J. Basic. Appl. Sci. Res., 2(5)4368-4376, 2012
© 2012, TextRoad Publication
ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

Graphical Password Security Evaluation Criteria by Fuzzy Analytical Hierarchical Process (FAHP)

Arash Habibi Lashkari[1], Azizah Abdul Manaf[1], Maslin Masrom[2]

[1] Advanced Informatics School, Universiti Technologi Malaysia (UTM), Kuala Lumpur, Malaysia
[2] Razak School of Engineering and Advanced Technology, Universiti Technologi Malaysia (UTM), Kuala Lumpur, Malaysia

ABSTRACT

In today's day and age, one of the important topics in information security is authentication and Graphical Password or Graphical User Authentication (GUA) is one of the most secure techniques. This paper will touch on the security aspect of those algorithms and what most researchers have been working on trying to define these security features and attributes. The goal of this study is to develop a complete decision model that allows automatic selection of available GUA algorithms by taking into considerations the subjective judgments of the decision makers based on the Fuzzy Analytic Hierarchy Process (FAHP).

Keywords – Graphical Password, Authentication Security, Attack Patterns, Brute force attack, Dictionary attack, Guessing Attack, Spyware attack, Shoulder surfing attack, Social engineering Attack, Password Entropy, Password Space.

1. INTRODUCTION

In describing Graphical Based Passwords, researchers coined the term "Picture Superiority Effect" which shows the effect of GBP being used as a solution for the conventional password techniques. It also underlines the impact of GBP and highlighting the fact that graphics and text are easier to commit to memory than those techniques.

Initially, the concept of Graphical User Authentication (GUA) (Graphical Password or Graphical Image Authentication (GIA)) described by Blonder (Blonder, 1996), one image would appear on the screen of whereupon the user would click on a few chosen regions on the image. Authentication is done when the user clicks on the correct regions. Security is one of the major issues in graphical passwords and should be evaluated and measured [1-3]. There are many researches on this area that shows the security of GP are related to the multiple factors such as entropy, password space and related attacks [1, 3]. These factors proved that it is not possible to simply find a formula that evaluates graphical password algorithms. So, till now, there isn't a complete evaluation model for evaluating the security of graphical password algorithms based on all the related aspects [3].

Meanwhile, there are many types of multi-criteria techniques for decision making like PROMETHEE, ELECTRE, and Analysis Hierarchy Process (AHP). These techniques use the best opinions from all possible alternatives using multiple, sometimes conflicting, decision criteria. The AHP technique investigated in the present study, is a multi-criteria decision making technique developed by Saaty [4]. Although traditional AHP technique may display expert knowledge, it cannot reflect human thinking [4]. Therefore, FAHP technique was developed [4]. So, we will try to propose a complete security evaluation criterion for most graphical password (GP) algorithms including the related aspects in GP.

2. Our Proposed Framework

For the proposed Fuzzy AHP technique, five steps have been defined, as shown on figure 1 below.

***Corresponding Author:** Arash Habibi Lashkar, Advanced Informatics School, Universiti Technologi Malaysia (UTM), Kuala Lumpur, Malaysia. E –mail : a_habibi_l@hotmail.com

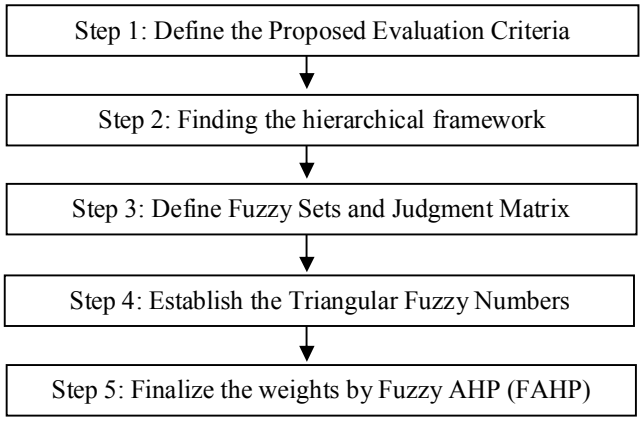

Figure 1: The framework of proposed evaluation criteria

3. Graphical Passwords' Security Evaluations

In regards to the Magic Triangle evaluation criteria [3], that we have proposed, we defined a triangular of attributes that can be used to test graphical password security, namely attack, password space and password entropy as shown in figure 3. With reference to previous researches [3], it is possible to calculate the password space and entropy by using mathematical formulas. However in order to measure the attacks attribute, we must evaluate the attack resistance of each graphical password related attacks.

