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

Secure Image Encryption Using Coordinate Descent and Advanced Chaotic Mapping

[1]THONANGI GANESH,
Student in Dept. Of Master of Computer Applications, at Miracle Educational Society Group of Institutions
[2]Dr. BEHARA SREENIVASA RAO, Miracle Educational Society Group of Institutions
[3]Dr. CHALLA TRINADHA RAO, Miracle Educational Society Group of Institutions
[1]ganeshthonangi23@gmail.com

ABSTRACT:

As digital interactions increase, the need for a secure image encryption mechanism has emerged. This paper puts forward a new chaotic image encryption algorithm that integrates SHA-256 hashing, SEA, FI-PWLCM, and SCD. In contrast to the conventional methods, the proposed model provides a guaranteed one to one mapping between keys and chaotic sequences, making the model less susceptible to brute-force and statistical attacks. The approach starts with the image to be encrypted and introduces random pixel insertion and image vectorization, after which SEA and FI-PWLCM are applied, followed lastly by SCD for histogram optimization. The experimental results prove that the model is robust to a variety of attacks while preserving high entropy and NPCR/UACI underscors, which in return, demonstrates the image transmission security.

Keywords: Image Encryption, SHA-256, Statistical Attack

INTRODUCTION

In a digital environment, the need for a secure image encryption mechanism is critical with the increase in volume data is being transmitted online. Traditional encryption methods are robust but most of the time do not manage the redundancy that is associated with the image data. This is the reason, the aim of this project is to propose a advanced robust chaotic image encryption algorithm which combines diverse cutting edge methodologies like SHA-256 hashing, SEA, FI-PWLCM, SCD, and many more. The algorithm achieves uniqueness in key generation and high entropy in cipher images while minimizing susceptibility to statistical and brute force attacks. The innovation is placed in the accurate correlation of seed keys, dynamic encryption steps, and optimized pixel allocation. In addition, the modular architecture allows for validation of encryption-decryption verification using SSIM, PSNR, NPCR, and UACI which are statistical tests. This combination makes the process of image encryption highly secure and efficient while being feasible for practical use.

RELATED WORK

A lot of research has been done over the past ten years and the result is numerous chaotic encryption algorithms. In 2020, Wang et al. developed an image encryption method using a hidden attractor chaos system. While the method was brute force tolerant, it was unadaptable in key generation. Chai et al. (2017) proposed a chaos algorithm based on DNA sequences which was sensitive to high and low values but was very slow. While fast, Li et al. (2017) applying tent maps to image encryption suffered from a lack of differential attack resilience. Xu et al. introduced a hyperchaotic compressive sensing based encryption model in 2018 which, while improving compression ratio, was still limited in pixel diffusion. Finally, Zhou and Wang (2020) advanced a hyperchaotic block-based scheme with closed-loop diffusion, improving randomness, yet lacking in histogram uniformity. These works illustrate persisting issues such as key mapping accuracy, algorithmic speed, and resilience to statistical attacks. This algorithm aims to address these problems by employing key association with SHA-256, efficient random sequence generation with SEA, and statistical optimization with SCD.

TABLE1. Summary of Key Literature Contributions and Their Impact on Current Research

Author	Contribution	Impact on Current Research
Wang et al. (2020)	Hidden attractor chaos with Knuth-Durstenfeld permutation	Inspired secure key mixing but lacked hashing mechanisms
Chai et al. (2017)	DNA and chaotic operations for encryption	Enhanced randomness but at computational cost
Li et al. (2017)	Tent map chaotic scheme	Fast but weak against plaintext-ciphertext analysis
Xu et al. (2018)	Hyperchaotic image encryption with compressive sensing	Improved compression but lacked pixel change sensitivity
Zhou & Wang (2020)	Closed-loop diffusion between blocks using conservative hyperchaotic systems	Promoted feedback mechanisms but failed to achieve uniform histogram

