Image Encryption Techniques Using Fractal Function : A Review

Article *in* International Journal of Information Technology and Computer Science · April 2017

DOI: 10.5121/ijcsit.2017.9205

1 author:

Shafali Agarwal
JSS Academy of Technical Education
27 PUBLICATIONS **271** CITATIONS

IMAGE ENCRYPTION TECHNIQUES USING FRACTAL FUNCTION: A REVIEW

Shafali Agarwal

[1]Department of Computer Applications, JSS Academy of Technical Education, Noida, India

ABSTRACT

An increasing demand of secure data transmission over internet leads to the challenge of implementing a consistent cryptosystem. In 2004, USA navy published the patent which highlights the importance of fractal as an encryption/decryption key in a cryptosystem [1]. Fractal possess butterfly effect i.e. sensitivity to initial condition, due to which small change in input produces a major change in output. This paper summarizes the various recent image encryption techniques in which fractal key is used to encrypt/decrypt followed by substitution, scrambling and diffusion techniques to provide strong cryptosystem. The algorithms covered both private key encryption as well as public key encryption technique in the paper. The analysed algorithms include a set of fractal function such as Mandelbrot set, Julia set, Hilbert curve, 3D fractal, multi-fractal, IFS and chaotic function to generate a complex key used in the encryption process. Corresponding performance of each algorithm is analysed by PSNR test, key space, sensitivity analysis and correlation coefficient value between the adjacent pixels of both images (Original image and encrypted image) which shows significant improvement in performance over the traditional encryption methods.

KEYWORDS

Image Encryption, fractal, chaotic function, Scrambling, NIST test suite

1. INTRODUCTION

Now a days, a huge amount of data in terms of text, image, audio and video has to transmit over the network. An image carries lot of information compared to text hence importance of secure transmission of an image increases. Because of sensitivity of image data, enormous size, high correlation among pixels of images and strong redundancy of uncompressed data traditional encryption methods are not suitable to achieve strong level of security of transmitted data. The requirement of such a system arises so that illegal acquisition, modification, alteration, copying and unauthorized accessing can be prevent and data must be transferred with original contents. In some systems, image transmission is an important tool to pass detailed information like medical imaging, military communication, scientific observation, health care, multimedia, picture messaging application on cell phone, biological data etc. An efficient, strong and reliable encryption method is required to achieve a secure transmission of confidential data over the network.

Image encryption is a technique used to convert original image into another image which is not identifiable by unauthorized user [2, 3]. This is a method of transferring the information embedded in a digital image to a non-recognizable form so that no one can access the data except those having details of decryption method with key required to decrypt the data.

DOI:10.5121/ijcsit.2017.9205

An important tool in image encryption is scrambling deals with change in position of the pixels and helps to minimize the correlation coefficient value[4]. If correlation coefficient between original image and encrypted image is zero or near to zero, hacker will beunable to guess the encryption method or key.Recently authors [5] used DNA sequences as a secret key and implemented permutation process using Hao's fractal representation. They also used diffusion and scrambling to make the encryption process more secure and complicated. There are remarkable methods available to achieve this such as steganography, water marking and cryptography. The effectiveness of an image encryption algorithm can be analysed in terms of parameters like histogram analysis, adjacent pixel correlation analysis, mean value analysis, key space analysis, encryption speed and number of pixels change rate (NPCR) and unified average changing intensity (UACI) tests. In the paper [6], authors conducted all the above given tests to measure the security and performance issues of an image encryption algorithm using a key image which is a binary image of same size as of original image (Introduction). This paper focuses on reviewing cryptography methods using fractal & chaos to encrypt/decrypt the digital images.

2. PRELIMINARIES

2.1 Cryptography

Cryptography: The art of converting plain image into an unidentifiable cipher image is known as cryptography. The basic terms used in cryptography [7]:

1. Plain image: An original Image which is to be transmitted from sender side to receiver side over a network.
2. Cipher image: After applying an encryption technique, obtained coded image is known as cipher image.
3. Encryption: A method used to transform a plain image to cipher image is known as encryption.
4. Decryption: The process of restoring plain image from cipher image at receiver side is known as decryption.

A cryptosystem uses two different keys to encrypt/decrypt the data known as public key and private key. On the basis of these keys, cryptography can be categorized broadly in two categories:

1. Private Key Cryptography: Private key/symmetric key encryption deals with the same key used to encrypt and decrypt the data. At the time of transmission, sender uses the secret/private key to encrypt the data. The encrypted data with secret key is then transmitted to the receiver so that decryption process can executed using the shared secret key at receiver side. In this cryptosystem shared key has to be transmitted from one location to another required a secure transmission channel so that an unauthorised person should not be able to access the key. Figure 1 represents the working of public key cryptosystem.

   This is the area in which researchers are doing continuous research to generate a secure shared cryptographic key and a strong key transmission process to establish a highly reliable and acceptable cryptosystem.

