I. J. Computer Network and Information Security, **2019, 2, 1-12**
Published Online February 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.02.01

A Chaotic Cryptosystem using Conjugate Transcendental Fractal Function

Shafali Agarwal
Independent Researcher
Plano, Texas 75025, USA
E-mail: shafali.agarwal@gmail.com
(ORCID ID: 0000-0002-2542-8578)

Received: 28 December 2018; Accepted: 18 January 2019; Published: 08 Febuary 2019

Abstract—A cryptosystem designed by using the combined features of fractal function and chaotic map, provides a secure and real time encryption environment. In this paper, a 2D-chaotic map is employed to create a chaotic key sequence to comply with the requirement of the key sensitivity. The set of initial values of the chaotic map has derived by iterating a conjugate transcendental fractal function (CTFF) i.e. $z_{n+1} = conj(\sin(z_n^2)) + c$. The fractal function produced three sets of initial values after iterating it using Picard, Mann, and Ishikawa iteration methods. Resultantly, three chaotic key sequences will be generated by executing 2D Sine Tent composite map (2D-STCM) for each set of initial values. Afterwards, perform zigzag scanning to each key stream to decorrelate the adjacent image pixels and combined them using XOR operation. By using a different summation of plain image pixels for each pixel encryption, improves the cryptosystem resistant against known/chosen-plaintext attack. Moreover, an encryption of a plain image pixel achieved using corresponding key sequence pixel and a previously ciphered pixel value. The proposed encryption/decryption scheme is evaluated using key space analysis, key sensitivity analysis, differential analysis and other statistical analyses. The performance result indicates the given scheme is efficient and reliable to be used with great potential for a secure image transmission application.

Index Terms—2D Sine Tent composite map, Fractal Function, Zigzag Scan, Image Encryption, Diffusion Process.

I. INTRODUCTION

Now days, multimedia transmission became common in every aspect of communication like military, picture messaging application for cell phones, biological data, medical imaging, scientific observation, etc. With the advancement in the internet and computer technologies, a rapid transmission occurs over various transfer networks. A secure communication system is essential to achieve a reliable multimedia circulation.

A cryptographic system is a key component to realize the requirement of a secure system and achieved by transferring the encrypted data over the unsecure network. The received data can only be readable by decrypting it with the help of a security key at the other end. Image encryption is a part of a cryptographic system in which a scrambled form of an input image is created, which is unidentifiable by an unauthorized user [1].

Developing an image encryption algorithm, is inevitably a challenging job as compared to encrypting a textual data. An image size is a critical challenge in terms of an acceptable time frame while executing an algorithm. The image also has a high correlation value between its adjacent pixels which can be used in cryptanalysis. A competent image encryption algorithm must be able to distribute image pixels uniformly in the cipher image to increase the randomness. Various parameters are used to prove the effectiveness of the cryptographic method, which in turn, achieve the required level of accuracy and security.

Considering the notable characteristics of a chaotic system, like non-periodicity, butterfly effect (sensitive to the initial condition), ergodicity and pseudo-randomness attract the researchers to utilize the feature in the design of a cryptosystem. The chaotic map plays a crucial role to introduce confusion and diffusion between the image pixels. Sometimes, 1D-chaotic maps like Tent, Logistic, and Sine map are good enough to produce the required confusion and diffusion impact during the process execution [2–3]. But the chaotic orbits and initial values of the said maps (i.e. 1D chaotic maps) may be analyzed by the unauthorized person to eavesdropping the system [4–6]. Later, multidimensional chaotic maps such as Arnold, henon, 2D Logistic etc. with enhanced chaotic performance were introduced by the researchers. However, a combined form of 1D chaotic maps has also been successful to obtained a secure and reliable cryptosystem [7–9]. Rhouma et al. analyzed the weaknesses and possible security attacks on the cryptosystem designed using the high-dimensional chaotic map [10–11].

A fractal image is the graphical presentation of a complex structure at local and global irregularity level [12]. It is generated by iterating a mathematical function for pre-determined number of times. A fractal image possesses high variation in detail at discrete scales, also determines a wide choice in terms of key space. Few

real-life examples are cauliflower, coastlines, clouds, tree, etc.

A well-known fractal introduced by Benoit Mandelbrot, in 1979, is a set of complex points in which the boundary exhibits a different structure at each scale, known as Mandelbrot set [13]. The Mandelbrot set (MS) fractal can be defined as "The MS fractal is designed by iterating a simple mathematical function z^2+c for which the value c remains within the boundary and does not escapes to infinity." Similarly, a Julia set fractal is formed by using the same mathematical function i.e. z^2+c. But, the Mandelbrot set draws a fractal image by assigning $z = 0$ and varying c for each pixel, whereas, for each c value of MS fractal, a Julia set fractal will be formed using a non-zero z value [14]. At each pixel in Mandelbrot set, a distinct Julia set image is obtained. One pixel shifting in Mandelbrot function will generate a totally different Julia image, consequently, a unique key sequence will be generated. Many researchers considered the fractal structure and applied in various applications such as graphic design, medical, antenna design, image encryption, etc. Unlimited resources are available to design the fractal images including parametric program.

The paper aims to provide a secure cryptosystem by utilizing a chaotic map recently suggested in an image encryption method. The author [15] proposed a 2D Sine Tent composite map (2D-STCM) to create a chaotic key sequence which considers better trajectory than the other maps. Here, the method used the same chaotic map, but the initial condition used by 2D-STCM are generated by iterating the CTFF using Picard, Mann and Ishikawa iteration method separately. As a result, three distinct chaotic key sequences have generated after executing 2D-STCM. Further, the key stream is scanned using zigzag scanning method separately. Conclusively, a security key is obtained by XORing the three-scanned chaotic key sequences. In the next phase, a diffusion process is implemented to modify the image pixel values and thus break the correlation between the adjacent image pixels. The encrypted images are analyzed using various parameters such as histogram distribution, entropy, correlation coefficient, NPCR, UACI, MSE, and PSNR.

The rest paper is discussed as follows. In section 2, previous work on image encryption is discussed. The design of the newly suggested cryptosystem is illustrated in section 3. Section 4 presents the performance analysis of the proposed method to prove its efficacies towards the real-life applications. The last section concludes the paper by summarizing the finding of the given scheme.

II. Related Work

Since 1990s, researchers have employed a chaotic system in the design of a cryptosystem after observing its characteristics. In 2000, Fidritch has patented a chaotic cryptosystem to encrypt the data such as image using two and three-dimensional chaotic Baker map [16]. To encrypt the data/image, single dimensional as well as multidimensional chaotic map has been extensively used in various research. An image encryption method was proposed by the author by combining two 1D chaotic map to have better chaotic behavior [17].