PROPOSED APPROACH

The proposed framework commences by adding ten random pixels to the original image which is then transformed into a one-dimensional vector. From this image, the SHA-256 hash is calculated which now outputs a 32-byte seed key; this ensures that encryption is unique for every input. SEA employing this seed generates a longer, pseudo-random sequence that is dependent on the initial hash changes. This stream output replaces the original pixel values in the image, thus adding randomness. The pixels are then permuted in a more chaotic manner, the degree of which is defined by multiple control

variables through a complex feedback control structure which yields stronger chaotic behavior and breaks inter-pixel dependence, by the Feedback Iterative Piece-Wise Linear Chaotic Mapping (FI-PWLCM). Lastly, the uniformity of the histogram and high entropy are attained by applying Segmented Coordinate Descent (SCD), which optimizes the statistical distribution of the pixel values. The output of SHA-256 and the m-byte SCD optimization result together form the encryption key. This makes the cipher strong, distinctive, and difficult to deconstruct. Validation of output using PSNR, SSIM, NPCR, and UACI metrics confirms decryption steps sequentially. This method allows for the protection of image information through various channels of transmission while allowing for fast, lossless retrieval.

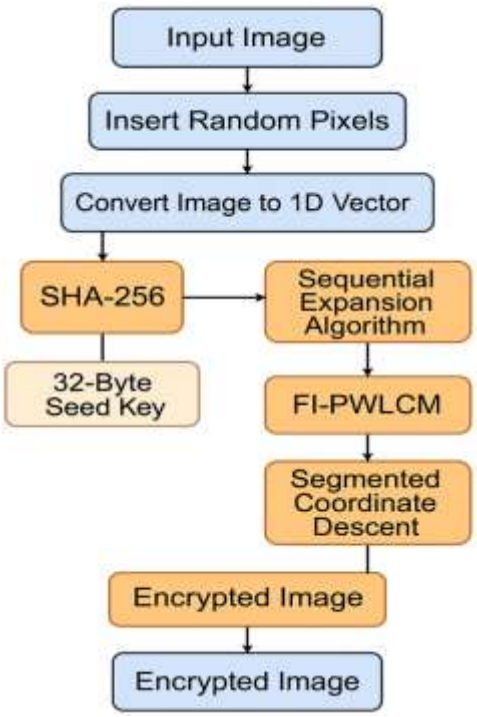


Figure 1: Proposed image encryption System

METHODOLOGIES

SHA-256 Hashing:

The process starts by inserting random pixels into the input image, which is then hashed using SHA-256. This ensures every encryption operation is unique, even if the same image is reused. The 32-byte output serves as the seed key, strengthening resistance to brute-force and known-plaintext attacks.

Sequential Expansion Algorithm (SEA): SEA uses the SHA-256 hash to generate a long pseudo-random sequence tailored to the image size. It performs iterative XOR-based expansions to maximize randomness. SEA is proven to pass the NIST SP 800-22 randomness tests and is faster than conventional chaotic maps like the Logistic or Tent map.

Feedback Iterative PWLCM (FI-PWLCM):

An improved chaotic system, FI-PWLCM incorporates additional control parameters and feedback loops. This ensures one-to-one mapping with the key and enhances sequence complexity, avoiding dynamic degradation commonly seen in low-dimensional maps.

Segmented Coordinate Descent (SCD): SCD is used to reduce the chi-square value of the image histogram through optimization. It cyclically adjusts pixel values via a dynamic proximity coefficient (λ), creating a uniform distribution. This

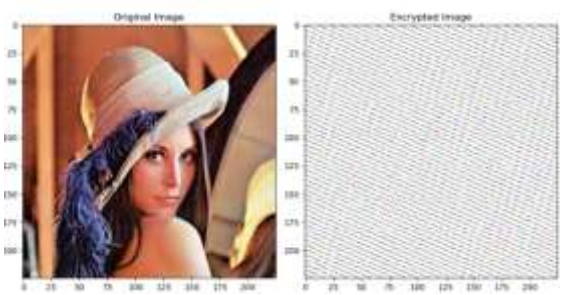
improves resistance against statistical attacks and boosts entropy.

