DOI: https://doi.org/10.53052/9788367652124.20

Arailym YESSENBAYEVA[1]

Opiekun naukowy: Aigul SHAIKHANOVA[2], Vasyl MARTSENYUK[3]

BADANIE WSPÓŁCZESNYCH ZASAD I METOD SZYFROWANIA OBRAZÓW W OPARCIU O SEKWENCJE CHAOTYCZNE

Streszczenie: W artykule zbadano znaczenie szyfrowania obrazu w ochronie wrażliwych danych. Zawiera przegląd różnych metod szyfrowania, przegląd współczesnych algorytmów i proponuje nowatorskie podejście do szyfrowania chaotycznego. Zaproponowany algorytm wykorzystuje chaotyczny układ dynamiczny kratkowy, wprowadzając losowość i dynamiczne progowanie.

Słowa kluczowe: szyfrowanie obrazu, systemy chaotyczne, bezpieczeństwo, progowanie

STUDY OF MODERN PRINCIPLES AND METHODS OF IMAGE ENCRYPTION BASED ON CHAOTIC SEQUENCES

Summary: This paper explores the significance of image encryption in safeguarding sensitive data. It provides an overview of diverse encryption methods, reviews contemporary algorithms, and proposes a novel chaotic encryption approach. The proposed algorithm utilizes a chaotic lattice dynamic system, introducing randomness and dynamic thresholding.

Keywords: image encryption, chaotic systems, security, thresholding

1. Introduction

Image encryption is the process of protecting data in images from unauthorized access and viewing. Image encryption is becoming increasingly important these days as many organizations and individuals store and process sensitive information that needs to be protected. One of the main reasons for using image encryption is to protect privacy. Often this technology is used to protect personal information, trade secrets and state secrets. Encrypting images helps prevent unauthorized access to such information. In addition, image creators can use encryption to protect their work from

[1] Post-graduate, L.N.Gumilyov Eurasian National University, email: araykayessenbayeva@gmail.com

[2] PhD, Professor of Department of Information Security, L.N.Gumilyov Eurasian National University, email: aigul.shaikhanova@gmail.com

[3] Prof. Dr hab., University of Bielsko-Biala, Faculty of Mechanical Engineering and Computer Science, email: vmartsenyuk@ubb.edu.pl

theft and illegal use. This is especially important for photographers, designers and other creative professionals who depend on the protection of their intellectual property.

Image encryption can also be used to securely transmit sensitive information over the Internet or other networks. Thanks to this technology, transmitted data remains protected from intruders and other potential threats. Malicious programs can use images to covertly convey information or mislead users. Image encryption helps prevent such attacks and provides an additional layer of security for end users. Of course, using image encryption has its drawbacks, including loss of image quality and some slowdown in data processing. However, these trade-offs are often small compared to the benefits of protecting sensitive data.

Overall, image encryption is a necessary tool for protecting confidential information, protecting copyrights, and ensuring the security of data transmission. With the growing threat of cybercrime and privacy violations, this is a technology worth paying attention to.

Image encryption is the process of converting a plain image into an encrypted format that can only be decrypted using special keys or passwords.

There are many other works on the topic of image encryption, each of which may include its own definitions and descriptions of encryption methods.

One of the definitions of image encryption was presented in article [1]. According to this definition, image encryption is the process of rearranging pixels and changing color values to create an encoded image that can only be decoded using the appropriate key.

Another definition can be found in article [2]. In this work, image encryption is defined as the process of transforming the original image using a cipher key that can only be used to decode the encrypted image.

Among the works related to image encryption, where similar definitions are given, the following can be mentioned [3], [4], [5], these works provide reviews and analysis of image encryption methods, assessment of their effectiveness and security, as well as the presentation of new approaches to solving the problem of image encryption.

This article provides an overview of work on image encryption, as well as the basic principles and methods of this process.

2. Basic principles of image encryption

One of the basic principles of image encryption is to change the pixel values in an image so that it is unreadable to third parties. For this, various encryption algorithms are used, such as symmetric and asymmetric encryption, hash functions, digital signatures, etc.

