iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.42003

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

A Survey on Multidimensional Chaotic Maps and Genetic Operator

Sudeep Nooly B[1], Ravindra S[2]
[1, 2]*M.Tech Scholar, Dept.of CSE, JNN College of Engineering, Shivamogga 577201*

Abstract: ***The image encryption and decryption is the one of the ways to providing security to digital image. Encryption technique is a process of converting plain image into a cipher image. Decryption technique is a process of converting cipher image into a plain image. In this paper a survey of several multidimensional chaotic maps along with genetic operator were used in order to secure an image are discussed and along with the advantages and disadvantages of those maps.***
Keywords: ***Chaotic system, Chaotic maps, 1-dimensional logistic map,2-dimensional henon map,3-dimensional chebyshev map.***

I. INTRODUCTION

A massive amount of data that are shared over the internet is images due to rapid evolution of internet technologies. While accessing information on internet there is risk that the valuable information can be stolen, changed or misused. Earlier, information was printed on paper and locked in a file cabinet so information was secure. But with network and internet the electronically recorded information such as text and images can be stolen by intruders from any part of the world. Therefore the security of these images are very important. To overcome with these problems a various methodologies of cryptographic algorithms were proposed .Cryptography is one of the major area in-order to secure the information/data from the cyber attacks.Some of the conventional encryption and decryption algorithms such as RSA, AES, DES etc. are not more efficient algorithms in order to secure the images each and every algorithm has it own limitations with respect to securing an image. RSA Algorithm has its own limitation, it can be very slow in case of a large data needs to be encrypted by the same computer. It requires a third party to verify the reliability of public keys. Data transferred through RSA algorithm could be compromised through middlemen attack. It can be also broken using short message attack and cycling attack. The main limitation of DES and AES Algorithms are DES Algorithm is broken by brute-force attack and AES Algorithm uses too simple algebraic structure which could also be broken by brute-force method.

In current era, chaotic systems are analyzed to be extremely powerful for real time implementation in secure communications. The security of chaotic systems is due to its inherent properties like sensitivity to control parameters, initial conditions, non-periodicity and deterministic pseudo-random behavior.

II. CHAOTIC SYSTEM

It is a dynamical system showing sensitivity to initial conditions such as weather forecasting and stock market. Such systems containing some uncertainty in the beginning can produce rapid changes in the prediction of the system's behavior in future. Accurate long-term behavior prediction of such systems can only be done if the initial conditions are known in their entirety and with good level of accuracy. It is impossible without knowing initial behavior to predict the future behavior of chaotic system.

A dynamical system is said to be a chaotic system if it satisfies the following these characteristics :

1) It must be sensitive to initial conditions.
2) It must be topologically transitive.
3) Its periodic orbits must be dense.

A. Sensitivity to Initial Conditions

Sensitivity to initial conditions means a small change at one place in a nonlinear system can result in large differences to a later state. The long term behavior of dynamical systems is not possible to be predicted without knowing the initial conditions. The chaotic output produced by the systems can be changed over time even by modifying even a single bit in the initial conditions.

B. Topological Transitivity

Topological transitivity means that the system will evolve over time so that any given region or open set of its phase space will eventually overlap with any other given region. i.e., the end behavior of the system is dependent on where the system is started and no matter how close together two points are, at any time they can move in completely different directions. Sensitivity and topological mixing are closely related and for chaotic systems both should be satisfied.

C. Density of Periodic Orbits

The points in the chaotic system make up orbits. The periodic orbits of a chaotic system are surrounded by points that are very dense around the orbits. An attractor represents the behavior of chaotic systems. Every point in the attractor for the chaotic system is arbitrarily close to some point on a periodic orbit. When a point is picked in the attractor and a distance of greater than zero is travelled a periodic orbit is reached.

III.CHAOTIC MAPS

A chaotic map is evolution function that exhibits characteristic such as sensitivity to initial conditions, topological transitivity and contains dense periodic orbits. Maps are controlled by parameters. Parameters can be either discrete-time or continuous-time parameters. Iterated maps are usually controlled by discrete time parameters.

The main advantage using chaos maps is the generation of chaotic signals which looks like noise for unauthorized users. Chaotic signals can be generated by iterating chaotic maps and the cost of generation is low so it is suitable for using it as stream ciphers. Chaotic maps are used to generate pseudorandom numbers which can be used as a key to encrypt plaintext element by element.

