www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 11, November 2024, pp : 2666-2671

e-ISSN : 2583-1062
Impact Factor : 7.001

CHAOS-BASED IMAGE ENCRYPTION USING LORENZ SYTEM

Hassan Raza[1], Priya Y M[2], Sachin K[3], Varsha S[4], Mrs. Kavya S[5]

[1,2,3,4]BE Student, Computer Science and Design Department, PES Institute of Technology and Management, Shivamogga, Karnataka, India.

[5]Assistant Professor, Computer Science and Design Department, PES Institute of Technology and Management, Shivamogga, Karnataka, India.

ABSTRACT

The abstract depicts a chaos based image encryption scheme based on Lorenz system for overcoming the computational and security difficulties of classical one-dimensional chaotic maps. The usage of a single dimension chaotic map like a logistic map for image encryption goes back in the ages, but even with this, there are deficiencies because its iterations are highly determinable and time-consuming, especially for large images. The speculative approach contributes to finding solution to these issues by employing the Lorenz system which constitutes of multiple dimensions. It has a high degree of sensitivity towards variations in initial parameters making it unpredictable for attackers to even accurately forecast or reconstruct the phase of a multi-dimensional chaotic system. In the encryption making use of substitution-permutation network, SPN which is one of the structural ciphers in use for this purpose, incorporates two core concepts: substitution for replacement of data and shuffling data as the second function. The Lawrence system is particularly employed in creating the S-box which essentially forms a part of the encryption that brings about non-linearity ensuring that multiple environment pixels are substituted in a random fashion. This ensures that as long as there is small variation in the input, the output will be entirely different ensuring that the enciphered data system is endurable to differential attacks.

1. INTRODUCTION

We have tried to touch the different areas where mathematics, and specifically calculus finds itself in. We want to present the existing methodologies and frameworks in the applications in practice. In particular Chaos based Image Encryption. We make an effort to explain the different systems that we have and outline their previous use. Image pixel encryption is achieved through the use of a logistic growth equation, which is elaborated on later.

Logistic map

The logistic map is widely used to show the properties of chaotic dynamics. A rough description of chaos is that chaotic systems exhibit a great sensitivity to initial conditions—a property of the logistic map for most values of r between about

3.57 and 4(as noted above). A common source of such sensitivity to initial conditions is that the map represents a repeatedfolding and stretching of the space on which it is defined.

Chaos

Chaotic systems,in the field of mathematics, are generally systems defined by equations and exclusive parameters which display an unfathomable degree of randomness when plotted. They are extremely sensitive to initial conditions and a extremely minor change leads to a completely,seemingly new, plot. There are various examples of chaotic systems some ofwhich are The Lorenz system,the Rossler system,the Van der pol model and many more.

Fractals

A fractal is a never-ending pattern. Fractals are infinitely complex patterns that are self-similar across different scales. They are created by repeating a simple process over and over in an ongoing feedback loop. Recursion-driven, fractals are images of dynamic systems – the pictures of Chaos. Geometrically, they exist in between our familiar. Fractal patterns are extremely familiar, since nature is full of fractals. For instance: trees, rivers, coastlines, mountains, clouds, seashells, hurricanes, etc.

2. LITERATURE REVIEW

1. Quantum-enabled chaotic image encryption: How to improve digital data security using 1-D sine-based chaoticmaps and quantum coding

Mujeeb Ur Rehman

Journal of King Saud University-Computer and Information Sciences 36 (3), 101980, 2024

The proposed work explores the use of chaotic maps in combination with the quantum mechanisms to enhance the security of the digital images and overcome the weaknesses of the traditional 1-D chaotic systems that suffer from pseudorandom and periodic properties. The proposed research takes advantage of the inherent uncertainty in quantum

theory to introduce a new image encryption scheme. This approach is based on the theories of two-dimensional quantum coding and the 1-D sine-based chaotic map (1-D SBCM). In this proposed encryption technique, a random sequence is first generated by varying the seed parameters using 1-D SBCM. This sequence is then used for scrambling purposes. Later, a PRNG is carefully designed with inspiration from the concept of quantum coherence. This PRNG produces a private code stream that is unguessable and inconsistent with the plaintext image, thus making it more secure. The later part of the research makes use of the new advanced quantum representation model, known as NEQR. Under this model, the study introduces the quantum right cyclic shift operator and the quantum XOR operator. These operators are crucial in the development of highly robust encrypted images. The use of these quantum operators not only strengthens the security measures but also increases the complexity of the encryption process Statistical evidence obtained from extensive experimentation supports the fact that the proposed image encryption scheme is effective. On close analysis, it can be seen that the system shows robust performance in terms of strong security. The integration of quantum principles and quantum coding demonstrates that the proposed encryption scheme is resilient against potential threats.

