Journal of Mathematics and Statistics 5 (3):183-189, 2009
ISSN 1549-3644

A New Approach in Cryptographic Systems Using Fractal Image Coding

Nadia M.G. Al-Saidi and Muhammad Rushdan Md. Said
Institute for Mathematical Research,
University Putra Malaysia, 43400, Serdang, Selangor, Malaysia

Abstract: Problem statement: With the rapid development in the communications and information transmissions there is a growing demand for new approaches that increase the security of cryptographic systems. **Approach:** Therefore some emerging theories, such as fractals, can be adopted to provide a contribution toward this goal. In this study we proposed a new cryptographic system utilizing fractal theories; this approach exploited the main feature of fractals generated by IFS techniques. **Results:** Double enciphering and double deciphering methods performed to enhance the security of the system. The encrypted date represented the attractor generated by the IFS transformation, collage theorem was used to find the IFSM for decrypting data. **Conclusion/Recommendations:** The proposed method gave the possibility to hide maximum amount of data in an image that represent the attractor of the IFS without degrading its quality and to make the hidden data robust enough to withstand known cryptographic attacks and image processing techniques which did not change the appearance of image.

Key words: Iterated function system, attractor, affine transformation, collage theorem, iterated function system mapping

INTRODUCTION

The digital information revolution has brought about changes in our society and our lives. The many advantages of digital information have also generated new challenges and new opportunities for innovation. Every few years, computer security has to re-invent itself. New technology and new applications bring new threats and force us to invent new protection mechanisms[6]. The fractals theory has proved to be suitable in many fields and particularly interesting in various applications of complex systems. Recently, some researchers developed cryptosystem based on fractals, since one of the fractal properties was having extremely high visual complexity while having low information contents, which can make simple cryptographic and Steganography methods very complex[4].

In most applications, image data is two-dimensional data; therefore, an image can be considered as two-dimensional memory. Fractal archiving is based on image representation in compact form by means of iterated function system coefficients. First important advances are due to Barnsley[1], who introduces for the first time the term of Iterated Function Systems (IFS), 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 the use of IFS simple transformations.

The natural question may appear: "Can we use IFS to approximate images?" The seminal research by Jacquin[3], then a Ph.D. student of Barnsley at Georgia Tech, provided the basis of block-based fractal image coding which is still used today. Jacquin's research launched an intensive activity in fractal image compression[2,7]. From this assumption, the IFS can be seen as a relationship between the whole image and its parts, thus exploiting the similarities that exist between an image and its smaller parts. At that point, the main problem is how to find these transformations or, (what is the same) how to define the IFS. 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 Arnaud Jacquin[3], who developed an algorithm to automate the way to find a set of transformations giving a good quality to the decoded images.

MATERIALS AND METHODS

The major concepts and results of IFS and their application to the study of functions are presented. A more detailed review of the topics was given in[1,5,6].

Corresponding Author: Nadia M.G. Al-Saidi, Institute for Mathematical Research, University Putra Malaysia, 43400, Serdang, Selangor, Malaysia Tel : +60162144183/+03 8946 6878 Fax: +03 89423789

IFS Theory: Let's consider a metric space (£, d) where d is a given metric. A Hausdorff space H (£) is defined to be the space of all compact subset of £ with the Hausdorff distance h. A contractive transformation is defined by: $\beta: £ \to £$, that satisfies:

$$d(\beta(x),\beta(y)) \leq sd(x,y),\ x,y \in £,\ 0 \leq s \leq 1$$

We write Con(£, d) for the set of all contractive maps $\beta: £ \to £$. An IFS consists of a complete metric space (£,d) and a number of contractive mappings β_i defined on £. The fractal transformation associated with IFS is defined by:

$$B(E) = \bigcup_{i=1}^{N} \beta_i(E)$$

where, E is any element of the space H of non-empty compact subsets of £. If β_i is contractive for every i, then B is contractive and there exist a unique fixed point for which:

$$A = B(A) = \bigcup_{i=1}^{N} \beta_i(A)$$

or

$$\lim_{n \to \infty} B^n(E) = A$$

A is called the attractor of B. If B is continuous then A is called a fixed point of B. The fundamental result upon which the entire theory of iterated function systems is founded is the Banach Contraction Mapping Principle (BCMP) or Fixed Point Theorem, which state that, if (£,d) is a complete metric space and $\beta \in Con(£,d)$ with contractivity factor s, then β has a unique fixed point $A \in £$. Furthermore, A is the attractor of B.