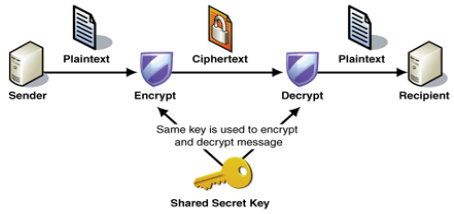

Figure 1. Private Key Cryptosystem

2. Public Key Cryptography: Public key/asymmetric key encryption method was discovered by R. Rivest, A. Shamir and L. Adieman in August 1977 issue of Scientific Americans [8,9]. The idea of public key cryptography is to encrypt the image using public key of receiver at sender side and transmit it to the receiver. On the other hand, receiver used its private key to decrypt the cipher image and translate it in plain image. The entire working of public key cryptosystem is depicted in figure 2.The technique ensures that cipher image is originated using public key of owner of paired private key whereas at receiver side, private key of that particular paired key is used to decrypt the data without compromising the security of the system. Security lies in the fact that public key may be used by anyone to encrypt the data and private key kept private to the owner of paired key.

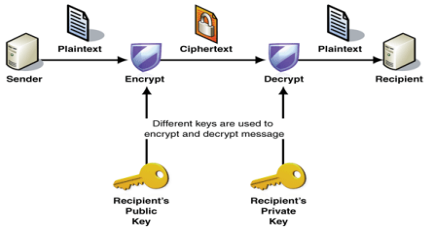

Figure2. Public Key Cryptosystem

Diffie Hellman established one of the earliest example of public key exchange protocol in the field of cryptography [10]. In which key exchange notion established a secure channel between sender and receiver so that both parties can exchange data over that network without having prior knowledge of each other. With the help of exchanged data both sender and receiver produced their private keys which is further used in encryption/decryption process.

2.2 Fractal in Cryptography

Fractals [11] are non-regular geometric shapes that have the same degree of non-regularity on all scales. French mathematician Gaston Julia in 1918 investigated the iteration process of complex function and attained a Julia set and gave a direction to the fractal world [12]. Later Benoit Mandelbrot in 1979 studied a very complex & perturbed structure that is known as Mandelbrot set [13]. Researchers have done incredible research to unveil the geometrical and functional ambiguity of both the sets[14][15]. The definition of Mandelbrot set is given in [16] as "The Mandelbrot set is the set of values of c in the complex plane for which the orbit of 0 under iteration of the complex quadratic polynomial $z_{n+1}=z_n^2+c$ remains bounded". Similarly Julia Set is the set of points K whose orbits are bounded under the iteration is called the Julia set. We choose the initial point 0, as 0 is the only critical point of the given function [17, 18].

Fractal images exhibits the randomness property, appropriate to design a secure and reliable cryptosystem. Fractal based cryptosystem is designed using complex number rather than the prime numbers, thus the generation of private key and public key is carried out using complex numbers arithmetic. The chaotic nature of fractal leads to the sensitiveness of the key value towards initial value, makes it difficult to produce accurate key by intruder. Additional advantage

of using fractal as key is the key size which generally impact on the number of guesses that an attacker would need to make in order to find the key e.g. brute force attack *i.e.* it determines the feasibility of a collision attack. In previous traditional techniques, key size depends on the existed prime numbers in the given range. In case of using the fractal key, the exchange key space depends on size of the keys, which extend the key space, shrink the key size and make it more complex [19].

A project was carried out in 2003 to encrypt a message with the help of random numbers and Mandelbrot set fractal. At that time fractal was not so much popular in cryptography system. Author succeed to encrypt the data but unable to decode the same. A perfect decoder required a mapper so that no number came out twice [20].A new approach of encryption using fractal geometry is discussed by the author in which a fractal is generated by using some initial parameters and then use it to encrypt a predetermined length of message by using fractal orbits to corresponding alphabet mapping [21].A novel Image encryption technique using single as well as multi-fractal images is proposed in the paper [22]. The information about source image is hidden in the complex structure of used fractal. The structure of the underlying system consists of three main processing sub-blocks: key generator (depends on the selected fractal and shift values), delay and multiplexing block. It has been noticed from the correlation result that to increase the pixel confusion, a non-linear multiplexing with one bit delay is required. Sometimes encrypting compressed images gives a reduced time outcome as well as good quality image reconstruction. A stream cipher encryption algorithm implemented on a compressed image in which a fractal dictionary encoding method is used in the image compression to achieve good quality image reconstruction [23]. This is followed by a data pre-processing step before performing actual encryption on the plain text. To introduce perturbation in the stream cipher, diffusion is realised to a certain extent.

3. LITERATURE REVIEW OF FRACTAL BASED IMAGE ENCRYPTION TECHNIQUES

In 2004, secretary of the navy of USA published the patent which shows the importance of fractal as an encryption key in the encryption process [1]. A symmetric key encryption method is used to encrypt/decrypt image data with the help of fractal key. In the whole process image data as well as encryption key will be represented in the form of 2D matrix.

Process: The encryption procedure can be explained in two parts. One part is concerned with the generation of fractal key whereas actual encryption of given image takes place in next step.
Key Generation Method:

1. Initially select a fractal and fractal key matrix size (square matrix) which must be aligned with the data matrix.
2. Choose fractal initial condition such as starting location within fractal image, resolution, bailout etc. to compute fractal.
3. Obtain a fractal image using fractal initial conditions, sampled it and then map it to fractal key matrix.
4. Compute rank of matrix. If it is full rank then proceed otherwise reiterate it with different fractal parameters.

