Structured Image Authentication System

Falah Mahdi Abduallh & Nidhal Ali Huseen

الملخص :

تؤثر بعض العوامل البشرية سلبا على الكثير من المنظومات الامنية ومن بينها ضمان هوية المستخدم ،هذه العوامل البشرية كالاتي : اولها بطء الانسان وعدم الاعتماد عليه في معالجة ومقارنة حزم كلمات السر الطويلة وغيرذات المعنى ، وثانيا محدودية ذاكرة الانسان في تذكر كلمات السر أو الرقم الشخصي ،فالحزم العشوائية الطويلة صعبة التذكر على العكس من الصور فهي سهلة التذكر لدى الانسان.

يتناول هذا البحث نقاط الضعف الاساسية في نظم التحقق ،ودراسة كيفية استخدامها وامنية هذه النظم وكيفية تحسينها باستخدام تقنية الاعتماد على الصور بدلا من الحزم الابجدية ،وكذلك دراسة متطلبات المستخدم فيما يخص الحزم ، خصوصا حاجته مرارا وتكرارا للتحقق من سلامة البيانات ،حيث يمكن للمستخدم ان يتذكر بسهولة الصور التي تم إنشاؤها.

من خلال هذه التقنية سترتفع امنية النظم لاعتمادها على الادراك (التمييز) المبني على اساس ضمان التحقق ،حيث يتم التأكد من هوية المستخدم بواسطة تمييزه لصور قد رأها سابقا فهي اكثر اعتمادية واسهل استخدام من تقنية الاسترجاع التقليدية ، علاوة على ذلك امتلاكها لميزة منع المستخدمين من اختيار كلمات سر ضعيفة وتقلل كثيرا من الصعوبات في كتابة كلمات السر أو مشاركتها مع الآخرين.

Abstract

Some of human factors negatively affect many security systems, including the security of user authentication. These human factors are: first, people are slow and unreliable at processing and comparing

long meaningless password string; and second, people have limitation difficulties in remembering secure passwords or Personal Identification Number (PIN). Long random strings are difficult to remember, while it is much easier for people to deal with images instead of meaningless strings.

In this paper, fundamental weaknesses of knowledge - based authentication schemes are addressed. Then we have investigated how the usability and security of the authentication systems can be improved using hash visualization technique that replaces alphabetical string with structured images. We also examine the requirements of user particularly useful in strings, where people need to repeatedly verify the integrity of data, because people can easily remember the generated images.

This approach improves the security, since it relies on the recognition - based authentication. It authenticates a user through recognizing the previously seen images. It is more reliable and easier to use than the traditional recall - based schemes. Furthermore, it has the advantage that it prevents users from choosing weak passwords and limited the difficulties to write down the passwords or sharing them with others.

Keywords :

User authentication hash visualization, human factors, password authentication system . genetic programming, structured images.

1. Introduction

User authentication is the necessary foundation for all computer and data security. It is a central component of currently deployed security infrastructures. Several secure technologies have evolved to offer ways for a computer to authenticate that a specific electronic identity (an on-line personal) actually represent the human being who was originally assigned

specific rights and authority by a trusted administrator. There are three types of information that a computer can usefully process to independently authenticate, that a person at a remote terminal is. In fact, whom he or she claims to be. These are typically referred to as the "Three Factors of Identification"[1]

i. **"Something known"**:- evidence that a person knows a secret (e.g, a memorized password) that has been given to a specific person.

ii. **"Something hold"**:- evidence that the person holds a token (e.g.. a credit card, or an Automatic Teller Machine (ATM) card) that is given to a specific person.

iii. "Something one is":- a biometrics: some human attribute, difficult to counterfeit. It can be scanned and digitally documented (e.g.. a fingerprint or retina scan) so that it can be compared to previously recorded scan , taken from a specific person [1].

