I. J. Mathematical Sciences and Computing, **2023, 3, 12-25**
Published Online on August 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijmsc.2023.03.02

Design and Development of Multidimensional Chaotic Maps with Genetic Operator

Sudeep Nooly B*
JNN College of Engineering/Department of Computer Science and Engineering, Shimoga, 577204, India
E-mail: sudeepnooly@gmail.com
ORCID iD: https://orcid.org/0000-0001-5432-982X
*Corresponding Author

Ravindra S
JNN College of Engineering/Department of Computer Science and Engineering, Shimoga, 577204, India
E-mail: ravindra@jnnce.ac.in
ORCID iD: https://orcid.org/0000-0002-2601-0181

Received: 29 November, 2022; Revised: 23 December, 2022; Accepted: 29 January, 2023; Published: 08 August, 2023

Abstract: Security of a digital image can be achieved in number of ways including image Encryption and Decryption. Encryption technique tries to convert a plain image into the cipher image which is hard to understand. The decryption technique tries to convert a cipher image into the plain image. The image encryption is done inorder to provide security from attacks. In this work we aim to develop an image encryption technique based on multidimensional chaotic map with genetic operator. One of the powerful features of genetic operator is crossover which is used to confuse the pixels of the image. A combination of multidimensional chaotic maps, namely, Logistic, Henon and Chebyshev will be used to generate pseudorandom sequence which will be XOR'ed to obtain an unpredictable sequence. This sequence will be then applied to the Crossover unit and upon XOR'ed to obtain an encrypted image. Later the same upredictable sequence is generated while decrypting the image. By combining the entire different dimensional chaotic map namely Logistic, Henon, Chebyshev map along with the gentic operator called crossover will enhance the extra security to the digital image.

Index Terms: Multidimensional Chaotic Maps, Statisical Analysis, Image Encryption

1. Introduction

With the evolution of internet, large amount of information is being accessed and shared over the network. The valuable information that is accessed on internet that has the high risk of being stolen, altered, or utilised improperly. In the past, information was safeguarded by printing it on paper and locking it in a filing cabinet. But with network and internet, attacker can steal electronically recorded data, including text and photos[12]. The solution to protect data from attacker is cryptography. Efficient solutions can be devised using cryptography to provide security to the valuable information.

The problem statement is by having different algorithm separately to encrypt the data which are not much secure and the existing solution for the mentioned problem are AES, DES, RSA etc. Since all these algorithms are used different to encrypt the data. In this research the combination of multidimensional chaotic maps with genetic operator will enhance the more security to the digital image. The main objectives of this research is to study the different dimensional chaotic maps, design different chaotic sequence, Implementing the security model using the chaotic sequences and along with the statistical evaluation factors such as histogram analysis and correlation Coefficient Analysis.

It is the science of secret codes, methods of protecting data from unauthorized disclosure and modification. Plaintext is data that can be read and understood without any special measures. Using key, cryptographic systems can convert plaintext into cypher text. The method of modifying plaintext in order to hide its content is called encryption. It guarantees that the information will be sent without any modification and only the intended recipient will be able to access and read it[13]. The process of reverting back from cipher text to its original plaintext is called decryption. Cryptography provides number of security services to ensure the privacy on-alteration of data. Information security services replicate the type of function normally associated with the physical document. Important components of

security include authentication, authorization, integrity, Confidentiality, non-repudiation and access control.

Multimedia data includes image, audio and video. DES, triple DES and AES are the traditional encryption algorithms that are suitable only for text or binary data because multimedia data has high redundancy and correlation of data, large volumes and include real-time operations so multimedia encryption algorithms have more requirements. To adapt the requirements of multimedia data, multimedia encryption algorithm makes certain changes to the traditional encryption algorithm. Image, audio and video encryption are the classification of encryption algorithm. Substitution and transposition are the two techniques of encryption, to change the pixel values and position and to make the image look different from original image. In second classification of encryption the original audio signals is converted so that it is not understandable. Video is collection of image frames and data is of large volume so often encryption is carried on compressed data to make it look different from the original video. Complete, partial and compression-combined encryption is the three classification of image encryption algorithm. The entire multimedia file is encrypted directly using encryption key[15]. It is symmetric so encryption and decryption uses same key in Complete also it provides good security since it encrypts the largest data volumes and low efficiency where as in partial only some part of the image need to be encrypted then in compression-combined encryption, the encryption and compression operations are merged, and both operations are carried out at the same time. Partial and compression-combined encryption uses small amount of data compared to complete encryption so it offers higher efficiency and lower security. Based on the properties of encryption algorithm the complete image encryption are classified into four types namely permutation, random modulation, confusion diffusion and partial DES algorithm. In chaos based encryption a chaotic map is used to generate sequence. The sequence is used for confusion and diffusion process. Initial value acts as its input, the control parameters determine its action and the output is the sequence produced by the iterated maps in the chaotic map. It has some typical features which is suitable for encryption. The chaotic map generates the sequence with random properties by giving the initial value. The sequence is sensitive to the initial value i.e two initial values with a small changes will cause major change after multiple iterations. Because of the above properties of randomness and sensitivity chaos based encryption is more suitable for multimedia data.

The stochastic search algorithm is known as genetic algorithms (GA) which combines both genetics with selection. GA differing from other search techniques and algorithms starts with a population which is a solution satisfying boundary or system constraints to the problem. One of the genetic operators is Crossover which combines two parent chromosomes to produce a new child chromosome are known as Crossover and also known as offspring. The concept behind crossover is that the new chromosome has best feature of both the parents and may even be superior to parent chromosomes. The Crossover operators are classified into five types namely One-Point, Two-Point, Uniform, Cut and Splice, Multi-Point crossover.