2. A cryptanalysis of a chaotic image encryption method

Shujun Li, Xuan Zheng

2002 IEEE International Symposium on Circuits and Systems (ISCAS) 2, II-II, 2002

Recently, the security of digital images attracts much attention, and many image encryption methods have been proposed. In IS-CAS2000, a new chaotic key-based algorithm CKBA for image encryption is presented. This paper finds out that CKBA is highly vulnerable to the chosen/known-plaintext attack even using only one plainimage and the security of the authors overestimates that to the brute-force ciphertext-only attack. That is to say, CKBA is not secure at all from the cryptographic viewpoint. Some experiments are made to show the feasibility of the chosen/known-plaintext attack. We also discuss some remedies to the original scheme and their performance, and we find none of them can essentially improve the security of CKBA.

3. Chaos-based image encryption: Review, application, and challenges

Bowen Zhang, Lingfeng Liu Mathematics 11 (11), 2585, 2023

Chaos has been one of the most effective cryptographic sources since it was first used in image-encryption algorithms. This paper closely examines the development process of chaos-based image-encryption algorithms from various angles, including symmetric and asymmetric algorithms, block ciphers and stream ciphers, and integration with other technologies. The unique features of chaos, such as sensitivity to initial conditions, topological transitivity, and pseudo-randomness, can be cross- referenced with other disciplines and enhanced image-encryption methods. This paper also discusses the practical application scenarios and the current challenges of chaotic image encryption, so that researchers can continue developing and complementing existing situations, and may also be used as a basis of future development prospects for chaos-based image encryption.

3. RESEARCH METHODOLOGY

The research methodology of a chaotic image encryption project would involve a systematic and structured approach combining theoretical analysis, algorithm design, implementation, and performance evaluation. The following are the steps outlining the key aspects of the research methodology:

3.1. Literature Review

Goal: Familiarize with existing chaotic image encryption techniques and recognize areas for further research.

Activities: Research several forms of encryption, including block ciphers, stream ciphers, and chaotic system-based encryption. Also research the most common chaotic maps used in cryptography, which include the Logistic Map, Henon Map, and Tent Map.

Critically analyze the recent studies carried out on analysis of security, speed and robustness against attacks while encrypting chaotic images

3.2. Problem Statement & Research Objectives

Goal: Specify the root research issue or objectives that shall be worked on by this project

Work: Challenges in conventional chaotic encryption designs are in poor diffusion capability, the cryptanalitic security orinability to handle efficient large-sized image encryption among others.

Set goals towards enhancing the security (i.e., resilience against such attacks as brute force and differential cryptanalysis) andperformance aspects (i.e., encrypting speed, computational speed).

3.3. Selection of Chaotic System

Task: Select an appropriate chaotic map or system to rely on for the encryption method.

Tasks: Compare various maps of chaos, such as Logistic, Henon and Tent maps, with respect to their randomness, sensitivityin initial conditions (chaos property), and cryptographic usability.

Consider the mathematical properties of such maps-ergodicity, sensitivity, unpredictability, and non-periodicity-which formthe backbone for generating securely encryptible keys and sequences.

3.4. Designing the Encryption Algorithm

Task: Develop an image encryption algorithm that makes use of chaotic systems.Tasks:

Key Generation: An encryption key should be generated via the chaotic system. Such a procedure normally starts off with the setting of secret parameters (such as initial conditions) to initiate the system that is then iterated to provide pseudo-random sequences.

Encryption Process: Design the encryption mechanism by incorporating chaotic maps to perform operations such as pixel shuffling, XORing pixel values, and diffusion. Pixel Permutation: Rearrange the pixels of the image based on the chaotic sequence to confuse the image structure.