Encryption/Decryption Method:

1. After generating fractal key, form a two dimensional matrix of buffered data which is to be encrypted.

2. Apply matrix multiplication between fractal key matrix and data matrix and obtain encrypted data using function:
   $E=P*K$ (1)
   Where P=the buffered data matrix ($J*N$);
   K=the fractal key matrix ($N*N$);
   E=the encrypted data matrix ($J*N$).
3. Transmit the encrypted data, encrypted data matrix dimension and fractal initialization values to the receiver.
4. At the receiver end, receiver regenerate fractal key and its inverse fractal key matrix so that it can be multiply with encrypted data matrix using function:
   $P=E*K^{-1}$ (2)
   Where K^{-1} is the inverse fractal key matrix, such that P is the matrix of decrypted, original, buffered data of dimension $J*N$.

Once the required data is decrypted, sometimes reformatting is essential to get the original data.

Performance Analysis

In the proposed method fractal is used as an encryption key, provides a more secure medium to generate key. Author used 2D matrix multiplication operation to generate cipher data, mark it widely acceptable for any kind of data *i.e.* text, image etc. which can be convertible into 2D matrix form.

Key exchange is a method used in a public key cryptographic system, in which sender and receiver exchanged secret key or few parameters over a public channel. In 2007, Alia and Samsud in proposed a key exchange protocol utilized the intrinsic relationship between Mandelbrot set and Julia set [24].

1. Authors used c and x as global variables and known to the public, e and n as private variables for the sender and k and d as private variables for the receiver.
2. Using Mandelbrot set function system generated corresponding public keys for sender $(z_n\, e)$ and receiver $(z_k d)$.
3. These public keys are then exchanged between both parties.
4. Private keys are produced with the help of information retained on the respective side itself and received other's public key $(z_n\, e)$ and $(z_k \mathrm{d})$ using Julia function.
5. As a resultant, private keys $(z_k d)_n e$ and $(z_n e)_k d$ are generated on both sides. So security lies in the fact that no need to transmit private keys over the network.
   At sender side,

   Mandelfn: $z_n = c*f(z_{n-1})$
   $f(z_{n-1})=z_{n-1}*c*e,\ z_0=c$ (3)

   Juliafn: $z_n = c*f(z_{n-1})$
   $f(z_{n-1})=z_{n-1}*e,\ z_0=(z_k d)$ (4)

Similarly both functions will work for receiver side also.

Performance Analysis

Key size plays an important role to prevent brute force attack. If we consider 128 bits size key, Diffie- Hellman protocol depends on the number of primes existed in 2^{128} possible key values whereas key space in fractal key exchange protocol based on the size of the key.

Authors utilized the same concept of key exchange between the sender and receiver and generated private key secretly. Following this process by creating cipher text at sender side using Juliafn with input parameters*k* and *d*. After receiving cipher text, receiver also used the same Juliafn with input parameter *n* and *e* and decrypt the message to the original [25].

Performance Analysis

A detailed comparative analysis is carried out by the authors to depict the importance of recent fractal based cryptosystem over traditional RSA based cryptosystem. The proposed algorithm is better resulted in terms of key generation time and execution time (encryption as well as decryption).

The proposed cryptosystem used key based on fractal image to encrypt the plain image in the paper [26]. The main advantage to use fractal key is its small key storage requirement and robustness to the attack.

Encryption and Decryption Process:

1. Fractal image is converted into three matrices representing R, G & B layers of pixels of the image.
2. Fractal key is generated using the given equation-

$$dij = \sum_{k=1}^{k_{max}} \sum_{l=1}^{l_{max}} r(i,j,k,l) * d_{K,L} \tag{5}$$

3. To calculate it, grid of coloured pixels is constructed with spacing δ.
4. Now for each grey pixel, add all the pixels from the grid with let suppose $\delta = 4$.
5. Identify one black pixel with appropriate weight and calculate distance between black pixel and each of the grey pixel.
6. The distance value would be different for each pixel, hence a stronger key will be generated.
7. Repeat the process for all three layers of the image to be encoded.
8. Perform encryption of plain image with the generated fractal key using given equation:

$$e'_{ij} = (e_{ij} + d'_{ij}) \bmod 256 \tag{6}$$

9. In decryption process, first key is generated using fractal parameters and then reverse the modulo operation to get decrypted image:

$$e_{ij} = (e'_{ij} - d'_{ij}) \bmod 256 \tag{7}$$

Performance Analysis

In the proposed method, δ must be chosen wisely so that algorithm could lead to a secure encrypted image. It must not be so close as well as not extremely large (such as size of an image). Author also performed PSNR test in the interval $\delta \in \{20, 120]$ to test the efficiency of the proposed cryptosystem and concluded that the improved result are possible for $\delta = 1023$.

A new cryptographic system based on fractal generated by IFS transformation proposed by the author in 2009 [27]. To increase the security of the given system, double enciphering and deciphering method was applied to the data. The main purpose to fractal based image coder is to utilize self-similar property of the IFS. In this way, determine a subset of the whole image and approximate it using contractive affine transformation to the object.

Encryption Process

1. At first level of enciphering, author assumes the total number of chosen characters n=29.
2. Divide complete message into the length of three m=3 represented by $p_i p_{i+1} p_{i+2}$.
3. Calculate numeric value of each unit using $p_i n^2+p_{i+1} n+p_{i+2}$ (first level of enciphering code in integer value).

Note: In the given method, sender and receiver must be agreed upon the classical encryption method as well as order of affine IFS maps.

Fractal based on IFS can be used as a secret key to encrypt the p unit data of length m at a time in n letter alphabet if f$GCD(D,n_m)$= 1, where D= determinant of $m*m$ matrix.

