Frequency of Occurrence Analysis Attack and its Countermeasure

Lip Yee Por
Faculty of Computer Science and Information Technology, University of Malaya, Malaysia

Abstract: *This paper addresses a newly discovered security threat named Frequency of Occurrence Analysis (FOA) attack in searchmetics password authentication scheme. A countermeasure technique that utilises Metaheuristic Randomisation Algorithm (MRA) is proposed to address the FOA attack. The proposed algorithm is presented and an offline FOA attack simulation tool is developed to verify the effectiveness of the proposed method. In addition, a shoulder surfing testing is conducted to evaluate the effectiveness of the proposed method in terms of mitigating shoulder surfing attack. The experiment results show that MRA is able to prevent FOA and mitigate shoulder surfing attacks. Moreover, the proposed method is able to provide larger password space compare to the benchmarking scheme.*

Keywords: *FOA, MRA, picture-based password, graphical authentication, shoulder surfing.*

Received November 28, 2010; accepted May 24, 2011

1. Introduction

The idea of a picture-based password authentication scheme was pioneered by Greg Blonder who also holds the US patent 5559961 in 1996 [1]. Throughout the years, various picture-based password schemes were proposed to exploit the utility of pictures or images for user authentication. In 2005, De-Angeli *et al*. [5] have proposed a cluster of three categories (locimetrics, drawmetrics and cognometrics) for classifying picture-based password authentication. The cognometrics terminology was being revised to searchmetrics by Renaud and De-Angeli *et al*. [15] in 2009.

According to the authors in [5, 12], a locimetric system is a mnemonic system which enables a user to identify any relevant points or objects with or without the aid of various recalling methods when performing an authentication. In the drawmetric authentication scheme, users are required to draw a preset outline figure on a grid. Subsequently, the position, sequence, as well as the visual appearance of a redrawing, are used as the analysis metrics for users' verification. In searchmetric authentication scheme, users are required to identify the "target" images/icons/symbols (which have been identified by the users during their password creation stage) along with a set of distracter images/icons/symbols for an authorised authentication [7, 12, 15].

Currently, most of the existing picture-based password authentication schemes especially those from searchmetric authentication schemes fail to address a newly discovered threat named Frequency of Occurrence Analysis (FOA) attack. In this context, FOA refers to an approach of identifying the rate of recurrence of a set of picture images generated by a secure system. FOA occurs only in searchmetric picture-based password authentication scheme in which users are required to search a number of secret password pictures used among the other distracter pictures from a challenge set of images. An off-line simulation can be used by an attacker to observe and analyse the frequency of occurrence of a set of generated picture images. Thereafter, the attacker is able to identify the secret password pictures used by a user by increasing the number of iteration of the simulation because the uniform random algorithm used by the searchmetric picture-based password authentication schemes are always prone to select the secret password pictures used compared to the other distracter pictures. Therefore, the secret password pictures will always produce higher frequency of occurrence compared to the other distracter pictures. Once the attacker obtains the secret password pictures used, the attacker can launch password guessing attacks as well as shoulder surfing attacks and gain access as a legitimate user.

In order to alleviate the aforementioned issue, a searchmetric authentication scheme that utilises metaheuristic random algorithm was proposed. The remainder of this paper is organised into the following sections: In section 2, the related work review and analysis is presented. In section 3, the FOA attack is presented. The proposed method is discussed in section 4 and the experimental testing and results analysis are discussed in section 5. The password space analysis and the shoulder surfing testing are presented in sections 6 and 7 respectively. Finally, a conclusion and future work are presented to summarise the deliverables of the proposed method.

2. Related Work

One of the earlier instances where picture-based password uses the searchmetrics mechanism is Passfaces™. Passfaces™ is a commercial product produced by Passfaces Corporation in year 2000. During the password creation phase, each Passfaces™ user is required to select four human face pictures for his/her password portfolio. Throughout the authentication process, one human face picture will be selected from the user portfolio together with eight distracter human face pictures to form a grid of nine human face pictures shown in Figure 1. In order to gain access into a Passfaces™ system, a user is required to click on the correct human face picture in four continuous attempts. In order to increase the security level against the detection of keystroke logging and packet-sniffing attacks, a randomised mechanism has been applied to alter the order of the human face pictures within each grid for each attempt.

Figure 1. Passfaces™ scheme (adopted from [14]).

Based on the users' study survey results obtained at Brostoff *et al.* [2], had drawn a conclusion that Passfaces™ is easier to remember compared to textual passwords. However, based on the literature and empirical study from [3, 10], the Passfaces™ scheme does encounter several limitation and challenges such as:

1. Limited password spaces.
2. Psychology effects and biases which can highly influence a user to choose a predictable password.
3. Unpleasant login session for certain users due to the predefined human face pictures generated by the Passfaces™ system.
4. Face-blind (a disease which affects a person's ability to tell faces apart) problem.