2. Related Works

The large amount of information in a digital images and the more correlation among pixels, traditional encryption techniques such as DES, AES and RSA are found to be inefficient for image encryption. Some of those recent existing encryption techniques are analyzed in this work. Block cipher is applied on various multidimensional chaotic maps such as Chebyshev Map, Logistic Map, Cubic Map, Sine Map , Henon Map and Tent Map which enhance the robustness, key space and security of the satellite image. Here they use variable length secret key S (2 7, 2 8, 2 9) to generate keys of varying size as an input bits. Using a secret key S it evaluates the initial conditions of various multidimensional chaotic maps [1]. Logistic map, quantification, crossover, and mutation are the four general structure of algorithm. Based on the given parameters and initial values the Logistic map produce four chaotic sequences which gives keys the four chaotic sequences are mapped to the four key streams are used for the operations of mutation and crossover. Normalization, threshold level functions or ordered chaotic sequence is the ways where quantification is performed. The crossover unit is used to modify the rows and column to order the pixels of an image [2]. A chaotic theory which is based on the encryption algorithm high technologies are developing day by day security for the data has become more severity than earlier for this reason the cryptography presume a key technology in the security. For stream cipher encryption the chaotic algorithm is useful for its structure which is hard to forecast, analyze but not for sensitivity to the initial condition and characteristics of chaotic maps are mentioned [3]. The chaotic maps plays very important role in the diffusion and permutation mechanism to confuse the relationship between plain and cipher images. Firstly the chaotic sequences are generated by the Henon map and these sequences are generated by applying the initial condition and parameter values to the map then it produces the chaotic sequences further it is applied on plaintext as a row and column scrambling. Encryption is done by bit-wise XOR or two's complement addition and subtraction of pixel value with the generated chaotic sequence. As the symmetric key approach is used [4]. Logistic map and Tent map to produce the chaotic sequences instead of random values in Genetic Algorithm process. One of the powerful feature of genetic operator is crossover and mutation. The Chaotic Genetic Algorithm (CGA) hides the local convergence than the traditional Genetic Algorithm. This method reduces the iterations in optimization problems and the performance of Genetic Algorithm was improved [5]. The multimedia data or any information is growing gradually as a result data security plays vital role in the storing of data and transmitting of digital data that is audio signals, video signals and images. Encryption using chaotic maps which guarantees the secure communication of the image data. This techniques are used in many areas such as military, satellite images, medical science. To protect these data the pillers of

information security such as confidentiality, integrity and availability which plays very improtant role [6]? To enhance the security and efficiency of the encryption method a chaotic Tent map were used. To build a digital chaotic system a chaotic Tent map are used. To designing the encryption schema the features of Tent maps are very useful [7]. An image encryption algorithm using Logistic and Sine maps. Firstly, Arnold map were used inorder to scrambling of the pixels of an image. Next by using Logistic Sine map a 2 8 bit keys are generated. Finally the pixel values of scrambled image will be altered by XORing with the key which give rise to an encrypted image [8]. Data transmission is the major concern for the multimedia communication. Hence the security is the major area where everyone needs to be focused. In this research they focused on multidimensional chaotic maps they are used in encryption of an image also it consisting of merits and demerits. The features of chaotic maps such as highly sensitive to initial condition, ergodicity, stochastic make them more reliable for encryption of an image. The lower dimensional chaotic maps were developed earlier which exhibits the low level of security and cannot handle brute force and statistical attacks. To overcome with this issue this research provides various high dimensional chaotic maps [9]. In this generation an image are the largest media. The encryption techniques such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest–Shamir–Adleman (RSA) etc. shows lower level of security and very weak anti attack ability. To overcome this issue chaotic based cryptography were proposed. It is sensitively to the parameters and initial conditions so it is holds good for an image encryption [10]. The combination of henon map and chebyshev map where the output of the single map is used to as the input of the another map and its result shows the good chaotic performance, chaotic behaviors and high chaotic index along with great chaotic range in 2D- Henon chaotic map[12]. Replacing the pixels of an image and also changing the gray level values simultaneously. Firstly, the logistic chaotic map is used to shuffling the pixels of an image and then values of gray level using same orbit. 80 bit secure key is used to pick initial condition[13]. Henon map is used here for encryption process algorithm can be compared here with a conventional algorithm approach. Finally, a robustness of algorithm can be proved by security analysis[14]. Combination of both row wise and column wise are used to shiffle the pixels of an image and also diffusion principle is also applied using Chinese remainder[15].

3. Methodology

Encryption and Decryption model is designed based on chaotic maps. The system designed for encryption and decryption is shown in Figure 8. To generate the chaotic sequence the initial condition is considered from the chaotic map. To get an scrambled encrypted image a crossover is appiled on plain image futher to obtain the cipher image, the scrambled encrypted image is XORed with the chaotic sequence. In decryption process, to obtain the scrambled decrypted image same initial condition are used to generate keystream and XOR-ed with the cipher image[11]. To obtain the decrypted image a crossover is performed on scrambled decrypted image[11].

The system is divided into three different modules.

1. Chaotic sequence generation based on multidimensional chaotic maps namely Logistic, Henon and Chebysev.
2. Unpredictable sequence generation based on combination of multidimensional maps.
3. Encryption and decryption process.

3.1. Chaotic Sequence Generation Based on Multidimensional Maps

To produce real valued pseudo random numbers, chaotic maps are used.

- ***Logistic Map* :**

The Logistic map is represented by equation 1.

$$x_{n+1} = \lambda x_n(1 - x_n) \tag{1}$$

where the parameter λ is chosen to be 4 and it is belongs to the interval [0,4]. The n represents the length of the sequence, and x_0 is the initial condition which is given as input. The sequence generator and sequence of real numbers is the output and is shown in the Figure 1.

Fig. 1. Logistic sequence generator

Algorithm are given below,
Step 1: Input the length and initial condition to generate the Logistic sequence.
Step 2: Select parameter value r as 3.9999.
Step 3 : Iterate the Logistic map given in the equation 1 and store the values in arraylist.

Step 4: Stop the iteration once the numbers generated is equal to input length n which is the length of the sequence.

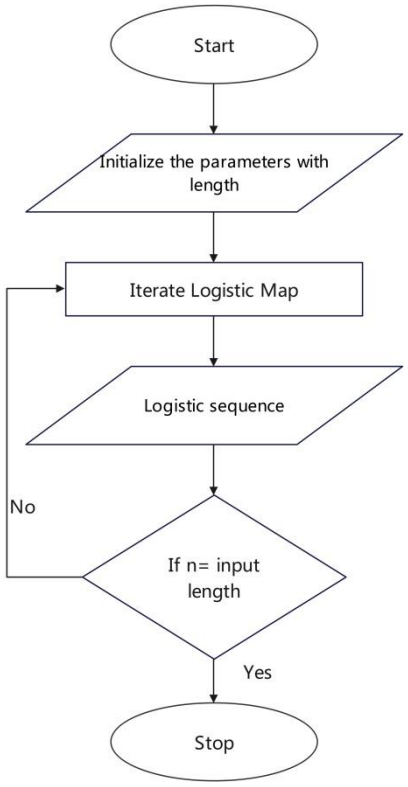

Fig. 2. Flow chart of Logistic map sequence generation

- ***Henon Map :***

The chaotic sequence of Henon map is generated by the using the equation 2 and 3. The Henon map is dependent on two parameters 'a' and 'b'. The α = 1.4 and b = 0.3 are the values of Henon map. The n and x_0 , is represented in terms of length of the sequence. The initial condition which is given to the input to the map. The sequence generator and a sequence of real numbers are the output as shown in the Figure 3.

