall based technique are Passdoodle, Draw a secret, grid selection algorithm, qualitative
53 DAS algorithm etc.

54 **2.1.1 Draw a Secret (DAS) Algorithm**

55 In 1999 Jermyn et al. proposed a new graphical password scheme called Draw-a-Secret
56 algorithm. It is a typical implementation in which user draw a design on the grid using mouse or
57 stylus. This method consisted of an interface that had a rectangular grid of size $G * G$, which
58 allowed the user to draw a simple picture on a 2D grid. Goldberg in his 2002 survey concluded
59 that the majority of users could not remember their stroke order. Another weakness is that users
60 tend to select extremely weak graphical passwords which make this authentication scheme
61 predictable and susceptible to various attacks (Lashkari et al., 2009).

62 **2.1.2 Grid Selection Algorithm**

63 In 2004 Thorpe and Oorschot proposed a new graphical authentication scheme that is called
64 Grid selection algorithm to enhance security. A user chooses a smaller grid for drawing within a
65 larger selection grid. Then the user zooms in this piece of grid and creates a drawing like in
66 original Draw-a-Secret (DAS) scheme. This technique of authentication dramatically increases
67 the password space (Muhammad Daniel et al. 2008). Whilst this method significantly increases
68 the DAS password space, it however introduces additional job to memorize and time to input the
69 password. In other words, the security enhancement is achieved by sacrificing password usability
70 and memorability (Suo et al., 2005).

71 **2.2 Cued recall-Based Techniques**

72 In this technique, the system provides a framework of reminders, hints and gestures for the users
73 to reproduce their passwords selected during Registration phase. Examples of cued recall based
74 techniques are Blonder, Passlogix v-Go, PassPoint, pass-Go, Passmap etc.

75 **2.2.1 Blonder Algorithm**

76 Blonder algorithm was proposed by Greg E. Blonder in 1996. During the registration the user is
77 presented with a pre-determined image on a visual display so that the user can point to one or
78 more predetermined positions on the image (tap regions) in a predetermined order as a way of
79 pointing out his or her authorization to access the resource. At authentication phase the user has
80 to click on previously selected locations on the image or close to those locations. The image acts
81 as a hint for the user to recall graphical passwords and therefore this method of authentication is
82 considered more convenient than unassisted pure recall-based schemes (Wiedenbeck et al). The
83 major problem of this scheme is that the number of predefined click regions is relatively small as
84 such the password has to be long for it to be secure.

85 86 **2.2.2 PassPoint Algorithm**

87 PassPoint was created in 2005 in order to improve upon the shortcomings of the Blonder
88 Algorithm. In this method the image could be any natural picture or painting but at the same time
89 must be rich enough so as to have several possible click points. The existence of the image helps
90 the user to remember the click point. The authentication process involves the user selecting
91 several points on picture in a particular order. When logging in, the user clicks close to the
92 selected click points, within some (adjustable) tolerance distance, for instance within 0.25 cm
93 from the actual click point (Susan et al., 2005b). The login time, in this method, is longer than in
94 the alphanumeric method (Susan et al., 2005b). Also the user has more difficulty in learning and
95 memorizing in their password. So, users have to go to several trial sessions for completing the
96 process (Susan et al. 2005a).

97 98 **2.3 Recognition Based Techniques**

99 In recognition-based techniques, users select pictures, icons or symbols from a bank of images.
100 During the authentication process, a user is authenticated by challenging him/her to identify one
101 or more images he or she chooses during the registration stage. Examples of recognition based
102 technique are Passface, Déjà vu, Triangle, story, WIW etc.

103 104 **2.3.1 Story Algorithm**

105 Story Scheme was proposed in 2004, this scheme categorizes the available pictures into nine
106 categories namely animals, cars, women, foods, children, men, objects, natures and sports
107 (Farnaz *et al.*, 2009). Users have to select their passwords from the mixed pictures of nine
108 categories in order to make a story easily to remember (Darren et al. 2004). Research showed
109 that the story scheme was difficult to commit to memory in comparison to pass face
110 authentication (Radhika et al., 2014).

