Appendix A

List of Publications and Patents Filed

Journal

1. Por, L. Y. (2011) Frequency of Occurrence Analysis attack and its countermeasure, *The International Arab Journal of Information Technology*, *10*(1). [ISSN: 1683-3198, Indexed by Thomson ISI]. (Accepted for publication)

2. Por, L. Y. & Mat Kiah, M. L. (2010) Shoulder-surfing resistance using penup event and neighbouring connectivity manipulation, *Malaysia Journal of Computer Science*, *23*(2), 121-140. [ISSN 0127-9084, Indexed by Thomson ISI, INSPEC (IEE), Scopus.]

3. Por, L. Y. & Lim, X. T. (2008) Multi-Grid Background Pass-Go, *Journal of WSEAS Transactions on Information Science and Applications*, *5*(7), 1137-1148. [ISSN 1790-0832, Indexed by INSPEC (IEE), Scopus, ACM]

4. Por, L. Y., Lim, X. T., Su, M. T., & Kianoush, F. (2008) The design and implementation of background pass-go scheme towards security threats, *Journal of WSEAS Transactions on Information Science and Applications*, *5*(6), 943-952. [ISSN 1790-0832, Indexed by INSPEC (IEE), Scopus, ACM]

Conference

1. Por, L. Y., Lim, X. T., & Kianoush, F. (2008) *Background Pass-Go (BPG), a New Approach for GPS*. Paper presented at the 12th WSEAS International Conference on COMPUTERS (part of the 12th WSEAS CSCC Multiconference), Heraklion, Crete Island, Greece, pp. 369-374. [ISSN 0127-9084, Indexed by Thomson ISI]

2. Por, L. Y., & Lim, X. T. (2008) *Issues, Threats and Future Trend for GSP*. Paper presented at the 7th WSEAS International Conference on Applied Computer & Applied Computational Science (ACACOS '08), Hangzhou, China, pp. 627-633. [ISSN1790-5117, Indexed by Thomson ISI]

Intellectual Property Rights

A national patent on the proposed partial password selection and metaheuristic randomisation algorithm was filed. (Application No.: PI2010003271, Title: A method of image-based password authentication.)

Appendix B

A SURVEY ON COLOUR USAGE

The purpose of this survey is to identify the user preferred colour. This survey is meant for research purposes only. All data collected and analysis made will be treated with the strictest confidence. As soon as the data have been recorded and double-checked, the questionnaires will be shredded.

Please do not identify yourself in any way.

For each of the following question, please tick the checkbox that best applies to you.

1. **What is your group age?**

   ☐ Age < 18 ☐ 18 ≤ Age < 25 ☐ 25 ≤ Age < 35

   ☐ 35 ≤ Age < 45 ☐ 45 ≤ Age < 55 ☐ Age ≤ 55

2. **Gender?**

   ☐ Male ☐ Female

3. **Do you use Microsoft Office Word?**

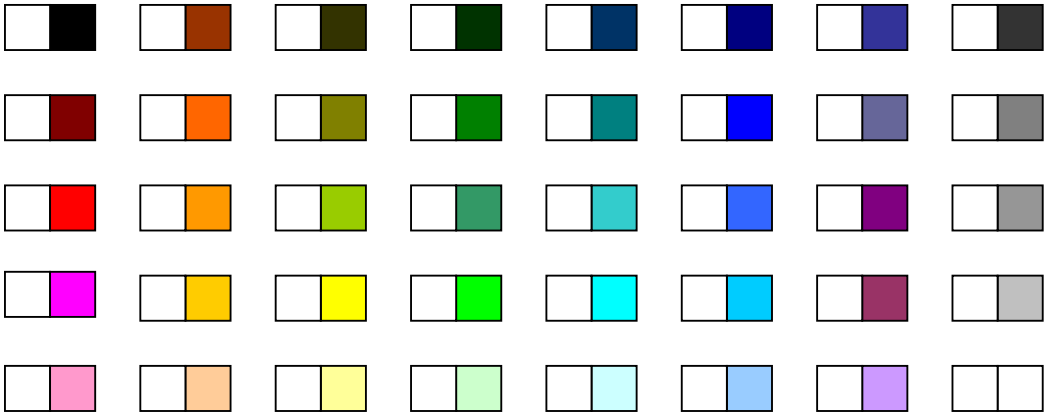
   ☐ Yes ☐ No

4. **Are you familiar with the Colour Scheme used in Figure 1?**

   ☐ Yes ☐ No

Figure 1: Colour Scheme from Microsoft Office Word 2003

5. What colour do you like (choose 10 colours only)?



Thank you for taking the time to participate in our survey.

Appendix C

A SURVEY ON USABILITY (PART I)

The purpose of this survey is to:

i. Determine the effectiveness of the proposed upload background picture feature in aiding users' memorability.
ii. Determine the effectiveness of the proposed grid line scaling feature in aiding users' memorability.
iii. Determine the effectiveness of the proposed loose authentication feature in aiding users' memorability.

This survey is meant for research purposes only. All data collected and analysis made from the data will be treated with the strictest confidence. As soon as the data have been recorded and double checked, the questionnaires will be shredded.

Please do not identify yourself in any way.

For each of the following question, please tick the checkbox that best applies to you.

1. **Current academic degree that you are pursuing?**

   ☐ Undergraduate ☐ Postgraduate

2. **Gender?**

   Male ☐ Female ☐

3. **Do you know what picture-based password authentication is?**

   ☐ Yes ☐ No

4. **Do you agree that superimposing a background picture onto the BPG system is can users in memorising their password?**

☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree

Please state your reason(s) if your answer is not 'Strongly Agree'.

5. **Do you agree that the "Grid Line Scaling" function used in the enhanced BPG system is able to aid users in memorising their password?**

☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree

Please state your reason(s) if your answer is not 'Strongly Agree'.

6. **Do you agree that the loose authentication function used in the enhanced BPG system is able to aid users in memorising their password?**

☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree

Please state your reason(s) if your answer is not 'Strongly Agree'.

7. **Do you know what shoulder-surfing attack is?**

☐ Yes ☐ No

Thank you for taking the time to participate in our survey.

Appendix C

A SURVEY ON USABILITY (PART II)

The purpose of this survey is to:

i. Evaluate the effectiveness of the proposed chronological story-based cued recall technique in aiding users' memorability.

This survey is conducted as part of a research on picture-based password authentication methods. All data collected and results obtained from the analysis of the data will be treated with the strictest confidentiality. This questionnaires form will be shredded at the conclusion of the research.

Please do not identify yourself in any way.

For each of the following question, please tick the checkbox that best fits your answer.

1. **Academic programme level?**

   ☐ Undergraduate ☐ Postgraduate

2. **Gender?**

   ☐ Male ☐ Female

3. **Do you know what graphical authentication is?**

   ☐ Yes ☐ No

4. **Do you have any difficulty in memorising the password that you have chosen prior to using the Chronological Story-Based Cued Recall Technique in the VIP Pro System?**

   ☐ Yes ☐ No

Chronological Story-Based Cued Recall Technique: A technique that can help you in memorising your password by creating a story with your selected pictures.

5. **Do you agree that the Chronological Story-Based Cued Recall Technique used in the VIP Pro system can help users in memorising their password?**

☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree

Please state your reason(s) if your answer is NOT 'Agree' or 'Strongly Agree'.

Thank you for taking the time to participate in our survey.

Appendix D

Table A1: Analysis and Observation Result for $R_1^{J_{4,4}}$

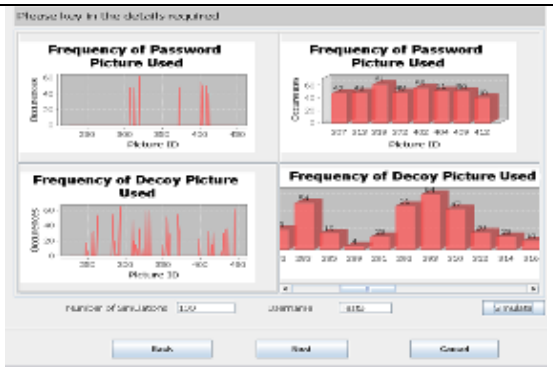
Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table A2: Analysis and Observation Result for $R_2^{j_{4.4}}$

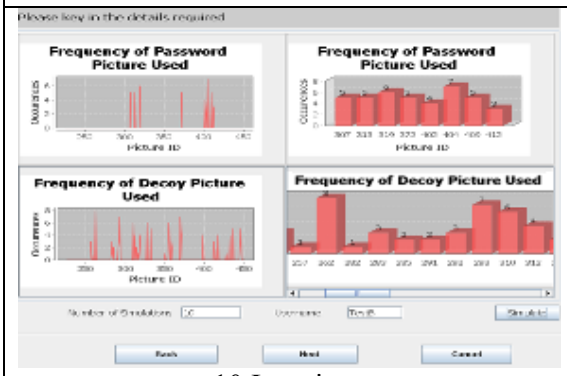
Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table A3: Analysis and Observation Result for $R_3^{j_{4.4}}$

Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table A4: Analysis and Observation Result for $R_4^{j_{4.4}}$

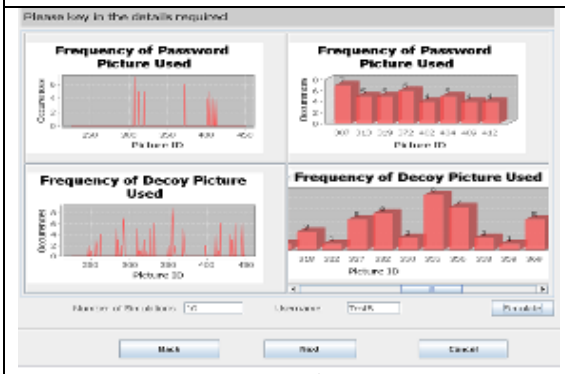
Simulation Result	
 10 Iterations	 100 Iterations
 10000 Iterations	 100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table A5: Analysis and Observation Result for $R_5^{j_{4.4}}$

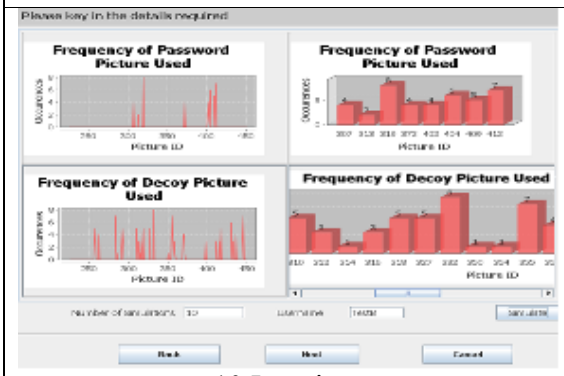
Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table A6: Analysis and Observation Result for $R_6^{j_{4.4}}$

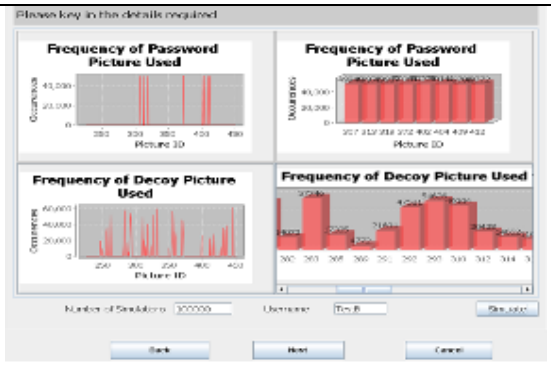
Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table A7: Analysis and Observation Result for $R_7^{j_{4.4}}$

Simulation Result	
 10 Iterations	 100 Iterations
 10000 Iterations	 100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table A8: Analysis and Observation Result for $R_8^{j_{4.4}}$

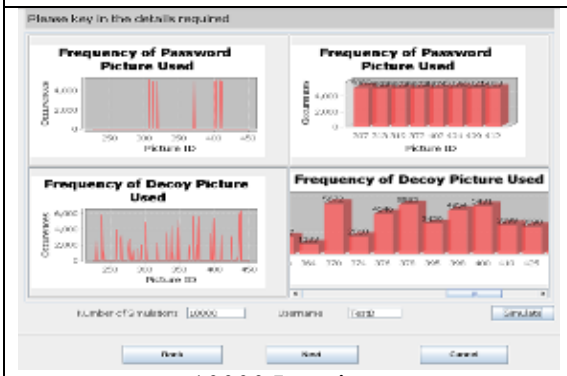
Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table A9: Analysis and Observation Result for $R_9^{j_{4.4}}$

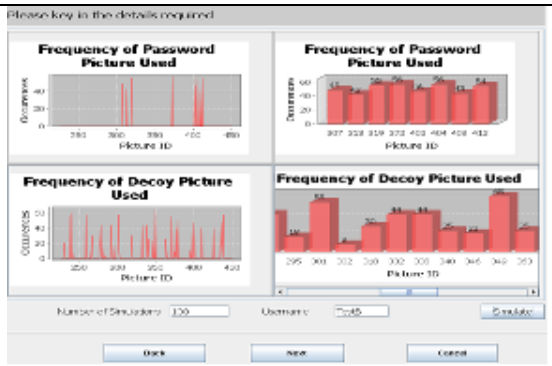
Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table A10: Analysis and Observation Result for $R_{10}^{j_{4.4}}$

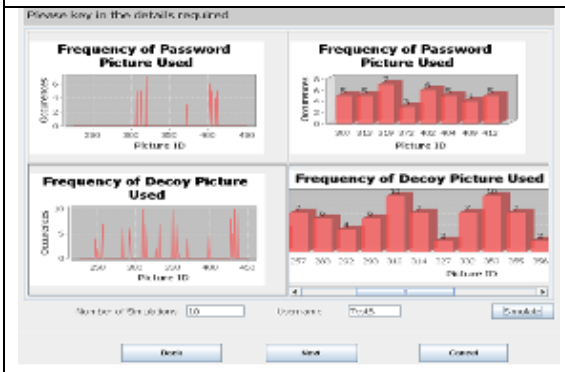
Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table A11: Analysis and Observation Result for $R_{11}^{j_{4.4}}$

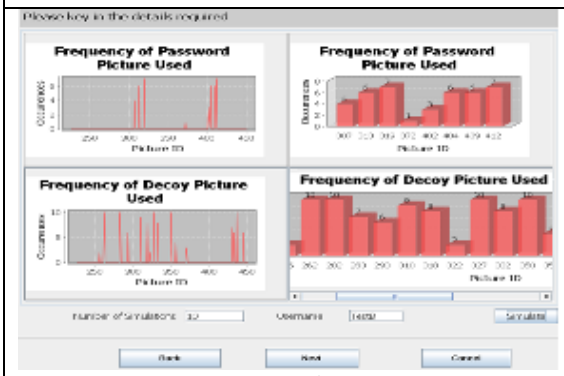
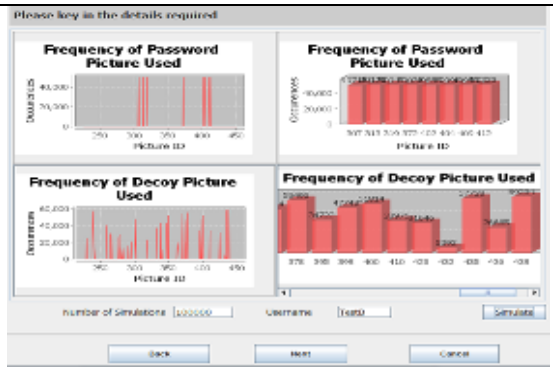
Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table B1: Analysis and Observation Result for $R_1^{j_{4.5}}$

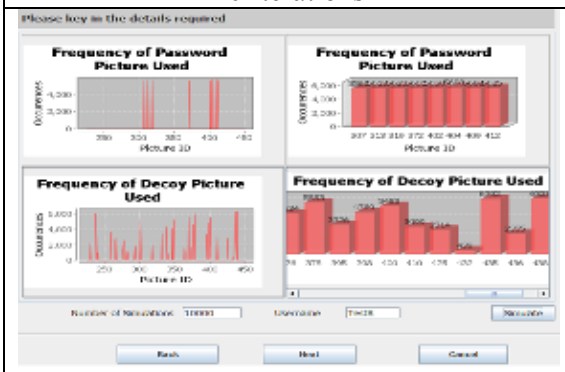
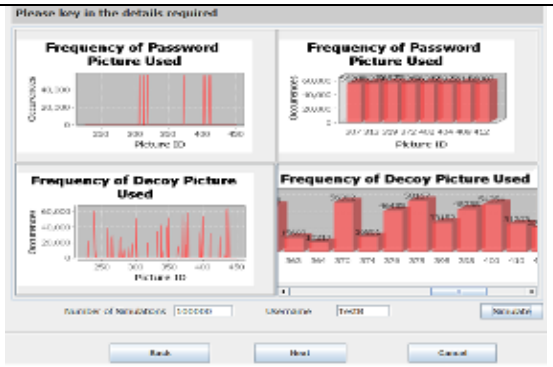
Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table B2: Analysis and Observation Result for $R_2^{j_{4.5}}$

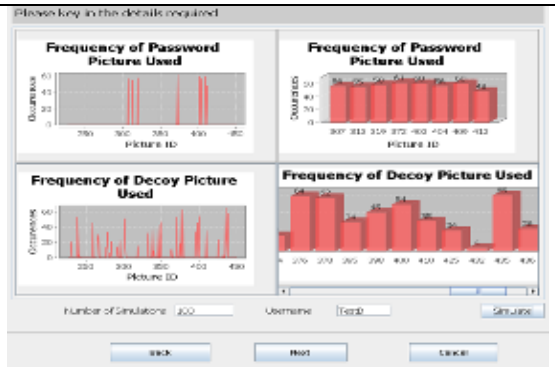
Simulation Result	
 10 Iterations	 100 Iterations
 10000 Iterations	 100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table B3: Analysis and Observation Result for $R_3^{j_{4,5}}$

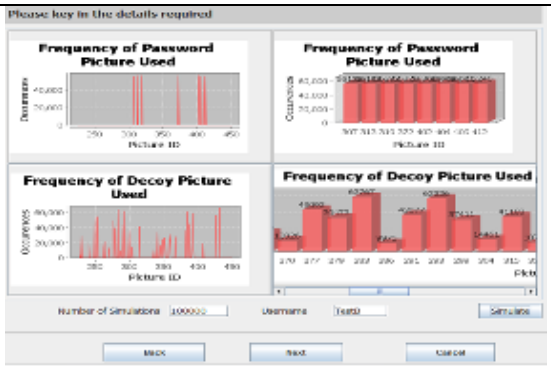
Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table B4: Analysis and Observation Result for $R_4^{j_{4,5}}$

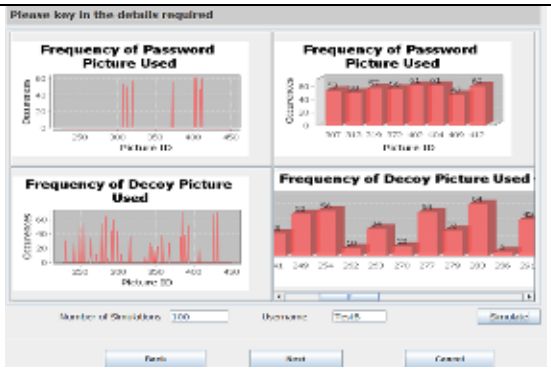
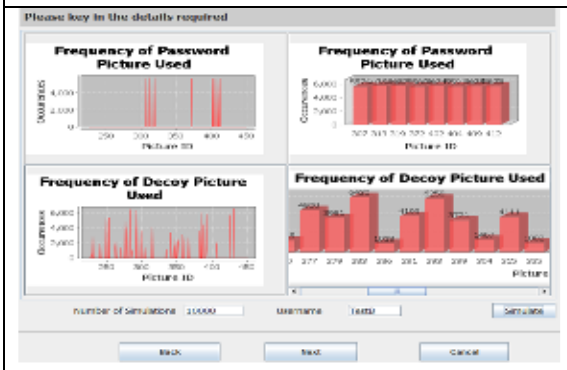
Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table B5: Analysis and Observation Result for $\overset{j_{4.5}}{R_5}$

Simulation Result	
 10 Iterations	 100 Iterations
 10000 Iterations	 100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table B6: Analysis and Observation Result for $\overset{j_{4.5}}{R_6}$

