iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** III **Month of publication:** March 2022

DOI: https://doi.org/10.22214/ijraset.2022.40834

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 III Mar 2022- Available at www.ijraset.com

A Study of Colour Image Encryption with Chaos Logistic Map and DNA Encoding Techniques

Anmol Kumar Chaukade[1], P. Murali[2]
[1, 2]*Department of Computer Science and Engineering, SRMIST*

Abstract: ***The encryption of image has really become an important task in today's world as there is a continuous advancement of technology day-by-day. There is a need to protect the images like texts, encrypt them and then transfer them through a channel. As the fast-growing era is more inclined towards the usage of images during conversations, cryptography becomes an essential tool to cipher the information before transferring it over a medium. The transmission channel could be insecure therefore data that is getting transferred must be secured enough so that only the genuine receiver should decode the original meaning of the image. Moreover, the general compatibility of an image should be done before encrypting it and that image could be pre-processed using existing image processing techniques. However, the proposed system is a study of how cryptography tends to be an efficient tool for security and the proposed system is implementation of DNA sequence encoding which provides an additional layer to it. It is divided into four modules. The first module consists of generating a secret key with the help of chaotic logistic map and check the behaviour of the chaotic system. Next phase is to apply the DNA concepts thereby making the quality of image more complex and after that perform the overall encryption with the help of confusion and diffusion technique to get the result as encrypted image. The last phase would be to decode the image and get the original plain image. The performance metrics and evaluated and analysed with the existing methodologies as a comparison. Moreover, a good encrypted image should be able to deal with the different types of attacks that are happening while transmission.***
Keywords: Chaos logistic map, DNA, encryption, image processing, confusion, cryptography

I. INTRODUCTION

Cryptography, a branch of computer science that deals with the techniques to provide security to a system, a data or a mechanism in order to decrease the rate of attacks and cybercrimes. We have several algorithms to secure the data in the form of text, but the digital image relies on security too. The extracting of useful information from the digital image ad processing it for analysing patterns and keen observation is called as digital image processing. Now as the complete word comprises of three different words that are digital, image and processing, we combine the functioning of all three to get into the world of data science and get a term called as image processing.

There is a saying that "A picture is worth thousand words", by applying this principle we can say that a picture could be analysed with the key concepts of what it's all about, the kind of information it gives, the overall conclusion it draws and what message it showcases. We go for this concept of digital image processing only for two specific reasons that are the improvement of pictured information that could be interpreted by humans easily and the next is processing of the overall data which the image provides for storage, transmission and utilizing the same as machine inputs. Let us move towards the main concept of cryptographic techniques. The basic meaning of cryptography is studying of secured information that could be applicable on both sides that is the sender and the receiver that could be derived from any mathematical concept or a probabilistic set of rules. Encryption is one such technique to protect the information which can be used on images as a useful source to protect it from unauthorized users. The world is getting into a digitalization era and people are rather preferring utilizing online resources rather than communication offline. Images that are highly confidential and contains crucial information could be easily hacked and used for unfair means and purposes. There is a slight difference between staying secure and being secure. User needs to understand the importance of security whether it is their home, data, image or anything else. Appling security to a transmitted image which is transferred between two parties is very necessary as the transmission channel is open and the attackers can go any limits to get the crucial information at any cost. Image encryption has become an important task in today's world as we need to secure every data that is sent through a channel. We have some existing techniques which can be amalgamated and modified to make a new technique and implement the same with different images to evaluate the properties and performance metrics. One such technique is to combine chaos logistic map for generating the secret key and using DNA encoding to encrypt the image.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

A. Chaos Theory

Chaos theory is been widely utilised in the filed of cryptography of images as it persists the properties like pseudo randomness that generates the random values in each iteration, and the other properties which chaos depicts are ergodicity, non-linear arrangement. The only drawback that exists that it has very limited chaotic range. Chaotic properties are very desirable for the generation of secret key and then encrypting an image with the same. Moreover, it remains to be unpredicted as there is a new value generated in each iteration. Implementation of the chaos is also very easy as it could be structured in a very simple manner but before that the analysis of behavioural characteristics and determining the range is an important task. Other analysis that could be considered before encryption are time-series analysis, 0-1 Test, Chi- Square test, Phase portrait

