A New Approach to Encoding and Hiding Information in an Image

Dr. Fadhil Salman Abed
Technical Institute of Kalar
Diyala,Iraq

Abstract

The information age brings some unique challenges to society. New technology and new applications bring new threats and force us to invent new protection mechanisms. So every few years, computer security needs to reinvent itself. In this paper we propose a new image encoding system utilizing fractal theories; this approach exploits the main feature of fractals generated by IFS techniques. Two levels of encryption and decryption methods performed to enhance the security of the system, this is based on the fact that all fractal functions use real number to ensure satisfaction of contraction property. 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. The encrypted date represents the attractor generated by the IFS transformation, Collage theorem is used to find the IFS for decrypting data. The proposed method gives the possibility to hide maximum amount of data in an image that represent the attractor of the IFS without degrading its quality.
Also to make the hidden data robust enough to withstand known cryptographic attacks and image processing techniques which do not change the appearance of image. The security level is high because the jointly coded images cannot be correctly reconstructed without all the required information.

Keywords: Image processing , Hiding, Fractal Image Compression, Quadtree, Steganography

1.0 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. 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 **[1]**.

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. Many properties of chaotic systems have their corresponding counter

parts 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 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 **[2]**.

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. 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**[3]**.

2.0 The Proposed Encoding and Hiding System

The main objects of the proposed system contain two stage, firstly by cryptography(encryption) the information massage by using new approach in cryptography based on iterated function system(IFS), secondly by hiding the encryption information by using proposed technique based on fractal image compression.

2.1 Proposed Approaches(Cryptography Units)

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 analyses. The proposed approach for enciphering and deciphering apply two level method for each, for enciphering, firstly, one, by arranging the resulting code in a chosen manor of affine IFS transformation, and the resulting enciphering code is the attractor of the IFS system, secondly by hiding the enciphering text in an image by using Fractal Image Compression.

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 $GCD(D, n^m)=1$.

Proof:-

If B is secret key then B is one to one map from Z_t to Z_t where $\boldsymbol{t= n^m}$ 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 are constructed from $\boldsymbol{(C_{ij}/n^m)}$ where $\boldsymbol{C_{ij}=p_1n^m+p_2n^{m-1}+\ldots+p_m}$.

2.1.1 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 an 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**[4]**.

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 $\{b_i; i=1,\ldots, n\}$ 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 b_i maps, as follows:

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

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

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

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

$$\beta\begin{bmatrix}x\\y\end{bmatrix}=\begin{pmatrix}0 & a_{12}\\ a_{21} & 0\end{pmatrix}\begin{bmatrix}x\\y\end{bmatrix}+\begin{bmatrix}0\\0\end{bmatrix}=AX\rightarrow 110000$$

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:

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

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

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

2.1.2 The Implementation

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.

2.1.3 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.

2.1.4 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 $\mathbf{p_i p_{i+1} p_{i+2}}$
- Calculate the numeric value of each unit using the polynomial $\mathbf{C = p_i\, n^2 + p_{i+1} n + p_{i+2}}$, or matrices operation to perform first level of the proposed method.
- The contraction factor used is $\mathbf{r = 1/n^m}$
- The elements of the chosen affine IFS transformations βi are calculated by $\boldsymbol{\beta_i}$ = **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].**

(1) Initialize x=0, y=0 (Starting point).
(2) Choose arbitrary k to be one of the numbers 1 , 2, 3 , ...n , with probability p_k .
(3) Apply the transformation w_k on the point (x, y) to obtain the point (x', y').
(4) Plot the point (x', y').
(5) Set x = x' and y = y'.
(6) Goto step 2.

- The enciphering code is the picture represents the Attractor A.