111 112 **2.3.2 Triangle Algorithm**

113 Sobrado and Briget (Davis et al., 2004) introduced an algorithm to overcome the problem of
114 shoulder surfing attack named Triangle. This scheme randomly places a set of N objects (a few
115 hundred or a few thousand) on the screen. Additionally, there is a subset of K pass objects
116 previously chosen and memorized by the user. The system will select the placement of N objects
117 randomly in the log-in phase. The system initially chooses a patch randomly covering half the
118 screen, and then randomly again places the K password objects in that patch. In the log-in phase,
119 the user must be able to find the location of three pass-objects and then click inside the invisible
120 triangle that is possible to create those three objects. But, for each login this process will be
121 repeated using a different group of n objects. The disadvantage of this algorithm is that the log-in

122 phase must use a minimum of 1000 images in order to resist shoulder surfing attack. As a result
123 too many objects are displayed, making it harder for the users to pin point the pass-objects while
124 too few objects makes the password space small and hence become simpler to predict or hack
125 (Xiaoyuan *et al.* 2005).
126

127 3. Methodology and Design

128 3.1 System Description

129 The system uses a combination of Draw a Secret (DAS) and Story algorithms. Users are
130 instructed to mentally construct a story to connect their selected images to aid memorability. It
131 requires users to draw a curve across their password images (pass-images) orderly rather than
132 directly clicking on them. The curve drawn by the user passes through both pass-images and
133 decoy images, which is used to confuse peepers. The drawing begins and ends with given
134 random images to avoid exposing the first and the last pass-images. The drawing trace is cleared
135 off as the user draws the curve which reduces the probability of passwords being exposed. In
136 addition, random curves are displayed as user draws a curve across pass images. The system
137 displays degraded images at the login phase which are difficult to distinguish from a distance or
138 from a side view.

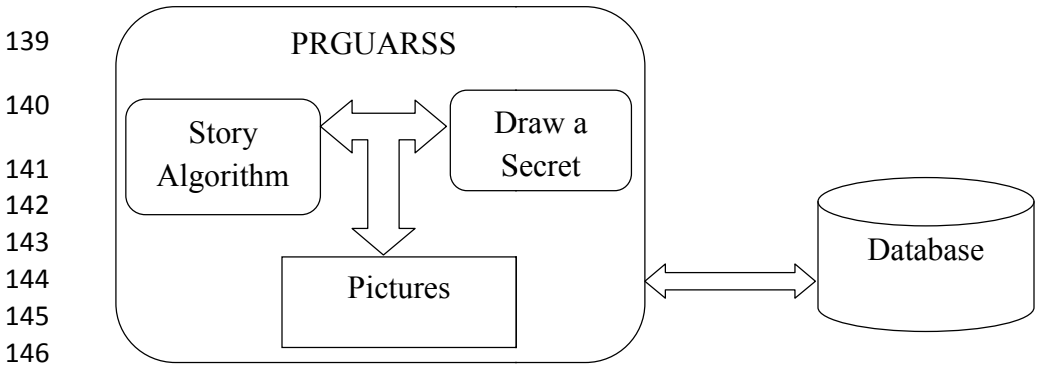
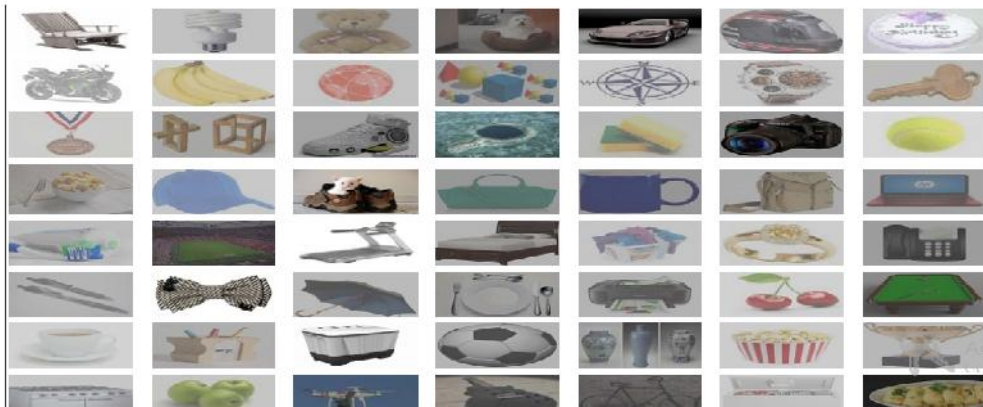


Figure 1: Architectural Design of the System



Figure 2: Screenshot of Pass pictures selection page for Registration

Select Pass-Pictures



150
151 Figure 3: Screenshot of Pass pictures selection for login page.