In order to prevent the issues which occurred in Passfaces™ and to alleviate the face-blind problem, Rachna had proposed a scheme named Déjà Vu in year 2000. Déjà Vu is a picture-based recognition password which uses non-describable abstract pictures that are generated on the fly from stored seed values shown in Figure 2. The Déjà Vu scheme consists of three phases: portfolio creation, training and authentication phases. During the portfolio creation phase, a user is required to identify a set of pictures which will be used as the password for the system authentication. After creating a portfolio, the user has to go through a training session to familiarise and improve the memorability of the pictures used. During the authentication phase, a $n_i \times n_j$ (n_i: number of row, n_j: number of column) grid picture-based authentication challenge set which consists of several random pictures from the user's portfolio together with other distracter or decoy pictures chosen from the system will be formed. The user then has to select the pictures that belong to his/her portfolio in order to gain access to the system.

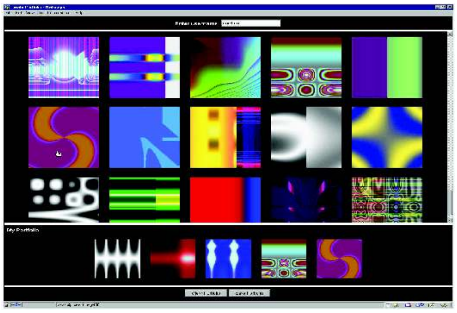
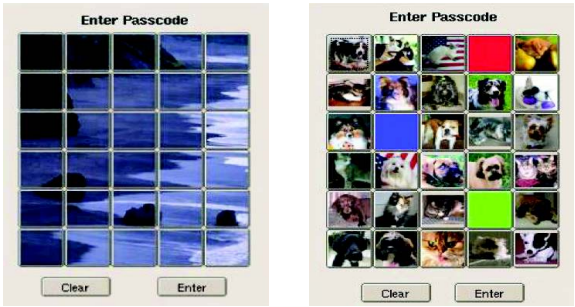


Figure 2. Déjà Vu scheme (adopted from [6]).

However, the seeds storing on the server of the Déjà Vu system is vulnerable to several security threats such as guessing attack and shoulder surfing.

1. There are possibilities that an attacker can launch a brute force attack by trying all combination of picture selections in the challenge set due to the limited password space produced by the Déjà Vu scheme. Moreover.
2. If an attacker knows the user very well, then there is a possibility of the attacker making an educated guess attack on the system by guessing what pictures the user might have in his portfolio [9, 10, 11] Besides.
3. Similar to the Passfaces™ Scheme, the Déjà Vu system has no resistance to shoulder surfing attack. The password used by a user can be easily stolen or obtained by an attacker if the login process has been recorded.



a) Sea and shore theme. b) Cats and dogs theme.

Figure 3. Picture password scheme (adopted from [8]).

Jansen *et al.* [8] had proposed a scheme named picture password in 2003. According to, the picture password scheme is a 5×6 grid picture-based

authentication system designed especially for mobile devices such as PDAs. During the password creation phase, a user is required to identify a sequence of pictures within the three predefined themes such as cats and dogs theme and Sea and shore theme as his/her password shown in Figure 3-a and 3-b. However, according to the authors, the authentication process for the Picture Password scheme is dependent on the need of a system. For instance, a user can be requested to identify his/her password using an eight-entry picture sequence or two pictures in an attempt during the system authentication. The degree of security level solely relies on the system itself. However, the user is still required to recognise and identify the correct pictures and sequence in order to be authenticated.

The picture password scheme is able to enlarge the password space by increasing the grid size used. However, a brute force attack can still be launched and the password used by a user can still be observed and learned by an attacker if the login process has been recorded. As a result, the picture password scheme is still not able to solve the guessing attack and shoulder surfing problems. Besides, the picture password scheme will encounter extra security threat such as keystroke logging attack due to the static and fix location of all the generated pictures used in all attempts.

a) VIP1/VIP 2 Interface. b) VIP3 Interface.

Figure 4. Visual Identification Protocol (VIP) models (adopted from [4]).

De-Angeli *et al*. [4] presented a series of Visual Identification Protocol (VIP) models. The similarity of all VIP series proposed by the authors is that they all use pictorial concept to replace PIN numbers as used in Automatic Teller Machine (ATM) authentication. According to [4], the VIP pictures used can be clustered into nine semantic categories such as flowers, animals, rocks, landscapes, humans, vegetables, buildings, skies, and boats.

In the VIP1 scheme, a user has to select a sequence of four pictures out of ten in the same position at each authentication attempt. For every authentication attempt, the pictures from the user's selected categories and a new set of distracter pictures will be extracted from the visual database. For obtaining an authorised authentication, the user has to identify the correct picture within three attempts which is identical to that of a normal ATM transaction. However, for all authentication processes, no reshuffling of pictures and relocation is done. As a result, the VIP1 scheme is vulnerable to keystroke logging attack as in the picture password scheme.

The VIP2 scheme differs from the VIP1 scheme in that the four pictures forming the authentication code were displayed in random positions around the visual keypad at the beginning of each authentication attempt [5]. However, according to [5], in order not to disclose any clue about the authentication code, the same visual configuration will be displayed if an invalid authentication has been detected. Refer to Figure 4-a for the VIP1 and VIP2 graphical user interfaces.