1. *Logistic Map:* - Works on the iterative equation of

$$x_{n+1}=rx(1-x_n)$$

where r is the control parameter which shows the chaotic behaviour between the range of [3.6 to 4]. The bifurcation diagram plotting sub divides the chaotic equation in two parts though linear at its initial stage. The white spaces represent no chaotic behaviour for iterative sequence generation whereas the dense range represents the n number of chaotic sequences that can be generated from the value of x. Furthermore, the Lyapunov Exponent is another factor which depicts the behaviour of chaos. The equation of Lyapunov Exponent is

$$\lambda_{\max} = \frac{1}{t_m - t_0}\sum_{k=1}^{M} \ln \frac{L(t_k)}{L(t_{k-1})}$$

It is a dynamical system which is used to calculate the actual rate of separation between two close trajectories of two nearby located points. The computational quality of Lyapunov exponent tends to increase with the increase in the dimension of the dynamic system. If there is only one positive exponent, then the system is considered to be chaotic whereas if it has more than one positive exponent, the it is considered as a hyperchaotic system. As you can see that there is a variation in the Lyapunov exponents value at 3.6. For the number of iterations to be 1000 with the last iteration of 100^{th} value, I have displayed the bifurcation diagram of the 1D chaos logistic map. And below I have shown the Lyapunov exponent which initially starts at -0.6 and touches the value 0 three times before showing a chaotic behavior and after the r>3.6 it shows positive which means that the equation is of chaotic nature. In logistic map equation, r is the control parameter which is between 3.8 to 4 in mapping.

