International Journal of Cryptology Research 2(1): 1-13 (2010)

A New Public Key Cryptosystem Based on IFS

[1] Nadia M. G. AL-Saidi and [2] Mohamad Rushdan Md. Said
[1,2]Institute for Mathematical Research (INSPEM),
Universiti Putra Malaysia,
43400 UPM Serdang, Selangor, Malaysia
Email: [1]nadiamg08@gmail.com and [2]mrushdan@fsas.upm.edu.my

ABSTRACT

Most public key encryption methods suffers from the inability to prove the difficulty of the algorithms, which summarizes under the category of mathematical problems that have inverses which are believed (but not proven) to be hard. The length and strength of the Cryptography keys are considered an important mechanism. The keys used for encryption and decryption must be strong enough to produce strong encryption. Fractals and chaotic systems have properties which have been extensively studied over the years, and derive their inherent complexity from the extreme sensitivity of the system to the initial conditions. In this paper a new cryptographic system based on Iterated Function Systems (IFS) have been proposed to reduce the computation cost and increase the security for the public-key cryptography protocols. In the proposed public-key encryption algorithm, generate iterated function systems as a global public element, then its Hutchinson operator is used as a public key. To encrypt the plaintext with the receiver's public key we use one of the key agreement protocols to generate a shared private key that used to find the attractor of the IFS. The chaotic nature of the fractal functions ensures the security of the proposed public-key cryptosystem schemes

INTRODUCTION

Cryptography is the study of mathematical and computational techniques related to aspects of information security. It is a method of transferring private information and data through open network communication, so only the receiver who has the secret key can read the encrypted messages which might be documents, phone conversations, images or other form of data. Modern telecommunication networks, and especially the Internet and mobile-phone networks, have tremendously extended the limits and possibilities of communications and information transmissions. Associated with this rapid development, there is a growing demand of cryptographic techniques, which has spurred a great deal of intensive research activities in the study of cryptography [15].To implement privacy simply by encrypting the information intended to remain secret can be achieved by using methods of Cryptography. The information must be scrambled, so that other users will not be able to access the actual information. For example, in a multi-users system, each user may keep his privacy intact via her/his own password. On internet, a large number of internet users use internet application, such as business, research, learning, etc. These activities are very important for the users' application; hence, the importance of using Cryptography has been highlighted to help them keep the privacy [3].

Since 1976, numerous public-key algorithms have been proposed; three most widely used public-key crypto-systems are: RSA, Rabin and ElGamal. The security of the RSA system, named after its inventors Rivest, Shamir, and Adleman, is based on the intractability of the integer factorization problem. In the Rabin public-key encryption scheme, the problem faced by a passive adversary is computationally equivalent to factoring. The security of the ElGamal public-key system is based on the intractability of the discrete logarithm problem [20].

Since 1990s, many researchers have noticed that there exists an interesting relationship between chaos, fractal and cryptography. Dynamical systems theory is closely related to fractal geometry. One can show that fractals attractors of iterated function systems in particular- have a naturally associated dynamical system which is chaotic. Fractals are attractors of dynamical systems; the place where chaotic dynamics occur [10]. For details on the relation between chaos and fractals, we refer the reader to [4,6].

Many properties of chaotic systems have their corresponding counterparts in traditional cryptosystems; they are characterized by sensitive dependence on initial conditions, similarity to random behavior, and continuous broad-band power spectrum. The suggested guidelines address three main issues: implementation, key management, and security analysis, aiming at assisting designers of new cryptosystems to present their work in a more systematic and rigorous way to fulfill some basic cryptographic requirements. In recent years, a large amount of work on chaos-based cryptosystems has been published. Much work has been done by incorporating chaotic maps into the design of symmetric and asymmetric encryption scheme. In 2003, Kocarev and Tasev [13] proposed a public key encryption algorithm based on chebyshev chaotic maps, and after that many works that proposed a new key agreement protocol based on chaotic maps are developed. Also some works for incorporating of fractal functions into the design of symmetric and asymmetric encryption schemes using the similar mechanism have been proposed in [1,3,12], However many of the proposed schemes have several advantages such as computational efficiency, ease of generating of public-private key pars etc, but fail to explain or do not possess a number of features that are fundamentally important to all kind of cryptosystems.