The VIP3 scheme uses different mechanism in password identification and generation. A user is required to create a portfolio that has eight pictures selected from the nine predefined semantic categories in the first place. However, to prevent replication of the categories of the code items displayed in the current challenge set, only four pictures from the portfolio will be randomly used together with another 12 distracter pictures which will be selected randomly from the remaining categories as to form a 4×4 grid cells picture-based authentication system shown in Figure 4-b. To avoid unnecessary disclosure of the authentication code, the same visual configuration will be displayed if an invalid authentication has been detected. On the other hand, a user is required to identify the four pictures used from the portfolio in the correct sequence before he/she can gain access to the system.

The authors from [5] claimed that all the VIP series presented is able to increase the ease of memorising passwords for users. However, those VIP series presented by the authors are still opened to guessing attack due to the small password space used in the VIP1, VIP2 and VIP3 schemes. Nevertheless, the VIP2 and VIP3 schemes are able to improve the keystroke logging attack by using the random positions and random picture selections from a user's portfolio mentioned earlier. Due to the four-choose-eight password selection mechanism used, the VIP3 scheme is able to secure the password used by a user from an attacker although the login processes have been recorded. As a result, the VIP3 scheme has better shoulder surfing prevention compared to the other two schemes. Nevertheless, the shoulder surfing issue cannot be totally resolved due to the fact that the VIP3 is exposed to Frequency of Occurrence Analysis (FOA) attack.

3. FOA Attack

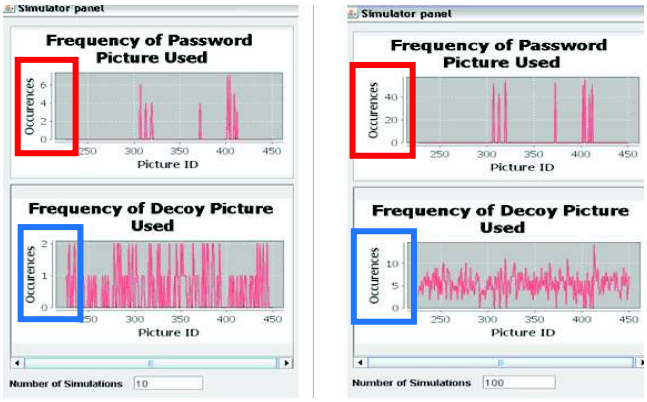
FOA occurs when uniform random algorithm is used to select both secret password pictures and the other distracter pictures to form a challenge set. To illustrate FOA attack, an offline FOA attack simulation tool was

developed using JAVA programming. The algorithm used by VIP3 has been modelled and used as an instance to demonstrate the FOA attack. From the simulation result shown in Figure 5, the secret password pictures created by the user can be identified easily because the secret password pictures produce obvious peaks compared to the other distracter pictures. As a result, a shoulder surfer can apply an educated guess based on the highest frequency of occurrence of the selected pictures when attacking. Therefore, to alleviate the aforementioned issue, a proposed scheme that utilises a metaheuristic random algorithm to reselect the old distracter pictures in the previous challenge set was proposed.

Table 1. Synthesis result.

Searchmetric Authentication Scheme	Password Space	Robustness to	
		Shoulder Surfing	FOA
Passfaces™	• Generic Password Space: N^K [16] N is the total number of pictures generated at each round, K is the number of attempts.	×	×
Déjà Vu	• Generic Password Space: $\frac{N!}{K!(N-K)!}$ [16] N is the total number of pictures generated at each round, K is the number of password pictures used during an authentication process.	×	×
Picture Password	• Generic Password Space: $\left(\frac{N!}{K!(N-K)!}\right)^J$ N is the total number of pictures generated at each round, K is the number of password pictures used during an authentication process, J is the number of attempts.	×	×
VIP1	• Generic Password Space: N^K N is the total number of pictures generated at each round, K is the length of the password.	×	×
VIP2	• Same as in VIP1	×	×
VIP3	• Generic Password Space: $\frac{N!}{K!(N-K)!}$ N is the total number of pictures generated at each round, K is the number of selected password pictures.	×	×
Proposed Scheme	• Generic Password Space: $\frac{N!}{K!(N-K)!}$ N is the total number of pictures generated at each round, K is the number of selected password pictures. • Lager password space compared to VIP3	√	√

SS: Shoulder Surfing Attack
FOA: Frequency of Occurrence Analysis
× : vulnerable to
√ : invulnerable to
N/A : Not Applicable



a) 10 Iteration simulation. b) 100 Iteration simulation.

Figure 5. Offline FOA attack simulation and its observation result for VIP3.

The secret password pictures used have higher occurrence compared to the other distracter pictures in Figure 5-a. The result is more obvious when the number of iteration increases as shown in Figure 5-b.

Table 1 summarises the synthesis results for the searchmetric research. From the Table, it shows that none of the reviewed schemes are able to resist FOA and shoulder surfing attacks.

