IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IMAGE ENCRYPTION WITH CHAOTIC SYSTEM AND CML

Deepali Patil, Dhaval Jain, Deep Dave
Assistant Professor, Student, Student
Department of Information Technology,
Shree L R Tiwari College of Engineering, Mumbai, India

Abstract
The chaos-based image cryptosystems have been widely investigated in recent years to provide real-time encryption and transmission [4]. Chaos-based encryption techniques have been widely used for real-time encryption and decryption [5]. But techniques with only chaos theory are prone to the same attacks as other encryption techniques. So to enhance the security mechanism and the robustness as well as to keep up with the newly developing 'real time' technology a color image encryption algorithm by using 'Coupled Map Lattice' as well as 'Fractional-order chaotic system' system will be implemented[4]. To make the encryption procedure more confusing and complex, an image division-shuffling process is put forward, where the plain image is first divided into four sub-images, and then the position of the pixels in the whole image is shuffled. In order to generate the initial conditions and parameters of two chaotic systems, a 280-bit long external secret key is employed. The cryptosystem speed is analyzed and tested moreover [5].

Keywords: *Image-Encryption, Cryptosystem, Image-Decryption, Coupled Mapped Lattice, Chaotic System, Fractional- Order Chaotic System, Permutation and Diffusion, Secret Key...*

1. Introduction

A coupled-map lattice (CML) could be a phase space that models the behavior of nonlinear systems (especially partial differential equations) [3].
They are predominantly accustomed to qualitatively study the chaotic dynamics of spatially extended systems.
A coupled map consists of elements of a given discrete-time ("map") that interact ("couple") with other elements from a suitably chosen set.
To extend the protection of this algorithm, an external secret key of 280-bit length is employed, to come up with initial conditions and parameters of the CML and fractional-order chaotic system by making some algebraic transformations to the key [3].
In practical applications, three forms of methods, i.e., permutation, diffusion, and their combined form, are usually employed to style image encryption algorithms [1].
For the aim of high security, it's very promising to use CML and fractional-order chaotic systems in color image encryption [3].

2. Problem Statement

Image encryption scheme has been proposed using two chaotic maps which are Arnold Cat map for Permutation and Logistic Map for diffusion using an 80-bit randomly generated key.
In Arnold's cat map, a picture is hit with a metamorphosis that apparently randomizes the initial of its pixels. However, if iterated enough times, the first image reappears.
Cryptanalysis image encryption method isn't secure enough from both theoretical and experimental viewpoints organization because it uses 16-bit secret key [2].
The simplest idea to boost the initial encryption scheme is increasing the bit size (n) of key1 and key2. When n = 280 (280-bit data is widely employed in digital computers), the complexity is going to be approximately 2^ 280 [5].
The simplest idea to reinforce the first encryption scheme is increasing the bit size (n) of key1 and key2. When n = 280 (280-bit data is widely employed in digital computers), the complexity is going to be approximately 2^ 280 [5].

2.1 PDRCML Algorithm:

[1] This paper proposes a completely unique high-sensitivity image encryption algorithm with a random cross-diffusion supported dynamically random coupled map lattice model implemented by piecewise linear chaotic map (PDRCML). Through theoretical analysis and experimental results analysis, it may be demonstrated that the system has a larger parameter space, and also the state of every lattice is more practical compared with traditional coupled logistic map lattices (CML). The system is suitable for chaotic encryption and secure communications. Moreover, the proposed image encryption algorithm combines S-box, fast disturbance handling, and random cross-diffusion to comprehend non-linear diffusion, which breaks traditional diffusion methods supported permutation. By analyzing the simulation performance of encryption, it is often easily determined that the algorithm features a high degree of security, sensitivity, good statistical performance. And it further demonstrates the wonderful features of the PDRCML model.

