iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: III Month of publication: March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67447

A Novel Chaotic Image Encryption Algorithm based on Coordinate Descent and SHA-256

S Ankitha Patil[1], Avvolla Sandhya[2], Babburi Kavitha[3], Sureddy Ashritha[4]
[1]*Assistant Professor, Department of CSE (AI&ML), CMR College, Hyderabad, Telangana, India*
[2, 3, 4]*Student, Department of CSE (AI&ML), CMRCET, Hyderabad, Telangana, India*

Abstract: Since each encryption necessitates the transmission of the key, chaotic image encryption methods with key and plaintext association have emerged in recent years. These algorithms are essentially one-time pad at a time. Nevertheless, some current systems are unable to map the seed key to the chaotic system's initial value in a unique way, which reduces the encryption system's key space. Furthermore, some techniques defy the one-time pad strategy by encrypting the same image with the same key. These issues are resolved in this paper in two ways. On the one hand, SHA-256 is used to calculate a hash value after randomly inserting pixels into a plain image. Even if the same image is encrypted, several seed keys can be obtained. However, to achieve the one-to-one connection between the seed key and the encrypted key stream, the Sequential Expansion Algorithm (SEA) and Feedback Iterative Piece-Wise Linear Chaotic Mapping (FI-PWLCM) are suggested. Random and seed key sensitive sequences can be produced rapidly via SEA. FI-PWLCM uses feedback iteration with additional control settings to achieve one-to-one correspondence with the seed key. The mapping can generate more intricate chaotic sequences in addition to having the speed of PWLCM. Additionally, in order to strengthen cryptosystems' resistance to statistical attacks, this study suggests the Segmented Coordinate Descent (SCD) technique for histogram statistical optimization of images. The algorithm can withstand brute force attacks, statistical attacks, chosen-plaintext (chosen-ciphertext) attacks, and more, according to experiments and security research. It performs best in the statistical qualities of entropy and histogram when compared to the majority of existing algorithms.

Keywords: SHA-256, SCD, Coordinate descent, Image encryption, and Chaotic systems.

I. INTRODUCTION

The necessity for robust encryption techniques is highlighted by the growing reliance on digital images in many different sectors. However, the special difficulties presented by image data, such as its quantity and redundancy, are frequently insurmountable by conventional encryption methods. In order to increase security and efficiency, this study presents a novel encryption technique that combines the advantages of SHA-256 hashing with coordinate descent.

Our primary objective is to address several flaws in the chaotic image encryption techniques now in use. For increased security, we want to ensure that every encryption use a distinct key and adheres to the one-time pad technique. This is accomplished by using SHA-256 hashing to generate distinct seed keys for every encryption and adding random pixels. Furthermore, we securely link seed keys with encrypted key streams using the Sequential Expansion Algorithm (SEA) and Feedback Iterative Piece-Wise Linear Chaotic Mapping (FI-PWLCM). Finally, we optimize picture statistics using the Segmented Coordinate Descent (SCD) technique, strengthening our encryption against intrusions.

In order to increase security and efficiency, this research focuses on creating a chaotic picture encryption technique that combines SHA-256 hashing and coordinate descent. The suggested technique combines SHA-256 hashing and coordinate descent optimization to improve the security and effectiveness of image encryption.

II. LITERATURE REVIEW

Numerous studies examining chaotic systems and their uses in picture encryption are examined in this survey of the literature.

A. Hidden Attackors

S. Wang, C. Wang, and C. Xu's paper "An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm" (2020): This work shows improved security and performance in image encryption by proposing an encryption algorithm based on the Knuth–Durstenfeld algorithm and a hidden attractor chaotic system.

B. Compressive Sensing

In 2018, X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen published "An image encryption algorithm based on chaotic system and compressive sensing", which This paper presents an encryption technique that exhibits enhanced security and robustness by combining compressive sensing with a chaotic system.

