INTERNATIONAL JOURNAL FOR ENGINEERING RESEARCH

International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

IJIEMR Transactions, online available on 21th Dec 2024. Link

https://ijiemr.org/downloads.php?vol=Volume-13&issue= Issue12

DOI:10.48047/IJIEMR/V13/ISSUE12/71

Title: " COLOR IMAGE ENCRYPTION USING 2D SINE COSINE COUPLING MAPS"

Volume 13, ISSUE 12, Pages: 527 - 533

Paper Authors

P. Eswara Vara Prasad, U. Sumanth

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COLOR IMAGE ENCRYPTION USING 2D SINE COSINE COUPLING MAPS

P. Eswara Vara Prasad, U. Sumanth

Department of ECE, CMR Institute of Technology, Medchal, Hyderabad, Telangana, India.

Correspondence mail: usumanthsagar2003@gmail.com, prasade885@gmail.com

ABSTRACT:

In this paper, the authors propose a new two-dimensional sine-cosine coupling chaos map (2D-SCCM) and evaluate its performance through various methods such as trajectory distribution maps, Lyapunov exponents, sample entropy, and sequence sensitivity. The results indicate that the 2D-SCCM exhibits superior randomness and ergodicity compared to existing two-dimensional chaotic systems. Additionally, it demonstrates a wider hyperchaotic range, making it a promising candidate for practical applications.To test its practical use, the authors integrate the 2D-SCCM into a color image encryption algorithm. The process begins by combining a plain image with a hash function to generate a key. Then, random sequences produced by the 2D-SCCM and the Arnold map are used to construct substitution boxes (S-Boxes). The final encryption algorithm utilizes these S-Boxes alongside the chaotic map and hash function to encrypt the image.

Experimental results and security tests show that the proposed encryption algorithm is highly efficient, with strong security features. The algorithm effectively protects images against various types of attacks, demonstrating its potential for safeguarding sensitive image data. This work highlights the potential of the 2D-SCCM in cryptographic applications, particularly in the context of image encryption, where both high efficiency and robust security are crucial. The combination of chaotic systems and cryptographic techniques offers a promising approach to enhancing image protection.

INTRODUCTION

The rapid development of modern network technology has made the use of images for information transmission increasingly common, leading to growing concerns about image security. To protect image information, various techniques such as data hiding, watermarking, and image encryption have been proposed. Among these, image encryption stands out as one of the most straightforward and effective methods. However, due to the high redundancy and strong correlation between image pixels, image encryption differs from text encryption, making it more complex. Traditional encryption schemes like AES and DES, while effective, tend to be inefficient for image encryption, requiring a lot of time to process images.

In response, researchers have developed alternative image encryption methods that include techniques like image filtering, DNA coding, frequency domain transform, and chaotic systems. Chaotic systems, with their unique characteristics such as high sensitivity to initial conditions and internal randomness, have become particularly popular for image encryption. Since the first application of chaotic systems in image encryption by J. Fridrich, numerous schemes based on chaotic systems have been proposed. For example, Wu et al. used a combination of chaotic sequences and DNA coding for image diffusion and scrambling. Despite their advantages, some of these schemes have been shown to be insecure due to the simple nature of one-dimensional chaotic maps, which have small key spaces and predictable chaotic orbits.

To address these shortcomings, this paper proposes a new two-dimensional chaotic map called 2D-SCCM. This system improves upon one-dimensional chaotic maps by introducing a cosine function, resulting in a more complex chaotic behavior and a larger key space. The 2D-SCCM is analyzed through various methods, including Lyapunov exponents and sample entropy, which demonstrate its better randomness and ergodicity. The paper then presents a color image encryption algorithm based on this map.