To encrypt an image, Benyamin used a hyper-chaotic system to generate a key sequence. The algorithm comparatively faster due to the single round of diffusion [18]. Whereas, in [19], hyper-chaos shuffled the plain image and then compress and diffuse the shuffled image by applying Chinese remainder theorem. In [20], a color image encryption algorithm proposed by using coupled-map lattices (CML) and a fractional-order chaotic system to increase the robustness and security of the system. A combination of two or more chaotic maps were also analyzed to enhance the complexity of the cryptosystem [21]. The two Logistic sequences were used to label the row coordinates and column coordinates of scrambled image and then MOD and XOR operations were applied to diffuse the plain image [22]. A noisy Logistic map provides the set of initial values to the Clifford strange attractor function to shuffle the pixel position and pixel values of a plain image in Navy [23]. The researchers always explore the new possibilities to provide better system in each domain. In [24], the author introduced a new Beta chaotic map based on Beta function to generate a key sequence. A parametric switching chaotic system is responsible for image pixel substitution and permutation and encode the given image to encrypted image [25]. It is suggested that the image encryption method should consider a set of complex operations to design a secure cipher [26]. However, permutation only image cipher is fragile to known-plaintext attack [27].

Since researchers are known to innovate new ideas by experimenting in a different way. The authors combined a chaotic system with DNA sequence and then applied confusion and diffusion process [28–30]. In ref. [28], the plain image pixels are bit XORed using the pseudo-random sequence formed by the spatiotemporal chaotic system CML (coupled map lattice). Then a DNA permutation and DNA confusion process have been executed to completely reshuffled the original image. Recently, author [29] utilized the concept of ACP (Artificial societies, Computational experiments, Parallel execution) given by Fei-Yue Wang and performed the encryption process in two steps. The chaotic data in reality and chaotic data in simulation were used to convert artificial random image and original image respectively. To obtain a cipher image, performed DNA-XOR operation on the combined impact of the applied chaotic data of two groups. A DNA arrangement is used as a key sequence to permute and diffuse the plain image matrix [30]. To encrypt an image, the author utilized chaotic random phase masks, Gyrator transform and Jigsaw transform along with the random permutation of resulting image [31]. A new phenomenon, i.e. particle swarm optimization is introduced with the logistic map to optimize the encrypted image to get improved performance results. The approach helps to minimize the correlation coefficient value between image pixels, hence exhibits the optimum efficacy as compared to other image encryption method [32]. Also the chaotic map

helps to encrypt medical images as well [33].

Fractal geometry helps to enhance the complexity of the cryptosystem design due to its complex mathematical structure. Initially, in 2003, a team designed a cryptosystem to encrypt a message using random numbers and Mandelbrot set fractal. At that time fractal was not so much popular in the cryptography system. Author succeeds to encrypt the data, but unable to decode the same. A perfect decoder required a mapper so that no number came out twice [34]. Later, in 2004, an approach was suggested to use fractal based encryption/decryption key and USA navy published the patent for the same [35]. There are numerous fractal functions, that can be employed in many applications such as Mandelbrot set, Julia set and more [36]. In this paper a conjugate transcendental fractal function is used to create a set of initial values. A detailed analysis of Mann iterated CTFF with respect to cosine function has been carried out by the author in [37]. The finding of the paper includes beautiful fractal images and the presence of tricorn and Mandelbrot set images on the external rays. The author analyzed the fractal structure and then utilized the fractal geometry to encrypt the predetermined length of the message [38]. Although, Suthikshn [39] applied RSA to encrypt the message using a secret key generated from the Mandelbrot set fractal.

A compression-encryption scheme was proposed by the author in which a fractal dictionary encoding pattern is applied to compress an image followed by XOR operation using JuliaStreamCipher and a diffusion step [40]. A finite field cosine transformation (FFCT) and multi-fractal images based private key encryption algorithm was suggested by the researcher in [41]. In FFCT phase, a plain image is transformed into a temporary cipher image, which is further encrypted using a secret key obtained through multi-fractal images. Similarly, in [42], a system key was generated by using multiple fractal images by adding feedback delay, multiplexing and independent horizontal and vertical shifts in the process. However, a cryptosystem was designed by using different keys at each iteration to encrypt the image [43]. A fractal function can be used in conjunction with the chaotic map to introduce more randomness and butterfly effect. An idea has been suggested by the author in which the initial values provided to the 2D composite chaotic map by iterating a fractal function [15]. The paper presents an image encryption method which combines the features of fractal function, chaotic map and the zigzag scanning method to create a key sequence. Further, image cipher obtained after performing algebraic transformation on plain image using the secret key sequence.

III. The Proposed Cryptosystem

The proposed cryptosystem consists of two major steps:

1. Generation of a security key
2. Convert plain image into cipher image

A. Key Stream Generation

The secret key used in the proposed cryptosystem is obtained in three steps: 1) a set of initial values using CTFF, 2) key sequence using 2D-STCM, 3) zigzag scanning of chaotic key sequences.

The fractal images are designed by using the feedback system in which at each iteration, outcome of each operation becomes the input to the same system [12]. It can be characterized as:

One-step feedback machine is considered by Peano–Picard iteration method. Let Z be a nonempty set of complex variable and f: $Z \to Z$. For any point $x0 \in Z$, the equation can be represented as:

$$z_{n+1} = f(z_n), n \geq 0 \quad (1)$$

In two-step feedback machine, The function $z_{n+1} = f(z_n, z_{n-1})$, requires two numbers as input and returns an output [44]. For the same point $x0 \in Z$, the Mann iterated sequence $\{z_n\}$ is defined by [45]:

$$z_{n+1} = s * f(z_n) + (1 - s) * z_n, n \geq 0 \quad (2)$$

Also, the Ishikawa iterated set of sequence $\{y_n\}$ and $\{x_n\}$ is defined by [46]:

$$y_n = s' * f(x_n) + (1 - s') * x_n, n \geq 0 \quad (3)$$

$$x_{n+1} = s * f(y_n) + (1 - s) * x_n, n \geq 0 \quad (4)$$

Where $0<s\leq 1$ and $0<s' \leq 1$, and s and s' both must be non-zero numbers. In fact, for $s = 1$, Mann iteration reduces to Picard's iteration, and for $s' = 1$, the Ishikawa iteration reduces to Mann's iteration and for $s=s'=1$, the Ishikawa iteration reduces to Picard's iteration.

The function $f(z)$ can be a quadratic, cubic, or biquadratic polynomial. Here the function $f(z)$ is:

$$z_{n+1} = conj(\sin(z_n^2)) + c \quad (5)$$

Where c is a complex variable. The fractal image will be obtained by repetitive iteration of the transcendental conjugate function for n times. The paper generates three sets of preliminary values by iterating the above given function using Picard, Mann, and Ishikawa iteration method respectively. Fig. 1 shows the images of executing the fractal function with reference to the above said iteration methods using Ultrafractal™ software (Please ignore evaluation word in the images).

The paper used the Picard iterated, Mann iterated, and Ishikawa iterated transcendental fractal function to get three different sets of preliminary values so that three chaotic secret key sequences can be generated using 2D-STCM.