Algorithm (1) Image generation with random IFS

Table (1): English alphabet used for encryption

2.1.5 Decryption Algorithm

- 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* in nxn blocks referred to as Range blocks (R_b). Similarly, A_d will denote another partition of *A*, this time in 2nx2n blocks or Domain blocks (D_b) in steps of nxn pixels.
- The goal of the encoding 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. The receiver then modifies the entries of the retrieved IFS system *B* to get β_i as they agreed on.
- 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.
- Finally Apply some algebraic calculation to find p_1, p_2, p_3 in each cipher unit, as follows.

  p_1=int(C/n^2), R= C mod n^2 ,p_2=int(R/n) ,p_3=R mod n

Example: To encrypt the message, "**We must be good in cipher system.**", 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 are constructed as follows:

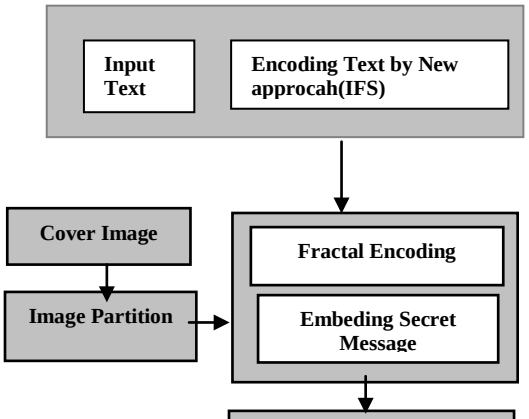
$$B=\bigcup\left\{\begin{array}{ll}\frac{1}{29^3}\begin{pmatrix}18644 & 10690\\ 16734 & 0\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}+\begin{pmatrix}0\\ 4124\end{pmatrix}, & \text{Prop.}=.1\\ \frac{1}{29^3}\begin{pmatrix}12183 & 0\\ 2211 & 21932\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}+\begin{pmatrix}12822\\ 0\end{pmatrix}, & \text{Prop.}=.2\\ \frac{1}{29^3}\begin{pmatrix}15068 & 20725\\ 3738 & 0\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}, & \text{Prop.}=.7\end{array}\right.$$

Message units	Value	Message units	Value
We$	18644	$ci	21932
Mus	10960	phe	12822
T$b	16734	R$s	15068
E$g	4124	yst	20725
ood	12183	Em.	3739
$in	22111	-	-

Table (2): Message units and their enciphering code

2.2 The Proposed Hiding System(hiding Units)

Figure (1) describes the proposed system starting with loading cover image, then performing the quad-tree partition and then hiding module by starting search process for similarity between the image blocks (range blocks and domain blocks) and embedding the secret message in the scaling and offset values of the blocks. The output of this stage is a data file of stego-image which is sent from a sender to a recipient. When the recipient receives the data file of the stego-image, the process of extraction could be applied to obtain the secret message with an approximate or the reconstructed image.



English letters w				
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

Figure (1): Embedding information unit

The extraction stage illustrated in **figure (2)** starts by loading the file of the stegoimage and extracting the hidden information that received with fractal decoding side by side. Fractal decoding starts by setting all the domains to arbitrary shapes, it goes then into loop. The first iteration applies the transformation to domains that all are black. This creates range that may already after this single iteration, slightly resembles the original ranges. With recreating every block of the ranges the hidden characters will be extracted and the receiver will receive the secret message.

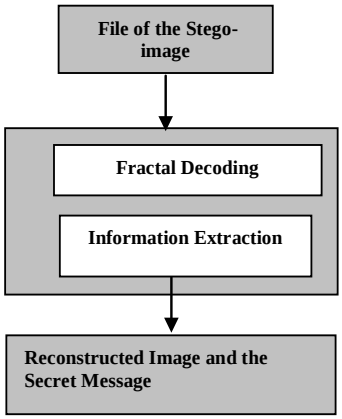


Figure (2): Information extraction unit

2.2.1 Hiding Unit

The structure of the hiding unit; mainly it consists of eight modules:

- Loading cover image.
- Colour separation.
- Convert the image formula from RGB to YCbCr **[5]**

$$Y = (77/256)\,R + (150/256)\,G + (29/256)\,B$$
$$Cb = -(44/256)\,R - (87/256)\,G + (131/256)\,B + 128$$
$$Cr = (131/256)\,R - (110/256)\,G - (21/256)\,B + 128$$

- Partitioning the cover image by using Quad-tree colour image Partition
- Down sampling.
- Fractal encoding.
- Embedding the secret message.
- Stegoimage data file saving.