Block Diagram

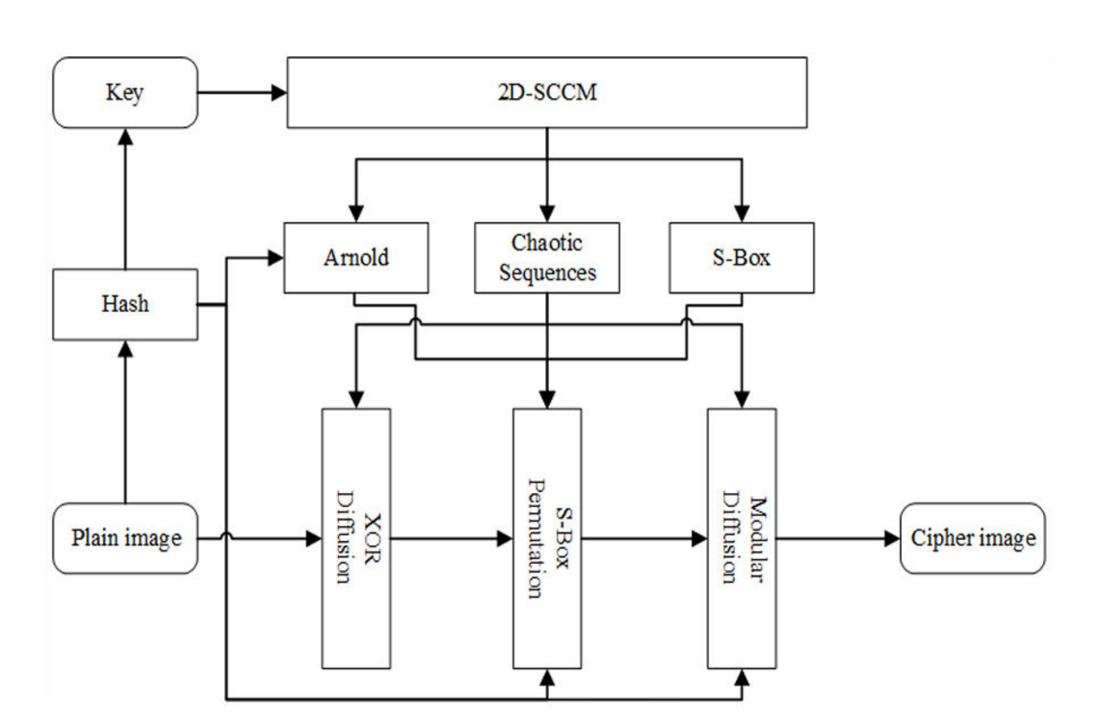

Figure 1: Block Diagram of the Overall Encryption Algorithm

The block diagram of an overall encryption algorithm illustrates the essential components and flow of data during the encryption process. At the start of the process, the plaintext—which is the original data or message—serves as the input to the encryption system. This is the information that needs to be protected. In many encryption algorithms, a cryptographic key is required to transform the plaintext into ciphertext (the encrypted form). The key is either generated by a specific algorithm, derived from a user input (e.g., a password), or shared between parties in secure key exchange protocols.

Once the key is available, the core component of the encryption process, the encryption function, comes into play. The encryption function applies a series of mathematical or logical operations to the plaintext using the key. This function might involve multiple steps, such as substitution (where each part of the plaintext is replaced with another element), permutation (where the data is shuffled or rearranged), or mixing (where the plaintext and key are combined in complex ways). These operations aim to transform the plaintext into ciphertext, which appears random and unrecognizable without the appropriate key.

The ciphertext is the result of this transformation and is the version of the data that is transmitted or stored. Since the ciphertext is unreadable without the key, it ensures that the data remains secure even if intercepted. On the receiving end, the ciphertext is passed through the decryption function, which reverses the encryption process. The decryption function uses the key (the same key in symmetric encryption or a different key in asymmetric encryption) to retrieve the original plaintext from the ciphertext.

In symmetric encryption systems, the same key is used for both encryption and decryption, while in asymmetric encryption, two different keys are used: a public key for encryption and a private key for decryption. The security of the entire encryption process hinges on the effective management of the key, which includes ensuring its secure generation, distribution, and storage. This process is typically handled by a key management system to prevent unauthorized access to the key, thus maintaining the integrity and confidentiality of the encrypted data.

The overall flow of the encryption algorithm involves taking the plaintext and, using the appropriate key, applying the encryption function to generate ciphertext. Later, the decryption function, using the corresponding key, reverts the ciphertext back to the original plaintext. This fundamental process ensures that sensitive data remains secure during transmission or storage, protected from unauthorized access.