To perform next level enciphering, first specify the encryption key which is the set of contractive affine transformation $B(X)=AX+b$, depends on the arrangement of the elements in IFS invertible map. Apply random iterated algorithm to generate attractor A that is nothing a representation of unique fixed point of contractive form of B.

Decryption Process:

After receiving attractor A by receiver, It works on range block (R_b) refers to a big block of an image and domain block (D_b) which was generated by partitioning an image into non-overlapping block of fixed size. The objective of deciphering algorithm is to express R_b as a set of transformation to be applied on a particular D_b. Ultimately find out affine IFS transformation B using inverse problem. At last perform algebraic calculation to find the values of p_1, p_2 and p_3 and combine the result to frame the actual message.

Performance Analysis

The possibility of high security enhanced with the proposed IFS fractal based encryption techniques. The complex visual property hides maximum amount of data in an image without degrading the quality of it.

The paper is designed to implement asymmetric cryptographic approach to encrypt digital Images. Author utilized the complex mathematical structure and deterministic nature of fractal to propose a new public key cryptosystem based on IFS [28]. The paper is explained mainly in three parts:

- Key Generation
- Encryption
- Decryption

In key generation process, take matrix H, g and p (prime numbers) variables, which are known to the public. In first step generate numbers (x, y, s) and (x', y', r) as receiver and sender private keys. Now calculate $F_s=g^s(mod\ p)$ and $F_r = g^r(mod\ p)$ and exchange between sender and receiver as public key. After receiving F_r, a shared private key $n=(F_s)^r(mod\ p)$ is generated by receiver, used as a number of iterations in generating fractal attractor W^n.

At last receiver and sender calculate their public keys (u, v, 1) $=W^n(x, y, 1)$ and (u', v', 1)$=W^n(x$', y', 1) with the help of W^n and exchanged it.

In encryption process, sender uses its fractal attractor W^n and its private key (x', y') to encrypt the given text sent to the receiver.

To decrypt, receiver receives cipher text and uses his private key (x, y) and fractal attractor W^n to recover the text from the cipher text.

Performance Analysis

Authors proposed and analysed the fractal based cryptosystem using RSA system. According to study, the proposed system is more efficient in terms of key generation time, key space and time required for encryption as well as decryption [29].

Mandelbrot set is one of the complex fractal with infinite boundaries. Author utilized the randomness of Mandelbrot set and generated encryption key using Mandelbrot set and Hilbert curve transformation [30].

Process started with the formation of three matrices of each layer of a colour image i.e. red, green and blue. The value range of each pixel in matrix is [0, 255].

The used encryption function is:-

$$T(x, y) = (O(x, y) + k(x, y)) \bmod 256 \quad (8)$$

Here T represents the image after encryption and k represents encryption key.

To generate an encryption key, apply Hilbert curve transformation to the Mandelbrot set, which makes key more secure and sensitive. Authors calculated interval distance 'r' from one point to another in the matrix and then checked the distance between points $H(x_n,y_n)$ and $i(x, y)$. If the distance value is multiple of 'r', then the value of $H(x_n,y_n)$ is multiplied by the real distance. The equations are-

$$\forall\, D \in R_{key}, B_{key}, G_{key}\ \exists D_{x,y} \colon \forall x \in [1, n], \forall\, y \in [1, n]$$

$$K(x,y) = \sum_{i=0}^{p} H(x_n,\ y_n) * d(H, i)$$

Where $p = (n*n)/r$, $d(H,i) = \sqrt{(x_n - x)^2 * (y_n - y)^2}$ (9)

Where n represents number of columns = number of rows (assuming matrix size $n*n$)

Performance Analysis

In this paper, a comparative performance analysis is carried out with the paper proposed by Rozouvan[26].

The range of interval distance r in current experiment is [1, 65025], whereas in paper [26], it was [0, 254]. PSNR value rapidly increases when r crossed its critical value. In the experiment implemented by Rozouvan, the critical value of r was 150, whereas Yuan-Yuan Sun et al. achieved a remarkable improvement in the critical value of interval distance r i.e. 40,000.

Author proposed a cryptosystem based on hash algorithm MD5 and fractal [31]. This system is suitable to encrypt/decrypt text file, image file and audio file.

Encryption Process:

1. Author starts the encryption process by guessing a variable length key.
2. Selected key is used to generate 128 bits message digest using MD5 hash algorithm (one way hash function).

3. This message digest worked as a seed to generate a fractal using Julia set algorithm.
4. At last generated fractal will be used as chaos to encrypt the given data through XOR operation on each block of data.

Decryption Process

1. In decryption process, selected key is transmitted to the receiver end with encrypted data.
2. Evaluate message digest using the hash algorithm i.e. MD5.
3. Generate fractal using message digest as a seed in Julia set algorithm.
4. Perform XOR operation with the cipher file to get back the original data file.

Performance Analysis

Author utilized the usual feature *i.e.* sensitive to initial condition and pseudo randomness of fractal images. They also performed signal to noise ratio test and concluded that higher the cipher text value gives better confusion to crack the code.

Author proposed a method to improve the performance of DES algorithm by using 3D fractal images as a key [32]. The method works according to the following steps-

1. Author selected a colour fractal image and used diamond square algorithm to take midpoint depends on points in four directions and then apply Brownian self-similarity method to increase randomness by adding some random number to the average of these four points.
2. Convert this 2D image into 3D image to increase key space so that choice of control points makes counterfeit impossible and make the key more differentiable and random.
3. Clip as many different keys from the resultant image as you want.
4. Split to be encrypted plaintext according to the length of key.
5. Convert plaintext into binary representation.
6. Each individual key clipped from the 3D image encrypted the plaintext segment using DES algorithm and generated cipher text.
7. At the receiver end, fractal parameters were passed and generated the same secret key to decrypt the data.