2.2.2 Quad-tree Partition

One of the most familiar partition techniques is the quadtree method, which subdivides a region of an image into four equal blocks when a given homogeneity criterion is not met by that region. It continues to divide each sub-division until the criteria is met or minimum block size is reached. Typically, an image is initially divided into a set of large blocks (their size equal to the maximum allowable block size). The variance is computed and compared to a threshold for each of these blocks. Any sub-blocks created by failure of the homogeneity test undergo the same procedure. The subdivision will continue until a block either reaches a minimum size or it satisfies the homogeneity criterion. Each block test constitutes a node of the quadtree. A node for which no further subdivision is needed is called a leaf. The tree structure and accompanying encoding for each leaf node are stored or transmitted for later reconstruction. **Figure (3)** illustrates the quadtree partitioning procedure.

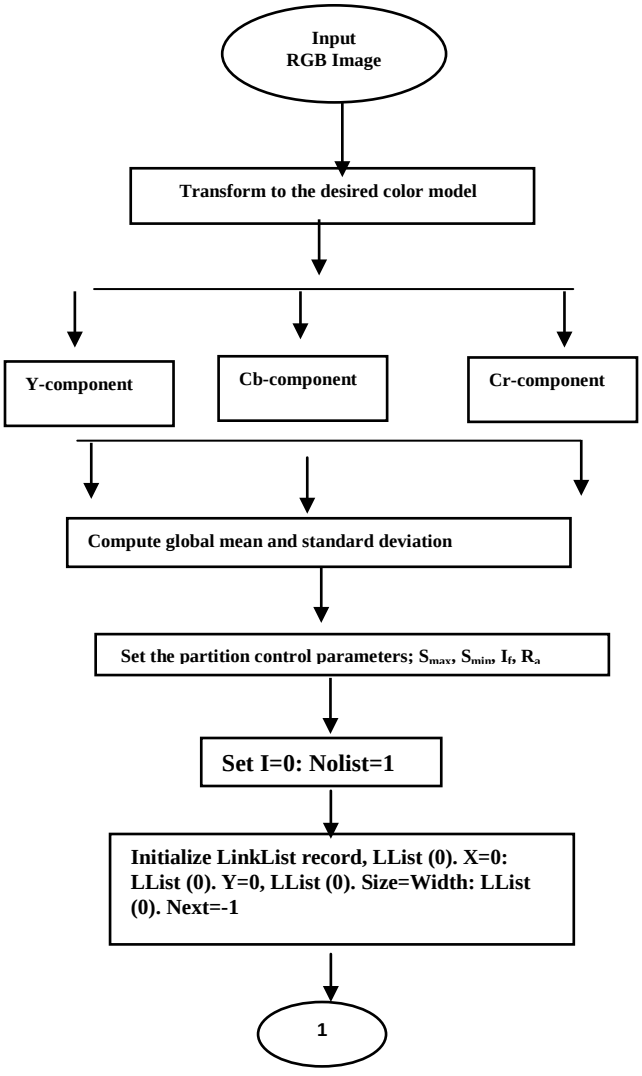
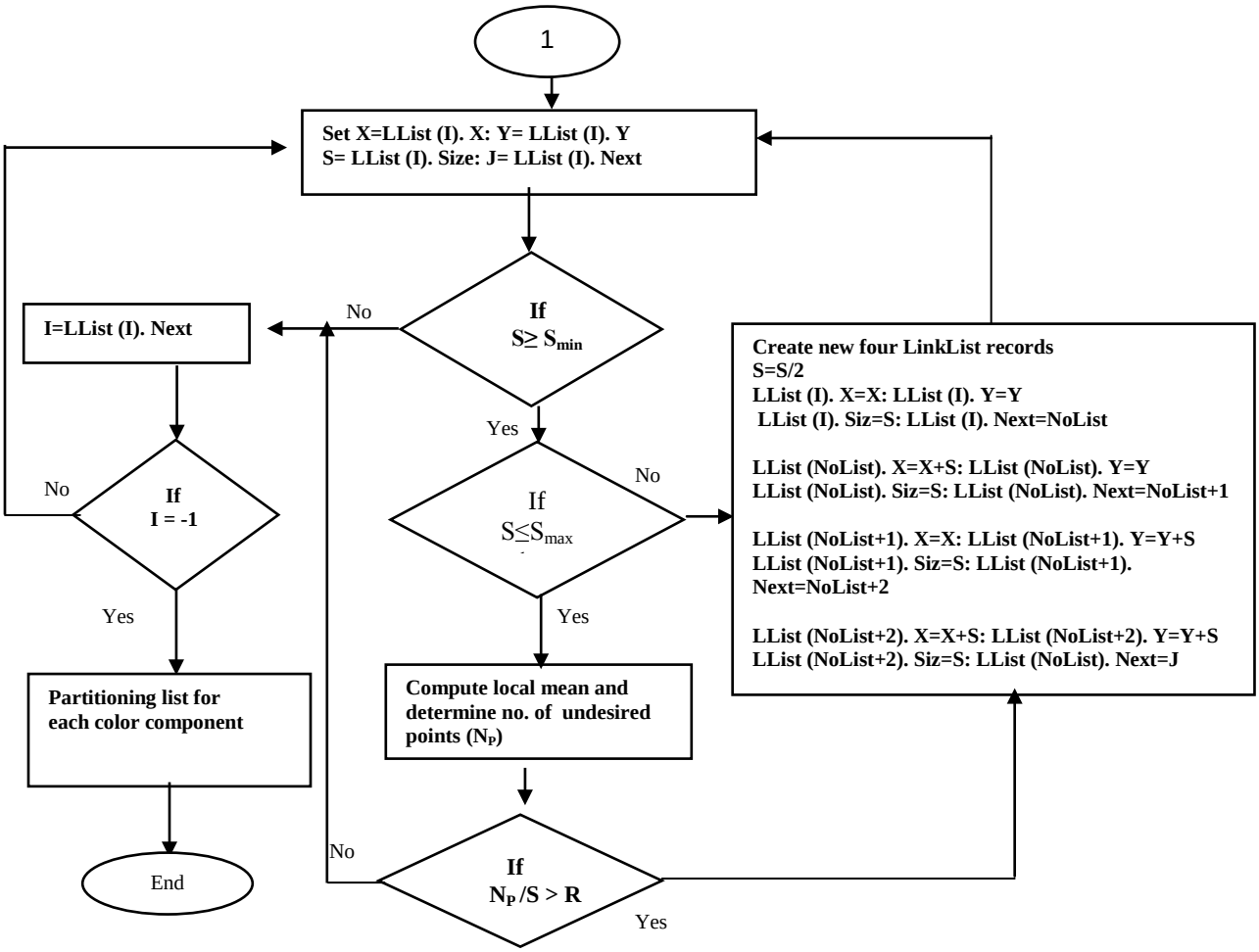