4. Proposed Method

As mentioned in the previous section, FOA occurs due to the uniform random Algorithm used by the searchmetric picture-based password authentication schemes which has the tendency of selecting the secret password pictures identified by a user compared to the other distracter pictures. To retain the randomness of selecting a secret password, uniform random Algorithm is still adapted in the proposed method. However, the idea of reselecting the old distracter pictures in the previous challenge set was proposed to increase the likelihood of those selected distracter pictures being selected again to overcome FOA attack. As a proof of concept, the proposed method is implemented on top of VIP3 to verify its basic performance.

The proposed scheme consists of two main modules such as portfolio creation module and user authentication module. Before an authentication takes place, a user is required to register a set of secret password pictures, $X \in x_1, x_2, x_3 \ldots x_{|X|}$, from the predefined categories within the significant interval of $8 \leq |X| \leq 16$. After the user has identified and registered the secret password pictures, the user is able to gain access into the proposed system using the user authentication module. Once the authentication module has been initiated, a uniform random Algorithm is used to select a set of partial secret password pictures, $J \in j_1, j_2, j_3 \ldots j_{|J|}$, from X where $4 \leq |J| \leq 5$.

If a user fails to identify his/her password in the first attempt, the uniform random Algorithm will be used to select a brand new set of partial secret password,

$J_{new} \in j_1, j_2, j_3 \ldots j_{|J_{new}|}$, from X where $4 \leq |J_{new}| \leq 5$. After that, the proposed metaheuristic random Algorithm will be used to randomly identify and reuse a set of decoy pictures which have been used in the previous attempt based on the determined distribution range. Finally, the remaining pictures will be filled by a set of new decoy pictures which are identified from the remaining sampling pool. In general, the total pictures produced in the second attempt can be denoted as the summation of J_{new} secret passwords, $P_A(k)$ of decoy pictures from the previous attempt and $P_B(N-|X|-k)$ new decoy pictures from the remaining sampling pool, where N is the total sample pictures used in the sampling pool, k is the number of decoy pictures used in the previous attempt, P_A is the probability of decoy pictures used in the previous attempt and it has the MRA distribution range of $\overset{j_{4..5}}{R_4} - \overset{j_{4..5}}{R_7}$ and P_B is the probability of new decoy pictures with $P_B=1-P_A$. (The definition of MRA distribution range notation, $\overset{j_{n..m}}{R_i}$, can be obtained in the following section).

If the user was unable to identify his secret passwords in two continuous attempts, the same proposed mechanism will be used to select the secret password and decoy password pictures. Similarly, a brand new set of secret passwords, J_{new}, will be identified using the uniform random Algorithm. Then, the metaheuristic random Algorithm will randomly identify and reuse the decoy pictures which have been generated in the second attempt followed by a brand new set of decoy pictures which are identified from the remaining sampling pool. The total pictures produced in the third trial can be denoted as the summation of J_{new} secret passwords, $P_A(P_A(k)+P_B(N-|X|-k))$ of decoy pictures from the second attempt and $P_B(N-|X|-(P_A(k)+P_B(N-|X|-k)))$ new decoy pictures from the remaining sampling pool, where P_A and P_B have the probability MRA distribution range of $\overset{j_{4..5}}{R_4} - \overset{j_{4..5}}{R_7}$ and $\overset{j_{4..5}}{R_3} - \overset{j_{4..5}}{R_6}$ respectively.

5. Testing and Result Discussion

This section discusses the parameters used in the proposed method together with the testing results and its result discussion. In general it can be represented as follows:

- *Step 1:* $|X|$ secret password interval determination.
- *Step 2:* $|J|$ secret password interval determination.
- *Step 3:* MRA distribution range determination.

Initially it begins with the determination of the number of secret password pictures used, $X \in x_1, x_2, x_3 \ldots x_{|X|}$, via the comparison of the permutation results produced by each value of X with the benchmark scheme. Next, the range of the partial secret password pictures, $J \in j_1, j_2, j_3 \ldots j_{|J|}$, is identified using an offline FOA simulation. The value of j is only considered usable if the secret password pictures do not produced higher frequency of occurrence compared to the other distracter pictures. The value of j is then incremented until the simulation results no longer significant to prevent FOA attack. Then the range of J is then determined. Finally, the range of the MRA, for the reused decoy pictures is determined using the offline FOA simulation. Each of the reused decoy picture intervals, R_i with $i \in N_0$, is tested until the simulation results are no longer significant to prevent FOA attack. After that, a heuristic approach is used to fine-tune the MRA distribution range. All the significant R_i are grouped. The lower value of R_i is then eliminated from one to another if the simulation results no longer significant to prevent FOA attack. After determining the lower bound MRA range, the upper value of R_i is eliminated from one to another until the simulation result is able to prevent FOA attack. The upper bound MRA range is then determined.

5.1. $|X|$ Secret Password Interval

The $|X|$ significant interval of the proposed Algorithm is tested to determine the number of selection of secret password pictures used in the proposed system. Permutation is used to calculate the total number of selection based on the following formula:

$$\left[({}^{N}P_{x}) \sum_{j=4}^{x} ({}^{x}P_{j}) \frac{16!}{(16-j)!} \right]^{-1} \quad (1)$$

Figure 6 shows the $|X|$ secret password interval analysis. From the graph, the proposed method required a user to register at least eight pictures as the password in order to achieve a number of selections, which is higher than the benchmark system VIP3. Thus, the significant interval of $|X|$ should be within 8 to 16.