The transformations B are usually chosen to be affine. For the two dimensional case the affine transformations have the following forms:

$x_{n+1} = ax_n + by_n + e$
$y_{n+1} = cx_n + dy_n + f$

The coefficients a,..., f are the IFS "code". This also be written in the affine form as:

$$\beta\begin{bmatrix} x \\ y \end{bmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix} = AX + b$$

β is said to be linear, if e = f = 0.

Now, suppose that we are given $\alpha \in £$. A natural question that was first asked in IFS theory is whether or not it is always possible to find a contractive operator $B \in Con(£, d)$ whose fixed point is α. We expect that, in general, this is not possible and that one must be satisfied in finding fixed points α_i of contractive operations β_i that are approximations to α. Even in this case, however, we are faced with the problem of finding such fixed points α_i. This problem is called the Inverse Problem. It is generally stated as follows. Given $(Y; d_Y)$ a metric space, $y \in Y$ and $\varepsilon > 0$, can we find a non constant $\beta \in Con(Y; d_Y)$ such that $d_Y(y; y_\beta) < \varepsilon$?

Before commenting on this question, an additional question that arises is, "given $y \in Y$ and $\beta \in Con(Y; d_Y)$, how close is y to y_β"? The following proposition lends an answer. Let y; Y and β be as above. Then:

$$d_Y(y, y_\beta) \leq \frac{1}{1-s} d_Y(y, \beta(y))$$

This is often called the collage theorem. It is important in helping to identify the functions to use in an IFS in order to approximate the attractor. The Collage Theorem is fundamental to the theory of IFS because it states that if $\beta(y)$ is close to y, then y_β is also close to y. Of course, if $s \cong 1$, the right hand side of the inequality might not be very small. Thus, this gives some insight into finding our desired function. We should find $\beta \in Con(Y; d_Y)$, which takes y close to itself. We recall from the BCMP that y_β is the attractor of β if Y is complete. Hence we can iterate β to retrieve y_β and get the desired approximation to y. Therefore, the Inverse Problem is often formulated as follows: Let $(Y; d_Y)$ be a complete metric space and let $y \in Y$. Given $\varepsilon > 0$, can we find a non constant $\beta \in Con(Y; d_Y)$, such that $d_Y(y; \beta(y)) < \varepsilon$?

A formal solution to this problem was given in[12] in the case of IFS on grey-level maps. This will be important in our study of approximations of images. Once β is determined, it is easy to get the decoded image by making use of the BCMP, the transformation B is applied iteratively on any initial point until the succession of images does not vary significantly. However, given a set M, how to find a contractive transformation B such that its attractor A is close to M? To answer this question in symbols is to apply the collage theorem.

For a set M and a contraction B with attractor A:

$$h(M, A) \leq \frac{h(M, B(M))}{1-s}$$

where, h is the Hausdorff Distance. That is to say that M and A will be sufficiently close, if M and B(M) are made close enough in terms of β_i and combining the following two expressions:

$$B(M) = M;\ B(M) = \bigcup_{i=1}^{N} \beta_i(M)$$

Which implies:

$$\bigcup_{i=1}^{N} \beta_i(M) \approx M$$

So, M can be partitioned as:

$$M = \bigcup_{i=1}^{N} m_i$$

Then, m_i can be closely approximated by applying a contractive affine transformation β_i on the whole M:

$$m_i = \beta_i(M)$$

From IFS to IFSM fractal Transform: The concepts of IFS, first developed by Barnsley and Demko[5] and IFS on grey-level maps (IFSM), was introduced by Forte and Vrscay[9]. We continue with a discussion of the inverse problem for IFSM. The main idea of a fractal based image coder is to determine a set of contractive transformations to approximate each block of the image (or a segment, in a more general sense), with a larger block. More details and explanation can be found in[12].