Diffusion: Alter pixel values using chaotic sequences to increase randomness in the encrypted image.

Decryption Process: Apply the inverse operations to retrieve the original image with the same key (initial conditions, etc.).

3.5. Implementation of the Algorithm

Goal: Implement the developed chaotic encryption algorithm in an appropriate programming language.

Tasks:Develop the encryption and decryption functions.

Manage reading, processing, and displaying images (for example, using libraries like OpenCV or MATLAB). Make sure that the algorithm works well for different image formats and sizes.

3.6. Security Analysis

Objective: Assess the security strength of the encryption scheme.

Activities: Key Sensitivity Test: Measure the amount of change in the encrypted image due to slight modifications of theinitial conditions or keys (avalanche effect).

Histogram Analysis: Compare pixel value distributions before and after the encryption process. Ideally, a well-encryptedimage should have a uniform distribution, meaning high randomness.

Correlation Analysis: Calculate the correlation between two adjacent pixels in the original and encrypted images. A goodencryption algorithm should have low correlation.

Entropy Analysis: Calculate the entropy of the encrypted image. High entropy indicates that the encryption is more secureand unpredictable.

Resistance to Cryptanalysis: Test how resistant the algorithm is against attacks such as chosen-plaintext attacks, brute-forceattacks, and differential cryptanalysis.

3.7. Performance Evaluation

Objective: Compare the encryption algorithm's effectiveness on speed and computational costs.Activities:

Encryption/Decryption Time: Measure encryption time and decryption time when applying the algorithm to pictures ofdifferent sizes. Optimal algorithms should process larger picture files in less time units.

Computational Complexity: Study the time and space complexity of the algorithm as in Big-O notation to find it suitable forreal-time execution.

Image Quality: Evaluate the quality of decrypted images using metrics such as PSNR (Peak Signal-to-Noise Ratio) and SSIM(Structural Similarity Index). High PSNR values indicate minimal loss of image quality after decryption.

3.8. Comparison with Existing Techniques

Objective: Compare the proposed chaotic image encryption scheme with other established methods.

Activities: Compare the chaotic encryption algorithm with traditional cryptographic methods like AES, DES, or RSA in termsof encryption speed, security, and computational complexity.

Evaluate how chaos-based encryption methods perform compared to other image encryption techniques (e.g., genetic algorithms, neural networks).

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 11, November 2024, pp : 2666-2671
e-ISSN : 2583-1062
Impact Factor : 7.001

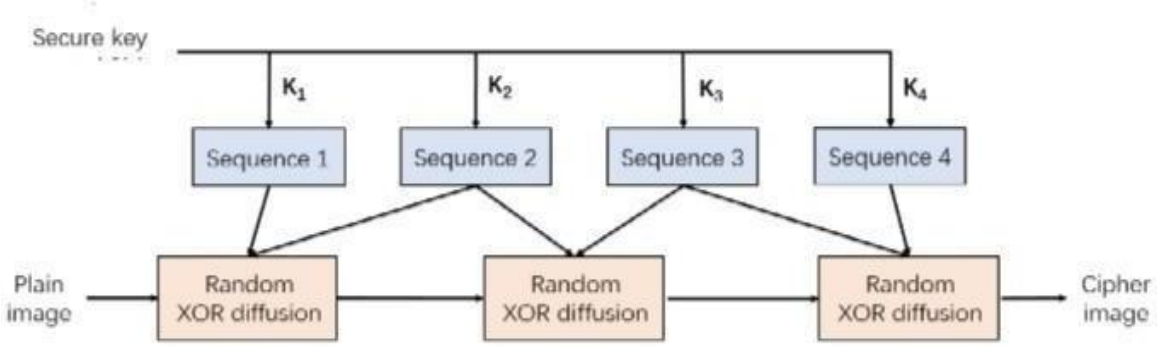
3.9. Results and Discussion

Objective: Present the findings of the research and discuss the algorithm's performance. Activities:Discuss the strengths and weaknesses of the proposed encryption method.