152 4. Result

153 4.1 Security Test and Evaluation

154 The two methods of evaluating security in GUA algorithms are password space and password
155 entropy. One of the methods “Graphical Password Space” is defined and a comparative table
156 between some previous algorithms and the newly proposed algorithm is generated. The second
157 method “Graphical Password Entropy” is also defined and a comparison between some previous
158 algorithms and newly proposed algorithm represented in a table is generated. The system is also
159 tested against shoulder surfing attack and a comparative table is used to compare the result of the
160 proposed system with previous algorithms.

161 162 4.1.1 Shoulder Surfing Attack Test

163 A user study was conducted to test the effectiveness of the proposed method in reducing
164 shoulder-surfing attack. Thirty participants were involved in carrying out the shoulder surfing
165 attack; 16 of them were male, while 14 of them were female. Shoulder-surfer intent is to steal
166 authentication information by either looking over the victims’ shoulders or recording user
167 authentication process using camera, recruiting a participant group that would represent the true
168 population was practically impossible. However, a participant group with authentication system
169 experience was deemed appropriate to represent “potential shoulder surfers,” as they use
170 password-based logins on a daily basis and are conversant with authentication in general.

171 Half of the participants were assigned to the Attacker group and the remaining half to the Victim
172 group. Participants in Victim group consist of registered users i.e. users that are already familiar
173 with the authentication system. The Attacker group participants were briefly introduced to the
174 scheme. They received a short training session after the introduction on how the authentication
175 system is used. Subsequent to the training session, the Attacker group participants were
176 instructed to act as an attacker using ‘shoulder-surfing’ method to acquire user password. In
177 order to gain access to the system through shoulder-surfing, participants from the Attacker group
178 were given “optimal” shoulder-surfing conditions in which they had the choice to sit next to the
179 person (victim group participant), entering their password or to stand behind them. Attacker
180 group participants had the liberty to record authentication process using camera or move from

181 one side to the other depending on how they felt the most comfortable trying to obtain the
 182 “victim group participants” password.

183
 184 **4.1.1.1 Result**

185 The shoulder-surfing test resulted in none of the participants from the attacker group being able
 186 to discover users password because random pictures are displayed at each of the three login
 187 rounds, it was difficult to know which of the three rounds contains correct order of user
 188 passimages, the random curves displaying as user draws a curve was distracting making it
 189 difficult to track the curve pattern, it was difficult to follow user drawing trace because the trace
 190 cleared off as user draws and only the tail part is left to show the current location of the mouse.
 191 Attacker group participants were given five trial attempts to guess the password used. The results
 192 of the shoulder-surfing test in the user study indicate that the proposed system is resistant to
 193 shoulder-surfing attacks, despite the fact that the attackers know how the proposed system and
 194 the underlying algorithm work. The table below shows the result of the five trial attempts of the
 195 participants.

196
 197 Table 1: Result of Participants’ shoulder surfing attack Trial.
 198

Participants/ Trials	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

199
 200 The strategy used by the participants to obtain the password was inquired. 33.3% of the
 201 participants stated that they applied direct observation method and repeated some of the pictures
 202 selected by the victim, while 13.4% of the participants selected pictures in the exact identified
 203 location victim selected his/her pictures. Other participants (53.3%) selected pictures randomly
 204 in the challenge set because they did not have any hint as to which picture is the pass or decoy
 205 images.

206 Table 2: Comparative Table of existing algorithms and PRGUARSS based on their resistant to
 207 shoulder surfing attack

Name of author or scheme	Resistant to Shoulder Surfing
Blonder (Blonder 1996)	No. Because users’ actions are captured easily by clicking directly on the image.
Draw-A-Secret (DAS) (Jermyn et al. 1999)	No. Because users re-draw their pattern on the same grid.
Syukri, Okamoto and Mambo (Syukri et al.1998)	No. Because attacker can easily capture users’ actions through the use of video capture device.
PassPoint (Birget et al.2003)	No. Because the attacker can use a video capture device to record user’s action and gain user’s password.
Déjà vu (Dhamija et al. 2000)	No. Because user clicks directly on the image which makes

	users' actions easier to capture.
Picture Password (Jansen et al. 2003)	No. Because users' actions can be easily captured since users click directly on the image.
Triangle	No
Movable Frame	No
Story password	No
WIW	No
Proposed System (PRGUARSS)	Yes

208
209
210
211
212
213
214
215
216
217
218

4.1.2 Graphical Password Space

Password space is the number of options in the scheme available to users for choosing a password. It is not possible to define a formula for password space but for all algorithms it is possible to calculate the password space or the number of passwords that can be generated by the algorithm. Some of the previous algorithms and the proposed system password space are calculated and a comparative analysis of the algorithms is made.