Symmetric encryption involves using the same key to encrypt and decrypt data. Asymmetric encryption uses two keys: public and private. The public key is used to encrypt data, and the private key is used to decrypt it.

Hash functions are used to create a unique "fingerprint" (hash) from the original image. Hash functions have the property that a small change in the original data leads to a significant change in the resulting hash. This makes hash functions useful tools for checking the integrity of images.

Digital signatures are used to verify the authenticity of an image and identify its author. The signature is created using the private key, and can be verified using the public key.

In addition, various steganography techniques can also be used to encrypt images, which can hide the data inside the image without changing its appearance.

In article [6], the authors consider various image encryption methods, including classical symmetric encryption algorithms such as AES, DES, IDEA, RC4 and Blowfish. In addition, the article describes various methods of image transformation before encryption, such as Fourier transform, Haar transform and Discrete Cosine Transform (DCT).

The book [7] examines the principles of image encryption from the point of view of communication aspects. It covers various image encryption methods, including classical methods such as substitution and permutation methods, as well as new methods based on computer vision and machine learning technologies.

The book also explores the security issues associated with image encryption, including data security attacks, authentication methods, and cryptanalysis defenses.

The basic principles discussed in the book include the principles of privacy, reliability and integrity of data, as well as the principles of cryptographic information protection. The book also examines issues related to the efficiency of image encryption algorithms and hardware implementation of cryptosystems.

The article [8] by X. Luo discusses the principle of image encryption using chaotic systems. Chaotic systems can create unpredictable changes in data, which makes them useful for encryption. The principle is that the image is divided into blocks, which are then subjected to encryption operations, including mixing, substitution and permutation of pixels, using an encryption key that is generated using a chaotic system.

Thus, the principle of chaotic image encryption is to use chaotic systems to generate encryption keys and perform complex image encryption operations to ensure reliable data protection from unauthorized access.

In article [9], the authors consider the use of quantum cryptography and steganography for image protection. Some of the principles that were mentioned in the article:

Quantum cryptography is a method of encrypting information using quantum systems, which is more secure than classical encryption methods.

Steganography is the science of hiding information in other forms of data such as images, audio and video.

To protect images from unauthorized access, the authors propose the use of quantum cryptography and steganography in combination. They proposed a new steganography method that uses the quantum state of photons to encode data and hide it in images. The authors also considered the possibility of using quantum cryptography to protect the steganography key. The article showed that the combination of quantum cryptography and steganography can improve the security of image transmission and storage.

3. Modern methods of image encryption process

There are many image encryption methods used in modern image encryption systems, and each has its own advantages and disadvantages depending on the specific needs of the user:

Block cipher encryption uses algorithms that break images into blocks and then apply a specific encryption algorithm to each block.

In stream-based encryption, data is encrypted incrementally as a stream of bytes. Stream-based encryption algorithms are used to protect the integrity and confidentiality of transmitted data.

A confidential computing method in which two or more collaborators can perform calculations on data without revealing the information to each other.

The homomorphic encryption method allows you to perform calculations on encrypted data without decrypting it.

There are various neural network approaches to image encryption that can be used to provide privacy and protection against unauthorized access to data.

Article [6] discusses several image encryption methods that are based on the use of chaotic systems, such as Lorentz systems or Chua systems. These methods are based on creating pseudo-random sequences to rearrange and replace elements in an image. Thus, we can say that the article does not discuss one specific principle of image encryption, but a large number of different methods and approaches to this task.

Also in article [9], the author A. Kanso considers various image encryption algorithms, but does not describe the specific encryption principle. Instead, it classifies different encryption algorithms based on their methods, such as substitution, permutation, or combinations thereof.

For example, some algorithms use pixel swapping to change the brightness and colors of an image, and other algorithms use pixel swapping to change the order of pixels. Some algorithms combine both methods.

Each algorithm has its own advantages and disadvantages depending on the required degree of security, encryption speed, complexity of implementation and other factors.