Figure (3): Illustrates the quadtree partitioning procedure



Continuation of figure (3)

2.2.3 Fractal Image Compression

For more details about fractal image compression[**[6], [7], [8].**

2.2.4 Secret Message Embedding

For embedding the secret massage, a new method has proposed and in this a new method a huge number of characters can be embedded, beside the characters or the secret message there may not necessary be a text, it may consist of equation or numbers with another language. After the IFS mapping is coming to the end of the last block and the parameter values

have been set, the process of embedding starts by reading the inputted secret message and

converting it to its binary representation then store them in a new array separately**[9].**

Next, the secret message (SecData) characters are taken one by one and they are converted to its ASCII representation. The length of the secret message is limited to the number of blocks. As the number of blocks increase in tern more characters can be embed, in other words this embedding method depends upon the number of blocks.

Length of secret message (SecData) = (No. of blocks ×2) -1

Each character is embedded in the scaling value of the blocks by taking the integer part of the scaling using this equation

V= IFS(I). Scl – Fix (IFS(I).Scl)

Then taking the two digit of the fraction part (2 digit after the decimal point) of the value and neglecting the other digits

IntFraction = fix(V×100)

Fraction =IntFraction ×0.01

Now the secret message will be added to the fraction value in order to occupy the **3rd, 4th** and **5th** places after the decimal point without affecting the **1st** and **2nd** places of the original fraction.