C. 3D Cat Maps

G. Chen, Y. Mao, and C. K. Chui's 2004 paper, "A symmetric image encryption scheme based on 3D chaotic cat maps": This study develops a real-time secure symmetric encryption system that improves attack resistance by generalizing the 2D chaotic cat map to 3D.

D. Logistic Maps

N. K. Pareek, V. Patidar, and K. K. Sud and their work "Image encryption using chaotic logistic map" (2006): Using chaotic logistic maps, this study suggests a novel technique to picture encryption that offers a safe and effective way to encrypt images in real time.

E. Summary of Findings

Due to their sensitivity and complexity, chaotic systems have demonstrated significant potential in picture encryption; yet, many current encryption algorithms suffer from problems such as non-unique key mapping and departures from the one-time pad approach. By guaranteeing that every encryption employs a unique key and safely connecting seed keys with encrypted key streams, our study presents a novel technique that overcomes these difficulties. We also adjust image statistics to improve security against intrusions.

III. PROBLEM STATEMENT

Existing chaotic image encryption algorithms often struggle with two main issues. First, they sometimes fail to create a unique link between the secret key and the initial settings of the chaotic system, which weakens the encryption. Second, some algorithms reuse the same key to encrypt the same image, which goes against the recommended one-time pad method for strong encryption. Moreover, many algorithms rely on low-dimensional chaotic systems that are vulnerable to dynamic degradation in finite precision devices, leading to predictable keystreams and poor encryption security. Additionally, the complexity and computational demands of some chaotic systems can hinder their practicality in real-time applications. There is also a need for enhanced security measures to protect against advanced cryptanalytic attacks. In the past, many algorithms have been introduced that cannot uniquely map the seed key to the initial value of the chaotic system, which leads to the reduction of the key space of the encryption system.

To tackle these problems, we're introducing a new chaotic image encryption method. It combines the Sequential Expansion Algorithm (SEA), Feedback Iterative Piece-Wise Linear Chaotic Mapping (FI-PWLCM), and Segmented Coordinate Descent (SCD). This approach ensures each encryption uses a distinct key and securely links seed keys with encrypted key streams. Additionally, it fine-tunes image statistics to enhance security against attacks.

IV. MODULE DESCRIPTION

The proposed chaotic image encryption algorithm is structured into the following modules:

1) Upload Sample Image: This module allows users to select and upload a sample image to the application. Users can browse their local file system, choose an image, and load it into the application for encryption.

2) Run Proposed Encryption: This module applies the proposed encryption algorithm to the uploaded sample image. It executes the encryption process, transforming the original image into an encrypted image. The original and encrypted images are then displayed to the user.

3) Run Proposed Decryption: This module enables users to upload an encrypted image for decryption. Users can select an encrypted image file, upload it to the application, and initiate the decryption process. The encrypted and decrypted images are then presented to the user. The module also calculates and displays the PSNR and SSIM values to evaluate the quality of the decrypted image.

4) Calculate NPCR and UACI Values: This module calculates the NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) values. It encrypts the original image, generates a cipher image, modifies a single pixel in the original image, and re-encrypts it to produce another cipher image. The two cipher images are then used to compute the NPCR and UACI values, which are displayed to the user.

V. REQUIREMENTS

A. *Requirements for the External Interface*

- User Interface: This system user interface is a very friendly Python Graphical User Interface.
- Hardware Interfaces: It is done using Python so that the user will communicate with the console.
- Software Interfaces: The software that is needed is Python
- Operating Environment: Windows XP.

1) Hardware Requirements

- Processor - intel i3(min)
- Speed -1.1 Ghz
- RAM - 256 MB (min)
- Hard Disk - 20 GB
- Monitor – SVGA

2) Software Requirements

- Operating System – Windows 10(min)
- Programming Language – Python 3.7.0

VI. METHODOLOGY

This paper proposes image encryption scheme that is designed to overcome the shortcomings of present chaotic encryption techniques, we propose the image encryption scheme with multi-level mechanism. We present a hybrid approach that includes Segmented Coordinate Descent (SCD), Feedback Iterative Piece-Wise Linear Chaotic Mapping (FI-PWLCM), Sequential Expansion Algorithm (SEA) and SHA-256 hashing to build the highly robust and computationally effective encryption framework. The focus on randomness, pixel correlation, key sensitivity, and resilience to both statistical data reliability and brute-force attacks is then the key objective of this encrypting scheme. It combines chaotic map-based and well-established cryptographic methods with an innovative hybrid approach that maximizes the use of chaotic sequences while keeping high efficiency compared to current encryption standards.

