IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Dynamic Image Encryption Using Chaotic Maps And Scanning

Dr. Sahana Salagare, Avinash P, Chethan N, Nithish Gowda K J , Vinith P
Assistant Professor, Department of Artificial Intelligence and Machine Learning, KSIT, Bengaluru, India
Students Department of Artificial Intelligence and Machine Learning, KSIT, Bengaluru, India

Abstract: The superior breadth of data transmission through the internet is rapidly increasing in the current scenario. The images are really critical in Banking, Military, Medicine, etc, especially, in the medical field as people are unable to travel to different locations, they rely on telemedicine facilities available. All these areas hold equal importance vulnerable to intruders. So, to prevent such an act, encryption of these data can be accomplished through images. using chaos encryption. Chaos Encryption has made significant strides in the realm of Secure Communication. Its distinctive features provide a level of security that surpasses traditional algorithms. Numerous straightforward chaotic maps can be utilized for encryption purposes. In this study, we initially employ the Henon chaotic map for encryption. A comparison of this algorithm with standard algorithms is also presented. Additionally, a security assessment is conducted to demonstrate the algorithm's strength. Various existing versions, along with some novel combinations, are compared to determine if a new configuration could yield improved results. The simulation findings indicate that the proposed algorithm is both robust and user-friendly for this application. Moreover, a new combination of the map has been identified for use in this application.

Keywords: Data Transmission, Chaotic Encryption, Scan Pattern, Security Analysis

I. Introduction

In the present digital realm, the authorized access to digital information is of paramount importance. Communication through social media and other private platforms requires some privacy which could be established by a simple method called encryp- tion [1]. Fast and efficient encryption schemes are necessary to do the same. There are many real- life examples that require the application of encryption. In tele-medicine, especially when we see the current pandemic situation, patient’s data from one place is digitally transferred to a specialist located at another part of the world. Similarly, in banking, military and other technological fields, security of transmission is a prime0020concern. Exceptional performance of chaotic systems manifested it in various applications [2]. One such example is encryption. While there are numerous traditional encryption algorithms like AES and DES, their effectiveness in image encryption diminishes due to value redundancy, large data volumes, and pixel correlation. This led to the exploration of chaotic systems, which are recognized for their dynamic behaviors and sensitivity to initial conditions and control parameters. Many algorithms have been introduced over time [3], showcasing impressive theoretical capabilities, though many remain confined to theoretical ideals. This study demonstrates image encryption using a single Henon chaotic map and includes a related security analysis conducted on the MATLAB platform. A comparative analysis of the algorithm against various noise types is also performed. Finally, the algorithm's response to modified versions is assessed to determine which version performs more effectively.

Numerous methods are currently available for the encryption and decryption of multimedia data across 1D, 2D, and 3D formats. Image encryption techniques are regularly examined to fulfill the need for real-time security of information during online data transfers. The traditional algorithm, known as the Data Encryption Standard (DES), has several drawbacks, including low efficiency when handling large multimedia files, as it is primarily designed for general data encryption rather than multimedia content. Chaotic encryption has been proposed as a fast and highly secure method for encryption.

The various usages of this image encryption method are:

1. Medical imaging systems
2. Secure video calls
3. Military image archives
4. Online personal photo collections
5. Cable television, and more

In this proposed image encryption strategy, a 32-bit external secret key, a chaotic logistic map, and a DNA encoding technique are incorporated. The initial conditions for the logistic map are derived from the external secret key by performing logical operations on all its bits and then encoding them into a DNA sequence. Additionally, the encryption procedure involves processing the input image alongside the key image, resulting in the final encrypted output.