Performance Analysis

With the Introduction of fractal in the key generation, a modified DES is applied to the system, resulting high randomness and more secure cryptosystem is achieved.

Author utilized the Infiniteness and chaotic behaviour of Julia set and complex structure of Hilbert curve to implement the cryptosystem [4]. The complete process is described as follows:

Encryption Process

The security of the proposed cryptosystem lies in the fact that the final cipher image is generated in two steps:

1. Apply escape time algorithm to generate Julia set image
2. Use boundary of the Julia set image because it is observed that tiny perturbation can cause drastic change in Julia Image at the boundary.
3. Convert image into two dimensional array in the form of R, G and B matrix.

4. Scramble each matrix with Hilbert curve to a key image matrix using scramble function as:

$$a_i = \begin{cases} b_i \,\&\, a_i, & i=1, 3, 5, 7 \\ c_i \,\&\, a_i, & i=0, 2, 4, 6 \end{cases} \quad (10)$$

5. Encrypt plain Image with scrambled image using modulo operation:

$$e'_{ij} = (e_{ij} + d_{ij}) \bmod l \quad (11)$$

Where e_{ij} – pixel value of (i, j) coordinate of plain image

d_{ij} - pixel value of (i, j) coordinate of scrambled image
l – length of used colours in image *i.e.* 256

6. Apply diffusion to temporary cipher image using following function:

$$q_i = (p_i + p_{i+1} + q_{i-1}) \bmod l \quad (12)$$

Where q_i and q_{i-1} are pixel values in the cipher Image, p_i&p_{i+1} are the pixel values in the temporary cipher Image. Finally obtain encrypted image which is to be transmitted to the receiver side.

Decryption Process

1. At receiver side, same key will be use to decrypt the received cipher image. Decryption process is just opposite of the encryption method. The procedure starts with the diffusion using the equation:

$$P_i = (q_i - p_{i+1} - q_{i-1}) \bmod l \quad (13)$$

2. In next step, modulo operation decryption takes place with the help of following equation:

$$e_{ij} = (e'_{ij} - d_{ij}) \bmod l \quad (14)$$

3. At last unscramble the matrices to obtain the plain image.

Performance Analysis

In the paper, authors obtained cipher image by applying Hilbert scrambling and diffusion process which makes the proposed cryptography more secure in terms of key sensitivity, chosen plain image attack and entropy attack. Even the given system passed sp800-22 test suit and proved the randomness of obtained cipher image.

The authors have used the strong connection between Mandelbrot set and Julia set to create a shared private key on sender as well as receiver side. The proposed algorithm focused on superior Mandelbrot set and superior Julia set to obtain a highly secure and complex cryptosystem [33].

1. Authors used c as global variables and known to the public, e and n as private variables for the sender and k and d as private variables for the receiver.
2. Using Superior Mandelbrot set function *supMS* system generated corresponding public keys for sender ($z_n\, e$) and receiver ($z_k d$).
3. These public keys are then exchanged between both parties.
4. Private keys are produced with the help of information retained on the respective side itself and received other's public key ($z_n\, e$) and (z_kd) using Superior Julia set function *supJS*.

5. As a resultant, private keys $(z_k d)_n e$ and $(z_n e)_k d$ are generated on both sides which do not need to transfer over the network.
   At sender side,
   supMS: $f(z_n) = z_n * c * e$; $c, z \in Z$ and $z_0 = c$

$$z_{n+1} = s * f(z_n) + (1-s) * z_n \quad (15)$$

   supJS: $f(z_n) = z_n * c * e$; $c, z \in Z$ and $z_0 = z_n e$ (at receiver side)

$$f(z_n) = z_n * c * e;\ c, z \in Z \text{ and } z_0 = z_k d \text{ (at sender side)} \quad (16)$$

Equation (17) is common to both sides:

$$z_{n+1} = s * f(z_n) + (1-s) * z_n \quad (17)$$

Note: Superior Mandelbrot set and superior Julia set are obtained by applying Mann iteration to the Mandelbrot set and Julia set function respectively [34].

Performance Analysis

The given algorithm also utilized the property of fractal in terms of randomness, highly sensitive to initial condition and key size. The use of fractal as an encryption/decryption key provides a wide range of available keys as compared to traditional Diffie-Hellman algorithm [10].

Authors have applied wavelet transform, fractal based encryption key and substitution of pixels through chaos function to design a cryptosystem used in social networking [35]. The advantages of wavelet transform to reduce the image size, consequently minimized the calculation time of proposed method as well. The complexity of the system is enhanced by applying two levels of encryption using fractal and chaos function.
Encryption and Decryption Process

1. The process starts with the image size reduction by approximately one quarter using "Haar" wavelet transform method.
2. Derive three matrices having data corresponding to rounded absolute value, decimal digits and sign value of resultant image respectively.
3. Initially apply encryption method expounded by Rojouvan in [26] to achieve first level of encryption of the extracted image.
4. In next step, chaotic function is used to obtain final encrypted image in two parts:
   - The replacement of rows and columns take place using a logistic function:

$$x_{n+1}=4x_n(1-x_n) \quad (18)$$

   The given process repeated until a new x_0 is obtained such that the following equation satisfied:

$$l=\text{mod}(x_0 * 10^4, M) \quad (19)$$

   Where M denotes the number of rows or columns of an image matrix and l must be a distinct value and lies in the range [0, M-1].