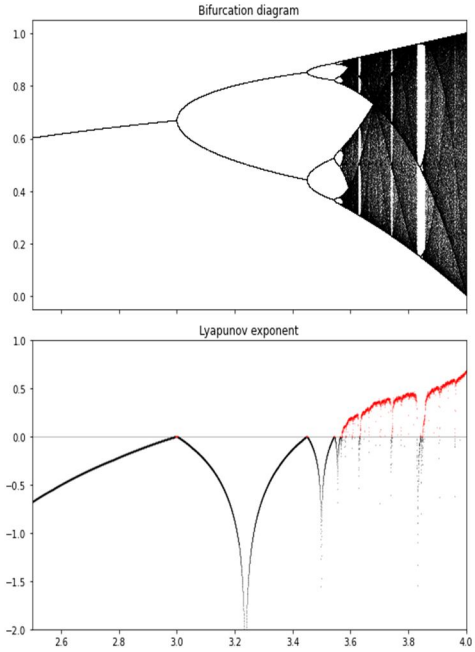


Fig. 1 : Depicts the plotting of bifurcation diagram and Lyapunov Exponent

II. RELATED WORK

The paper [1] discuss the basic terms of the chaos logistic mapping and how this technique can be made much stronger by applying other algorithms like DNA encoding, substitution box, wave function-based algorithm and Latin square. It gives a clear knowledge about the dimensions used in chaos logistic map and the benefits of using it for image encryption. Furthermore, this paper has implemented two techniques of the existing algorithms in an improvised way namely ILM and IQM which makes the image encryption system more efficient and it can overcome the existing problems of low chaotic range and higher execution time. After that, with the help of performance evaluation analysis factors like Approximation Entropy, Map Sensitivity, Sequence Uniformity and their respective graphical interpretation, it has proved its points. The initial step for every encryption method is to generate a secret key. Here MD5 is used to do the same that can generate a 128-bit hash value. Also, MD5 can be recognised as an irreversible method which prevents the key from being attacked. A chaos map [2] is highly productive in the field of image encryption which is why the researchers go for different dimensionalities and propose new methods. This paper proposed to use chaos-based image encryption using 3D logistic map and after that performing post encryption tasks. Chaos has gained popularity in recent years due to its pseudo randomness behaviour. The technique used in this paper is first converting any colour image into grayscale and this grayscale image is converted into binary form of 0's and 1's. Thereafter, the confusion method is performed by scrambling the pixel positions. Now the chaos comes into picture which generates a 3D positioned matrix and then combine this matrix with the key. Last, they have XOR the shuffled matrix with the original image. The weakness [3] of not protecting your classified information is that it can be leaked and it won't be a secret anymore. There should be a guaranteed protection of image when it is transmitted from source to destination. For this, cryptography has significantly a great impact in secure data transmission over a channel. The two steps for chaotic map encryption is permutation and substitution. The general equation for chaos logistic map was provided and the encryption process was theoretically explained. After that, the analysis of image was done with two evaluation parameters that is histogram analysis and correlation coefficient for all the types of images that are plain image, encoded image, encrypted image, decoded image and decrypted plain image. The authors [4] have proposed a system to employ a three chaotic sequence so that a high level of encrypted image can be produced. They have proposed to use logistic map and Ikeda map at the same time. Here the diffusion is performed at pixel level and confusion is performed at bit level. And several performance metrics were evaluated for the encrypted image which includes information entropy analysis, differential attack analysis etc. The step by step algorithm is provided in this paper for diffusion and confusion process. If the image is decrypted with the wrong key, then the original image was not produced. In the chaos [5] logistic map the main idea is to perform substitution and permutations iteratively so that the original image's pixels can be modified. Here in this paper, the authors have combined this stage with a 1D chaotic map to deliver high performance. The algorithm has focused on securing the image data from different types of attacks and to increase the efficiency and security and different levels of encryption. The mechanism used in the chaos is called 'stretching and squeezing'. They have generated a higher value for chaotic range and has tested the chaotic behaviour with Lyapunov exponent, bifurcation, approximation entropy and 0-1 test. There should be [20] more than 1 positive Lyapunov exponent in order to call a system hyperchaotic. This paper has implemented Chen's hyperchaotic mechanism along with the DNA coding to make an image more secure and efficient. Though there is a limitation that hyperchaotic system is more complex and using Chen' hyperchaotic system, it is difficult to predict the generated values using brute force attacks. Proposed system is divided into different modules like key generation, scrambling, diffusion. Every image encryption [21] algorithm typically focuses on generating a great value of noisy image so that the secrecy of the data must be maintained. Such techniques are designed to protect the data and increase the efficiency. A chaos that has proposed has typically four main components namely secret and sharing segmentation, sequential permutation, chaotic dynamical systems and modern cryptography features.

The other papers referred are as follows

S.no Paper

1) A new image encryption scheme based on hybrid chaotic maps [6]
2) An improved digital logistic map and its application in image encryption [7]
3) Image encryption based on new Beta chaotic map [14]
4) Color image encryption using DNA based cryptography [15]
5) An efficient medical image encryption using hybrid DNA computing and chaos in transform domain [16]
6) Color Image Encryption Algorithm Based on Hyper-Chaos and DNA Computing [18]
7) Secure Image Encryption Algorithm Based on Hyper chaos and Dynamic DNA Coding [19]
8) A Survey and Analysis of the Image Encryption Methods [22]
9) A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system [23]

III. METHODOLOGY

The above-mentioned papers do not consist of a clear knowledge of what is chaos-based encryption. The title itself is not justified properly. All the discussion concluded are theoretical and there is no information provided if anyone wants to develop a novel technique to work on image encryption algorithm that utilizes the concepts of DNA sequencing along with the chaos logistic mapping. The study gives the naïve learner a better perspective to understand the system as well as know its key points and mapping. Also, after gaining knowledge about chaos, DNA encoding algorithm can be implemented with the same approach and codes and for future implementation, it can be modified where the researcher is free to develop their own random DNA sequences in order to increase the efficiency of the system.