II. LITERATURE REVIEW

It plays a vital role in secure communication, safeguarding images from unauthorized access. Over time, different encryption techniques have been employed, including conventional cryptographic methods, transform-based strategies, and chaos-based encryption

[1] Chaotic Map-Based Image Encryption And Related Analysis

Chaos Encryption has made significant strides in the realm of Secure Communication. Its distinctive features provide a higher level of security compared to traditional algorithms. Several straightforward chaotic maps can be employed for encryption purposes. In this paper, the Henon chaotic map is initially utilized for encryption. A comparison with conventional algorithms is also presented. Finally, a security evaluation is conducted to demonstrate the algorithm's robustness. Additionally, various existing methods and some new variations are assessed to determine if a novel combination can yield improved outcomes. The simulation results indicate that the proposed algorithm is both resilient and user-friendly for this application.

[2] Exploring the Efficacy of Image Encryption using Independent, Combined, and Improved Chaotic Maps

Securing sensitive data and protecting the privacy of images are of utmost importance in image transmission systems. Due to their inherent complexity, sensitivity to the initial conditions, and random-like behavior, chaotic maps have become effective tools in image encryption algorithms. These maps act as a foundation for generating random numbers used in data concealment, key generation, and encryption.

The use of chaotic maps in image encryption has several benefits. They are predictable since their deterministic nature ensures that the same input consistently produces the same output. Furthermore, chaotic maps produce sequences with high Entropy, uniform distribution, and resistance to various attacks thanks to their excellent statistical features. Additionally, they offer extra security by adding a certain level of randomness to image encryption systems, which makes them resistant to brute- force assaults and other traditional cryptanalysis techniques

[3] Image Encryption and Decryption Using Chaotic Logistic Maps and DNA-Based Encoding

Many different encryption methods have been introduced, each with its unique benefits and drawbacks. One such method is the chaos-based cryptographic algorithm, which is touted for its effectiveness in image encryption. This approach is regarded as advantageous due to its rapid processing speed, adequate computational efficiency, and robust security features. While this system exhibits some chaotic characteristics, its behavior is ultimately deterministic. By specifying an initial value and its parameters, we can create a confusion matrix that is highly sensitive to those initial conditions. In this study, we also incorporate a DNA encoding technique that enhances the encryption's complexity and randomness. This method involves transforming pixel values into a DNA sequence composed of the nucleic acid bases A, T, G, and C. We propose a novel strategy for encrypting images that combines chaotic logistic mapping with DNA encoding to achieve a securely encrypted image.

Currently, numerous techniques exist for the encryption and decryption of multimedia data across one-dimensional, two-dimensional, and three-dimensional formats. Researchers frequently examine image encryption methods to address the need for real-time information security during internet data transfers.

Traditional algorithms, such as the Data Encryption Standard (DES), have notable limitations, including low efficiency with large multimedia files, and are primarily designed for data encryption rather than multimedia applications. In contrast, chaotic encryption is suggested as a swift and highly secure technique for this purpose.

III. SYSTEM ARCHITECTURE AND METHODOLOGY

In this work, first of all the encryption and decryption using the original version of chaotic map is done. Followed by which an analysis of the same under different noise conditions are analyzed. After this, different versions are reviewed. But it is always desired to find a better chaotic combination for this application. So for that a combination of these three single chaotic maps are defined and simulated. Pixel Permutation Using Scan Patterns: A predefined scan pattern (Hilbert, Peano, Zigzag, or Morton) is applied to rearrange pixel positions, breaking spatial correlations and increasing security. Diffusion Using a Chaotic Map: A Logistic-Sine Chaotic Map (LSCM) generates a pseudo-random sequence to modify pixel intensities using an XOR operation, ensuring high randomness and key sensitivity. The decryption process follows the reverse steps, ensuring accurate image reconstruction with the correct key. Security analysis, including histogram analysis, correlation tests, NPCR, UACI, and entropy evaluation, demonstrates that the suggested approach provides strong resistance against statistical and differential attacks while maintaining computational efficiency.