   - In second step of encryption process, Chan chaotic sequence is generated. After processing image pixels with Chan chaotic sequence, an encrypted image is obtained which has to be transmitted over the network.

5. After receiving encrypted image, receiver apply XOR operation to decrypt the image using chaotic function.
6. Use fractal key to decrypt the image derived from previous step followed by using inverse of Haar wavelet transform function to execute final decryption step.
7. As a resultant decrypt original image obtained after executing steps 5 and 6.

Performance Analysis

The strength of proposed encryption algorithm tested using PSNR test, which indicates smaller the value of special parameter δ, gets the lower PSNR value results stronger encryption method. Next parameter to evaluate the strength of algorithm is the correlation between adjacent pixels of original image and encrypted image which may help hacker to decrypt the image. A test driven on both images and concluded that the correlation between original image pixels and encrypted image pixels is nearly to zero so no explicit relation exists between these two images. A well-known advantage of using fractal as encryption key is sensitiveness to its initial condition protects hacking of encryption key.

In a symmetric key encryption, host system has to transmit secret key through the communication channel, which is insecure and can be prone to hack by unauthorized user even though it is encrypted. To avoid exchange of key, author proposed a model to generate a real time encryption/decryption keys using quaternion Julia fractal image [36]. The various steps used in the given system are:

Initially host system established a connection with the receiver using SSL protocol.At the time of connection establishment, few parameters were initialized such as z, c&t=1.
At the transmitter side:

1. Construct a 3D plane inside a cube and compute Julia set for the parameter.
2. Checked intersection points of Julia set and the 3D plane.
3. Used curve fitting techniques to prepare curves and their corresponding polynomial equations.
4. Either choose block data or stream data to encrypt for time t.
5. Perform encryption of data with the pseudo random values from the prepared curve.
6. Transmit the encrypted data.
7. Set $t = t+1$

Further initialize z, n&c for new timestamp value, which is also used to check authenticity of the transmitting host. One important feature of this method is the use of AES symmetric encryption method but with different keys from the real time symmetric key generator for each block of data to be transmitted.

At the receiver end:

Receiver send either positive acknowledgement or negative acknowledgement to the transmitter based on the following fact that if receiving host is able to decrypt the encrypted data successfully, it sends positive acknowledgement to the transmitter. On successful completion of process, both host simultaneously update their time stamp by adding the number of iteration used in the last Julia set. In case of failure, a negative acknowledgement sent to the transmitter. Once response is received by transmitting host, a new session starts with updated timestamp.
Performance Analysis

Fractal images exhibit a complex mathematical structure and show chaotic behaviour. Due to which an infinite number of quaternion Julia set images can be generated within the given time

interval, make it impossible to identify parameters from the image.Three degree of randomness of symmetric key make it difficult to cryptanalysis and key prediction. Julia image intersect 3D plane at a random angle resulting in entirely different point of intersection. Also author verified that the proposed method proves all cryptography properties i.e. confidentiality, authenticity, integrity and non-repudiation.

A symmetric key stream cryptography algorithm is proposed by the authors in which cipher image incorporates both logistic chaotic map and Tent map [37]. The main feature lies in the use of secret key derived from the biometric images. The compete method can be described into three steps: key generation from biometric image, encryption and decryption. The detail is as:

Key Generation

1. Consider a biometric image *BI* in a matrix form *r*c*.
2. Merge pixel values horizontally using function-

$$BI(i,j) = BI(i,j) \oplus \Psi, 1 \leq \mathrm{i} \leq \mathrm{r} \;\&\; 1 \leq j \leq c$$

3. Divide the resultant matrix into *h*h* blocks and calculate the rounded mean value of each block (*M*).
4. Calculate the median value of main diagonal of each block (*N*).
5. Obtain secret key after performing BitXoring*M* and *N*.

Encryption Process

1. Convert source image to 1D pixel vector and encrypt pixel by pixel to its corresponding cipher pixel.
2. The used encryption function is-

$$C_i = \left((P_i \oplus C_{i-1}) \ggg round\left(10^4 * \sum_{j=1}^{rounds_j} T(X_j) \right) \right) mod\ 256$$

Where rounds are calculated using the function-

$$rounds_j = \left(K_{j\ mod\ 32+1} + C_{i-1}\right) mod\ 256$$

3. Repeat the above step for all pixels and then convert cipher pixels into 2D array to get decrypt image.

Decryption Process

1. At receiver side, same biometric image is used to derive the same secret key used to encrypt the image.
2. Perform all encryption function in reverse to obtain actual source image.

Performance Analysis

Author used somewhat a different way to derive a secret key from a biometric image and performed NIST statistical tests to confirm the randomness of generated key. The cipher image

relies on the secret key, previous pixel's encryption information and used logistic chaotic map or Tent map. Authors also carried out the security and performance analysis of given algorithm using histogram analysis, adjacent pixel correlation analysis, Information entropy analysis and key sensitivity analysis.