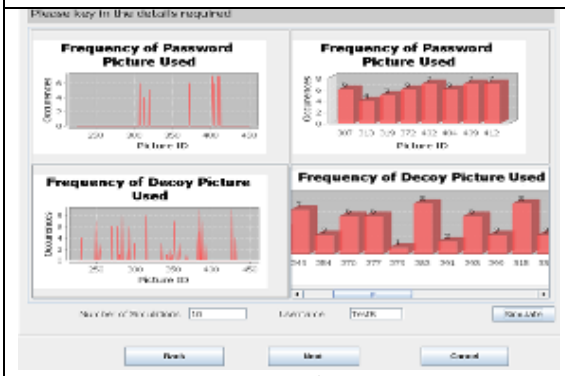
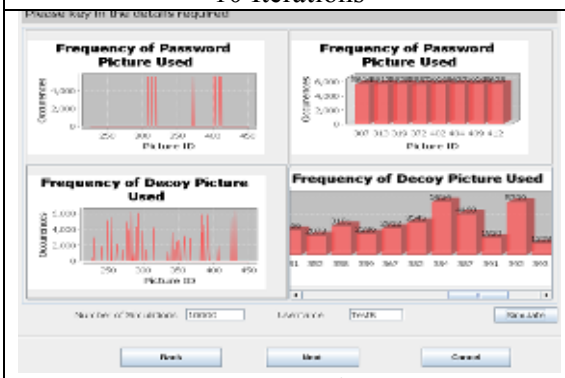
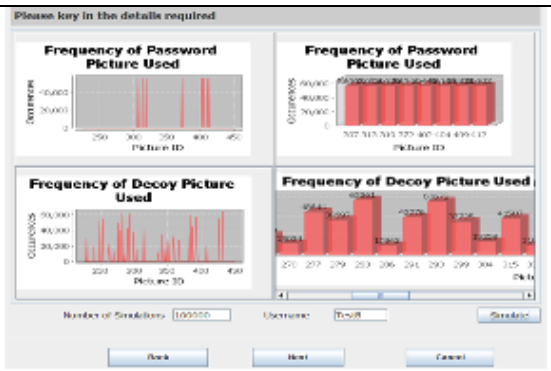
Simulation Result	
 10 Iterations	 100 Iterations
 10000 Iterations	 100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table B7: Analysis and Observation Result for $R_7^{j_{4,5}}$

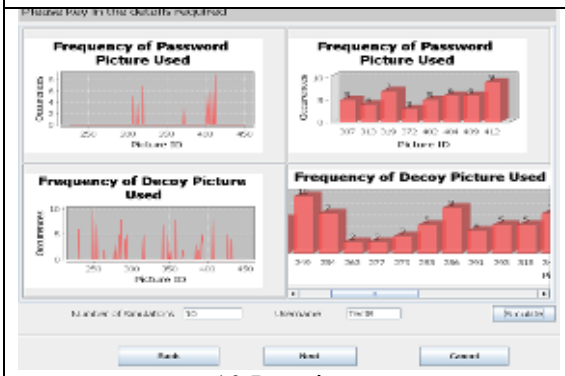
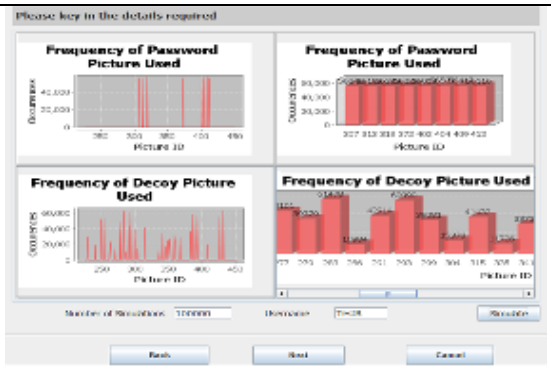
Simulation Result	
 10 Iterations	 100 Iterations
 10000 Iterations	 100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table B8: Analysis and Observation Result for $R_8^{j_{4,5}}$

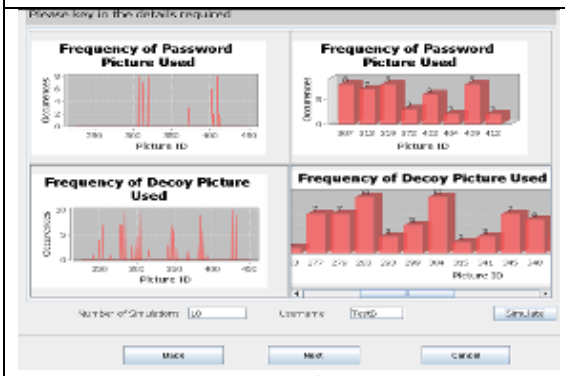
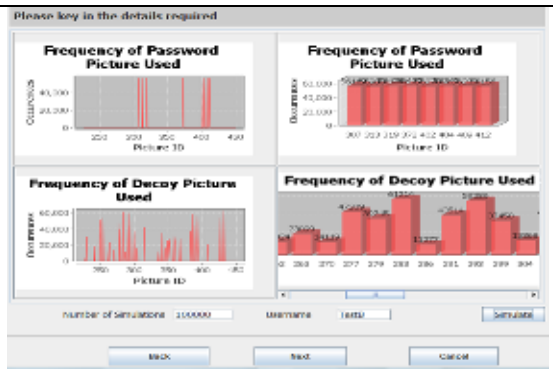
Simulation Result	
 10 Iterations	 100 Iterations
 10000 Iterations	 100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table B9: Analysis and Observation Result for $R_9^{j_{4.5}}$

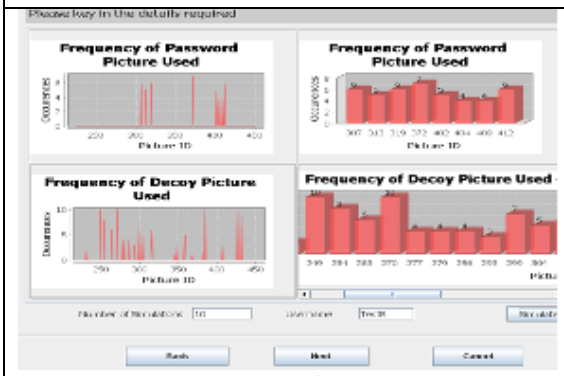
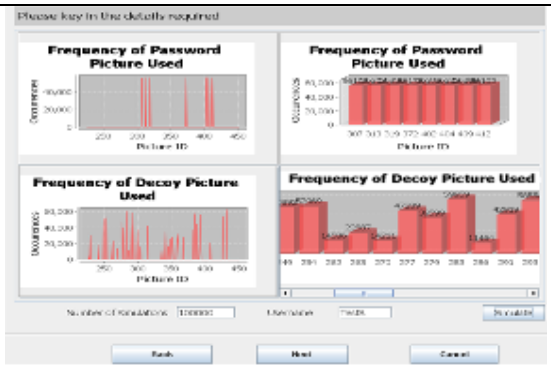
Simulation Result	
 10 Iterations	 100 Iterations
 10000 Iterations	 100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table B10: Analysis and Observation Result for $\overset{j_{4.5}}{R_{10}}$

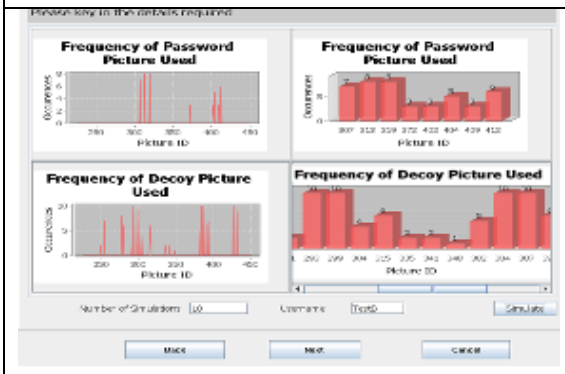
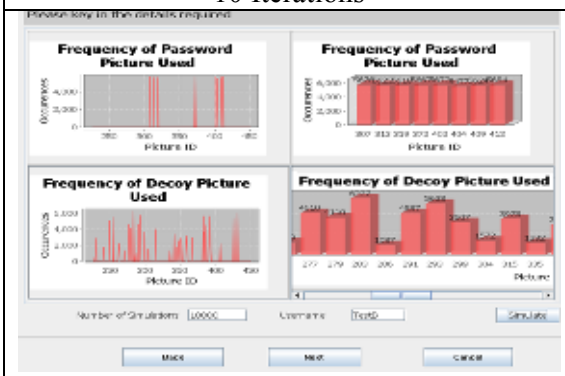
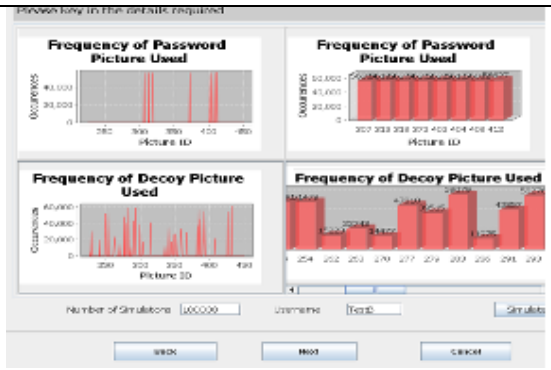
Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations
Observation Result	
Secret password used cannot be obtained based on highest frequency of occurrence.	

Table C1: Analysis and Observation Result for $R_1^{j_{4.6}}$

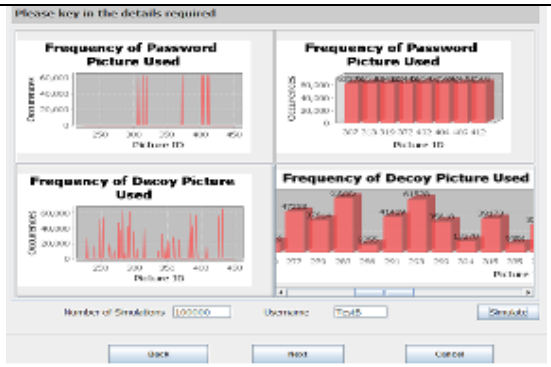
Simulation Result	
 10 Iterations	 100 Iterations
 10000 Iterations	 100000 Iterations
Observation Result	
One of the secret password pictures has higher frequency of occurrence compared with the decoy pictures in 10 iteration simulations. Only a few decoy pictures have higher frequency of occurrence when compared with the secret password pictures in 100, 10,000 and 100,000 iteration simulations. It is predictable that the secret password used can be obtained based on the highest frequency of occurrence when the number of iterations has increased beyond 100,000 iterations. (Reason: The upper bound *j* secret password used is high.)	

Table C2: Analysis and Observation Result for $R_2^{j_{4.6}}$

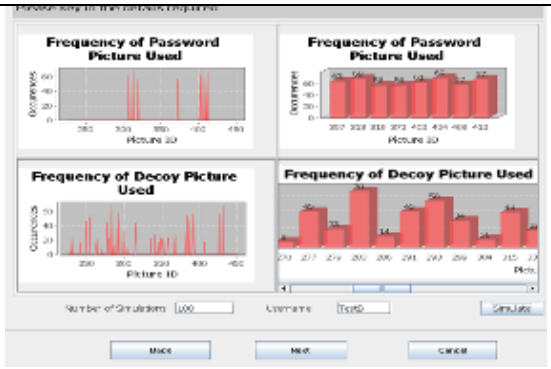
Simulation Result	
 10 Iterations	 100 Iterations
 10000 Iterations	 100000 Iterations
Observation Result	
Only a few decoy pictures have higher frequency of occurrence when compared with the secret password pictures in 10, 100 and 10,000 iteration simulations. The secret password used can be obtained based on the highest frequency of occurrence in 100000 iteration simulations. (Reason: The upper bound *j* secret password used is high.)	

Table C3: Analysis and Observation Result for $R_3^{j_{4.6}}$

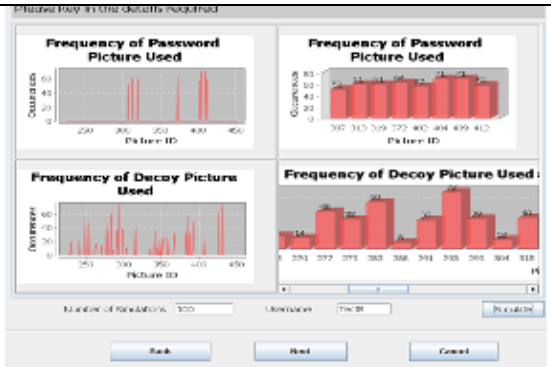
Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations
Observation Result	
One of the secret password pictures produces the same peak value as the decoy pictures in 10 iteration simulations. Only a few decoy pictures have higher frequency of occurrence when compared with the secret password pictures in 100 and 10,000 iteration simulations. The secret password used can be obtained based on the highest frequency of occurrence in 100,000 iteration simulations. (Reason: The upper bound *j* secret password used is high.)	

Table C4: Analysis and Observation Result for $R_4^{j_{4.6}}$

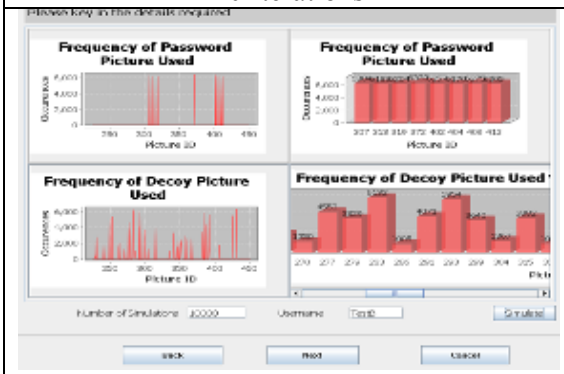
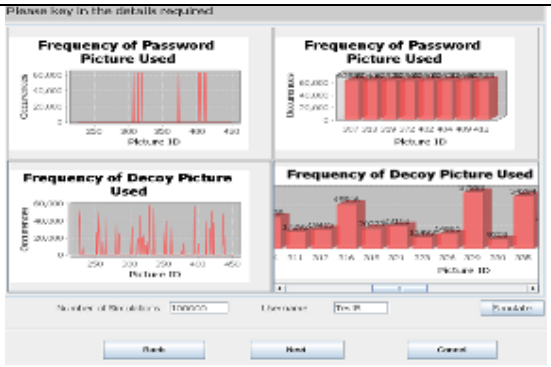
Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations
Observation Result	
One of the secret password pictures produces the highest value of frequency of occurrence in 10 iteration simulations. In 100 iteration simulations, the decoy pictures that have higher frequency of occurrence are not many compared to the secret password pictures. However, the secret password used can be obtained based on the highest frequency of occurrence in 10,000 and 100,000 iteration simulations. (Reason: The upper bound j secret password used is high. It may require higher distribution range to produce better result.)	

Table C5: Analysis and Observation Result for $\overset{j_{4.6}}{R_5}$

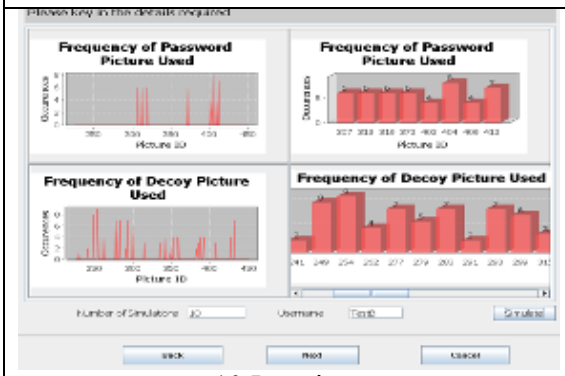
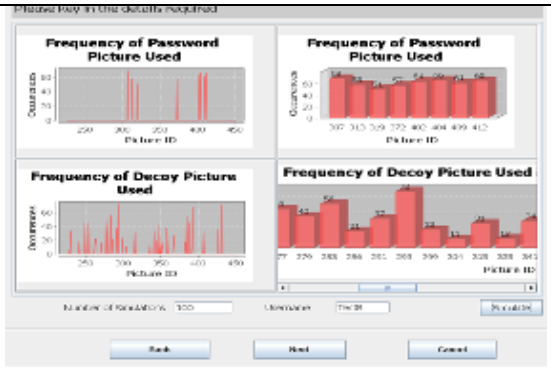
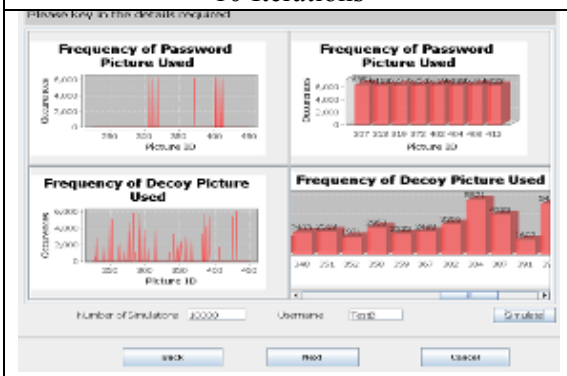
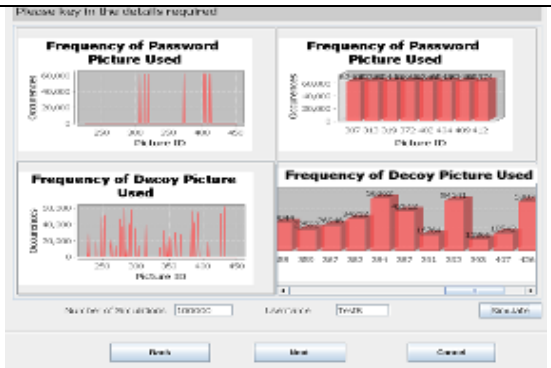
Simulation Result	
 10 Iterations	 100 Iterations
 10000 Iterations	 100000 Iterations
Observation Result	
The observation result is similar to $\overset{j_{4.6}}{R_4}$ where the secret password used cannot be obtained based on the highest frequency of occurrence in 10 iteration simulations. A few decoy pictures produced have higher frequency of occurrence when compared with the secret password pictures in 100 iteration simulations. The secret password used can be obtained based on the highest frequency of occurrence in 10,000 and 100,000 iteration simulations. (Reason: The upper bound j secret password used is high.)	

Table C6: Analysis and Observation Result for $\overset{j_{4.6}}{R_6}$

Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations

Observation Result

The observation result is similar to $\overset{j_{4.6}}{R_5}$ where the secret password used cannot be obtained based on the highest frequency of occurrence in 10 iteration simulations. A few decoy pictures produced have higher frequency of occurrence when compared with the secret password pictures in 100 iteration simulations. The secret password used can be obtained based on the highest frequency of occurrence in 10,000 and 100,000 iteration simulations. (Reason: The upper bound *j* secret password used is high.)

Table C7: Analysis and Observation Result for $\overset{j_{4.6}}{R_7}$

Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations
Observation Result	

The observation result is similar to $\overset{j_{4.6}}{R_6}$ where the secret password used cannot be obtained based on the highest frequency of occurrence in 10 iteration simulations. A few decoy pictures produced have higher frequency of occurrence when compared with the secret password pictures in 100 iteration simulations. The secret password used can be obtained based on the highest frequency of occurrence in 10,000 and 100,000 iteration simulations. (Reason: The upper bound j secret password used is high.)

Table C8: Analysis and Observation Result for $R_8^{j_{4.6}}$

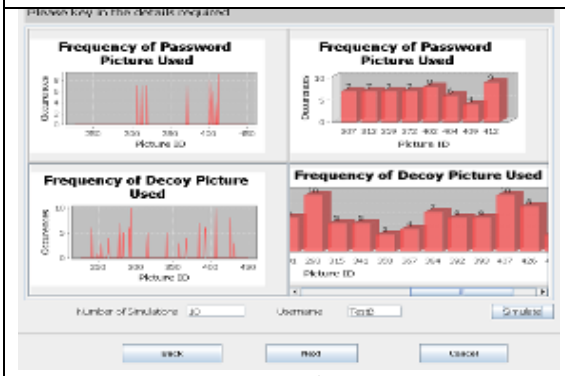
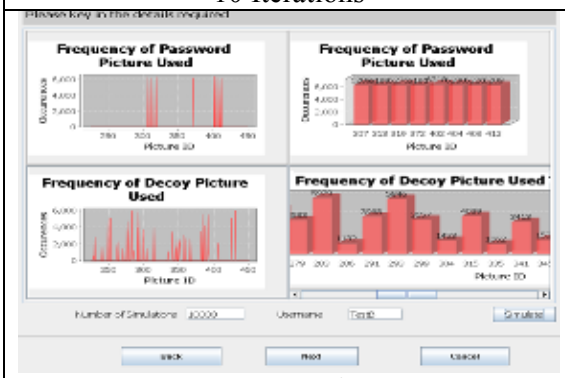
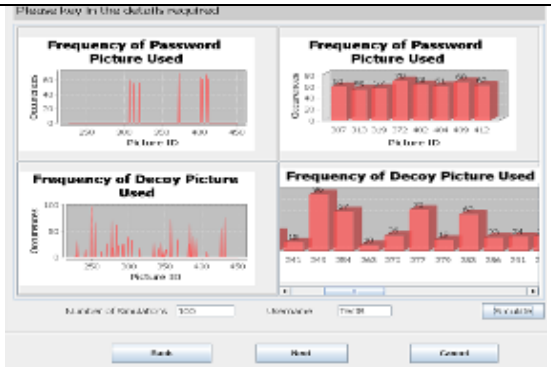
Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations
Observation Result	
Only a few decoy pictures have higher frequency of occurrence compared to the secret password pictures in 10 and 100 iteration simulations. However, the secret password used can be obtained based on the highest frequency of occurrence in 10,000 and 100,000 iteration simulations. (Reason: The upper bound *j* secret password used is high. It requires higher distribution range to produce better result.)	

