IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Toward Robust Image Encryption Based on Chaos Theory and DNA Computing

RAVI KUMAR H K Research Scholar Bundelkhand University
Dr M K Agarwal Professor Bundelkhand University

Abstract

The rapid expansion of digital communication has increased the need for secure image transmission. Traditional encryption algorithms are not well-suited for images due to their inherent properties such as high redundancy and strong pixel correlation. This paper proposes a robust image encryption scheme that integrates chaos theory and DNA computing. Chaotic systems provide high sensitivity and randomness, while DNA computing introduces efficient encoding and parallel processing. The hybrid approach enhances security, enlarges key space, and improves resistance against statistical and differential attacks. Experimental and theoretical analyses demonstrate the effectiveness of the proposed method.

Keywords: Image encryption, Chaos theory, DNA computing, Cryptography, Logistic map, Security analysis

I. Introduction

With the widespread use of digital images in communication systems such as healthcare, defense, and cloud storage, protecting image data has become essential. Conventional encryption algorithms like AES and DES are effective for textual data but inefficient for images due to:

- Large data size
- High pixel redundancy
- Strong correlation among adjacent pixels

To address these limitations, researchers have explored alternative encryption techniques. Chaos-based encryption and DNA computing have emerged as promising approaches.

Chaos theory offers properties such as unpredictability and sensitivity to initial conditions, making it suitable for generating secure keys. DNA computing, inspired by biological processes, enables complex encoding and parallel operations.

This paper presents a hybrid encryption model combining both techniques to achieve improved security and performance.

II. Related Work

Several image encryption techniques have been proposed:

- Chaos-based methods using logistic and Henon maps for pixel scrambling
- DNA-based methods utilizing nucleotide encoding and operations
- Hybrid models combining permutation and substitution techniques

However, individual approaches often suffer from limited diffusion or reduced resistance to attacks. The integration of chaos and DNA computing overcomes these drawbacks by providing both confusion and diffusion.

III. Preliminaries

A. Chaos Theory

Chaos systems are deterministic but exhibit random-like behavior. A commonly used chaotic map is the logistic map:

xn+1=r·xn(1−xn)x_{n+1} = r \cdot x_n (1 - x_n)xn+1=r·xn(1−xn)

Where:

- xn∈(0,1)x_n \in (0,1)xn∈(0,1)
- r∈(3.57,4)r \in (3.57, 4)r∈(3.57,4)

Key properties:

- High sensitivity to initial conditions
- Ergodicity
- Pseudo-random sequence generation

B. DNA Computing

DNA computing encodes binary data into nucleotide sequences:

Binary	DNA
00	A
01	C
10	G
11	T

Basic operations:

- DNA addition
- DNA subtraction
- DNA XOR

These operations enhance encryption complexity and security.

IV. Proposed Method

A. System Overview

The proposed encryption scheme consists of two main stages:

1. **Confusion** – Pixel permutation using chaotic sequences
2. **Diffusion** – DNA encoding and operations

B. Encryption Algorithm

Step 1: Image Input
The input image is converted into a matrix of pixel values.

Step 2: Chaotic Sequence Generation
A logistic map is used to generate pseudo-random sequences based on initial parameters.

Step 3: Pixel Permutation
Pixels are rearranged using chaotic sequences to remove spatial correlation.

Step 4: DNA Encoding
Each pixel value is converted into binary and mapped to DNA sequences.

Step 5: DNA Operations
DNA XOR or addition is performed using chaotic keys.

Step 6: DNA Decoding
DNA sequences are converted back to binary values.

Step 7: Cipher Image Generation
The final encrypted image is obtained.

C. Decryption Algorithm

The decryption process reverses the encryption steps:

1. Generate identical chaotic sequences
2. Perform inverse DNA operations
3. Decode DNA sequences
4. Reverse pixel permutation

Correct key usage ensures accurate reconstruction of the original image.

V. Security Analysis

A. Key Space Analysis

The combination of chaotic parameters and DNA rules results in a large key space, making brute-force attacks infeasible.

B. Statistical Analysis

Histogram Analysis
Encrypted images show uniform distribution, preventing statistical attacks.

Correlation Analysis
Adjacent pixel correlation is reduced to near zero.

C. Differential Attack Resistance

Metrics used:

- NPCR (Number of Pixels Change Rate)
- UACI (Unified Average Changing Intensity)

High values indicate strong resistance to differential attacks.

D. Information Entropy

Entropy value approaches the ideal value of 8 for grayscale images, indicating high randomness.

E. Key Sensitivity

A slight change in the key produces a completely different encrypted image, ensuring strong security.

VI. Performance Evaluation

Advantages

- High security level
- Strong resistance to attacks
- Efficient for large image data
- Supports parallel processing

Limitations

- Increased computational complexity
- Sensitive parameter selection
- Implementation overhead

VII. Applications

- Secure medical image transmission
- Military communication systems
- Cloud storage protection

- Digital watermarking
- Surveillance systems

VIII. Future Work

Future improvements may include:

- Integration with machine learning techniques
- Hardware implementation (FPGA/GPU)
- Optimization for real-time processing

IX. Conclusion

This paper presents a robust hybrid image encryption technique based on chaos theory and DNA computing. The approach combines the randomness of chaotic systems with the complexity of DNA encoding to provide enhanced security. The proposed method effectively resists various cryptographic attacks and is suitable for modern secure communication systems.

References

[1] G. Chen and Y. Mao, “Chaos-based image encryption,” IEEE Trans.
[2] A. Kanso, “DNA-based cryptography,” Journal of Security
[3] C. E. Shannon, “Communication theory of secrecy systems,” Bell Labs
[4] X. Zhang, “Image encryption using DNA encoding and chaotic maps”
[5] W. Stallings, *Cryptography and Network Security*, Pearson