An Image Encryption Algorithm with Hermite Chaotic Polynomials and Scan Pattern

T.Sivakumar, M.Pandi, N.Senthil Madasamy, R.Bharathi

Department of CSE, Dr.Mahalingam College of Engineering & Technology
Pollachi, Coimbatore, Tamilnadu-642 003, India

msg2sk2010@gmail.com

Abstract. In today’s digital world, massive amount of sensitive information is being generated in the form of image and further it is shared via Internet. Maintaining the confidentiality of these data has become a major issue due to security vulnerability present in the network and transmission media. Image encryption algorithms are developed by various researchers to permit only authorized users to access and view sensitive images. This paper presents a novel image encryption scheme based on Hermite polynomials chaos function. First, random key stream is generated by using Hermite polynomial with different initial and incremental values of the variables. Next, the original image is scrambled with scan pattern to rearrange the pixels position. The scrambled image is XORed with the random key stream to get the encrypted image. The proposed method is experimented and observed that it is efficient and confirms the confusion and diffusion properties of a secure image encryption method. Large key space, low relation between the pixels of encrypted image, and sensitivity to initial seed value of the key are the strength of the proposed image encryption method.

1. Introduction
Image data is frequently generated from the sources such as medical space research, military, personal photograph etc. Image data generated from the medical and military domains are much sensitive than other sources. With the rapid development of network technology and their increasing popularity, the sensitive images are exchanged more frequently through internet. Thus, image data protection has become more important [1]. The encryption techniques like DES, AES, IDEA etc. are good algorithms for text encryption, but they are unsuitable for image encryption [7]. Thus, researchers introduced several image protection methods. Due to the properties of ergodicity, unpredictability and high sensitivity to initial conditions, chaotic systems have been extensively researched for digital image encryption [7].

Chaos sequences are random sequences generated by chaotic mapping. These structures are very complex and prediction of chaos sequences are too difficult. In 1970, Chaos theory was proposed, which was used in number of research areas, such as mathematics, engineering, physics, biology, and so on [3]. In 1998, Fridrich proposed a chaos based encryption algorithm composing of two stages: permutation and diffusion [1]. The permutation stage is used to rearrange the position of pixels in the image. It will change the image structure and weaken the correlation between adjacent pixels. The
diffusion stage is used to change the image pixel values to random values. The drawbacks of the Fridrich’s algorithm are (a) the permutation and diffusion is independent with each other, (b) diffusion function is too simple to break, and (c) key stream is not related to the plain image [1]. Some chaos based image encryption with permutation-diffusion structure is practically weak to resist common cryptanalysis. To overcome the drawbacks in the existing chaos based image encryption schemes, many researches turn to design improved chaos based cryptosystem with large keyspaces and efficient permutation-diffusion mechanisms. In unprocessed images, neighboring pixels are highly correlated. Owing to this correlation, any pixel value can be predicted from their neighboring pixels. Value transformation algorithms are based on the technique in which the value of each pixel is changed to some other value [4].

In this paper, a new image encryption scheme using Hermite chaos polynomials is proposed. The proposed method adopts the classic framework of the substitution-permutation network of cryptography and this ensures both confusion and diffusion properties. The proposed method is a private key encryption method, in which the same key is used for both encryption and decryption processes.

The rest of the sections in the paper are organized as follows. Section 2 provides a brief overview of the existing image encryption techniques based on chaotic maps and scan pattern. Section 3 describes the proposed image encryption method and the results of the experiment with analysis are discussed in Section 4. Section 5 concludes the paper.

2. Literature Survey

In this section, the existing and related image encryption methods developed by various researchers are presented.

The one-time pad (OTP) is a famous encryption scheme which provides semantic security. However, it is not practical to use since the randomly generated key needs to be the same length with the plaintext and it should be used only once. In [1], the authors designed to achieve the effect of one-time pad using asymmetric chaotic encryption scheme based on Chebyshev polynomials. The key establishment algorithm is used to generate three chaotic pseudo-random sequences to permute the rows and the columns of the plain image randomly. The first sequence is used to apply cyclic shift to each row, whereas the second sequence applies a cyclic shift to each column. The third sequence is used to mask each pixel in its new position with the help of first two sequences. Then each pixel is XORed with respect to a random value obtained based on its new position to mask its value.