A highly complex and secure algorithm is proposed by the authors which used Haar wavelet to achieve lossless reconstructionafter transforming the image from time domain to wavelet domain [38]. An additional complexity is introduced by the use of multi chaotic mapping which is obtained after combing all three sub-chaos matrices. The process is:

Encryption and Decryption Process:

1. The process starts with the execution of DWT on the source image and then recombine all four coefficient matrices to obtain scrambled matrix.
2. A secret key is obtained by combining all three subchaotic matrices generated with the help of few initial parameters.
3. Perform BitXOR operation between scrambled image and multichaotic matrix and got an encrypted image.
4. Perform all operation in reverse order to get the original decrypted image.

Performance Analysis

Author executed many statistical analysis tests and compared the performance with the existing algorithms. The results showed that the proposed algorithm has better NPCR and UACI values than the previous one. Further analysis proves that the given method has high range key space, high key sensitive and ability to resist attacks.

The authors derived encryption key from the chaotic function such as logistic mapping and Hannon mapping [39]. The detailed process is as:

Encryption and Decryption Process:

1. Select an input image to be encrypted.
2. Construct two chaotic sequences using logistic mapping and arranged them in ascending order.
3. Rearrange the pixel positions in original image to increase the complexity.
4. Extract pixel position from the fractal key using Hannon map.
5. Perform XOR operation between the pixel values of fractal key and original image and get the encrypted image.
6. At receiver side, just execute all operations in reverse order to obtain the source image.

Performance Analysis

Author utilized the random behaviour and sensitiveness of chaotic system to obtained a secure cryptosystem. The analysis report of many statistical tests (histogram analysis, key space analysis, information entropy and correlation coefficient analysis) proved it a suitable cryptosystem for real world applications.

4. CONCLUSION

The paper examined numerous essential and used widely image encryption algorithms using different fractal function such as Mandelbrot set, Julia set, IFS and Quaternion Julia set. The main

emphasis of using fractal function in a cryptosystem is the use of fractal encryption key in the light of the fact of its sensitiveness to the initial condition which makes an algorithm difficult to be cracked. Huge number of proposed algorithm use additional strategies like scrambling, diffusion, substitution etc. to keep security level high which can be primary concern in a number of applications. However some measures have also been taken to encouraging reduced size image using wavelet transformation, which subsequently provide a secure encryption method in terms of decreased computation time.

In this review paper, selective algorithms based on shared key generation have been discussed to avoid the transmission of key over the network, hence attain considerable security. This survey paper also covered the performance analysis of each algorithm in terms of key size, key generation time, execution time, PSNR test etc. to ensure the best suitable image encryption algorithm for a given application.

REFERENCES

[1] Huntress G. B., 2004"Encryption using Fractal Key", United States Patent 6782101.

[2] Khan M. & Shah T., 2014"A Literature Review on Image Encryption Techniques", © 3D Research Centre Kwangwoon University and Springer-Verlag Berlin Heidelberg, 5(4), DOI 10.1007/s13319-014-0029-0, Page 1.

[3] Abed F. S., 2011 "A New Approach to Encoding and Hiding Information in an Image", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, ISSN (Online): 1694-0814.

[4] Sun Y, Chen L, Xu R, Kong R, 2014"An Image Encryption Algorithm Utilizing Julia Sets and Hilbert Curves". PLoS ONE, 9(1): e84655. doi:10.1371/journal.pone.0084655.

[5] Zhang Q., Zhou S. and Wei X.,2011 "An Efficient Approach for DNA Fractal-based Image Encryption", Applied Mathematics & Information Sciences, 5(3), pp 445-459.

[6] SomarajS. and Hussain M. A., 2015 "Performance and Security Analysis for Image Encryption using Key Image", Indian Journal of Science and Technology, Vol 8(35), DOI: 10.17485/ijst/2015/v8i35/73141.

[7] Stallings W., 1999 "Cryptography and Network Security: Principles and Practice". Upper Saddle River, N.J: Prentice Hall, ISBN:0136097049 9780136097044.

[8] Rivest R. L., Shamir A. and Adleman L., 1978"A method for obtaining digital signatures and public key cryptosystems", Communication of the ACM, 21: pp 120-126.

[9] Boneh D., 1999 "Twenty years of attacks on the RSA cryptosystem", American Mathematical Society (AMS), Vol. 46, No. 2, pp. 203-213.

[10] Diffie W., Hellman M., 1976 "New Directions in Cryptography", IEEE Transactions on Information Theory, 22(6): 644-654 doi-10.1109/TIT, 1055638.

[11] Pickover C. "Computers, Pattern, Chaos, and Beauty", St. Martin's Press, NewYork, 1990.

[12] Julia G., 1918 "Mémoire sur l'itération des fonctions rationnelles." Journal de MathématiquesPures et Appliquées 1: 47-246 (Translated in English by Alessandro Rosa in 2001).

[13] Mandelbrot B. B. "The Fractal Geometry of Nature", W. H. Freeman, New York, 1983.

[14] Devaney R. L., 1992 "A First Course in Chaotic Dynamical Systems: Theory and Experiment", Addison-Wesley, MR1202237 Zbl 0768.58001.

[15] Barnsley M. "Fractals everywhere", Academic Press Professional, Inc., San Diego, CA, 1988.

[16] Crownover, R. M., "Introduction to Fractals and Chaos", Jones &Barlett Publishers, 1995.

[17] Jonathan F. "An Introduction to Julia sets",2009.

[18] Zakeri, S., 2006 "On biaccessible points of the Mandelbrot set". Proceedings of the American Mathematical Society, 134(8), pp 2239-2250.