The Collage Theorem tells us that in order to find an IFS whose attractor looks like a given set, we must find a set of contractive transformations on a suitable space, in which the given set lies, such that the distance between the given set and the union of the transformations is small. In other words, the union of the transformations is close to, or looks like, the given set. The IFS which satisfies this may be a good candidate for reproducing the given set, or image, by the attractor of the IFS. Thus this image can be stored using much less space[14].

Consider applying this theory to images, (i.e., computer images). One can think of an image as being a compact subset of R^n. One can model a computer screen by £ = $[0,1]^2$ or R^2 and define an image on the screen to be a set A in £, with points being screen pixels. If $x \in A$, the associated pixel is plotted white. If $x \notin A$, leave the pixel black. Hence a white screen represents $A \subseteq [0,1]^2$. Since the world is not black and white. What is needed is an IFS-type method, which allows for, greys, i.e., maps, which move pixels around and then scale their grey-levels. These thoughts lead to IFSM theory. There is however a fundamental difference between the IFS and IFSM. The IFS works with measure and a set of probabilities p_i associated with the β_i which acts as multiplicative weight. The IFSM work with function $u:£ \rightarrow [0,1]$ and function $\phi_i:[0,1] \rightarrow [0,1]$ which are composed with the u. From the viewpoint of image processing the value u(x) may be interpreted as a nonnegative gray level or brightness value at the point (or pixel) $x \in £$[13].

Let us consider a compact subset A of R^2 to stimulate some ideas. Formulate a definition of A being a grey-scale image is to think of the image as a function, rather than a set. That's mean formulate IFS method on functions from sets to grey-levels in the form of $A = \{(x_i, y_i, u(x_i, y_i)), i = 1,\ldots,N\}$, where $u(x_i, y_i)$ represent the grey level value of the set (x_i, y_i)[10].

These developments of IFS give a necessity to define a complete metric space of these functions. A local metric for the gray level maps with respect to an element $u \in £$ was contracted and the continuity of attractor u_k with respect to ϕ_i maps was then established. Let $\Omega(£) = \{\beta:£ \rightarrow R \mid \beta^{-1}(r) \in H(£), \forall r \in R\}$, this set is defined as the set of grey level maps on £. Now a metric on this space must be defined such as:

$$D(u, v) = \text{Sup}\ h(u^{-1}(r), v^{-1}(r))\ \forall u, v \in \Omega(£), \forall r \in R$$

If (£,d) is complete metric space then (Ω (£),D) is also. The operator T on Ω(£), is defined by, $Tu(x) = \max u(\beta^{-1}(x))$, $\forall u \in \Omega(£)$, $x \in £$. Thus, to find an IFS whose attractor is `close to' or `looks like' a given image, one must find a set of contraction mappings such that the union, or collage, of the given set under the transformations is `close to' or `looks like' the given image. This leads to the next result. Let (£, d) be a metric space and let $B = \{\beta_n: n = 1,2,\ldots,N\}$ is contractive with contractivity factor s_n. Then T is contractive with contractivity $S = \max\{s_n: n = 1, 2,\ldots,N\}$. Also T has a unique attracting fixed point $p \in T$, T (p) = p. Since u took only two values, modify this new operator to the grey level values, so a grey level component is added.

The IFSM operator $T_u(x) = \max \phi(u(\beta^{-1}(x))) \forall x \in £$, ϕ: $R \rightarrow R$. where ϕ is defined by, $\forall u \in \Omega$ (£), $\phi(u(\beta^{-1}(x))) = \alpha\ u(\beta^{-1}(x)) + \xi$. Therefore define the operator T on $u \in \Omega(£)$ by $T_u(x) = \sum_i \alpha_i u(\beta_i^{-1}(x)) + \xi_i$ $\forall x \in £$, where Σ indicates that the sum runs over the all

indices i with $x \in \beta_i(£)$. The diagram in Fig. 1 shows these operations.