In the suggested technique, as depicted in Fig. 2, the input image is first transformed into a monochrome version. This monochrome image is then adjusted to a standardized format, modifying the intensity values as needed. Subsequently, a mathematical mapping function is utilized to produce a random encryption key. This key is then combined with the standardized image using a bitwise XOR operation, ultimately generating a protected output. The quality and strength of encryption are compared for all 1D chaotic, hybrid, and improved maps. 1D chaotic maps are a helpful tool. Their simplicity and comp006Cex behavior make them adaptable and widely valuable for various scientific, engineering, and computing domains. Different chaotic maps can be combined to produce hybrid maps or existing ones can be altered. The advantages of hybrid maps include enhanced behavior, security, statistical properties, and performance. Improved maps are created to solve shortcomings or specific problems with existing chaotic maps. Enhanced maps are being developed to strengthen chaotic qualities, obtain better statistical properties, boost security, and investigate novel dynamics and applications.

VI. REVIEW OF IMPLEMENTATION AND RESULTS

Securing digital images is crucial to prevent unauthorized access, maintaining both confidentiality and protection. Unlike encrypting text, safeguarding images demands unique methods because of their high redundancy and the strong interconnection between adjacent pixels.

1. Chaotic Map for Diffusion.

A chaotic map is a mathematical model that produces sequences highly dependent on initial values, exhibiting extreme sensitivity to small changes. This property makes chaotic maps ideal for encryption, as even a small change in input values leads to completely different outputs.

Several methods for image encryption:

Logistic Map: A straightforward yet powerful approach for generating chaotic sequences with strong randomness.

Henon Map: A two-dimensional chaotic system that produces complex, unpredictable sequences.

Arnold’s Cat Map: Mainly used for image scrambling, this method alters pixel positions in a structured but highly unpredictable way.

In this approach, a chaotic map generates a sequence that modifies pixel values, ensuring that the encrypted image looks entirely distinct from the original.

2. Scan Pattern for Permutation

A scan pattern determines how pixels are rearranged before encryption. Rearranging pixel positions reduces redundancy and enhances security. Common scan patterns include:
Zig-Zag Scan: Moves diagonally across the image, scattering adjacent pixels.
Spiral Scan: Starts from the center and moves outward in a circular pattern, ensuring even distribution.
Morton Scan: Arranges pixels in a Z-shaped pattern, improving randomness.

By applying a scan pattern, the structure of the image is disrupted, making it harder for attackers to identify patterns.

3. Encryption Process

It contains two main steps: permutation and diffusion.

Step 1: Image Preprocessing: Convert the image to grayscale (if required). Normalize pixel values within the required range.

Step 2: Generate Chaotic Sequence: Select an initial value and parameters for the chaotic map. Generate a pseudo-random sequence of numbers. Normalize the sequence to match pixel intensity values.

Step 3: Apply Scan Pattern for Permutation: Rearrange pixels according to the selected scan pattern. Store the mapping of pixel positions for later decryption.

Step 4: Apply Chaotic Diffusion: Modify pixel values using the chaotic sequence. Perform an encryption operation such as bitwise XOR or modular addition. The resulting encrypted image looks entirely unrecognizable compared to the original.

4. Decryption Process

Decryption follows the reverse steps:
Regenerate the chaotic sequence using the same initial conditions.
Apply inverse diffusion to retrieve permuted pixel values.
Apply inverse scan pattern to restore the original pixel arrangement.

The original image is accurately restored. Due to the extreme sensitivity of chaotic maps to initial conditions, even a slight variation in the key prevents proper decryption, reinforcing robust security.

5. Security Analysis

Histogram Analysis: A well-encrypted image has a uniform histogram, meaning pixel values are evenly distributed. This prevents statistical attacks, as no useful patterns can be extracted.
Correlation Coefficient Analysis: In a non-encrypted image, pixels that are close to each other tend to have similar values. Once the image is encrypted, the correlation between neighboring pixels should be reduced. This prevents an attacker from deducing any information by analyzing adjacent pixels.
Key Sensitivity Analysis: The encryption method is extremely sensitive to the initial conditions of the chaotic map. A slight alteration in the key can lead to a vastly different encrypted image. This characteristic offers strong protection against brute-force attacks, meaning even an almost accurate guess of the key won't successfully decrypt the image.
Pixel Change Rate and Intensity Analysis: An effective encryption technique guarantees that altering just one pixel in the original image will cause significant changes in the encrypted output. This feature prevents attackers from making small alterations and observing consistent results.