The use of fractal have advantage since; only few parameter would have to be stored, and this kind of key is very robust to attacks for these two reasons; if the attacker managed to obtain parts of the key (or almost the entire key), but a small digit is missing or is incorrect, the fractal image is changed dramatically. In this case the attacker has no way to extrapolate the rest of the key. The second reason, the brute force attack will not work since a fractal key is time consuming to generate especially at high zoon levels [19].

Fractal geometry and, in particular, the theory of fractal functions, has evolved beyond its mathematical framework and has become a powerful and useful tool in the applied sciences as well as engineering. The realm of applications includes structural mechanics, physics and chemistry, signal processing and decoding, and cryptography. The reason for this variety of applications lies in the underlying complicated mathematical structure of fractal functions, specifically their recursive construction. For certain problems they provide better approximants than their classical non-recursive counterparts.

This paper concentrates more on the mathematical aspects of fractal functions and briefly exposes the reader to one, the latest, application of fractal functions, namely public key cryptosystems. In Section 2 some theoretical concepts and the main properties of iterated function systems are given. In section 3 the relation between fractal functions and cryptography are mentioned in addition to the derivation of a recurrence formula from IFS function in order to use it in public key systems are discussed in details. Some conclusions are given in section 4. Finally the reader is referred to the references for more details.

THEORETICAL CONCEPTS OF ITERATED FUNCTION SYSTEM

An important concept in our study is the idea of iterated function systems (IFS). In this section we present an overview of the major concepts and results of (IFS) and their application. A more detailed review of the topics in this section was given in [4].

Definition 1. A map from R^m to R^n is affine if it is the sum of a linear map and a translation. Then we can write $f(x) \in R^n$ in the form $f(x) = Ax + B$; where A is an $n{\times}m$ constant real matrix, and B is a constant $n{\times}1$ matrix [9]. Let $S{\subset}X$ be a subset of a metric space (X,d). S is compact if every infinite sequence $\{x_n\}_{n=1}^{\infty}$ x in S contains a convergent subsequence [18].

Definition 2. A metric space (X,d) is complete if and only if every Cauchy sequence converge in X with respect to the metric d [2]. Moreover if $S \subset X$. Then S is compact if and only if it is closed and totally bounded.

Definition 3. A function $f{:}X{\rightarrow}X$ is said to be Lipschitz if and only if there exists an $s\in[0,\infty)$ such that $\forall x,y{\in}X$ we have $d(f(x),f(y)){\leq}sd(x,y)$. We call s a Lipschitz constant of f. If there exist such an s<1, we say f is contractive or is contraction and call s a contractivity factor of f.

Notation: For $x{\in}X$, we define the n-fold composition of a function f at x recursively by $f^1(x)=f(x)$;
$f^{n+1}(x)=f(f^n(x))$, we call $f^n(x)$ the n-th iteration of f at x.

Definition 4. Let (X,d) be a complete metric space. The Hausdorff distance between nonempty compact sets $A,B{\subset}X$ is defined by :

$$h(A,B) = \max\left(\max_{a\in A}\min_{b\in B} d(a,b), \max_{b\in B}\min_{a\in A} d(b,a)\right) \tag{1}$$

Let $H(X)$ denote the collection of all compact and nonempty subsets of X; then h is a metric on $H(X)$. Moreover, the metric space $(H(X), h)$ is complete [17].

Theorem 1. (Contraction Mapping Theorem). [2]. Let $f{:}X{\rightarrow}X$ be a contraction mapping on a complete metric space (X, d). Then f possesses exactly one fixed point $a{\in}X$, and for any point $x{\in}X$, the sequence $\{f^n(x)\}$ converges to a, so $\lim_{n\to\infty} f^n(x) = a$; $\forall x \in X$.

Definition 5. An (hyperbolic) iterated function system (abbreviated IFS) is a couple (X, w), where $w = [w_1,\ldots,w_N]$ is a vector of N operators $w_i : X{\rightarrow}X$ which are contractions of contractivity factors $\lambda(w_i)\in[1,0)$ with respect to the metric d. The image of a nonempty compact subset of X under a contraction mapping is a nonempty compact set; thus each mapping from *w* can also be regarded as an operator on the space $H(X)$, that is $w_i:H(X)\to H(X)$, $i = 1,\ldots, N$. Furthermore, each w_i is a contractive operator on $H(X)$ of the contractivity factor $\lambda(w_i)$ with respect to the Hausdorff metric *h* [17].