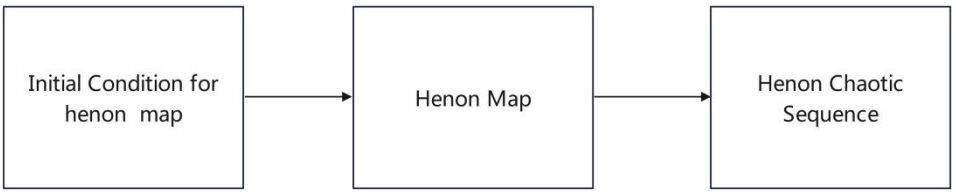

Fig. 3. Henon sequence generator

$$x_{n+1} = 1 - \alpha n^2 + yn \tag{2}$$

$$y_{n+1} = bx_n \tag{3}$$

Algorithm are given below,
Step 1 : Input the length and initial condition to generate the Henon sequence.
Step 2 : Select parameter value a as 1.4 and b as 0.3.
Step 3 : Iterate the Henon map given in the equation 2 and 3 and store the values in arraylist.
Step 4 : Stop the iteration once the numbers generated is equal to input length n which is the length of the sequence.

- ***Chebysev Map :***

The Chebysev map chaotic sequence is generated using the equation 4. For Chebysev map, the parameters λ is chosen as 4. The n and x_0 is the initial condition which is given as input and it represents the number of elements in the sequence[12]. Chebysev sequence generator is in Figure 5.

$$x_{n+1} = cos(\lambda cos^{-1} x_n) \tag{4}$$

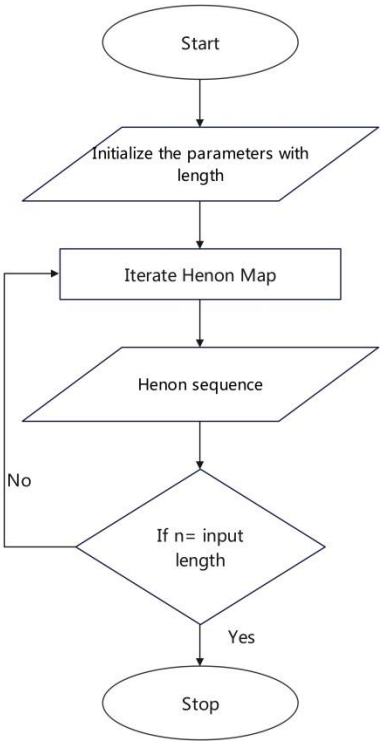

Fig. 4. Flow chart of Henon map sequence generation

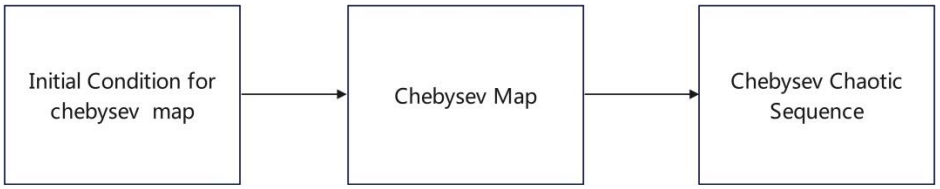

Fig. 5. Chebysev sequence generator

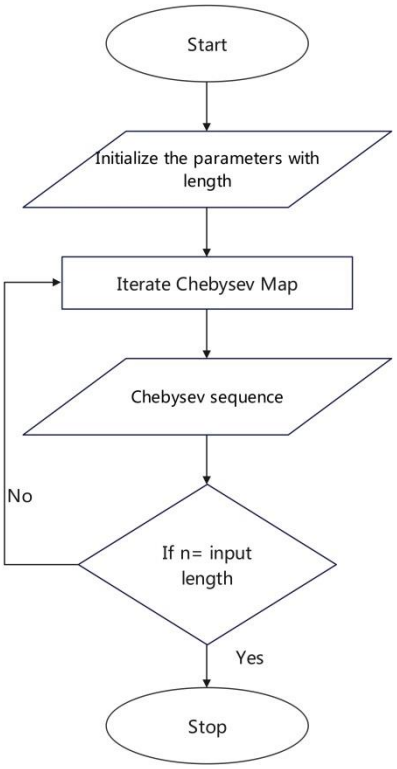

Fig. 6. Flow chart of Chebysev map sequence generation

Algorithm are given below,
Step 1 : Input the length and initial condition to generate the Chebysev sequence.
Step 2 : Select parameter value as 4.
Step 3 : Iterate the Chebysev map given in the equation 4 and store the values in arraylist.
Step 4 : Stop the iteration once the numbers generated is equal to input length n which is the length of the sequence.

3.2. Unpredictable Sequence Generation Based on Combination of Maps :

The multidimensional chaotic sequences namely Logistic, Henon and Chebysev are combined to get a single sequence. Combining is done by performing XOR operation of the three sequences as in Figure 7.

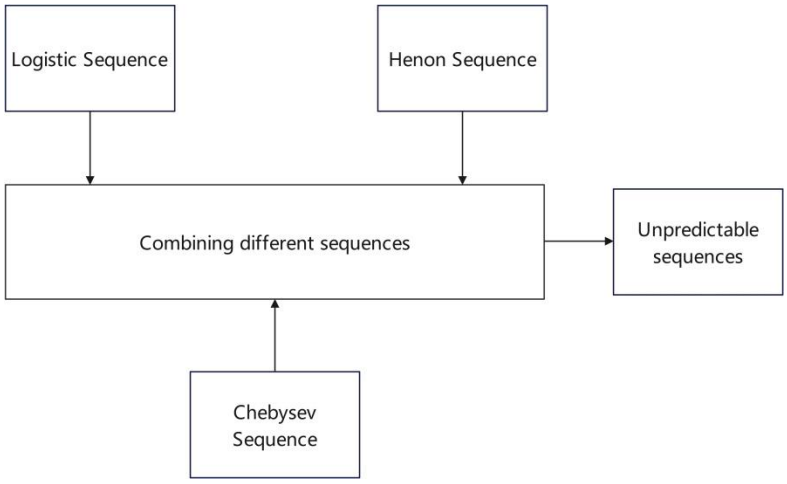

Fig. 7. Unpredictable sequence generation

The Unpredictable sequence is represented as K. The ith number in the unpredictable sequence is calculated using the equation 5.

$$K_i = LK_i \oplus HK_i \oplus CK_i \tag{5}$$

Where i varies from 1 to n and n is the length of the sequence. The ith number in the unpredictable sequence is K_i which is got by doing XOR operation of ith number of multidimensional chaotic sequences. LK is Logistic sequence, HK is Henon sequence, CK is Chebysev sequence.