Table C9: Analysis and Observation Result for $R_9^{j_{4.6}}$

Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations

Observation Result

In 10 iteration simulations, the secret password used cannot be obtained based on the highest frequency of occurrence. However, only several decoy pictures produce higher frequency of occurrence when compared with the secret password pictures in 100 iteration simulations. The secret password used can be obtained based on the highest frequency of occurrence in 10,000 and 100,000 iteration simulations. (Reason: The upper bound *j* secret password used is high. It needs higher distribution range to produce better result.)

Appendix E

Table D1: Analysis and Observation Result for Classification 1

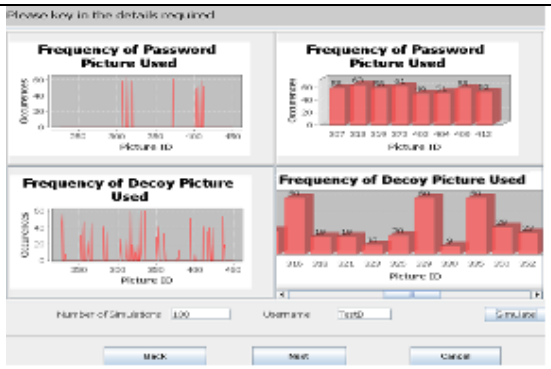
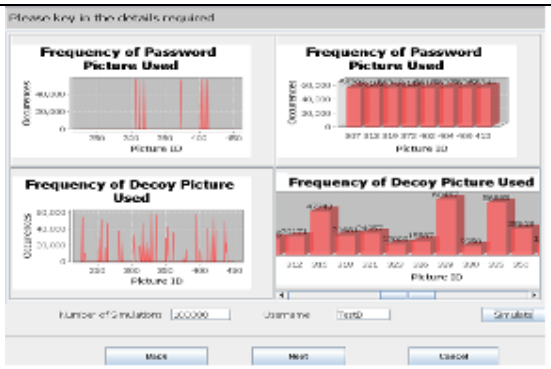
Simulation Result	
 10 Iterations	 100 Iterations
 10000 Iterations	 100000 Iterations
Observation Result	
The peak value of the frequency of occurrence goes to one of the secret password pictures in 10 iteration simulations. A few secret password pictures have higher frequency of occurrence when compared with the decoy pictures in 100 iteration simulations. However, The secret password used cannot be obtained based on the highest frequency of occurrence in 10,000 and 100,000 iteration simulations. (Reason: The upper bound volume for the decoy pictures used is too low.)	

Table D2: Analysis and Observation Result for Classification 2

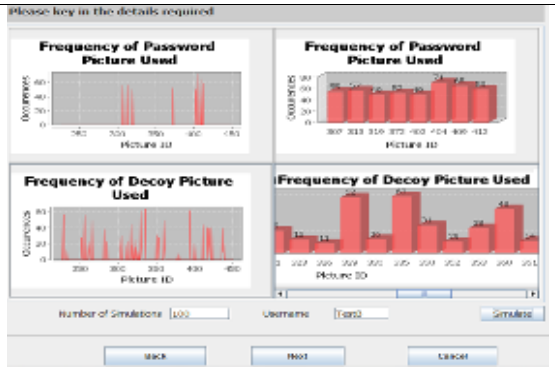
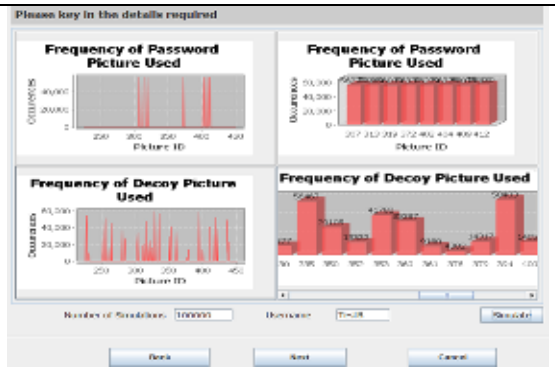
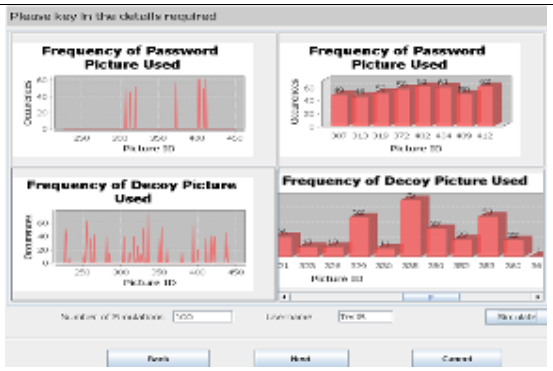
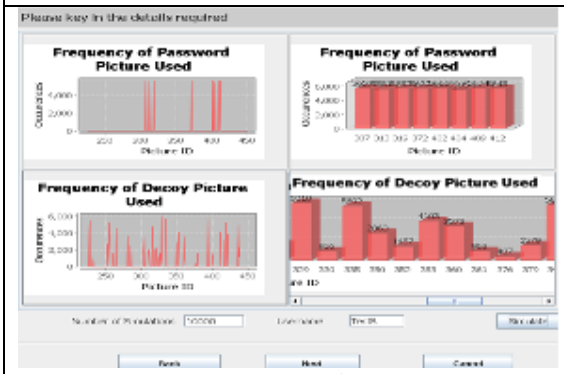
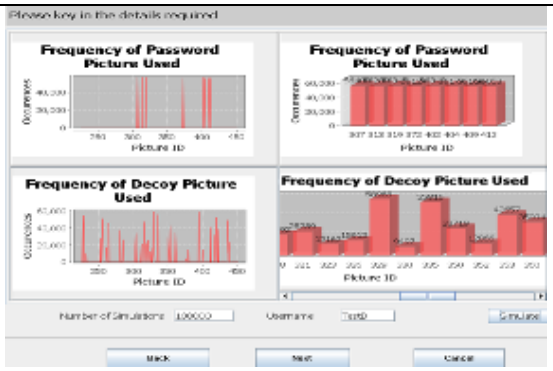
Simulation Result	
 10 Iterations	 100 Iterations
 10000 Iterations	 100000 Iterations
Observation Result	
A few decoy pictures have higher frequency of occurrence compared to the secret password pictures in 10 iteration simulations. However, one of the secret passwords has the highest frequency of occurrence value when compared with the decoy pictures in 100 iteration simulations. In 10,000 iteration simulations, there are few decoy pictures produced have higher frequency of occurrence compared with the secret passwords pictures. Nevertheless, the secret password used cannot be obtained based on highest frequency of occurrence in 100,000 iteration simulations. (Reason: The upper bound volume for the decoy pictures used is too low.)	

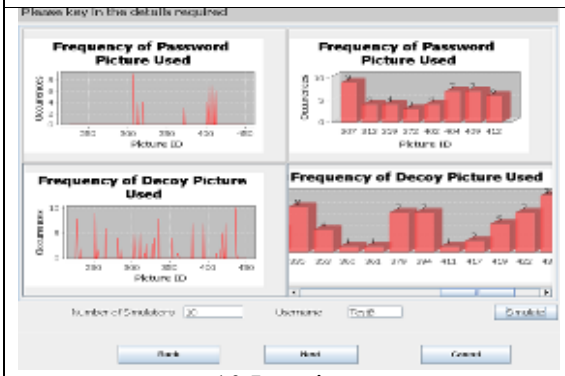
Table D3: Analysis and Observation Result for Classification 3

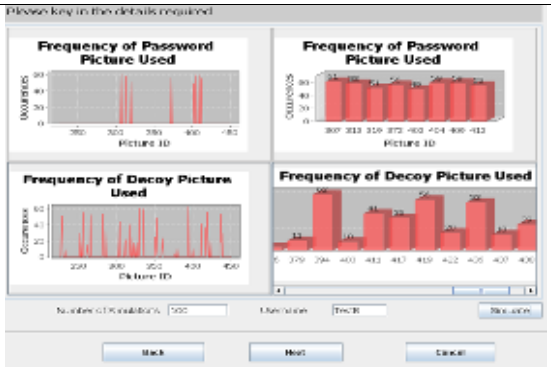
Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations

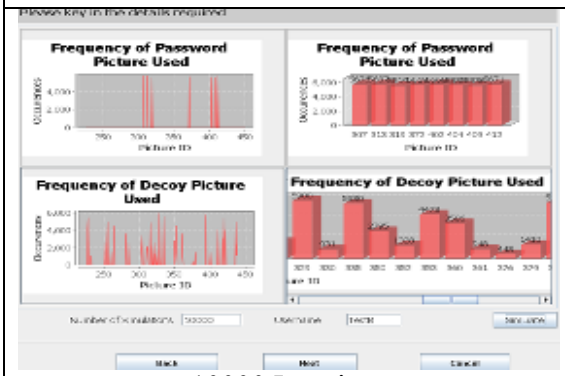
Observation Result

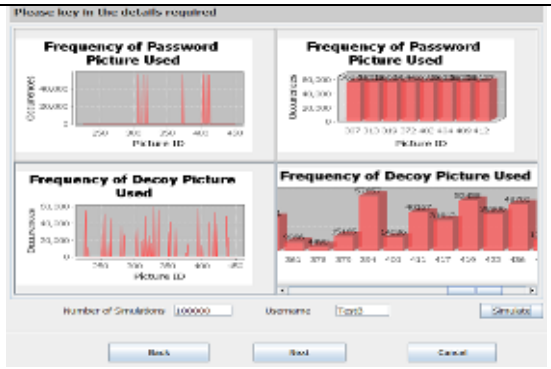
One of the secret password pictures produces the highest frequency of occurrence in 10 iteration simulations. A few decoy pictures produced have higher frequency of occurrence when compared with the secret passwords in 100 iteration simulations. However, the secret password used cannot be obtained based on highest frequency of occurrence in 10,000 and 100,000 iteration simulations. (Reason: The upper bound volume for the decoy pictures used is too low.)

Table D4: Analysis and Observation Result for Classification 4

<table>
<tr><td colspan="2">Simulation Result</td></tr>
<tr><td> 

10 Iterations</td><td> 

100 Iterations</td></tr>
<tr><td> 

10000 Iterations</td><td> 

100000 Iterations</td></tr>
<tr><td colspan="2">Observation Result

The secret password used cannot be obtained based on highest frequency of occurrence in 10, 100, 10,000 and 100,000 iteration simulations.</td></tr>
</table>

Table D5: Analysis and Observation Result for Classification 5

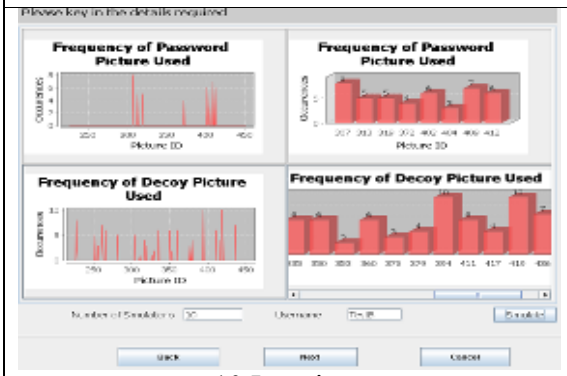
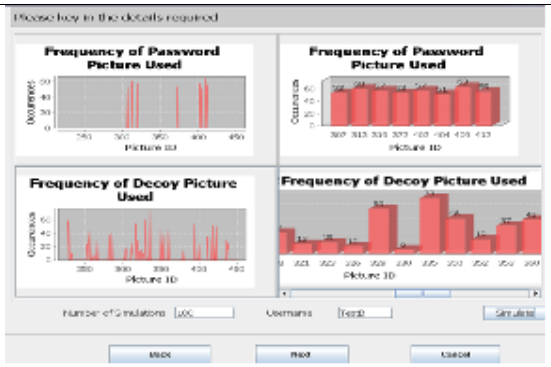
Simulation Result	
 10 Iterations	 100 Iterations
 10000 Iterations	 100000 Iterations
Observation Result	
The secret password used cannot be obtained based on highest frequency of occurrence in 10, 100, 10,000 and 100,000 iteration simulations.	

Table D6: Analysis and Observation Result for Classification 6

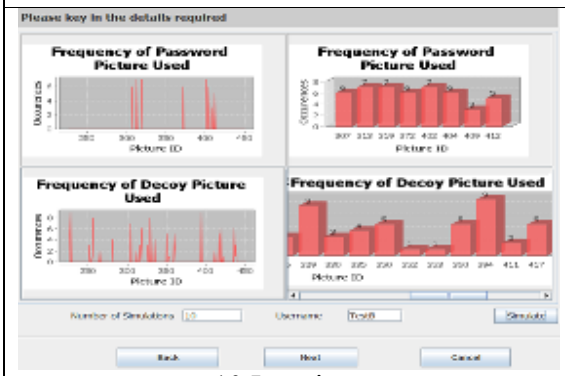
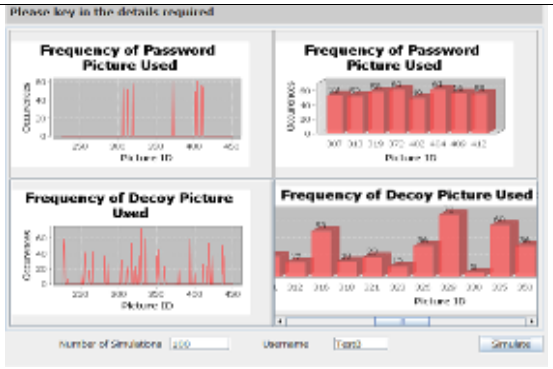
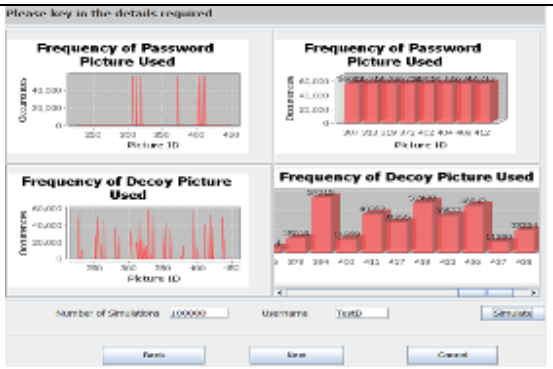
Simulation Result	
	
10 Iterations	100 Iterations
	
10000 Iterations	100000 Iterations
Observation Result	
The secret password used cannot be obtained based on highest frequency of occurrence in 10, 100, 10,000, and 100,000 iteration simulations.	

Table D7: Analysis and Observation Result for Classification 7

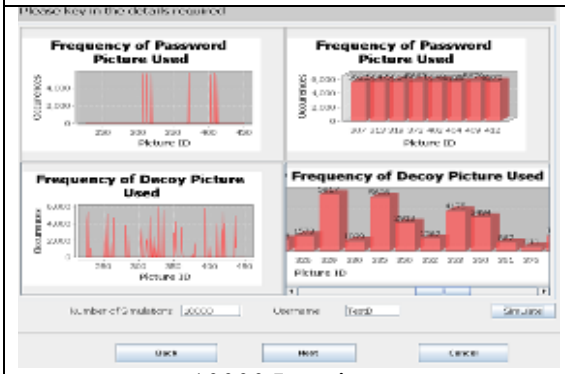
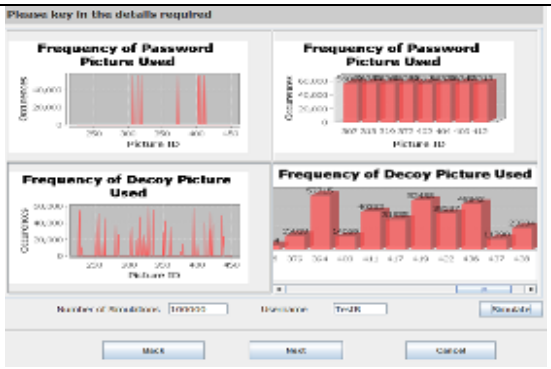
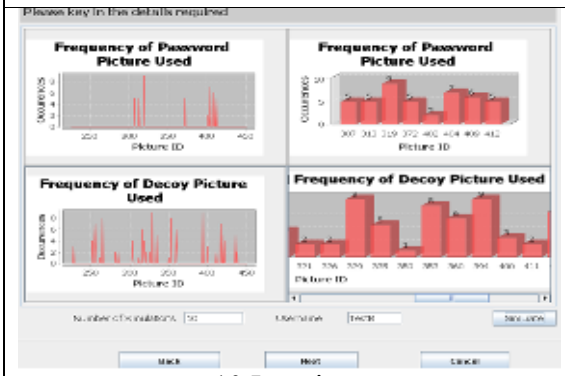
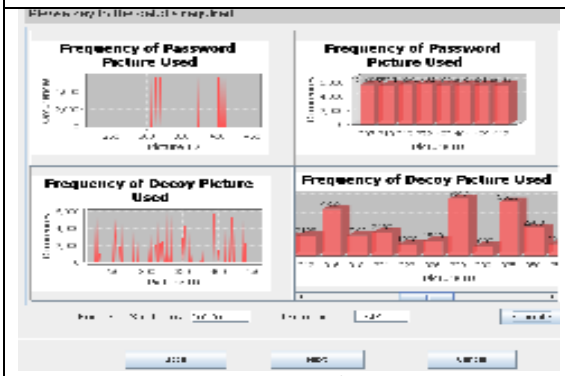
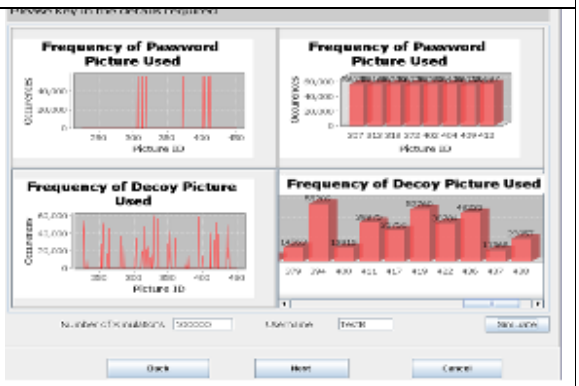
Simulation Result	
 10 Iterations	 100 Iterations
 10000 Iterations	 100000 Iterations
Observation Result	
The secret password used cannot be obtained based on highest frequency of occurrence in 10, 100, 10,000, and 100,000 iteration simulations.	

Table D8: Analysis and Observation Result for Classification 8

Simulation Result	
 10 Iterations	 100 Iterations
 10000 Iterations	 100000 Iterations
Observation Result	
One of the secret password pictures produces the same peak value as the decoy pictures in 10 iteration simulations and one of the secret password pictures produces the highest value of frequency of occurrence in 100 iterations simulation. Moreover, in 100 iterations simulation, the decoy pictures that have higher frequency of occurrence are not many compared to the secret password pictures. However, the secret password used can be obtained based on the highest frequency of occurrence in 10,000, and 100,000 iteration simulations. (Reason: The lower bound volume for the decoy pictures used is too low.)	