IFS(I). Scl = Fix(IFS(I).Scl) + Fraction +SecData(I) ×0.00001

The output is a set of scale and offset values that contain the secret massage (SecData) is the last stage in hiding unit

2.2.5 Information Extraction Unit

Extraction units are arranged in a reverse order to the hiding unit. It consists of these stages as illustrates in **figure (4)**

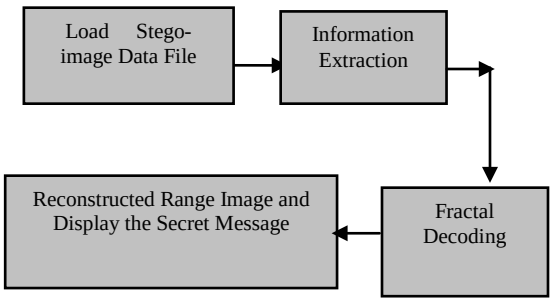


Figure (4): Structure of extraction unit

2.2.6 Information Extraction

After the data file (stego-image) has been loaded, the process of reconstructing SecData is applied to extract the array of embedded secret characters, which have been stored in the (IFS) coefficients (s, o) in a reverse way. This stage implies the following steps:

1. Extract the two digit of the fraction part of the coefficient (s and o) with keeping the integer part.

V= IFS(I).scl – Fix (IFS(I).scl)

Vs = v ×1oo

2. Convert the extracted data to byte

SecData(I) = CByte((Vs – Fix(Vs)) ×1000

3. Convert the bytes to string representation

recSecData =recSecData & CStr(Chr(SecData(I)))

4. Display the secret message.

3. System Implementation

The goal of this system is encoding and embedding or hiding information (text, numbers, symbols or equations) in a cover-image (BMP format) after compressing the image to produce the stego-image as a data file. System implementation accepts six inputs in the embedding stage**:**

1. Input Text to be Encoding and Hiding
2. Encoding the text by using new IFS cryptography approach
3. Loading the cover image (BMP. format) as the input file
4. Input control parameters
5. Quad-tree partitioning the colour component
6. Domain generating
7. Inputting the secret message for embedding
8. Fractal encoding which include embedding.

System implementation accepts one input in the extracting stage:

1. Input the data file which contains the secret message beside image data array.
2. Extracting the secret message and reconstructing the image in the same time.

3.1 System Requirements

The Microsoft Window XP has been used as an operation system and Visual Basic (VB6) as a programming language.

3.2 System Steps

The proposed system steps:-

- **Input Secret Message**
- **Encoding Stage by using New IFS Cryptograph method.**
- **Partitioning the Cover Image**

After the cover-image has been chosen, control parameter will be entered to perform quad-tree partition for each colour component (R component, G component, B component) separately.

- **Generating the Domain Image**

Generating the domain image and domain pool is next to the partition step, the domain size taken is quarter the image size with overlapped blocks.

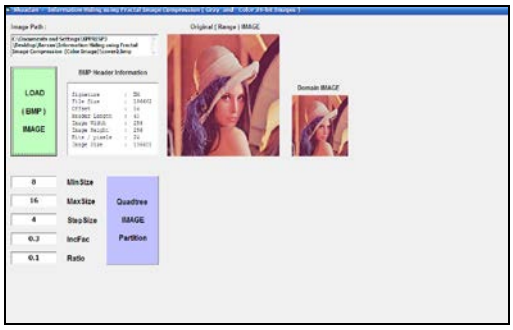


Figure (5): Domain image generating

- **Fractal Encoding**

Searching for similarity is performed between the range and the domain blocks and the information is stored in an index, then the image (cover-image) information is stored as a structure array of data.

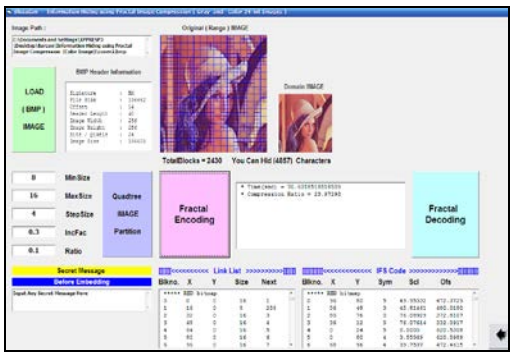


Figure (6): Fractal encoded data

- **Fractal Decoding**

The received data is a collection of data that represent the image with the secret message. The receiver will extract the embedded information (secret message) and then reconstruct the cover image.