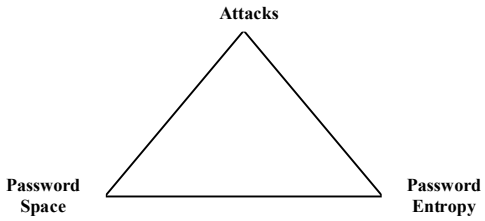

Figure 2: Magic triangle evaluation for graphical passwords security

This also proves that we cannot use a general evaluation method to compare and test different algorithms. In the following section, we will try to explain the different attacks and the related formulas that will be use to calculate password space and entropy.

3.1. Graphical Passwords related Attacks

Based on the International Attacks Patterns Standard (CAPEC 2011) as well as related researches, at present there are seven common graphical password attacks, namely:

Brute Force Attack (BFA): The attack that tries to find every possible combination of password in order to break it (CAPEC-49).
Dictionary Attack: This method checks for words in a preset dictionary and test whether they are being used as a password or not (CAPEC-16).
Spyware Attack: Spyware installed themselves on a users' computer and records sensitive data for the attacker [3]
Shoulder Surfing Attack: Attackers will peer over a person's shoulder in order to find out their password [3]
Social Engineering Attack (Description Attack) (SEA): An attacker that impersonates an authorized employee by getting information through other employees in the organization (CAPEC-403).
Guessing Attack: This type of attack guesses a user's password by using common personal information such as name of their pets, passport number, family name and so forth [1]
Manipulation Attack (MA): This attack exploits the file location algorithm of a file by creating another file with the same name as the protected and privileged file. Then system can then be manipulated once it accepts the fake file as a trusted application component and loads it instead of the original file. Applications tend to load external components or files such as system libraries and configuration files and should be protected again malicious manipulation attempts. Unfortunately, an attacker can create a file with the same name and place it in the directory

that will be search before the legitimate directory is selected, especially if the application only locates using the filename (CAPEC-177 Child of CAPEC-165 that is file manipulation).

3.2. Password Space

The last resource on December 2010 defines the password spaces formula [1]:

$$PS= M^N$$

In this formula, M represents the number of images in each round while N represents the number of rounds. However, in regards to the triangle method and movable frame algorithms in this formula along with the process of finding and selecting the line and triangle values, it is not possible to calculate the accurate password space using this formula. This means that the algorithms for graphical password space must be calculated using the conditional probability formula based on case by case situation and not using one unique formula to evaluate every available algorithm.

3.3. Password Entropy

In order to measure the security of passwords that has been generated, password entropy is used. It is a method of measuring the level of difficulty in guessing the password blindly. For example, let's assume that all passwords are distributed evenly; we can use the formula below to calculate the password entropy of the GP [1].

$$PE = N \log_2 (|L||O||C|)$$

Basically, graphical password entropy measures the probability of an attacker randomly guessing the correct password. In the formula, N represents the length or number of runs, L is the locus alphabet as the set of all loci, O represents and object alphabet and colour is represent by C. Although, it is possible to calculate the password entropy for some algorithms using this formula, it is not applicable to all algorithms. For example, this formula cannot be used to calculate triangle algorithm because the major process of triangle selection is not valued in this formula. This problem also is similar for movable frame algorithm where the process of finding a line and select it is not valued [1].

4. Fuzzy Logic and Fuzzy Set

The word "fuzzy" in the dictionary means "not clear, indistinct, non coherent, vague". However, in a technical sense, fuzzy systems are systems that precisely defined and fuzzy control is a non-linear control that is precisely defined. The goal of fuzzy logic is to mirror (or improve) "human-like" reasoning. Fuzzy systems are either knowledge-based or rule-based. Specifically, the key component of a knowledge based fuzzy systems are the sets of IF-THEN rules obtained via human experience and expertise. The fuzzy systems are multi-input-single-output mappings from a real-valued vector to a real-valued scalar [5].

Fuzzy logic systems are created to handle mathematical vagueness and uncertainties. It is also designed to provide a formalized tool that deals with the imprecision and intrinsic issues of many problems. Fuzzy systems allows inference morphology that enable human reasoning capabilities to be included into knowledge-based systems. The theory of fuzzy logic provides a mathematical strength to capture the uncertainties associated with human cognitive processes, such as thinking and reasoning [6-8].

The classical theory set of either a member or not a member is based on the fundamental set concept. In this theory, there is a sharp and unambiguous distinction existing between a non-member and a member for any set of defined entities. An entity that belongs to a set has a precise and clear boundary that separates it from others. Unfortunately, in the real world, not all applications can be handled using the classical set theory. The fuzzy set is actually an extension of the crisp set. Crisp set only allow full membership or non-membership at all, whereas fuzzy sets allow partial membership [9].

Fuzzy numbers are the special classes of the fuzzy quantities. It is a fuzzy quantity M that represents the generalization of r, a real number. Intuitively, M(x) should be a measure of how well M(x) approximates "r" [10].