A. *System Workflow*

Overview:

1) The algorithm begins with preprocessing the input image and inserting random pixels.
2) The preprocessed image is then passed through the SHA-256 hash function to generate a unique hash value.
3) The Sequential Expansion Algorithm (SEA) and Feedback Iterative Piece-Wise Linear Chaotic Mapping (FI-PWLCM) are employed to generate the encryption key.
4) The image is encrypted by performing XOR operations to unique key generated and image pixels.
5) The Segmented Coordinate Descent (SCD) method is used to optimize the image histogram.
6) The decryption process mirrors the encryption process.

B. *Technologies & Tools Used*

The technologies and tools used for project implementation are:

1) Python programming language
2) Tkinter library for GUI development
3) OpenCV library for image processing
4) NumPy library for numerical computing
5) Matplotlib library for data visualization
6) h5py library for working with HDF5 files
7) TensorFlow library for machine learning
8) SciPy library for scientific computing

C. Implementation

The implementation of the proposed chaotic image encryption algorithm as follows:

1) Image Preprocessing and Hash Generation: First, the input image is loaded and converted into a one-dimensional array. To enhance security and introduce variability, ten random pixel values are appended to this array. This modified array is then converted into bytes, and the SHA-256 hash function is applied to generate a unique 32-byte hash value. This hash value serves as a crucial component for subsequent key generation.

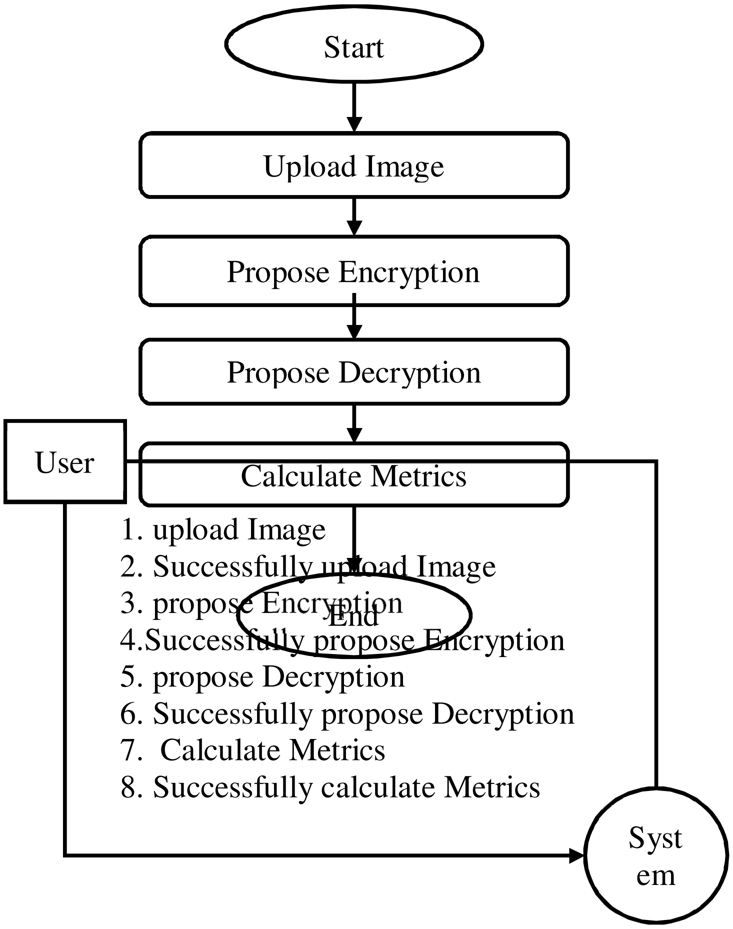
2) Key Generation: The generated hash value is then used as the seed for key generation. The Sequential Expansion Algorithm (SEA) is employed to rapidly produce seed key sensitive and random sequences. Subsequently, the Feedback Iterative Piece-Wise Linear Chaotic Mapping (FI-PWLCM) is utilized to establish a one-to-one correspondence between the seed key and the encrypted key stream, ensuring a robust and complex key generation process.