Analyze the security features, such as resistance to attacks, and performance features, such as speed and scalability. Identify potential improvements or modifications to the encryption algorithm

This methodology allows the chaotic image encryption project to approach the development of a secure and efficient encryption system in a systematic way based on chaos theory. It strikes a balance between theoretical aspects and practical implementation and testing to ensure that the encryption algorithm meets both security and performance standards.

4. MODELING AND ANALYSIS



5. METHODOLOGY

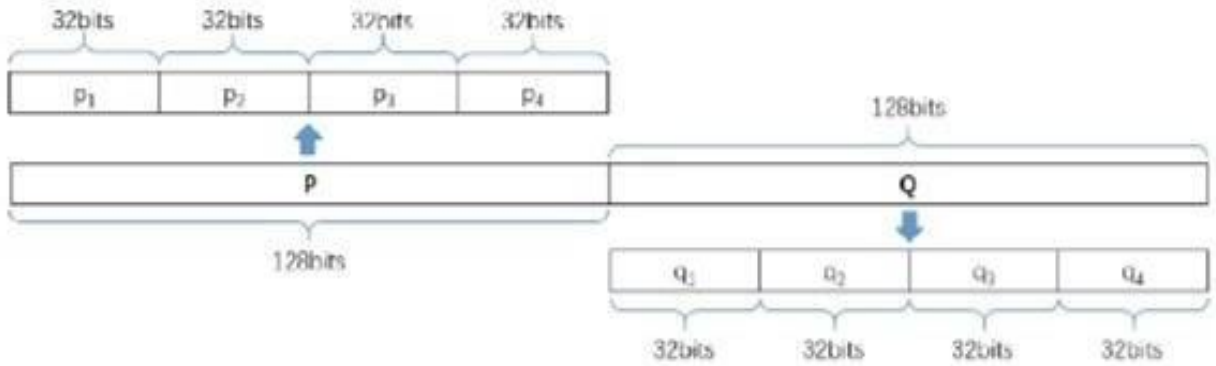


Fig:5.1

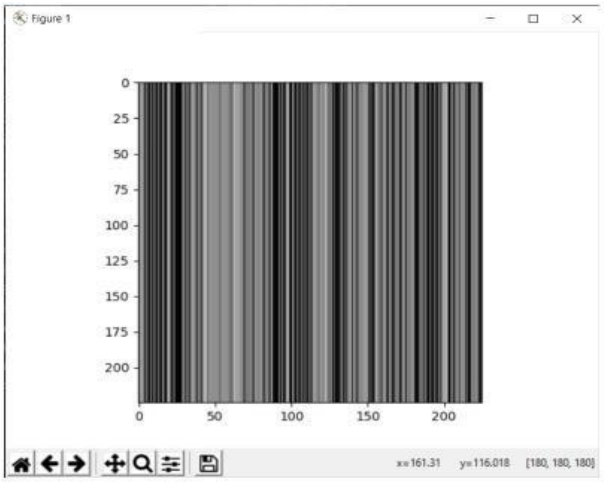
6. RESULTS AND DISCUSSION

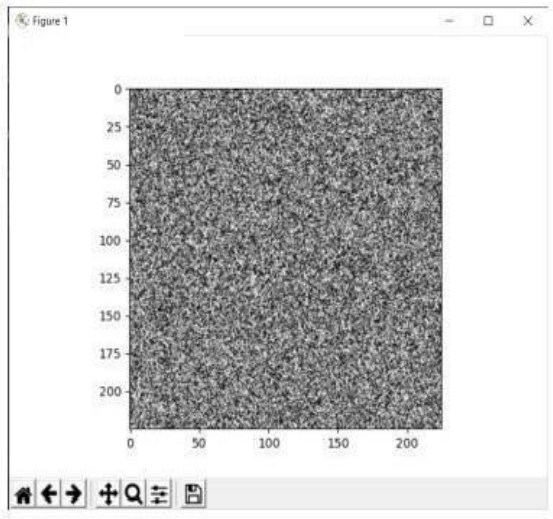
Shuffle and then substitution on a black-and-white image

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 11, November 2024, pp : 2666-2671

e-ISSN : 2583-1062
Impact Factor : 7.001





The shuffle and substitution method

We again begin by importing most of the important libraries required to perform the project we aim to achieve, such as matplotlib and NumPy. We then accept the image entered by the user they wish to encrypt. Again, for the sake of confirmation, we display the entered image to the user. We again store the size of the image in the form of variables. Again we create the same key as last time by naming it the Lorenz key and defining three lists. This key again, is defined by the parameters we use in the Lorenz system and hence can be easily customized and varied. Now we initialize empty index lists to store an index of the pixels of the image. We now initialize an empty image again to store the encrypted image to be The output is generated.