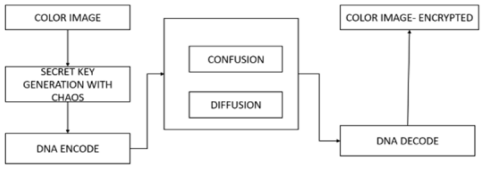


Fig. 2: Depicts the plotting of bifurcation diagram and Lyapunov Exponent

A. Generation of Secret Key with Chaos Logistic Map

The steps for the generation of secret key in order to encrypt a plain image is explained below in a step by step procedure. This step can make anyone understand the basic implementation of chaos logistic system that is explained above and how one can get the randomly generated chaotic values.

1) *Step 1:* Evaluate the chaotic behaviour of the system by applying the random initial values and get the parametric values that depicts the chaotic behaviour
2) *Step 2:* Fetch the original plain image
3) *Step 3:* Generate the key using the control parameter and image pixel values
4) *Step 4:* XOR the image pixels with the randomly generated chaotic range
5) *Step 5:* Get the encrypted image as a result

B. DNA Sequence Operation

Basically, a DNA encoding is done using four different nucleic acids namely Adenine (A), Cytosine (C), Guanine (G) and Thymine (T) collectively called as nucleotides. There are codes for addition and subtraction which can be used to encode an image which is in binary form. The code A and T are complement to each other and similarly, C and G are complement to each other. It depends on the values that are assigned for each nucleotide. Let us assume the value of each DNA sequence can be

TABLE 1
Assign the Binary Code for each DNA code

Nucleotide	Value	Complement
A	00	11
C	01	10
G	10	01
T	11	00

TABLE 2
Addition Operation for DNA Sequence

+	A	G	C	T
A	A	G	C	T
G	G	C	T	A
C	C	T	A	G
T	T	A	G	C

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

According to the Crick- Watson rule, there could be 4! =24 combinations available for the DNA sequencing, out of which only 8 rules are compatible for image encryption. Following up with the last phase, the image can be either converted into binary form, or separate RGB color in order to convert them to DNA sequence. Apply the function so that DNA sequence should be generated randomly without following any pattern. Now, the information of the original image is depicted in the form of random DNA codes comprising of four nucleotides.

C. Apply confusion and Diffusion

This phase is nothing but scrambling of the pixels and then changing the intensity of pixel values is termed to be diffusion and confusion respectively which is the most important phase after generating secret key with chaos and encoding the image with DNA. This can be performed with the following algorithm

1) *Step 1:* Fetch the image that is already existing in the database in order to form the process
2) *Step 2:* Define the key generation function and apply the chaos logistic mapping equation
3) *Step 3:* Get the index values and pixel values which has to be changed into the new position and mapping the indexing with the interchanged value

```
for x in range(n):
   for y in range(n):
      if (k[x] > k[y]):
         k[x], k[y] = k[y], k[x]
         index[x], index[y] = index[y], index[x]
```

4) *Step 4:* Traverse to all the pixels in the image one single time and shuffle the image pixel with the new generated index value

```
for i in range(x):
   k = 0
   for j in range(y):
      eimg[i][j]=img[i][index[k]]
```

5) *Step 5:* Reshuffle the image by replacing the pixels with the original index values rather than taking the new index values.

D. Decode the Encrypted Image

In order to decode the image, again we have to follow the same encoding standards and convert the DNA codes into binary values. Thereafter, the binary values and converted into 0 to 255 pixels values and after that the original encrypted image is generated. This encrypted image can be accessed using the secret key generated at the time of encryption. A slight difference in the secret key will lead to a drastic change in the image decryption and the parameters that can applied over to generate the secret key must also be same while decrypting the image, else the image would not be decrypted to original one.