Definition 6. Given an IFS (X, w), a set-valued mapping *W* can be associated with (X,w) by setting

$$W(E) = \cup_{i=1}^{N} w_i(E), E\subset X \tag{2}$$

Any finite union of nonempty compact sets is a nonempty compact set, so *W* can be regarded as an operator on $H(X)$. Moreover, it is a contraction of the contractivity factor $\lambda(W)=\max_{i=1,\ldots,N}\lambda\,($ with respect to the metric *h*. The mapping W is usually referred to as the *Hutchinson operator*. As the Hutchinson operator is a contraction mapping on the complete metric space$(H(X),h)$, by the Banach fixed-point theorem the operator possesses the only fixed point $A\in H(X)$ that is $A = W(A)$ and moreover $\lim_{i\to\infty} W^{\circ i}(E) = A,$ for any $E\in H(X)$. Such a unique set is called the attractor of the IFS which the operator *W* is associated with [14].

An IFS is a standard way to model natural objects. The intuitive key for deriving IFS that models any given object is self-tiling (similarity). One can always view an object as the union of several sub-objects. Let the sub-objects be actually scaled-down copies of the original object. Each of these subjects is called a tile. In particular, each sub-object is obtained by applying an affine transformation to the entire object. Now consider the original object with two or more affinely transformed copies of itself [1]. The tiling scheme should completely cover the object, even if this necessitates overlapping the tiles. Each transformation used to "create" a tile corresponds exactly to one map in the IFS. In order to create an IFS, one first specifies a finite set of contractive affine transformations $\{W_i\ ;\ i=1,\ldots,n\}$ in R^2. In general the contractive affine transformation *W* in R^2 is of the form,

$$F\begin{pmatrix}x\\y\end{pmatrix} = \begin{bmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}\begin{pmatrix}x\\y\end{pmatrix} + \begin{pmatrix}e\\f\end{pmatrix} = A\vec{X} + \vec{B} \tag{3}$$

For which all eigenvalue of A has modulus less than 1. The maximum of the set of modulo of eigenvalues of A is called contractivity factor for A. Now we can define a set function W, which maps sets to sets:

$$W(A_0) = \cup_{i=1}^{n} W_i \;(A_0) = A_1 \qquad (4\;)$$

where A_0 is a compact subset (i.e closed and bounded) of two-dimensional space. A set A_∞ can be defined as the limit of the sequence A_n, where $A_{n+1}=W(A_n)$, n=0,1,… [5].

FRACTAL BASED CRYPTOGRAPHY

The methods of constructing the algorithm are classified into: traditional methods, where the constructing of cryptosystems based on application of number theory and algebra, and untraditional methods (or emerging methods), which is of much important approach to construct public –key cryptosystems based on application of the theory of dynamical systems. In the last decade, the analog as well as discrete dynamical systems have been utilized to develop cryptosystems and there have been a variety of attempts along this line.

I-Public-key Cryptography

In a public-key encryption system each entity A has a public key *e* and a corresponding private key *d*. In secure systems, the task of computing *d* given *e* is computationally infeasible. The public key defines an encryption transformation E_e, while the private key defines the associated decryption transformation D_d. Any entity *B* wishing to send a message *M* to *A* obtains an authentic copy of *A*’s public key *e*, uses the encryption transformation to obtain the ciphertext $c=E_e(M)$, and transmits *c* to *A*. To decrypt *c*, *A* applies the decryption transformation to obtain the original message $M=D_d(c\ )$.

Public-key encryption schemes are typically substantially slower than symmetric-key encryption algorithms. For this reason, public-key encryption is most commonly used in practice for encryption small data items and/or for transport of keys, subsequently used for data encryption by symmetric-key algorithms [15]. From a dynamical point of view, all three encryption algorithms RSA, El-Gamal, and Rabin employ one single system,