Proposed approach: There are many types of cryptography, in which there are "double enciphering" and "double deciphering" processes, that make the codes more difficult to crack and to analyze. For enciphering, firstly, one of the classical Cryptographic methods are used to convert message letter into integer numbers, secondly arranging the resulting code in a chosen manner of affine IFS transformation and the resulting enciphering code is the attractor of the IFS system. For deciphering, the receiver of the attractor A retrieves affine IFS transformation B using "Inverse Problems" techniques to perform the first level of deciphering method, then some algebraic calculation applied to obtain the plain text. To illustrate the method some algebraic facts are recalls. Let m be a positive integer, the idea is to take m linear combination of the n alphabetic characters in one plaintext element thus producing the m alphabetic characters in one ciphertext element. An $m \times m$ matrix $K = (k_{i,j})$ is taken as a first key. Let $X = (x_1, x_2, \ldots, x_m)$ and $k \in K$ (the set of all $m \times m$ invertible matrices), we compute $y = eK(X) = (y_1, y_2, \ldots, y_m)$. We say that the ciphertext is obtained from the plaintext by means of a linear transformation and K^{-1} is used for deciphering as $X = YK^{-1}$[8]. A matrix K has an inverse if and only if its determinant is non-zero. Z_n denotes the ring of integer's modulus n. Z_n is Galois field if and only if n is prime number. So we assume that our language has n-letter, n is prime, enciphering and deciphering m units of messages of length l at a time. K represents an $m \times m$ matrix whose entries belong to Z_t for which $t = n^m$, D represents the det(K). The relevant result for our purpose is that a matrix K has an inverse modulo n if and only if GCD(det(K),n) = 1[11].

Theorem: $\beta(X) = AX + b$ could be used as a secret key to encipher p messages of length m at a time in n-letter alphabet if and only if GCD(D, n^m) = 1.

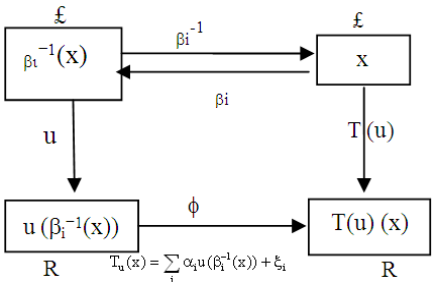

Fig. 1: Block diagram for IFSM transformations

Proof: If B is secret key then B is one to one map from Z_t to Z_t where $t = n^m$ and hence onto and so invertible. Thus GCD(D, n^m) = 1. Conversely if GCD (D, n^m) = 1, then A is invertible and hence β is one to one.

The sender arranges each unit of length m in entries with value one in the affine IFS transformation. The elements of the B maps constructed from (C_{ij}/n^m) where $Cij = p_1 \times n^m + p_2 n^{m-1} + \ldots + p_m$.

Affine IFS maps: 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 affine transformed copies of itself. 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 $\{\beta_i; i = 1,\ldots, n\}$ in R^2. In general, a contractive affine transformation β in R^2 is of the form: $\beta(X) = AX + b$, which could be used as a secret key to produce an enciphering code. There are different possibilities to arrange element in IFS invertible maps, therefore, for abbreviation, binary sequences of 0's and 1's used to represent all possibilities for element arranging in the β_i maps, as follows:

$$\beta\begin{bmatrix} x \\ y \end{bmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & 0 \end{pmatrix}\begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \end{bmatrix} = AX \rightarrow 111000$$

$$\beta\begin{bmatrix} x \\ y \end{bmatrix} = \begin{pmatrix} a_{11} & 0 \\ a_{21} & a_{22} \end{pmatrix}\begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \end{bmatrix} = AX \rightarrow 101100$$

$$\beta\begin{bmatrix} x \\ y \end{bmatrix} = \begin{pmatrix} a_{11} & 0 \\ 0 & a_{22} \end{pmatrix}\begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \end{bmatrix} = AX \rightarrow 100100$$

$$\beta\begin{bmatrix} x \\ y \end{bmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \end{bmatrix} = AX \rightarrow 111100$$

$$\beta\begin{bmatrix} x \\ y \end{bmatrix} = \begin{pmatrix} 0 & a_{12} \\ a_{21} & 0 \end{pmatrix}\begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \end{bmatrix} = AX \rightarrow 011000$$