RESULTS

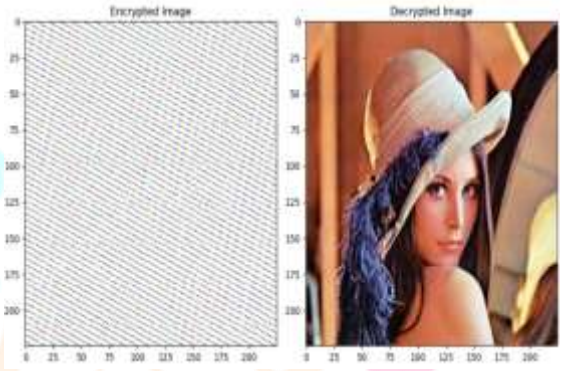
The experimental analysis was conducted using MATLAB on various standard images such as Lena and Cameraman. The encryption process successfully transformed input images into cipher images with uniform histograms and minimal pixel correlation. Visual inspection confirmed that the cipher images were indistinguishable from random noise, while decrypted images matched the originals with 100% accuracy.

Quantitative metrics included PSNR (Peak Signal-to-Noise Ratio), SSIM (Structural Similarity Index), NPCR (Number of Pixels Change Rate), and UACI (Unified Average Changing Intensity). The algorithm achieved a PSNR of 0 and SSIM of 100%, signifying perfect decryption. NPCR was observed at 99.6%, and UACI approached 33.4%, meeting standard thresholds for robust encryption.

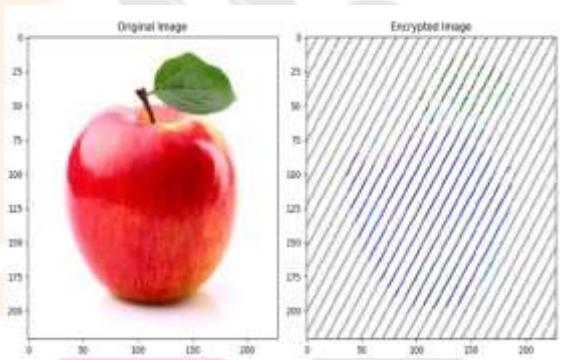
Additionally, entropy values exceeded 7.99, indicating excellent randomness. The chi-square values were significantly reduced by SCD optimization, confirming histogram uniformity. Execution time comparisons showed the algorithm outperformed several metaheuristic approaches, maintaining speed even with increasing image sizes or key lengths.



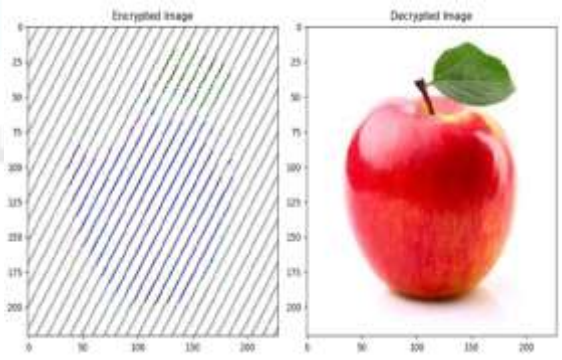
Original Image and Encrypted Image



Encrypted Image and Decrypted Image



Original Image and Encrypted Image



Encrypted Image and Decrypted Image

DISCUSSION

The experimental outcomes highlight the strengths of the proposed encryption scheme. One of the major achievements is the generation of a one-to-one mapping between the encryption key and the cipher sequence using SEA and FI-PWLCM. This significantly strengthens key sensitivity, making brute-force attacks computationally infeasible due to the enormous key space (2^256+8m).

Another strength is the statistical robustness achieved through SCD optimization. The algorithm successfully minimizes the chi-square value of encrypted images, which results in flat histograms and high information entropy. These properties protect against statistical and differential attacks.

The decryption mechanism is straightforward due to preserved key sequences, enabling exact image recovery. Furthermore, the dynamic nature of the key unique for each encryption ensures compliance with the one-time pad concept.

However, the algorithm's performance slightly degrades with high-resolution images due to computational overhead. Optimizations such as parallel processing or block-based encryption can address this limitation.