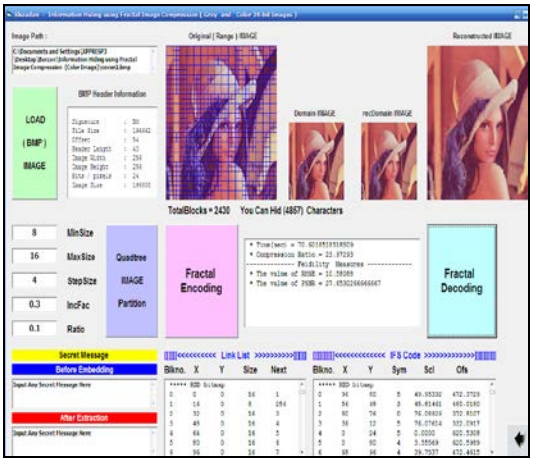


Figure (7): Secret message extraction and cover image reconstruction

3.3 The Effect of Hiding Secret Message

The main objective of the proposed hiding scheme is to embed a secret message with a huge number of characters as possible with different languages and numbers without degrading the quality of the reconstructed cover image. So to evaluate the effect of the secret message embedding on the cover image, a set of tests is applied. **Table (3)** show the result of hiding different message process.

Table(3) Hiding effect on Lena image

Max=8, Min=4, StepSize=4, R_a = 0.1, I_f =0.3, PSNR1= Stegoimage fidelity,PSNR2= After extraction fidelity, PSNR3= Without embedding					
N0.char	**Type**	**Time(sec)**	**PSNR1**	**PSNR2**	**PSNR3**
9653	**English-text**	**100.78**	**31.056**	**31.056**	**31.064**
10283	**Arabic-text**	**101.78**	**31.694**	**31.055**	**31.064**
11390	**Mixed**	**102.94**	**31.0644**	**31.064**	**31.064**

Table (4) Testing the effect hiding on Baboon image

Max=8, Min=4, StepSize=4, *Ar* = 0.1, *If*=0.3, PSNR1= Stegoimage fidelity, PSNR2= After extraction fidelity, PSNR3= Without embedding					
N0.char	**Type**	**Time(sec)**	**PSNR1**	**PSNR2**	**PSNR3**
9653	**English-text**	**116.54**	**23.246**	**23.246**	**23.246**
10248	**Arabic-text**	**117.85**	**23.246**	**23.246**	**23.246**
19950	**Mixed**	**118.74**	**23.246**	**23.246**	**23.246**

4.0 Conclusions

1. In this paper we have presented a new method to design a cryptographic system utilizing fractal theories. This approach employs two level methods, the firstly by using new approach fractal cryptography (encoding and decoding), and the secondly by hiding the encoding text by using proposed fractal image compression , which make the decoding more difficult, by embedding the attractor in a colored image using the LSB; and sending it to the recipient to decode the colored image and applying the key agreement to get back the message characters, by the collage method. This way to hide information is very useful cause even if the third party (intruders), recognized that there is a difference in the received image, wont figure what its , whether a lose in the information or just a rubbish data.

2. For embedding the secret massage, a new method has proposed and in this new method a huge number of characters can be embedded, beside the characters or the secret message there may not necessary be a text, it may consist of equation or numbers with another language.

3. The proposed system does not affect the image quality; we can say it is not noticeable for human eyes. To prove this we show the cover-image and the stego –image to a team of 15 persons to take their opinion if there is any difference between the stego-image and the cover-image and their answer that there is no difference between both images.

References

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

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

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

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

[5] Fadhil Salman Abed, Nada Abdul Aziz Mustafa**, " A proposed Technique for Information Hiding Based on DCT",** International Journal of Advancements in Computing Technology Volume 2, Number 5, December 2010.

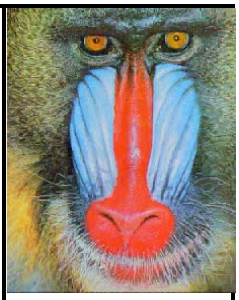
[6] Y. Fisher, "**Fractal Image Compression: Theory and Application**", Springer-Verlag, New York, NY, USA, 1995.

[7] Fadhil Salman Abed,"**Adaptive Fractal Image Compression**", Ph.d Thesis, Al-Rasheed College of Engineering and Science, University of Technology, 2004.

[8] Sua'd Kakil Ahmad, "**Image in Image Hiding System Using Iterated Function System (IFS)**", Msc Thises, University of Sulaimani, 2009.