The convex normalized fuzzy set is the fuzzy number f. It characterized the given interval if real numbers, with a grade between 0 and 1 for each membership. Of course, it is possible to use different fuzzy number for different conditions. Generally in practice triangular and trapezoidal fuzzy numbers are used [11]. Typically, it is more convenient to work with triangular fuzzy numbers (TFNs) in applications because it is computationally simpler. Also, they are more useful when promoting the representation and information processing in a fuzzy environment. Figure 4 below shows the triangular fuzzy number, M:

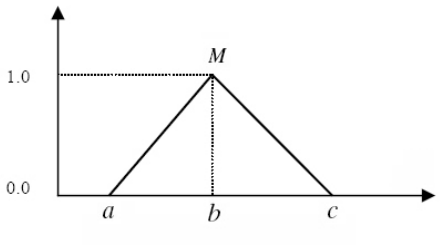

Figure 4: A triangular fuzzy number, M

Three real number, expressed as a, b and c, are defined in TFNs. These parameters respectively represent the smallest value possible, followed by the most promising value and finally the largest possible value that describes the fuzzy event. The function of the membership can be described as;

$$\mu(x/M) = \begin{cases} 0, & x < l \\ \frac{x-a}{b-a} & a \le x \le b \\ \frac{c-x}{c-b} & b \le x \le c \\ 0, & x > u \end{cases} \quad \text{(Eq. 1)}$$

The different operations can be defined by the triangular fuzzy numbers. However, there are three important operations being used in this study. For example, if we define two positive fuzzy numbers of x= (x_a, x_b, x_c) and y= (y_a, y_b, y_c) then it would be:

$x+y= (x_a, x_b, x_c)+ (y_a, y_b, y_c) = (x_a +y_a, x_b +y_b, x_c +y_c)$ (Eq. 2)

$x*y= (x_a, x_b, x_c)* (y_a, y_b, y_c) = (x_a\, y_a, x_b\, y_b, x_c\, y_c)$ (Eq. 3)

$x^{-1}= (x_a, x_b, x_c)^{-1} = (1/x_a, 1/x_b, 1/x_c)$ (Eq. 4)

$z*x=z*(x_a, x_b, x_c)= (zx_a, zx_b, zx_c)$ (Eq. 5)

Other algebraic fuzzy numbers operations can be found in [12-13].

5. FUZZY MULTI-ATTRIBUTE DECISIONMAKING METHODS

There are two main characteristic that gives fuzzy system an advantage in performance for specific applications are: fuzzy systems are better at approximate reasoning especially when dealing with mathematical models that are difficult to derive. With fuzzy logics, decision making with estimated values is still possible with incomplete or uncertain information [6-8].

One fuzzy system that caused a lot of attention and interested in decision science, systems engineering, management science, evaluation systems, and operations research is the Fuzzy Multi-Criteria Decision Making (FMCDM). The most important component in FMCDM is fuzzy multi-attribute decision making. There are many efficient methods in dealing with fuzzy multi attribute decision making problems which is according to the decision maker's own preference and whether the information is known or completely unknown.

In order to solve a fuzzy multi-criteria decision making problem, the key is how to obtain the preference information on the weight of the decision-maker's criteria. These efficient methods includes Analytical Hierarchy Process (AHP), average weighted comprehensive method, fuzzy optimum seeking method, minimum membership degree method, average weighted programming method, fuzzy neutral networks comprehensive decision making method, fuzzy iteration method, and target decision by entropy weight and fuzzy. For the evaluation criteria, we propose using the AHP technique to find the best decision-making criteria weight [13-15].

6. AHP and Fuzzy-AHP (FAHP) Method

There are several fuzzy AHP methods, but the authors of this paper prefer Chang's extent analysis method since the steps of this approach is relatively easier compare to the other methods. In the following, the outlines of the extent analysis method on fuzzy AHP are given as: Let X = (x_1, x_2, . . . ,x_n) be an object set, and U = (u_1,u_2, . . . ,u_m) be a goal set. Based on Chang's extent analysis [16], each object is taken and extent analysis for each goal, gi, is performed respectively. Therefore, m extent analysis values for each object can be obtained, with the following signs:

$M_{gi}^1, M_{gi}^2, \ldots, M_{gi}^m \qquad i = 1,2, \ldots, n$

Where all the $M_{gi}^j \ \ (i = 1,2, \ldots, n)$ are triangular fuzzy numbers (TFNs). Respectively, they are the lowest possible value, most possible value and largest possible value. Figure 6 illustrates a TFN that is represented as a, b, and c.