4.1.2.1 *Result versus existing algorithms*

219 Table 3: Comparative Table of PRGUARSS and previous algorithms based on graphical space.

Algorithm	Formula
Textual (with 6 characters length include capital and small alphabets)	52^6
Passface (4 rounds, 9 pictures)	9^4
Story (4 rounds, 9 images)	9^4
Picture password (30 images, 4 rounds)	30^4
DAS (represented on 5*5 grid with 6 strokes)	25^6
Triangle (100 picture objects with 3 registered objects)	100^3
Blonder (4 pixels and assuming 30 salient points)	30^4
PassPoint (5 number of pixels with 30 locations to be clicked)	30^5
PRGUARSS (select 5 images from 70 images, and 3 rounds in Log-in phase)	$(70*3)^5$

220
221
222
223

4.1.3 Graphical Password Entropy

Password entropy is usually used to measure the security of a generated password, which conceptually means how hard to blindly guess out the password. In other words, Graphical

224 password entropy tries to measure the probability that the attacker obtains the correct password
 225 based on random guessing. Password entropy of a graphical password can be calculated as:

226 $Entropy = N \log_2 (|L||O||C|)$

227 N is the length or number of runs, L is locus alphabet as the set of all loci, O is an object alphabet
 228 and C is color of the alphabet.

229 **4.1.3.1 Result versus existing algorithms**

230 Table 4: Comparative Table of PRGUARSS and existing algorithms based on Password Entropy

Algorithm	Formula	Entropy (bits)
Textual (with 6 characters length include capital and small alphabets)	$6 * \text{Log}_2 (52)$	34.32
Passface algorithm (4 runs, 9 pictures)	$4 * \text{Log}_2 (9)$	12.68
Picture password (30 images, 4 rounds)	$4 * \text{Log}_2 (30)$	19.63
Story (4 rounds, 9 images)	$4 * \text{Log}_2 (9)$	12.68
DAS (represented on 5*5 grid with 6 strokes)	$6 * \text{Log}_2 (25)$	27.86
Triangle (100 picture objects with 3 registered objects)	$3 * \text{Log}_2 (100)$	19.93
PassPoint (5 number of pixels with 30 locations to be clicked)	$5 * \text{Log}_2 (30)$	24.53
Blonder (4 loci and assuming 30 salient points)	$4 * \text{Log}_2 (30)$	19.63
PRGUARSS (select 5 images from 70 images, and 3 rounds in Log-in phase)	$5 * \text{Log}_2 (70*3)$	40.28

231
 232 The results from the test and evaluation based on usability and security features demonstrated
 233 that the proposed system is more secure when compared with previous algorithms. Finally, the
 234 result of test and evaluation shows that the proposed system not only covers the usability features
 235 but was also more secure in comparison with other algorithms. In other words, the algorithm is
 236 successfully balanced the usability and security features.

237
 238 **5. CONCLUSION**

239
 240 This project presents a web based GUA system combining recognition based (Story) and pure
 241 recall based (Draw a Secret) graphical password to prevent shoulder surfing attack. The main
 242 contribution is that it overcomes a shortcoming of recall-based systems by erasing the drawing
 243 trace and introduces the drawing method to a variant of Story to resist shoulder-surfing attack.
 244 The result of the three categories of evaluation indicates that PRGUARSS performed very well,

245 beyond the shoulder-surfing resistant properties of the system, it also covers the usability and
246 security features. It means the PRGUARSS provides a good balance between usability and
247 security features in GUA algorithms. Therefore, the system can be run as Login part on all secure
248 websites such as Bank, Police, Companies, Universities and Schools.