2.2 LDMLNCML Algorithm:

[2] This paper proposes a brand new high-sensitivity image encryption algorithm with random diffusion supported the spatiotemporal chaos of the Logistic-dynamic mixed linear-nonlinear coupled map lattices (LDMLNCML). The proposed LDMLNCML system possesses prominent cryptographic characteristics, which are extremely suitable for image encryption. The proposed image encryption algorithm adopts the strategy of random diffusion. Firstly, the pending sequence is generated in keeping with the number of image pixels, and so two index chains are generated combining the conflict handling process. Finally, the cipher image is obtained by random diffusion. Index chains are sensitive to changes in position, and changes in the position of any one element will produce completely different index chains. The cipher value of every pixel within the diffusion phase depends on two random non-adjacent pixels and chaos interference value, which might greatly reduce the correlation between the adjacent pixels. Theoretical analysis and experimental results demonstrate the protection and practicability of the cryptosystem.

2.3 CML and DNA sequences:

[3] During this paper, a replacement image encryption scheme supported CML and DNA sequences is proposed. First, a sort of DNA encoding rule is chosen to encode the first image to a DNA matrix. Then, we perform a cyclic shift on the even rows and columns of the DNA matrix so perform further index scrambling operations on the odd rows within the scrambled DNA matrix. Using the DNA sequence generated by the CML system and designed DNA calculation rules, the scrambled DNA matrix is further diffused. Finally, decode the diffused DNA matrix and find the ultimate encrypted image. Simulation experiments and security analysis show that the scheme achieves a satisfactory effect and has the capacity to resist all types of classical attack methods.

2.4 DNA sequence operations and spatiotemporal chaos:

[4] A lossless and robust color image encryption algorithm is proposed supported by DNA sequence operations, one-time keys, and spatiotemporal chaos. The NCA map-based CML has excellent chaotic properties compared with the standard CML and other chaotic systems. The ultimate key streams are closely associated with both the key keys and therefore the original image. The DNA-level merge-shuffling process, the division, and DNA-level diffusion process, and also the pixel-level diffusion process are designed to strengthen the safety and robustness of the cryptosystem. During this paper, we introduce a completely unique color image encryption algorithm supported by DNA sequence operations, one-time keys, and also spatiotemporal chaos. Firstly, the key streams are generated by the NCA map-based CML, where the hash function SHA-256 is employed to update the system parameters and initial conditions combining with the plain-image and therefore the secret keys. Secondly, decompose the plain image into the red, green, blue components, and convert them randomly into three DNA matrices by the DNA encoding rules. Further, combine three DNA matrices into a replacement DNA matrix, so perform the row-wise and column-wise permutations thereon. Thirdly, divide the shuffled DNA matrix into three equal blocks and implement the DNA addition, subtraction, and XOR operations on these DNA blocks. Finally, transform the DNA matrices into the decimal matrices separately consistent with the DNA decoding rules. To reinforce the protection of the cryptosystem, a diffusion process is further distributed by using the key streams. Thus, the resulting cipher-image is attained. Experimental results and security analysis show that the presented encryption algorithm has a good encryption effect and can resist various typical attacks.

2.5 Coupled Map Lattice:

[5] This paper deals with the problem of key diffusion in chaotic image encryption algorithms. Usually, these approaches use multiple pseudo-random sequences for operations done during encryption and decryption. As each of these sequences is generated by part of the selected key, in case that only a small portion of the key is changed, some of the sequences could remain the same. This problem is solved by the usage of Coupled Map Lattice which introduces dependencies between chaotic maps used for the generation of the pseudo-random sequences. The Paper also mentions other approaches and compares their results with those achieved by the proposed algorithm by means of commonly used measures. The main advantages of our proposal include high values of entropy and Unified Average Changing Intensity.

3. Flowchart:

The plain color image is taken as the input. Then by division and shuffling process the image is divided into parts and shuffled. After that by using the Image permutation process the position of the pixel of the image is shuffled and by the image diffusion process the value of the pixel of the image is changed. Simultaneously for the secret key generation CML and fractional order Chen chaotic system. Together that cipher/encrypted image is formed. Below figure shows how the flowchart goes:

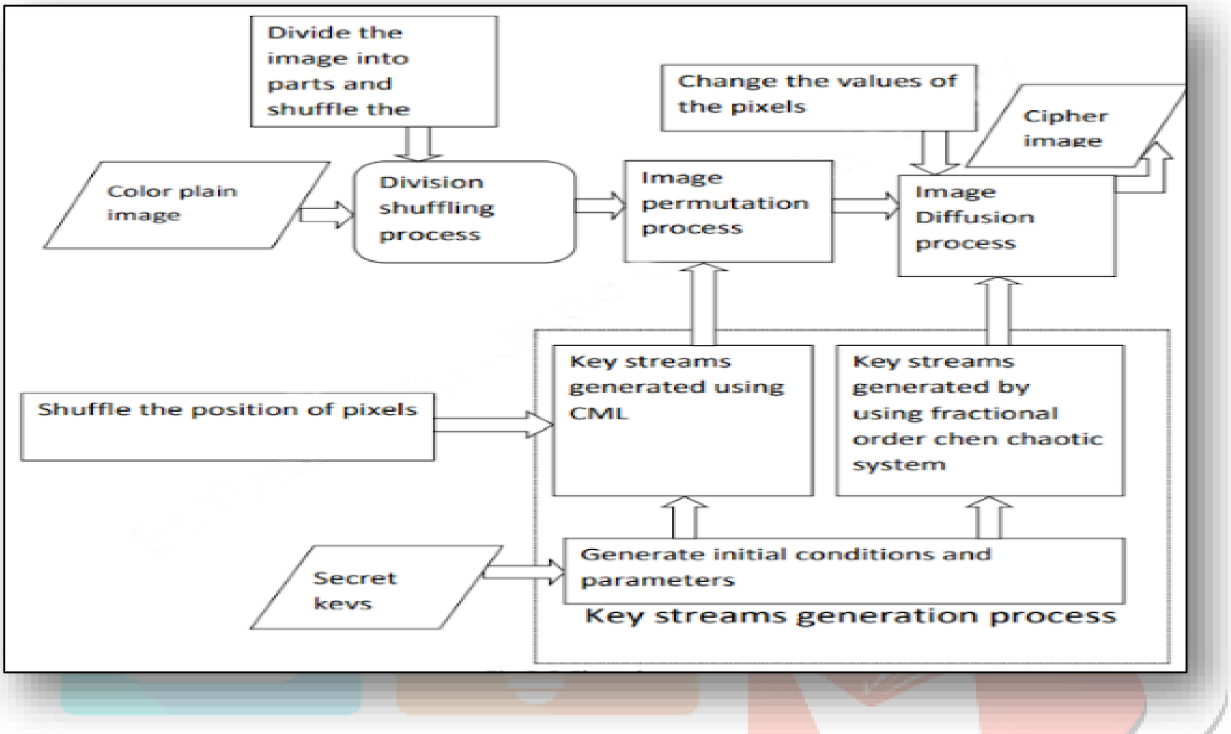
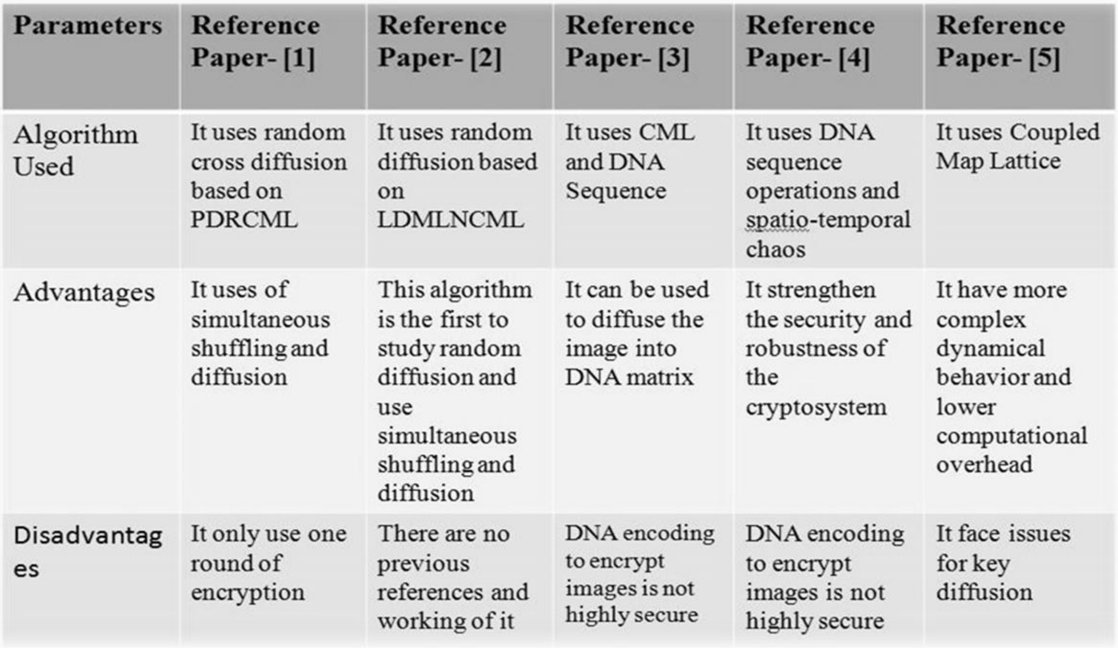