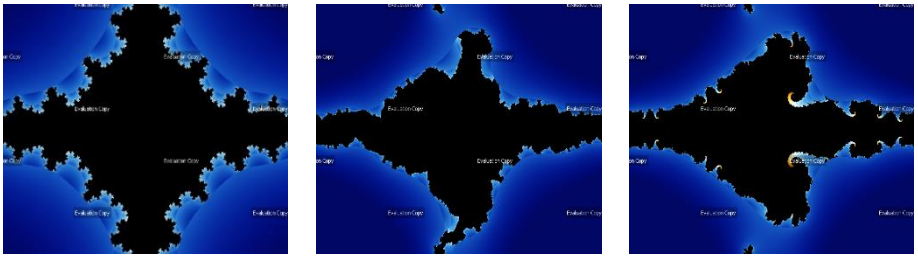
The next step of key generation is to create a chaotic sequence by executing the 2D-STCM. The paper employed a 2D chaotic map to overcome the boundaries of the one-dimensional chaotic maps [47–48]. A 2D-STCM is described as:

$$x_{n+1} = \begin{cases} ((\sin(\pi y_n) + 3) * x_n/2) \bmod 1, & x_i < 0.5 \\ ((\sin(\pi y_n) + 3) * (1 - x_n)/2) \bmod 1, & x_i \geq 0.5 \end{cases} \quad (6)$$

$$y_{n+1} = \begin{cases} ((\sin(\pi x_{n+1}) + 3) * y_n/2) \bmod 1, & y_i < 0.5 \\ ((\sin(\pi x_{n+1}) + 3) * (1 - y_n)/2) \bmod 1, & y_i \geq 0.5 \end{cases} \quad (7)$$

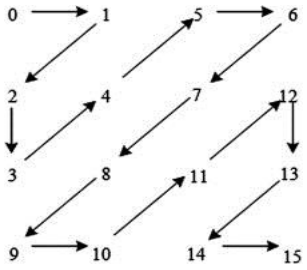
The set of initial values (*x*, *y*) got in the previous step are inputted into the chaotic map function. Accordingly, three chaotic key sequences will be generated for each set of inputted values. The sequences generated through the above function are non-periodical and much sensitive to the initial conditions.

To get a secure key sequence, zigzag scanning method is applied to the chaotic sequence produced in the previous



(a) (b) (c)

Fig.1. Conjugate Transcendental Fractal Images using Iteration Method (a) Picard; (b) Mann; (c) Ishikawa



0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Fig.2. Zigzag Scan Method

Step. The zigzag scanning method helps to minimize the correlation coefficient value of adjacent pixels by tracing the elements of a matrix in a particular sequence. The method starts with the scanning of a 2D matrix and produced a definite sequence of elements in a 1D form [49]. The fig. 2 depicts the used zigzag scanning approach.

B. The Encryption Method

This section discussed the anticipated encryption algorithm implemented for the color images and the gray images. The method diffused the plain image by using a security key in single phase. The detailed description is as follows:

Step 1: Process starts by inputting a plain image PI of size M*N to be encrypted and a set of values (*x0*, *n*, *s*, *s'*) to be keyed in the fractal function.

Key Generation Process:

Step 2(a): Step 2(a): Using the set of values (*x0*, *n*, *s*, *s'*), iterates the conjugate transcendental fractal function (refers eq. (5)) and get three sets of preliminary values (*x*, *y*) by iterating it using Picard, Mann and Ishikawa iteration methods. The value of constant variable *s* and *s'* is 0.5 and 0.8 respectively and complex value *c* used in each iteration is (-0.025, 0.0125), (-0.296875, 0.78125), and (0.6, -0.025) which are obtained by implementing the fractal function using UltraFractal™ software. The initial values obtained through this method are nothing, but the fixed point of the CTFF obtained after repeating the same operation for definite times.

Step 2(b): Pass each set of preliminary values (*x*, *y*) and the dimensions of the input image (M*N) to the 2D-STCM function (refer eq. (6 & 7)) three times and obtained chaotic key sequences accordingly (*S*1, *S*2, *S*3).

Step 2(c): Apply zigzag scanning to each sequence separately and got one-dimensional three scanned chaotic sequences resultantly.

Step 2(d): Convert each chaotic sequence into two-dimensional (M*N) form and XORed all sequences to get the security key SK of size M*N.

Encryption Process:

Step 3(a): Start the encryption process by summing the plain image pixel values as:

$$PIsum = \sum_{i=1}^{M*N} PI_i \quad (8)$$

Step 3(b): Start with $i \rightarrow 1$, calculate:

$$PIsum = PIsum - PI(i) \quad (9)$$

$$Temp = floor\big(mod(PIsum * SK(i) * 2^{256}, 256)\big) \quad (10)$$

Here mod() function helps to maintain the value range between 0 and 255 and give the nearest integer value as the resultant because of the use of a floor() function. The variable Temp is calculated on each iteration using the current key value and a new calculated pixel sum value i.e. PIsum.

PIsum variable consists of the sum of pixel values, starts from second to last and gradually it becomes zero after each iteration.

Step 3(c): If (*i*=1), then start encryption with the first pixel of the input image by XORing it with first security key value and Temp according to the given equation:

$$CI(i) = PI(i) \oplus SK(i) \oplus mod(Temp + var, 256) \quad (11)$$

Step 3(d): Otherwise, use *i*th security key value and previously enciphered CI(CI_{i-1}) to encrypt the *i*th plain image pixel. Also, the new calculated Temp value is used to encrypt the corresponding pixel. The formula will be:

$$TempCI = mod(SK(i) + CI(i-1), 256) \quad (12)$$

$$CI(i) = PI(i) \oplus TempCI \oplus Temp \quad (13)$$

Note that the value Temp changed on each iteration. Hence, contribute differently towards the cipher image computation.

Step 4: Increment $i \leftarrow i + 1$, go to step 3(b) and continue the process till *i* reaches to M*N.

Step 5: At last, we will have an array of encrypted values CI = {CI_1, CI_2, …, CI_{M*N}}. Reshape the CI values into two-dimensional array and that will be our required encrypted image.

C. The Decryption Method

Generally, the decryption method is the inverse process of the encryption method except few initial steps. The decryption process starts with the security key which can be generated by using the accurate input values at the receiver end. The detailed process can be defined as:

Step 1: Generate the security key sequence SK by using the given set of values (*x*0, *n*, *s*, *s*').

Step 2: Scan the cipher image and arrange image pixels in one-dimensional array as CI = {CI_1, CI_2,…, CI_{M*N}}.

Step 3: Step 3: Start the decryption process by applying the encryption process in reverse from the last pixel of a cipher image. Set Temp ← 0, $i \leftarrow$ M*N, and PIsum ← 0 (after completion of the encryption process, the value of PIsum will be zero). Compute the following steps:

$$TempPI = mod(SK(i) + CI(i-1), 256) \quad (14)$$

$$PI(i) = CI(i) \oplus TempPI \oplus Temp \quad (15)$$

$$PIsum = PIsum + PI(i) \quad (16)$$

$$Temp = floor\big(mod(PIsum * Sk(i-1) * 2^{256}, 256)\big) \quad (17)$$

Step 4: Decrement $i \leftarrow i - 1$, go to step 3 and continue the process till *i* reaches to 2.