249

250 **Competing Interests**

251 Authors have declared that no competing interests exist.

252

253 **REFERENCES**

- 254 1. Blonder, G. (1996). "Graphical passwords". US Patent 5 559 961, Sept. 24, 1996.
- 255 2. Davis, D., Monroe, F., and Michael, K.R., (2004), "On user choice in graphical
256 password schemes". Proceedings of the 13th Usenix Security Symposium. Volume 13,
257 pages 11-11. San Diego, CA, 2004.
- 258 3. Dhamija, R., and Perrig, A., (2000). "Déjà Vu: a user study using images for
259 authentication". Proceedings of the 9th Conference on USENIX Security Symposium,
260 Volume 9, pages 4-4.
- 261 4. Farnaz, T., and Maslin, M. (2009). "A Survey on Recognition-Based Graphical User
262 Authentication Algorithms". International Journal of Computer Science and Information
263 Security (IJCSIS), Vol. 6, No. 2, 2009. ISSN: 1947-5500.
- 264 5. Goldberg, J., Hagman, J., and Sazawal, V. (2002). "Doodling our way to better
265 authentication". ACM Conference on Human Factors in Computing Systems (CHI).
- 266 6. Hu, W., Wu, X., and Wei, G. (2010). "The Security Analysis of Graphical Passwords".
267 International Conference on Communications and Intelligence Information Security,
268 pages 200-203, Oct. 13-14. ISBN: 978-1-4244-8649-6
- 269 7. Jermyn, I., Alain, M., Fabian, M., Michael, K. R., and Aviel, D. R. (1999), "The design
270 and analysis of graphical passwords". Proceedings of the 8th USENIX Security
271 Symposium, Volume 8, pages 1-1, August 1999.
- 272 8. Lashkari, A. H., Azizah, A. M., Maslin, M., and Salwani, M. D. (2011). "Security
273 Evaluation for Graphical Password". The International Conference on Digital
274 Information and Communication Technology and its Applications, Volume 166, pages
275 431-444. ISBN: 978-3-642-21984-9.
- 276 9. Lashkari, A. H., Samaneh, F., Rosli, S., and Zakaria, O.B., (2009). 'Shoulder Surfing
277 attack in graphical password authentication'. International Journal of Computer Science
278 and Information Security, (IJCSIS), Volume 6, No. 2, pp. 145-154, ISSN: 1947 5500.
- 279 10. Muhammad, D.H., Abdul, H. A., Norafida, I., and Hazinah, K. M. (2008). "Towards
280 Identifying Usability and Security Features of Graphical Password in Knowledge Based
281 Authentication Technique". Proceedings of the 2nd Asian International Conference on
282 Modeling and Simulation, pages 396-403.
- 283 11. Pering, T., Murali, S., John, L., and Roy, W. (2003). "Photographic authentication
284 through untrusted terminals". Pervasive Computing, IEEE and IEE Communications
285 Society, Volume 2, pages 30-36.
- 286 12. Radhika and Siddhartha, S. B. (2014). "Comparative Study of Graphical User
287 Authentication Approaches". International Journal of Computer Science and Mobile
288 Computing (IJCSMC), Vol. 3, Issue. 9, pages 361 – 375, ISSN 2320–088X.

- 289 13. Suo, X., Zhu, Y. and Owen, G. S. (2005). "Graphical Passwords: A Survey". Proceedings
290 of the 21st Annual Computer Security Applications Conference (December, 5-9), pages
291 463-472. ISSN: 1063-9527.
- 292 14. Susan, W., Birget, J.C., and Brodskiy, A., (2005). "Authentication Using Graphical
293 Passwords: Effects of Tolerance and Image Choice". Symposium on Usable Privacy and
294 Security (SOUPS), July 6-8, Pittsburgh, PA, USA.
- 295 15. Susan, W., Jim, W., Birget, J. C., Alex, B., and Nasir, M. (2005). "Authentication Using
296 Graphical Passwords: Basic Results". In Human-Computer Interaction International
297 Conference, Las Vegas, November.
- 298 16. Thorpe, J., and Oorschot, P.C.V., (2004). "Towards Secure Design Choices for
299 Implementing Graphical Passwords". Proceedings of the 20th Annual Computer Security
300 Applications Conference, ISSN: 1063-9527, pages 50-60, doi: 10.1109/CSAC.2004.44,
301 <http://dx.doi.org/10.1109/CSAC.2004.44>.
- 302 17. Xiaoyuan, S., Z. Ying, et al. (2005). "Graphical passwords: a survey", Computer Security
303 Applications Conference, 21st Annual.
- 304 18. Yesseyeva, E. K., Abdulrazaq, M. M., Lashkari, A. H., and Sadeghi, M. (2014), "Tri-
305 Pass: a new graphical user authentication scheme", International Journal of Circuits,
306 Systems and Signal Processing, Vol 8, P:61 – 67.
- 307 19. Yokota, K. & Yonekura, T., 2005, 'A proposal of COMPASS (community portrait authentication
308 system), International Conference on Cyber worlds.
- 309

310

311

312

313

314