Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2012, Article ID 340861, 16 pages
doi:10.1155/2012/340861

Research Article

Password Authentication Based on Fractal Coding Scheme

Nadia M. G. Al-Saidi,[1] Mohamad Rushdan Md. Said,[2] and Wan Ainun M. Othman[3]

[1] *The Branch of Applied Mathematics Applied Sciences Department, University of Technology, Baghdad, Iraq*
[2] *Institute for Mathematical Research (INSPEM), University Putra Malaysia, Darul Ehsan, 43400 Serdang, Malaysia*
[3] *Institute of Mathematical Sciences, University of Malaya, 50603 Kula Lampur, Malaysia*

Correspondence should be addressed to Nadia M. G. Al-Saidi, nadiamg08@gmail.com

Received 15 April 2012; Revised 10 September 2012; Accepted 11 October 2012

Academic Editor: Marcelo A. Savi

Password authentication is a mechanism used to authenticate user identity over insecure communication channel. In this paper, a new method to improve the security of password authentication is proposed. It is based on the compression capability of the fractal image coding to provide an authorized user a secure access to registration and login process. In the proposed scheme, a hashed password string is generated and encrypted to be captured together with the user identity using text to image mechanisms. The advantage of fractal image coding is to be used to securely send the compressed image data through a nonsecured communication channel to the server. The verification of client information with the database system is achieved in the server to authenticate the legal user. The encrypted hashed password in the decoded fractal image is recognized using optical character recognition. The authentication process is performed after a successful verification of the client identity by comparing the decrypted hashed password with those which was stored in the database system. The system is analyzed and discussed from the attacker's viewpoint. A security comparison is performed to show that the proposed scheme provides an essential security requirement, while their efficiency makes it easier to be applied alone or in hybrid with other security methods. Computer simulation and statistical analysis are presented.

1. Introduction

Passwords have been present in information technology since the earliest days before the age of the PC. Using consumer password recovery software, the eight character password can be cracked in under an hour. More experienced hackers can crack 14 character password including alpha-numeric with special characters by using rainbow table and some free tools

in less than three minutes. So adding numeric and other characters does not mean adding some level of protection but may increase the time needed [1].

In a client/server system scenario, password-based authentication schemes play crucial role to identify the validity of a remote user to maintain user's information and make it more difficult to have unauthorized access to restricted resources. The first remote authentication scheme was introduced in 1981 by Lamport [2]. He proposed a password authentication scheme that was based on password tables to authenticate legitimate user over insecure channel. Since then, many password-based authentication schemes were proposed and analyzed to improve the security, efficiency, or cost [3–7]. Traditional alphanumeric passwords are widely used for authentication. In these schemes, the security of the remote user authentication is based on the password only. Simple passwords can be easily obtained by an attacker given enough attempts and time. There is always a threat due to the availability of simple, rapid, and perfect duplication and distribution means using simple dictionary attacks. Given the explosive growth of internet and the exponential increase in computer performance that facilitated the exchange of multimedia information, there is a necessity to invent new protection mechanisms to maintain user information. Many emerging methods have been designed today to solve this problem, some of them are biometric-based remote user authentication which is considered as a secure and reliable method compared to traditional one, but they are more costly and require specialized hardware, such as those proposed by Lee et al. [8]. The others are based on one time password by using smart cards, for example those proposed by Hwang and Li [4] in 2000 and many others. Wang et al. [9] applied FIC scheme to refine characteristic values of a specific image and embed them into the LSB of pixels in the image. The system has the ability to detect and restore the tampered images decoding process of the FIC. In 2007, E. J. Yoon and K. Y. Yoon [10] proposed an efficient chaotic hash based fingerprint biometric remote user authentication scheme on mobile devices. In 2011, Motýl and Jašek [11] proposed advanced user authentication process based on the principles of fractal geometry. The system is based on polynomial fractal sets, specifically the Mandelbrot set. The system meets all the conditions for the construction of hash functions.

In this paper we propose a new password authentication scheme based on fractal image coding scheme. Its properties are addressed and its security is analyzed and compared to some of the aforementioned methods by Lamport [2], Hwang and Li [4], and Lee et al. [8].

The fractals theory is a new discipline that offers a new method to research the self-similarity objects and irregular phenomena. It is an active branch of nonlinear science starting from the 1970s. Fractal has proven to be suitable in many fields and particularly interesting in various applications of image processing. Some phenomena which cannot be explained with Euclidean geometry could be interpreted with fractal geometry. Fractal theory and its methodology provides people with a new view and new ideas to know the world, and it makes our way of thinking enter into the nonlinear stage. First important advances are due to Barnsley et al. [12, 13], who introduced for the first time the term "Iterated Function Systems (IFSs)" based on the self-similarity of fractal sets. Barnsley's work assumes that many objects can be closely approximated by self-similarity objects that might be generated by use of IFS simple transformations. From this assumption, the IFS can be seen as a relationship between the whole image and its parts, the main problem being how to find these transformations (the IFSs) [14]. There is, in fact, a version of the IFS theory, the Local Iterated Function Systems theory that minimizes the problem by stating that the image parts do not need to resemble the whole image but it is sufficient for them to be similar to some other bigger parts

in it. It was Jacquin [15], who developed an algorithm to automate the way to find a set of transformations, providing good quality to the decoded images.