Step 5: Till the previous step execution, the complete cipher image will convert to original input image except its first pixel. Now to decrypt that pixel of cipher image, execute the given formula:

$$PI(i) = CI(i) \oplus SK(i) \oplus mod(Temp - var, 256) \quad (18)$$

After execution, we will get a sequence of pixels in one-dimensional array which has to be reshaped into a two-dimensional array to get the plain image.

A system block diagram of key generation is given in fig. 3.

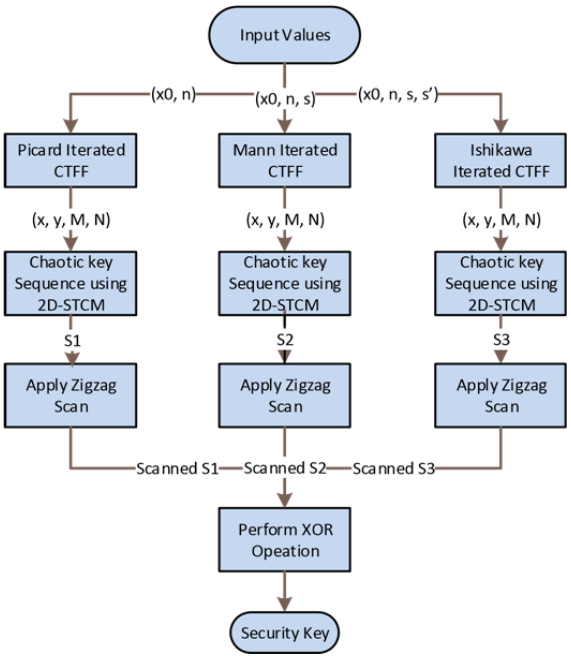


Fig.3. Key Generation Process Diagram

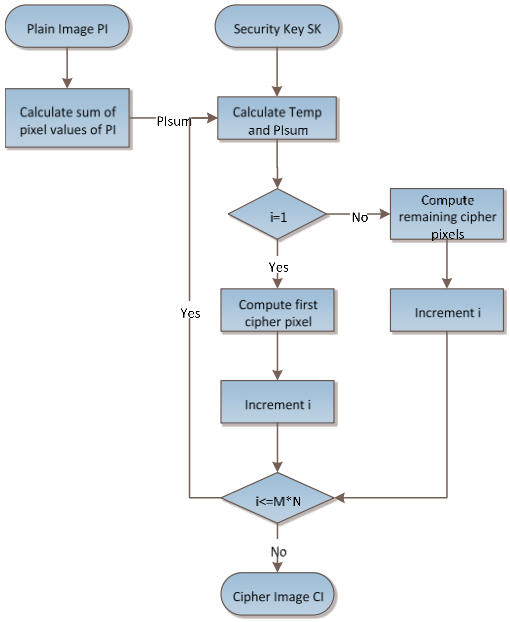


Fig.4. The Proposed Cryptosystem

A plain image PI is the original image which is supposed to be converted to cipher image CI. The above given diagram in fig. 4 shows the various steps used in the proposed cryptosystem design.

IV. Performance and Security Analysis

The above discussed encryption algorithm applied to the gray image and the color image of size 256*256. The set of values used to generate key stream is $x0$=0.0, n=100, s=0.5 and s'=0.8 and the variable 'var' is chosen as 10. The method is implemented using MATLAB™ software with system configuration Intel® Atom™ x7-z8700 CPU @1.60 GHz and 4 GB RAM to measure the performance. Further, the simulation results and the performance of the algorithm given in terms of various measures.

A. Simulation Results

Fig. 5 displays the simulation result of applying the given algorithm to encrypt/decrypt the gray image and color image. The simulation result shows the encrypted image looks like a noisy image, in which pixels are randomly distributed throughout the image. The histogram of the Lena and peppers images and their corresponding encrypted images is also shown in the same figure. A histogram of an image refers to the image pixel distribution at each intensity level. The outcome shows that all plain images have a specific pattern in histogram whereas in cipher image, histogram distributed uniformly. It makes difficult to guess the original image by looking only at the cipher image histogram.

B. Computational Time Analysis

The encryption speed depends on various factors such as CPU, RAM size, compiler, and operating system, etc. A speed analysis is given for a test image of size 256*256 after conducting the complete process. The method implementation consists of two major parts: 1) key generation, 2) encryption/decryption. A key sequence is generated by performing the three steps (use of fractal function, chaotic map and zigzag scan), despite that the total time taken by the process is much less i.e. 0.107006s to 0.162707s. It proves that the use of fractal function in the key generation process does not require much time to execute. The estimated time to encrypt/decrypt the gray image and color image of size 256*256 was 1.367196s and 3.8807s respectively. The table 1 shows the execution time needed by the proposed method and other image encryption schemes.

C. Key Space Analysis

To secure a cryptosystem from the brute-force attack, a key space must be greater 2^{100} [50]. A key sequence in the given method is produced by inputting a set of values ($x0$, n, s, s') to the fractal function. If the used programming language complies with the IEEE floating point standard [51], the variables will be stored in the double data type. The memory space needed to accumulate a single parameter is 8 bytes with the computational precision about 10^{-15}. In that case, the possible secret key space will be $10^{-15}*10^{-15}*10^{-15}*10^{-15} \approx 2^{200}$, which is quite enough to resists the brute-force attack.

D. Entropy Analysis

Entropy analysis is a statistical measure of the predictability of randomness and unpredictability of an information source given by Shannon in 1949 [52]. The entropy E(s) of the source can be defined as:

$$E(s) = -\sum_{i=0}^{2^N-1} P(s_i) log_2 P(s_i) \quad (19)$$

Here $P(s_i)$ is the expected occurance frequency of an image pixel si and depicted in bits. To compute entropy, the number of occurrences of symbol *si* with its probability of occurrence in cipher image is computed. The results in table 2 shows the entropy value of cipher image and the entropy values of other image encryption methods. As can be seen that the proposed scheme is having the resultant value 7.9989 (color image) i.e. nearby to the standard value 8. It proves that the cipher image has high randomness so secure from the entropy attack.

E. NPCR and UACI Analysis

The impact of the differential attack on the cryptosystem is necessary by observing, how a change in input affects the corresponding outcome. The number of pixel change rate (NPCR) and unified averaged changed intensity (UACI) are standardized test to analyze the strength of the proposed encryption scheme [53]. NPCR measures the influence of the change in plain image pixel to the corresponding cipher image. Consider two plain images "P1" and "P2" with one-pixel change and their corresponding encrypted images "C1" and "C2" respectively, then the NPCR can be defined as:

$$NPCR = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N} d(i,j) * 100\% \quad (20)$$

Where, d will be calculated as:

$$d(i,j) = \begin{cases} 0, & if\ C1(i,j) = C2(i,j) \\ 1, & if\ C1(i,j) \neq C2(i,j) \end{cases} \quad (21)$$

A significantly high NPCR result considered as much sensitive to the change in an image pixel, hence strong resistance against differential attack. Considering the fact that, no two random images can be completely different, the maximum expected NPCR value is assumed to be 255/256 = 99.6093%.

UACI test computes the average intensity difference between C1 and C2 and is defined as:

$$UACI = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{C1(i,j)-C2(i,j)}{255} * 100\% \quad (22)$$

The experimental values of NPCR and UACI are 99.5920% and 33.4446% respectively, quite close to the theoretical values. Table 3 compares the obtained results of the implemented algorithm with the other five methods. Therefore, the proposed scheme results are closest to the average NPCR and UACI scores to the expected ones.

F. Adjacent Pixels Correlation

An image always possesses the high correlation within its adjacent pixels in horizontal, vertical and diagonal direction. The requirement of an efficient image encryption algorithm is to obtain such an encrypted image in which correlation between adjacent pixels must be equivalent to zero in all directions. To quantify the correlation factor, calculate the parameter using the given formula:

$$cc = \frac{cov(x,y)}{\sigma x * \sigma y} \quad (23)$$

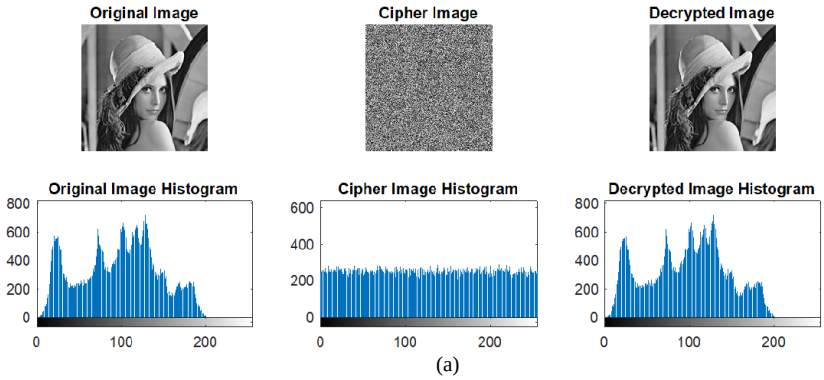
Where $\sigma x = \sqrt{var(x)}$ and $\sigma y = \sqrt{var(y)}$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (24)$$

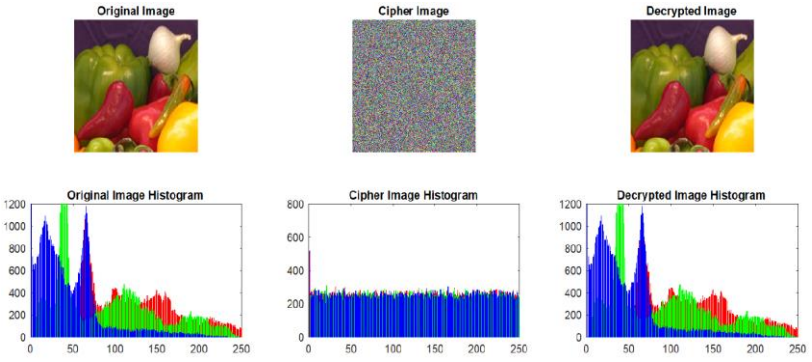
$$var(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (25)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \quad (26)$$

Fig 6 shows the implementation results by plotting pixel correlation in all directions (i.e. horizontal, vertical and diagonal). The visual testing proved that the strong correlated pixels in the original image are scattered uniformly in the encrypted image, hence greatly reduce the correlation between the pixels. Also, a table 4 shows the quantitative result of applying the proposed method along with other five methods. The values show the plain image pixels are strongly correlated to each other while it is quite weak in the cipher image. Therefore, the given method has successfully reduced the adjacent pixel correlation in all directions as needed.



(a)



(b)

Fig.5. (a) Lena Original, Cipher and Decrypted Images with its Corresponding Histogram; (b) Peppers Original, Cipher and Decrypted Images with its Corresponding Histogram

Table 1. Execution Time Comparison (time unit: sec)

Method	Proposed Method	Ref. [18]	Ref. [19]	Ref. [40]	Ref. [20]	Ref. [21]
Processor Speed	1.60 GHz	2.40 GHz	2.40 GHz	2.40 GHz	2.0 GHz	3.1 Hz
Lena	1.367196	0.4	0.018	0.031	1.25	10.3959

Table 2. Information Entropy of Various Image Encryption Methods

Image / Method	Lena	Cameraman	Baboon	Peppers
Plain Image	7.4139	7.0097	6.8178	7.6338
Proposed Algorithm	7.9970	7.9969	7.9989	7.9989
Ref. [18]	7.9980	7.9974	7.9973	7.9976
Ref. [19]	7.9973	-	7.9973	7.9975
Ref. [20]	7.9895	-	-	-
Ref. [21]	7.9993	-	7.9992	7.9992

G. Correlation Analysis between Plain and Cipher Image

A Correlation coefficient (CC) of two images represents the relationship between them that how much close/related to each other. The formula to compute CC is as:

$$CC = \frac{\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\left(A_{ij}-\overline{A)}\left(B_{ij}-B\right)\right)/}{\sqrt{\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\left(A_{ij}-\overline{A)}^2\right)\left(\sum_{i=1}^{M}\sum_{j=1}^{N}(B_{ij}-\bar{B})^2\right)}} \quad (27)$$

Where

$$\bar{A} = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}A_{ij}$$

and

$$\bar{B} = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}B_{ij}.$$

The variable A and B represents the plain image and cipher image respectively. Ideally the range of CC lies between -1 to +1. The value -1 depicts that the both images do not correlate to each other, whereas +1 depicts that the both images are close to each other. According to the given table 5, CC value of various images is close to zero, indicate that the both images are significantly different from each other.

H. Mean Square Error and Peak Signal-to-Noise Ratio Analysis

A mean square error value (MSE) indicates about how far the input image (P) pixels are from an encrypted image (C) pixels. The greater the MSE value, corresponds to the great difference between these two images. The formula to compute MSE is as:

$$MSE = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}(P(i,j)-C(i,j))^2 \quad (28)$$

A PSNR value is a standard way to compute the visual quality of encrypted image corresponding to its plain image. It is a ration between the maximum intensity of an image and MSE of that image. PSNR is calculated as:

$$PSNR = 20\ log_{10}\left[\frac{I_{max}}{\sqrt{MSE}}\right] \quad (29)$$

Here I_{max} is 255, the maximum image pixel value in which each pixel is represented using 8 bits. A low PSNR value implies high difference between a plain image and its corresponding encrypted image. See table 5 for the results. The comparison shows the better results of the implemented scheme than the other algorithm.

I. Key Sensitivity Analysis

A secure cryptosystem requires a large key space and a strong key sensitivity to the small change, otherwise an intruder might recreate the original image by guessing the security key. The previous section discussed about the available key space which proved adequate to the system requirement. Now the impact of key sensitivity to the encryption and the decryption quality of the proposed cryptosystem is examined.

A key sensitivity is important while doing encryption as well into decryption phase: (1) the minor change in a secret key must be able to produce a completely different cipher image while encrypting the same plain image. (2) Similarly, a different original image should be produced when a slightly modified secret key is used to decrypt the cipher image.