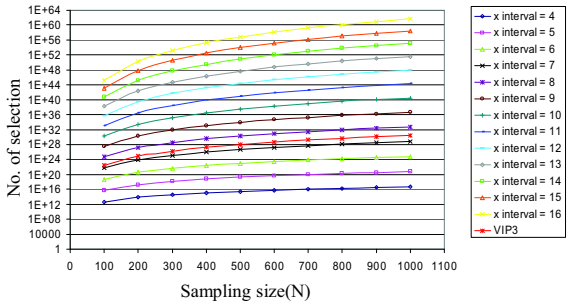


Figure 6. Empirical analysis of the $|X|$ secret password interval.

5.2. $|J|$ Secret Password Interval

To determine the metaheuristic interval used in the proposed method, the relation between the $|J|$ secret password pictures and the MRA interval was listed and analysed shown in Table 2. Let $\overset{j_{n..m}}{R_i}$ be the generic MRA interval for the proposed scheme where n and m

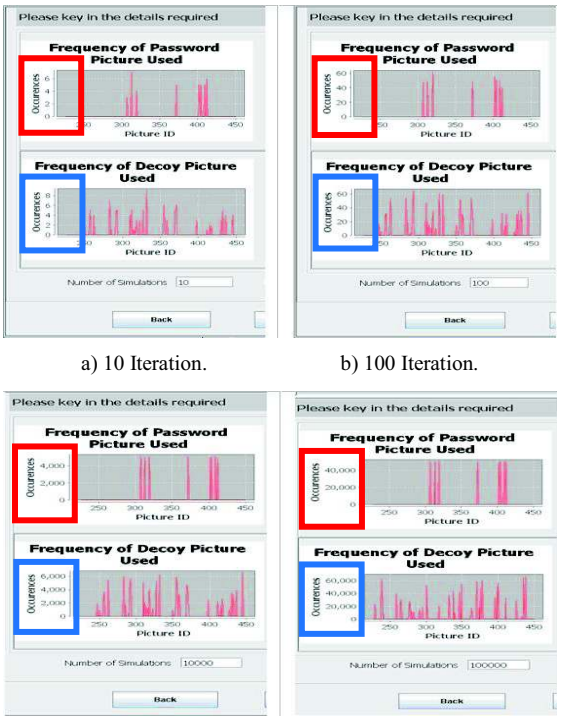
is the minimum and maximum number of secret password used during authentication respectively and R_i is the reused decoy pictures interval with $i \in N_0$. Table 2 shows that the first and the last distributions are not suitable to be used because it is highly vulnerable to shoulder surfing and password guessing attacks due to the fact that the decoy pictures generated from the previous attempt will either all be selected or none of them will be selected.

Table 2. MRA interval with minimum and maximum j=4.

Range	Probability Distribution	Reuse's Frequency
$\overset{j_{4..4}}{R_0}$	0.00	0
$\overset{j_{4..4}}{R_1}$	0.01-0.16	1
$\overset{j_{4..4}}{R_2}$	0.17-0.24	2
$\overset{j_{4..4}}{R_3}$	0.25-0.33	3
$\overset{j_{4..4}}{R_4}$	0.34-0.41	4
$\overset{j_{4..4}}{R_5}$	0.42-0.49	5
$\overset{j_{4..4}}{R_6}$	0.50-0.58	6
$\overset{j_{4..4}}{R_7}$	0.59-0.66	7
$\overset{j_{4..4}}{R_8}$	0.67-0.74	8
$\overset{j_{4..4}}{R_9}$	0.75-0.83	9
$\overset{j_{4..4}}{R_{10}}$	0.84-0.91	10
$\overset{j_{4..4}}{R_{11}}$	0.92-0.99	11
$\overset{j_{4..4}}{R_{12}}$	1.00	12

Figure 7 shows an instance of the offline FOA simulation attack for $\overset{j_{4..4}}{R_1}$. From the Figure, the secret password pictures used cannot be obtained based on highest frequency of occurrence after implementing the proposed method. Therefore, it is proven that the reused decoy picture concept is able to produce better results compared to VIP3 in terms of increasing the challenge of offline FOA attack.

The testing is then carried out for the other i values for $\overset{j_{4..4}}{R_i}$. The simulation results show that the value of i which is within the interval of 1 until 11 are significantly more robust against FOA attack. To improve the fix number of secret password selection, the upper value for j is then increased. From the simulation result, although the maximum number of secret password picture used for an authentication was increased to 5, the proposed method was still able to produce positive results for the following intervals: $\overset{j_{4..5}}{R_i}$, i={1, 2, 3, 4, 5, 6, 7, 8, 9 and 10}. However, when the maximum value of j was increased to 6, the simulation results were no longer significant to prevent FOA attack shown in Figure 8. Thus, the significant interval of J which is within the domain of $4 \leq |J| \leq 5$ is identified.