The steps of Chang's extent analysis can be given as follows:

Step1:
The value of the fuzzy synthetic extent with respect to the ith object is defined as (Eq. 6):

$$S_i = \sum_{j=1}^{m} M^j{}_{gi} * \left[\sum_{i=1}^{n}\sum_{j=1}^{m} M^j{}_{gi}\right]^{-1}$$

To obtain $\sum_{j=1}^{m} M^j{}_{gi}$ perform the fuzzy addition operation of m extent analysis values for a particular matrix as (Eq. 7):

$$\sum_{j=1}^{m} M^j{}_{gi} = \left(\sum_{j=1}^{m} \mathrm{a}_{ij}, \sum_{j=1}^{m} \mathrm{b}_{ij}, \sum_{j=1}^{m} \mathrm{c}_{ij}\right), \qquad i = 1,2,\dots,n$$

Regarding to the fuzzy addition operation such as Eq. 5, it is possible to define (Eq. 8):

$$\sum_{i=1}^{n}\sum_{j=1}^{m} M^j{}_{gi} = \left(\sum_{i=1}^{n}\sum_{j=1}^{m} \mathrm{a}_{ij}, \sum_{i=1}^{n}\sum_{j=1}^{m} \mathrm{b}_{ij}, \sum_{i=1}^{n}\sum_{j=1}^{m} \mathrm{c}_{ij}\right)$$

And then compute the inverse of the vector in Eq. such that (Eq. 9):

$$\left[\sum_{i=1}^{n}\sum_{j=1}^{m} M^j{}_{gi}\right]^{-1} = \left(\frac{1}{\sum_{i=1}^{n}\sum_{j=1}^{m} \mathrm{c}_{ij}}, \frac{1}{\sum_{i=1}^{n}\sum_{j=1}^{m} \mathrm{b}_{ij}}, \frac{1}{\sum_{i=1}^{n}\sum_{j=1}^{m} \mathrm{a}_{ij}}\right)$$

So it is possible to compute S_i such that (Eq. 10):

$$S_i = \left(\sum_{j=1}^{m} \mathrm{a}_{ij}, \sum_{j=1}^{m} \mathrm{b}_{ij}, \sum_{j=1}^{m} \mathrm{c}_{ij}\right) * \left(\frac{1}{\sum_{i=1}^{n}\sum_{j=1}^{m} \mathrm{c}_{ij}}, \frac{1}{\sum_{i=1}^{n}\sum_{j=1}^{m} \mathrm{b}_{ij}}, \frac{1}{\sum_{i=1}^{n}\sum_{j=1}^{m} \mathrm{a}_{ij}}\right) \quad i = 1,2,\dots,n$$

Step2:
The degree of possibility of $M_2 = (a_2, b_2, c_2) \geq M_1 = (a_1, b_1, c_1)$is defined as (Eq. 11):

$$V(M_2 \geq M_1) = \underset{Y \geq x}{\mathrm{Sup}}[\min(\mu_{M1}(X),\ \mu_{M2}(y))\ ]$$

And can be equivalently expressed as below (Eq. 12):

$$V(M_2 \geq M_1) = hip(M_1 \cap M_2) = \mu_{M2}(d) = \begin{cases} 1, & if\ b_2 \geq b_1 \\ 0, & if\ a_1 \geq c_2 \\ \dfrac{a_1 - c_2}{(b_2 - c_2) - (b_1 - a_1)}, & Otherwise \end{cases}$$

Where d is the ordinate of the highest intersection point D between μ_{M1} and μ_{M2} (Figure 5).

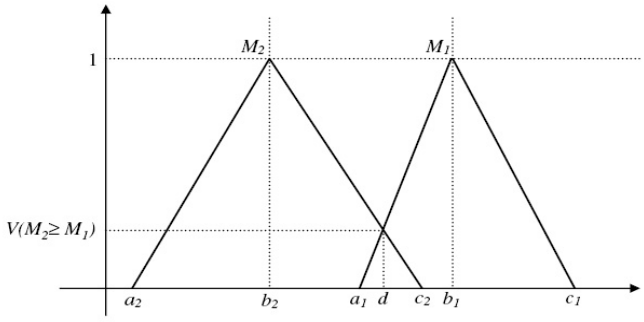

Figure 5: the intersection between $M_1 and\ M_2$

For comparing M_1 and M_2, we need both the value of $V(M_2 \geq M_1)$ and $V(M_1 \geq M_2)$.

Step3:
The degree of possibility for a convex fuzzy number to be greater than Kconvex fuzzy number $M_i (i = 1,2,\dots,k)$ can be defined by (Eq. 13):

$$V(M \geq M_1, M_2, \ldots, M_K) = V[(M \geq M_1) and (M \geq M_2) and \ldots and\ (M \geq M_k)]$$
$$= \min V(M \geq M_i), \qquad i = 1,2,3 \ldots, k$$

Assume that (Eq. 14):
$d(A_i) = \min V(S_i \geq S_k)\ \ K = 1,2, \ldots, n\ ;\ k \neq i$
Then the weight vector is given by (Eq. 15):
$W' = (d'(A_1), d'(A_2), \ldots, d'(A_n))^T$
That $A_i (i = 1,2, \ldots, n)$ are n elements.