Algorithm are given below,
Step 1: Input the length of the sequence and initial conditions for three chaotic maps.
Step 2 : Generate three sequences of specified input length.
Step 3 : Combine the three sequences using the equation 5.
Step 4 : Stop when the length of sequence equals the input length.

3.3. Process of Encryption and Decryption :

Here the encryption and decryption process using unpredictable chaotic sequence is explained. Encryption and Decryption process using unpredictable chaotic sequence is generated by appling XOR operation on multidimensional maps then two unpredictable chaotic sequences are generated to form an ordered sequence by sorting it in ascending order. In the quantification unit and using the position of number in the sorted sequence key stream(K1 and K2) is generated and is used for row (K1) and column (K2) crossover. A scrambled encrypted image is obtained after performing crossover operation then to get encrypted image an intermediate image is XOR'ed with third chaotic sequence.

In order to perform decryption, an cipher image is first XOR'ed with the sequence S3.After performing XOR column crossover is performed using keystream K2.Finally row crossover is performed using keystream K1 to get the original image.

Encryption and decryption process using unpredictable chaotic sequence. Encryption is achieved using chaotic map and crossover genetic operator. Steps involved are,

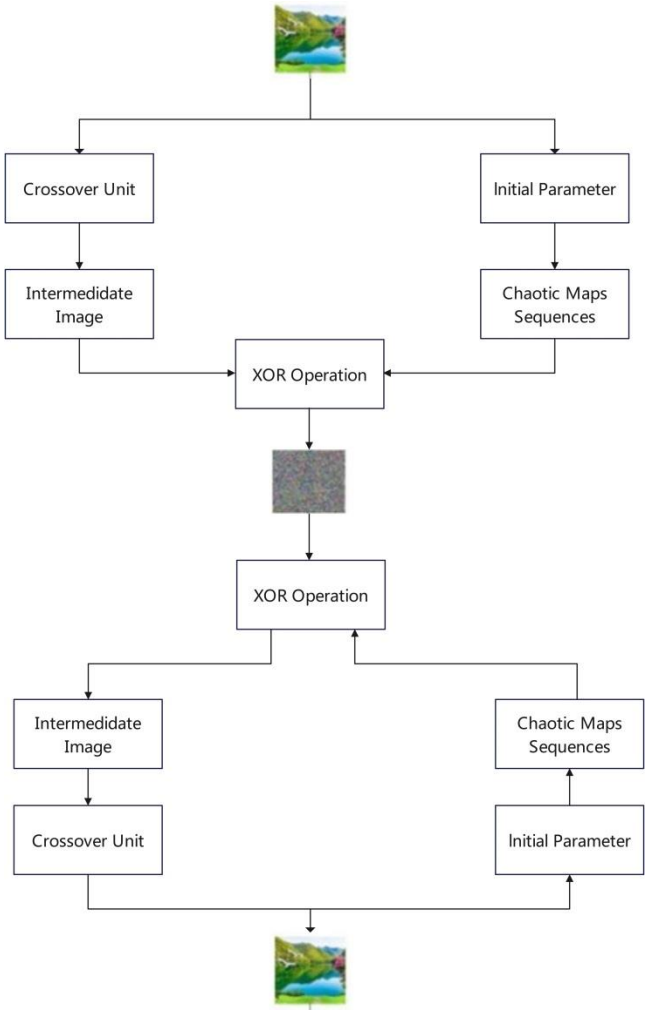

Fig. 8. Process of Encryption and Decryption

- ***Encryption :***

Step 1 : Use the read method to read the image to be encrypted.
Step 2 : Input the chaotic map to be used and the initial condition for the maps.
Step 3 : Generater the sequence from the three chaotic maps.
Step 4 : Apply quantification to the sequences to get key streams(K1 and K2). In quantification unit the three chaotic sequences are taken and to form an ordered sequence in an ascending order.
Step 5 : Using the key stream K1 row-wise crossover is perform on input image.Crossover points are computed by using the equation 5.
Step 6 : Using the key stream K2 column-wise crossover is perform. Crossover points are computed by using the equation 5.
Step 7 : Each number in chaotic sequence is selected and XOR'ed with each pixel read from the intermediate image to produce the cipher image.

- ***Decryption :***

In order to perform decryption, the cipher image is first XOR'ed with the sequence. After performing XOR column crossover is performed using key stream K2. Finally row crossover is performed using key stream K1 to get the decrypted image.

4. Results and Discussion

4.1 Result for three chaotic maps :

- ***Logistic Map* :**

Logistic sequence generated with initial value 0.4999 and 0.4899 is shown in Table 1. From both the sequence it is notice that with a slight variation in initial value has a significant impact on the output produced.

Table 1. Logistic sequence with varied initial value

Initial Value 0.4899	Initial Value 0.4999
0.9956	0.99997
0.00173	1.00154
0.00691	4.00569
0.02746	0.00160
0.10682	0.00639

- ***Henon Map :***

Henon sequence is generated with initial value 0.21 and 0.194 and parameters a, b are selected as 1.4 and 0.3 respectively. The x values generated are considered in two dimensional Henon map and are shown in Table 2. With the change in initial value, the sequence generated is completely different.

Table 2. Henon sequence with varied initial value

Initial Value 0.194	Initial Value 0.21
1.15730	1.13226
-0.81691	-0.73181
0.41291	0.58989
0.51623	0.29328
0.75077	1.05654

- ***Chebysev Map :***

Chebysev sequence is generated with initial value 0.4999 and 0.5060 and parameters value 4. The values generated are shown in Table 3.

Table 3. Chebysev sequence with varied initial value

Initial Value 0.4999	Initial Value 0.5060
-0.49959	0.86780
-0.49839	0.96640
-0.49358	0.99156
-0.47418	0.99789
-0.39435	0.99947

4.2 Unpredictable Sequence Generation Based on Combination of Maps :

The multidimensional chaotic sequences namely Logistic, Henon and Chebysev maps are generated with initial values 0.4999, 0.21, 0.21, 0.4999, 0.4999 and 0.4999 respectively. The three sequences generated are combined to get a single sequence. Combining is done by performing XOR operation of the three sequences. The sequence obtained is shown in Table 4.