Applying chaos to cryptography was a great contribution to improving the security of information and communications. Rabinovich-Fabrikant equations are a chaotic dynamical system of three ordinary differential equations. In [2], the authors adopted the classic framework of the permutation-substitution network in cryptography and this ensures both confusion and diffusion properties of a secure cipher. In confusion stage, the rich chaotic properties of the Rabinovich-Fabrikant equations is used to shuffle the plain image using initial conditions and control parameters as the key. In the diffusion stage, the cipher image is obtained by performing the MOD and bit XOR operations on the shuffles image using the chaotic sequence generated from the Rabinovich-Fabrikant equations.

The three-dimensional chaotic logistic map is modified to generate key stream. The chaos-based key stream is generated by a three-dimensional chaotic logistic map achieve better performance in terms of randomness properties and security level. It provides the necessary properties for a secure image encryptions scheme including the confusion and diffusion properties [3]. In [4], the plain image is converted into binary matrix and use the sum of all bits in the binary matrix as a part of secret keys to resist chosen plain text attack and known plain text attack. Then, a mapping which maps a random bit position to another random bit position is performed. Further, a chaotic map with Markov properties is used in the diffuse process. The permutation stage is used to rearrange the position of pixels in the image. The Lorenz system is used to generate the parameters of 3D cat map. The permutations process is based on double random position mapping with reverse 3D cat map and 3D cat map can to confuse image information and to make the histogram as flat.
Substitution boxes are built for the advanced encryption standard (AES) cryptosystem using chaos, and generated by a non-linear differential equation. The boxes non-linearity is quantified using the Walsh function. Probabilistic encryption is an approach in which different cipher texts are generated each time same plaintext is encrypted using the same key [5]. In [6], the authors employed a random bit insertion phase followed by four rounds of two staged diffusion involving simple XOR operation making it computationally efficient random bit insertion makes the scheme probabilistic. It comprises of two phases namely random bits insertion and four rounds of two-staged diffusion. A pixel-wise XOR operations is applied to the original image followed by a pixel-wise random permutation. The image is decomposed into the four blocks according to the quadtree decomposition strategy. Fractals are based on repeated replacements in a recursive mathematical formula which generates fractal geometry and pattern by several repeated times. A fractal image can be effectively used as a key in encryption. Breaking this type of key against attacks is very difficult. Hennon mapping is a reversible two-dimensional chaotic mapping used to generate pseudorandom sequences and select pixels from fractal key. In [7], the authors utilized a combination of permutation and diffusion to get high computational security.

A fourth order reversible MCA is applied, the blocks obtained from the quadtree decomposition are considered as the initial MCA configuration, and the transition rules are determined using the chaotic map. The key streams in the encryption scheme [8] are divided from the SHA-256 hash function. Hash function produces the digest of the input plain text, known as a hash value, which can be considered as a unique signature of the input. The cryptography scheme in [8] involves three stages of encryption. Firstly, to induce diffusion, image pixels are bitwise XOR with a chaotic sequence using Logistic-Sine (LS) map. The permutation of image pixels is then carried out using a pseudo-random number generator (PRNG) to induce confusion. Finally, the resulting image is split into four blocks of equal size using the quadtree decomposition strategy, and a fourth order reversible MCA is applied to them. These four blocks are considered as the initial configuration of MCA, and the transition rules are determined using the chaotic map. Then a combination of chaotic system and reversible MCA is used for inducing diffusion.