Step 4:
Via, normalization, the normalized weight vectors are (Eq. 16):
$W = (d(A_1), d(A_2), \ldots, d(A_n))^T$
That W is a non-fuzzy number.

It is impossible to create mathematical operations directly using security evaluation values especially the common attack values. The best way is to convert the attack scale into a fuzzy scale. There is a variety of different fuzzy scales [17-20], The triangular fuzzy conversion scale in this paper - shown in table 4 below, is used in the evaluation model founded by Gumus (2009) [13].

Table 4: Triangular fuzzy conversion scale

Row	Security value scale	Triangular fuzzy scale	Triangular fuzzy reciprocal scale
1	Just equal	(1,1,1)	(1,1,1)
2	Moderate importance	(1,3,5)	(1/5,1/3,1)
3	Weakly more important	(3,5,7)	(1/7,1/5,1/3)
4	Strong importance	(5,7,9)	(1/9,1/7,1/5)
5	Very strong importance	(7,9,11)	(1/11,1/9,1/7)

7. Proposed system and hierarchical diagram

We would like to propose an evaluation methodology to examine the security strength of graphical password algorithms. In order to yield the proper result, the method that was chosen - fuzzy AHP, requires a hierarchical structure. Referring to the last security evaluation criteria which is the magic rectangle discovered by Lashkari (2011) [21], The main variables for security evaluation in graphical passwords are C_1: Password Space (PS), C_2: Password Entropy (PE) and Common Attacks namely C_3: Brute Force Attack (BTA), C_4: Dictionary Attack (DA), C_5: Spyware Attack (SA), C_6: Shoulder Surfing Attack (SSA), C_7: Social Engineering Attack (Description Attack) (SEA), C_8: Guessing Attack (GA), C_9: Manipulating Attack (MA). Figure 6 shows the hierarchical structure that is considered for this proposed system. It is based on a graphical password technique (GPT) and will be evaluated by the system.

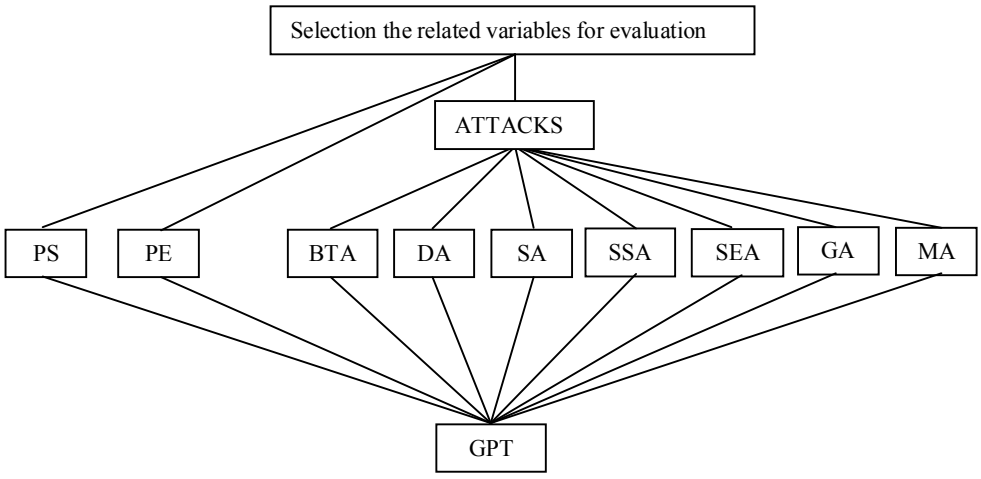

Figure 6: The hierarchy to security evaluation of graphical passwords based on magic triangle found by Lashkari 2011

8. Discussion based on numerical application

Many professionals as well as academics have worked to build pair-wise comparison matrixes for the attributes. Figure 7 below shows an example of a questionnaire that is provided to retrieve the first numerical evaluation matrix. The geometrical mean of individual evaluations is taken and calculated to get the accurate result.

No	Attributes	Fuzzy Scale					Reciprocal Scale					Attributes
		1	2	3	4	5	1	2	3	4	5	
Q1	Password Space (PS)											Password Entropy (PE)
Q2												Brute Force Attack (BTA)
Q3												Dictionary Attack (DA)
Q4												Spyware Attack (SA)
Q5												Shoulder Surfing Attack (SSA)
Q6												Social Engineering Attack (Description Attack) (SEA)
Q7												Guessing Attack (GA)
Q8												Physical Attack (Attack to the main gallery)(PA)
Q9	Password Entropy (PE)											Brute Force Attack (BTA)
Q10												Dictionary Attack (DA)
Q11												Spyware Attack (SA)
Q12												Shoulder Surfing Attack (SSA)
Q13												Social Engineering Attack (Description Attack) (SEA)
Q14												Guessing Attack (GA)
Q15												Physical Attack (Attack to the main gallery)(PA)
Q16	Brute Force Attack (BTA)											Dictionary Attack (DA)
Q17												Spyware Attack (SA)
Q18												Shoulder Surfing Attack (SSA)
Q19												Social Engineering Attack (Description Attack) (SEA)