$$X_{n+1} \equiv \left(X_n\right)^p (\mathrm{mod}\, N) \qquad (5)$$

where X is an integer, $0 \le X \le N-1$, and, X_0, p, and N are properly chosen integers. For example, in the ElGamal public-key scheme, one uses (5), where N is a prime, X_0 is a generator of the multiplicative group $Z_N{}^*$ of integers modulo N, and $1 \leq p \leq N-2$. In the RSA algorithm, $N=PQ$, where P and Q are two random distinct primes, p is an integer $1<p<\phi$, where $\phi=(P-1)(Q-1)$, such that $\gcd(p,\phi)=1$, and X_0 is the message to be encrypted. Rabin public-key encryption scheme uses (1) with $p=2$, $N=PQ$, where P and Q primes both congruent to 3(mod4), and X_0 is the message to be encrypted. In the ElGamal public-key scheme, the entity A generates a large random prime N and a generator X_0 of the multiplicative group $Z_N{}^*$ of integers modulo N and also generates a random integer $s \leq N-2$ and compute $A = X_0$ s (mod N). A's pubic key is (X_0 ,A,N); A's private key is s. To encrypt a message m, the entity B selects a random integer $r \leq N-2$, computes $B=X_0^{\mathrm{r}}(\mathrm{mod}\ N)$ and $X=mA^r(\mathrm{mod}\ N)$, and sends the cipher-text $c=(B,X)$ to A. To recover the message m from c, A uses the private key s to recover m by computing $m=B^{-s}X(\mathrm{mod}\ N)$ [13]. From the dynamical point of view all three schemes use the following property of (1):

$$\left(X^p\right)^q \equiv X^{pq} (\mathrm{mod}\, N) \qquad 1 \qquad\qquad (6)$$

In addition, RSA algorithm and Rabin public-key encryption scheme use some properties of (6) related to the period of the sequence X, X_2 (mod N), X_3 (mod N) , ... Can another dynamical system be used in public-key encryption algorithms?

Even though fractals are re-creatable, they are very sensitive to any change in initial condition, with the property of sensitive dependence on initial condition similarity to random behavior and generated by simple recursive calculations, we felt confident that we could develop encryption and decryption algorithms that take the advantage of fractals, for these reasons chaos and fractal has been widely introduced into various aspects of cryptography, since there properties are analogous to the requirement of cryptography, and is excellent for use in encryption algorithm because it makes the encrypted code much harder to decrypt without the proper key. Recently chaos maps were introduced into public-key cryptography by [13, 21]. The purpose of this paper is to find a viable and re-creatable algorithm for encrypting and decrypting data in public key cryptosystem using the properties of fractals functions. In this section fractal functions are constructed using techniques from the theory of iterated function systems. Examples of such fractal functions show the versatility and flexibility of this function class.

II-Fractal public and private keys.

The proposed public-key primitives were designed to be resistant against attacks. Therefore, the major motivation of this research is to reduce the computation cost and increase the security for the public-key systems, and this leads us to propose new public-key cryptosystem based on Fractal. Since, there are many previous works in fractal cryptography. Most of these protocols were design in the symmetric approaches. The idea behind our proposed method based on generating an affine IFS transformation as private key then finds its Hutchinson operator to be used as a public key.

We refer the reader with a strong mathematical interest in the topic to [4]. Although it is difficult to give an all encompassing definition since fractals can be objects of different types, it is usually agreed that (deterministic) fractals arise from the repeated iteration of a transformation, or it is an image generated from a recursive formula. In other words, fractals are mathematical objects which can in general be written as**:**

$$A = \lim_{n \to \infty} W^n (A_0) \qquad (7)$$

where A_0 denotes an initial object, and $W^n = W \circ W \circ W \circ \ldots \circ W$ denotes n iterations of W, ($W = \bigcup_{i=1}^{n} w_i$) and, $\{w_i \; ; \; i=1,\ldots,n\}$ is a finite set of contractive affine transformations in R^2). They are typically generated by computing and displaying a sequence of iterates $A_0, A_1, A_2, \ldots$ where $A_n = W(A_{n-1})$. From Eq. (7), it is clear that fractals satisfy the invariance equation $A=W(A)$, which confers to them a property which we generically refer to as self-transformability, and which leads to the well-known properties of fractals to be rugged objects with an infinite amount of detail [5].

III-The Proposed Method.

To generate fractal attractor, the Hutchinson operator is constructed based on a given affine transformation. Consider an IFS consisting of the maps,

$$w_i(x, y) = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e_i \\ f_i \end{pmatrix}, \quad \mathrm{i} = 1, 2, \ldots, N. \qquad (8)$$

Instead of writing them as above, they can be written in a matrix form [2],

$$\begin{pmatrix} \mathrm{a}_1 & \mathrm{b}_1 & \mathrm{c}_1 & \mathrm{d}_1 & \mathrm{e}_1 & \mathrm{f}_1 \\ & & \ldots\ldots\ldots & & & \\ & & \ldots\ldots\ldots & & & \\ \mathrm{a}_2 & \mathrm{b}_2 & \mathrm{c}_2 & \mathrm{d}_2 & \mathrm{e}_2 & \mathrm{f}_2 \\ \mathrm{a}_N & \mathrm{b}_N & \mathrm{c}_N & \mathrm{d}_N & \mathrm{e}_N & \mathrm{f}_N \end{pmatrix} \qquad (9)$$