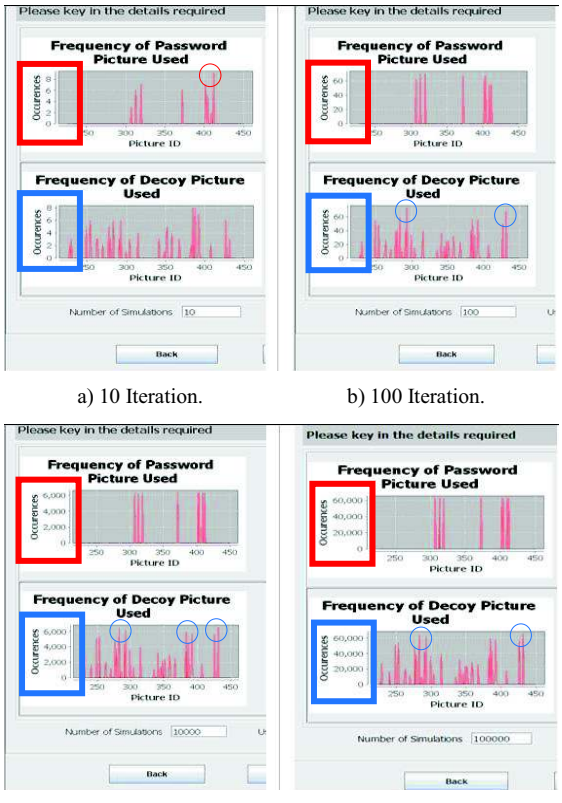


a) 10 Iteration. b) 100 Iteration.

c) 10000 Iteration. d) 100000 Iteration.

Figure 7. Analysis and observation result for $\overset{j_{4..4}}{R_1}$.

The secret password pictures used cannot be obtained based on highest frequency of occurrence although the number of iteration has increased from 10 until 100000.



a) 10 Iteration. b) 100 Iteration.

c) 10000 Iteration. d) 100000 Iteration.

Figure 8. Analysis and observation result for $\overset{j_{4..6}}{R_1}$.

One of the secret password pictures has higher frequency of occurrence compared to the decoy

pictures in 10 iterations simulation (circled in red). Only few decoy pictures have higher frequency of occurrence compared to the secret password pictures in 100, 10000 and 100000 iterations simulation (circled in blue). Therefore, 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 100000 iterations.

5.3. MRA Distribution Range

After determining the significant interval of J, a heuristic approach is used to fine-tune the MRA interval in suspense to strengthen the proposed method. In the heuristic approach testing, all the significant R_i intervals were grouped. The lower bound MRA range were tested and determined if the testing result was able to prevent FOA attack. After that, the upper bound value was tested and determined using the similar method shown in Table 3.

Table 3. MRA interval classification

Classification 1	Classification 2	Classification 3	Classification 4
${}^{j4..5}R_1$, ${}^{j4..5}R_2$, ${}^{j4..5}R_3$, ${}^{j4..5}R_4$, ${}^{j4..5}R_5$, ${}^{j4..5}R_6$, ${}^{j4..5}R_7$, ${}^{j4..5}R_8$, ${}^{j4..5}R_9$, ${}^{j4..5}R_{10}$	${}^{j4..5}R_2$, ${}^{j4..5}R_3$, ${}^{j4..5}R_4$, ${}^{j4..5}R_5$, ${}^{j4..5}R_6$, ${}^{j4..5}R_7$, ${}^{j4..5}R_8$, ${}^{j4..5}R_9$, ${}^{j4..5}R_{10}$	${}^{j4..5}R_3$, ${}^{j4..5}R_4$, ${}^{j4..5}R_5$, ${}^{j4..5}R_6$, ${}^{j4..5}R_7$, ${}^{j4..5}R_8$, ${}^{j4..5}R_9$, ${}^{j4..5}R_{10}$	${}^{j4..5}R_4$, ${}^{j4..5}R_5$, ${}^{j4..5}R_6$, ${}^{j4..5}R_7$, ${}^{j4..5}R_8$, ${}^{j4..5}R_9$, ${}^{j4..5}R_{10}$
Classification 5	**Classification 6**	**Classification 7**	**Classification 8**
${}^{j4..5}R_4$, ${}^{j4..5}R_5$, ${}^{j4..5}R_6$, ${}^{j4..5}R_7$, ${}^{j4..5}R_8$, ${}^{j4..5}R_9$	${}^{j4..5}R_4$, ${}^{j4..5}R_5$, ${}^{j4..5}R_6$, ${}^{j4..5}R_7$, ${}^{j4..5}R_8$	${}^{j4..5}R_4$, ${}^{j4..5}R_5$, ${}^{j4..5}R_6$, ${}^{j4..5}R_7$	${}^{j4..5}R_4$, ${}^{j4..5}R_5$, ${}^{j4..5}R_6$

From the FOA simulation analysis, the distribution ranges that have been assigned to the classification number 1, 2, 3 and 8 were not suitable to be used due to the fact that the secret password pictures used can be obtained based on the highest frequency of occurrence in lower iteration simulation. On the other hand, the classification numbers 4, 5, 6 and 7 were able to produce significant results with the respective distribution range. However, in order to prevent the proposed method from generating a high volume of reuse decoy pictures, the significant upper bound MRA distribution range, which is equal to, ${}^{j4..5}R_7$ was identified. (The more decoy pictures were produced, the easier for a password guessing attacker to eliminate the unused decoy pictures at each authentication attempt.) Thus, the lower bound and upper bound of the MRA distribution range for the proposed scheme was identified as ${}^{j4..5}R_4$ and ${}^{j4..5}R_7$ respectively shown in Table 4.

Table 4. MRA Interval with minimum j=4 and maximum j=5.

Range	Probability Distribution	Min. Reuse's Frequency	Max. Reuse's Frequency
${}^{j4..5}R_0$	0.00	0	0
${}^{j4..5}R_1$	0.01-0.18	1	2
${}^{j4..5}R_2$	0.19-0.27	2	3
${}^{j4..5}R_3$	0.28-0.36	3	4
${}^{j4..5}R_4$	0.37-0.45	4	5
${}^{j4..5}R_5$	0.46-0.55	5	6
${}^{j4..5}R_6$	0.56-0.63	6	7
${}^{j4..5}R_7$	0.64-0.72	7	8
${}^{j4..5}R_8$	0.73-0.81	8	9
${}^{j4..5}R_9$	0.82-0.90	9	10
${}^{j4..5}R_{10}$	0.91-0.99	10	11
${}^{j4..5}R_{11}$	1.00	11	12

6. Password Space Analysis

Table 5 shows the password space comparison among VIP3 and the proposed system. From the table, it is shown that the proposed system is able to improve approximately 49 times the security to password guessing attack compared to the benchmarking scheme (assuming the total sampling size (N) used by both schemes are identical). In addition, the benchmarking scheme is approximately 3770 times more vulnerable to the password guessing attack compared to the proposed scheme if the secret password pictures selection used by the proposed scheme was increased to the maximum limit.

Table 5. Password space comparison.

Scheme	Password Space	Number of Tries to Password Guessing Attack
VIP3	$\left[({}^{N}P_8)({}^{8}P_4)\frac{16!}{(16-4)!} \right]$	$[73382400\ ({}^{N}P_8)]^{-1}$
Proposed System	$\left[({}^{N}P_8)\sum_{j=4}^{5}({}^{8}P_j)\frac{16!}{(16-j)!} \right]$	$[3595737600\ ({}^{N}P_8)]^{-1}$
***Proposed System**	$\left[({}^{N}P_8)\sum_{j=4}^{5}({}^{16}P_j)\frac{16!}{(16-j)!} \right]$	$[276651648000\ ({}^{N}P_8)]^{-1}$
* utilise maximum secret password pictures.		

7. Mitigate Shoulder Surfing

In order to test and verify whether the proposed method is able to resist shoulder surfing attack, 30 participants who are undergoing postgraduate study from the FSCIT, UM, Malaysia were randomly identified to perform shoulder surfing attacks. The role of the attacker was explained to each individual before the attacker began his/her attacks. Each of the identified shoulder surfing attacker was given three continuous attempts to guess an authorised password after a

successful login demonstration was carried out in front of the attacker. If the attacker is unable to get authorisation, his/her account will be locked after the third attempt.

The case study result shows that all the identified shoulder surfing attackers were unable to shoulder surf and guess the correct password used. An interview was conducted with each of the shoulder surfing attacker regarding the choices of selection. According to the interview results, most of the shoulder surfing attackers were dazed when they noticed that only several selected password pictures were displayed in the challenge sets. As a result, most of the choices that were selected by the attackers were based on the position of the secret password pictures used during the demonstration set (using key logging attack concept), redundant pictures that have been generated in the previous attempt (FOA attack), new pictures that were generated in the current challenge set, similarity concept of the secret password pictures used such as colour, shape and category at the demonstration set. As a conclusion, this experiment suggests that the proposed scheme is able to mitigate shoulder surfing attack.

8. Conclusions

In this paper, a new security threat for searchmetrics picture-based password authentication schemes was discovered. To prevent FOA attack, a new method that utilises the metaheuristic random Algorithm was proposed. The parameters used in the proposed method was scrutinised and evaluated to achieve optimum results in preventing the aforementioned attack. An offline FOA simulation attack and shoulder surfing attacking task were carried out to verify the proposed method. The experimental results shows that the proposed method was able to resist FOA attack and mitigate shoulder surfing attack irrespective to gender and competency levels. In addition, the proposed method is able to improve the password space compared to the benchmark scheme.

In future, research on other graphical authentication method such as [20] and improving other security threats such as man in the middle and alleviating user memorability will be our main focus. Subsequently, data hiding method such as in [13, 17, 18, 19] will be considered to secure the registered password.

Acknowledgement

I would like to acknowledge and extend my heartfelt gratitude to Dr. Wong, Dr. Ravi and Prof. Sulaiman for proof reading and providing constructive feedback for this publication. I would also like to express my gratitude to Ministry of Science, Technology and Innovation (MOSTI), KPT (FRGS FP031/2012), Malaysia and UM (UMRG RG079-11ICT) for providing research funds to make this project a success.