Figure 7: questionnaire for collect the evaluators' feedbacks

In the first step of the analysis, in regards to the decision maker's preferences for our criteria, the pair-wise comparison values are converted into TFN values, as shown in the table matrix where the main attribute is being built:

Table 5: Fuzzy Pairwise comparison matrix

Criteria	C1	C2	C3	C4	C5	C6	C7	C8	C9
C1	1,1,1	1,1,1	1,3,5	1,3,5	1,3,5	1,3,5	1,3,5	1,3,5	1,3,5
C2	1,1,1	1,1,1	3,5,7	3,5,7	3,5,7	3,5,7	3,5,7	3,5,7	3,5,7
C3	1/5,1/3,1	1/7,1/5,1/3	1,1,1	1,3,5	1,3,5	1,1,1	1,3,5	1,1,1	1,1,1
C4	1/5,1/3,1	1/7,1/5,1/3	1/5,1/3,1	1,1,1	1,3,5	1,1,1	1,1,1	1,3,5	1,1,1
C5	1/5,1/3,1	1/7,1/5,1/3	1/5,1/3,1	1/5,1/3,1	1,1,1	1,1,1	1,1,1	1,1,1	1,1,1
C6	1/5,1/3,1	1/7,1/5,1/3	1,1,1	1,1,1	1,1,1	1,1,1	1,3,5	3,5,7	1,3,5
C7	1/5,1/3,1	1/7,1/5,1/3	1/5,1/3,1	1,1,1	1,1,1	1/5,1/3,1	1,1,1	1,3,5	1,1,1
C8	1/5,1/3,1	1/7,1/5,1/3	1,1,1	1/5,1/3,1	1,1,1	1/7,1/5,1/3	1/5,1/3,1	1,1,1	1,1,1
C9	1/5,1/3,1	1/7,1/5,1/3	1,1,1	1,1,1	1,1,1	1/5,1/3,1	1,1,1	1,1,1	1,1,1

Once the fuzzy pair-wise comparison matrix has been formed, the weights of all criteria can be determined with the help of FAHP. The first synthesis value should be calculated according to the FAHP method. Table 5 below shows that the synthesis values in respect to the main goal is calculated the same way as in Eq. (6) using operation based on Eq. (3):

Sc1= (9.000, 23.000, 37.000) ⊗ (0.005, 0.008, 0.013) = (0.049, 0 .181, 0.469)

Sc2= (23.000, 37.000, 51.000) ⊗ (0.005, 0.008, 0.013) = (0.125, 0.291, 0.646)

Sc3= (7.343, 13.533, 20.330) ⊗ (0.005, 0.008, 0.013) = (0.040, 0.106, 0.258)

Sc4= (6.543, 10.867, 16.333) ⊗ (0.005, 0.008, 0.013) = (0.036, 0.085, 0.207)

Sc5= (6.543, 6.867, 8.333) ⊗ (0.005, 0.008, 0.013) = 0.036, 0.054, 0.106)

Sc6= (9.343, 15.533, 22.333) ⊗ (0.005, 0.008, 0.013) = (0.051, 0.122, 0.283)

Sc7= (5.743, 8.200, 12.333) ⊗ (0.005, 0.008, 0.013) = (0.031, 0.064, 0.156)

Sc8= (4.886, 5.400, 7.667) ⊗ (0.005, 0.008, 0.013) = (0.027, 0.042, 0.097)

Sc9= (6.543, 6.867, 8.333) ⊗ (0.005, 0.008, 0.013) = (0.036, 0.054, 0.106)

These values are obtained by comparing the fuzzy values using Eq. 12:

V(Sc1≥Sc1) =	-	V(Sc2≥Sc1) =	1.000	V(Sc3≥Sc1) =	1.000	V(Sc4≥Sc1) =	0.624	V(Sc5≥Sc1) =	0.309
V(Sc1≥Sc2) =	0.757	V(Sc2≥Sc2) =	-	V(Sc3≥Sc2) =	0.418	V(Sc4≥Sc2) =	0.285	V(Sc5≥Sc2) =	1.000