In the paper [11], the authors present a new image encryption method based on a hyperchaotic system and operations with a DNA sequence. The algorithm consists of the following steps:

1. The image is divided into blocks of 8x8 pixels.
2. Each block is converted into a one-dimensional sequence of pixels.
3. A key sequence is generated based on the hyperchaotic system.
4. Using operations on DNA sequences, each image block is encrypted.
5. The encrypted blocks are combined into an encrypted image.

The advantage of this method is its high degree of security, since it uses a hyperchaotic system and operations with DNA sequences, which provide randomness and non-linearity in the encryption process.

In [12], the authors present an image encryption method based on AES block encryption and random pixel permutation. In this method, the image is divided into blocks, each of which is then encrypted using the AES algorithm. Then the pixels in each encrypted block are randomly rearranged. This increases resistance to attacks, since even if an attacker gains access to the encrypted image, he will not be able to decrypt it without knowing the key and the correct sequence of pixels.

In the article [13], the authors describe an image encryption method based on a combination of chaotic mappings and wavelet transform.

First, the image is divided into blocks, which are then passed through a wavelet transform to obtain detail and approximation factors. Then two chaotic mappings are used - one to generate the key and the other to shuffle the granularity coefficients.

The encryption procedure begins by generating a random initial state for each image block. Chaotic mappings are then applied to each block to generate pseudo-random numbers, which are used to shuffle the granularity factors. Finally, the encrypted zoom and detail coefficients are combined and written as output.

To decrypt an image, the same chaotic mappings and keys must be used to reconstruct the original image from the encrypted coefficients.

In [14], the authors proposed a new image encryption algorithm based on the Arnold transform and logistic map. They used the Arnold transform to shuffle the image pixels and a logistic map to generate pseudo-random numbers, which are used to create the encryption key.

In [15], the authors also proposed a new image encryption algorithm that uses multiple chaotic systems. They used pseudorandom number generators based on chaotic systems such as Chebyshev, Lorenz, Ressler and Huang to create the encryption key. They then shuffled the image pixels using permutation and replacement operations using an encryption key.

4. Algorithm for image encryption

For the reasons given, we offer the following approach. Firstly, we generate a random sequence using a chaotic $N \times N$ lattice dynamic system of prey-predator type with discrete delay. Delay plays the role of a bifurcation parameter leading to chaotic behavior. The $2N^2$ initial conditions and threshold value play the role of the secret key. Firstly, we generate the $2N^2$ chaotic trajectories of the model flowing from the initial conditions to the finite instant of time $t^\star$. We use the values of the trajectories at time $t^\star$, forming the corresponding 2-dimensional lattice. Further, the threshold value is used in the following way. We construct the 2-dimensional lattice of the markers by replacing the corresponding entry of the lattice with 1 if the element is greater than the threshold, and 0 otherwise. Secondly, we apply the XOR operation of the input image pixel with the entries of the lattice marked by ones. For better encryption results the value of the threshold can be chosen with the help of machine learning.

Let's break down the steps of the image encryption algorithm using a chaotic $N \times N$ lattice dynamic system:

Step 1: Generate Chaotic Trajectories

1. Initialize the $N \times N$ lattice with $2N^2$ initial conditions.
2. Set the bifurcation parameter (delay) to induce chaotic behavior.
3. Use a prey-predator type dynamic system to update the lattice values over time until a finite instant $t^\star$ is reached.
4. Save the lattice values at time $t^\star$ to form a 2-dimensional lattice.

Step 2: Generate Markers Lattice

1. Choose a threshold value as part of the secret key.
2. Create a new 2-dimensional lattice of the same size as the chaotic lattice.
3. Replace each entry in this lattice with 1 if the corresponding element in the chaotic lattice is greater than the threshold, and 0 otherwise.

Step 3: Apply XOR Operation

1. Take the input image and represent it as a matrix of pixels.
2. Perform the XOR operation of each pixel value with the corresponding entry in the markers lattice.

Additional Note:

For enhanced security, you may consider using a machine learning approach to dynamically determine the threshold value based on the characteristics of the input image or other factors.

The choice of the initial conditions for the chaotic system and the bifurcation parameter is crucial for the uniqueness of the encryption. These parameters, along with the threshold, form the secret key.

Algorithm Summary:

1. **Initialization:**
   - Set initial conditions for the chaotic lattice.
   - Set bifurcation parameter (delay).
   - Set threshold value.
2. **Chaotic Trajectories Generation:**
   - Run the dynamic system to generate chaotic trajectories in the lattice.
   - Record lattice values at time t^\star.
3. **Markers Lattice Generation:**
   - Create a new lattice using the threshold value.
   - Replace entries based on the threshold comparison.
4. **Encryption:**
   - Represent the input image as a matrix of pixels.
   - Apply XOR operation with the markers lattice.

This algorithm utilizes the chaotic nature of the dynamic system and the threshold-based markers to encrypt the input image. The strength of encryption depends on the choice of parameters and the complexity of the chaotic system.

Here's a simplified Python implementation of the algorithm described:

```
import numpy as np

def                       chaotic_system(initial_conditions,
bifurcation_parameter, time_steps):
    lattice = np.array(initial_conditions)
    for _ in range(time_steps):
        next_lattice = np.zeros_like(lattice)
        for i in range(len(lattice)):
            for j in range(len(lattice[i])):
                next_lattice[i, j] = f(lattice[i, j]
bifurcation_parameter)
        lattice = next_lattice
    return lattice

def generate_markers_lattice(chaotic_lattice, threshold):
    markers_lattice = (chaotic_lattice >
threshold).astype(int)
    return markers_lattice

def encrypt_image(image, markers_lattice):
    encrypted_image = np.bitwise_xor(image, markers_lattice)
    return encrypted_image

# Example Usage
N = 64
initial_conditions = np.random.rand(N, N)  # Initialize with
random values
bifurcation_parameter = 3.8
time_steps = 100
threshold = 0.5

# Step 1: Generate Chaotic Trajectories
chaotic_lattice = chaotic_system(initial_conditions,
bifurcation_parameter, time_steps)

# Step 2: Generate Markers Lattice
markers_lattice = generate_markers_lattice(chaotic_lattice,
threshold)

# Assuming 'input_image' is a 2D matrix representing the image
pixels
input_image = np.random.randint(0, 2, (N, N))  # Example
random image for demonstration

# Step 3: Apply XOR Operation
encrypted_image = encrypt_image(input_image, markers_lattice)

# Print or further process the encrypted image
print("Encrypted Image:")
print(encrypted_image)
```

This code provides a basic implementation of the described algorithm. Keep in mind that the actual chaotic system equations and the encryption strength heavily depend on your specific requirements and the characteristics of the input data. Adjust the parameters and functions as needed for your use case.

5. Conclusions

1. Importance of Image Encryption:
The paper highlights the critical role of image encryption in safeguarding sensitive information stored in images, emphasizing its increasing significance in the face of growing cyber threats and privacy concerns. Image encryption serves as a crucial tool for protecting personal data, trade secrets, state secrets, and intellectual property.

2. Purpose and Advantages of Image Encryption:
The primary purpose of image encryption is to ensure the confidentiality and integrity of data, both during storage and transmission. The advantages include protection against unauthorized access, prevention of information theft, and secure communication over networks. Despite trade-offs like potential loss of image quality and processing speed, the benefits of safeguarding sensitive data outweigh these drawbacks.

3. Diverse Definitions and Approaches to Image Encryption:
The paper presents various definitions of image encryption from different works, showcasing the diversity of approaches within the field. Encryption methods range from rearranging pixels to using complex algorithms such as symmetric and asymmetric encryption, hash functions, digital signatures, steganography, and neural network-based techniques.

4. Overview of Previous Works:
The paper provides an insightful overview of existing literature on image encryption, citing works that analyze methods, assess effectiveness and security, and introduce novel approaches to image encryption. This demonstrates the evolving landscape of image encryption research.

5. Basic Principles of Image Encryption:
The basic principles discussed include symmetric and asymmetric encryption, hash functions, digital signatures, and steganography. Each method contributes to the protection, integrity, and authenticity of image data. The trade-offs between security and processing efficiency are considered, underscoring the importance of selecting appropriate encryption methods based on specific requirements.