A security key is generated by executing the CTFF using the complex variables z and c. To evaluate the key sensitivity, a slight change is made to the value of complex variable ‘c’ in each iteration and observed the behavior of encrypted and decrypted images. The set of changed values is:

(1) Case 1: Change only (0.6, -0.025) to (0.6001, -0.025)
(2) Case 2: Change (-0.296875, 0.78125) and (0.6, -0.025) to (-0.296874, 0.78125) and (0.6001, -0.025)

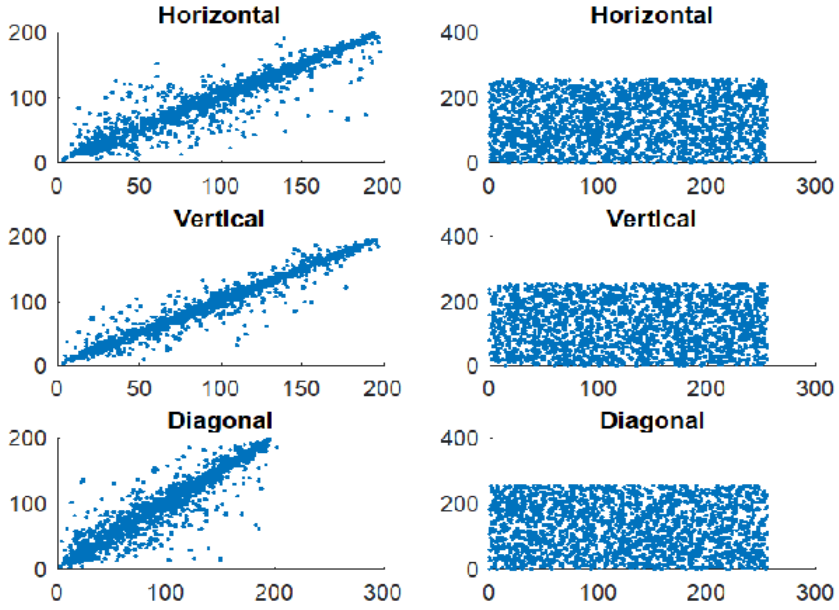


Fig.6. (a) Correlation Distribution of Adjacent Pixels of Plain Image Horizontally, Vertically and Diagonally Respectively; (b) Correlation Distribution of Adjacent Pixels of Cipher Image Horizontally, Vertically and Diagonally Respectively

Table 3. Comparison of NPCR and UACI value of Different Image Encryption Methods

Method / Parameter	Proposed Scheme	Ref. [18]	Ref. [28]	Ref. [40]	Ref. [20]	Ref. [21]
NPCR	99.5920	99.8023	99.65	99.62	99.7915	99.61
UACI	33.4446	33.5548	33.48	33.38	49.2191	33.40

Table 4. Correlation Coefficient Analysis of Two Adjacent Pixels in Cipher Image

Method	Correlation Coefficient		
	Horizontal	Vertical	Diagonal
Plain Image	0.954125922	0.977809985	0.932092722
Proposed Scheme	0.002998127	0.002911998	-0.000473064
Ref. [18]	−0.00051014	−0.00576844	0.00029585
Ref. [28]	0.0020	-0.0007	-0.0014
Ref. [22]	0.0086	0.0014	0.0009
Ref. [20]	-0.00368	0.00014	-0.02298
Ref. [21]	0.009118	−0.027993	−0.008005

Table 5. Correlation Coefficient (CC), MSE & PSNR of Various Images

Image	Proposed Scheme			Ref. [18]		
	CC	MSE	PSNR	CC	MSE	PSNR
Lena	-0.006285	8602.6	8.7845	0.00338909	9032	8.5731
Cameraman	0.001105	9388.4	8.4048	0.0014570	9415	8.3928
Baboon	-0.002226	12528	7.1519	−0.0007028	7385	9.4474
Peppers	0.000662	11287.7	7.60474	0.0023854	8261	8.9603

(1) Case 3: Change (-0.025, 0.0125), ((-0.296875, 0.78125), and (0.6, -0.025) to (-0.025001, 0.0125), ((-0.296874, 0.78125), and (0.6001, -0.025)

The resultant images are shown in fig. 7. Also, an additional test is executed to compare the pixels of two cipher images obtained using correct security key and modified security key. According to table 6 data, the NPCR and UACI values verified the sensitiveness of the given scheme in all three cases. Small change in the key value produces a great difference between the cipher images. So, an intruder will not be able to decrypt the cipher image even having an almost perfect key information.

J. Robustness to Data Loss and Noise

A network always contaminated by a kind of noise and may have data loss while transferring the data from one end to another. An image encryption method must be robust enough to resist the noise and data loss and be able to recover the results. The scheme is tested by implementing three types of noise attacks (speckle, salt & pepper and gaussian) and data loss of few pixels to the encrypted images. The decrypted images in fig. 8 show the robustness of the proposed method against data loss and noise. As shown, that the given algorithm can recover the original images in spite of being infected during the transmission. Although the obtained images are having some noise, still most of the information can be recognized.

V. Conclusion

The paper is designed to utilize the characteristics of a fractal function and a chaotic map in the field of the image encryption. It is a symmetric key encryption method with a single round of the diffusion process.

In the proposed algorithm, a security key was generated by executing three steps which makes it difficult to guess by an intruder. A 2D chaotic map i.e. 2D-STCM used the initial values derived by iterating a conjugate transcendental fractal function (CTFF) to generate a chaotic key sequence. To decorrelate the adjacent image pixels, an additional step has been taken by performing zigzag scanning to the chaotic key sequence. In the first phase of cryptosystem design, the plain image is modified using diffusion process. Each original image pixel is encrypted using the corresponding security key pixel and the previously encrypted cipher image pixel. Through the experimental results, the effectiveness, correctness, security and robustness of the proposed method is verified. The following observations take place during the analysis process:

- The method possesses a larger key space to make brute-force attack infeasible.
- The uniform distribution of the pixels in the cipher image demonstrates the reduced correlation between the adjacent pixels.
- Information entropy results indicate the value is close to the standard value 8, hence secure from entropy attack.
- All differential analysis measurements i.e. NPCR, UACI, MSE and PSNR proved the system is secure from differential attack and has a good encryption quality.
- The value of correlation coefficient is close to zero, indicates that the anticipated scheme works well to minimize the correlation after encrypting an original image.
- Key sensitivity also verified in the case of encryption and decryption using a slightly modified key. The results showed that the image transmission is secure from the unauthorized access.
- The above discussion verified the suitability of the proposed cryptosystem for image transmission over the unsecure network.