Table 4. Unpredictable Sequence

Unpredictable Sequence
-0.14337
0.00326
-0.00705
-0.02491
-0.01482

4.3 Unpredictable Encryption and Decryption Process :

The results of Encryption and decryption process using unpredictable chaotic sequence are discussed in the below section.

- ***Encryption Process :***

In this module, unpredictable sequence is generated with initial values 0.4999, 0.21, 0.21, 0.4999, 0.4999 and 0.4999 for Logistic, Henon and Chebysev maps respectively. Once the sequence is generated row and column crossover is applied on the input image as shown in Figure 9 (Original Input Image) to get the scrambled encrypted image (Scrambled Encrypted Image). To obtain encrypted image, a intermediate image is XOR-ed with the third sequence as shown in the Figure 9 (Cipher Image).

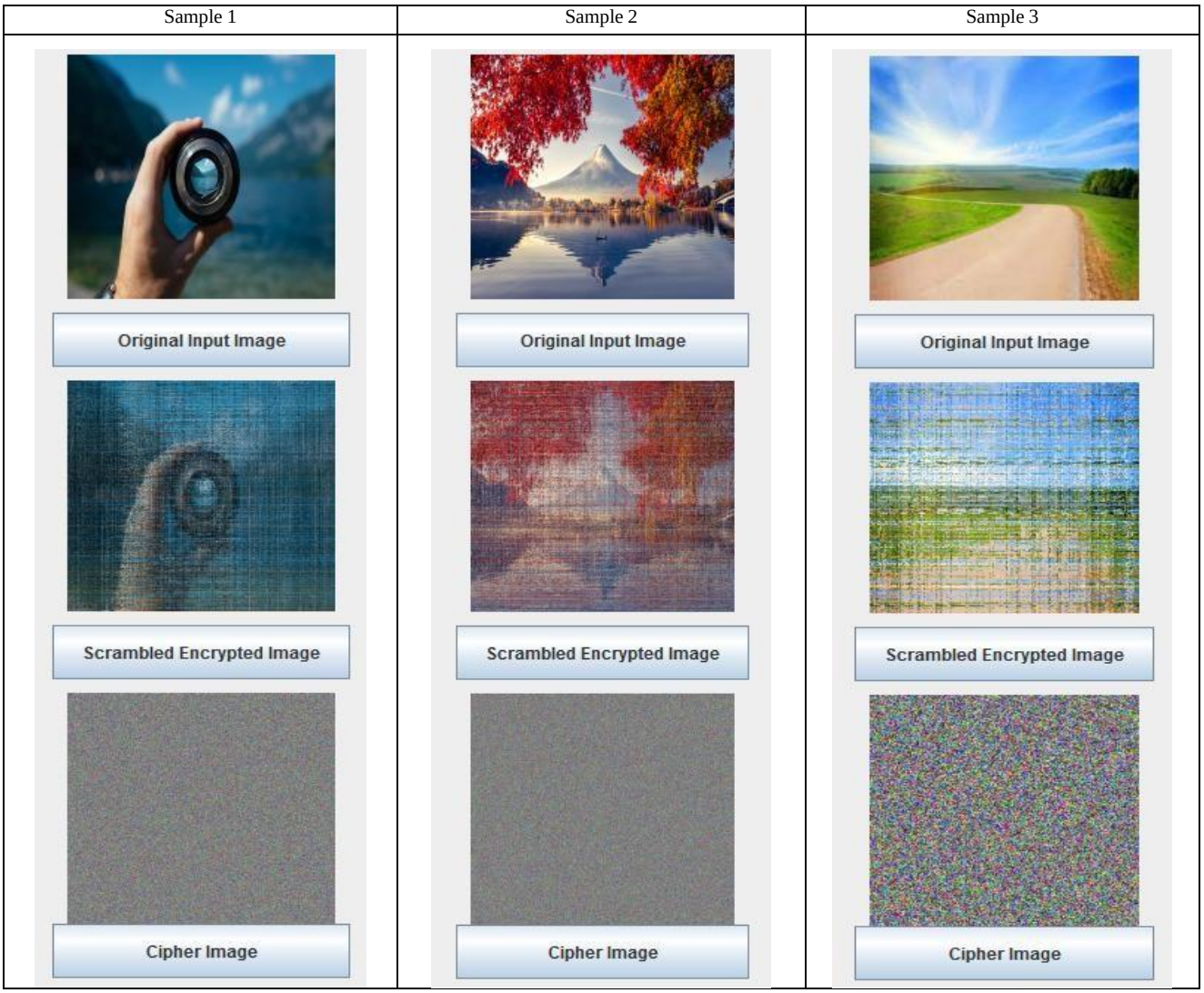

Fig. 9. Encryption Process Using Unpredictable Sequence

- ***Decryption Process :***

In this section, In order to perform decryption process, an encrypted image is considered as shown in the Figure 10 (Cipher Image) to get scrambled decrypted image the unpredictable sequence is first XOR-ed as shown in the Figure 10 (Scrambled Decrypted Image). After performing XOR, column crossover and row crossover is performed to get the decrypted image in the Figure 10 (Original Output Image).