All the above orders are for linear affine transformation. Now for non- linearity order each one of the above maps is extended to three forms by adding

the translation part b. For example, for β = 111000, we have:

$$\beta\begin{bmatrix}x\\y\end{bmatrix} = A\begin{bmatrix}x\\y\end{bmatrix} + \begin{bmatrix}e\\0\end{bmatrix} = AX + b \rightarrow 111010$$

$$\beta\begin{bmatrix}x\\y\end{bmatrix} = A\begin{bmatrix}x\\y\end{bmatrix} + \begin{bmatrix}e\\f\end{bmatrix} = AX + b \rightarrow 111011$$

$$\beta\begin{bmatrix}x\\y\end{bmatrix} = A\begin{bmatrix}x\\y\end{bmatrix} + \begin{bmatrix}0\\f\end{bmatrix} = AX + b \rightarrow 111001$$

RESULTS

Conversion of the plain-text message to the unreadable format is known as enciphering of the message. Similarly, conversion of the enciphered message back to the human readable form through the reversal of the encryption algorithm is known as deciphering of the message[8].

Encryption method: Let's assume that there are two parties(sender and receiver) in two far places that need to communicate secretly in a way that a third person (intruder) won't figure or recognize that they are exchanging information between them. However, the alphabetic, the classical encryption method and the order of the affine IFS maps must be agreed upon between sender and receiver.

Enciphering algorithm: In this algorithm an alphabet of n = 29 character is chosen:

- The message characters are given a numbers as it appear in Table 1, show the length of the message
- Divide the message of length l into units of length m = 3, represented by $p_i p_{i+1} p_{i+2}$
- Calculate the numeric value of each unit using the polynomial $C = p_i n^2 + p_{i+1} n + p_{i+2}$, or matrices operation to perform first level of the proposed method
- The contraction factor used is r = 1/nm
- The elements of the chosen affine IFS transformations β_i are calculated by β_i = r*C. Notice that $B = \{\beta_1, \beta_2, \ldots \beta_i\}$ called a (hyperbolic) IFS
- The attractor A is generated using Random Iterated Algorithm[1]
- The enciphering code is the picture represents the Attractor A

Example: To encrypt the message, "We will attack at dawn through the left flack", the sender and the receiver agreed on an alphabet mentioned in Table 1. The message is divided into units of three characters and used as inputs to the affine transformations after applying the polynomial $C = p_i n^2 + p_{i+1} n + p_{i+2}$, the enciphering code is shown in Table 2.

If the affine mappings, 111001, 101110, 111000, 100111 are chosen, then the IFS for example 1 are constructed as follows:

$$B = \bigcup \begin{cases} \beta_1 = \left\{ \frac{1}{29^3}\begin{pmatrix}18644 & 18745\\ 10005 & 0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} + \begin{pmatrix}0\\6530\end{pmatrix}, p = .1 \right. \\ \beta_2 = \left\{ \frac{1}{29^3}\begin{pmatrix}199 & 0\\ 577 & 2545\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} + \begin{pmatrix}11706\\0\end{pmatrix}, p = .1 \right. \\ \beta_3 = \left\{ \frac{1}{29^3}\begin{pmatrix}6394 & 17291\\ 22424 & 0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}, p = .7 \right. \\ \beta_4 = \left\{ \frac{1}{29^3}\begin{pmatrix}4129 & 0\\ 0 & 3528\end{pmatrix} + \begin{pmatrix}22022\\68\end{pmatrix}, p = .1 \right. \end{cases}$$

Applying the random iterated algorithm, the attractor of these transformations is shown in Fig. 2.

Table 1: English Alphabet used for encryption

English letters with integer values			
A = 0	B = 1	C = 2	D = 3
E = 4	F = 5	G = 6	H = 7
I = 8	J = 9	K = 10	L = 11
M = 12	N = 13	O = 14	P = 15
Q = 16	R = 17	S = 18	T = 19
U = 20	V = 21	W = 22	X = 23
Y = 24	Z = 25	$ = 26	. = 27 ? = 28

Table 2: Message units and their enciphering code

M. unit	Value	M. unit	Value
we$	18644	hro	6394
wil	18745	ugh	17291
l$a	10005	$th	22424
tta	16530	e$l	4129
ck$	1998	eft	3528
at$	577	$fl	22022
daw	2545	ack	68
n$t	11706	-	-