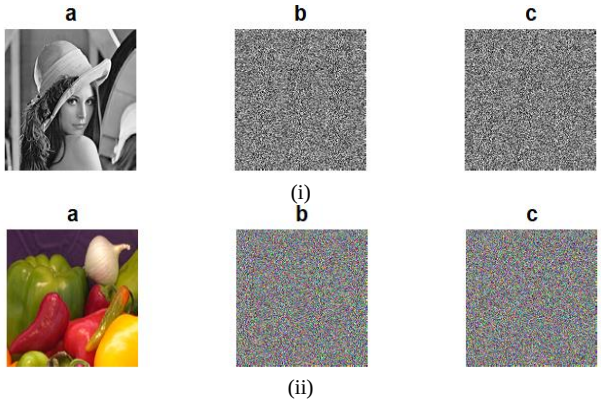
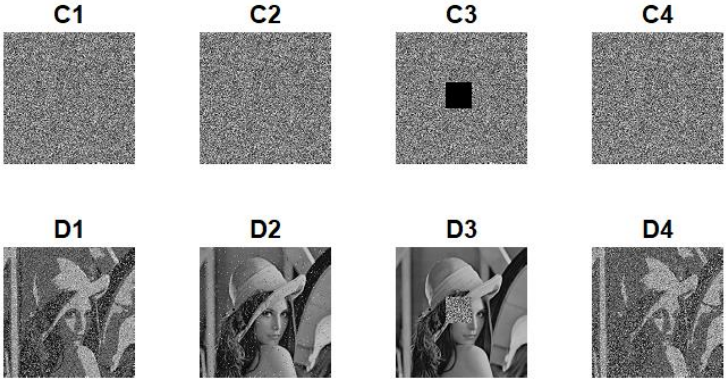


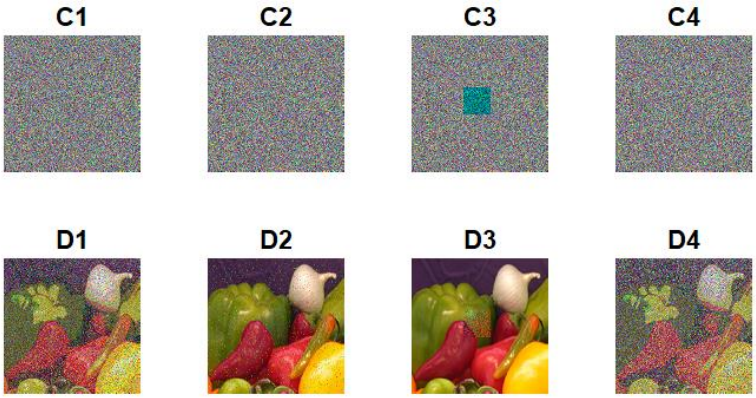
Fig.7. Key Sensitivity Analysis of Gray and Color Image; (a) Plain Image; (b) Encrypted Image with Correct Key; (c) Decrypted image with Modified Key

Table 6. NPCR and UACI Values between Cipher Images

Change in Key Value	NPCR (%)	UACI (%)
Case 1	99.6124	33.5277
Case 2	99.6673	33.3514
Case 3	99.6322	33.5138



(i)



(ii)

Fig.8. Robustness of the Proposed Method against Data Loss and Noise for Gray and Color Image. (C1) The Cipher Image with 1% Speckle Noise; (C2) The Cipher Image with 2% Salt & Pepper Noise; (C3) The Cipher Image with 3.81% Data Loss; (C4) The Cipher Image with .01% Gaussian Noise; (D1), (D2), (D3), and (D4) are Corresponding Decrypted Images.

REFERENCES

[1] W. Stallings, *Cryptography and network security: principles and practice*, 4th ed (Upper Saddle River, N.J: Pearson/Prentice Hall, 2006).

[2] R. C. Hilborn, *Chaos and nonlinear dynamics: an introduction for scientists and engineers* (Oxford University Press on Demand, 2000).

[3] A. G. Radwan & S. K. Abd-El-Hafiz, Image encryption using generalized tent map. *Electronics, Circuits, and Systems (ICECS), 2013 IEEE 20th International Conference on* (IEEE, 2013), pp. 653–656.

[4] X. Wu, H. Hu, & B. Zhang, Parameter estimation only from the symbolic sequences generated by chaos system. *Chaos, Solitons & Fractals*, **22** (2004) 359–366.

[5] R. Rhouma & S. Belghith, Cryptanalysis of a spatiotemporal chaotic cryptosystem. *Chaos, Solitons & Fractals*, **41** (2009) 1718–1722. https://doi.org/10.1016/j.chaos.2008.07.016.

[6] S. Li & X. Zheng, Cryptanalysis of a chaotic image encryption method. *2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No.02CH37353)* (2002), pp. II-708-II–711 vol.2. https://doi.org/10.1109/ISCAS.2002.1011451.

[7] R. Parvaz & M. Zarebnia, A combination chaotic system and application in color image encryption. *Optics & Laser Technology*, **101** (2018) 30–41. https://doi.org/10.1016/j.optlastec.2017.10.024.

[8] Z. Hua, Y. Zhou, C.-M. Pun, & C. P. Chen, 2D Sine Logistic modulation map for image encryption. *Information Sciences*, **297** (2015) 80–94.

[9] Z. Hua & Y. Zhou, Image encryption using 2D Logistic-adjusted-Sine map. *Information Sciences*, **339** (2016) 237–253.

[10] R. Rhouma & S. Belghith, Cryptanalysis of a chaos-based cryptosystem on DSP. *Communications in Nonlinear Science and Numerical Simulation*, **16** (2011) 876–884.

[11] E. Solak, R. Rhouma, & S. Belghith, Cryptanalysis of a multi-chaotic systems based image cryptosystem. *Optics Communications*, **283** (2010) 232–236.

[12] C. A. Pickover, *Computers, Pattern, Chaos, and Beauty: Graphics from an Unseen World* (Courier Corporation, 2001).

[13] B. B. Mandelbrot, *The fractal geometry of nature* (WH freeman New York, 1983).

[14] R. M. Crownover, *Introduction to fractals and chaos* (Jones & Bartlett Pub, 1995).

[15] S. Agarwal, Secure Image Transmission Using Fractal and 2D-Chaotic Map. *Journal of Imaging*, **4** (2018) 17.

[16] J. Fridrich, Method for encrypting and decrypting data using chaotic maps, 2000.

[17] Y. Zhou, L. Bao, & C. L. P. Chen, A new 1D chaotic system for image encryption. *Signal Processing*, **97** (2014) 172–182. https://doi.org/10.1016/j.sigpro.2013.10.034.

[18] B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, & M. R. Mosavi, A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. *Multimedia tools and applications*, **71** (2014) 1469–1497.

[19] H. Zhu, C. Zhao, & X. Zhang, A novel image encryption–compression scheme using hyper-chaos and Chinese remainder theorem. *Signal Processing: Image Communication*, **28** (2013) 670–680.

[20] X. Wu, Y. Li, & J. Kurths, A New Color Image Encryption Scheme Using CML and a Fractional-Order Chaotic System. *PLoS ONE*, **10** (2015). https://doi.org/10.1371/journal.pone.0119660.

[21] H. Zhu, X. Zhang, H. Yu, C. Zhao, & Z. Zhu, A Novel Image Encryption Scheme Using the Composite Discrete Chaotic System. *Entropy*, **18** (2016) 276.

[22] X. Wang, S. Wang, Y. Zhang, & K. Guo, A novel image encryption algorithm based on chaotic shuffling method. *Information Security Journal: A Global Perspective*, **26** (2017) 7–16. https://doi.org/10.1080/19393555.2016.1272725.