With identical chaotic injection from a master laser with two optical feedbacks, two slave lasers can output similar chaotic signals served as chaotic carrier to transmit image and used to generate the core part of the encryption system [9]. A 128-bit key is selected to generate the original value of the double chaotic system, which decides the DNA complementary rule. A large chaotic sequence can be obtained by CML (coupled map lattice) chaotic system. Obtaining lot of sequence by iterating the CML chaotic system to shuffle the sequence of optical chaos. In the masking process, the parts of the image are XORed to improve the sensitivity of the image. The digital image is transformed into a plane of DNA. It selects the first and the second bit of every pixel to make the first DNA-plane, the third and fourth bit to make the second DNA-plane, the fifth and sixth bit to make the third DNA-plane and seventh and eighth bit to make the fourth DNA-plane in order to improve the key sensitivity. Generating the twelve new DNA planes by the sixth kinds of the DNA complementary rules. A big DNA plane is obtained by connecting four DNA planes, thus forming three big DNA planes. After permutation and diffusion process, the DNA plane is converted into a digital image [9].

Arnold’s cat map is a special type of chaotic map and transforms the original positions of the pixels. The algorithm is based on pixel permutation using a variation of the Arnold’s cat map algorithm. For an image each pixel is replaced by another pixel from the image. A random pixel is then selected and the pixel value, at that location serves as the key. A new matrix is then constructed and initialized. A bitwise XOR is performed between the normalized image and the newly constructed matrix to obtain the encrypted image. This encrypted image is then masked into a general image, called the key image, to elude the intruder [10].

The encryption method in [11] is based on scan methodology and random key stream. Scan is a formal language-based two-dimensional spatial access, which could generate large number of scanning paths. Scan is a special purpose context-free language devoted to describe and generate a wide range of 2-D array. The concept of Z-Order (ZO) curve is used in spatial, text, and multimedia
databases to implement one-dimensional index and search on multi-dimensional data. The pixels coordinates are permuted by using the Z-Ordering based scan pattern to obtain the scrambled image. The pixels value of the scrambled is changed by the symmetric bitwise XOR operation to obtain the encrypted image. The random number to perform XOR operation is generated by using Blum Blum Shub (BBS) generator.

In [23], random numbers are generated by Linear congruential generator. These numbers are used as index for shuffling of rows, columns and pixels of an image. In this scheme [23], two random numbers sequences are generated by choosing appropriate parameters and seed value. Then by using values of these random numbers, image permutation occurs by shuffling of rows, columns and pixels of image. One sequence is used for row shuffling and another is used for column shuffling. A masking operation is used after row and column shuffling by simple XOR operations between adjacent rows and columns. The system in [24] uses affine transformation provided by a three dimensional matrix. The chaotic sequence was sorted and the one dimensional data. The number of iterations was calculated, all the pixel values of color image were transformed into graycode iteratively and then the chaotic sequence was generated from the four-dimensional hyperchaotic system. Pixel matrix after graycode transformation was converted to one-dimensional matrix. The chaotic sequence was sorted and the one-dimensional matrix positions was changed correspondingly to complete the whole domain scrambling and then, bit-operation was executed for image diffusion. In [17], two encryption schemes for grayscale and color images are proposed. The first scheme starts with reading the grayscale or color image, then, divide it into blocks of size N×N. The image is divided into blocks of sizes 8×8, 16×16 and 32×32 pixels. Then, each 2D plain block is converted in to 1D block array by using Zigzag pattern. The resulted block arrays are encrypted with its analogue secret key using the XOR operation. In the second scheme, the plain image block is XORed with the previous encrypted image block before it is in turn encrypted according to the Cipher Block Chaining (CBC) mode. The encryption of each image block depends on all the previous blocks. So, each cipher image block is dependent not just on the plain image block that generated it but on all the previous plain image blocks.