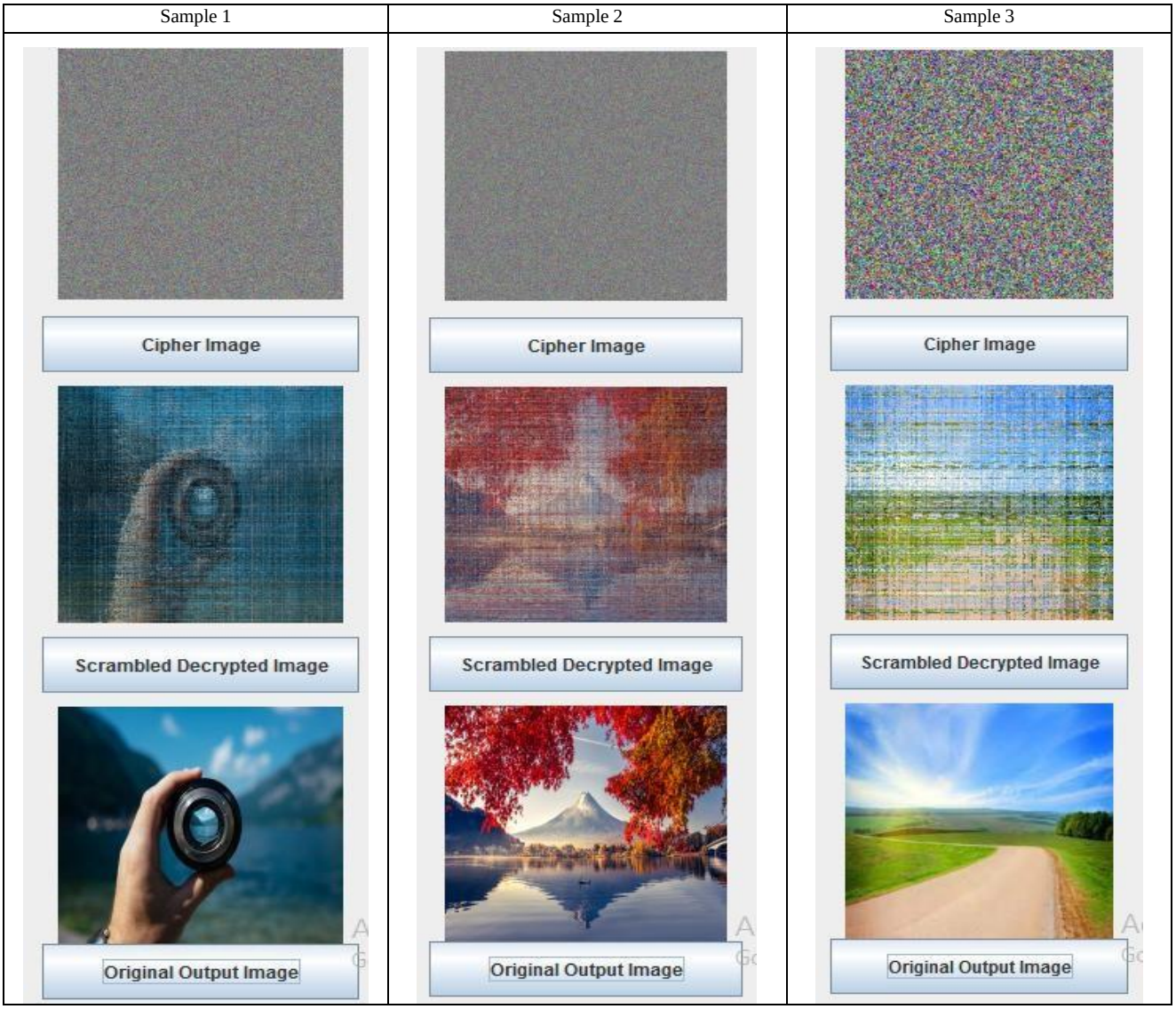

Fig. 10. Decryption process Using Unpredictable Sequence

4.4 Analysis :

The performance analysis of the obtained result is done by using Histogram and Correlation Coefficient.

1. Histogram Analysis :

A histogram of a pixel intensity values is referred to an image. The number of pixels in an image is shown in the histogram graph at different intensity value of a particular image[14].

The histogram explains how the pixel elements are distributed in an image by graphically and also measure the amount of colour intensity of each pixel element.The colour component of image (red, green and blue) are considered individually for histogram analysis. The original image histogram refers to an unequal distribution of the colour components. However, the encrypted image's histogram refers that colour components are uniform. Each pixel appears exactly same in the encrypted image of sample 1, 2 and 3 is shown in the Figure 11, 12 and 13 respectively.