The outline of the paper is organized as follows: the theoretical concepts of fractal image coding are explained in Section 2, while a brief explanation of the methodology is provided in Section 3. The core of this paper is Section 4, which discusses the algorithm. In Section 5, the experimental results are described. Section 6, analyzes the security and evaluates the efficiency of the proposed scheme, while a security comparison between the proposed scheme and other password authentication scheme are presented in Section 7, followed by a brief conclusion in Section 8.

2. The Fractal Theory

With the exponential development in the field of multimedia systems, the need for storing images in less memory leads to a direct reduction in storage cost and faster data transmissions. Fractal Image coding is a mathematical process used to encode bitmaps containing a real-world image as a set of mathematical data that describes the fractal properties of the image. Most data contains amount of redundancy, which can be removed from storage and replaced for recovery [16]. Based on this reality and on Bernsley's assumption, many objects can be closely approximated by self-similarity objects which might be generated by use of IFS, where the IFS can be seen as a transformation between the whole and its parts, the fractal image coding evolved. Hence, the main problem that arises is how to find these IFS transformation. It was Jacquin [15] who solved this problem by developing an algorithm to automate the way to find these transformation based on the fact that different parts of the image at different scales are similar and on the assumption that the image parts do not need to resemble the whole image, but it is sufficient for them to be similar to some other bigger parts in it. Using these advantages, the FIC became an inspiration for solving several techniques whose main characteristic is the use of the similarity property in image block [17].

2.1. Mathematics for Fractal Image Coding

The main idea of fractal image coder is to determine a set of contractive IFS transformation to approximate each block of the image to generate the whole image. Some background for fractal theory to understand the IFS and FIC are given as follows. A more detailed review of the topics can be found in [18–20].

Definition 2.1. Given a metric space (X, d), the space of all nonempty compact subset of X is called the Hausdorff space $H(X)$. The Hausdorff distance h is defined on $H(X)$ by

$$h(A, B) = \max\{\inf\{\varepsilon > 0;\ B \subset N_\varepsilon(A)\}, \inf\{\varepsilon > 0;\ A \subset N_\varepsilon(B)\}\}. \tag{2.1}$$

Definition 2.2. For any two metric spaces (X, d_X) and (Y, d_Y), a transformation $w : X \to Y$ is said to be a contraction if and only if there exists a real number s, $0 \leq s \leq 1$, such that $d_Y(w(x_i), w(x_j)) < s d_X(x_i, x_j)$, for any $x_i, x_j \in X$, where s is the contractivity factor for w.

Theorem 2.3 (Fundamental Theorem of Iterated Function Systems). *For any IFS $w = \{w_i\}, i = 1, \ldots N$ there exists a unique nonempty compact set $A \in R^n$ the invariant attractor of the IFS, such that $A = w(A)$.*

Another important property (Theorem 2.4) of contractive transformations of a complete metric space within itself is known as the contraction mapping theorem.

Theorem 2.4. *Let $w : X \to Y$ be a contraction on a complete metric space (X, d). Then, there exists a unique point $x_f \in X$ such that $w(x_f) = x_f$. Furthermore, for any $x \in X$, we have $\lim_{n\to\infty} W^{\circ n}(x) = x_f$, where $w^{\circ n}$ denotes the n-fold composition of w.*

Definition 2.5. Any affine transformation $w : R^2 \to R^2$ of the plane has the following form:

$$\begin{pmatrix} u \\ v \end{pmatrix} = W\begin{bmatrix} x \\ y \end{bmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix} = A\vec{X} + b, \qquad (u, v), (x, y) \in R^2. \tag{2.2}$$

By considering a metric space (X, d) and a finite set of contractive transformation $w_n : X \to X, 1 \le n \le N$, with respective contractivity factors s_n, we proceed to define a transformation $W : H(X) \to H(X)$, where $H(X)$ is the collection of nonempty, compact subsets of X, by

$$A = W(A) = \bigcup_{i=1}^{N} w_i(B) \quad \text{for any } B \in H(X). \tag{2.3}$$

It is easily shown that W is a contraction, with contractivity factor $s = \max_{1\le n\le N} sn$. The mapping W is usually referred to as *Hutchinson operator*. It follows from the contraction mapping theorem that, if (X, d) is complete, W has a unique fixed point $A \in H(X)$, satisfying the remarkable self-covering condition:

$$A = W(A) = \bigcup_{i=1}^{N} w_i(A). \tag{2.4}$$

However, given a set M, how can one find a contractive transformation W such that its attractor A is close to M? To answer this question we have to apply the *Collage Theorem.*

Theorem 2.6. *For a set M and a contraction W with attractor A:*

$$h(M, A) \le \frac{h(M, W(M))}{1 - s}, \tag{2.5}$$

where h is the Hausdorff Distance.