6. Performance Evaluation

The encryption method is evaluated based on:

Execution Time: The time taken to encrypt and decrypt an image should be minimal for practical applications.

Memory Usage: The encryption algorithm should be efficient in terms of computational resources.

Image Encryption:

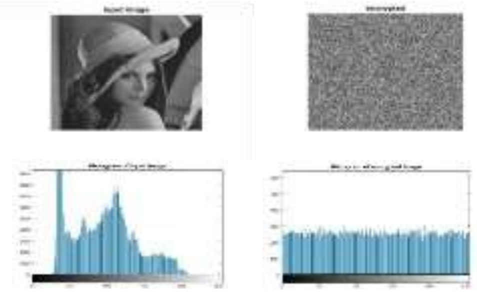
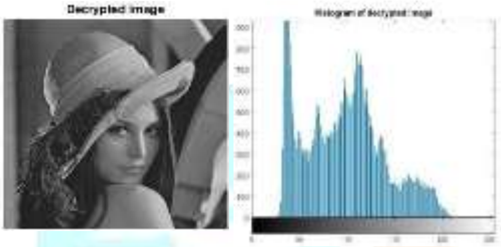


Image Decryption



VII. Conclusion

Investigating several chaotic systems performance analyses in 1D, combined, and improved scenarios has yielded necessary knowledge about their effectiveness and future uses. Correlation, histogram and Differential analysis prove that the Logistic map, Tent map, and Sine map are better than the other maps. Overall, comparing all three domains, these maps give better encryption. As a result, this approach can be applied to various use cases as required.

Moving forward, key generation will be enhanced by combining three one- dimensional chaotic systems along with advanced hybrid chaotic models to further improve the efficiency and security of image encryption.

VIII. References

[1] S. J. Sheela, “Image encryption based on modified Henon map using hybrid chaotic shift transform”, Springer Science Business Media, LLC, part of Springer Nature 2018.

[2] Mohamed Zakariya Talhaoui, “Fast image encryption algorithm with high security level using the Bu¨lban chaotic map”, Springer-Verlag GmbH Germany, part of Springer Nature 2020

[3] J. Gayathri, “A survey on security and efficiency issues in chaotic image encryption”, Int. J. Information and Computer Security, Vol. 8, No. 4, 2016.

[4] Jai Ganesh Sekar and Dr. C. Arun “Comparative Performance Analysis Of Chaos Based Image Encryption Techniques”, Journal of Critical Reviews ISSN- 2394-5125 Vol 7, Issue 9, 2020.

[5] Mousa Farajallah, Safwan El Assad and Olivier Deforges “Fast and secure chaos-based cryptosystem for images” International journal of bifurcation and chaos in applied sciences and engineering , World Scientific Publishing, 2016.

[6] Yaghoub Pourasad ,“A New Algorithm for Digital Image Encryption Based on Chaos Theory”, MDPI 2021.

[7] Lidong Liu, “A Fast Chaotic Image Encryption Scheme With Simultane- ous Permutation-Diffusion Operation”, IEEE Access February 5,2020.

[8] Alireza Arab and Mohammad Javad Rostami, “An image encryption method based on chaos system and AES algorithm”, The Journal of Supercomputing (2019).

[9] Hao Li and Lianbing Deng "A Robust Image Encryption Algorithm Based on a 32-bit Chaotic System", IEEE ACCESS January 2020.

[10] Shuqin Zhu and Congxu Zhu, "Secure Image Encryption Algorithm Based on Hyperchaos and Dynamic DNA Coding", MDPI Entropy 2020.