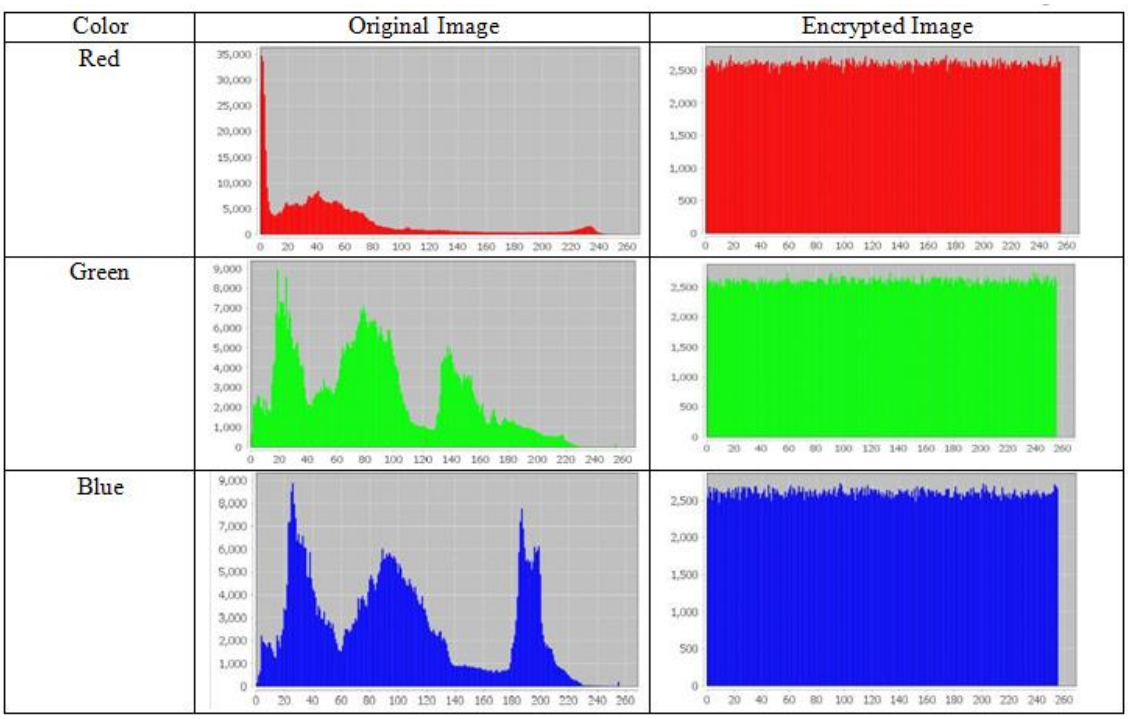

Fig. 11. Histogram of an original and encrypted image of sample 1

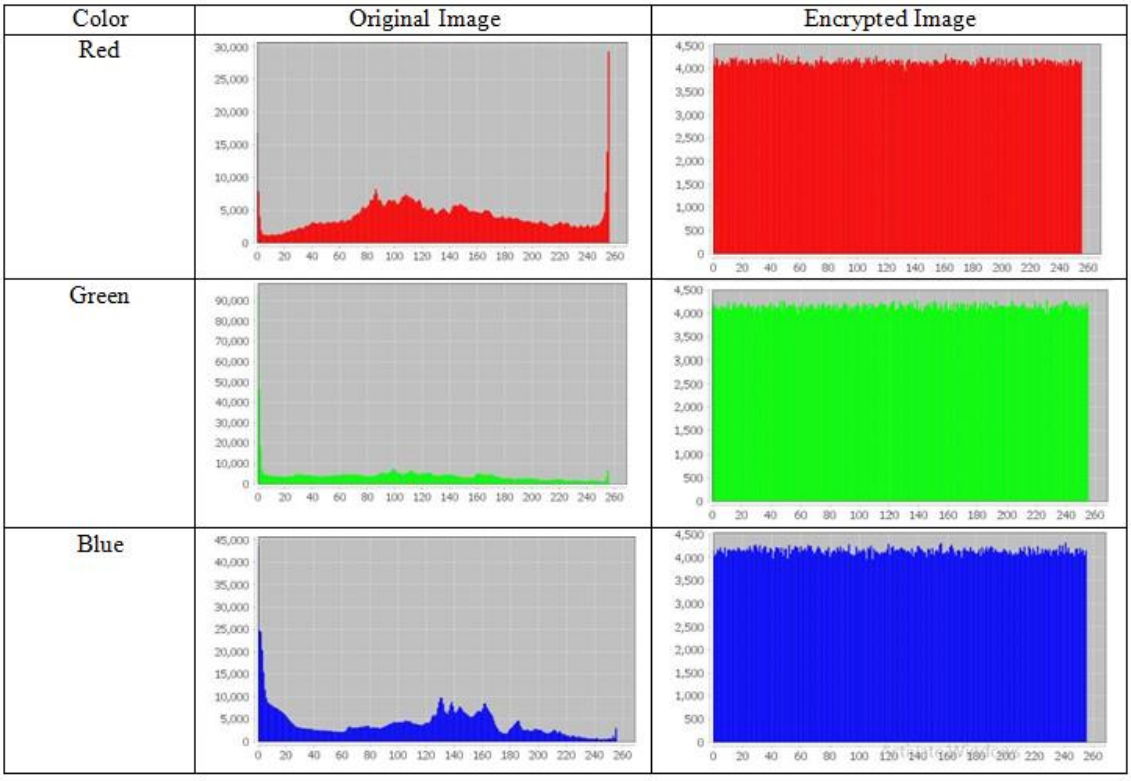

Fig. 12. Histogram of an original and encrypted image of sample 2

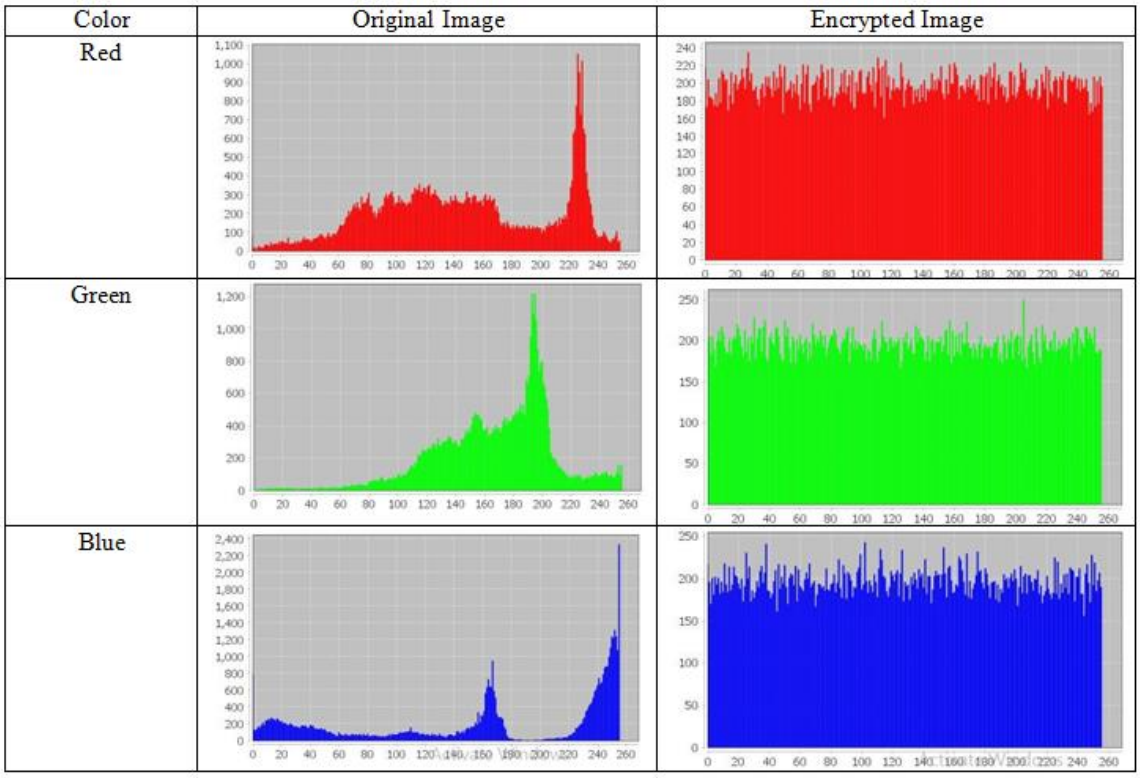

Fig. 13. Histogram of an original and encrypted image of sample 3

2. Correlation Coefficient Analysis :

It calculates the Correlation between adjacent pixels in original image and their encrypted image. Each pixel in the original image is typically highly correlated with its adjacent pixels. Correlation values are calculated using the equation 6 for red component. The values obtained along horizontal and vertical directions are shown in the Table 5.

$$Correlation\ Coefficient = \frac{Cov(x,y)}{\sqrt{D(x)} * \sqrt{D(y)}} \tag{6}$$

$$Cov(x,y) = \frac{1}{N}\sum\big(x_i - E(x)\big)\big(y_i - E(y)\big) \tag{7}$$

$$E(x) = \frac{1}{N}\sum x_i \tag{8}$$

$$E(y) = \frac{1}{N}\sum y_i \tag{9}$$

$$D(x) = \frac{1}{N}\sum\big(x_i - E(x)\big)^2 \tag{10}$$

$$D(y) = \frac{1}{N}\sum\big(y_i - E(y)\big)^2 \tag{11}$$

Correlation coefficients depends on covariance of adjacent pixels which is represented by the equation 7, mathematical expectation of intensity values of the pixels represented by the equation 8 and 9 and variance represented by equation 10 and 11. In the equations, X and Y referred as the intensity values of colour component of red, green and blue of adjacent pixels.