That is to say, M and A are sufficiently close, if M and $W(M)$ are made close enough in terms of w_i, and combe the following two expressions:

$$W(M) = M, \tag{2.6}$$

where,

$$W(M) = \bigcup_{i=1}^{N} w_i(M), \tag{2.7}$$

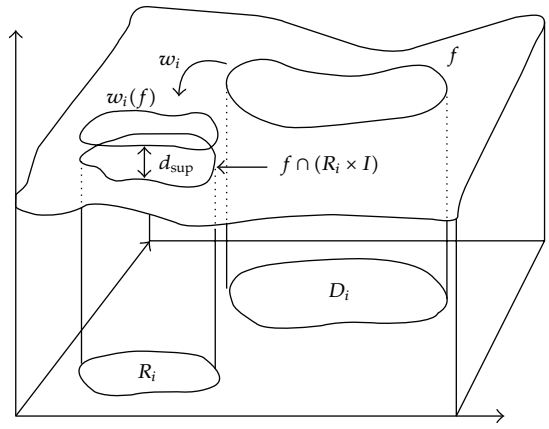


Figure 1: Domain and range illustration.

which implies

$$\bigcup_{i=1}^{N} w_i(M) \approx M. \tag{2.8}$$

M can be partitioned as: $M = \bigcup_{i=1}^{N} m_i$ and m_i can be closely approximated by applying a contractive affine transformation w_i on the whole M, where, $m_i = w_i(M)$.

2.2. Fractal Image Coding

The goal of FIC is to be able to store an image as a set of IFS transformation instead of storing individual pixel data. We use a type of transformation called Partition Iterated Function System (PIFS), because we work on a section of the image instead of the whole image. The process of encoding the image M requires us to find a collection of contractive maps $w_1, w_2, \ldots, w_n$ with $W = \cup w_i$ and M as the fixed point (or attractor) of the map W. The fixed-point equation $M = W(M) = w_1(M) \cup w_2(M) \cup \cdots \cup w_n$ suggests that we partition M into pieces to which we apply the transforms w_i to get back the original image M [21]. Let the metric space of a digital image be set by the pair (μ, rms), where rms is the root mean square metric instead of the Hausdorff metric discussed above to compress the image $M \in \mu$. It is necessary to find $W : \mu \to \mu$, such that $\text{rms}(M, W(M) \cong 0$. This metric space is determined by partitioning the original image M into a set R of nonoverlapping range blocks that cover M and a set D of overlapping domain block that has twice the side of the range blocks and must intersect M. The aim of FIC is to enable the collage theorem find the set of IFS transformation W for the image M whose attractor looks like M. This theorem allows also for the scaling factor in addition to rotations and reflections.

The question now, is how do we map domains to ranges? To find the corresponding domain block for each range block, we have to test all the domain blocks. After we find the optimized domain that minimize the rms distance, the coordinate of domain pixels will be recorded in the compressed file. The illustration of "Domain" and "Range" can be shown in Figure 1.

Every pixel in the blocks is represented as a point P with the coordinates (X, Y, Z), where X and Y represent the standard geometric position of P. The gray level of P is represented by the Z-coordinate. To include the gray scale value 3-dimentional matrix is used. The transformations are specified by

$$w_i \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} a_i & b_i & 0 \\ c_i & d_i & 0 \\ 0 & 0 & s_i \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} e_i \\ f_i \\ o_i \end{bmatrix}, \tag{2.9}$$

where a, b, c, d, e, and f represent the scaling, rotation, reflection, and translation parameters, and the gray scale is controlled by $m(Z) = S \cdot Z + O$, where S is the contrast and O is the brightness. The distance that we need to minimize is the distance between the gray scale levels. S and O can be computed using the least squares regression:

$$R_{\text{lsr}} = \sum_{i=1}^{n} (s \cdot a_i + o - b_i)^2. \tag{2.10}$$

The minimum of R_{lsr} occurs when the partial derivatives with respect to S and O are zero, which result in

$$S = \frac{\left[n \sum_{i=1}^{n} a_i b_i - \sum_{i=1}^{n} a_i \sum_{i=1}^{n} b_i\right]}{\left[n \sum_{i=1}^{n} {a_i}^2 - \left(\sum_{i=1}^{n} a_i\right)^2\right]}, \tag{2.11}$$

$$O = \frac{1}{n}\left[\sum_{i=1}^{n} b_i - s \sum_{i=1}^{n} a_i\right]. \tag{2.12}$$

The rms difference is calculated using

$$R_{\text{lsr}} = \frac{1}{n}\left[\sum_{i=1}^{n} b_i^2 - s\left(s \sum_{i=1}^{n} a_i^2 - 2 \sum_{i=1}^{n} a_i\, b_i + 2o \sum_{i=1}^{n} a_i\right) + o\left(no - 2 \sum_{i=1}^{n} b_i\right)\right]. \tag{2.13}$$

Each range block is compared to all possible transformed domain blocks by calculating R_{lsr} to choose the one that minimizes R_{lsr}.

The decoding process is much simpler and (starting with an initial image M_0—usually a uniform grey or white image) can be achieved by iterating through the collection of maps. On the first iteration, $M_1 = W(M_0)$, and on the second iteration, $M_2 = W(M_1) = W(W(M_0))$, and so forth. This process can be repeated until the attractor resembles the original image.

3. Material and Methods

A message authentication code is a method by which two parties who share a common secret key can exchange messages in an authenticated manner; namely, they can detect modifications or fabrications by an unauthorized third party. The shared common key between the two parties is usually chosen uniformly at random from the set of all possible keys [22].