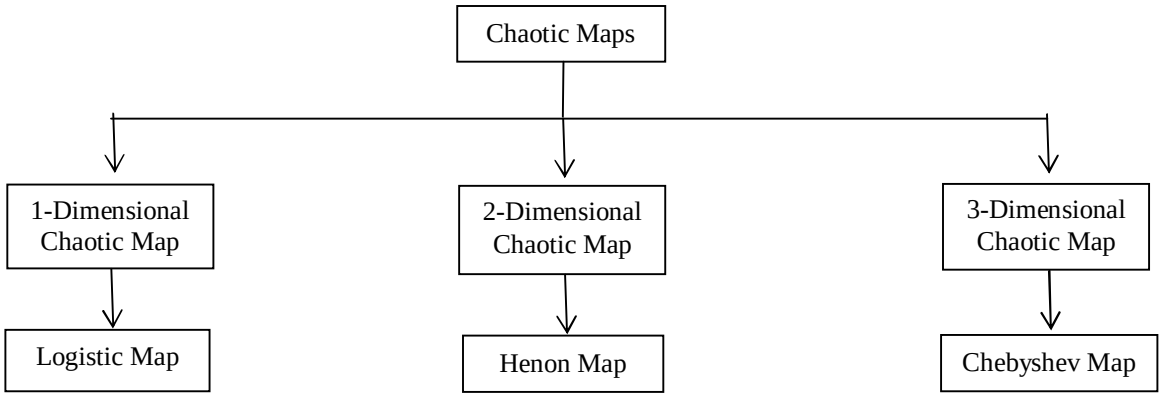


Figure 1. Classification of Multidimensional Chaotic Maps.

IV.1 - DIMENSIONAL CHAOTIC MAP

There are various 1-dimensional chaotic maps such as Logistic map, Tent map, Skew map etc. and it has variable and limited parameter its chaotic orbits and design are very simple. Here we are mainly considering the 1-dimensional Logistic map.

A. Logistic Map (LM)

The logistic map is one of the widely used and simplest chaotic maps. It was introduced in 1845 by Verhulst as a model to calculate population growth of a species over a period of time, it is expressed as iterative equation. Initially developed to calculate population but because of its chaotic nature it finds its application in areas like cryptography.

$$x_{n+1} = \quad r\, x_n(1 - x_n)$$

Where the parameter r belongs to the interval [0,4] and r is chosen in the range between (3.57,4). The length of the sequence is represented by n and x_0 is the initial condition given as input to the map. The output is sequence of real number.

V. 2 - DIMENSIONAL CHAOTIC MAP

There are various 2-dimensional chaotic maps such as Henon map, Baker map, ACM etc.

A. Henon Map (HM)

Arnold Cat Map is the one of the 2 dimensional chaotic map it can be applied only to the square matrix M*M and ideal encryption strategy should not have periodicity. Due to this limitation henon map came into picture to provide more security to the digital image. The Henon map is one of the 2-dimensional chaotic map that perform pseudo random sequence. The Henon map is a two dimensional chaotic map. It is an iterated function with discrete-time parameters. The map was introduced by Michel Henon. It is one of the most studied two dimensional maps that exhibit chaotic behavior. The Henon map takes a point (x_n, y_n) and maps it to a new point.The map is depends on two parameters a and b which for the henon map takes the values range between [0.3,1.4]. The length of the sequence is represented by n and x0 is the initial condition given as input to the map.The output is the sequence of real numbers.

$$x_{n+1} = 1 - ax_n^2 + y_n$$

$$y_{n+1} = bx_n$$

The advantages of using henon map is that after various time period the original image and encrypted image will be different.Hence this map overcomes the problem of 2-dimensional Arnold Cat Map.

VI.3 - DIMENSIONAL CHAOTIC MAP

There are various 3-dimensional chaotic maps such as Chebyshev,3D ACM,3D cat map etc.

A. Chebyshev map

The chebyshev map is one of the 3-dimensional chaotic map. Chebysev map is a dynamical system that exhibits chaotic behaviour.

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

The map depends on parameter λ which for chebyshev map is chosen as 4 .The number of elements in the sequence is represented by n and x0 is the initial condition gives as input to the map.