Appendix F

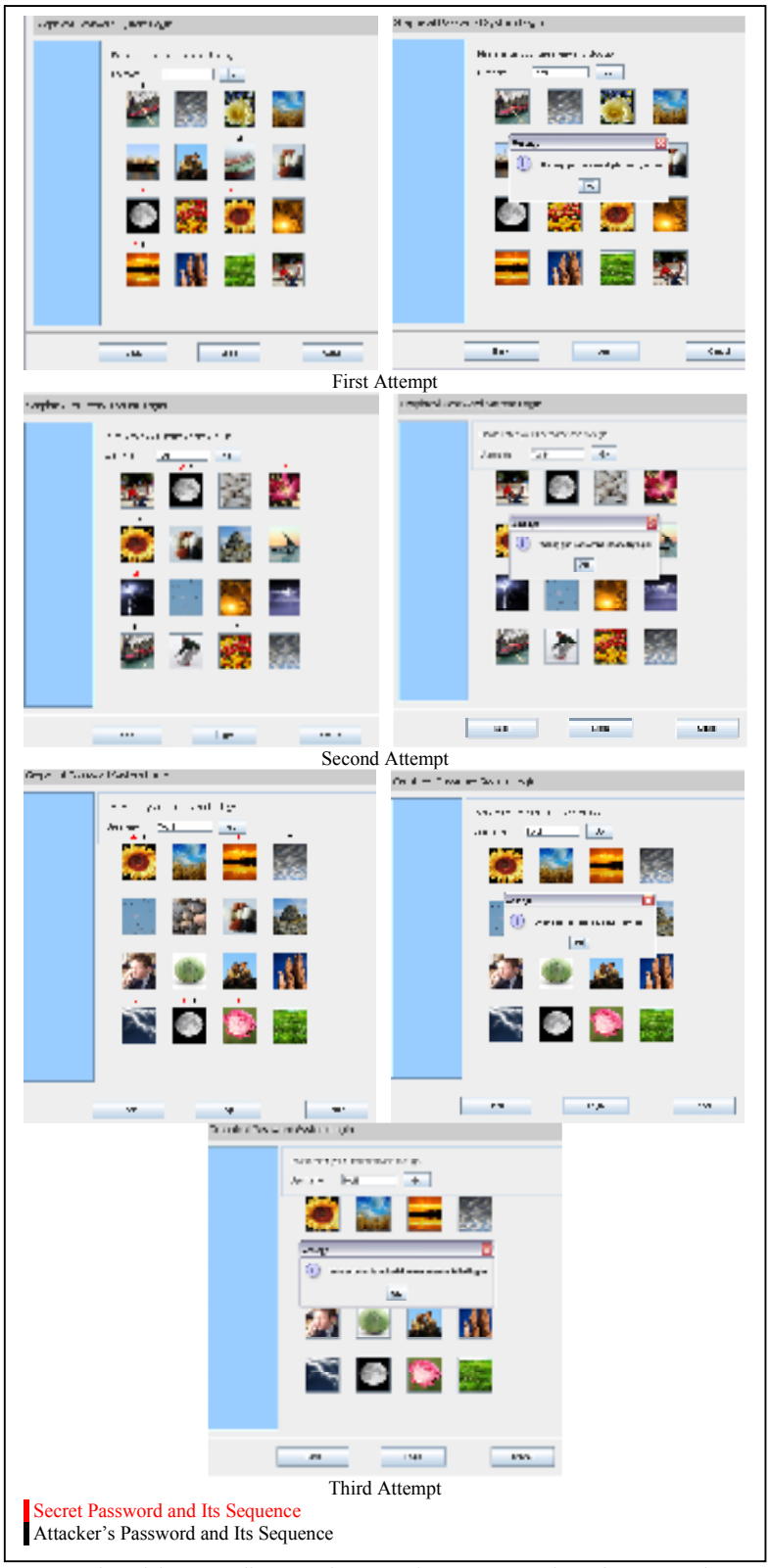


Figure 1: Shoulder-Surfing and Guessing Screenshot for Attacker No.1

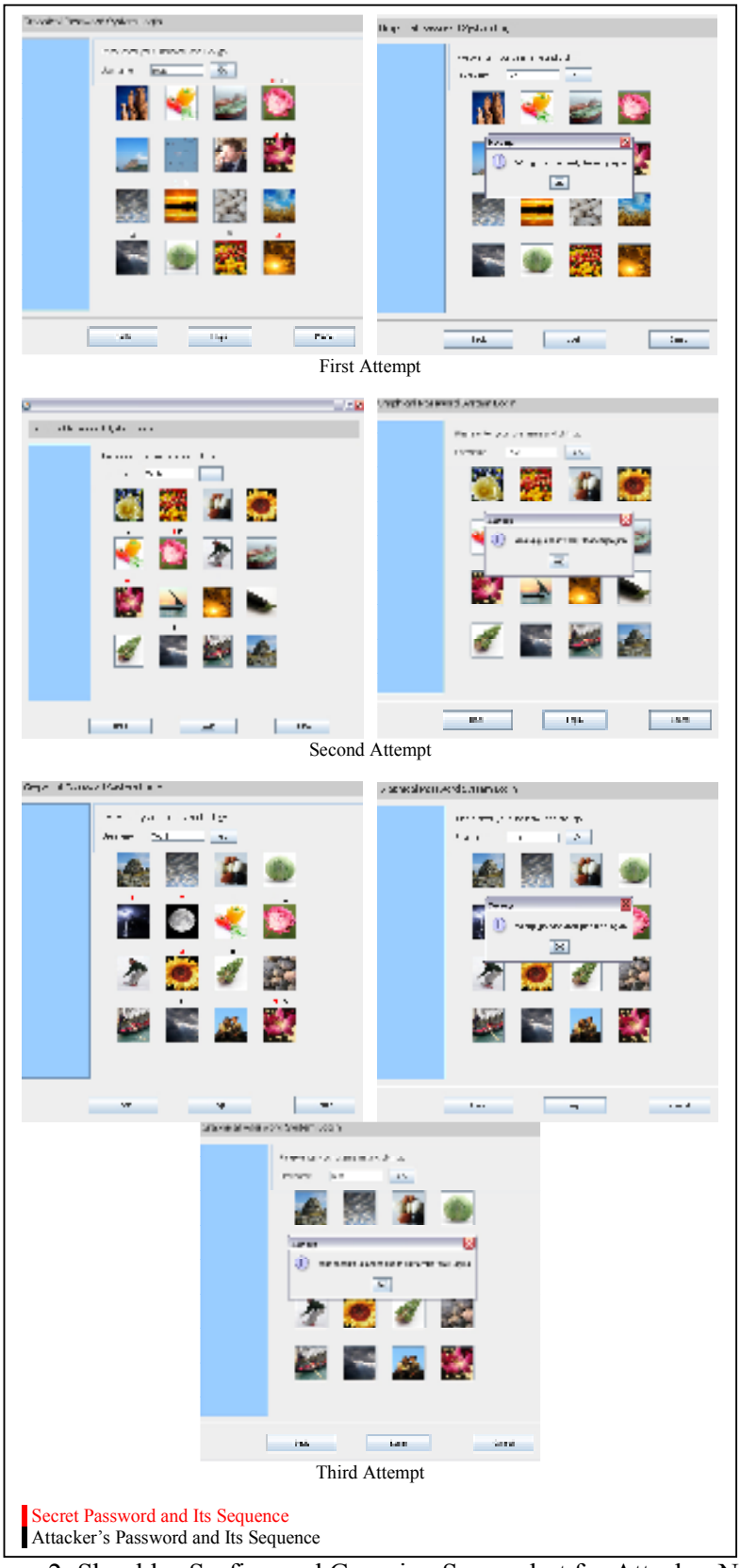


Figure 2: Shoulder-Surfing and Guessing Screenshot for Attacker No.2

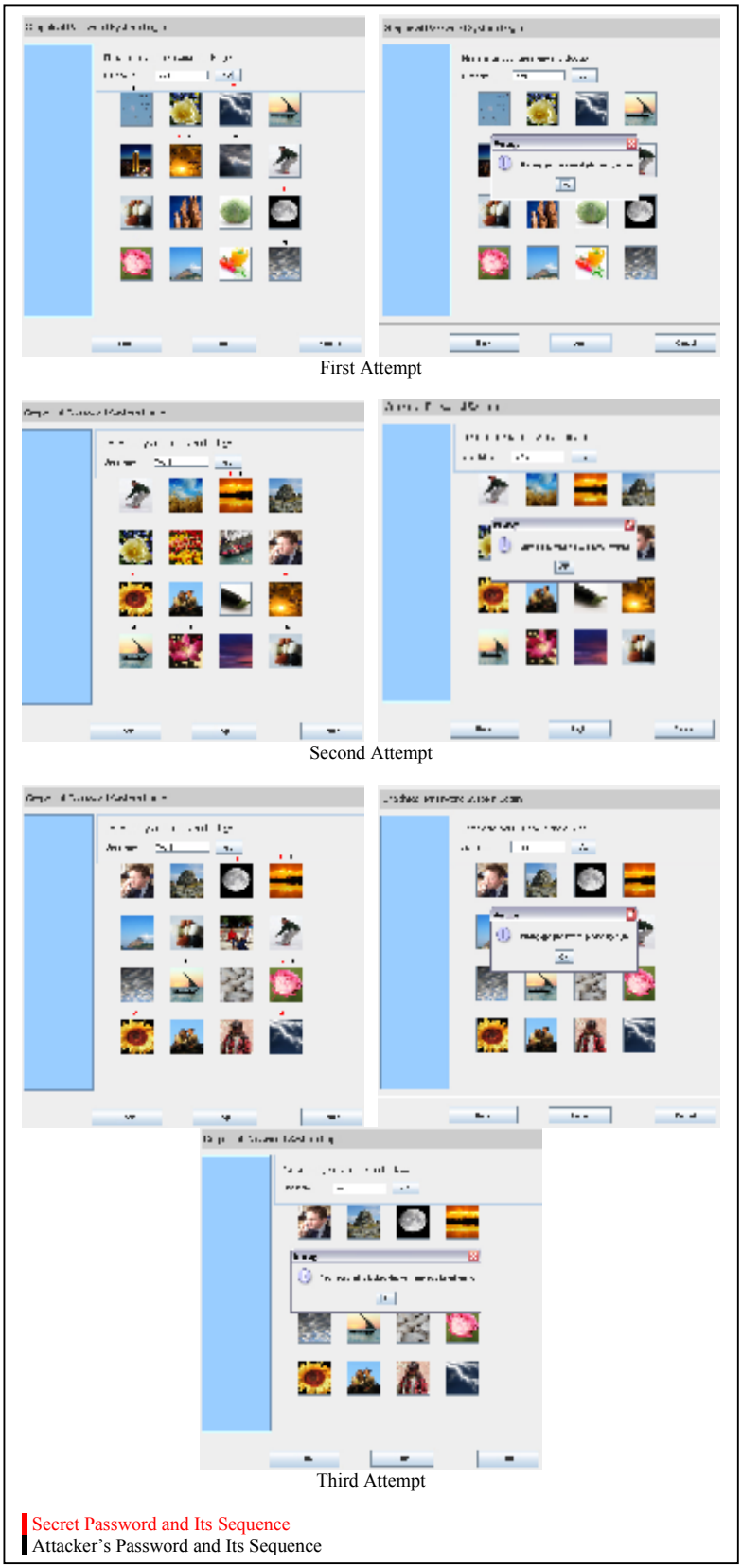


Figure 3: Shoulder-Surfing and Guessing Screenshot for Attacker No.3

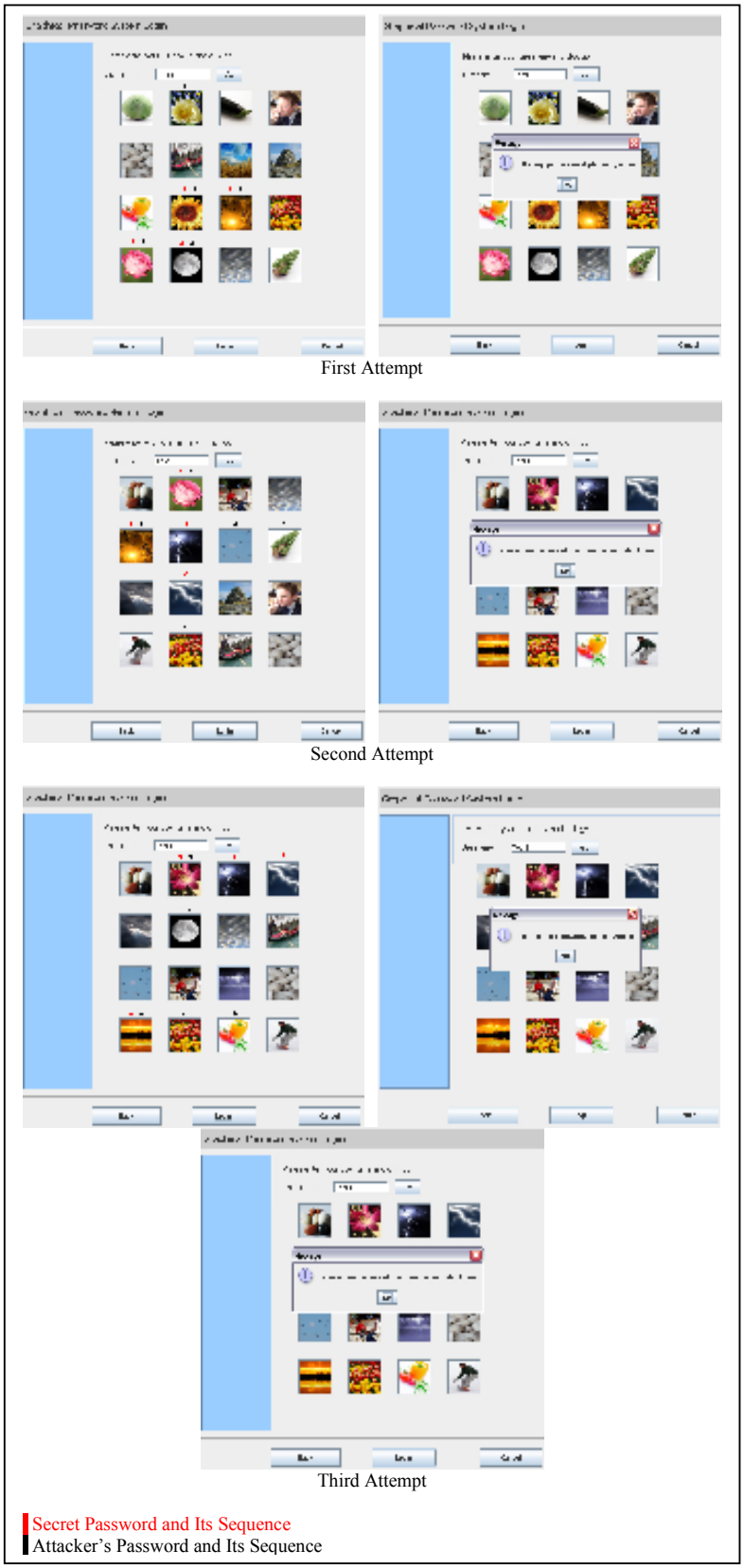


Figure 4: Shoulder-Surfing and Guessing Screenshot for Attacker No.4

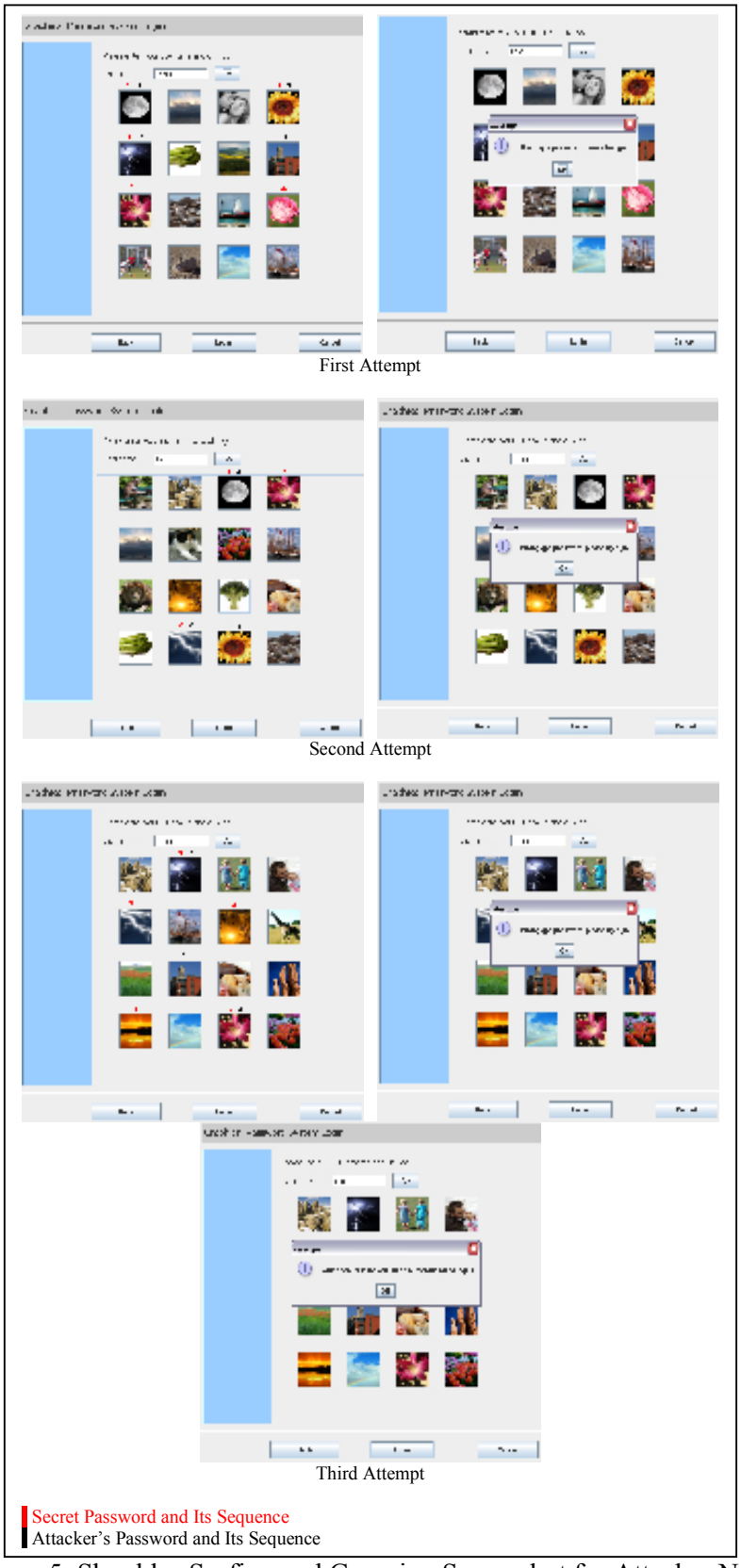
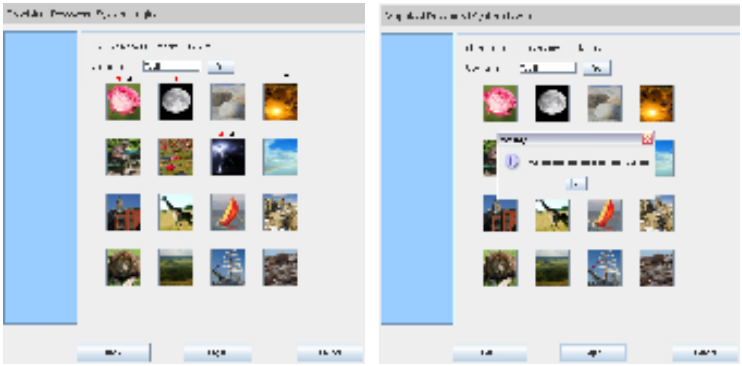
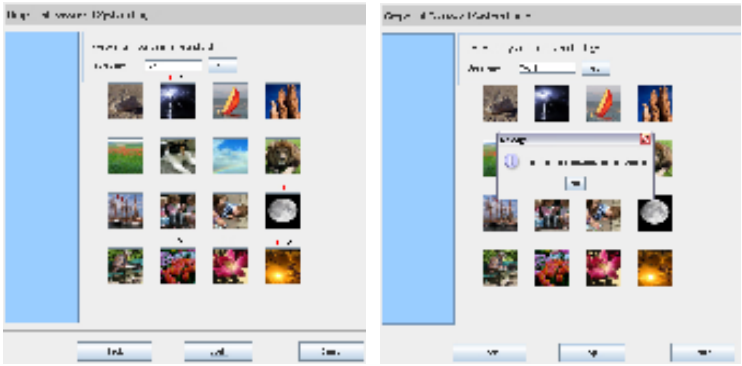


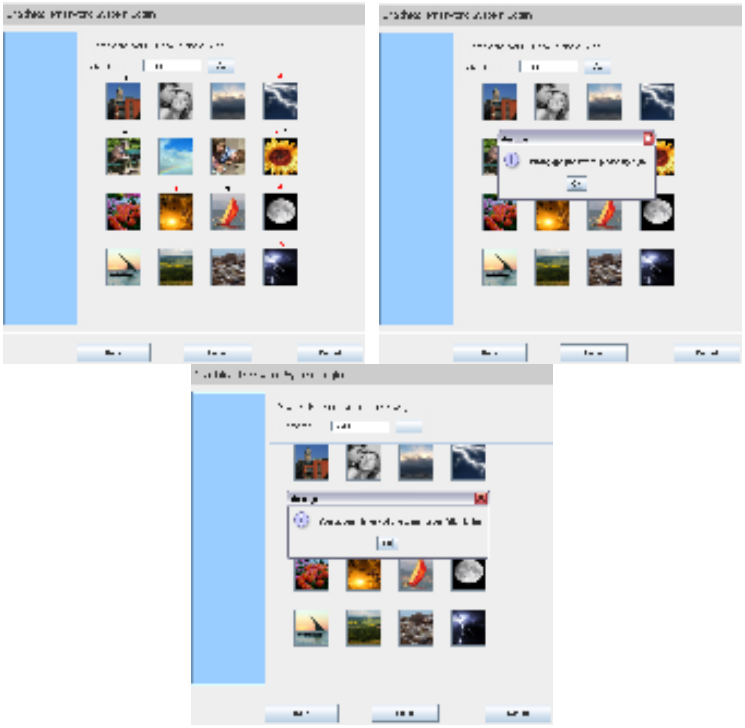
Figure 5: Shoulder-Surfing and Guessing Screenshot for Attacker No.5