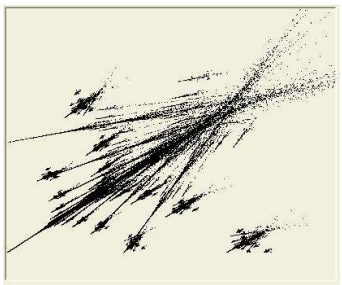

Fig. 2: The attractor A generated by the IFS system B

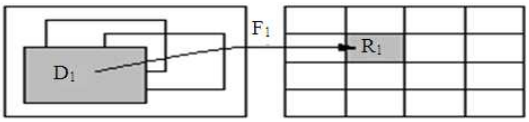

Fig. 3: The transformation from domain block to range block

Decryption method: The main idea to automate the searching of local IFS relies on a partition of the image into N non-overlapping blocks of a fixed size, called Range Blocks. Each range block R_i, for $i \in \{1,...,N\}$, is coded independently by matching it with a bigger block D_i in the image, called Domain Blocks. This match defines a transformation τ_i and the global fractal code is then given by the union $\tau = \cup\tau_i$ of local transforms as shown in Fig. 3. Moreover, each local code τ_i restricted to consist of a reduction, a discrete isometric and an affine transformation on the luminance. Hence, τ_i can be modeled by:

$$\tau_i \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{pmatrix} a_i & b_i & 0 \\ c_i & d_i & 0 \\ 0 & 0 & s_i \end{pmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} t_{i,1} \\ t_{i,2} \\ o_i \end{bmatrix}$$

where, a_i, b_i, c_i, d_i, $t_{i,1}$, $t_{i,2}$ represent the geometric transforms and s_i, o_i the grey-levels transform; x, y are the pixel coordinates and z the corresponding luminance value[14].

Deciphering algorithm:

- 1-Upon the receipt of the attractor (picture) A, the receiver retrieves B using "Inverse Problems" techniques. Let A denote the image we want to encode. Let also A_r denote a partition of A to n×n blocks referred to as Range Blocks (R_b). Similarly, A_d will denote another partition of A, this time to 2×2 n blocks or Domain Blocks (D_b) in steps of n×n pixels. The goal of the deciphering algorithm is to establish a relationship between A_r and A_d in such a way that any R_b can be expressed as a set of transformations to be applied on a particular D_b. This algorithm is illustrated by the flowchart in Fig. 4[6]
- The receiver then modifies the entries of the retrieved IFS system B to get β_i as they agreed on before
- By multiplying each entry in the affine IFS map by n^m and rounding them to the nearest integer we perform the first level of decrypting method

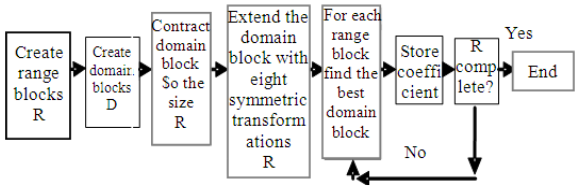

Fig. 4: Flow chart to find the IFSM maps

The second level is performed by applying some algebraic calculation to find p_1, p_2, p_3 in each cipher unit, as follows:

- $p_1 = \text{int}(C/n)$
- $R = C \bmod n^2$
- $p_2 = \text{int}(R/n)$
- $p_3 = R \bmod n$

DISCUSSION

The theory of IFS was extended to local IFS where each part of the image is approximated by applying a contractive affine transformation on another part of the image: $m_i = \beta_i(D_i)$. D_i is the bigger part from which m_i is approximate. The main idea of a fractal based image coder is to determine a set of contractive transformations to approximate each block of the image (or a segment, in a more general sense), with a larger block. In this paper we propose a new Cryptographic method using the fractals theory (more precisely the IFS theory). For enciphering, firstly, one of the classical Cryptographic methods are used to convert message letter into integer numbers, secondly arranging the resulting code in a chosen manner of affine IFS transformation and the resulting enciphering code is the attractor of the IFS system. For deciphering, the receiver of the attractor A retrieves affine IFS transformation B using "Inverse Problems" techniques to perform the first level of deciphering method, an algorithm based on Jacquin's work is used, then some algebraic calculation applied to obtain the plain text.