IV. RESULTS AND DISCUSSION

There are numerous performance metrics which are used in every paper. My survey was about the metrics used in different types of papers and what benefit it yields. Typically, almost every paper talked about the research algorithm, the implementation technique and the proposed way of implementation, but none of them gave a clear concept about what chaos is. By the name, it is clear that the definition of chaos is to create confusion or a series of misconceptions. But in general, this algorithm can solve the image encryption problems with a greater extent of efficiency and security. Also, I have analyzed the techniques to implement the DNA Sequence algorithm which provides an additional security over the above-mentioned maps which are iteratively used for image encryption irrespective of the confusion diffusion duo. Below given is the number of performance metrics that are used to analyze the proposed systems capability for different papers. The total number of metrics cannot be determined but it can be divided under statistical, key analysis, entropy and attack analysis.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

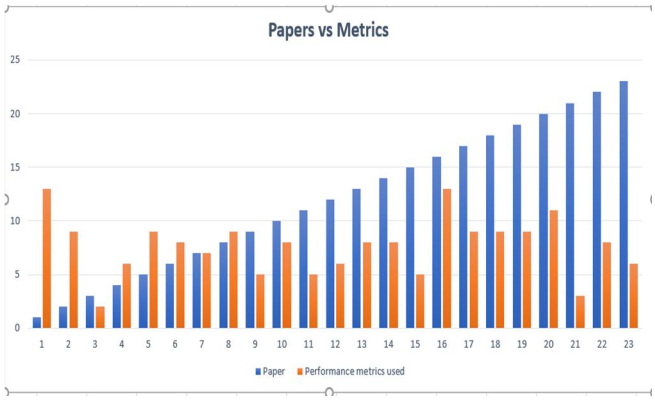


Fig. 3: Total Number of Metrics along with the research paper

V. CONCLUSIONS

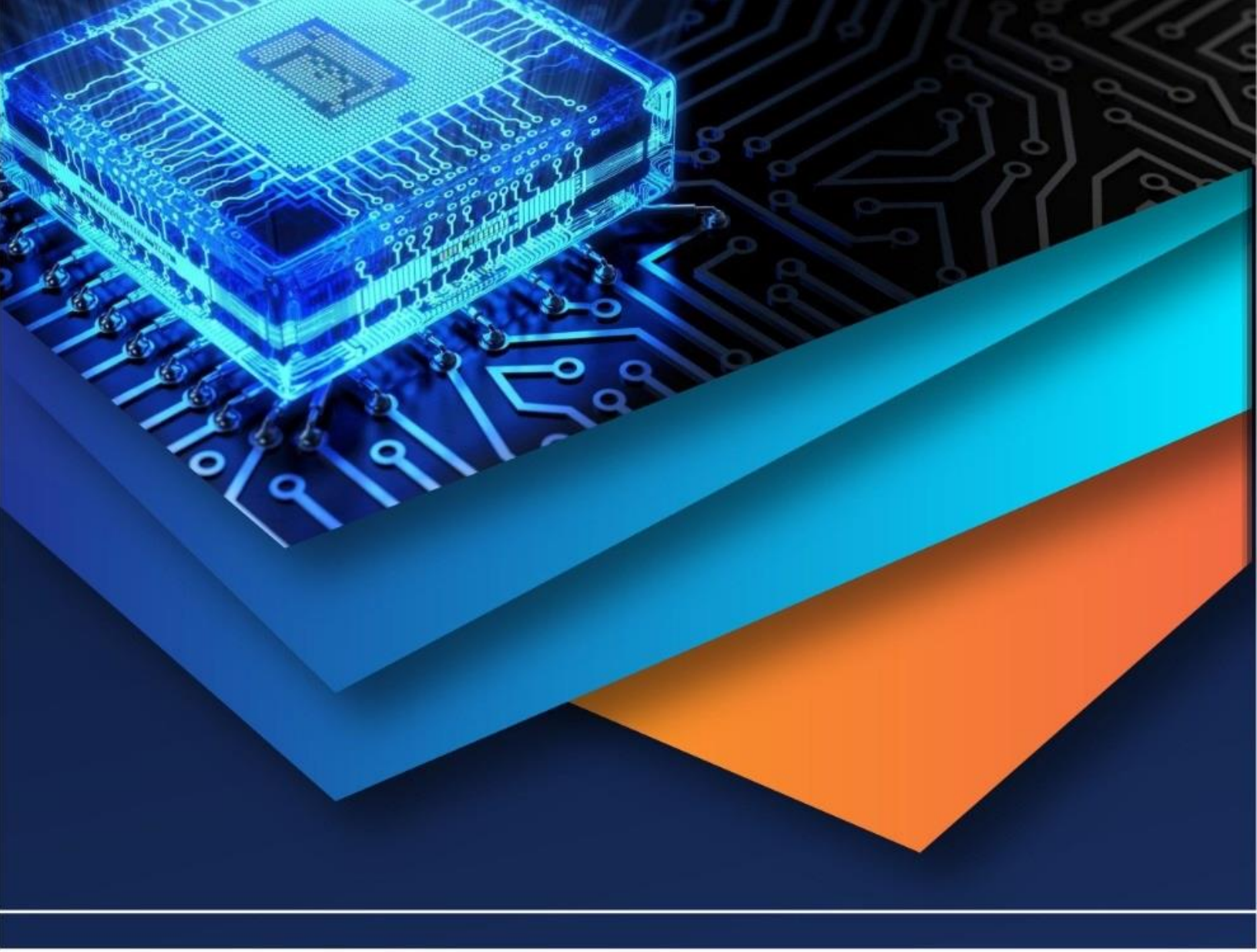
In this paper, the study of papers that proposed to implement new chaotic techniques are considered and studied about the way they have implemented their proposed technique. There was no proper explanation given about what exactly a chaos system is, on what dimension does it work and how it can be implemented for a secure image encryption algorithm. The novelty and segmentation of the whole working phase is drafter inside the paper, also the existing works and the formal introduction about the chaos and its methods are given, but the demonstration of the work does not follow up if a naïve person wants to research in the field of cryptography. Some papers have given an idea about cryptography techniques and compared it with the chaos implementation and other encryption system but that can just be a theoretical knowledge which one could interpret. Above all, the performance metrics that are used in each paper are mentioned in the graph and it is observed that only one paper that has implemented hybrid DNA computing algorithm along with the chaos consists of the maximum number of metrics to evaluate the performance of the proposed and designed system. The least could be three for which the paper was theoretical and general information about chaos, chaotic behavior and only three performance metrics was given. The DNA encryption could be non-linear as well as highly encrypted process as when the encryption is performed over an image, it generates a different sequence in every iteration, the encryption system works on the non- repetitive principle.