3.1. Diffie–Hellman

Diffie–Hellman (DH) is a key-agreement algorithm invented by Diffie and Hellman [23], involving exponentiation modulo a large prime number. It can be used for key exchange to generate a secret key, but it cannot be used to encrypt and decrypt messages. The difficulty in breaking DH is generally considered to be equal to the difficulty in computing a discrete logarithm modulo a large prime number. This is summarized as follows, for the given p and g, which are both publicly available numbers. Users pick private values a and b and compute public values $x = g^a \bmod p$, $y = g^b \bmod p$. These public values are then exchanged. Compute shared private key, $k_a = y^a \bmod p$, $k_b = x^b \bmod p$. algebraically, it can be easily shown that $k_a = k_b$, which is a secret key that both parties computed independently [18].

3.2. Hash Function

Hash function is a public function that maps a message of any length into a fixed-length hash value, which serves as an authenticator. It is a four-tuple $(\mathcal{X}, \mathcal{Y}, \mathcal{K}, \mathcal{H})$, where the following conditions are satisfied [24].

(1) $\mathcal{X}$ is a set of possible *messages.*

(2) $\mathcal{Y}$ is a finite set of possible *message digests* or *authentication tags.*

(3) $\mathcal{K}$, the *key space,* is a finite set of possible *keys.*

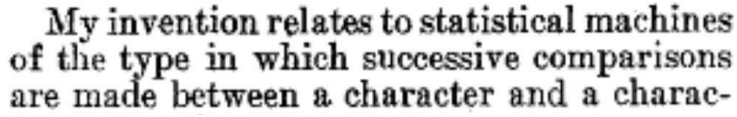
(4) For each $k \in \mathcal{K}$, there exists a *hash function* $\mathcal{HS} \in \mathcal{H}$, such that $\mathcal{HS} : \mathcal{X} \to \mathcal{Y}$.

- (i) It is very simple to find $\mathcal{HS}(x) = h.$, but it should be computationally infeasible to find x given h. This is the "one-way" property.
- (ii) For any given block x, it should be computationally infeasible to find $x \neq y$ with $\mathcal{HS}(y) = \mathcal{H}(x)$. This is called a non-collision property.
- (iii) It should be computationally infeasible to find any pair (x, y) such that $\mathcal{H}(x) = \mathcal{H}(y)$.
- (iv) Finally the output of the hash function must be random. This property is called random oracle.

Hash function represented in many areas of the information systems (e.g., password identification, integrity control, database comparing, etc.). Through the hash function, a small amount of data can be obtained from a large amount of data.

3.3. Optical Character Recognition

Optical Character Recognition (OCR) is a software designed to electronically identify and translate printed or handwritten characters by means of an optical scanner. OCR is composed of three elements: scanning, recognition, and reading text. The OCR software scans and determines whether it is identifying images or text. Then, the machine determines letters and words by recognizing their shape by repetitions or patterns of familiar forms as in the following example [25].


My invention relates to statistical machines
of the type in which successive comparisons
are made between a character and a charac-

My invention relates to statistical machines of the type in which successive comparisons are made between a character and a charac-.

4. The Proposed Authentication Scheme

In this paper, a personal identification scheme based on the advantages of fractal image coding is described. The system works on the binary image of the encrypted hash function for the individual information. In an authentication process, the information of the individual is compared with the information of every individual stored in the database. When the matching factor crosses the determined threshold, the system verifies the individual as an authentic user. Some of the notations used throughout this paper are described as follows:-

C: the client.

S: the server.

A: the attacker.

ID, PW: the client user name and password, respectively.

K: the shared key using Diffie-Hellman key exchange protocol.

HS: the hash function to be stored in the database.

$Y(HS, K)$: the encrypted hash function using a non-linear equation.

IM: image created using any converter text to image software.

T: the set of the coefficient of the IFS transformation W, constructing using fractal image coding scheme.

IM1: the decoded image that is generated using fractal image decoding scheme, which is look likes IM.

$X(Y, K)$: the decrypted hash using inverse nonlinear function.

4.1. The Proposed Method

Let us assume that the server generates a shared secure key K between the client and the server using DH protocol. If the client C_i wants to register with the server, the user name and the password should be first submitted to the server database through a secure channel.

The proposed scheme consists of three parts: registration, login, and authentication, they are described in detail as follows. The server and the client will share secure key K using DH protocol.

4.1.1. Registration and Login

(1) In Client

(a) Enter the user name and the password (ID, PW).
(b) C sends to S the current request (login, registration, and change password).
(c) C calculates the PW hashing value HS(PW)
(d) The hash function HS is encrypted using nonlinear function to give Y(HS, K).

(e) The ID and Y are captured in IM using a text to image converter.

(f) Calculate T, the matrix of the IFS transformation constructed from IM using fractal image coding scheme.

(g) T is sent to S.

(2) In Server

(a) Decode T to find the attractor IM1 using fractal image decoding.

(b) Use OCR program to read the data in IM1 and determine ID, and the encrypted Y.

(c) Use inverse function to decrypt Y and find HS_d

(d) For each request status (registration, login, and change password), S is authenticated as follows.

4.1.2. Authentication

(1) Registration

(i) S searching the database for ID.

(ii) If ID not found then return (User Name existed).