[19] Negi D., Negi A., Agarwal S., 2016 "The Complex Key Cryptosystem", International Journal of Applied Engineering Research, ISSN 0973-4562 Volume 11, Number 1, pp 681-684.

[20] Fractal Cryptology , New Mexico High School, Supercomputing Challenge Final Report April 2, 2003 , Team Members: Brandi Howell Anna Reese Michael Basile Team Sponsor: Paula Avery Project Mentor: Garth Reese.

[21] Motýl I., Jašek R., Vařacha P., 2012 "Analysis of the Fractal Structures for the Information Encrypting Process", International Journal of Computers, Issue 4, Volume 6, pp 224-231.

[22] Abd-El-Hafiz1 S. K., Radwan A. G.Haleem S. H. A., Barakat M. L., 2014 "A fractal-based image encryption system"IET Image Processing, Vol. 8, Issue 12, pp. 742–752 doi:10.1049/iet-ipr.2013.0570
[23] Sun YY, Xu R., Chen L., Hu X., 2014 "Image Compression and Encryption Scheme Using Fractal Dictionary and Julia Set", IET Image Processing, Vol. 9, Issue. 3, pp. 173–183 doi:10.1049/iet-ipr.2014.0224
[24] Alia, M. A. and Samsudin A. B., 2007 "New Key Exchange Protocol Based on Mandelbrot and Julia Fractal Sets", International Journal of Computer Science and Network Security, VOL.7 No.2, pp 302-307.
[25] Alia, M. A. and Samsudin A. B., 2007"A new public-key cryptosystem based on mandelbrot and julia fractal sets". Asian Journal of Information Technology, 6(5): pp 567-575.
[26] Rozouvan V., 2009 "Modulo image encryption with fractal keys", Optics and Lasers in Engineering, 47(1), pp.1-6.
[27] Nadia M. G. AL-Saidi and Said M. R. M., 2009"A New Approach in Cryptographic Systems Using Fractal Image Coding", Journal of Mathematics and Statistics, 5 (3):ISSN 1549-3644, pp183-189.
[28] Nadia M. G. AL-Saidi and Said M. R. M., 2010 "A New Public Key Cryptosystem Based on IFS", International Journal of Cryptology Research, 2(1): pp 1-13.
[29] Nadia M. G. AL-Saidi and Said M. R. M., et al., 2011"Efficiency Analysis for Public Key Systems Based on Fractal Functions", Journal of Computer Science, 7 (4): pp 526-532, ISSN 1549-3636.
[30] Sun YY, Kong RQ, Wang XY,et al.,2010 "An Image Encryption Algorithm Utilizing Mandelbrot Set". International Workshop on Chaos-Fractal Theories and Applications, pp170–173.
[31] Shaw J., Saha O., Chaudhuri A.,2012 "An Approach for Secured Transmission of Data using Fractal based Chaos" IJCA Proceedings on National Conference on Communication Technologies & its impact on Next Generation Computing, CTNGC(4): pp 13-17.
[32] Hala B. Wahab A., Sarab S. A., 2013 "Modify Symmetric Block Cipher Algorithm Using Generated Digital 3D Fractal Image", Iraqi Journal of Science, Vol 54, No.4, pp: 955-964.
[33] Negi A., Agarwal S., 2014 "A Key Agreement Protocol Based on Superior Fractal Sets", Journal of Mathematical and Computational Science, Vol 4, No 2, pp 471-478, ISSN: 1927-5307.
[34] Mann W. R., 1953"Mean value methods in iterations", Proc. Amer. Math. Soc., 4, pp 506-510.
[35] Sattari S., Akkasi A., Lari R. A., et al., 2015"Cryptography in social networks using wavelet transform, fractals and chaotic functions", International Research Journal of Applied and Basic Sciences, Science Explorer Publications, ISSN 2251-838X / Vol, 9 (9): 1627-1635.
[36] Feasibility Study on Random Number Generators for Symmetric Key Cryptography, Chapter 6, pp 156-204.
[37] Ali M. Meligy, HossamDiab, Marwa S. El-Danaf,2016"Chaos Encryption Algorithm using Key Generation from Biometric Images", International Journal of Computer Applications (0975 – 8887) Volume 149 – No.11.
[38] Wang W., Tan H., Pang Y., Li Z., Ran P. and Wu J.,2016 "A Novel Encryption Algorithm Based on DWT and Multichaos Mapping", Hindawi Publishing Corporation Journal of Sensors Volume Article ID 2646205, 7 pages,http://dx.doi.org/10.1155/2016/2646205.
[39] Kashanian H., Davoudi M. and Khorramfar H., 2016 "Image Encryption using chaos functions and fractal key", International Journal of Advanced Biotechnology and Research (IJBR) ISSN 0976-2612, Online ISSN 2278–599X, Vol-7, Special Issue-Number4, pp1075-1082.

AUTHOR

Shafali Agarwal has received MCA degree from UPTU, Lucknow in 2004 and M.Phil in Computer Science from Alagappa University, Karaikudi, Tamil Nadu in 2013. She got her Ph.D. in Computer Science from Singhania University, India in 2014. She has served as a faculty member in department of Computer Applications in JSSATE, Noida till June, 2016. She has published more than 10 research papers in various International journals and conferences indexed in springer, ACM, Scopus, Thomson Reuters, google scholar and in many more. Her research interest includes fractal, cryptography and image processing.