3) Histogram Optimization (SCD): To further enhance the security of the encryption, the Segmented Coordinate Descent (SCD) method is applied. This technique optimizes the key sequences by converting the high-dimensional optimization problem into a lower-dimensional one. This process helps in reducing the key space while simultaneously improving the algorithm's resistance to statistical attacks.

4) Encryption: The core encryption process involves using the optimized key sequences to transform the preprocessed image. The encryption is performed by combining permutation and diffusion techniques. Specifically, the pixel values of the image are XORed with the generated key, effectively scrambling the image data and rendering it unintelligible. The output of this stage is the encrypted image.

5) Decryption: In essence, the decryption procedure is the encryption procedure in reverse. The encrypted image is restored to its original state using the same key that was used for encryption. The encryption process is reversed and the original image data is restored by XORing the key with the encrypted image's pixel values. This guarantees that the original image may only be accessed by authorized people who possess the appropriate key.

VII. FLOWCHART



VIII. BENEFITS

The proposed system offers several key advantages that contribute to robust and efficient image encryption.

1) Enhanced Security – The algorithm uses a combination of SHA-256, SEA, FI-PWLCM, and SCD, making it highly resistant to various attacks.
2) Improved Efficiency – The use of SCD helps in reducing the key space, making the algorithm computationally efficient.
3) High Key Sensitivity – The algorithm exhibits high sensitivity to the secret key, ensuring that even a slight change in the key results in a completely different encrypted image.
4) Reduced Pixel Correlation – The encryption process minimizes the correlation between adjacent pixels, making it difficult for attackers to deduce information about the original image.
5) Robustness – The algorithm is designed to be robust against statistical and brute-force attacks, ensuring the security of the encrypted images.

IX. RESULT

A number of performance indicators are used to assess our suggested chaotic picture encryption technique.

A. Performance Evaluation

1) NPCR (Number of Pixels Change Rate)
- Calculates the proportion of distinct pixels between two encrypted pictures.
- Range: 0% to 100%. Strong sensitivity to even little changes is indicated by a high NPCR rating (around 100%).
- Achieved: High NPCR values, or 0.99, which show that the plain picture changed very little while the cipher image changed significantly.

2) UACI (Unified Average Changing Intensity)
- The average intensity of the variations between two cipher pictures is measured by UACI (Unified Average Changing Intensity).
- Range: from 0% to roughly 50%. 25–35% is a practical range.
- Achieved: UACI values that show a significant average change in pixel intensity fall within the predicted range, or 0.348.

3) PSNR (Peak Signal-to-Noise Ratio)
- Measures the quality of the encrypted image compared to the original.
- Range: Lower values indicate better image encryption.
- Achieved: Low PSNR values i.e 0, indicating maximal distortion in the encrypted image.

4) SSIM (Structural Similarity Index Measure)
- Measures the structural similarity between the original and decrypted images.
- Range: 0 to 1, where 1 indicates perfect similarity.
- Achieved: SSIM values close to 1, indicating high structural similarity.

B. Comparative Analysis

Our proposed system demonstrates significant improvements over previous works in terms of security and efficiency. The combination of SHA-256, SEA, FI-PWLCM, and SCD algorithms provides a robust encryption framework. The high NPCR and UACI values indicate strong resistance to differential attacks, while the PSNR and SSIM values confirm the high quality of the decrypted images. Additionally, the use of SCD helps in reducing the key space, making our algorithm computationally efficient compared to other chaotic encryption techniques.