In [13], the authors employed Ikeda map to generate random bit sequence. For each plain image a unique key dependent chaotic sequence is randomly generated to produce secrete sequences for driving bifurcation keys. The scheme applies three different chaotic maps and includes three steps such as unique random permutation key generator, confusion process, and diffusion process. In [14], the plain image can be recovered completely if the initial condition and parameter are exactly known. The cryptosystem is robust against cryptographic attacks, for the key space is large enough. The one-time pad cryptosystem can ensure two ciphered images differently, even if there is only one-bit difference between them. In [15], a simple and robust gray image encryption scheme using chaotic logistic map and artificial neural network is presented. In hyperchaotic system [16] “transforming-scrambling-diffusion” model is applied. Before scrambling, in accordance with the plaintext attributes, the number of iterations was calculated, all the pixel values of color image were transformed into graycode iteratively and then the chaotic sequence was generated from the four-dimensional hyperchaotic system. Pixel matrix after graycode transformation was converted to one-dimensional matrix. The chaotic sequence was sorted and the one-dimensional matrix positions was changed correspondingly to complete the whole domain scrambling and then, bit-operation was executed for image diffusion. In [17], two encryption schemes for grayscale and color images are proposed. The first scheme starts with reading the grayscale or color image, then, divide it into blocks of size N×N. The image is divided into blocks of sizes 8×8, 16×16 and 32×32 pixels. Then, each 2D plain block is converted in to 1D block array by using Zigzag pattern. The resulted block arrays are encrypted with its analogue secret key using the XOR operation. In the second scheme, the plain image block is XORed with the previous encrypted image block before it is in turn encrypted according to the Cipher Block Chaining (CBC) mode. The encryption of each image block depends on all the previous blocks. So, each cipher image block is dependent not just on the plain image block that generated it but on all the previous plain image blocks.

In [23], random numbers are generated by Linear congruential generator. These numbers are used as index for shuffling of rows, columns and pixels of an image. In this scheme [23], two random numbers sequences are generated by choosing appropriate parameters and seed value. Then by using values of these random numbers, image permutation occurs by shuffling of rows, columns and pixels of image. One sequence is used for row shuffling and another is used for column shuffling. A masking operation is used after row and column shuffling by simple XOR operations between adjacent rows and columns. The system in [24] uses affine transformation provided by a three-order invertible matrix and a dynamic translation vector. This vector is dynamically transformed at each iteration by an affine transformation composed of a chaotic matrix T not necessarily invertible and a pseudo random translation vector Y. The parameters of the matrix T and the vector Y are chosen dynamically and chaotically from the PWCLM chaotic map. The objective of this translation vector is to make the first pixels safe. This stage consists of two main parts. The confusion based on an improved method of Hill cipher. This step is an affine transformation determined by an invertible matrix A of order three in the ring G and a chaotic translation X. This vector is transformed dynamically at each iteration by a matrix T of order three in G and another vector of translation Y chosen randomly from the chaotic map. The confusion scheme proposed in [25] simultaneously changes the pixel locations and modifies their values. A pseudorandom number determines the kind of mapping employed in each bit plane. To permute a basic image unit using conventional confusion, two pseudorandom numbers should be generated to determine the new position of that basic unit. After that, the unit is relocated from the original memory address to the new memory address. In [28], an image encryption method using scan pattern and random key stream derived from laser chaos is presented. The cores of the algorithm of the paper [29] are based on the discrete chaotic maps namely Arnold’s cat map and a combination of three
generalized map, one continuous Lorenz chaotic system and two non-chaotic generators such as fractals and chess-based algorithms. A fractal object is self-similar at numerous scales of magnification and can be represented as a mathematical equation that is iterated for a finite number of times. In the algorithm [29], the permutation phase block represents one of the selected permutation techniques (Lorenz chaotic systems, Arnold’s cat map and chess-based algorithm) and the substitution phase block represents one of the selected substitution techniques. The non-chaotic methods have proved their existence in implementing the confusion.

Thus, it can be inferred that applying chaos to cryptography is being a great contribution to improving the security of information communicated over Internet. Chaotic system has an inherent property of hiding relationship between initial and final states. Thus, a new image encryption method using Hermite polynomial chaos and scan pattern is proposed in this paper.

3. The Proposed Image Encryption Method
In this section, the working model of the proposed image encryption method is presented with block diagram and algorithms.