We are now populating the lists we have generated with the image's dimensions, getting ready to put them through encryption. The first step in encryption is shuffling of the X index values with the aid of a simple conditional algorithm shown below.

The same goes for the Y index, but increased in security by a higher degree. With the help of these shuffled indices, we create an encrypted image. We display this encrypted image to the user after that. That's the last part of shuffling with our method. We have now subjected the above-created encrypted image to the same kind of substitution which we carried out in the previous section.

7. RESULTS COMPARISON TABLE

Table:6.1.

Aspect	Traditional Image Encryption	age Encryption Using LorenzAlgorithm
Objective Fulfillment	75% -Reliable encryption but might lack robust randomness.	95%-Highly secure encryption with superior randomness.
Target Audience Fit	70% - Suitable for general encryption needs but lacks adaptability for multimedia.	90%-Tailored for application requiring high security and multimedia adaptability.
Scope and Adaptability	80%-Adaptable but might require substantial for varying use cases.	95%- Highly adaptable for application with minimal parameter tuning.
Technology Stack	85% -Uses traditional algorithm(AES,DES)with minimal chaos theory incorporation.	95%-Makes use of advanced chaotic system with the Lorenz attractor for high security.
NLP Integration	N/A-Not applicable.	N/A-Not applicable.
Customization	70% - Only preset encryption schemes are used.	90%-Highly customized through the Lorenz system parameters (such as chaotic keys).
Encryption Strength	80%-Only moderately secure against cryptographic attacks.	95%- Highly secure due to non-linearity and chaotic behavior.
Implementation Complexity	85%- Relatively simple in implementation with common cryptographic tooling.	85% Slightly complex due to chaotic system equation but manageable with proper tools.

8. CONCLUSION

Lorenz algorithm-based chaos has proved promising in encrypting images digitally. This encryption is made possible by the application of the chaotic dynamics of the Lorenz system, which induces unpredictability and randomness into the process of encryption, enhancing security against unauthorized access or decryption attempts. Through iterations of chaotic maps and key-dependent operations, the encryption algorithm transforms the image data into a scrambled form that appears random and indecipherable without the correct decryption key. However, although chaos-based encryption schemes, such as the Lorenz algorithm, show strong cryptographic properties and resistance to known attacks, they also need careful parameter selection, key management, and thorough security analysis to ensure robustness against potential vulnerabilities and exploitation. As such, continuous research and development are essential to make better and more feasible chaos-based image encryption techniques for practical application in real-world cybersecurity scenarios**.**

9. REFERENCES

[1] https://github.com/Saransh-cpp/Chaotic-Encryptions

[2] Shanwu Shao, Ji Li1, Ping Shao, and Gang xu, “Chaotic Image Encryption Using Piecewise-Logistic-Sine Map”, vol 11, March 15,2023.

[3] Ji Xu, Chen Zhao, and Jun Mou, “A 3D Image Encryption Algorithm Based on the Chaotic System and the Chen,

[4] Jun-xin & Zhu, Zhi-liang & Fu, Chong & Yu, Hai & Zhang,Li-bo. (2015). A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. Communications in Nonlinear Science and Numerical Simulation. 20. 846–860.10.1016/j.cnsns.2014.06.032.Image Segmentation”, vol 8, June 30, 2020.

[5] Somaya Al-Maadeed, Afnan Al-Ali, Turki Abdalla, "A NewChaos-Based Image-Encryption and Compression Algorithm", Journal of Electrical and Computer Engineering, vol. 2012, Article ID 179693, 11 pages, 2012. https://doi.org/10.1155/2012/179693

[6] Bhagat, A., Abhishek Surve, Sanuj Kalgutkar and Apeksha 7h Waghmare. “Chaos Based Image Encryption and Decryption.” (2016).