X. CONCLUSION

In this paper, SEA and SCD methods are proposed, and PWLCM is improved to FI-PWLCM. This scheme works by randomly inserting pixel values and using SHA-256 to associate the key with the plain image. The proposed SEA and FI-PWLCM realize the one-to-one mapping between the seed key and the encryption key stream, which is very consistent with the one-time pad. The SCD method can effectively improve the histogram characteristics of the cipher image, make the distribution of pixels at all levels of the cipher image more uniform, and the information entropy is higher. This makes the scheme have better statistical characteristics of cryptography.

In addition, this approach can obtain better histogram properties, entropy values and correlation in less time than existing meta-heuristic image encryption algorithms. Several experiments and security analysis show that the algorithm has a large enough key space, and can effectively resist selective text attack, brute force attack, statistical statistics, noise attack and clipping attack. This research lays a solid foundation for secure image encryption using chaotic systems. In the future, this algorithm can be further enhanced by improving the algorithm's efficiency for large-sized image encryption. One approach is to reduce the amount of image data through compression techniques. Another promising direction is to speed up the encryption process by leveraging block and parallel computing technologies.

REFERENCES

[1] A hidden attractor chaos system and the Knuth–Durstenfeld algorithm serve as the foundation for an image encryption technique, according to S. Wang, C. Wang, and C. Xu. May 2020, Opt. Lasers Eng., vol. 128, art. no. 105995.

[2] In July 2018, X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen published "An image encryption algorithm based on chaotic system and compressive sensing" in Signal Process, vol. 148, pp. 124–144.

[3] "DNA chaos blend to secure medical privacy," by D. Ravichandran, P. Praveenkumar, and J. B. B. Rayappan December 2017, IEEE Trans. Nanobiosci., vol. 16, no. 8, pp. 850–858.

[4] A symmetric image encryption system based on 3D chaotic cat maps was developed by G. Chen, Y. Mao, and C. K. Chui. pp. 749–761 in Chaos, Solitons Fractals, vol. 21, July 2004.

[5] "Image encryption using chaotic logistic map," by N. K. Pareek, V. Patidar, and K. K. Sud, Image Vis. Comput., vol. 24, no. 9, pp. 926–934, 2006.

[6] Y. Wang, K.-W. Wong, X. Liao, T. Xiang, and G. Chen, ''A chaos-based image encryption algorithm with variable control parameters,'' Chaos, Solitons Fractals, vol. 41, no. 4, pp. 1773–1783, 2009.

[7] X. Chai, Y. Chen, and L. Broyde, ''A novel chaos-based image encryption algorithm using DNA sequence operations,'' Opt. Lasers Eng., vol. 88, pp. 197–213, Jan. 2017.