Depending on these information , user authentication can be distinguished into three main techniques:

a. **knowledge - based system (password authentication)** which relies upon comparing the newly presented password with the original password stored in the computer. As a password is secret, they must be enciphered before sending via transmission channels [2].
b. **Token – based system (token authentication)** is based on possession of some object that is combined with password [3]. It also called two - factor authentication because it is require at least two of three primary factors to use to authenticate an individual [1]. Token authentication system comes in different forms. The credit card is the most popular, and the ATM card that

needs the memorized password (PIN) [1] . There are another forms for token authentication, it may be hand-held calculator, diskette like cartridges, modems and so on.

c. **Biometrics - based system (biometrics authentication)** is based on physical features such as fingerprint, retina, iris, hand or face Although voice and signature identification do not involve physical characteristics, they are usually included with biometrics user authentication [4].

In today's security systems, knowledge-based schemes are predominantly used for user authentication because of these reasons [5] :

First, although biometrics can be useful for user identification, one problem with these systems is the difficult tradeoff between imposter pass rate and false rate. In addition, many biometrics systems require specialized devices, and some can be unpleasant to use [5].

Second, most token authentication systems also use knowledge-based authentication to prevent impersonation through theft or loss of the token. An example is ATM authentication, which requires a combination of token (a bankcard) and secret PIN [5].

2. Shortcomings of Password Authentication:-

Despite of their wide usage, passwords and PINs have a number of shortcomings. The problem in user authentication is that people have difficulties with choosing and memorizing secure passwords and personal identification numbers (PIN) [6]. Most security system still suffer from the fact they fail to account for human factors. Humans are slow and unreliable at processing long and meaningless strings, yet many security applications depend on this skill. These

humans' factors negatively affect many security systems, including the security of user authentication. Passwords and PINs have number of shortcoming [5, 6]:

a. The main weakness of knowledge-based system authentication is that it relies on precise recall of the secret information. If the user makes a small error in entering the secret information, the authentication fails. Unfortunately, precise recall is not a strong point of human cognition.

b. Simple meaningful passwords or that associated with the user are easier to remember, but are vulnerable to attack.

c. Password that are complex and arbitrary are more secure, but difficult to remember. The user tend to write them down. This compromises security since the user might forget, lose or leave the paper in insecure place.

d. the numbers of applications and services, which require password, have dramatically increased. Since users can only remember a limited number of passwords, the will use similar or even identical passwords for different purposes. All options increase the chance of a security compromise.

3. The Proposed Solution

In fact, classic cognitive science experiments show that humans have a vast and limitless memory for pictures in particular. The experiments show that humans can remember and recognize hundreds to thousands of pictures in fractions of a second.

Therefore by replacing prices recall of the password with image recognition, the user cognitive load can be minimized, and the mistakes done by the users can be minimized.

Our approach is to explore the user authentication aspects more thoroughly , and design a prototype system that perform and improve user authentication using image. In particular, we aim to satisfy the following requirements:

1. The system should be based on image recognition, to make the authentication task more reliable and easier for the users.
2. The system should prevent users from choosing weak passwords.
3. The system should make it difficult to write passwords down and to share them with others.

To explore these requirements and improve the security of these systems, we propose new **Hash Visualization technique** which is also called **Random Image Generation (RIG)**, that is based on a cognitive science.

3.1. Random Image Generation (RIG)

RIG is a technique that coverts alphabetical string into corresponding structured image. It is based on the idea of the **Random Art technique**, which is developed by Andrej Bauer [9]. The RIG technique consists of four components. Figure (1) shows the block diagram of RIG method.

All the images in the RIG are described by a formula. The computer generates a random formula depending on **the genetic algorithm for developing software (GADS)** and draws the corresponding structured image.

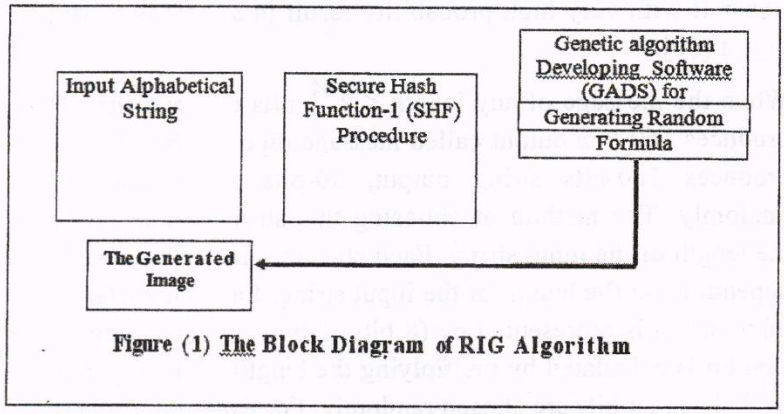


Figure (1) The Block Diagram of RIG Algorithm

3.1.2 Secure Hash Function (SHF)

A One-way hash function is a function, mathematical or otherwise, that takes a variable-length-input string (called pre-image] and converts it to a fixed-length (generally smaller) output string (called a hash value) [11]. One important type of one-way hash function is Secure Hash function (SHF) is found to be SHF-1 [10].

Hash visualization needs to satisfy the near one-way requirements of hash visualization. It is achieved by hashing the input during with SHF-1 to seed a cryptographically secure random number generator. Hence, we can achieve the pre-image resistance property. SHF-1 procedure is used in the RIG in order to make it one-way technique and to find two different strings, which generate the same image. Any change in a string in

transmit with very high probability result in a different message digest [10].

When the message of any length $< 2^{64}$ bits is input, the SHF-1 produces 160-bits output called message digest. After the SHF-1 produces 160-bits string output, 30-bits string are chosen randomly. The method of choosing this string is depending on the length of the input string. Each character in the input string is depending on the length of the input string. Each character in the input string is represented by (8 bits) 1-byte. The position of the first bit is calculated by multiplying the length of the input string by 8. The rest bits are chosen randomly. For example, if the input string is "My Mother", the length of this string is 9, each character is represented by 8 bits. The position of the first bit is at position 72, which forms the output SHF-1 and the rest bits are chosen randomly. Then the 30-bit string is divided into three 10-bit strings for red seed, green seed and blue seed. Each one of these seeds is input GADS to produce the expression formula for red, green and blue. Figure 2 shows the method of choosing the red. green and blue seeds.

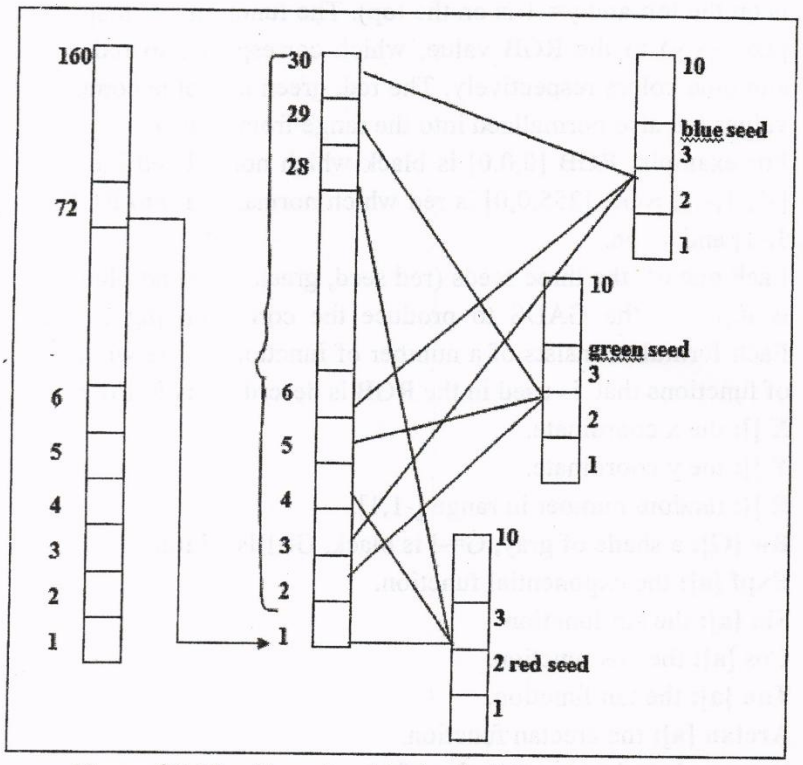


Figure (2) The Choosing Method of the Three Seeds.

3.1.3 Genetic Algorithm Developing Software (GADS)

The binary string is input as a seed for a random number generator. The randomness is used to construct a random expression, which describes a function that generates the image, mapping each image pixel to a color value. For each image the x and y coordinates are normalized between -1 and 1. (where x=-1

is on the left and y=-1 is on the top). The function "F" maps each pixel (x,y) to the RGB value, which corresponds to red, green and blue colors respectively. The red, green and blue component values are also normalized into the range from -1 to 1.

For example, RGB [0,0,0] is black which normalized into RGB [-1,-1,-1], RGR [255,0,0] is red which normalized into RGB [1,-1,-1] and so on.

Each one of the three seeds (red seed, green seed and blue seed) is input to the GADS to produce the corresponding formula. Each formula consists of a number of functions. The whole list of functions that is used in the RGB is described as follows:

X []: the x coordinate.

Y []: the y coordinate.

R []: random number in range [-1,1].

Bw [G]: a shade of gray, G=-l is black, G=1 is white.

Expf [a]: the exponential function.

Sin [a]: the sin function.

Cos [a]: the cos function.

Tan [a]: the tan function.

Arctan [a]: the arectan function.

Reverse [a]: the reverse color of a.

Add [a,b]: the sum of two colors.

Mult [a,b]: the product of two colors.

Div [a,b]: the division of two colors.

RGB [r,g,b]: a color specified by the RGB component.

If [cond,T, E]: the "if-then-else" function: if cond is positive, then the value is T, else the value is E.

Mix [a, b, c, d]: is the mixing of two color depending on the values c and d.

To generate a structured image, each of the three seeds (red, green and blue) is used as a seed to the random number generator and the randomness would construct the random mathematical formula, which defines the color value for each pixel on the image plane. Each random number, which is generated by the pseudo random number generator, is replaced by the corresponding production rule that is selected from the set of grammar rules.. as they are shown in figure (3).

0-	<Exp>::=	<Input>
1-	<Exp>::=	<operation>
2-	<Input>::=	X
3-	<Input>::=	Y
4-	<Input>::=	R
5-	<operation>::=	Add(<Exp, <Exp>)
6-	<operation>::=	Mult(<Exp, <Exp>)
7-	<operation>::=	Div(<Exp, <Exp>)
8-	<operation>::=	Mod(<Exp, <Exp>)
9-	<operation>::=	Sin(<Exp >)
10-	<operation>::=	Tan(<Exp >)
11-	<operation>::=	Arctan(<Exp >)
12-	<operation>::=	Cos(<Exp >)
13-	<operation>::=	Reverse(<Exp >)
14-	<operation>::=	Bw(<Exp >)
15-	<operation>::=	Expf(<Exp >)
16-	<operation>::=	Rgb(<Exp >, <Exp >,<Exp >)
17-	<operation>::=	If(<Exp >, <Exp >,<Exp >)
18-	<operation>::=	Mix (<Exp >, <Exp >,<Exp >)

Figure (3) The Set of Grammar Rules.

The method of randomly generating the formula is based on the initial population and ontogenic mapping of the GADS. We first review the initial population and ontogenic mapping of the **genetic algorithm developing software** and then discuss the new GADS that is used in our technique.

3.1.3.1 GADS

GADS is an implementation of genetic programming technique, where the genotype (genetic search space element i.e. chromosome) is distinct from the phenotype (solution space element i.e. program). The GADS genotype is a list of integers that represent the production in syntax. It is used to generate the phenotype, which is defined by the syntax [8]. The mapping from genotype to phenotype is called **onogenic mapping .**

In GADS, each gene in the initial population is generated as a random number, which is distributed uniformly over the range [0..n]. the production rules are numbered from 0 to n, so that any production rule can be represented by the number in the range [0..n]. as the set of rules is show in figure (4).

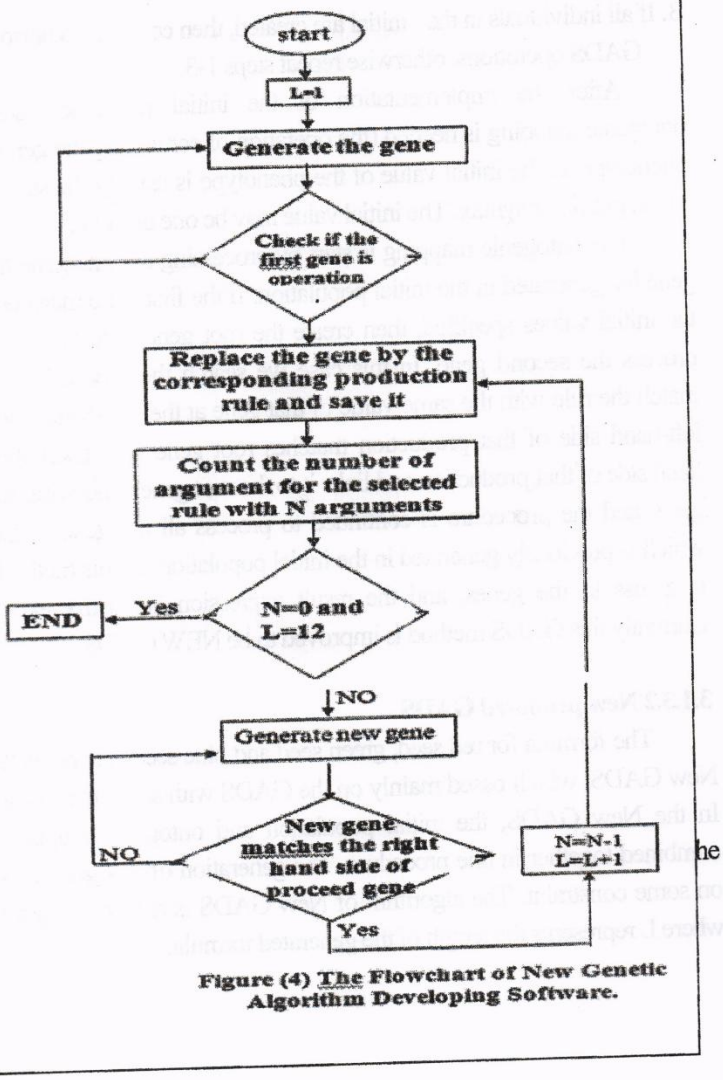


Figure (4) The Flowchart of New Genetic Algorithm Developing Software.

2. Repeat step 1 until the number the gene of that individual reaches the pre specified length.
3. If all individuals in the initial are created, then continue to perform other GADS operations, otherwise repeat steps 1-3.

After the implementation of the initial population steps, the ontogenic mapping is needed (the operation of converting the genotype to phenotype). The initial value of the phenotype is usually the start symbol of the grammar syntax. The initial value may be one or more.

The ontogenic mapping is start by processing the first gene from the gene list generated in the initial population. If the first gene matches one of the initial values specified, then create the root gene. After that, begin to process the second gene. In this case we search the production rules to match the rule with the same value of that gene at the left -hand side. If the left-hand side of that production matches root gene then takes the right-hand side of that production and links it to the root gene, otherwise, skip that gene, and the procedure is continued to process all the gene in the list , which is previously generated in the initial population. In this method, there is a loss in the genes, and the result expression is postfix expression. Currently this GADS method is improved to be NEW GADS.

3.1.3.2 New proposed GADS

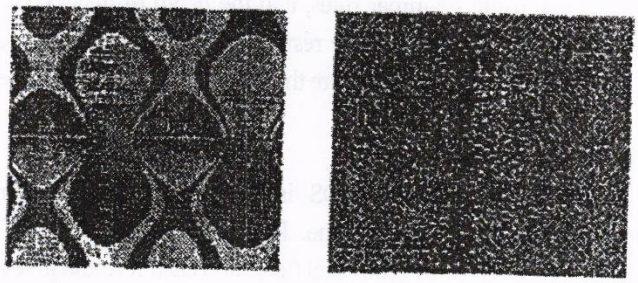
The formula for red seed, green seed and blue seed is constructed by New GADS, which based mainly on the GADS with some modifications. In the New GADS, the initial population and ontogenic mapping are combined together in one procedure. The generation of any gene depends on some constraint. The algorithm of New GADS is shown in figure (4), where L represents the length of the generated formula.