Divide the image into parts and shuffle the
Change the values of the pixels
Cipher image
Color plain image
Division shuffling process
Image permutation process
Image Diffusion process
Key streams generated using CML
Key streams generated by using fractional order chen chaotic system
Shuffle the position of pixels
Secret keys
Generate initial conditions and parameters
Key streams generation process

Figure 1: Flowchart

4. Comparative Study:

We have discussed different algorithms for image encryption.
First, we have seen the random cross-diffusion based on PDRCML which works on simultaneous shuffling and diffusion [1].
Second, we have seen the random diffusion based on LDMLNCML which works on random diffusion and simultaneous shuffling [2].
Third, we have seen the CML and DNA Sequence which works on the diffusion of the image into the DNA matrix [3].
Fourth we have seen the DNA sequence operations and Spatio-temporal chaos which work to strengthen the security and robustness of the cryptosystem [4].
And the last Fifth we have seen the Coupled Map Lattice which works on more complex dynamical behavior and lower computational overhead [5].
The comparative study of all these algorithms is given in tabular form as below in (table 1):



Parameters	Reference Paper- [1]	Reference Paper- [2]	Reference Paper- [3]	Reference Paper- [4]	Reference Paper- [5]
Algorithm Used	It uses random cross diffusion based on PDRCML	It uses random diffusion based on LDMLNCML	It uses CML and DNA Sequence	It uses DNA sequence operations and spatio-temporal chaos	It uses Coupled Map Lattice
Advantages	It uses of simultaneous shuffling and diffusion	This algorithm is the first to study random diffusion and use simultaneous shuffling and diffusion	It can be used to diffuse the image into DNA matrix	It strengthen the security and robustness of the cryptosystem	It have more complex dynamical behavior and lower computational overhead
Disadvantages	It only use one round of encryption	There are no previous references and working of it	DNA encoding to encrypt images is not highly secure	DNA encoding to encrypt images is not highly secure	It face issues for key diffusion

Table 1: Comparative Study

5. Conclusion and Future Work

The cryptosystem is composed of four processes to enhance the security and sensitivity of the cryptosystem i.e., an image division-shuffling process, a key stream generation process, an image permutation process, and an image diffusion process. Compared with that recently proposed bit-level permutation method is superior as the bits are shuffled among different bit- planes rather than within the same bit-plane. By further research in this area, features like video and audio encryption, text encryption might be added in near future. We will consider different aspects to which our system should justify and fine-tune its functionality and work to give the user the best experience.

References

[1] "*High-sensitivity image encryption algorithm with random cross diffusion based on dynamically random coupled map lattice model*" (Xingyuan Wang; Jingjing Yang; Nana Guan) - February, 2021.

[2] "*High-sensitivity image encryption algorithm with random diffusion based on dynamic-coupled map lattices*" (Wang Xingyuan; Zhao Hongyu; Feng Le; Ye Xiaolin; Zhang Hao)- November 2019

[3] "*A New Image Encryption Algorithm Based on CML and DNA Sequence*" (Xingyuan Wang; Yutao Hou; Shibing Wang; Rui Li) - November, 2018.

[4] "*Color image DNA encryption using NCA map-based CML and one-time keys*" (Wu Xiangjun; Wang Kunshu; Wang Xingyuan; Kan Haibin; Jürgen Kurths)- July, 2018.

[5] "*Image encryption technique with key diffused by coupled map lattice*" (Jakub Oravec; Jan Turan; Lubos Ovsenik) - June, 2018.