[23] M. Kanafchian & B. Fathi-Vajargah, A Novel Image Encryption Scheme Based on Clifford Attractor and Noisy Logistic Map for Secure Transferring Images in Navy. *International Journal of e-Navigation and Maritime Economy*, **6** (2017) 53–63. https://doi.org/10.1016/j.enavi.2017.05.007.

[24] R. Zahmoul, R. Ejbali, & M. Zaied, Image encryption based on new Beta chaotic maps. *Optics and Lasers in Engineering*, **96** (2017) 39–49. https://doi.org/10.1016/j.optlaseng.2017.04.009.

[25] Y. Zhou, L. Bao, & C. P. Chen, Image encryption using a new parametric switching chaotic system. *Signal processing*, **93** (2013) 3039–3052.

[26] R. Ye & W. Guo, An Image Encryption Scheme Based on Chaotic Systems with Changeable Parameters. *International Journal of Computer Network and Information Security*, **6** (2014) 37–45. https://doi.org/10.5815/ijcnis.2014.04.05.

[27] L. Y. Zhang, Y. Liu, C. Wang, J. Zhou, Y. Zhang, & G. Chen, Improved known-plaintext attack to permutation-only multimedia ciphers. *Information Sciences*, **430** (2018) 228–239.
[28] X.-Y. Wang, Y.-Q. Zhang, & X.-M. Bao, A novel chaotic image encryption scheme using DNA sequence operations. *Optics and Lasers in Engineering*, **73** (2015) 53–61.
[29] W. Zheng, F.-Y. Wang, & K. Wang, An ACP-based Approach to Color Image Encryption Using DNA Sequence Operation and Hyper-chaotic System. (n.d.).
[30] Q. Zhang, S. Zhou, & X. Wei, An efficient approach for DNA fractal-based image encryption. *Appl. Math. Inf. Sci*, **5** (2011) 445–459.
[31] J. M. Vilardy, C. J. Jimenez, & R. Perez, Image encryption using the Gyrator transform and random phase masks generated by using chaos. *Journal of Physics: Conference Series*, **850** (2017) 012012. https://doi.org/10.1088/1742-6596/850/1/012012.
[32] M. Ahmad, M. Z. Alam, Z. Umayya, S. Khan, & F. Ahmad, An image encryption approach using particle swarm optimization and chaotic map. *International Journal of Information Technology*, (2018) 1–9. https://doi.org/10.1007/s41870-018-0099-y.
[33] Department of Computer Science, Loughborough University, UK, R. S. Bhogal, B. Li, A. Gale, & Y. Chen, Medical Image Encryption using Chaotic Map Improved Advanced Encryption Standard. *International Journal of Information Technology and Computer Science*, **10** (2018) 1–10. https://doi.org/10.5815/ijitcs.2018.08.01.
[34] B. Howell, A. Reese, & M. Basile, Fractal Cryptology. *New Mexico High School, Supercomputing Challenge Final Report*, (2003).
[35] G. B. Huntress, Encryption using fractal key, US6782101 B1, 2004.
[36] S. Agarwal, Symmetric Key Encryption using Iterated Fractal Functions. *International Journal of Computer Network and Information Security*, **9** (2017) 1–9. https://doi.org/10.5815/ijcnis.2017.04.01.
[37] S. Agarwal & A. Negi, Midgets of Transcendental Superior Mandelbar Set. *IJCSI International Journal of Computer Science Issues*, **9** (2012) 214–220.
[38] M. Ivo, R. Jasek, & P. Varacha, Analysis of the Fractal Structures For the Information Encrypting Process. *International Journal of Computers*, **6** (2012) 224–231.
[39] S. Kumar, Public key cryptographic system using Mandelbrot sets. *Military Communications Conference, 2006. MILCOM 2006. IEEE* (IEEE, 2006), pp. 1–5.
[40] Y. Sun, R. Xu, L. Chen, & X. Hu, Image compression and encryption scheme using fractal dictionary and Julia set. *IET Image Processing*, 9 (2015) 173–183. https://doi.org/10.1049/iet-ipr.2014.0224.
[41] M. Mikhail, Y. Abouelseoud, & G. ElKobrosy, Two-Phase Image Encryption Scheme Based on FFCT and Fractals. *Security and Communication Networks*, (2017). https://doi.org/10.1155/2017/7367518.
[42] H. Oğraş & M. Türk, A Robust Chaos-Based Image Cryptosystem with an Improved Key Generator and Plain Image Sensitivity Mechanism. *Journal of Information Security*, **08** (2017) 23–41. https://doi.org/10.4236/jis.2017.81003.
[43] S. K. Abd-El-Hafiz, A. G. Radwan, S. H. A. Haleem, & M. L. Barakat, A fractal-based image encryption system. *IET Image Processing*, **8** (2014) 742–752. https://doi.org/10.1049/iet-ipr.2013.0570.
[44] H.-O. Peitgen, H. Jürgens, & D. Saupe, *Chaos and fractals: new frontiers of science* (Springer Science & Business Media, 2006).
[45] W. R. Mann, Mean Value Methods in Iteration. *Proceedings of the American Mathematical Society*, **4** (1953) 506–510. https://doi.org/10.2307/2032162.
[46] S. Ishikawa, Fixed points by a new iteration method. *Proceedings of the American Mathematical Society*, **44** (1974) 147–150.
[47] D. Arroyo, R. Rhouma, G. Alvarez, S. Li, & V. Fernandez, On the security of a new image encryption scheme based on chaotic map lattices. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, **18** (2008) 033112.
[48] W. Xiaofu & S. Songgeng, A general efficient method for chaotic signal estimation. *IEEE Transactions on signal processing*, **47** (1999) 1424–1428.
[49] S. S. Hedge & N. B. Rao, Visual cryptography (VC) using zigzag scan approach. *J. Comput. Sci. Eng. Technol*, **1** (2011) 456–461.
[50] G. Alvarez & S. Li, Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos*, **16** (2006) 2129–2151.
[51] Y. Wang, K.-W. Wong, X. Liao, T. Xiang, & G. Chen, A chaos-based image encryption algorithm with variable control parameters. *Chaos, Solitons & Fractals*, **41** (2009) 1773–1783.
[52] C. E. Shannon, Communication theory of secrecy systems. *Bell Labs Technical Journal*, **28** (1949) 656–715.
[53] Y. Wu, J. P. Noonan, & S. Agaian, NPCR and UACI randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, (2011) 31–38.

Authors' Profiles

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 15 research papers in various International journals and conferences indexed in Scopus, Emerging Sources Citation Index, springer, ACM, Thomson Reuters, google scholar and in many more. She was awarded with best paper presentation award in a conference ICVISP held in Las Vegas, USA. Her research interest includes fractal, cryptography and image processing.

How to cite this paper: Shafali Agarwal,"A Chaotic Cryptosystem using Conjugate Transcendental Fractal Function", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.2, pp.1-12, 2019.DOI: 10.5815/ijcnis.2019.02.01