3.1 Introduction to Hermite Polynomials
Chaotic systems are one of the most promising dynamical systems to design cryptosystems. The discrete dynamic chaotic system has an inherent property of hiding relationship between initial and final states. Polynomial chaos is a non sampling-based method to determine evolution of uncertainty in a dynamical system when there is a probabilistic uncertainty in the system parameters. The \( n \)th order hermite polynomial is a polynomial of degree \( n \). The distribution for hermite polynomial (1) is standard normal distribution:

\[
    f(x) = \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{x^2}{2}\right) \quad \text{for } x \in \mathbb{R}
\]

The probabilistic hermite polynomials \( \text{He}_n(2) \),

\[
    \text{He}_n(x) = \sum_{k=0}^{n} c_k x^k
\]

Where, \( n=0,1,2,3,.. \), the \( c_k \) = coefficient and for \( k \geq 0 \).

3.2 Properties of Hermite Polynomials
The Hermite polynomials are a classical orthogonal polynomial sequence. The polynomials arise in probability, combinatorics, numerical analysis, physics, systems theory and random matrix theory. The \( n \)th order Hermite polynomial is a polynomial of degree \( n \). The probabilists’ version \( \text{He}_n \) has leading coefficient 1, while the physicists’ version \( H_n \) has leading coefficient 2n. The sequence of probabilists’ Hermite polynomials satisfies the recurrence relation. The Hermite polynomials constitute an Appell sequence, i.e., they are a polynomial sequence satisfying the identity (3)

\[
    \text{He}_n(x)=n\text{He}_{n-1}(x)
\]

3.3 Cumulative Sum of the original image
The input image is stored in a matrix and the column-wise cumulative sum of the pixel values is performed to get the scrambled image that is it adds the value in its position with the previous row in the same column and the first column position value is added with the previous last row value. The first element of the cumulative matrix must be the first element of scrambled matrix. The cumulative sum of the scrambled matrix (4) for same column elements,

\[
    X(i,j)=x(i,j)+x(i-1,j)
\]

where \( i,j \) represents the row and column position in the matrix \( x \).

The first element of column is calculated as (5),

\[
    x(i,j)=x(i,j)+x(k,j-1)
\]

Where, \( k \) is the last row position in the matrix \( x \).
3.4 Random Key Generation using Hermite Polynomial

The real roots of the polynomials are used to generate random key values key of size nxn, where n is the size of the plain image in the proposed encryption method. Solve the Hermite Polynomial chaos and find the real roots of these polynomials. From the result, the real roots of the polynomials is used to generate random key stream. Separate the fractional and decimal parts and convert the decimal values into binary 8-bits values.

Function: Random Key Generator

Procedure Hermite Poly (n)

if (n ==0) then
    return poly (1,"x"," coeff ")
elseif (n ==1) then
    return poly ([0 1],"x"," coeff ")
else
    polyx = poly ([0 1],"x"," coeff ")
    yn2= poly (1,"x"," coeff ")
    yn1= polyx
    for k=2:n
        return polyx *yn1 -(k-1)* yn2
    yn2 =yn1
    yn1 =y
end

3.5 The encryption process

The original image to be encrypted is converted into grayscale image and resized into 256x256 pixels. Further, scrambling process is performed with the help of chosen scan pattern. The random key streams are generated from the real roots of the hermite polynomials. The cipher image is obtained by XORing the key stream with scrambled image. Figure 1 presents the working model of the proposed encryption method using a flowchart. The experimentation is done in Windows10 environment using Scilab 6.0.2 with ATOMS and GUI module.

The proposed encryption method consists of both confusion and diffusion. In confusion stage, the chaotic properties of Hermite polynomials are used to generate the key values to shuffle the binary image obtained by thresholding the plain image. In diffusion stage, the cipher image is obtained by performing bit-XOR operations between the scrambled image and the random key values. The following are the sequence of steps to be followed to encrypt the input image.