The random formula can be represented as an expression tree, which is generated using grammar rules, and the depth of generated expression tree can be 12. In addition, the resulted formula for red, green and blue seeds is a prefix expression, where the operation proceeds the operator.

3.1.4 Generated Image

The result of NEW GADS is three random formulas; one for red, one for green, and one for blue. In this procedure, each of the three formulas is evaluated to get a pixel (x, y) and each formula gives one result value (color value). Red formula represents the intensity for red color. Green formula represents the intensity of green color. Blue formula represents the intensity for blue color. The red, green and blue colors will mix to produce one value that represents the color for that pixel. This operation repeated for all pixels in the two- dimensional image and generates the final colored image.

The four above procedures will generate the random colored image corresponding to the given alphabetical string. The image in figure (5) is generated by new R/G and the corresponding expression tree is of depth 12, where the input string is " **user authentication** ". The corresponding three formula for the image in figure (5a) are:



(a) The Generated Image. (b) Frequency spectrum

Figure 5: Example of image generated by RIG.

Red formula=div(bw(add(mix(sin(if(arctan(expf(mult(div(rgb(y[ ],r,x[ ]), rgb(x[ ],x[ ],r)),bw(y[ ]))),bw(y[ ])),tan(y[ ]))),arctan(r),r,cos(y[ ]),sin(x[ ]))),mix(y[ ],r,y[ ],y[ ])).

Green formula=tan(mod(miilt(mod(mix(div(bw(tan(add(arctan(mult(Arctan(bw(r)),bw(x[ ]))),rgb(r,y[ ],y[ ]))))),y[ ]),add(y[ ],x[ ]),y[ ],x[ ]), add(x[ ],x[ ])),add(y[ ],y[ ]),bw(y[ ]))).

Blue formula=mod(sin)arctan(mix(mult(bw(div(mix(cos(if(tan(expf(expf(y[ ]))mod(y[ ],x[ ]),mult(r,r))),x[ ],y[ ],cos(x[ ],y[ ],cos(x[])),r)) ,mult(y[ ],r),reverse(r),mult(y[ ],x[ ]),bw(x[ ]))))),reverse(x[ ])).

4. Testing for the generated images

Every image generated by RIG must be tested before using the user authentication system. The test includes test image regularity, image complexity, and the entropy (the amount of the regularity property):-

4.1 The Regular Property

Humans are good at identifying geometric objects (such as circles, rectangles, triangles, and lines), and shapes in general. We call images, which contain mostly recognizable shapes, regular image. If an image is not regular. i.e. does not contain identifiable objects or patterns, or is too chaotic (such as white noise), it is difficult for humans to compare or recall it [9].

Non- regular images tend to have wide frequency spectra. Noisy images contain a high percentage of the energy in high frequencies. Hence we can transform an image to the Fourier domain and compute the magnitude spectrum. If the magnitude spectrum does not have too much energy in the high frequencies, then the image is regular [9]. The figure (5b) shows the frequency spectrum for the image.

4.2 The complexity Property

An immediate of tins property is that an image can not be too simplistic in shapes and patterns, or rely on subtle color differences. Just like for to the regularity property, we could use the frequency spectrum to detect images that are simplistic. For example, the frequency spectrum to detect images that are simplistic. For lowest frequency components [9].

4.3 The Entropy Property

It is the average of information in an image. The entropy for an NxN image can be calculated by the equation [12]:

$$\text{Entropy} = -\sum_{i=0}^{l-1} pi * \log_2(pi) - \quad \ldots (1)$$

Where pi= the probability of the i_{th} gray level = N_k / N^2.