V(Sc1≥Sc3) =	1.000	V(Sc2≥Sc3) =	1.000	V(Sc3≥Sc3) =	-	V(Sc4≥Sc3) =	0.888	V(Sc5≥Sc3) =	0.556
V(Sc1≥Sc4) =	1.000	V(Sc2≥Sc4) =	1.000	V(Sc3≥Sc4) =	1.000	V(Sc4≥Sc4) =	-	V(Sc5≥Sc4) =	0.690
V(Sc1≥Sc5) =	1.000	V(Sc2≥Sc5) =	1.000	V(Sc3≥Sc5) =	1.000	V(Sc4≥Sc5) =	1.000	V(Sc5≥Sc5) =	-
V(Sc1≥Sc6) =	1.000	V(Sc2≥Sc6)=	1.000	V(Sc3≥Sc6) =	0.929	V(Sc4≥Sc6) =	0.810	V(Sc5≥Sc6) =	0.445
V(Sc1≥Sc7) =	1.000	V(Sc2≥Sc7)=	1.000	V(Sc3≥Sc7) =	1.000	V(Sc4≥Sc7) =	1.000	V(Sc5≥Sc7) =	0.876
V(Sc1≥Sc8) =	1.000	V(Sc2≥Sc8)=	1.000	V(Sc3≥Sc8) =	1.000	V(Sc4≥Sc8) =	1.000	V(Sc5≥Sc8) =	1.000
V(Sc1≥Sc9) =	1.000	V(Sc2≥Sc9)=	1.000	V(Sc3≥Sc9) =	1.000	V(Sc4≥Sc9) =	1.000	V(Sc5≥Sc9) =	1.000

V(Sc6≥Sc1)=	0.799	V(Sc7≥Sc1)=	0.480	V(Sc8≥Sc1)=	0.258	V(Sc9≥Sc1)=	0.309
V(Sc6≥Sc2)=	0.483	V(Sc7≥Sc2)=	0.120	V(Sc8≥Sc2)=	0.276	V(Sc9≥Sc2)=	0.359
V(Sc6≥Sc3)=	1.000	V(Sc7≥Sc3)=	0.735	V(Sc8≥Sc3)=	0.472	V(Sc9≥Sc3)=	0.556
V(Sc6≥Sc4)=	1.000	V(Sc7≥Sc4)=	0.852	V(Sc8≥Sc4)=	0.589	V(Sc9≥Sc4)=	0.690
V(Sc6≥Sc5)=	1.000	V(Sc7≥Sc5)=	1.000	V(Sc8≥Sc5)=	0.842	V(Sc9≥Sc5)=	1.000
V(Sc6≥Sc6)=	-	V(Sc7≥Sc6)=	0.646	V(Sc8≥Sc6)=	0.367	V(Sc9≥Sc6)=	0.445
V(Sc6≥Sc7)=	1.000	V(Sc7≥Sc7)=	-	V(Sc8≥Sc7)=	0.750	V(Sc9≥Sc7)=	0.876
V(Sc6≥Sc8)=	1.000	V(Sc7≥Sc8)=	1.000	V(Sc8≥Sc8)=	-	V(Sc9≥Sc8)=	1.000
V(Sc6≥Sc9)=	1.000	V(Sc7≥Sc9)=	1.000	V(Sc8≥Sc9)=	0.842	V(Sc9≥Sc9)=	-

Eq. 14 is used to calculate the priority weights:

d'(C1)=min(0.757,1.000,1.000,1.000,1.000,1.000,1.000,1.000)=0.757
d'(C2)=min(1.000,1.000,1.000,1.000,1.000,1.000,1.000,1.000)=1.000
d'(C3)=min(1.000,0.418,1.000,1.000,0.929,1.000,1.000,1.000)=0.418
d'(C4)=min(0.624,0.285,0.888,1.000,0.810,1.000,1.000,1.000)=0.285
d'(C5)=min(0.309,1.000,0.556,0.690,0.445,0.876,1.000,1.000)=0.309
d'(C6)=min(0.799,0.483,1.000,1.000,1.000,1.000,1.000,1.000)=0.483
d'(C7)=min(0.480,0.120,0.735,0.852,1.000,0.646,1.000,1.000)=0.120
d'(C8)=min(0.258,0.2760.472,0.589,0.842,0.367,0.750,0.842)=0.276
d'(C9)=min(0.309,0.359,0.556,0.690,1.000,0.445,0.876,1.000)=0.309

Finally, the priority weight was w'=(0.757,1,0.418,0.285,0.309,0.483,0.120,0.276,0.309).