Step 1: Read the plain image of size m x n where m and n are the number of rows and columns.
Step 2: Perform Column wise cumulative sum of the image matrix.
Step 3: The random key values are generated using the roots of the Hermite Polynomials.
Step 4: Perform pixel permutation using zigzag scan pattern.
Step 5: Perform bitwise XOR operation between the Scrambled image and the random key values to obtain the cipher.
Step 6: Store the cipher image
3.6 The Decryption Algorithm

The decryption is the reverse process of the encryption procedure and the sequence of steps needed to decrypt the image are given below.

Step 1: Read the cipher image.
Step 2: Generate the random key streams by calling the random key generator function.
Step 3: Rearrange the pixel based on the zigzag scan pattern.
Step 4: Perform bit-XOR operations between the random key values generated by the polynomial chaos and the cipher image.
Step 5: Perform column wise cumulative subtraction to get the decrypted image.
Step 6: Store the decrypted image.

4. Experimental and Result Analysis

The proposed Hermite polynomial chaotic encryption method is tested with the standard test images used in the field of image process in with 256x256 pixels. The original Lena image is shown in Figure 2. For visual observation, the random key stream generated using the real roots of Hermite polynomials is shown in Figure 3.

Figure 1. Block Diagram of the Proposed Image Encryption Method

Figure 2. Original Lena image

Figure 3. Sample Random Key Stream
An encryption algorithm should have strong resistance to any kinds of attacks, such as known plain text attack, differential attack, chosen plain text attack and so on. The most widely used evaluation criteria are Shannon entropy, Histogram and Correlation etc. The encrypted image must be composed of totally random patterns and pixel values that do not reveal any of the features of the original image.

4.1 Information Entropy

The information entropy is used to measure the degree of uncertainties of the system. It can be used for evaluating the randomness of the image. Let m be the information source, the mathematical formula to compute the entropy of the message source is given in the equation (6)

\[ H(m) = - \sum_{i=0}^{2^R-1} P(m_i) \log_2 P(m_i) \]  

(6)

Where, R is the number of bits to represent the symbol \( m_i \) and \( P(m_i) \) is the emergence probability of the symbol \( m_i \). For ideally random image, the value of information entropy is 8. The entropy obtained by the proposed method is compared with the few existing methods in the Table 1.

| Encryption         | Entropy Value (Sh) |
|--------------------|--------------------|
| Proposed method    | 7.9960             |
| Ref. [4]           | 7.9972             |
| Ref. [7]           | 7.9966             |
| Ref. [12]          | 7.9924             |
| Ref.[23]           | 7.9617             |

4.2 Histogram Analysis

The histogram of the image before and after the encryption is analyzed the statistical performance. The histogram of the cipher image can give information of the original image. If it is not uniform enough, a mass of information may be analyzed by the statistic attack. Figure 6 shows the histogram of the original image and 7 shows the histogram of the decrypted image.
From the experimental results, one can find the histograms of the encrypted images have been modified and greatly different from those of the plain images. Furthermore, the histograms of the cipher images are all uniform which means the proposed algorithm is considered robust against histogram analysis attack.

4.3 Correlation Analysis

One notable feature for natural image with meaningful visual perception is redundancy. The correlation between adjacent pixels is usually high in the plain image. An effective encryption system should reduce the correlation between adjacent pixels greatly to resist the statistical attack. Zero correlation is the best result for an ideal cryptosystem. 3000 pairs of adjacent pixels at the horizontal, vertical and diagonal directions are selected from the plain image and ciphered image randomly to calculate the correlation coefficients. Table 2 shows the cross correlation between the original and encrypted images and Table 3 shows the correlation between the adjacent pixels of the encrypted image.

| Encryption Method | Cross Correlation |
|-------------------|-------------------|
| Proposed          | -3.4763x10^{-4}   |
| Ref. [6]          | -2.2056x10^{-4}   |
| Ref. [12]         | 3.66x10^{-2}      |
| Ref. [23]         | 1.26x10^{-2}      |

Table 2. Comparison of cross correlation

| Encryption Method | Directions |
|-------------------|------------|
|                  | Horizontal | Vertical  | Diagonal |
| Proposed          | 0.0109     | 0.0212    | 0.0032   |
| Ref. [4]          | 0.0220     | -0.0029   | -0.0083  |
| Ref. [7]          | -0.0103    | 0.0066    | 0.0014   |
| Ref. [8]          | -0.0027    | 0.0055    | -0.0016  |
| Ref. [12]         | 0.0045     | 0.0073    | 0.0241   |

Table 3. Correlation Coefficient between Adjacent Pixels

The graphical view of correlation between adjacent pixels of the original and encrypted Lena images in the horizontal, vertical, and diagonal directions are shown in Figures 8, 9 and 10.