References

[1] Blonder G., "Graphical Passwords," *in Lucent Technologies*, United States Patent 5559961, 1996.

[2] Brostoff S. and Sasse M., "Are Passfaces More Usable than Passwords: A Field Trial Investigation," *in Proceedings of Human-Computer Interaction*, UK, pp. 405-424, 2000.

[3] Davis D., Monrose F., and Reiter M., "On User Choice in Graphical Password Schemes," *in Proceedings of the 13th Conference on USENIX Security Symposium*, California, pp. 1-14, 2004.

[4] De-Angeli A., Coventry L., Johnson G., and Coutts M., "Usability and User Authentication: Pictorial Passwords VS. Pin," *in Proceedings of Contemporary Ergonomics*, London, pp. 253-258, 2003.

[5] De-Angeli A., Coventry L., Johnson G., and Renaud K., "Is A Picture Really Worth A Thousand Words? Exploring the Feasibility of Graphical Authentication Systems," *International Journal of Human-Computer Studies*, vol. 63, no. 1-2, pp. 128-152, 2005.

[6] Dhamija R. and Perrig A., "Déjà Vu: A User Study Using Images for Authentication," *in Proceedings of the 9th USENIX Security Symposium*, USA, pp. 45-58, 2000.

[7] Dirik A., Memon N., and Birget J., "Modeling User Choice in the PassPoints Graphical Password Scheme," *in Proceedings of the 3rd Symposium on Usable Privacy and Security*, USA, pp. 20-28, 2007.

[8] Jansen W., Gavrila S., and Korolev V., Ayers R., Swanstrom R., "Picture Password: A Visual Login Technique for Mobile Devices," available at: http://csrc.nist.gov/publications/nistir/nistir-7030.pdf, last visited 2007.

[9] Lip-Yee P. and Xui-Ting L., "Issues, Threats and Future Trend for GSP," *in Proceedings of the 7th WSEAS International Conference on Applied Computer and Applied Computational Science (ACACOS)*, China, pp. 627-633, 2008.

[10] Lip-Yee P. and Xui-Ting L., "Multi-Grid Background Pass-Go," *Journal of WSEAS Transactions on Information Science and Applications*, vol. 5, no. 7, pp. 1137-1148, 2008.

[11] Lip-Yee P., Xui-Ting L., Moon-Ting S., and Kianoush F., "The Design and Implementation of Background Pass-Go Scheme Towards Security Threats," *Journal of WSEAS*

Transactions on Information Science and Applications, vol. 5, no. 6, pp. 943-952, 2008.

[12] Moncur W. and Lepalâtre G., "Pictures at the ATM: Exploring the Usability of Multiple Graphical Passwords," *in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, USA, pp. 887-894, 2007.

[13] Nasser H., "Hiding Text Information in a Digital Image Based on Entropy Function," *The International Arab Journal of Information Technology*, vol. 7, no. 2, pp. 146-151, 2010.

[14] Passfaces™, Next Generation Graphical Authentication, Corporation, available at: http://www.passfaces.com/pfdemo/bankingdemo.htm, last visited 2008.

[15] Renaud K. and De-Angeli A., "Visual Passwords: Cure-All or Snake-Oil?," *Communications of the ACM*, vol. 52, no. 12, pp. 135-140, 2009.

[16] Xiaoyuan S., Ying Z., and Owen G., "Graphical Passwords: A Survey," *in Proceedings of 21st Annual Computer Security Applications Conference*, USA, pp. 463-472, 2005.

[17] Por L-Y., Wong K-S., and Chee K-O., "UniSpaCh: A Textbased Data Hiding Method Using Unicode Space Characters," *Journal of Systems and Software*, vol. 85, no. 5, pp. 1075-1082, 2012.

[18] Por L-Y., Delina-B., Ang T-F., and Ong S-Y., "An Enhanced Mechanism for Image Steganography Using Sequential Colour Cycle Algorithm," *The International Arab Journal of Information Technology*, vol. 10, no. 1, pp. 51-60, 2013.

[19] Por L., Lai W., Alireza A., Ang T., Su M., and Delina B., "StegCure: A Comprehensive Steganographic Tool Using Enhanced LSB Scheme," *Journal of WSEAS Transactions on Computers*, vol. 7, no. 8, pp. 1309-1318, 2008.

[20] Yee P-L. and Kiah M-L-M., "Shoulder Surfing Resistance Using Penup Event and Neighbouring Connectivity Manipulation," *Malaysian Journal of Computer Science*, vol. 23, no. 2, pp. 121-140, 2010.

Lip Yee Por is a senior lecturer for the Department of System and Computer Technology in the Faculty of Computer Science and Information Technology at University of Malaya. He received his PhD, BSc and MSc in computer science at University of Malaya, Malaysia. His current research interests include information security, steganography, image processing, graphical authentication, grid computing, and e-learning framework. He is a senior member of IEEE since 2011. His biography has been included in Marquis Who's Who in the World.