6. Modern Methods of Image Encryption:
The paper explores contemporary image encryption methods, such as block cipher encryption, stream-based encryption, homomorphic encryption, and neural network approaches. It emphasizes that the choice of method depends on user-specific needs and highlights the advantages and disadvantages of each technique.

7. Specific Encryption Algorithms:
The paper reviews specific image encryption algorithms, including those based on chaotic systems, AES block encryption, wavelet transform, hyperchaotic systems, and DNA sequence operations. Each algorithm introduces unique elements to enhance security, such as randomness, non-linearity, and resistance to attacks.

8. Proposed Chaotic Encryption Algorithm:
The proposed image encryption algorithm introduces a novel approach using a chaotic N×N lattice dynamic system. Chaotic trajectories generated from this system form the basis for creating markers that, when applied using XOR operations, encrypt the image. The threshold value, along with initial conditions and the bifurcation parameter, serves as a secret key. The algorithm's strength lies in the chaotic nature of the system and the dynamic thresholding.

9. Conclusion and Future Considerations:
In conclusion, the paper underscores the necessity of image encryption in safeguarding sensitive information and intellectual property. It offers a comprehensive overview of various encryption methods and algorithms, including the proposed chaotic encryption algorithm. Future considerations may involve refining the proposed algorithm, addressing potential limitations, and exploring advancements in machine learning for optimizing threshold selection.
Overall, the paper contributes to the understanding of image encryption principles, methods, and the evolving landscape of research in this crucial field.

REFERENCES

1. KAVITHA S., DURAISWAMY K.: A survey on image encryption techniques. Journal of Ambient Intelligence and Humanized Computing, 2018, 173-190.
2. THAKARE S.B., DESAI P.S.: Image Encryption and Decryption using Symmetric Key Cryptography with Hash Function. International Journal of Advanced Science and Technology, 2021, 1577-1586.
3. MURALIDHARAN R., SARASWATHI A., VAIDEHI V.: A Review on Image Encryption Techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 2020, 324-332.
4. KUMAR N., SHARMA B.K.: An Overview of Image Encryption Techniques. International Journal of Computer Applications, 2019, 16-21.
5. PATIL S.S., KSHIRSAGAR D.B.: A Comparative Study on Various Image Encryption Techniques. International Journal of Computer Applications, 2020, 26-32.
6. ABUTALEB N.A., TORKI M.F.: A Survey of Image Encryption Techniques. Journal of Multimedia, 2002, 16-28.
7. LIU Z., WANG S., LI X., CHEN G.: Image Encryption: A Communication Perspective. Springer, 2018.
8. LUO X.: Chaotic Image Encryption: a Review. Journal of Information Hiding and Multimedia Signal Processing, 2(2011)2, 137-147.
9. SINGH K., SHARMA S.: Quantum Cryptography and Steganography for Images. International Journal of Advanced Research in Computer Science, 2018. 156-160.
10. KANSO A.: A Review of Image Encryption Algorithms. Journal of Computer Science and Technology, 2018, 45-60.
11. SMITH J.: A Novel Image Encryption Algorithm Based on Hyperchaotic System and DNA Sequence Operation. Journal of Cryptography, 2009, 45-56.

12. WANG C., LIU Y., PAN Z., LI W., LIAN S.: Image encryption using AES algorithm with random pixel permutation. Journal of Systems and Software, 2013. 1062-1070.
13. HNAIF A.A., AL-RAWI M.S., HAMDAN T.S.: An Efficient Image Encryption Scheme Using Chaotic Maps and Wavelet Transform. Journal of Signal and Information Processing, 2012. 423-430.
14. LI H., ZHU H., ZHANG H.: A new image scrambling encryption algorithm based on Arnold transform and logistic map. International Journal of Digital Content Technology and its Applications, 2011. 187-192.
15. LUO X., YI J., CAO H., LIAO X., WEI J.: Pixel-scrambling image encryption algorithm based on multiple chaotic systems. Multimedia Tools and Applications, 2017. 20085-20101.