![Figure 8. Vertical Directions of Original and Encrypted Images](image-url)
From the above result analysis, it is seen that the proposed system is highly reliable against the statistical attacks. The result of security analysis shows the encryption algorithm is effective, such as the key is hypersensitive, histograms are mean distributed after encrypting, correlation between the adjacent pixel is infinitesimal and entropy is approximately equal to 8. The decrypted image is the same as the original image, which proves the cryptosystem is executable.

5. Conclusion and Future Work

This paper proposed a chaotic based image encryption using polynomial chaos. The process consists of key generation using Hermite polynomials followed by the permutation with the pixel values. Performance of the proposed system is evaluated using several evaluation metrics like histogram analysis, entropy and correlation. The system is not reliable against differential attack. In future, the system should resist differential attack and the processing time can be improved. The decryption process can also be improved since some cracks are found in the decrypted image.

References

[1]. Shakiba, Ali, 2019. A randomized CPA-secure asymmetric-key chaotic color image encryption scheme based on the Chebyshev mappings and one-time pad. Journal of King Saud University-Computer and Information Sciences.

[2]. Yakubu, H. J., E. G. Dada, S. B. Joseph, and A. K. Anukem, 2019. A new chaotic image encryption algorithm for digital colour images using rabinovich-fabrikant equations. International Journal of Computer Science and Information Security. 17(1), pp. 15-23.
[3]. Li, Chunhu, Guangchun Luo, and Chunbao Li, 2017. An image encryption scheme based on the three-dimensional chaotic logistic map. International Journal of Network Security. 21(1), pp. 22-29.

[4]. Ge, Meng, and Ruisong Ye, 2019. A novel image encryption scheme based on 3D bit matrix and chaotic map with Markov properties. Egyptian Informatics Journal. 20(1), pp.45-54.

[5]. Silva-García, V. M., Rolando Flores-Carapia, Carlos Rentería-Márquez, B. Luna-Benoso, and Mario Aldape-Pérez, 2018. Substitution box generation using Chaos: An image encryption application. Applied Mathematics and Computation.332, pp.123-135.

[6]. Dhall, Sakshi, Saibal K. Pal, and Kapil Sharma, 2018. A chaos-based probabilistic block cipher for image encryption. Journal of King Saud University-Computer and Information Sciences.

[7]. Kashanian, Houman, Masoud Davoudi, and Hamed Khorramfar, 2016. Image encryption using chaos functions and fractal key. International Journal of Computer Science and Network Security. 16(10), pp. 87-92.

[8]. Aslam, Md Nazish, Akram Belazi, Sofiane Kharbech, Muhammad Talha, and Wei Xiang, 2019. Fourth order MCA and chaos-based image encryption scheme. IEEE Access, 7, pp. 66395-66409.

[9]. Fu, Xing-Quan, Bo-Cheng Liu, Yi-Yuan Xie, Wei Li, and Yong Liu, 2018. Image encryption-then-transmission using DNA encryption algorithm and the double chaos. IEEE Photonics Journal. 10(3), pp. 1-15.

[10]. Anwar, Shamama, and Solleti Meghana, 2019. A pixel permutation based image encryption technique using chaotic map. Multimedia Tools and Applications. 78(19), pp. 27569-27590.

[11]. Sivakumar, T, and R. Venkatesan, 2014. A novel image encryption method with Z-order curve and random number. International Journal of Computer Applications. 103(12).