Else store ID and HS_d in database and return (Successful Registration).

(1) Log in

(i) S searching the database for ID.

(ii) If ID not found then return (Wrong user name or password).

Else compare the received HS_d with stored one as follows.

$$\begin{aligned} &\text{If HSd = HS then return (successful login)} \\ &\text{If HSd} \neq \text{HS then return (wrong user name or password).} \end{aligned} \tag{4.1}$$

(1) Change Password.

(i) S searching the database for ID.

(ii) If ID not found return (User Name is not available).

Else update the HS_d value in database and return (change password succeeds).

4.2. Software Implementation

The algorithm and its graphic user interface Figure 2 are carried out using Java under NetBeans IDE 7. All the results have been obtained using a computer with the specifications 2.4 GHz Intel Cor i3 CPU and 4 GB RAM.

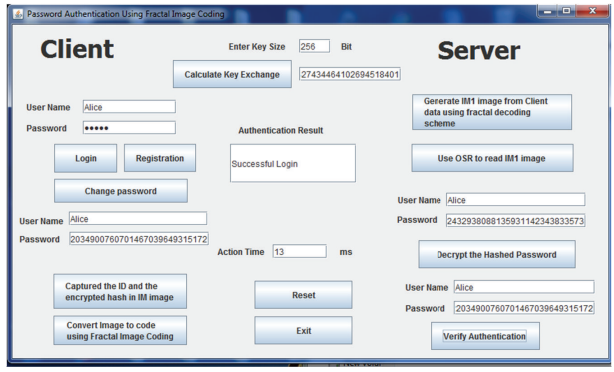
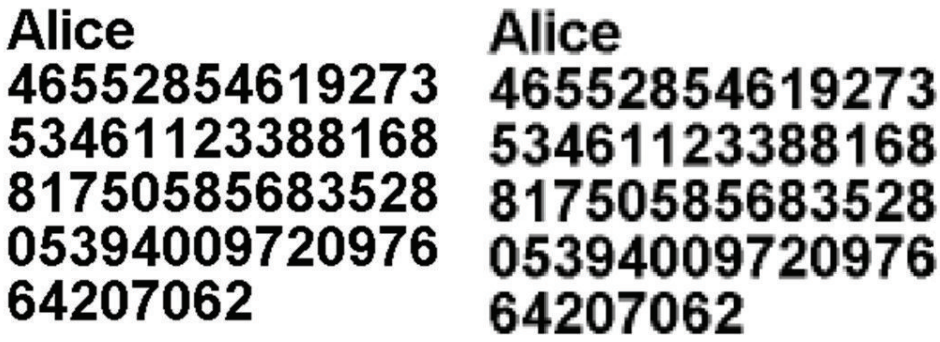


Figure 2: User Interface for password authentication using fractal image coding software.



(a) (b)

Figure 3: User name and hashed password.

Example 4.1. This is an illustration example for the scanned image (IM) using text to image mechanism in Figure 3(a), and the approximate image (IM1) using fractal image coding Figure 3(b).

5. Experimental Results

As indicated in Table 1 and Figure 4, the performance evaluation of the proposed scheme in terms of performance time and captured image size against the key size is shown. It is to conclude that the registration and login time changes is directly proportional with the key size, while the authentication time is depending on the number of users which were registered in the server. The proposed password authentication is a novel fractal based scheme which provides secure transmission of credential message over insecure communication channel. The registration and login phase in client side performs four steps: the password is hashed, encrypted, captured as an IM image, and then transformed to IFS codes using FIC scheme. Whereas, it performs three steps in server side, which are generating IM1 attractor using FID, reading data using OCR, and finally decrypting these data to find the hash function, to be used with the ID, either for authentication, or registration, depending on the request case.

Table 1: Performance time for different key size.

Key size	Key generation	Login time in client side	Login time in server side	Authentication time	IM–IM1 image size in kb
256	32	11387	8275	27	12–89
512	117	16615	11214	31	21–158
1024	581	18514	11336	29	32–246
2048	3141	20559	12012	22	44–301
4096	14983	21673	12643	30	52–327

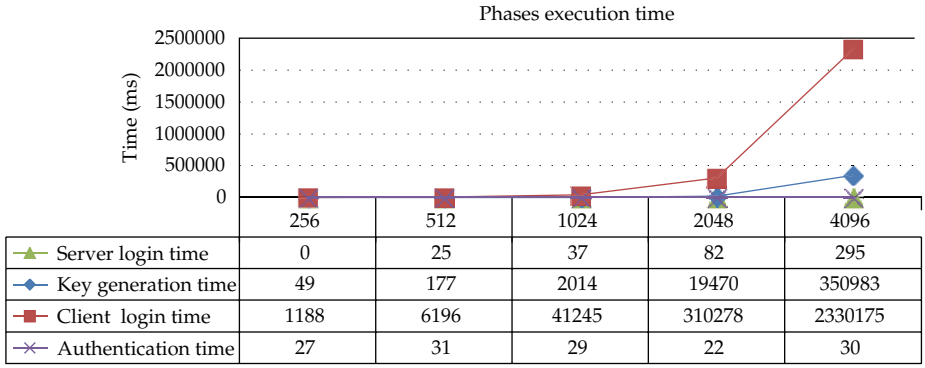


Figure 4: Comparison between phases in terms of execution time.