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

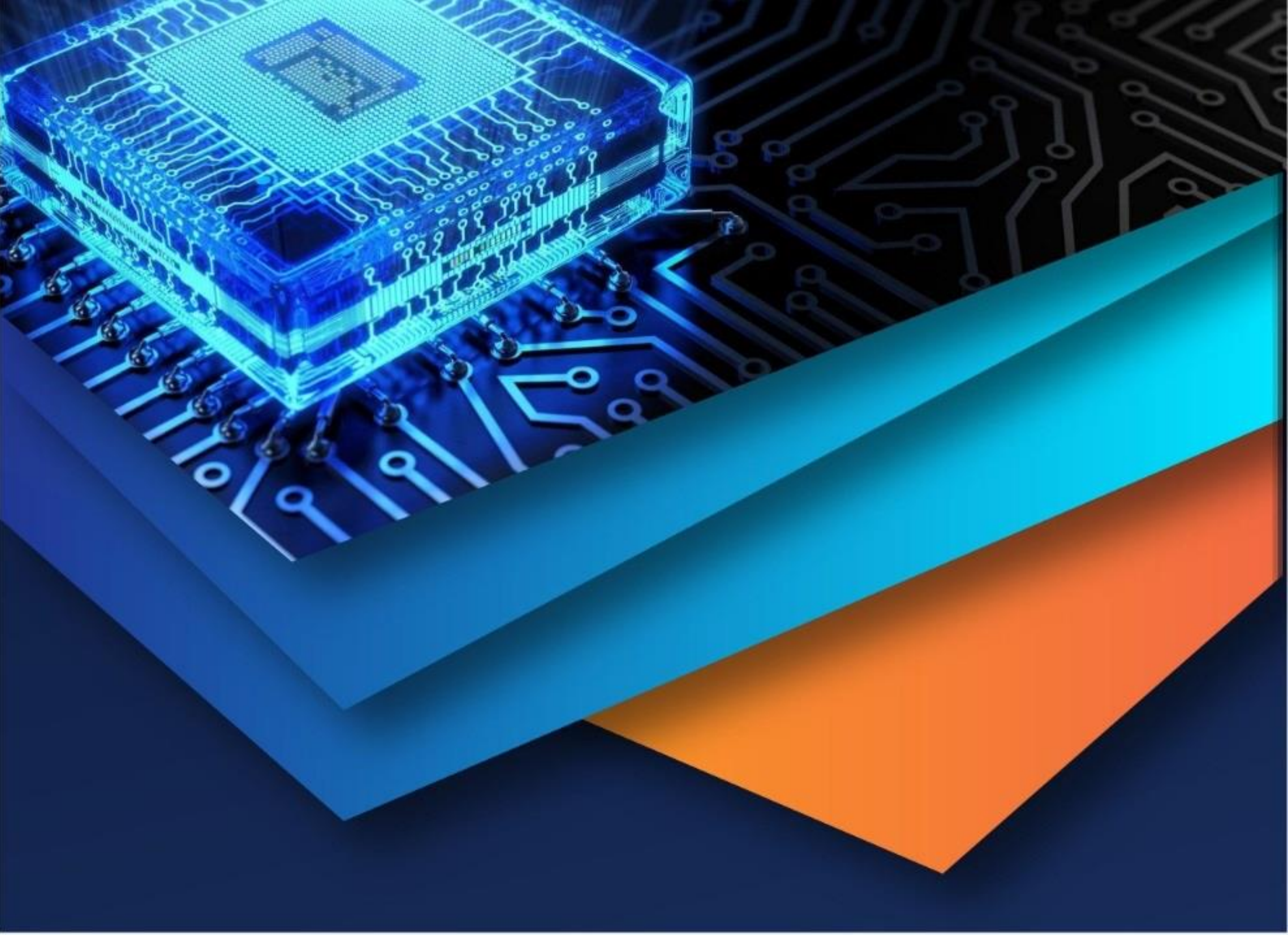
[9] Q. Xu, K. Sun, C. Cao, and C. Zhu, ''A fast image encryption algorithm based on compressive sensing and hyperchaotic map,'' Opt. Lasers Eng., vol. 121, pp. 203–214, Oct. 2019.

[10] M. Zhou and C. Wang, ''A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks,'' Signal Process., vol. 171, Jun. 2020, Art. no. 107484.

[11] S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian, and M. F. Abu-ElYazeed, ''A novel image encryption system merging fractional-order edge detection and generalized chaotic maps,'' Signal Process., vol. 167, Feb. 2020, Art. no. 107280.

[12] P. Sneha, S. Sankar, and A. S. Kumar, ''A chaotic colour image encryption scheme combining Walsh–Hadamard transform and maps,'' J. Ambient Intell. Humanized Comput., vol. 11, no. 3, pp. 1289–1308, 2020.

[13] Z. Hua, Z. Zhu, S. Yi, Z. Zhang, and H. Huang, ''Cross-plane colour image encryption using a two-dimensional logistic tent modular map,'' Inf. Sci., vol. 546, pp. 1063–1083, Feb. 2021.



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR: 7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429