9. Conclusion

In Information Security, user authentication is the most important and critical elements in this field of study. Researches dating from 1996 to 2011 has shown that a combination of geometrical shapes, patterns, textures and colors have higher chance of being memorized correctly compare to meaningless alpha-numeric characters. This makes graphical user authentication (GUA) the most desirable alternative to textual passwords. In order to select the best GUA algorithms based on issues related to security and their respective attributes, some arguments should be consider such as password spaces, password entropies and the strength and weakness to common attacks. To select the best GUA, this paper suggests the integration of Fuzzy AHP and Fuzzy TOPSIS. Fuzzy AHP can be used to determine the criteria weights and priority values of the GUA algorithms using the nine common security related attributes and issues. This method is very useful when evaluating complex multiple criteria alternatives that includes subjective and uncertain judgments. Meanwhile, the Fuzzy TOPSIS method is used to determine the rank of the GUA algorithms. It is a well known alternative ranking method suitable for multiple-criteria decision-making. The

combination of both Fuzzy AHP and Fuzzy TOPSIS gives the user and experts the capability to pick the best GUA algorithm that suits their purpose and requirements. In the future, other attributes such as usability can be studied and considered as part of the selection criteria for GUA algorithms.

REFERENCES

1. Lashkari, A.H. and F. Towhidi, *Graphical User Authentication (GUA)*. 2010: Lambert Academic Publisher.
2. Lashkari, A.H., et al., *Shoulder Surfing attack in graphical password authentication*. 2009, International Journal of Computer Science and Information Security (IJCSIS).
3. Lashkari, A.H., et al., *Security Evaluation for Graphical Password*, in *The International Conference on Digital Information and Communication Technology and its Applications (DICTAP2011)*. 2011, Communications in Computer and Information Science (CCIS) Series of Springer LNCS: Université de Bourgogne, France.
4. Saaty, T.L., *How to make a decision: The Analytic Hierarchy Process.* European Journal of Operational Research 1990. 48 p. 9-26.
5. Zadeh, L.A., *Fuzzy Set.* Information and Control, 1965. 8: p. 338-353.
6. Ates, N.Y., et al., *Multi Attribute Performance Evaluation Using a Hierarchical Fuzzy TOPSIS Method.* Springer StudFuzz 2006. 201: p. 537–572.
7. Saghafian, S. and S.R. Hejazi, *Multi-criteria Group Decision Making Using A Modified Fuzzy TOPSIS Procedure*, in *the 2005 International Conference on Computational Intelligence for Modelling, Control and Automation*. 2005, IEEE Computer Society.
8. Kahraman, C., et al., *Fuzzy Multi-Criteria Evaluation of Industrial Robotic Systems Using TOPSIS*. Springer Science + Business Media, LLC, 2008.
9. Chen, G. and T.T. Pham, *Fuzzy Sets, Fuzzy Logic, and Fuzzy Control Systems*. 2001: Florida: CRC Press.
10. Nguyen, H.T. and E.A. Walker, *A First Course in Fuzzy Logic*. 1997: CRC Press.
11. Klir, G.J. and B. Yuan, *Fuzzy Sets and Fuzzy Logic Theory and Applications*. 1995, New Jersey: Prentice Hall.
12. Zimmermann, H.-J., *Fuzzy Set Theory and its Applications*. Third Edition ed. 1996: Kluwer Academic Publishers.
13. Ballı, S. and S. Korukoğlu, *OPERATING SYSTEM SELECTION USING FUZZY AHP AND TOPSIS METHODS*. Mathematical and Computational Applications, 2009. 14(2): p. 119-130.
14. Wanga, Y.-J. and H.-S. Leeb, *Generalizing TOPSIS for fuzzy multiple-criteria group decision-making.* Elsevier Computers and Mathematics with Applications 2006. 53: p. 1762–1772.
15. Jian-wen, H., et al., *Study on the Application of Fuzzy TOPSIS to the Multi-objective Decision Making*, in *International Conference on Intelligent Computation Technology and Automation*. 2010, IEEE Computer Society.
16. Wang, Y.-M. and T.M.S. Elhag, *Fuzzy TOPSIS method based on alpha level sets with an application to bridge risk assessment.* Expert Systems with Applications, 2006. 31.
17. Kreng, V.B. and C.Y. Wu, *Evaluation of knowledge portal development tools using a fuzzy AHP approach: The case of Taiwanese stone industry.* European Journal of Operational Research, 2005.
18. Erensala, Y.C., T. Öncanb, and M.L. Demircan, *Determining key capabilities in technology management using fuzzy analytic hierarchy process: A case study of Turkey.* Information Sciences, 2006. 176(18): p. 2755-2770
19. Kahraman, C., U. Cebeci, and D. Ruan, *Multi-attribute comparison of catering service companies using fuzzy AHP: The case of Turkey.* International Journal of Production Economics, 2004. 87.
20. Leung, L.C. and D. Cao, *On consistency and ranking of alternatives in fuzzy AHP.* European Journal of Operational Research, 2000. 124: p. 102-113.
21. A.H. Lashkari, A.A.M., M. Masrom, S. M. Daud, *Security Evaluation for Graphical Password*, in *The International Conference on Digital Information and Communication Technology and its Applications (DICTAP2011)*. 2011, Communications in Computer and Information Science (CCIS) Series of Springer LNCS: Université de Bourgogne, France.