REFERENCES

[1] Mustafa Kamil Khairullah, Ammar Ahmed Alkahtani , Mohd Zafri Bin Baharuddin, Ammar Mohammed Al-Jubari, “Designing 1D Chaotic Maps for Fast Chaotic Image Encryption”, Electronics, August 2021.
[2] Supriya Khaitan , Shrddha Sagar, Rashi Agarwal, “Chaos based image encryption using 3-Dimension logistic map”, Materials Today: Proceedings, May 2021.
[3] Mutia Delina, Chandra Wijaya, Surano Muhasya, “Digital Image Security Based on the Chaotic Logistic Map”, AIP Conference Proceedings 2331, 030032, April 2021.
[4] Ashish Girdhar, Himani Kapur, Vijay Kumar, “A novel grayscale image encryption approach based on chaotic maps and image blocks”, Applied Physics B, February 2021.
[5] Mohamed Zakariya Talhaoui, Xingyuan Wang, “A new fractional one-dimensional chaotic map and its application in high-speed Image Encryption”, Information Sciences, October 2020.
[6] Ahmad Pourjabbar Kari, Ahmad Habibizad Navin, Amir Massoud Bidgoli, Mirkamal Mirnia, ” A new image encryption scheme based on hybrid chaotic maps”, Multimedia Tools and Applications, September 2020.
[7] Hongyue Xiang, Lingfeng Liu, “An improved digital logistic map and its application in image encryption”, Multimedia Tools and Applications, August 2020.
[8] Ying Niu, Zheng Zhou, Xuncai Zhang, “An image encryption approach based on chaotic maps and genetic operations”, Multimedia Tools and Applications, July 2020.
[9] Vijay Kumar, Ashish Girdhar, “A 2D logistic map and Lorenz-Rossler chaotic system based RGB image encryption approach”, Multimedia Tools and Applications, September 2020.
[10] K. Abhimanyu Kumar Patro, Bibhudendra Acharya, Vijay Nath, “Secure multilevel permutation-diffusion based image encryption using chaotic and hyper-chaotic maps”, Microsystem Technologies, March 2019.
[11] Haider M. Al-Mashhadi, Iman Q. Abduljaleel, “Color Image Encryption using Chaotic Maps, Triangular Scrambling, with DNA Sequences”, International Conference on Current Research in Computer Science and Information Technology, April 2017.
[12] I. Shatheesh Sam, P. Devaraj, R.S. Bhuvaneswaran, “Chaos Based Image Encryption Scheme Based on Enhanced Logistic Map”, R. Natarajan and A. Ojo (Eds.): ICDCIT , LNCS 6536, pp. 290–300, 2011.
[13] Sukalyan Som, Abhijit Mitra, Sarbani Palit, B. B. Chaudhuri, “A selective bitplane image encryption scheme using chaotic maps”, Multimedia Tools and Applications, September 2018.
[14] Rim Zahmoul, Ridha Ejbali, Mourad Zaied, “Image encryption based on new Beta chaotic maps”, Optics and Lasers in Engineering, April 2017.
[15] Nabarun Nandy, Debanjan Banerjee, Chittaranjan Pradhan, “Color image encryption using DNA based cryptography”, International Journal of Information Technology, February 2018.

[16] Dhivya Ravichandran, Aashiq Banu S, B.K Murthy, Vidhyadharini Balasubramanian, Sherin Fathima, Rengarajan Amirtharajan, "An efficient medical image encryption using hybrid DNA computing and chaos in transform domain", Medical & Biological Engineering & Computing, February 2021.
[17] K. Abhimanyu Kumar Patro, Bibhudendra Acharya, Vijay Nath, "Secure, Lossless, and Noise-resistive Image Encryption using Chaos, Hyper-chaos, and DNA Sequence Operation", IETE Technical Review, April 2019.
[18] M. G. Abbas Malik, Zia Bashir, Nadeem Iqbal, MD. Athar Imtiaz, "Color Image Encryption Algorithm Based on Hyper-Chaos and DNA Computing", IEEE Access, May 2020.
[19] Shuqin Zhu, Congxu Zhu, "Secure Image Encryption Algorithm Based on Hyperchaos and Dynamic DNA Coding", Entropy, July 2020.
[20] Xingyuan Wang, Maochang Zhao, "An image encryption algorithm based on hyperchaotic system and DNA coding", Optics and Laser Technology, June 2021.
[21] Yaghoub Pourasad, Ramin Ranjbarzadeh, Abbas Mardani, "A New Algorithm for Digital Image Encryption Based on Chaos Theory", Entropy, March 2021.
[22] Omar Farook Mohammad, Mohd Shafry Mohd Rahim, Subhi Rafeeq Mohammed Zeebaree, Falah Y.H. Ahmed, "A Survey and Analysis of the Image Encryption Methods", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 23, January 2017.
[23] Xiaopeng Wei, Ling Guoa, Qiang Zhanga, Jianxin Zhanga, Shiguo Lianb, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system", The Journal of Systems and Software, September 2011.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)