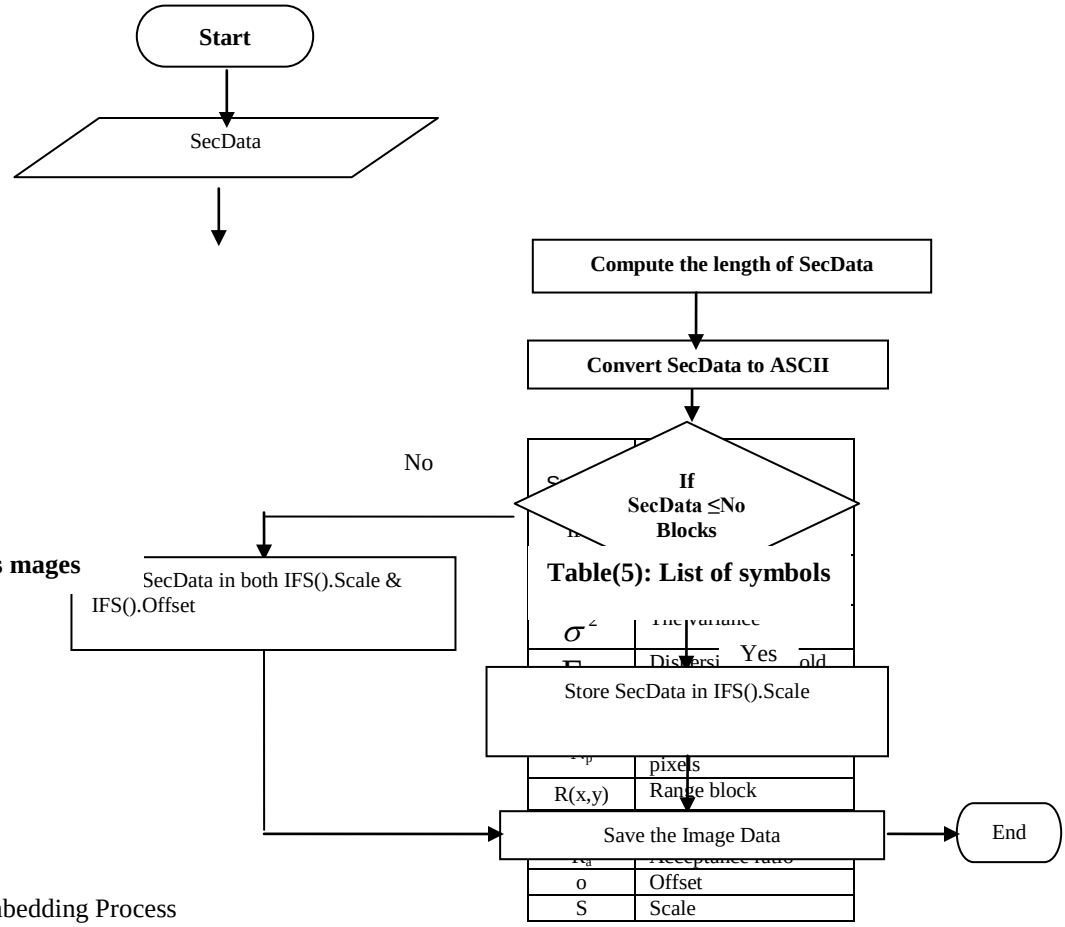
[9] Manoj Kumar Meena, Shiv Kumar, Neetesh Gupta**,"Image Steganography tool using Adaptive Encoding Approach to Maximize Image Hiding Capacity**", International Journal of Soft Computing and Engineering (IJSCE) , ISSN: 2231-2307, Volume-1, Issue-2, May 2011.

Fadhil Salman Abed is a lecturer at the Depratement of Computer Sciences, Technical Institute of Kalar.. He received the B.Sc. degree in Mathematic from the University of Basra, Iraq, in 1987. He obtained his M.Sc. in Applied Mathematic(Computer Security) from University of Technology in 1997 and Ph.D. degree in Applied Mathematic(Fractal Image Compression) from University of Technology in 2004 . His research interests are in the field of Cryptography, Image Processing, Network secur has many research papers in Image Processir computer security.

	
Original Lena image256×256	**Original Baboon image256×256**

Apendix

Table(6): The Some of Tests mages



Table(5): List of symbols

σ^2	The variance
	Dispersi old
	pixels
R(x,y)	Range block
	Acceptance ratio
o	Offset
S	Scale

Figure (8) Flowchart of Embedding Process