First Attempt



Second Attempt



Third Attempt

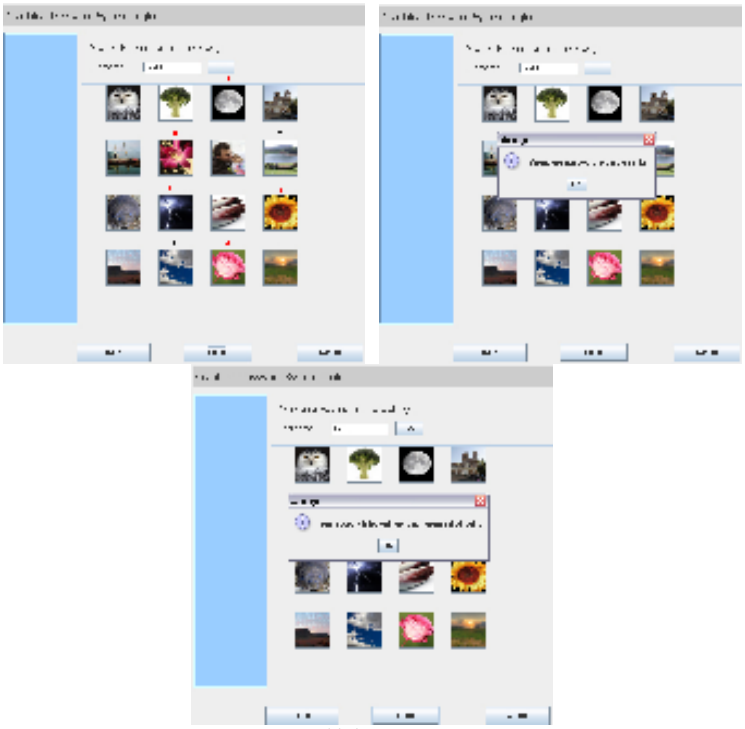
Secret Password and Its Sequence
Attacker's Password and Its Sequence

Figure 6: Shoulder-Surfing and Guessing Screenshot for Attacker No.6

Figure 7: Shoulder-Surfing and Guessing Screenshot for Attacker No.7

First Attempt

Second Attempt



Third Attempt

Secret Password and Its Sequence
Attacker's Password and Its Sequence

Figure 8: Shoulder-Surfing and Guessing Screenshot for Attacker No.8

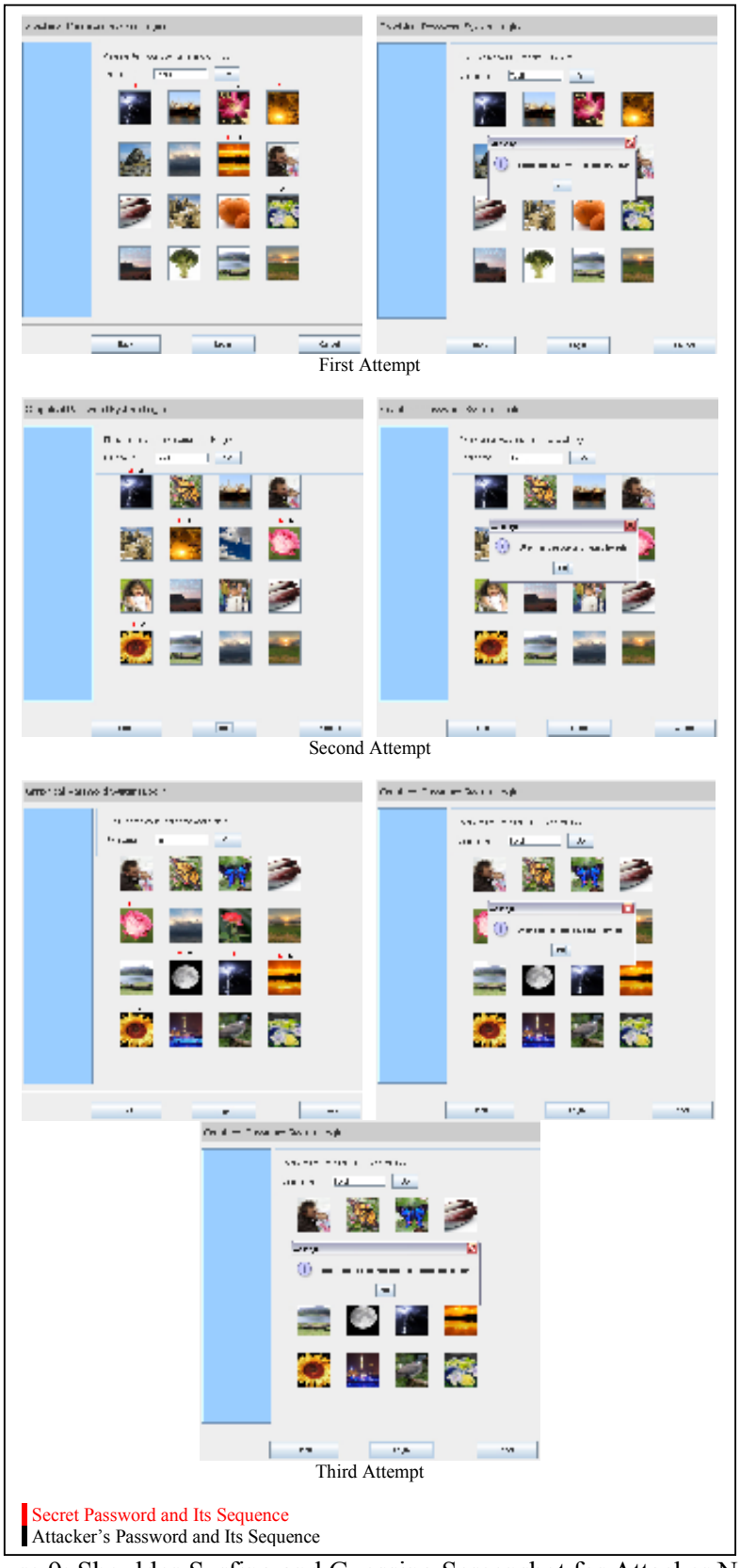


Figure 9: Shoulder-Surfing and Guessing Screenshot for Attacker No.9

First Attempt

Second Attempt

Third Attempt

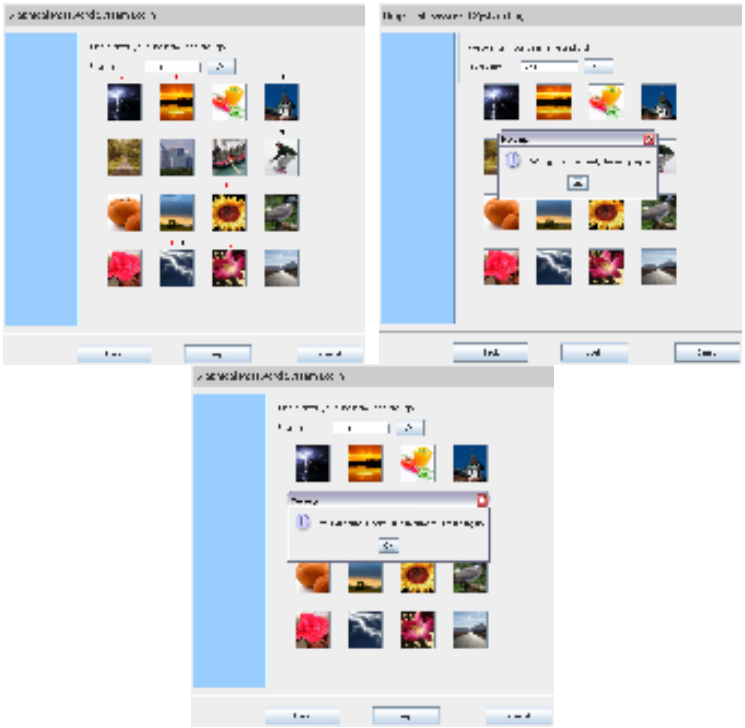
Secret Password and Its Sequence
Attacker's Password and Its Sequence