Literature Review

Xinjun Zhang, Shuqing Zhang, "Color image encryption based on improved Henon hyperchaotic mapping", 2024 3rd International Conference on Robotics, The paper "Color Image Encryption Based on Improved Henon Hyperchaotic Mapping" by Xinjun Zhang and Shuqing Zhang, presented at the 2024 3rd International Conference on Robotics, Artificial Intelligence, and Intelligent Control (RAIIC), focuses on enhancing the security of color image encryption by utilizing an improved Henon hyperchaotic map. The paper addresses the vulnerabilities of traditional image encryption methods that struggle with high redundancy and pixel correlation inherent in images. The authors propose an improved Henon hyperchaotic system that introduces greater unpredictability and complexity in the chaotic behavior, which is crucial for ensuring stronger encryption. This improved map is employed to generate chaotic sequences used in the scrambling and diffusion phases of the encryption algorithm.

The paper demonstrates that the enhanced encryption method offers better resistance to attacks, such as differential and statistical analysis, compared to conventional encryption methods. Experimental results show that the proposed approach achieves high encryption efficiency while effectively safeguarding color images from unauthorized access. By improving the Henon map, the method provides enhanced randomness, making it difficult for potential attackers to decode the encrypted images. The research contributes to the field of image security by presenting an efficient and robust encryption technique that can be applied in various fields, including secure communication, data protection, and cloud storage, where the confidentiality of visual data is critical.

Furthermore, the paper highlights the advantages of using chaotic systems like the improved Henon hyperchaotic map in the context of color image encryption. The authors demonstrate that the inherent sensitivity to initial conditions and the wide range of chaotic behaviors offered by the enhanced Henon map make it ideal for generating unpredictable and complex chaotic sequences. These sequences are then used for pixel scrambling and diffusion, which help disrupt the spatial and statistical patterns within the image, ensuring that the encrypted image appears as random noise. This significantly increases the difficulty of recovering the original image without knowledge of the encryption key. Additionally, the paper compares the proposed method with existing encryption techniques, showing that it outperforms them in terms of security, efficiency, and robustness. The study suggests that chaotic-based image encryption techniques, such as the one presented in this work, hold significant promise for providing high-level security in modern applications where visual data protection is essential.

Result

In this paper, we propose a new two-dimensional discrete chaotic system, called 2D SCCM, which is designed based on the study of the Logistic map and the cosine function. In order to better evaluate the chaotic behavior of the proposed system, we use various testing methods, including trajectory distributionmap, Lyapunovexponent, sampleentropy, sequencesensitivity. And the randomness of the generated time series was examined by using the NIST test tool. Experimental results and comparative analyses show that the 2D-SCCM has a wider hyperchaotic interval, more complex chaotic behavior, and

better ergodicity compared to some existing chaotic systems.

In addition to the superior chaotic behavior, the 2D SCCM system also demonstrates enhanced sensitivity to initial conditions, a key characteristic of chaotic systems. This sensitivity ensures that even small changes in the initial state lead to significantly different outcomes, making the system highly unpredictable. This trait is crucial for applications like encryption, where unpredictability and the ability to generate unique, non-repetitive sequences are essential. The robustness of the system, as evidenced by the variety of tests applied, confirms that it can produce high-quality chaotic signals with excellent randomness properties, making it a promising candidate for secure communication and cryptographic applications.

Furthermore, the comparative analysis of the 2D SCCM with other chaotic systems highlights its ability to maintain stability over a wider range of parameters while still exhibiting complex dynamics. This feature makes the 2D SCCM more adaptable to varying conditions, providing greater flexibility in its use. The system's broader hyperchaotic interval indicates that it can generate a wider spectrum of chaotic behaviors, enhancing its potential for real-world cryptographic implementations where diverse chaotic states are beneficial. Overall, the 2D SCCM presents a highly efficient and scalable chaotic system with improved performance in key areas, such as security, unpredictability, and versatility.

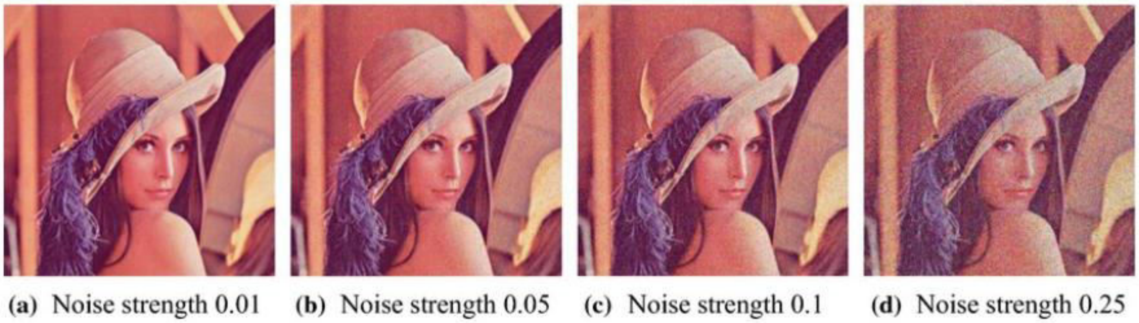
(a) Noise strength 0.01 (b) Noise strength 0.05 (c) Noise strength 0.1 (d) Noise strength 0.25