To explain this method, fractal generated using IFS of four affine transformation (w_1, w_2, w_3, w_4) are used, where the generalized case can be easily followed. Fractals generated by affine transformation (10) satisfy the semi-group property.

$$w_i(x, y) = \begin{pmatrix} a_i & 0 \\ 0 & d_i \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} c_i \\ d_i \end{pmatrix}, \; i = 1,2,...,N. \qquad (10)$$

A dummy coordinate Z with value 1 is added to represent the translation in the affine transformation, and the 2-dimensional matrix (10) is structured by (3 by 3) matrix as in (11).

$$w_i(x, y, 1) = \begin{pmatrix} a_i & 0 & c_i \\ 0 & b_i & d_i \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ 1 \end{pmatrix}, \; i = 1,2,...,N. \qquad (11)$$

Then the 4-affine transformations in (10) are arranged in a (4 by 4) matrix in (12),

$$H = \begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{pmatrix}. \qquad (12)$$

We calculate the Hutchinson operator $W = w_4 w_3 w_2 w_1$, and represent it in the form of (11), as

$$W(x, y, 1) = \begin{pmatrix} A & 0 & C \\ 0 & B & D \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ 1 \end{pmatrix}, \text{ where} \qquad (13)$$

$A= a_4a_3a_2a_1, \quad A\neq 1.$
$B=b_4b_3b_2b_1, \quad B\neq 1,$
$C=a_4a_3a_2c_1+a_4a_3c_2+a_4c_3+c_4.$
$D=b_4b_3b_2d_1+b_4b_3d_2+b_4d_3+d_4.$

THE ALGORITHM.

To conceal the value of fractal attractor during the transmission process, a shared secret key is needed, which is available only to the sender and the receiver. A DH key agreement protocol is used in generating the number of iteration to create the fractal attractor, which in turn is used to generate the public key and encrypt the message. The fractal public key scheme comprised three parts: Key Generation, Encryption, and Decryption.

Key Generation

Initially the parameters (matrix H, g, p) are regarded as public knowledge (where $g\in Z$, and p is prime number).

a. Generate numbers $(x,y\ s)$, (x',y',r) as receiver, and sender private keys, where $x,y,x',y'\in R$, and $r,s\in Z$.

b. Calculate and exchange $F_s=g^s$ (mod p), $F_r=g^r$ (mod p) as receiver, and sender public key.

c. After receiving F_r, the receiver calculates a private shared key $n=(F_s)^r$ (mod p), that is used as the number of iteration in generating fractal attractor W^n .

$$W^n = \begin{pmatrix} A^n & 0 & (T_n(A))C \\ 0 & B^n & (T_n(B))D \\ 0 & 0 & 1 \end{pmatrix}$$

where, $T_n(A)=A^{n-1}+A^{n-2}+\ldots+A+1$, and $T_{\underline{n}}(B)= B^{n-1}+B^{n-2}+\ldots+B+1$.

d. By using W^n the receiver and sender public key $(u,v,1)= W^n(x,y,1)$, and $(u',v',1)= W^n(x',y',1)$ are calculated and exchange, where

$$\begin{aligned} u &= A^n x + T_n(A)C \\ v &= B^n y + T_n(B)D \end{aligned} \text{, and } \begin{aligned} u' &= A^n x' + T_n(A)C \\ v' &= B^n y' + T_n(B)D \end{aligned}$$

Encryption

a. Determine the message to be encrypt and represent it as pairs $M=(m_1,m_2)$.

b. The sender uses fractal attractor W^n with his private key (x',y'), to find the cipher text Z, such that Z=(z_1,z_2)=$W^n(m_1ux',m_2vy',1)$.

c. Send the cipher text $(Z,,(u',v'))$ to the receiver.