CONCLUSION

This document developed a unique image encryption approach employing SHA-256, SEA, FI-PWLCM, and SCD to provide robust encryption with statistical security. Unlike most approaches, it provides a greater than and less than one decoding correspondence for each input key with its chaotic sequences, which is an improvement to brute force and statistical attack resilience. Entropy, PSNR, SSIM, NPCR, UACI, and other metrics showcased strong performance in the experimental validation. The SEA approach aids in the fast generation of sequences, while SCD optimizing histogram characteristics sharpens cipher complexity. Chaotic behavior and diffusion are also improved with FI-PWLCM. While high-resolution scenarios impose slight performance limitations, the model is proven to be reliable, efficient, and scalable. In medical imaging, surveillance, and cloud storage where image security is a necessity, this multi-faceted model enables seamless integration.

REFERENCES

[1] X. Sun and Z. Chen, "A Novel Chaotic Image Encryption Algorithm Based on Coordinate Descent and SHA-256," *IEEE Access*, vol. 10, pp. 114597–114610, 2022.

[2] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Optics and Lasers in Engineering*, vol. 88, pp. 197–213, 2017.

[3] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926–934, 2006.

[4] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," *Archives of Computational Methods in Engineering*, vol. 27, pp. 15–43, 2020.

[5] Z. Hua, Z. Zhu, S. Yi, Z. Zhang, and H. Huang, "Cross-plane colour image encryption using a two-dimensional logistic tent modular map," *Information Sciences*, vol. 546, pp. 1063–1083, 2021.

[6] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, 2017.

[7] X. Wang, X. Zhu, X. Wu, and Y. Zhang, "Image encryption algorithm based on multiple mixed hash functions and cyclic shift," *Optics and Lasers in Engineering*, vol. 107, pp. 370–379, 2018.

[8] Z. Chen, X. Wang, and Y. Wang, "A color image encryption algorithm based on multiple mixed chaotic systems and SHA-512," *Mathematics*, vol. 10, no. 5, 2022.

[9] R. Enayatifar, A. H. Abdullah, and M. Lee, "A weighted discrete imperialist competitive algorithm combined with chaotic map for image encryption," *Optics and Lasers in Engineering*, vol. 51, no. 9, pp. 1066–1077, 2013.

[10] X. Wang, C. Liu, and D. Xu, "Image encryption scheme using chaos and simulated annealing algorithm," *Nonlinear Dynamics*, vol. 84, no. 3, pp. 1417–1429, 2016.

[11] D. Ravichandran, P. Praveenkumar, and J. B. B. Rayappan, "DNA chaos blend to secure medical privacy," *IEEE Transactions on Nanobioscience*, vol. 16, no. 8, pp. 850–858, 2017.

[12] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd ed. CRC Press, 2020.

[13] C. Li, D. Lin, J. Lü, and F. Hao, "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography," *IEEE MultiMedia*, vol. 25, no. 4, pp. 46–56, 2018.

[14] M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Processing*, vol. 171, 2020.

[15] S. Zhu, C. Zhu, and W. Wang, "A novel image compression-encryption scheme based on chaos and compression sensing," *IEEE Access*, vol. 6, pp. 67095–67107, 2018.

[16] P. Sneha, S. Sankar, and A. S. Kumar, "A chaotic colour image encryption scheme combining Walsh–Hadamard transform and maps," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1289–1308, 2020.

[17] Y.-Q. Zhang, J.-L. Hao, and X.-Y. Wang, "An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map," *IEEE Access*, vol. 8, pp. 54175–54188, 2020.

[18] X. Zhang, Z. Zhou, and Y. Niu, "An image encryption method based on the Feistel network and dynamic DNA encoding," *IEEE Photonics Journal*, vol. 10, no. 4, pp. 1–14, 2018.

[19] C. Li, B. Feng, S. Li, J. Kurths, and G. Chen, "Dynamic analysis of digital chaotic maps via state-mapping networks," *IEEE Transactions on Circuits and Systems I*, vol. 66, no. 6, pp. 2322–2335, 2019.

[20] S. Wang, C. Wang, and C. Xu, "An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm," *Optics and Lasers in Engineering*, vol. 128, 2020.