VII. ENCRYPTION AND DECRYPTION TECHNIQUE

Figure 2 shows the technique of image encryption and decryption process, Firstly, Initial condition is considered for chaotic map to generate the chaotic sequence. Crossover is performed on original image to get an intermediate image. The intermediate image is XOR-ed with key stream of chaotic sequence to get the encrypted image. While the decryption process is the reverse of encryption, the same initial condition is used to generate key stream and XOR-ed with the encrypted image to get the intermediate image. Crossover is performed on intermediate image to get the decrypted image so called original image.

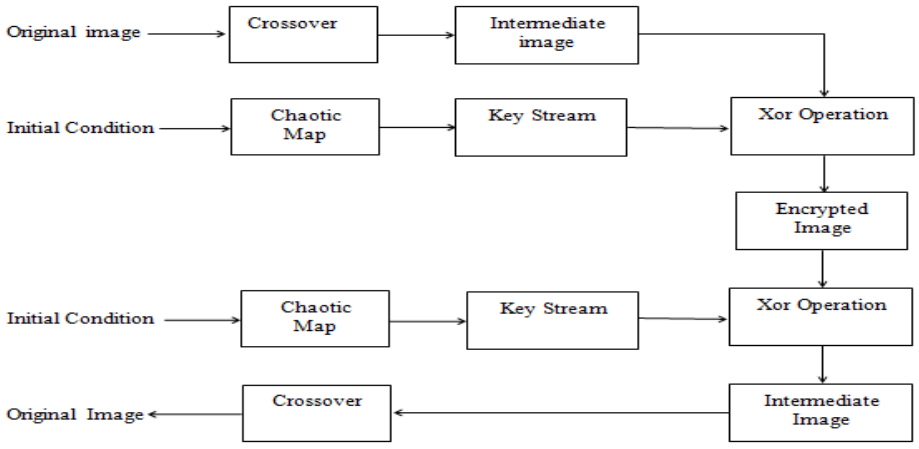


Figure 2 . Image Encryption and Decryption Technique.

Table 1.Comparison of chaotic Maps

Chaotic Maps	Properties			Advantage	Disadvantage
	Correlation coefficient	Key Sensitivity	Key Space		
1-Dimensional	-	-	-	Simple in Structure,Low Cost	It uses less parameters and short range of control parameter
1-Dimensional Logistic Map	High	High	High	Simple and its Implementation is easier.	Chaotic range is less,weak security.
2-Dimensional	-	-	-	Larger key space.	Less Periodic Window.
2-Dimensional Henon Map	High	High	2^128	Improve the security.	Less key space and key sensitivity.
3-Dimensional Chebyshev Map	High	High	2^167	-	-

Table 2. Review of Chaotic Maps

Year	Authors	Maps	Contribution	Limitation
2010	Muhammad Usama, Muhammad Khurram Khan, Khaled Alghathbar and Changhoon Lee.	Chebyshev,Logistic,Cubic,Sine,Henon,Tent Map	Combination of multiple chaotic maps were used	Using single map causes Low level of security
2011	El-Sayed M. El-Alfy, Khaled A. Al-Utaibi.	Logistic Map	Using genetic operator will enhance extra security	Key space is less
2013	Qiu Zhang.	Logistic Map	Drastic change in generation of sequences by changing Initial condition and parameter value	Range is very less
2015	Jansher Khan,Jawad Ahmad,Seong Oun Hwang.	Henon Map and Tent Map	Combining the both will enhance more security	Using the map separately causes Low level of security
2015	Mohammad Javidi, Roghiyeh Hosseinpourfard.	Logistic Map and Tent Map	Genetic operator is used for higher security	Key space and Range is very less
2015	Govind Chandra, Naveen Chandra, Swati Verma.	Multi dimensional Maps	Has lower mathematical complexity and better security	Low level of security without combining them
2017	Mohammed A. AlZain,Osama S. Faragallah.	Tent Map	Core of schema is used to achieve the security requirements	Key space is less
2019	Marwa Tarek Elkandoz.	Logistic Map and Sine Map	Combining both will have high level of security.	Key space and its range are less.
2019	Kanika Suneja, Shelza Dua, Mohit Dua.	Logistic,Henon, Chebyshev,Cubic, Sine,Tent,Cat,Baker,ACM,	Combining multi dimensional chaotic maps will have more security.	Iteration time is very limited.
2021	B. Sai Kumar,L. Vikhyath,R. Geetha Krishna Pavansai.	Henon,Logistic, ACM	Henon and Logistic Maps take less time to compute.	ACM take More time to compute.