The correlation coefficient of plain image, cipher image and decrypted image in both horizontal and vertical direction of a sample 1 image are shown in the table 5.

Table 5. Correlation Coefficient of Sample 1

Direction	Plain Image	Cipher Image	Decrypted Image
Horizontal	0.99291	0.02090	0.99148
Vertical	0.99259	0.00359	0.99495

The correlation coefficient of plain image, cipher image and decrypted image in both horizontal and vertical direction of a sample 2 image are shown in the table 6.

Table 6.Correlation Coefficient of Sample 2

Direction	Plain Image	Cipher Image	Decrypted Image
Horizontal	0.91582	0.00133	0.89144
Vertical	0.90823	0.00155	0.90454

The correlation coefficient of plain image, cipher image and decrypted image in both horizontal and vertical direction of a sample 3 image are shown in the table 7.

Table 7. Correlation Coefficient of Sample 3

Direction	Plain Image	Cipher Image	Decrypted Image
Horizontal	0.98830	0.01788	0.96754
Vertical	0.97227	0.01830	0.97999

5. Conclusions

Encryption and Decryption of an imagery is an important aspect maintaining and providing security to the images over network communication technology. The conversion of original image into the cipher image is the technique of image encryption which is hard to understand. An image encryption technique is based on multidimensional chaotic maps and genetic operator. The Pseudorandom key sequence is generated using chaotic maps which help in encrypt the images. Decrypting of an image involves the above-mentioned procedure, but all the steps are carried out in reverse way. The histogram analysis is used to determine how the pixel values of the input image and the final cipher image differ. The correlation coefficient is used to determine the correlation between adjacent pixels in plain image and their cipher image in both horizontal and vertical direction. Both the histogram and correlation coefficient analysis is done for various samples and the results are found to be satisfactory.

References

[1] Muhammad Usama, Muhammad Khurram Khan, Khaled Alghathbar and Changhoon Lee, "Chaos-based secure satellite imagery cryptosystem", In Journal of Computers and Mathematics With Applications, July 2010.

[2] El-Sayed M. El-Alfy, Khaled A. Al-Utaibi, "An Encryption Scheme for Color Images Based on Chaotic Maps and Genetic Operators", In Proceeding Seventh International Conference on Networking and Services, 2011.

[3] Qiu Zhang, "Study on Image Encryption Algorithm Based on Chaotic Theory", In Proceeding of International Conference on Information Science and Cloud Computing Companion, 2013.

[4] Jansher Khan, Jawad Ahmad, Seong Oun Hwang, "An Efficient Image Encryption Scheme Based on : Henon Map, Skew Tent Map and S-Box", In Proceeding of Sixth International Conference on Modeling, Simulation and Applied Optimization (ICMSAO), 2015.

[5] Mohammad Javidi, Roghiyeh Hosseinpourfard, "Chaos Genetic Algorithm Instead Genetic Algorithm", In Proceeding the International Arab Journal of Information Technology, March 2015.

[6] Govind Chandra, Naveen Chandra, Swati Verma, "A Review on Multiple Chaotic Maps for Image Encryption with Cryptographic Technique", In Proceeding of International Journal of Computer Application, July 2015.

[7] Mohammed A. Alzain, Osama S. Faragallah, "Efficient Chaotic Tent Map-based Image Cryptosystem". In Proceeding of Internaional Journal of Computer Application, 2017.

[8] Marwa Tarek Elkandoz, "Logistic Sine Map Based Image Encryption". In Proceeding of Signal Processing : Algorithms, Architectures, Arrangements and Application (SPA), 2019.

[9] Kanika Suneja, Shelza Dua, Mohit Dua, "A Review of Chaos based Image Encryption", In Proceedings of the Third International Conference on Computing Methodologies and Commuication (ICCMC), 2019.

[10] B. Sai Kumar, L. Vikhyath, R. Geetha Krishna Pavansai, "Image Encryption Using Chaos Maps", In Proceeding of International Journal of Scientific & Engineering Research, 2021.

[11] Sudeep Nooly B, Ravindra S, "A Survey on Multidimensional Chaotic Maps and Genetic Operator", In Proceeding of International Journal for Reserch in Applied Science and Engineering Technology, April 2022.

[12] Fei Qi, Sijiang Huang, Tong Li, Haotian Yang and Xuejing Kang," 2D Henon-Chebyshev Chaotic Map for Image Encryption", In the Proceeding of 21st International Conference on High Performance Computing and Communications, 2019.

[13] M. Sabery. K, M.Yaghoobi, "A New Apporach for Image Encryption using Chaotic Logistic Map", In Proceeding of International Conference on Advance Computer Theory and Engineering", 2008.

[14] Diya Achu Pradeep, A Harsha, Jaison Jacob, "Image Encryption Using Chaotic Map And Related Analysis", In Proceeding of International Conference on Advances in Computing and Communication (ICACC), 2021.

[15] Yanru Zhong, Huayi Liu, Rushi Lan, Ting Wang, Xiyan Sun, Xiaonan Luo, " 2D Chebyshev-Sine Map for Image Encryption", In Proceeding of Seventh International Conference on Digital Home (ICDH)", 2018.

Authors' Profiles

Sudeep Nooly B is born in Shivamogga, Karanataka, India on 13th JAN 1997 and he received his Bachelor of Engineering Degree and Master's of Technology Degree in the Department of Computer Science and Engineering from Visvesvaraya Technological University, Belgaum, Karnataka, India in 2019 and 2022 respectively.

He has 2.8 years of experience as an Cyber Security Engineer in the Private Organization, Bengaluru, and has published 1 research paper in International Journals. His areas of interest include, Cyber Security and Computer Networks.

Ravindra. S. received his B.E., in Electrical and Electronics Engineering., M.Tech., in Networking and Internet Engineering, and Ph.D in Faculty of Computer and Information Sciences from Visvesvaraya Technological University, Belgaum, Karnataka, India in 2006, 2008 and 2018 respectively.

At present he is working as Associate Professor, in Computer Science and Engineering department of JNN College of Engineering (affiliated to Visvesvaraya Technological University), Shivamogga, Karnataka, India. His areas of Interests include, Signal Processing for Wireless Communication, Data Science Etc.

How to cite this paper: Sudeep Nooly B, Ravindra S, "Design and Development of Multidimensional Chaotic Maps with Genetic Operator", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.9, No.3, pp. 12-25, 2023. DOI: 10.5815/ijmsc.2023.03.02