CONCLUSION

The proposed approach employs double enciphering and double deciphering process. The fractal image generation through the given parameters, needs a great amount of iterations to converge into an attractor, but at the same time, it provides non uniform randomness and it is independent of the image size[9]. In the proposed method the IFS (B(X) = AX + b) could be used as a secret key to encipher p units messages of

length m at a time in n-letter alphabet if and only if the GCD (D, n^m) = 1, then generates the fractals associated with the IFS. The receiver can recover the message using the collage theorem and simple algebraic calculations.

The proposed fractal encryption technique gives the possibility to hide maximum amount of data in an image that represent the attractor of the IFS without degrading its quality. The other advantage of using fractal as an encryption technique is to make the hidden data robust enough to withstand image processing technique which does not change the appearance of image. For better results images should be in 24-Bit bit map (bmp) format and much better results are obtained by using larger size image (512×512).

ACKNOWLEDGEMENT

The researchers would like to acknowledge the Institute for Mathematical Research (INSPEM), University Putra Malaysia (UPM) for its continuous support.

REFERENCES

1. Barnsley, M., 1993. Fractals Everywhere. 2nd Edn., Academic Press Professional Inc., San Diego, CA., USA., ISBN: 10: 0120790610, pp: 550.
2. Fisher, Y., 1995. Fractal Image Compression: Theory and Application. Springer-Verlag. New York, USA., ISBN: 0-387-94211-4, pp: 341.
3. Jacquin, A.E., 1992. Image coding based on a fractal theory of iterated contractive image transformations. IEEE Trans. Image Process, 1: 18-30. http://www.ncbi.nlm.nih.gov/pubmed/18296137
4. Gulati, K. and V.M. Gadre, 2003. Information hiding using fractal encoding. Dissertation for the Degree of Master of Technology, School of information Technology, Indian Institute of Technology Bombay, Mumbai. http://www.it.iitb.ac.in/~kamal/fractal.pdf
5. Barnsley, M.F. and S. Demko, 1985. Iterated function systems and the global construction of fractals. Proc. R. Soc. London, 399: 243-275. http://adsabs.harvard.edu/abs/1985RSPSA.399..243B
6. Puate, J. and F. Jordan, 1996. Using fractal compression scheme to embed a digital signature into an image. Proceedings of Photonics East '96-the SPIE's International Symposium on Intelligent Systems and Advanced Manufacturing, Nov. 1996, Boston, MA. http://infoscience.epfl.ch/record/86413
7. Ávalos, P.A.H., C.F. Uribe, R.L. Velázquez and R.A.C. Parra, 2007. Watermarking based on iterated function systems. Proceeding of the International Congress on Computing, Nov. 2007, IEEE Computer Society Press, Washington DC., USA., pp: 147-151. http://ccc.inaoep.mx/~cferegrino/Publicaciones/articulos/WatermarkingIFS.pdf
8. Stinson, R., 2006. Cryptography: Theory and Practice. 3rd Edn., CRC Press, ISBN: 1584885084, pp: 593.
9. Forte, B. and E.R. Vrscay 1995. Theory of generalized fractal transforms. Fractal image encoding and analysis. ftp://shear.informatik.unileipzig.de/pub/Fractal/papers/FoVr95b.ps.gz
10. Piche, D., 1997. IFSM wavelets and fractal-wavelets three methods of approximation. MSc. Thesis Waterloo, Canada. http://uwspace.uwaterloo.ca/handle/10012/29?mode=full
11. Neal Koblitz, 1994. A Course in Number Theory and Cryptography. 2rd Edn., Springer, ISBN: 0387942939, pp: 235.
12. Piche, D.G., 2002. complex bases, number systems and their application to fractal-wavelet image coding. Ph.D. Thesis in applied Mathematics. Waterloo, Ontario, Canada. http://uwspace.uwaterloo.ca/handle/10012/1057
13. Zhou, Y.M., C. Zhang and Z.K. Zhang, 2009. An efficient image coding algorithm using unified feature and DCT. Chaos Solitons Fract., 39: 1823-1830. DOI: 10.1016/j.chaos.2007.06.089
14. Dugelay, J.L., E. Polidori and S. Roche, 1996. Iterated Function Systems for still Image Processing. IWISP-96, Manchester, UK. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.42.623