Figure 10: Shoulder-Surfing and Guessing Screenshot for Attacker No.10

Figure 11: Shoulder-Surfing and Guessing Screenshot for Attacker No.11

First Attempt

Second Attempt



Third Attempt

Secret Password and Its Sequence
Attacker's Password and Its Sequence

Figure 12: Shoulder-Surfing and Guessing Screenshot for Attacker No.12

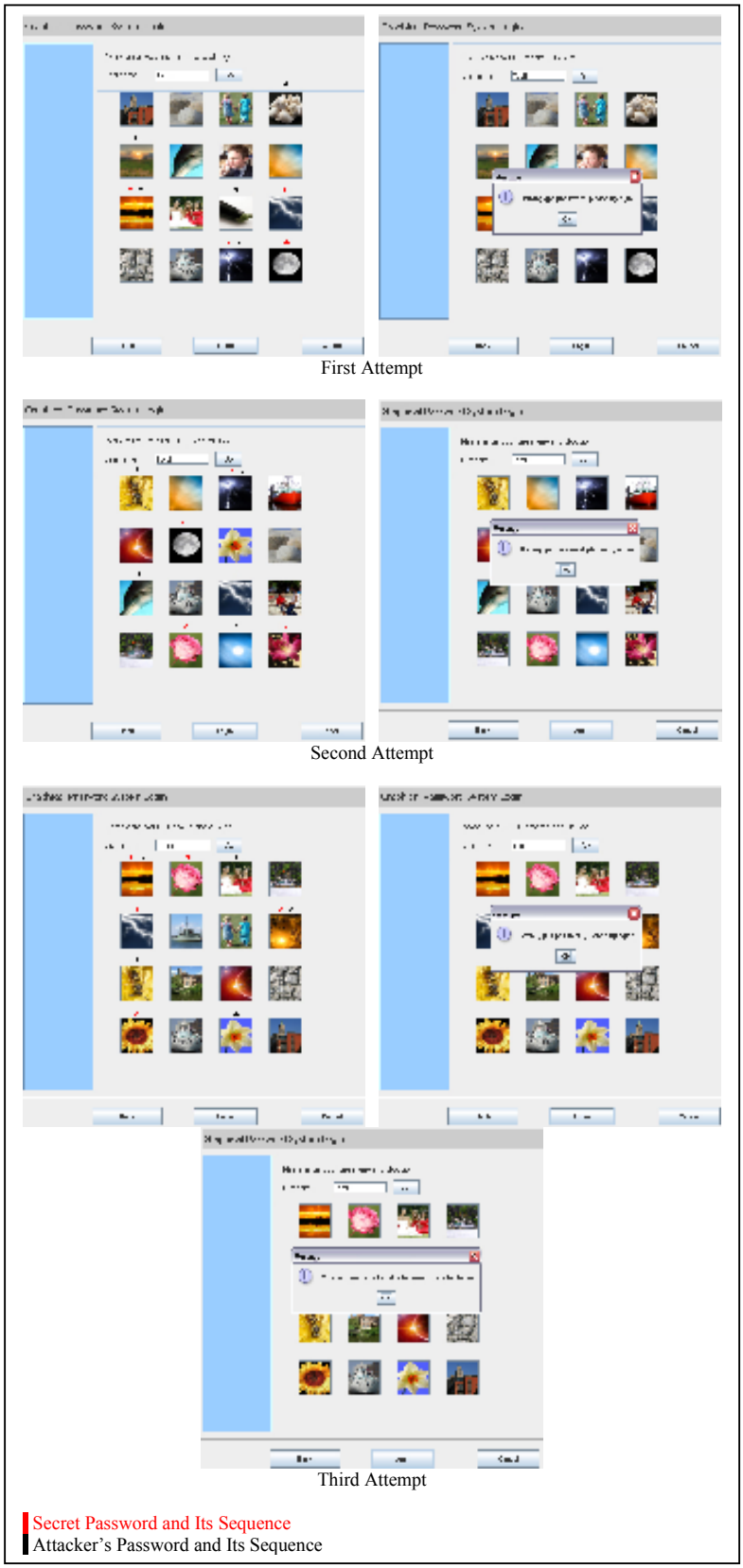


Figure 13: Shoulder-Surfing and Guessing Screenshot for Attacker No.13

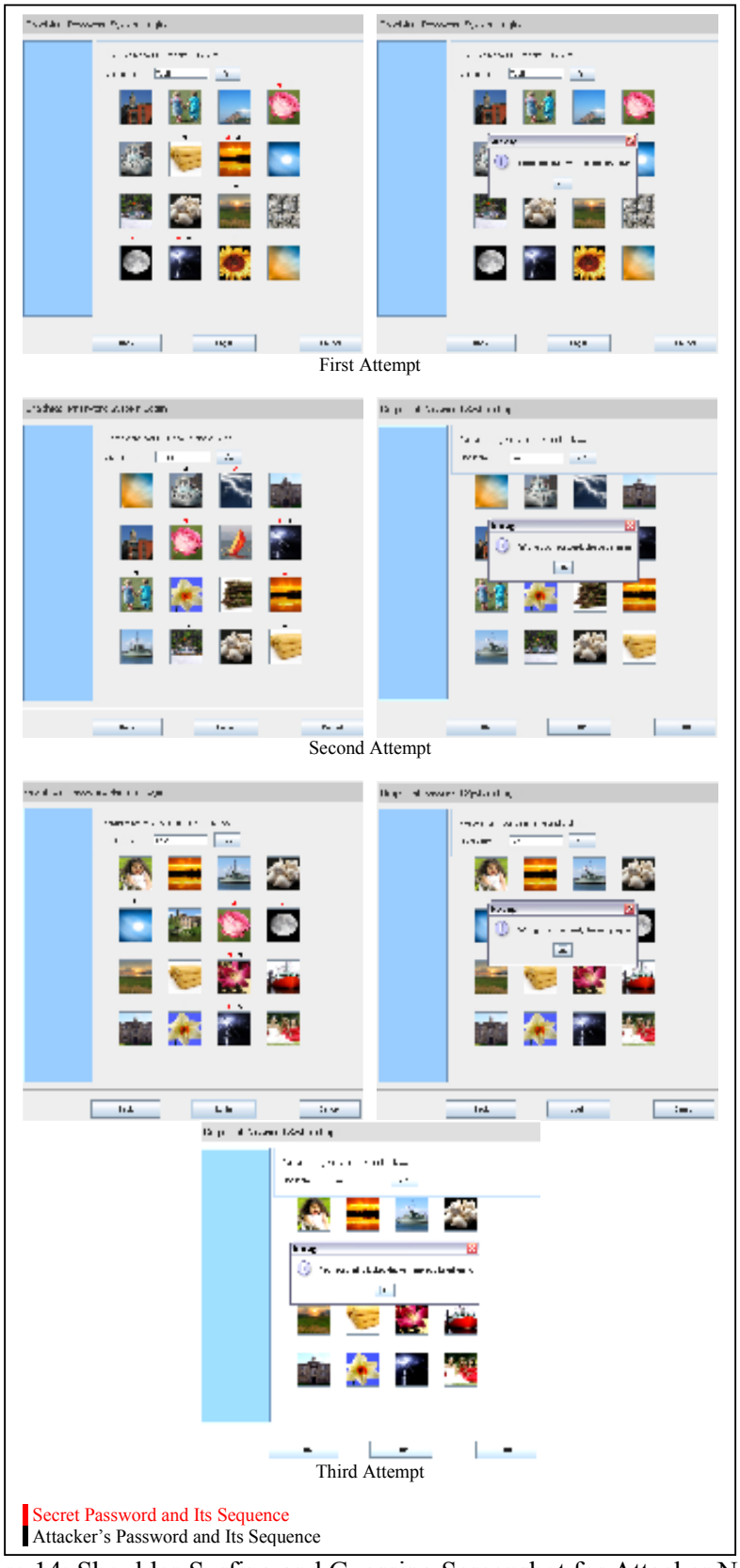


Figure 14: Shoulder-Surfing and Guessing Screenshot for Attacker No.14

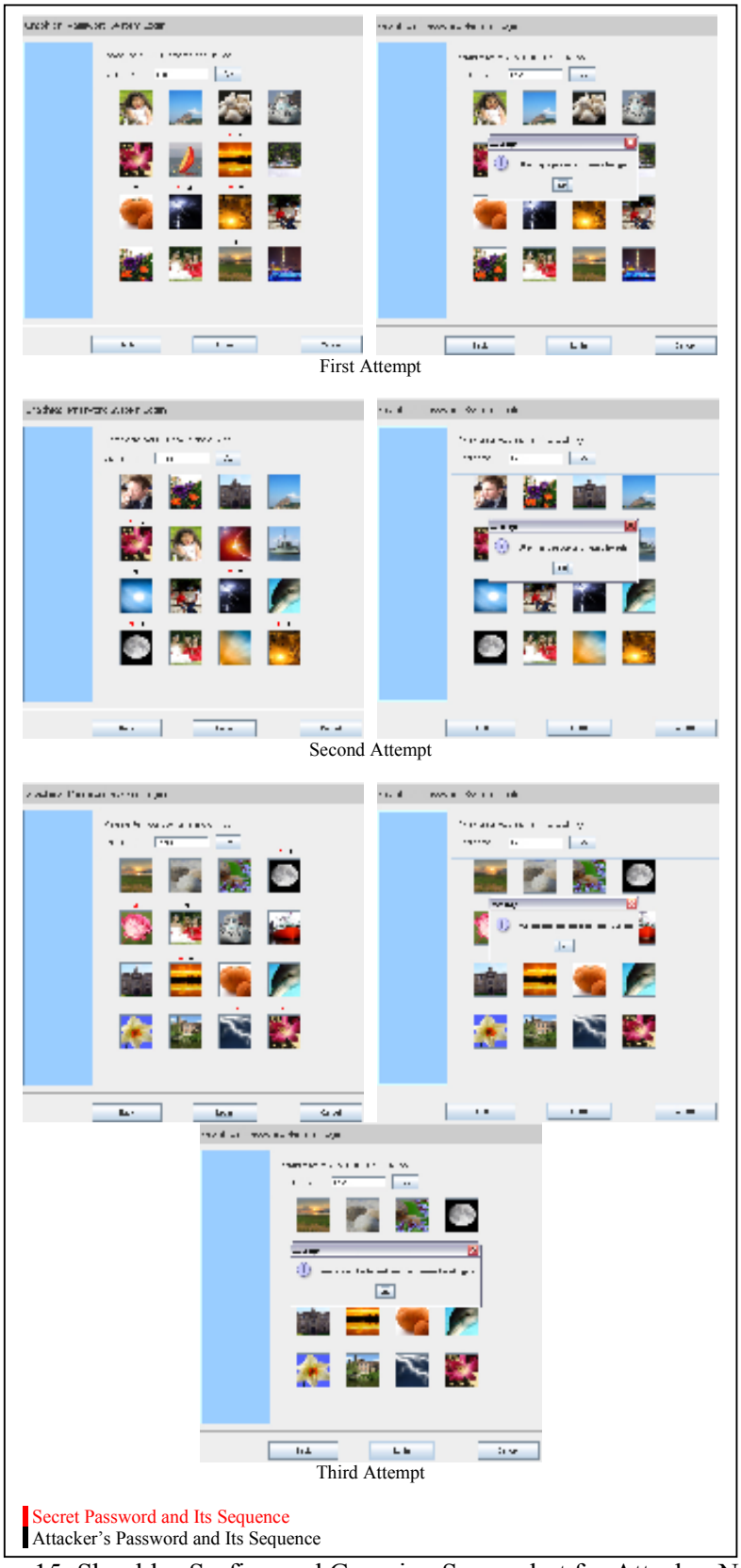


Figure 15: Shoulder-Surfing and Guessing Screenshot for Attacker No.15

Figure 16: Shoulder-Surfing and Guessing Screenshot for Attacker No.16

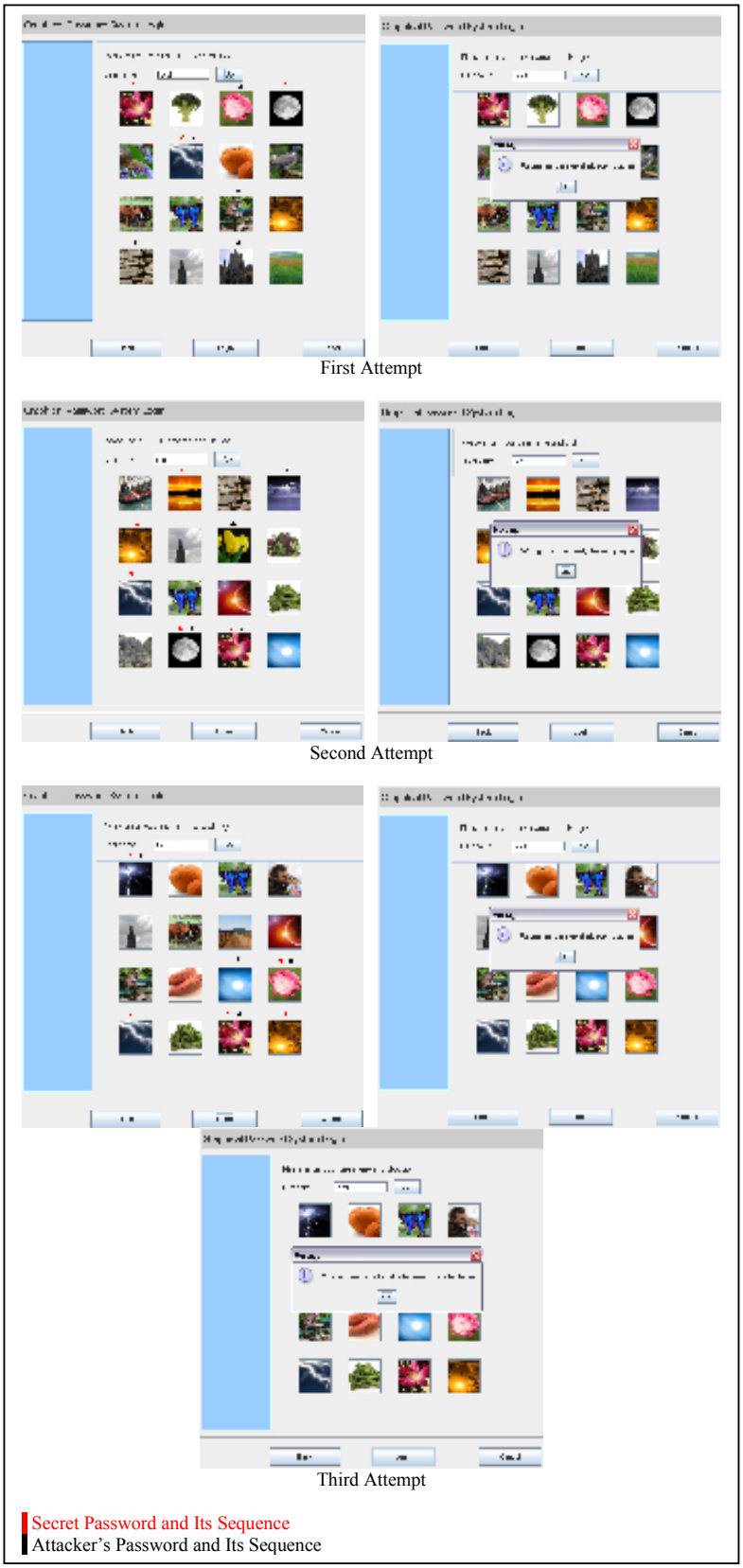


Figure 17: Shoulder-Surfing and Guessing Screenshot for Attacker No.17

Figure 18: Shoulder-Surfing and Guessing Screenshot for Attacker No.18

Figure 19: Shoulder-Surfing and Guessing Screenshot for Attacker No.19

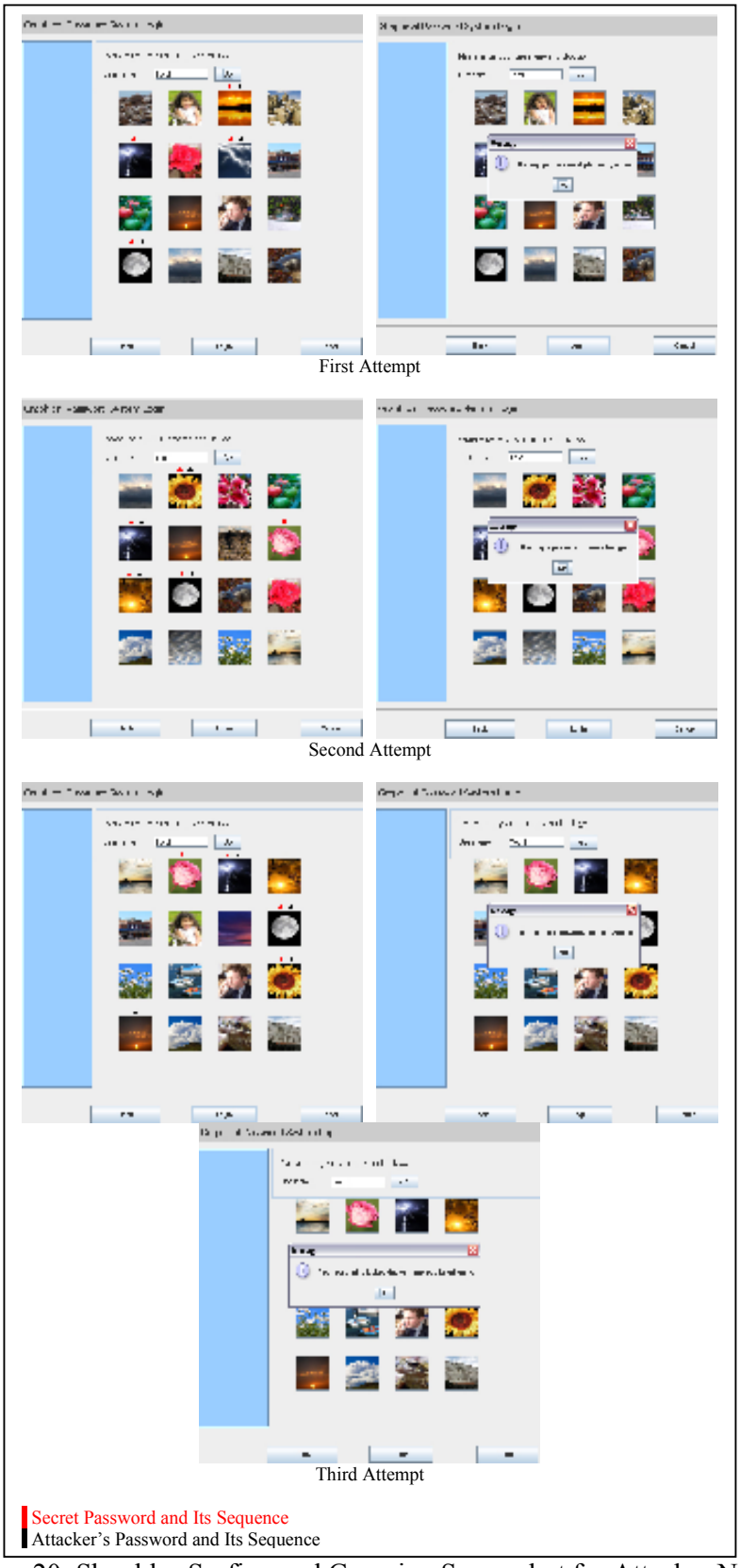


Figure 20: Shoulder-Surfing and Guessing Screenshot for Attacker No.20

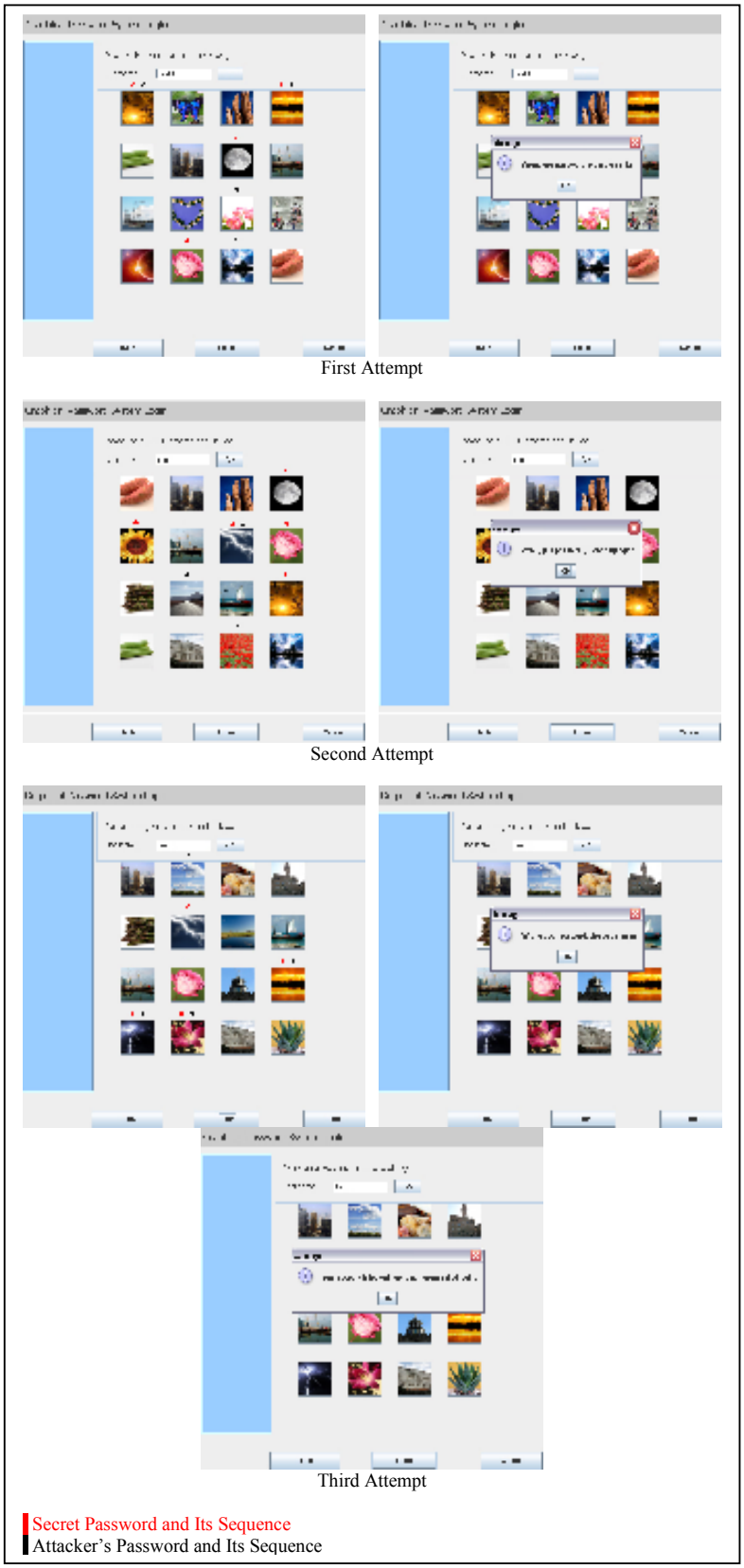


Figure 21: Shoulder-Surfing and Guessing Screenshot for Attacker No.21

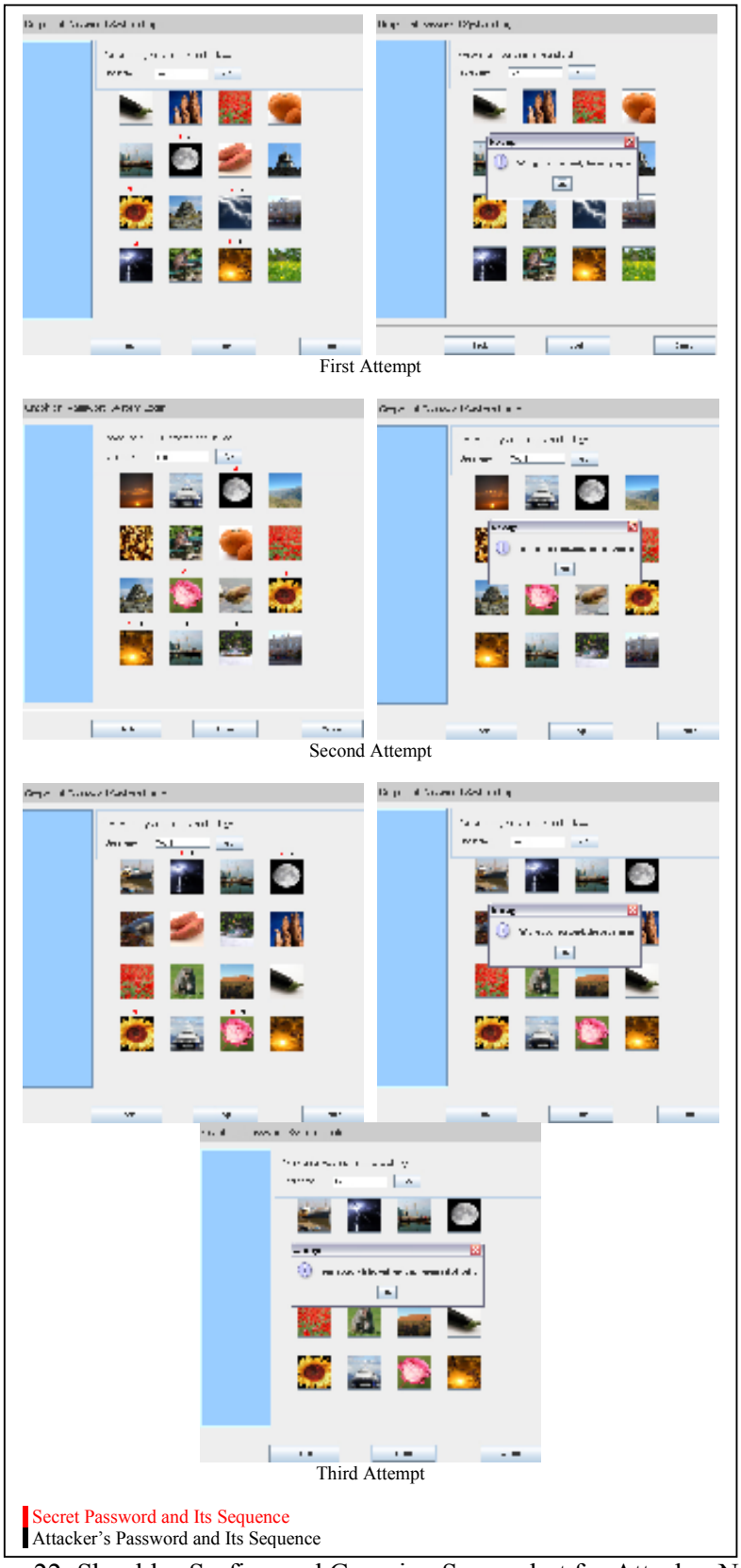


Figure 22: Shoulder-Surfing and Guessing Screenshot for Attacker No.22

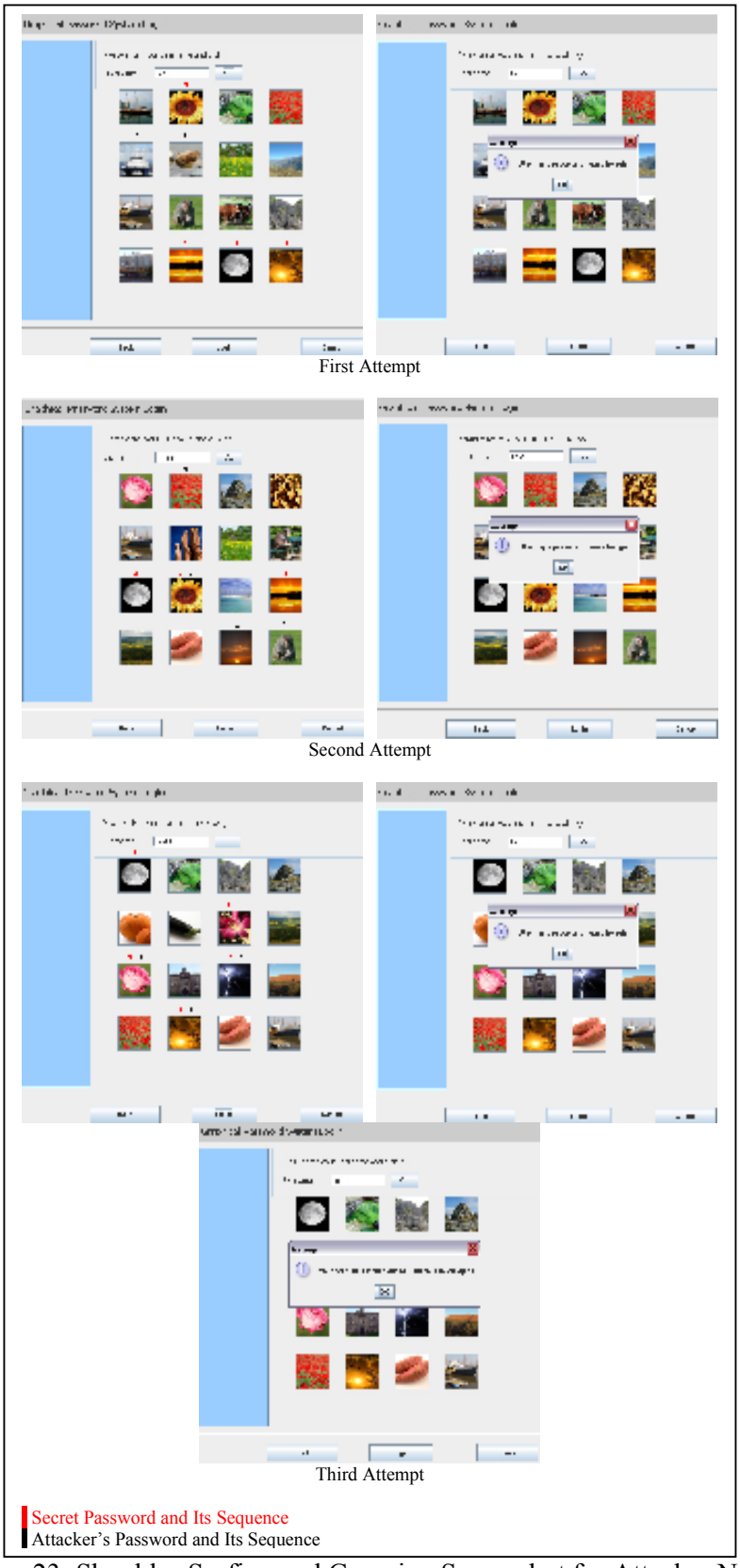


Figure 23: Shoulder-Surfing and Guessing Screenshot for Attacker No.23

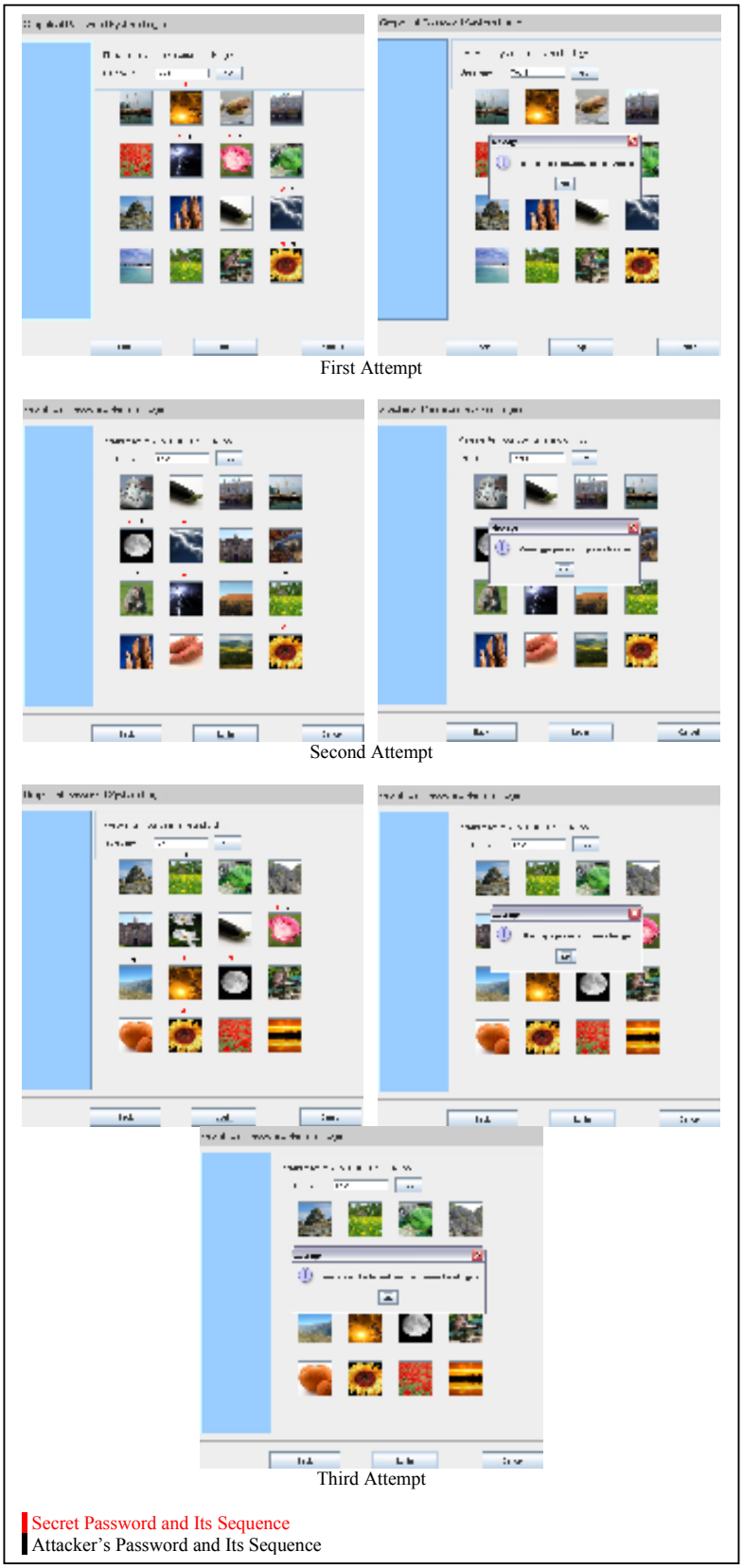


Figure 24: Shoulder-Surfing and Guessing Screenshot for Attacker No.24

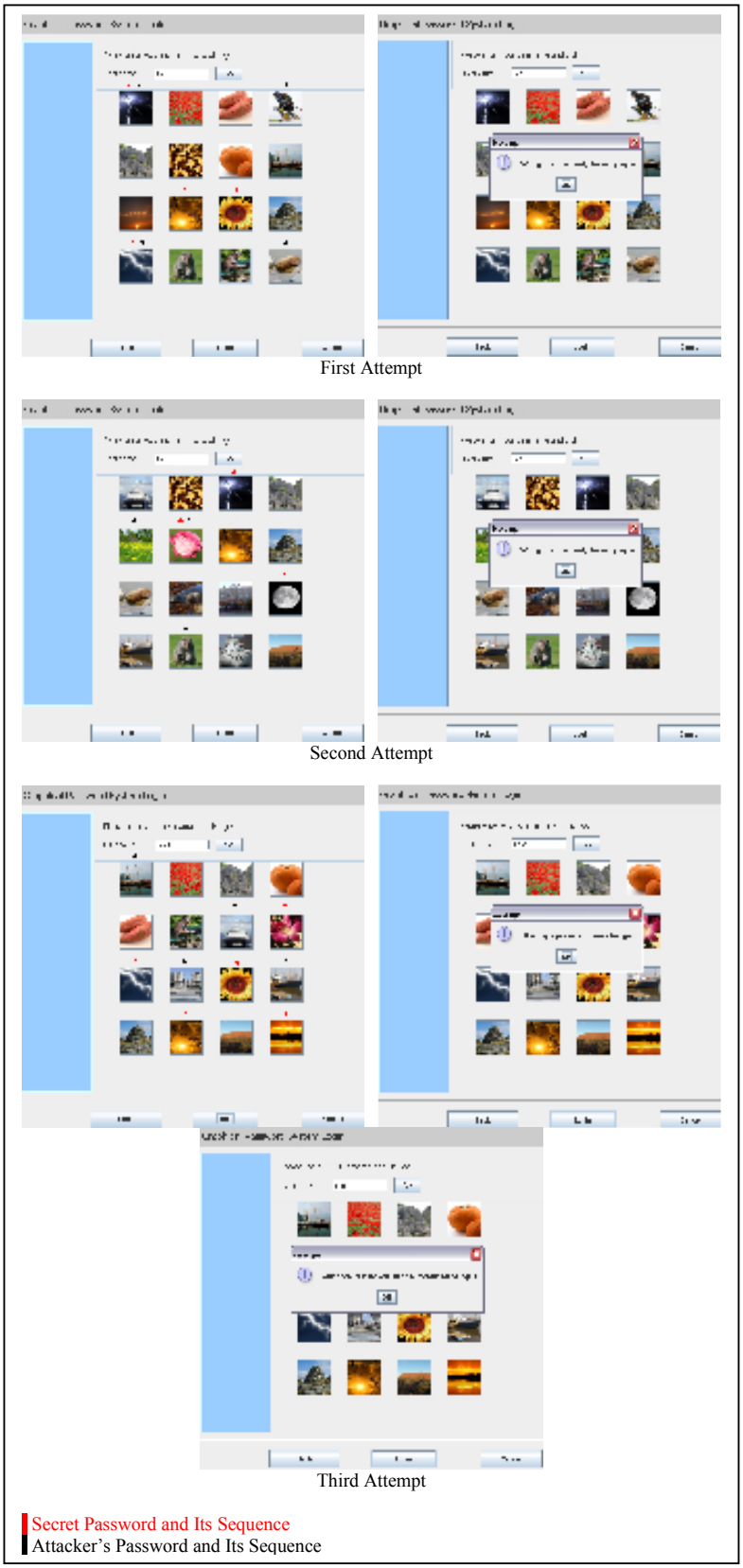


Figure 25: Shoulder-Surfing and Guessing Screenshot for Attacker No.25

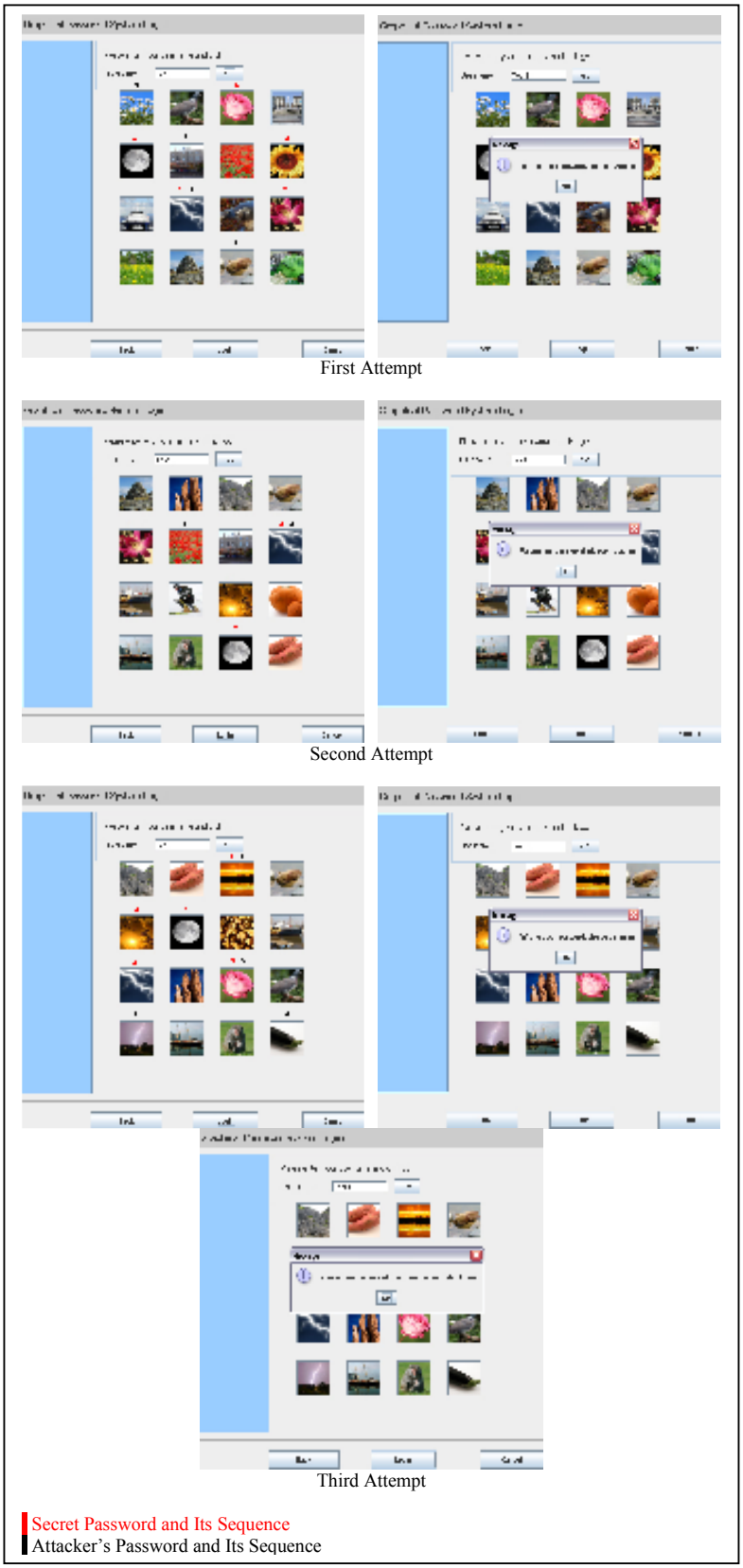
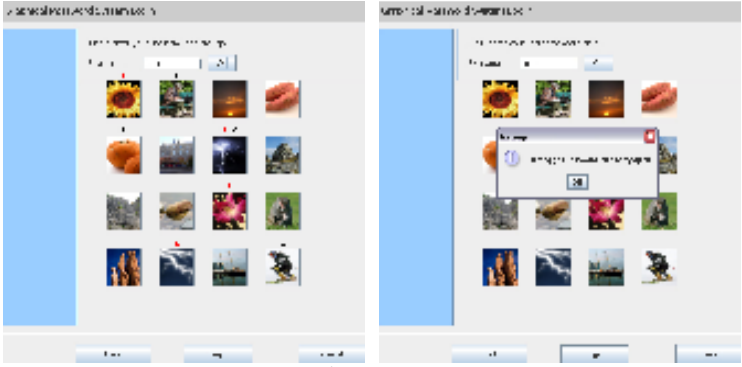
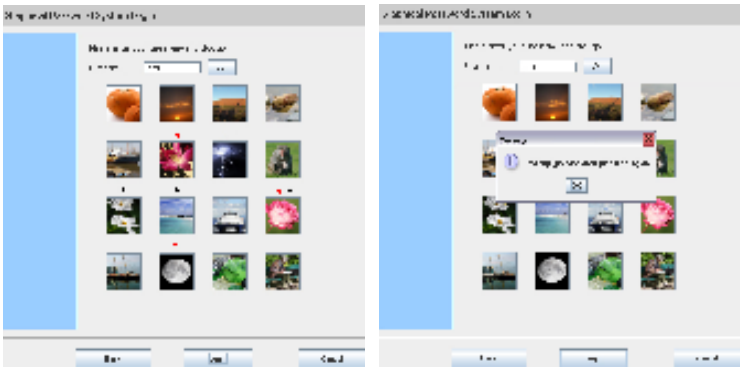


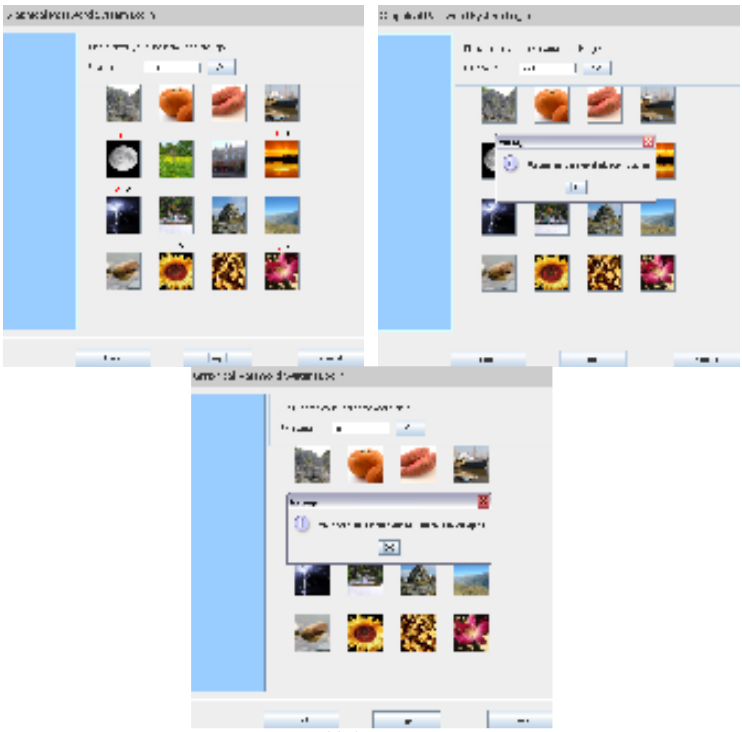
Figure 26: Shoulder-Surfing and Guessing Screenshot for Attacker No.26



First Attempt



Second Attempt



Third Attempt

Secret Password and Its Sequence
Attacker's Password and Its Sequence

Figure 27: Shoulder-Surfing and Guessing Screenshot for Attacker No.27

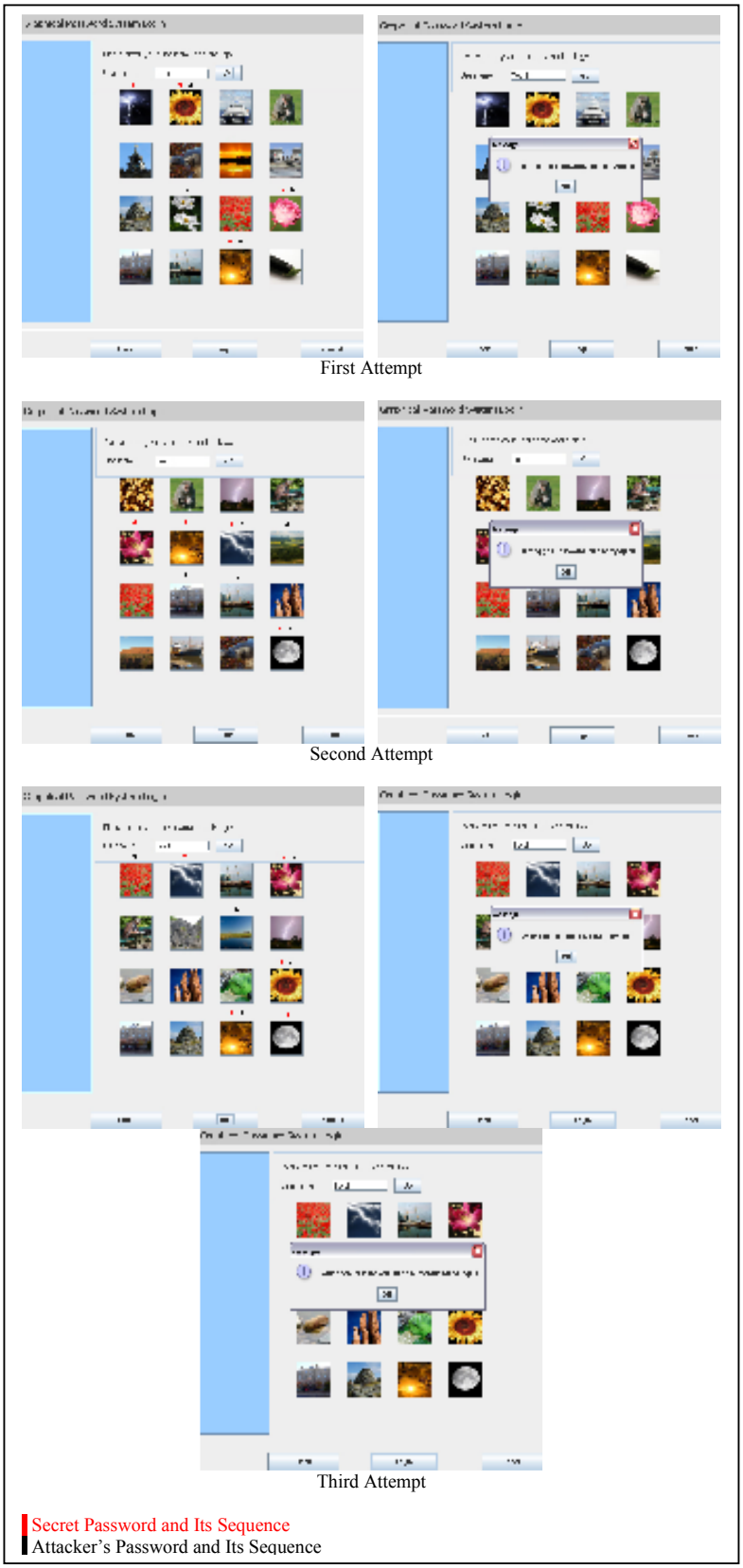


Figure 28: Shoulder-Surfing and Guessing Screenshot for Attacker No.28

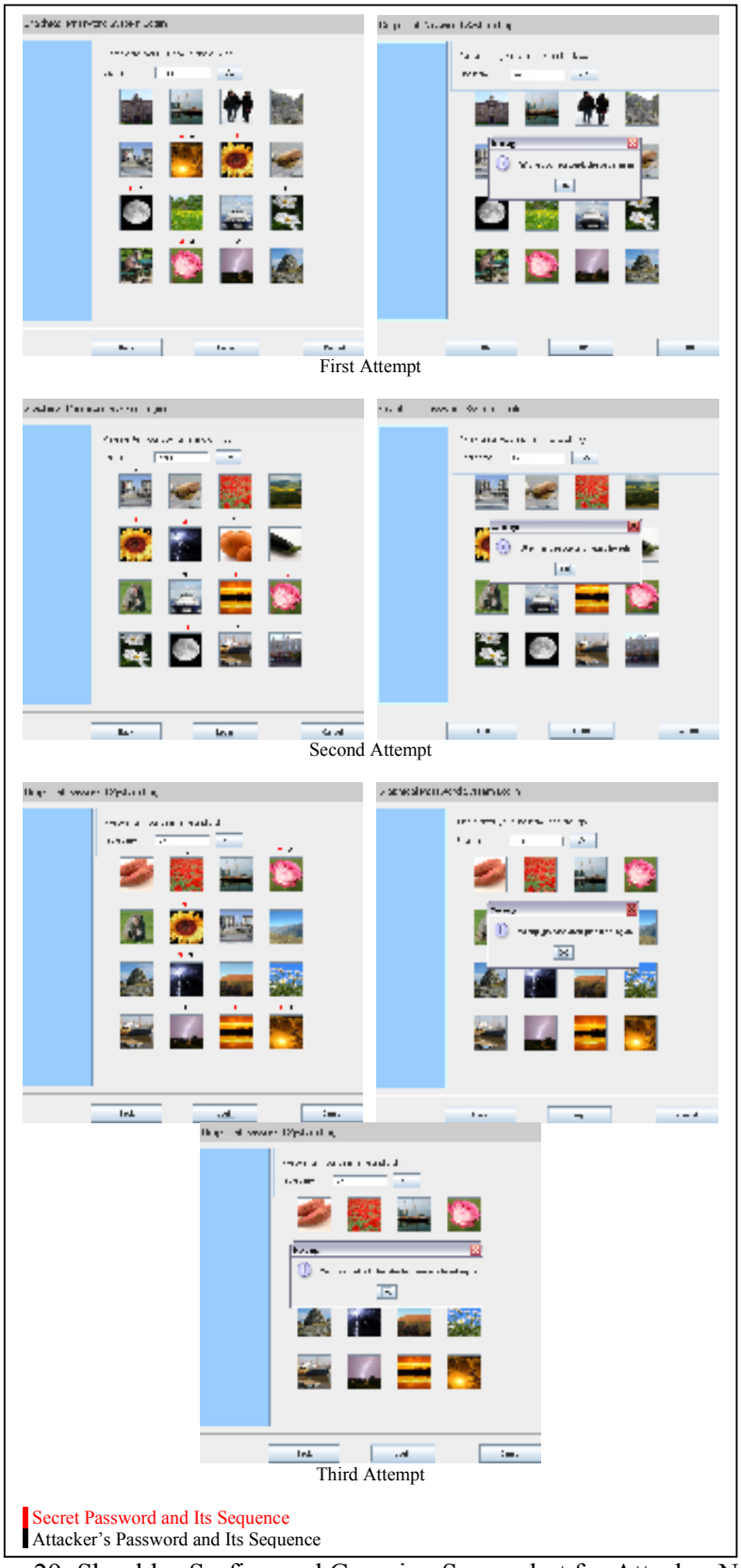


Figure 29: Shoulder-Surfing and Guessing Screenshot for Attacker No.29

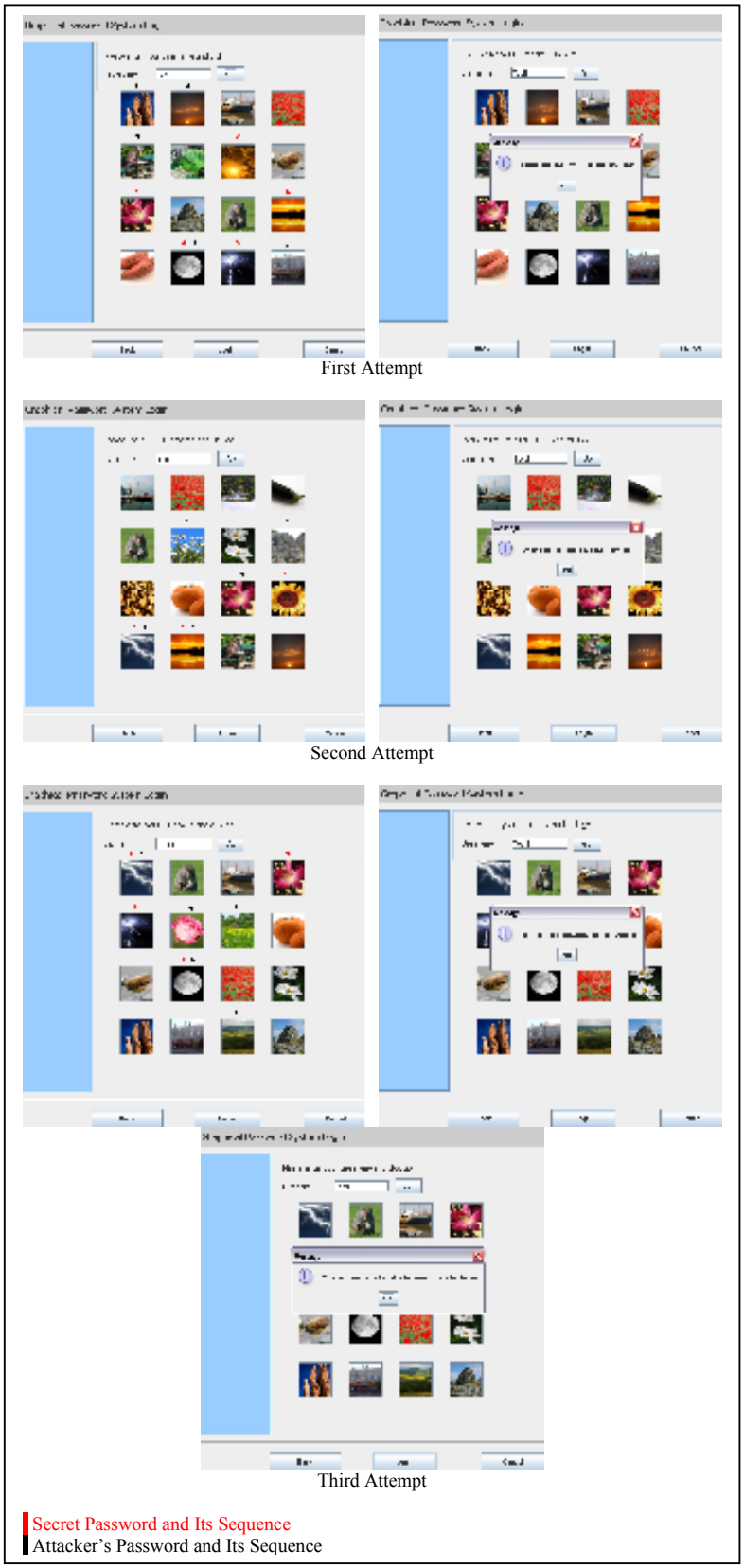


Figure 30: Shoulder-Surfing and Guessing Screenshot for Attacker No.30

Table E1: Analysis and Observation Results

No. of Attackers	No. of Attempts	Shoulder-Surfing And Guessing Result	Attacking Method
1	1	FAIL	based on demonstrated password pictures and redundant pictures
	2	FAIL	based on demonstrated password pictures and their categories
	3	FAIL	based on demonstrated password pictures and their categories
2	1	FAIL	based on demonstrated password pictures and their categories
	2	FAIL	based on demonstrated password pictures and similarity concept such as colour, shape, category
	3	FAIL	based on demonstrated password pictures and redundant pictures
3	1	FAIL	key logging
	2	FAIL	based on demonstrated password pictures and redundant pictures
	3	FAIL	based on demonstrated password pictures and redundant pictures
4	1	FAIL	based on demonstrated password pictures and flowers
	2	FAIL	based on demonstrated password pictures, flowers and new pictures
	3	FAIL	based on demonstrated password pictures, flowers and redundant pictures
5	1	FAIL	key logging
	2	FAIL	based on demonstrated password pictures and similarity concept such as colour, shape, category
	3	FAIL	based on demonstrated password pictures and random
6	1	FAIL	based on demonstrated password pictures and similarity concept such as colour, shape, category
	2	FAIL	based on demonstrated password pictures and flowers
	3	FAIL	key logging
7	1	FAIL	key logging
	2	FAIL	based on demonstrated password pictures and flowers
	3	FAIL	based on demonstrated password pictures, flowers and new pictures
8	1	FAIL	based on demonstrated password pictures
	2	FAIL	based on demonstrated password pictures and similarity concept such as colour, shape, category
	3	FAIL	based on demonstrated password pictures, similarity concept such as colour, shape, category and redundant pictures
9	1	FAIL	key logging
	2	FAIL	based on demonstrated password pictures and similarity concept such as colour, shape, category
	3	FAIL	based on demonstrated password pictures and similarity concept such as colour, shape, category
10	1	FAIL	key logging
	2	FAIL	key logging with larger shape
	3	FAIL	based on demonstrated password pictures and similarity concept such as colour, shape, category
11	1	FAIL	based on demonstrated password pictures and random
	2	FAIL	based on demonstrated password pictures and new pictures
	3	FAIL	based on demonstrated password pictures and similarity concept such as colour, shape, category
12	1	FAIL	based on demonstrated password pictures
	2	FAIL	based on demonstrated password pictures and similarity concept such as colour, shape, category
	3	FAIL	key logging
13	1	FAIL	based on demonstrated password pictures and similarity concept such as colour, shape, category
	2	FAIL	based on demonstrated password pictures and new pictures
	3	FAIL	based on demonstrated password pictures and redundant pictures
14	1	FAIL	key logging
	2	FAIL	based on demonstrated password pictures and redundant pictures
	3	FAIL	based on demonstrated password pictures and redundant pictures
15	1	FAIL	based on demonstrated password pictures and similarity concept such as colour, shape, category
	2	FAIL	based on demonstrated password pictures, similarity concept such as colour, shape, category and new pictures
	3	FAIL	based on demonstrated password pictures, similarity concept such as colour, shape, category and redundant pictures

Table E1: Analysis and Observation Results (continued)

No. of Attackers	No. of Attempts	Shoulder-Surfing And Guessing Result	Attacking Method
16	1	FAIL	key logging
	2	FAIL	based on demonstrated password pictures and similarity concept such as colour, shape, category
	3	FAIL	based on demonstrated password pictures and similarity concept such as colour, shape, category
17	1	FAIL	key logging
	2	FAIL	based on new pictures and flower category
	3	FAIL	based on thunders and flowers categories
18	1	FAIL	based on demonstrated password pictures
	2	FAIL	based on demonstrated password pictures and similarity concept such as colour, shape, category
	3	FAIL	random
19	1	FAIL	key logging
	2	FAIL	based on demonstrated password pictures and redundant pictures
	3	FAIL	based on demonstrated password pictures and redundant pictures
20	1	FAIL	key logging
	2	FAIL	based on demonstrated password pictures and similarity concept such as colour, shape, category
	3	FAIL	based on demonstrated password pictures and similarity concept such as colour, shape, category
21	1	FAIL	based on demonstrated password pictures and their categories
	2	FAIL	key logging
	3	FAIL	based on demonstrated password pictures and similarity concept such as colour, shape, category
22	1	FAIL	based on demonstrated password pictures
	2	FAIL	key logging
	3	FAIL	based on demonstrated password pictures and similarity concept such as colour, shape, category
23	1	FAIL	key logging
	2	FAIL	based on demonstrated password pictures and redundant pictures
	3	FAIL	based on demonstrated password pictures and redundant pictures
24	1	FAIL	based on demonstrated password pictures and similarity concept such as colour, shape, category
	2	FAIL	key logging
	3	FAIL	based on demonstrated password pictures & new pictures
25	1	FAIL	key logging
	2	FAIL	based on redundant pictures
	3	FAIL	based on plain background
26	1	FAIL	key logging
	2	FAIL	based on demonstrated password pictures and their categories & shapes
	3	FAIL	based on demonstrated password pictures and redundant pictures
27	1	FAIL	key logging
	2	FAIL	based on demonstrated password pictures and their categories & shapes
	3	FAIL	based on demonstrated password pictures and their categories & shapes
28	1	FAIL	based on demonstrated password pictures and their categories & shapes
	2	FAIL	key logging
	3	FAIL	based on demonstrated password pictures and their categories
29	1	FAIL	based on demonstrated password pictures and their categories
	2	FAIL	key logging
	3	FAIL	based on demonstrated password pictures and their categories
30	1	FAIL	key logging
	2	FAIL	based on demonstrated password pictures and redundant pictures
	3	FAIL	based on demonstrated password pictures and their categories

Appendix G

Table F1: Case Study Observation Results and Analysis

Attempt	Group No	Password Encoding Produced by the BPG System	Description/Observation Result
-	-	**UserName:**testing2 **Password:** {(3,5,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])}{(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])} **Password Hashing value:** bbd063a23bb6c1b4b927955888e2758a	The password for testing2 consists of two penup events. The first penup occurred at the following indicators: (3,5,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0]) The second penup event occurred at the following indicators: (6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0]) The line indicator is a direct connection from (3,5,[0,0,0]) to (5,7,[0,0,0]) without going through the nearest neighbouring cell (4,6,[0,0,0]).
First Second Third	2, 3, 5, 10, 11, 14, 15, 18, 19 1, 4, 8, 14, 15, 18, 19 13, 16	**UserName:testing2** **Password:** {(3,5,[0,0,0])(4,6,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])} **Password Hashing value:** c7aa8da023508e92b34cbfd89423512d **Percentage Matches:** 91%	The shoulder-surfing attackers failed to login although they have produced the same password drawing. Reason of failure: The shoulder-surfing attackers used one penup event to produce the password. Correct password first penup encoding: {(3,5,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])} second penup encoding: {(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])} Attacker's password {(3,5,[0,0,0])(4,6,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])} Group no. 1, 4, 8, 13 14, 15, 16, 18 and 19 failed to login although hints for the BPG connectivity and penup event were notified after the first failure of logging in. Group no. 14, 15, 18, 19 produced the same password encoding twice in the first two attempts. Group no. 13 and 16 failed to login in the third attempt although the importance of using the correct BPG connectivity and penup event were notified after the first two failure of logging in.
First Second Third	6, 12, 13, 16, 17, 20 - 4	**UserName:testing2** **Password:** {(3,5,[0,0,0])(4,6,[0,0,0])}{(4,6,[0,0,0])(5,7,[0,0,0])}{(5,7,[0,0,0])(6,5,[0,0,0])}{(6,5,[0,0,0])(5,4,[0,0,0])}{(5,4,[0,0,0])(4,3,[0,0,0])}{(4,3,[0,0,0])(3,5,[0,0,0])} **Password Hashing value:** 8d377dd68e62ed69e8e70348458781e0 **Percentage Matches:** 58%	The shoulder-surfing attackers failed to login although they have produced the same password drawing. Reason of failure: The shoulder-surfing attackers (Group no. 4, 6, 12, 13, 16, 17 and 20) used six penup event to produce the password. Correct password first penup encoding: {(3,5,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])} second penup encoding: {(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])} Attacker's password first penup encoding: {(3,5,[0,0,0])(4,6,[0,0,0])} second penup encoding: {(4,6,[0,0,0])(5,7,[0,0,0])} third penup encoding: {(5,7,[0,0,0])(6,5,[0,0,0])} forth penup encoding: {(6,5,[0,0,0])(5,4,[0,0,0])} fifth penup encoding: {(5,4,[0,0,0])(4,3,[0,0,0])} sixth penup encoding: {(4,3,[0,0,0])(3,5,[0,0,0])}

Table F1: Case Study Observation Results and Analysis (continue)

Attempt	Group No	Password Encoding Produced by the BPG System	Description/Observation Result
First	1, 8	**UserName:testing2** **Password:** {(3,5,[0,0,0])(4,6,[0,0,0])(5,7,[0,0,0])}{(5,7,[0,0,0])(6,5,[0,0,0])}{(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])}{(4,3,[0,0,0])(3,5,[0,0,0])}	The shoulder-surfing attackers failed to login although they had produced the same password drawing. Reason of failure: The shoulder-surfing attackers used four penup events to produce the password. Group no. 1 and 8 failed to login in the first attempt.
Second	11	**Password Hashing value:** 428489767a29b6eb5e5042fdabaf8596 **Percentage Matches:** 70%	Group no. 11 failed to login in the second attempt although suggestions about the connectivity and penup event were notified after the first failure of logging in. Group no. 4, 6, 8 and 19 failed to login in the third attempt although the importance of using the correct BPG connectivity and penup event were notified after the first two failure of logging in.
Third	4, 6, 8, 19		Correct password first penup encoding: {(3,5,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])} second penup encoding: {(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])} Attacker's password first penup encoding: {(3,5,[0,0,0])(4,6,[0,0,0])(5,7,[0,0,0])} second penup encoding: {(5,7,[0,0,0])(6,5,[0,0,0])} third penup encoding: {(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])} forth penup encoding: {(4,3,[0,0,0])(3,5,[0,0,0])}
First	7, 9	**UserName:testing2** **Password:** {(3,5,[0,0,0])(4,6,[0,0,0])(5,7,[0,0,0])}{(5,7,[0,0,0])(6,5,[0,0,0])}{(6,5,[0,0,0])(5,4,[0,0,0])}{(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])}	The shoulder-surfing attackers failed to login although they had produced the same password drawing. Reason of failure: The shoulder-surfing attackers used four penup events to produce the password. Group no. 7 and 9 failed to login in the first attempt.
Second	10, 12	**Password Hashing value:** 54d107ea1a320b2a54f8c97179c93935 **Percentage Matches:** 70%	Group no. 10 and 12 failed to login in the second attempt although suggestions about the connectivity and penup event were notified after the first failure of logging in. Group no. 20 failed to login in the third attempt although the importance of using the correct BPG connectivity and penup event were notified after the first two failure of logging in.
Third	20		Correct password first penup encoding: {(3,5,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])} second penup encoding: {(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])} Attacker's password first penup encoding: {(3,5,[0,0,0])(4,6,[0,0,0])(5,7,[0,0,0])} second penup encoding: {(5,7,[0,0,0])(6,5,[0,0,0])} third penup encoding: {(6,5,[0,0,0])(5,4,[0,0,0])} forth penup encoding: {(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])}

Table F1: Case Study Observation Results and Analysis (continue)

Attempt	Group No	Password Encoding Produced by the BPG System	Description/Observation Result
First	-	**UserName:testing2** **Password:** {(3,5,[0,0,0])(4,6,[0,0,0])}{(4,6,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])}{(6,5,[0,0,0])(5,4,[0,0,0])}{(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])} **Password Hashing value:** 27b70a32fda5450bbae215eb1818339a **Percentage Matches:** 70%	The shoulder-surfing attackers failed to login although they had produced the same password drawing. Reason of failure: The shoulder-surfing attackers used four penup events to produce the password. Group no. 9 and 2 failed to login in the second and third attempt respectively although suggestions and the importance of using the correct connectivity and penup event were notified after the after the first failure of logging in. Correct password first penup encoding: {(3,5,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])} second penup encoding: {(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])} Attacker's password first penup encoding: {(3,5,[0,0,0])(4,6,[0,0,0])} second penup encoding: {(4,6,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])} third penup encoding: {(6,5,[0,0,0])(5,4,[0,0,0])} forth penup encoding: {(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])}
Second	9		
Third	2		
First	-	**UserName:testing2** **Password:** {(3,5,[0,0,0])(5,7,[0,0,0])}{(5,7,[0,0,0])(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])}{(4,3,[0,0,0])(3,5,[0,0,0])} **Password Hashing value:** 72b850a2ca673cbf15620e808e7a8808 **Percentage Matches:** 85%	The shoulder-surfing attackers failed to login although they had produced the same password drawing. Reason of failure: The shoulder-surfing attackers used three penup events to produce the password. Group no. 6 and 9 failed to login in the second and third attempt respectively although suggestions and the importance of using the correct connectivity and penup event were notified after the after the first failure of logging in. Correct password first penup encoding: {(3,5,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])} second penup encoding: {(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])} Attacker's password first penup encoding: {(3,5,[0,0,0])(5,7,[0,0,0])} second penup encoding: {(5,7,[0,0,0])(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])} third penup encoding: {(4,3,[0,0,0])(3,5,[0,0,0])}
Second	6		
Third	9		

Table F1: Case Study Observation Results and Analysis (continue)

Attempt	Group No	Password Encoding Produced by the BPG System	Description/Observation Result
First	-	**UserName:testing2** **Password:** {(3,4,[0,0,0])(5,6,[0,0,0])(6,4,[0,0,0])(5,3,[0,0,0])(4,2,[0,0,0])}{(4,2,[0,0,0])(3,4,[0,0,0])} **Password Hashing value:** bb5b292437763d7f297199dd624915fc **Percentage Matches:** 80%	The shoulder-surfing attackers failed to login although they had produced the same password drawing. Reason of failure: The shoulder-surfing attackers used two penup events. However, the connectivity among the indicators within the first and the second penup events were wrongly identified.
Second	20		Group no. 20 failed to login in the second attempt although suggestions about the connectivity and penup event were notified after the first failure of logging in.
Third	1, 3, 12, 18		Group no. 1, 3, 12, and 18 failed to login in the third attempt although the importance of using the correct BPG connectivity and penup event were notified after the first failure of logging in. Correct password first penup encoding: {(3,5,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])} second penup encoding: {(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])} Attacker's password first penup encoding: {(3,4,[0,0,0])(5,6,[0,0,0])(6,4,[0,0,0])(5,3,[0,0,0])(4,2,[0,0,0])} second penup encoding: {(4,2,[0,0,0])(3,4,[0,0,0])}
First	-	**UserName:testing2** **Password:** {(3,5,[0,0,0])(4,6,[0,0,0])(5,7,[0,0,0])}{(5,7,[0,0,0])(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])} **Password Hashing value:** 7d5093ee8b39c7266138494e4bd1ea41 **Percentage Matches:** 85%	The shoulder-surfing attackers failed to login although they had produced the same password drawing. Reason of failure: The shoulder-surfing attackers used two penup events. However, the connectivity among the indicators within the first and the second penup events were wrongly identified.
Second	7, 16, 17		Group no. 7, 16 and 17 failed to login in the second attempt although hints were given.
Third	5, 11		Group no. 5 and 11 failed to login in the third attempt although hints were provided. Correct password first penup encoding: {(3,5,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])} second penup encoding: {(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])} Attacker's password first penup encoding: {(3,5,[0,0,0])(4,6,[0,0,0])(5,7,[0,0,0])} second penup encoding: {(5,7,[0,0,0])(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])}

Table F1: Case Study Observation Results and Analysis (continue)

Attempt	Group No	Password Encoding Produced by the BPG System	Description/Observation Result
First	-	**UserName:testing2** **Password:** {(3,5,[0,0,0])(4,6,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])}{(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])}{(4,3,[0,0,0])(3,5,[0,0,0])} **Password Hashing value:** b6487c69dcef0762ff84f3626bf01a9c **Percentage Matches:** 77%	The shoulder-surfing attackers failed to login although they had produced the same password drawing. Reason of failure: The shoulder-surfing attackers used three penup events. Group no. 13 failed to login in the second attempt although hints were given.
Second	13		Group no. 7 and 10 failed to login in the third attempt although hints were provided. Correct password first penup encoding: {(3,5,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])}
Third	7, 10		second penup encoding: {(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])} Attacker's password first penup encoding: {(3,5,[0,0,0])(4,6,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])} second penup encoding: {(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])} third penup encoding: {(4,3,[0,0,0])(3,5,[0,0,0])}
First	-	**UserName:testing2** **Password:** {(3,5,[0,0,0])(4,6,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])}{(4,3,[0,0,0])(3,5,[0,0,0])} **Password Hashing value:** 70b8a93c71a9e660ed032f6f83779717 **Percentage Matches:** 82%	The shoulder-surfing attackers failed to login although they had produced the same password drawing. Reason of failure: The shoulder-surfing attackers used two penup events. However, the connectivity among the indicators within the first and second penup events were wrongly identified.
Second	3, 5		Group no. 3 and 5 failed to login in the third attempt although hints were given. Group no. 15 and 17 failed to login in the third attempt although clues were provided. Correct password first penup encoding: {(3,5,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])}
Third	15, 17		second penup encoding: {(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])} Attacker's password first penup encoding: {(3,5,[0,0,0])(4,6,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])} second penup encoding: {(4,3,[0,0,0])(3,5,[0,0,0])}

Table F1: Case Study Observation Results and Analysis (continue)

Attempt	Group No	Password Encoding Produced by the BPG System	Description/Observation Result
First	-	**UserName:testing2** **Password:** {(3,5,[0,0,0])(4,6,[0,0,0])} {(4,6,[0,0,0])(5,7,[0,0,0])} {(5,7,[0,0,0])(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])} **Password Hashing value:** bb68ec1a2f4864c7b969fa6874ea504c **Percentage Matches:** 75%	The shoulder-surfing attackers failed to login although they had produced the same password drawing. Reason of failure: The shoulder-surfing attackers used three penup events. Group no. 2 failed to login in the second attempt although hints were given.
Second	2		Correct password first penup encoding: {(3,5,[0,0,0])(5,7,[0,0,0])(6,5,[0,0,0])} second penup encoding: {(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])}
Third	-		Attacker's password first penup encoding: {(3,5,[0,0,0])(4,6,[0,0,0])} second penup encoding: {(4,6,[0,0,0])(5,7,[0,0,0])} third penup encoding: {(5,7,[0,0,0])(6,5,[0,0,0])(5,4,[0,0,0])(4,3,[0,0,0])(3,5,[0,0,0])}