VIII. CONCULSION

Securing the image is very critical while exchanging the information over a communication channel.To transfer a data securely a few techniques can be used and one among them is encryption and decryption using multidimensional chaotic maps.This paper is discussed about the n dimensional chaotic maps and the benefits of those maps.

REFERENCES

Bibliography

[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.

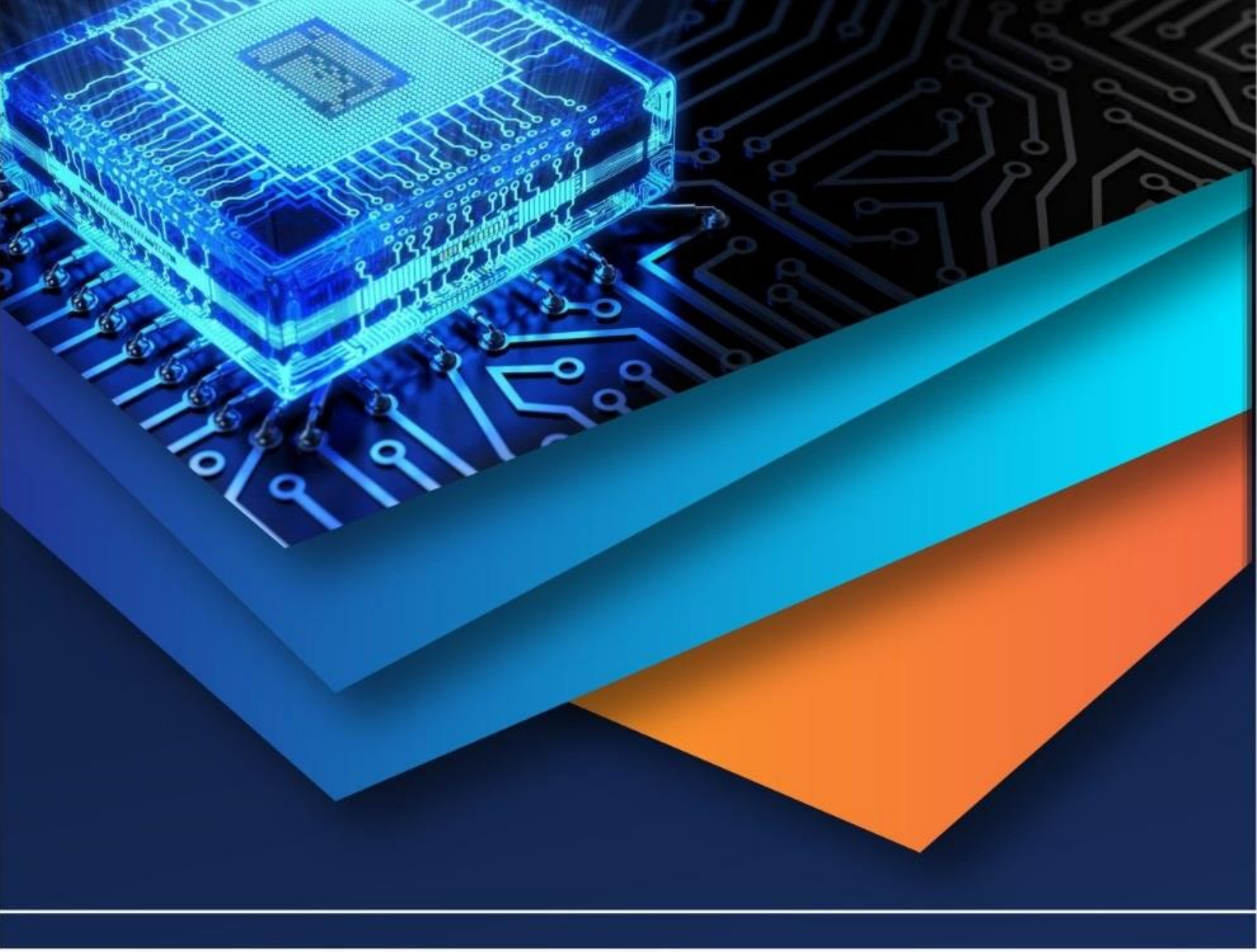
[6] Govind Chandra, Naveen Chandra, Swati Verma,"A Review on Multiple Chaotic Maps for Image Encryption with Cryptographic Technique", In Proceeding of International Journal of Computer Applications, July 2015.

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

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



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY