RV Educational Institutions ®
RV College of Engineering ®
Autonomous Institution Affiliated to Visvesvaraya Technological University, Belagavi
Approved by AICTE, New Delhi.

Go, change the world

Image Encryption Using DNA Cryptography

COMPUTER NETWORKS (18IS52)

EXPERENTIAL LEARNING REPORT

Submitted by

Prakhar Jaju	**1RV20IS033**
Mayank Somani	**1RV20IS069**

Under the guidance of

Prof. Rekha B S

Assistant Professor

Department

of

Information Science and Engineering

2022-2023

RV COLLEGE OF ENGINEERING®, BENGALURU-59

(Autonomous Institution Affiliated to VTU, Belagavi)

DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING

CERTIFICATE

Certified that the project work titled **'Image Encryption Using DNA Cryptography'** is carried out by **Prakhar Jaju (1RV20IS033) and Mayank Somani(1RV20IS069) in** partial fulfilment of the completion of the course **Computer Networks (18IS52**) of the V Sem. Information Science Engineering programme, during the academic year 2022-2023. It is certified that all corrections/suggestions indicated for the Internal Assessment have been incorporated in the project report and duly approved by the faculty.

Signature of Faculty **Signature of Head of the Department**

Table of Contents

ABSTRACT

Since computer networks have been widely applied, people's communications have had a revolutionary change, and transmission of digital images over the Internet has become more and more popular. However, the openness and sharing of networks exposes the security of digital images to serious threats in the process of transmission. Consequently, people have to pay more and more attention to security and confidentiality of multimedia information. Among various protection methods, the image encryption technique is one of the most efficient and common methods for the protection of image information. Traditional encryption algorithms, such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES), etc., are not suitable for image encryption. So, a new research method of image encryption is acquired urgently.

A new image encryption scheme based on DNA sequence addition operation and chaos is presented. First, a DNA sequence matrix is obtained by encoding the original image, then, divide the DNA sequence matrix into some equal blocks and use the DNA sequence addition operation to add these blocks. Next, perform the DNA sequence complement operation to the result of the added matrix by using two Logistic maps. Finally, decode the DNA sequence matrix from the third step, and we can get the encrypted image. The simulation experimental results and security analysis show that our scheme not only can achieve good encryption, but can also resist exhaustive attack, statistical attack and differential attack.

CHAPTER 1
INTRODUCTION

1.1 Domain Addressing

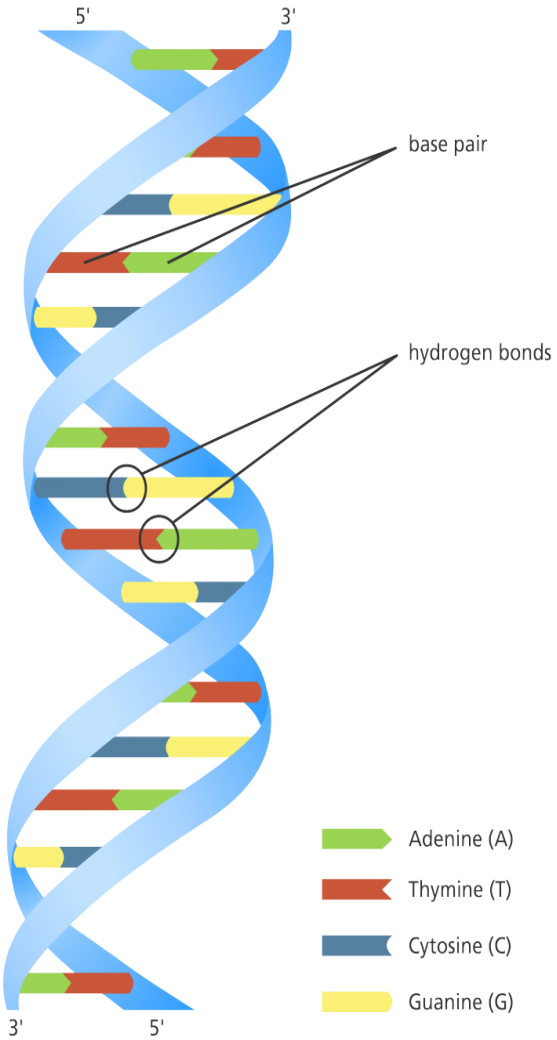
What is DNA?

DNA, or deoxyribonucleic acid, is the hereditary material in humans and almost all other organisms.

The information in DNA is stored as a code made up of four chemical bases: adenine (A), guanine (G), cytosine (C), and thymine (T).

Human DNA consists of about 3 billion bases, and more than 99 percent of those bases are the same in all people. The order, or sequence, of these bases determines the information available for building and maintaining an organism, similar to the way in which letters of the alphabet appear in a certain order to form words and sentences.

DNA can replicate itself into multiple copies.



How can it be used for computing?

DNA computing is **an emerging branch of computing** which uses DNA, biochemistry, and molecular biology hardware, instead of the traditional electronic computing.

The first theory of DNA computation was proposed by Leonard Adleman in 1994. The use of DNA strands to compute has led to high parallel computation.

However, synthesizing and using DNA requires highly equipped labs which is extremely expensive and thus is under study by many researchers.

What is DNA Cryptography and how is it useful?

DNA Cryptography can be defined as a technique of hiding data in terms of DNA sequence. In the cryptographic technique, each letter of the alphabet is converted into a different combinationof the four bases which make up the human deoxyribonucleic acid (DNA).

A DNA sequence contains four nucleic acid bases A(adenine), C(cytosine), G(guanine), T(thymine), where A and T are complementary, and G and C are complementary.

We use C, A, T, G to denote 00,01,10,11 respectively, as 00 and 11 are complementary and 01 and 10 are complementary.

The addition and subtraction operations for DNA sequences are performed according to traditional addition and subtraction like 11 + 10 = 01 and 01-11 = 10. Therefore, the additionand subtraction operations for these encodings are as follows:

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

Addition operations for bases

-	T	A	C	G
T	C	G	T	A
A	A	C	G	T
C	T	A	C	G
G	G	T	A	C

Subtraction operations for bases

1.2 Existing System

1. Triple Data Encryption Standard (TDES):

- Symmetric encryption is employed for the smooth operation of Triple DES.
- The modern version of the Triple-DES is evolved on the DES block cipher.
- This encryption technique uses a 56-bit key.
- These keys are used triple times or thrice that makes it a 168-bit key.

2. Advanced Encryption Standard (AES):

- AES uses the phenomenon of symmetric encryption.
- It uses higher length key sizes such as 128, 192 and 256 bits for encryption.
- AES algorithm is more robust against hacking
- AES in counter mode is complex to implement in software

1.3 Problem Statement

Digital images have become one of the most popular media types. Image transmission security is subject to potential threats. Digital images also need to meet the highest requirements of confidentiality. Image encryption technology has become an effective way to protect images being transmitted. Image encryption is very important to protect from any unauthorized user access.

Problem Statement: "To encrypt and decrypt images based on an algorithm which is less vulnerable to attacks and can be used efficiently".

CHAPTER 2
METHODOLOGY

2.1 Lorenz System

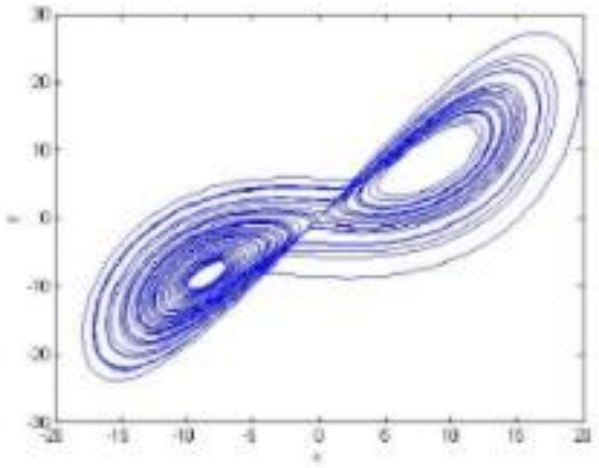
- The Lorenz equation is nothing else than a model of thermally induced fluid convectionin the atmosphere. The model was first reported and published by E.N Lorenz in 1963
- Lorenz chaotic equation is a 3D dynamical system, which is defined by x, y and z. Theequation system gives a chaotic behavior with regard to the initial system parameters.
- The equation system contains three differential equations:

$$x' = ay - ax \quad (1)$$

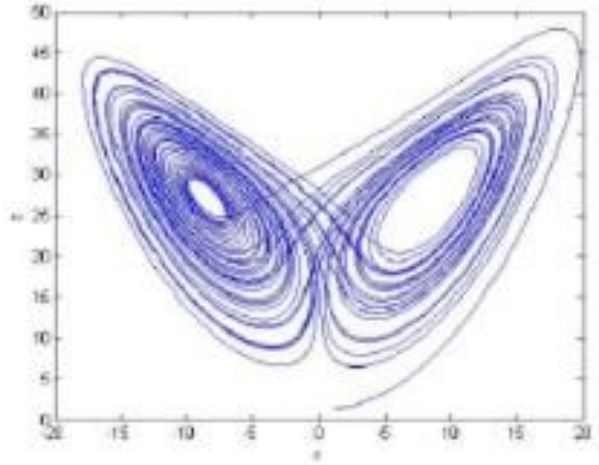
$$y' = -xz + rx - y \quad (2)$$

$$z' = xy - bz \quad (3)$$

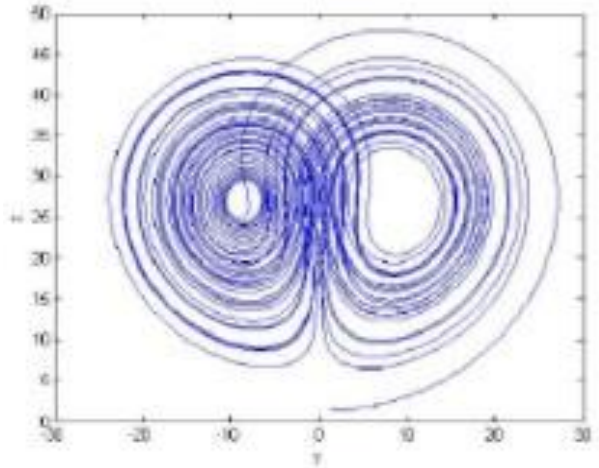
- Here x, y and z are the functions of time with the derivative forms (i.e. x‘, y’ and z’) anda, b, r are the system parameters for the deterministic system.
- In order to obtain chaos, a, b and r are usually defined as 10, 8/3 and 28, respectively.
- Fig (a),(b),(c) show the variances x-y x-z and y-z respectively.



a)



b)



c)

2.2 Processes Involved

The existing image encryption algorithms based on DNA coding involve four basic processes:

1. Scrambling the pixel position of the image by using a chaotic sequence.
2. Encoding the scrambled image matrix to the DNA sequence.
3. Disturbing the DNA sequence matrix by using a chaotic sequence combined withaddition, subtraction, XOR, or complement operation, or a combination of these operations.
4. Obtaining the encrypted image by DNA decoding and recombination.

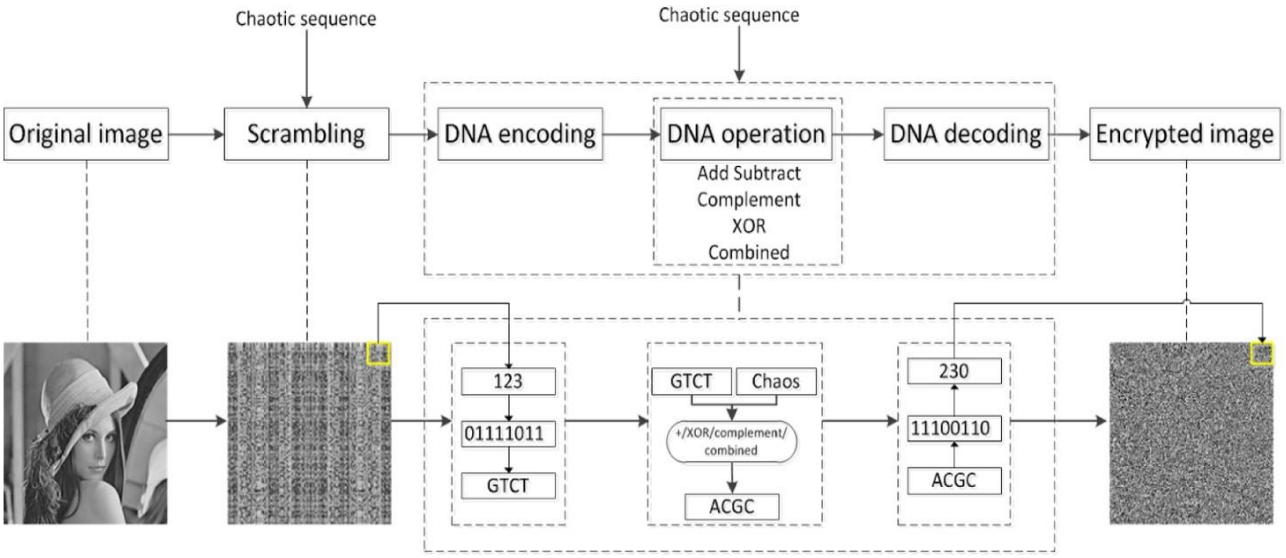


Figure 2.2.1 Block Diagram of image encryption based on DNA coding

2.3 Encryption Algorithm

DNA operations are randomly decided by a 1-D logistic map. Firstly, the SHA-256 is appliedon the original image to produce the sequence K. Secondly, R,G and B components of the original image and the key image are encoded into four DNA sequence matrices. Thirdly, employ encoded key images to conduct random DNA operations with the encoded plain imagesto obtain a transitional image. Fourthly, the transitional image is permuted by using a Lorenz chaotic sequence. Finally, we decode the permuted DNA matrix applying a randomly selected rule to gain the eventual cipher image. The details of the encryption algorithm is presented as follows:

Step 1: The input is an original image P(M,N,3) which M and N express the width and height of the image, respectively.

Step 2: Produce the key sequence K and the initial values x'_1,x'_2 and x'_3 of the Lorenz system.

Step 3: the plain image is divided into three components, and we obtain threecomponents, R, G and B, and convert the R, G, B to binary matrices R(M,N /2), G(M,N/2) and B(M,N /2), then encode R, G, B by rows with DNA rules and gain three DNAsequence matrices Pr(M,N /2), Pg(M,N /2) and Pb(M,N /2).

Step 4: The details about DNA rules. Each pixel of a row is coding by a particular DNA rule. After all pixels of image are encoded, the size of encoded images are M*N/2.

Step 5: Generate key image then encode Mk by rows with DNA rules and obtain anencoded DNA sequence matrix Mk (M, N /2).

Step 6: Execute DNA operations between the encoded plain image (Pr, Pg and Pb) andthe encoded key image (KI_e) row by row.

$$pr' = pr \text{ XOR } Mk$$

$$pg' = pg \text{ XOR } Mk$$

$$pb' = pb \text{ XOR } Mk$$

Step 7: Generate three chaotic sequences according to the initial value x'_1,x'_2 and x_3 ofthe Lorenz system. Continue to iterate Lorenz system, three pseudo-random sequences *sx*, *sy* and *sz* are generated, whose length is M *N *4 using Runge-Kutta method.

$$\begin{cases} (lx, fx) = sort(sx) \\ (ly, fy) = sort(sy) \\ (lz, fz) = sort(sz) \end{cases}$$

Step 8: Convert the three binary matrices P_r' , P_g' and P_b' to three vectors $V_r(M * N * 4)$, $V_g(M * N * 4)$ and $V_b(M * N * 4)$, respectively. Confuse V_r, V_g and V_b according to:

$$\begin{cases} Vr'(i) = Vr(lx(i)) \\ Vg'(i) = Vg(ly(i)) \\ Vb'(i) = Vb(lz(i)) \end{cases}$$

Step 9: Convert V_r' , V_g' and V_b' to three matrices Re(M, N * 4), Ge(M, N * 4) andBe(M, N * 4), respectively. Decode Re, Ge and Be exploiting a selected DNA encodingrule and generate three matrices Rb,Gb and Bb.

Step 10: Finally, merge Rb,Gb and Bb images and that is the ultimate cipher image. The cipher image is with size M *N

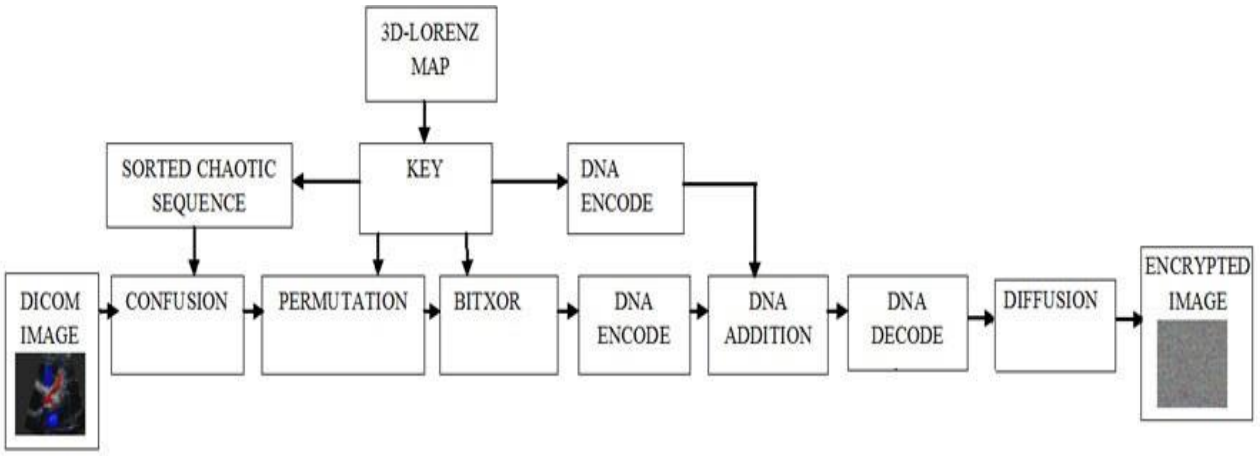


Figure 1b: Block description of the proposed Encryption scheme.

2.4 Decryption Algorithm

We can decode cipher images by following steps:

Step 1: Using randomly selected DNA rules, encode the R, G and B components of the ciphered image. We obtain three matrices Re, Ge and Be, and we convert them to three vectors Vr' , Vg' and Vb'.

Step 2: Vr' , Vg' and Vb' are confused vectors.

$$\begin{cases} Vr(i) = Vr'(lx(i)) \\ Vg(i) = Vg'(ly(i)) \\ Vb(i) = Vb'(lz(i)) \end{cases}$$

Step 3: Convert the three vectors Vr,Vg and Vb to three matrices Pr' ,Pg' and Pb' .

Step 4: Use encoded key image and encoded cipher image to generate the transitional encoded image. The particular DNA operation is illustrated in Step 5 of the Encryption algorithm. After we invert the step 5 of the encryption algorithm to obtain Pr, Pg and Pb,and KI_e is obtained and as it is mentioned in Step 4 of the encryption algorithm.

Step 5: Decode the Pr, Pg and Pb to get the R, G and B components of the plain image. The particular rule is illustrated in Step 3 of the encryption algorithm.

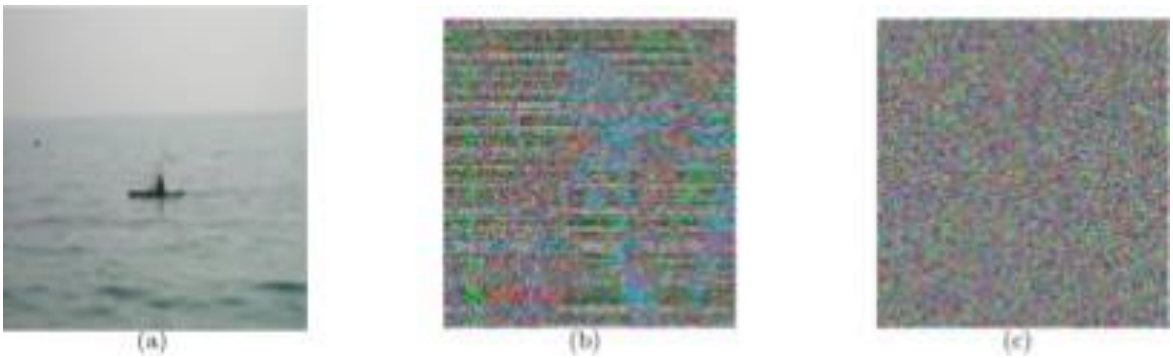
Step 6: Finally, merge R, G and B images and that is the ultimate original image.

CHAPTER 3
RESULT

3.1 Performance

The security performance of image encryption system is checked by evaluating different required measures such as:

1. **Key Space:** A key space larger than 2100 could guarantee a high level of security from the cryptography of view. The key space of the security SHA-256 is 2128, we can get the total key space S = 2128*1084 ≈ 3.4*10122, which is enough to prevent the exhaustive attack. Thus, brute force attacks on the key are impossible.
2. **Key Sensitivity:** A good encryption algorithm should be sensitive to the secret key; that is, a very tiny difference in the secret key will cause a greatly significant change in the output.



3. **Histogram Analysis:** Image histogram is a significant characteristic in image analysis. An ideal cipher image should have a uniform frequency distribution. The histograms of the cipher image are uniform and random-like, which suggests that the proposed algorithm has the histogram of the cipher image becomes fairly uniform.
4. **Run Time**:

- For conversion of images of size less than 500kb, it takes about 1-2 minutes for encrypting the cypher image from the plain image and then decrypting the cypher image to get the recovered image.
- For images of size around 5 mb, it takes about 30 minutes for the image to get converted.
- The average running time for the program is 5 minutes.

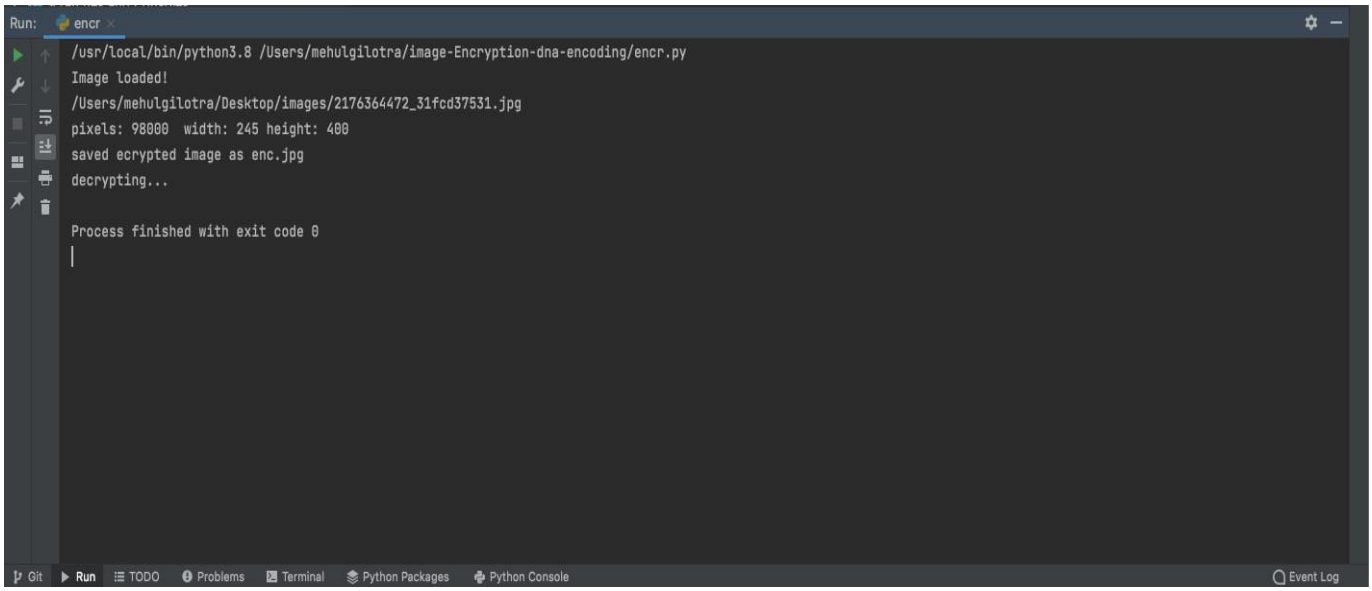
5. **Size:** The maximum size of the image to be encrypted and decrypted is 10 MB.

3.2 Snapshots

Decrypted Image **Original Image**

Decrypted Image **Original Image**

Terminal Window



5. REFERENCES

- Xiaodong Li, Cailan Zhou , Ning Xu“A Secure and Efficient Image Encryption Algorithm Based on DNA Coding and Spatiotemporal Chaos”, *International Journal ofNetwork Security, Vol.20, No.1, PP.110-120, Jan. 2018.*
- Riguang Lin, Sheng Li, "An Image Encryption Scheme Based on Lorenz Hyperchaotic System and RSA Algorithm", *Security and Communication Networks*, vol. 2021, ArticleID 5586959, 2021.
- L. Y. Zhang, Y. Liu, F. Pareschi et al., “On the security of a class of diffusion mechanisms for image encryption,” *IEEE Transactions on Cybernetics*, vol. 48, no. 4,pp. 1163–1175, 2018.
- G. Ye, C. Pan, X. Huang, and Q. Mei, “An efficient pixel-level chaotic image encryptionalgorithm,” *Nonlinear Dynamics*, vol. 94, no. 1, pp. 745–756, 2018.
- Y.-G. Yang, J. Tian, H. Lei, Y.-H. Zhou, and W.-M. Shi, “Novel quantum image encryption using one-dimensional quantum cellular automata,” *Information Sciences*,vol. 345, pp. 257–270, 2016.
- J. Chen, Z.-l. Zhu, L.-b. Zhang, Y. Zhang, and B.-q. Yang, “Exploiting self-adaptivepermutation-diffusion and DNA random encoding for secure and efficient image encryption,” *Signal Processing*, vol. 142, pp. 340–353, 2018.
- D. Huo, D.-f. Zhou, S. Yuan, S. Yi, L. Zhang, and X. Zhou, “Image encryption usingexclusive-OR with DNA complementary rules and double random phase encoding,”*Physics Letters A*, vol. 383, no. 9, pp. 915–922, 2019.
- F Yi, Y. Kim, and I. Moon, “Secure image-authentication schemes with hidden doublerandom-phase encoding,” *IEEE Access*, vol. 6, pp. 70113–70121, 2018.
- H. Liu, B. Zhao, and L. Huang, “Quantum image encryption scheme using Arnoldtransform and S-box scrambling,” *Entropy*, vol. 21, no. 4, p. 343, 2019.
- M. Ghebleh, A. Kanso, and H. Noura, “An image encryption scheme based on irregularly decimated chaotic maps,” *Signal Processing: Image Communication*, vol. 29,no. 5, pp. 618–627, 2014.