Decryption

Choosing the matrix H as in (11) ensures that W^n is commutation under composition, so due to this semi-group property, if $Z=W^nM$, it follows that $M=W^{-n}Z$.

a. After receiving $(Z,(u',v'))$, the receiver uses his private key (x,y) and the fractal attractor W^n, the message $M=(m_1,m_2)$ is recovered using,

$$M=(m_1,m_2)=\left(\frac{s_1-T_n(A)C}{(A^nx+T_n(A)C)(u'-T_n(A)C)},\frac{s_2-T_n(B)D}{(B^ny+T_n(B)D)(v'-T_n(B)D)}\right).$$

CONCLUSIONS

The public key cryptography and fractal function are both evoking lot of interest from mathematics. In this paper, we have proposed new public key cryptosystem based on using fractals IFS functions. The proposed scheme is both secure and practical, does not involve in factorization and discrete logarithms problem, and therefore is fast. The advantage of using this new technique over the existing public key algorithms is that, the use of IFS transformations makes it hard for cryptanalysis, since adversary has to generate a high resolution image to quickly determine M from C, and it is computationally infeasible in addition to its advantage in reducing the key length of the public key system. . If the cryptosystem parameters are based on real numbers (a continuous infinite interval) then the search space is massive. Hence, many well known attacks fail to solve the nonlinear systems and find the imprecise secret key parameter from the given public one. Even if it is theoretically possible, it is computationally not feasible.

REFERENCES

[1] AL-Sa'idi, N. 2009. Muhammad Rushdan Md Said., A New Approach in Cryptographic Systems Using Fractal Image Coding, *Journal of Mathematics and Statistics*, **5** (3): 183-189.

[2] AL-Sa'idi, N. 2002. *On the multi fuzzy fractal space*. Ph.D. Thesis, Al-Nahreen University, Baghdad, Iraq.

[3] Alia M., Samsudin, A. 2008. *A New Approach to public-key cryptosystem based on Mandelbrot and Julia*, *Ph.D*. Thesis Universiti Sains Malaysia.

[4] Barnsley, M. 1993. *Fractals Everywhere*. Academic Press Professional, Inc., San Diego, CA, USA.

[5] Barnaey, M. F. and Demko, S. 1985. Iterated function systems and the global construction of fractals. *Iroc. Roy. Sot.* A , **399**: 243-275.

[6] Becker, K.-H., DBrfler, M. 1989. *Dynamical Systems and Fractals*, Cambridge University Press, Cambridge.

[7] De-Jun Feng and Yang Wang. 2009. On the structures of generating iterated function systems of Cantor sets. *Advances in Mathematics,* **222**: 1964–1981.

[8] Fisher, Y. 1995. *Fractal Image Compression: theory and application.* Springer-Verlag. New York, USA.

[9] Gulati, K and Gadre, V.M. 2003. *Information Hiding using Fractal Encoding*. Dissertation for the degree of Master of Technology. School of information Technology. Indian Institute of Technology Bombay. Mumbai.

[10] Jacquin, A. 1992. Image Coding Based on a fractal Theory of Iterated Contractive Image Transformations, *IEEE Transactions on image processing,* **1**: 18-30.

[11] Kotulski, Z and Szczepanski, J. 2006. Discrete chaotic cryptography. *Ann. Phys,* **509** (5): 381-394.

[12] Kumar, S. 2006. Public key cryptography system using Mandelbrot sets. *Military Communications Conference, 2006.* MILCOM 2006. IEEE. 23-25 Oct.

[13] Kocarev, L., Sterjev, M., Fekete, A. and Vattay, G. 2003. Public-key encryption with chaos. *Chaos.* 2004, **14**(4):1078-82.

[14] Martyn, T. 2003. Tight bounding ball for affine IFS attractor. *Computer Graphics,* **27**: 535-552.

[15] Menezes, A. J., Oorschot, P.C.V., Vanstone, S.A. 1997. *Handbook of Applied Cryptography*, CRC Press, Boca Raton.

[16] Peter R. Massopust. 1997. Fractal Functions and their Applications. *Chas, Solitons & Fractal*, **8**(2):171-190.

[17] Puate, J. and Jordan, F. 1996. Using Fractal Compression Scheme to Embed a Digital Signature into an Image. *Proceedings of SPIE Photonics East'96 Symposium.*

[18] Rudin, W. 1976. *Principles of Mathematical Analysis*. 3rd Edition, McGraw-Hill Book Company.

[19] Rozouvan, V. 2009. Modulo image encryption with fractal keys. *Optics and Laser in Engineering*, **47**: 1-6.

[20] Tenny, R. and Tsimring, L. 2005. Additive mixing modulation for public key encryption based on distributed dynamics. *IEEE Trans Circuits Syst* I, **52**:672–9.

[21] Xiang, T., Wo Wong K. and Liao, X. 2009. On the Security of a novel key agreement protocol based on chaotic maps. *Chaos, Solitons and Fractals*, **40**: 672-675.