The program is designed to present error messages for certain cases as follows.

(i) The user enters wrong user name or password.

(ii) The user tries to register using ID which have been used before.

(iii) The algorithm is vulnerable to some attaches that try to change the data.

(iv) The OCR program resulted in wrong reading.

All these error cases can be expressed in the program by "wrong user name or password," or "the user is already exist."

The time in Table 1 are listed in milliseconds (ms). The result shows time needed in each phase for different key size.

6. Security Analysis

If we assume that an attacker A has a total control over the communication channel between C and S, this would mean that he can insert, delete, or change any message in the channel. The first step in the proposed system is the registration process. If the attacker masquerades as C and tries to change the ID or the PW and registers in the database using the wrong ID and PW, this does not give any advantage due to the lack of information in the stolen page at this stage. Therefore, the attacking process in this part is not feasible and the authorized user will have to reregister again. We conclude that the main goal of the attacker is to get the PW. Any attempt to change the ID will do nothing. If the attacker is skilled enough to recover the original image, using fractal image decoding, he will get an encrypted hash with a nonlinear function for two variables $Y(K, \mathrm{HS(PW)})$, where K is DH key exchange and HS(PW) is one way hash function of the user password, which is infeasible to be solved with exact values. The use of

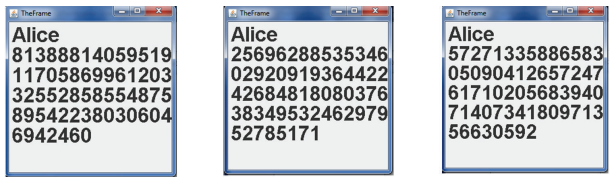


Figure 5: Different login attempts.

secured shared key DH that is based on the difficulty of discrete logarithm problems and it is computationally infeasible (unsolvable in polynomial time) for large prime number has a significant impact. This is in regard to increasing the security of the proposed scheme to resist many types of attacks over unsecure network.

The security analysis for the proposed scheme is discussed in details to show that the scheme withstands most of the following known attacking methods.

Password Guessing Attacks

The vulnerability to the attack happens in most passwords. When the ID of the client is known, then the attacker tries to guess the password to verify the correctness of his guess. To use this kind of attack, there are two ways, either the attacker tries to guess the password PW′ from the dictionary and login using the known ID to verify the correctness of his guess, he stops when PW′ = PW. In our scheme this is almost impossible, because the server will block this account after ten wrong login tries or if the attacker is knowledgeable enough and can intercept T from open network to decode T and find IM1 using fractal image decoding (FID). Eve can use opened OCR to read the data in IM1 and determine the ID and encrypted Y. Then, he should decrypt Y and find the Hash that should be used to guess PW, he stops when HS(PW) = HS(PW′). Hence, it is not easy for Eve to use inverse function to decrypt Y and find Hash, because Y is encrypted using two variables K and HS. Finding these two values depends on solving numerically the nonlinear function to recover the unknown's approximately, and that will involve truncation and cumulative errors. Regarding the value K, it is a secure value for large key size, while it is known only to the client and the server exclusively. In addition to unrepeatable property in each login (i.e., a different key is generated with each login). Moreover, for the second value HS, it is also not easy to be found, due to their properties that it should be computationally infeasible to find $x \neq y$ with $\mathrm{HS}(x) = \mathrm{HS}(y)$. Therefore, even if the attacker can find the hash, it is infeasible to find PW from the HS, and he will not be able to use this HS for authentication, because the server is designed to receive an encrypted hash not cleared hash, this value is decrypted to result in an unknown value. From the above we conclude that the proposed scheme is secured against password guessing attack.

Replay Attack

It is an attack in which an adversary impersonates another legal user through the reuse of information obtained in a protocol. In password authentication scheme, it is concerned with the case of attempts of an unauthorized user to impersonate an authorized one, by replaying the invalid message that is previously intercepted to the server. In our proposed method let us see Figure 5 for more details.

In this example, we showed that, for the same user in three different login attempts, a different message has been generated. This means that for the same user the login message is not repeatable, and it is infeasible to find two similar messages for any login session. If

the attacker Eve tries to intercept the captured message T from the login session and tries to resend it to the server again, the server will not authenticate the replayed message, because the key is changed in each login session. For this reason the proposed scheme is secured to the replay attack.

Denial of Service Attacks

In this attack, false verification information can be updated (applied) by the attacker for more than ten times, and as a result, the legal user will be blocked, and will not be able to login successfully anymore. The most vulnerable procedure is the password changing phase. In our scheme this phase is performed on the client side. While, the server should authenticate the user with the security question using the proposed secure scheme before starting the change password process; that is, it will help to enhance the security of password changing. The attacker is not able to modify data on storage, because only the authorized user is able to change the password. This is due to the security question that is preagreed before between the legal user and the server, as well as the difficulty of knowing the encrypted key.

Stolen Verifier Attack

One of the common features of password authentication schemes is the secure storage of the verification table in the server. If this table is stolen by the adversary, the system will be partially or totally broken. In the proposed scheme, the password is stored in the verification table as hashed value. Any attempt from the attacker to steel these data will do nothing, because these data is not stored explicitly. The strategy in the server is designed to receive an encrypted hash not an explicit hash, as result it will end with decrypting this information to unknown value, and this will cause failure in authentication process. So our scheme is secured against this attack.

Man in the Middle Attack

The proposed scheme is invulnerable to this attack, because when an adversary intercepts the message to prevent it from transmitting to server, this message is used later to impersonate the user to the server by the adversary. The server will not authenticate him, because if the user tries to reuse the information he will need time to steel the information and create the IM1 using FID, he uses OCR to read this information to recreate a new image IM2, then convert it to T1 (IFS codes). In this case, the time needed is very long and more than enough for the server to consider the current login session as expired. Hence, the attacker should start new login session which is impossible due to lack of information that he has.

7. Security Comparison

Password authentication schemes are the simplest and convenient schemes that provide the legal user a secure use of the server resources. The first scheme is suggested by Lamport [2]. It is a hash-based password authentication scheme. The researchers proved later that this scheme is vulnerable to some attacks, in addition, it uses high hash computation, and has password resetting problem. To overcome these drawbacks, Peyravian and Zunic [26] proposed a scheme that employs only hash function, which is simple and straight forward for applications. Later on, some researchers showed that this scheme is vulnerable to guessing attack, denial of service attack (DoS), stolen verifier attack, and many others. They tried to

Table 2: Security comparison of the proposed scheme against some password authentication scheme.

	Our proposed method	Lamport [2]	Hwang and Li's [4]	Lee et al.'s [8]
Guessing attack	Yes	No	No	Yes
Replay attack	Yes	No	No	Yes
Stolen-verifier attack	Yes	No	Yes	Yes
Denial of service attack	Yes	No	Yes	Yes
Man in the Middle attack	Yes	No	No	No

make some improvement to eliminate the weaknesses in this scheme, but to no vail. One of the common features of these schemes is the use of the verification table, which should be securely stored in the server. To overcome the drawbacks in these types of methods, password authentication mechanism is directed toward schemes based on smart cards strategy. It is to provide mutual authentication over insecure network, where the authentication is performed easily using a memorable password and without using verification table.

The first novel user authentication scheme using smart card was proposed in 2000 by Hwang and Li [4]. Later on, many researchers proposed several smart card based scheme, where each of them has its pros and cons. Some of these studies made improvements on Hwang scheme; however, most of them are still vulnerable to replay attack, reflection attack, DoS attack, guessing attack, parallel session attack, and many others. In addition, the existing smart card-based scheme is vulnerable to stolen/lost smartcard attack. Therefore, if any adversary steals a smartcard of a legitimate user, he can use it to impersonate as a legal client.

Since computing resources have grown hugely, there is always growing demands for emerging methods to enhance the security of password authentication protocols to be able to meet security requirement of modern application. Authenticated method based on physiological (biometric) features is considered a good alternative upon physical (smartcard) or knowledge (ID systems) authentication schemes. This is due to reliability (cannot be lost, forgotten, or guessed), in addition to its ease of use (there is nothing to be remembered or carried). These methods are based on distinguishing human features, the most common used biometric features are face, fingerprint, iris, voice, and palm print, and so forth. Authentication schemes based on fingerprint are given more attention than any other. Many Biometric-based password authentication scheme have been proposed. In 2002, Lee et al. [8] proposed a remote user authentication scheme using fingerprint and smartcards. Unfortunately, some researchers later on, showed that this scheme is vulnerable to some attacks even with the improvement that achieved. These methods are more costly and require specialized hardware.

However, in this paper, we proposed a novel password authentication scheme based on IFS theory. It enables us to represent an image in a compact way by means of a limited number of affine transformations. The proposed scheme is analyzed in details to show that it is invulnerable to many attacks, which can give us high security and few drawbacks. A security comparison of the proposed scheme with the Lamport [2], Hwang and Li [4], and Lee et al. [8] scheme from the attacker point of view is performed and summarized in Table 2. The proposed scheme is relatively more secure and less costly than the other schemes.

8. Conclusions and Future Works

A password authentication system based on the advantage of fractal image coding is proposed. The system works on the captured binary image of the client information (ID, PW).

After the password is hashed and encrypted, it is coded using FIC scheme and send it to the server instead of the image itself. The successful matching is performed at the server to verify the client user after the ID is recognized, and the hash is decrypted to be verified with the saved hash in database system. The security strength of the scheme relies on the security of the hash function, and DH protocol that is used as a key exchange in encryption and decryption of HS(PW), in addition to the complexity of the FIC scheme. We conclude that the proposed scheme is nontraditional password authentication, flexible to improvement, in addition to many other attributes, such as the following.

(i) The user cannot freely change the password without connecting to the server (i.e., only the authorized user is able to change the password), because of the security question that is preagreed before between the legal user and the server, as well as the difficulty of knowing the encrypted key.

(ii) The scheme has a facility of access denial or blocked any unauthorized user whose try to use wrong password for more than ten trials.

(iii) The scheme is secured against guessing, replay, denial of service, stolen-verifier, parallel session, and many other attacks.

(iv) The uses of FIC offer an advantage to increase the security because of the use of the fractal codes instead of original image.

(v) The server closes the session whenever it takes more than the usual time and will request a new session.

All of these points are considered an advantage, whereas, there is also some of disadvantages of using this scheme, such as: it is a little bit time consuming in comparing to some other schemes, that is due to using fractal image coding and decoding process, in addition to the nonaccurate reading of the OCR system, that may happen rarely. This is caused by using nonefficient OCR program, because the generated image is an approximate image not an explicit image. The proposed scheme provides mutual authentication between the client and the server. It establishes a common session key that provides confidentiality.

For future work, the scheme can be improved to be more secure and invulnerable to many types of attacks, if the encryption process is performed for the IFS codes after applying FIC scheme instead of its current use for the hashed password. With these improvements both the ID and the PW will be hidden, not the password only as in the current case.

Acknowledgment

The researchers would like to acknowledge the Institute for Mathematical Research (INSPEM), University Putra Malaysia (UPM) for supporting this work.

References

[1] C. Stoneff, "Fixing weak passwords," 2010, http://www.net-security.org/article.php?id=1528.
[2] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.
[3] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card," *Computers and Security*, vol. 21, no. 4, pp. 372–375, 2002.
[4] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28–30, 2000.

[5] M. Kumar, "A new secure remote user authentication scheme with smart cards," *International Journal of Network Security*, vol. 11, no. 2, pp. 88–93, 2010.
[6] K. Saraswathi, B. Jayaram, and R. Balasubramanian, "Retinal biometrics based authentication and key exchange system," *International Journal of Computer Application*, vol. 19, no. 1, 2011.
[7] Y. An, "Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards," *Journal of Biomedicine and Biotechnology*, vol. 2012, Article ID 519723, 6 pages, 2012.
[8] J. K. Lee, S. R. Ryu, and K. Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," *Electronics Letters*, vol. 38, no. 12, pp. 554–555, 2002.
[9] C. T. Wang, T. S. Chen, and S. H. He, "Detecting and restoring the tampered images based on iteration-free fractal compression," *Journal of Systems and Software*, vol. 67, no. 2, pp. 131–140, 2003.
[10] E. J. Yoon and K. Y. Yoo, "A secure chaotic hash-based biometric remote user authentication scheme using mobile devices," in *Advance in web and Network Technologies and Information Management*, vol. 4537 of *Lecture Notes in Computer Science*, 2007.
[11] I. Motýl and R. Jašek, "Advanced user authentication process based on the principles of fractal geometry," in *Proceedings of the 11th WSEAS International Conference on Signal Processing, Computational Geometry and Artificial Vision (ISCGAV '11)*, pp. 109–112, 2011.
[12] M. F. Barnsley and S. Demko, "Iterated function systems and the global construction of fractals," *Proceedings of the Royal Society. London. Series A*, vol. 399, no. 1817, pp. 243–275, 1985.
[13] M. F. Barnsley and L. P. Hurd, *Fractal Image Compression*, A K Peters, Wellesley, Mass, USA, 1993.
[14] C. H. Li and S. S. Wang, "Digital watermarking based on fractal image coding," *Journal of the Chinese Institute of Engineers*, vol. 23, no. 6, pp. 759–766, 2000.
[15] A. Jacquin, *A fractal theory of iterated markov operators with application to digital image coding [Doctoral thesis]*, Georgia Institute of Technology, 1989.
[16] Y. Fisher, *Fractal Image Compression*, Springer, New York, NY, USA, 1995.
[17] J. Puate and F. D. Jordan, "Using fractal compression scheme to embed a digital signature into an image," in *Video Techniques and Software for Full-Service Networks*, vol. 2915 of *Proceedings of SPIE*, pp. 108–118, Boston, Mass, USA, November 1996.
[18] M. F. Barnsley, *Fractals Everywhere*, Academic Press Professional, Boston, Mass, USA, 2nd edition, 1993.
[19] N. M. G. Al-Saidi and M. R. Md. Said, "A new approach in cryptographic systems using fractal image coding," *Journal of Mathematics and Statistics*, vol. 5, no. 3, pp. 183–189, 2009.
[20] N. M. G. Al-Saidi and M. R. M. Said, "Improved digital signature protocol using iterated function systems," *International Journal of Computer Mathematics*, vol. 88, no. 17, pp. 3613–3625, 2011.
[21] W. Yung-Gi, H. Ming-Zhi, and W. Yu-Ling, "Fractal image compression with variance and mean," in *Proceedings of the International Conference on Multimedia and Expo (ICME '03)*, vol. 2, pp. 353–356, 2003.
[22] Z. Yuliang, "Authenticated Public Key Encryption Schemes using Universal Hashing," IEEE P1363: Asymmetric Encryption, 1998.
[23] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE*, vol. 22, no. 6, pp. 644–654, 1976.
[24] C. Blundo and P. D'Arco, "The key establishment problem," in *Foundations of Security Analysis and Design II*, vol. 2946 of *Lecture Notes in Computer Science*, 2004.
[25] S. Vicky, H. Heather, and S. Samantha, "Optical character recognition and the visually impaired," *American Foundation for the Blind*, vol. 59, pp. 1–10, 2010.
[26] M. Peyravian and N. Zunic, "Methods for protecting password transmission," *Computers and Security*, vol. 19, no. 5, pp. 466–469, 2000.