N_k = the total number of pixels with gray value k.

L= the total number of gray level (e.g., 256 for 8 bits)

5. System Hierarchy

We have proposed **structured image authentication system** for user authentication. This system is based on the observation that people are extremely good at pointing out which images they have been seen [13] previously. The **structured image authentication system** consists of three levels each one contains 10 images. The user must determine three specific images to be his password images. The system use the tested images stored in special database. This database is divide into two parts, one for the password images to be selected by the user at the log on stage and it is called **password database**. And the other for the system levels at the processing of the system after logging on and it is called **level database**.

So the user must first select five images from the password database. To authenticate the user, the system presents three levels, each contains 10 images all of them from the level database except one from the selected five images. The user must first correctly identify the image in the three levels.

The **structured image authentication system** has two phases:

1. Choosing the Password Images Phase

In this phase, the user chooses only five images out of the sixteen-presented images, to be considered as the password of our system. The user can choose the five images at the log on stage.

The type of used images has a strong influence on the security of the system. For example, if the system were based on photographs, it would be easy for users to pick predictable levels, to describe their levels images. Write down this information, and share it with others. For this reason, we prefer to use the RIG

2. Authentication Phase

At authentication phase, the system has three hierarchical levels to strengthen the degree of security. Each level consists of 10 images from the level database and one of these images is from the password image, which the user must memorize and recognize it. At this stage, the user can point out three images, one at each level. If the user correctly identifies the entire password image in each level. The user is authenticated.

Suppose the chosen password images are M images and that for authentication the system shows N*3>M images because there are three levels. This gives :

$$\binom{N}{M} = \frac{N!}{(N-M)! * M!} \quad \text{combinations} \quad \ldots (2)$$

In our system M=5 and N=10 in each level. By evaluating the above equation, the number of combination will be 142506.

$$\binom{30}{5} = 142506 \text{ combinations.}$$

All the images in the database are tested to ensure that no weakness are use in this authentication system.

6. Conclusions and Future Work

Since people are much better at recognizing previously seen images than at precisely recalling pass phrases from memory, we employ a recognition-based approach for authentication. In this paper, we proposed new system for authentication in which we replace the precise recall of pass phrases with the recognition of previously seen images. This system has the advantage that the authentication task is more reliable, easier and fun to use. In addition, the system test each image used in it. This test includes the Fourier analyses and the entropy function. So the system prevents user from choosing weak passwords and makes it difficult for users to write passwords down and to communicate them to other.

Many improvements can be made to strengthen the system against and improve its usability. We are also thinking about is another user authentication system, which may combine the traditional password scheme and RIG user authentication.

References

1. Http://www.oga.co.th/syncom/secured/Resource/FAGs/index.htm.
2. Seberry. J. and Pieprzyk. J, "Cryptography, an introduction to computer security", Prentice hall of Australia ptd, ttd, 1989.
3. internet Communication "Authentication, hash function and digital signature. http://www.adfa.edu.ou.htm.
4. Http://www.dell.cz/biometrics user authentication. Htm.
5. Dhamija, R,and Perrig, A., "Deja vu: A User Study using Image for Authentication".
6. Dhamija, R., "Hash Visualization in User Authentication".
7. Perrig, a., and Song, D., "Hash Visualization : A new Technique to improve Real-word security".
8. Shaker, R., "New developments in genetic algorithm for developing software". MSc. Thesis, University of technology, Baghdad, 2000.
9. Andrej Bauer. "Gallery of random art" http:/ www.cs.cmu.cdu/-andrej/art/1998.
10. F1BSPUBISO-1, Superseds, "Secure Hash standard", Http:www.itl.nist.gov/div897/pubs/Fip. 180-l.htm.
11. Schneier, B. "Applied cryptography".John Wiley & Sons, 1996
12. Scott E Umbaugh, "Computer Vision and Image Processing" . A Simon and Scguster. 1998.
13. Kenneth R. Boff, liod Kaufman, and James p. Thomas. "Handbook of Perceptio and human performance", John wily and Sons. 1989.