[12]. Sivakumar, T, and R. Venkatesan, 2014. Image encryption based on pixel shuffling and random key stream. International Journal of Computer and Information Technology, 3(6).

[13]. Hikal, Noha A, and Marwa M. Eid, 2018. A new approach for palmprint image encryption based on hybrid chaotic maps. Journal of King Saud University-Computer and Information Sciences.

[14]. Liu, Hongjun, and Xingyuan Wang, 2010. Color image encryption based on one-time keys and robust chaotic maps. Computers & Mathematics with Applications. 59(10) pp.3320-3327.

[15]. Telem, Adelàide Nicole Kengnou, Colince Meli Segning, Godpromesse Kenne Hilaire Bertrand Fotsin, 2014. A simple and robust gray image encryption scheme using chaotic logistic map and artificial neural network. Advances in Multimedia.

[16]. Li, Chengai Fang Zheng Zhao, Chen Lieu, Lie Lie and Jie Zhang, 2019. A hyperchaotic color image encryption algorithm and security analysis. Security and Communication Networks.

[17]. Reyad, Omar, M. A. Mofaddel, W. M. Abd-Elhafiez, and Mohamed Fathy, 2017. A novel image encryption scheme based on different block sizes for grayscale and color images. 12th International Conference on Computer Engineering and Systems. pp. 455-461.

[18]. Ahadpour, Sodeif, and Yaser Sadra, 2012. A chaos-based image encryption scheme using chaotic coupled map lattices. University of Mohaghegh Aradabili.
[19]. Zhang, Xuefeng, and Jiulun Fan, 2007. Extended logistic chaotic sequence and its performance analysis. Tsinghua Science and Technology. 12(1), pp.156-161.

[20]. Anwar, Shamama, and SolletiMeghana, 2019. A pixel permutation based image encryption technique using chaotic map. Multimedia Tools and Applications. 78(19), pp.2769-27590.

[21]. Aarti Patel, MehulParikh, 2018. Multiple image encryption using chaotic map and DNA computing. International Journal of Research in Science, Engineering and Technology. 4, pp. 1395-1400.

[22]. Nestor, Tsafack, Nkapkop Jean De Dieu, Kengne Jacques, Effa Joseph Yves, Abdullah M. Iliyasu, and Ahmed A. Abd El-Latif, 2019. A multidimensional hyperjerk oscillator: dynamics analysis, analogue and digital implementation, and its application as a cryptosystem. Sensors. 20(1) pp.1-23.

[23]. Banthia, Arihant Kr, and Namita Tiwari, 2013. Image encryption using pseudo random number generators. International Journal of Computer Applications. 67(20), pp.1-8.

[24]. Hraoui, Said, Faïq Gmira, M. Fouad Abbou, A. Jarrar Oulidi, and Abdellatif Jarjar. 2019. A new cryptosystem of color image using a dynamic-chaos Hill Cipher algorithm. Procedia Computer Science. 148, pp. 399-408.

[25]. Nandeesh, G. S., P. A. Vijaya, and M. V. Sathyanarayana, 2013. An image encryption using bit level permutation and dependent diffusion. International Journal of Computer Science and Mobile Computing. 2(5), pp.145-154.

[26]. Norouzi, Benyamin, Seyed Mohammad Seyedzadeh, Sattar Mirzakuchaki, and Mohammad Reza Mosavi, 2015. A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos. Multimedia Tools and Applications. 74(3), pp-781-811.

[27]. Seyedzadeh, Seyed Mohammad, and Sattar Mirzakuchaki, 2012. A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. Signal Processing. 92(5), pp.1202-1215.

[28]. T Sivakumar, Pu Li, 2019. A Secure Image Encryption Method using Scan Pattern and Random Key Stream derived from Laser Chaos. Optics & Laser Technology. 111, pp. 196-204.

[29]. Radwan, Ahmed G., Sherif H. Abd Haleem, and Salwa K. Abd-El-Hazif, 2016. Symmetric algorithms using chaotic and non-chaotic generators: A review. Journal of Advanced Research. 7(2), pp.193-208.