Figure 2: The decryption results with different density noises

CONCLUSION

Building on the 2D-SCCM, the paper proposes a new image encryption algorithm designed to secure color images. The algorithm consists of four main stages: key update, XOR-diffusion, pixel scrambling combined with substitution using an S-Box, and modular diffusion. The key update is integrated with the plain image, enhancing protection against selective plaintext attacks. The XOR-diffusion and modular diffusion stages effectively alter the pixel values, while pixel scrambling and substitution disrupt the spatial correlation between pixels. This ensures that the encrypted image appears as noise, making it difficult to recover the original image.

Experimental simulations validate the effectiveness of the algorithm, showing that it transforms natural images into unrecognizable, noise-like images. Security analysis confirms that the proposed encryption method is robust against common cryptanalysis attacks. Overall, the paper presents a promising approach for secure image encryption with strong resistance to attacks and efficient performance.

Additionally, the proposed image encryption algorithm leverages the advantages of chaotic systems, particularly the 2D-SCCM, to enhance both the security and efficiency of the encryption process. The chaotic behavior introduced by the 2D-SCCM ensures that even slight changes in the input or key lead to vastly different encrypted outputs, providing strong resistance to attacks such as brute-force and differential cryptanalysis. The combination of key update, XOR-diffusion, pixel scrambling, and substitution offers multiple layers of security, making the algorithm highly resilient to various types of cryptographic attacks. Furthermore, the modular diffusion mechanism contributes to the algorithm’s efficiency by ensuring that the encryption and decryption processes are computationally feasible while maintaining a high level of security. This makes the proposed method a promising candidate for practical applications where both security and performance are critical, such as in secure communication, cloud storage, and digital media protection.

REFERENCES

1. M. Fallahpour, "Reversible image data hiding based on gradient adjusted prediction", IEICE Electron. Exp., vol. 5, no. 20, pp. 76-870, Oct. 2008.

2. C. Wang, X. Wang, Z. Xia and C. Zhang, "Ternary radial harmonic Fourier moments based robust stereo image zero-watermarking algorithm", Inf. Sci., vol. 470, pp. 109-120, Jan. 2019.

3. Z. Hua and Y. Zhou, "Design of image cipher using block-based scrambling and image filtering", Inf. Sci., vol. 396, pp. 97-113, Aug. 2017.

4. Z. Hua, Z. Zhu, Y. Chen and Y. Li, "Color image encryption using orthogonal Latin squares and a new 2D chaotic system", Nonlinear Dyn., vol. 104, pp. 4505-4522, May 2021
.

5. . Wu, X. Liao and B. Yang, "Image encryption using 2D henon-sine map and DNA approach", Signal Process., vol. 153, pp. 11-23, Dec. 2018.

6. Y. Luo, M. Du and J. Liu, "A symmetrical image encryption scheme in wavelet and time domain", Commun. Nonlinear Sci., vol. 20, no. 2, pp. 447-460, Feb. 2015.

7. M. Ramzan, T. Shah, M. M. Hazzazi, A. Aljaedi and A. R. Alharbi, "Construction of S-boxes using different maps over elliptic curves for image encryption", IEEE Access, vol. 9, pp. 157106-157123, 2021.

8. Z. Hua, K. Zhang, Y. Li and Y. Zhou, "Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing", Signal Process., vol. 183, Jun. 2021.

9. J. Arif, M. A. Khan, B. Ghaleb, J. Ahmad, A. Munir, U. Rashid, et al., "A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution", IEEE Access, vol. 10, pp. 12966-12982, 2022.

10. M. A. B. Farah, R. Guesmi, A. Kachouri and M. Samet, "A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation", Opt. Laser Technol., vol. 121, Jan. 2020.