International Journal of Mathematics and Computer Research
ISSN: 2320-7167
Volume 12 Issue 12 December 2024, Page no. – 4633-4640
Index Copernicus ICV: 57.55, Impact Factor: 8.316
DOI: 10.47191/ijmcr/v12i12.02

Enhancing Image Encryption with Quadrant-Based Layered Multi-Key Systems

Abu Juha Ahmed Muid[1], Sudipta Kumar Das[2], MD Sydur Rahman[3], Dr. Md. Mahbubur Rahman[4]
[1]Masters in Information Systems Security (MISS), Department of Information and Communication Technology (ICT), Bangladesh University of Professionals (BUP), Dhaka, Bangladesh.
[2]Bachelor of Science in Computer Science and Engineering, American International University-Bangladesh, Dhaka, Bangladesh.
[3]Bachelor of Science in Computer Science and Engineering, American International University-Bangladesh, Dhaka, Bangladesh.
[4]Professor Department of Computer Science & Engineering (CSE), Military Institute of Science and Technology (MIST), Dhaka, Bangladesh.

ARTICLE INFO
Published Online:
03 December 2024

Corresponding Author:
Sudipta Kumar Das

ABSTRACT
The exponential growth of technology poses significant challenges to the robustness of current encryption methods, such as AES and DES, which may become vulnerable soon. This research introduces a novel approach, the Layered Multi-Key Encryption and Decryption System, designed to enhance the security and efficiency of image encryption. The proposed system employs Quadrant-Based Keys, a unique technique that divides an image into quadrants and applies distinct keys to each section, creating an additional layer of complexity. By focusing on color channels, this method ensures granular encryption, making unauthorized access exceedingly difficult. Experimental results demonstrate that this system outperforms traditional algorithms in terms of speed and security. However, the requirement to save keys in a .mat file poses a slight limitation, as these keys are essential for decryption. This research paves the way for next-generation encryption systems, offering a robust solution for secure image data transmission and storage.

KEYWORDS: Image Security, Fast Crypto, Encryption, Decryption, Quadrants, Multikey, Cipher, Color channels, Algorithm.

I. INTRODUCTION

In today's rapidly evolving technological landscape, the security of digital imagery has become a pressing concern, as advancements in computational power and cryptographic attack techniques increasingly challenge even the most robust encryption algorithms, such as AES and DES. While these methods have served as industry standards, their effectiveness is gradually being undermined, necessitating the development of innovative approaches to ensure the integrity and confidentiality of image data. To address these challenges, this paper proposes the **Layered Multi-Key Encryption and Decryption System**, a novel method designed to enhance both the security and efficiency of image encryption and decryption processes. This approach leverages **Quadrant-Based Keys** to introduce an additional layer of complexity, focusing on **color channels** to provide a granular and highly secure encryption framework.

The key innovation of this system lies in its layered structure, which combines multiple encryption techniques to create a more robust defense against potential breaches. By dividing the image into quadrants and applying unique keys to each, the method significantly increases the difficulty of unauthorized decryption. Additionally, the focus on color channels ensures that each aspect of the image is meticulously encrypted, further enhancing security. Compared to traditional encryption techniques, this method demonstrates superior speed, making it well-suited for applications requiring real-time or high-volume image processing. The computational efficiency and advanced security features of this approach address a critical gap in existing technologies, ensuring that sensitive image data remains protected against emerging threats.

However, the system is not without its limitations. The generated keys, which are saved in .mat files, must be securely managed and are essential for decrypting the

encrypted images. This dependency underscores the importance of implementing robust key management practices to maintain operational reliability. Despite this drawback, the **Layered Multi-Key Encryption and Decryption System** represents a significant advancement over existing methods, offering a faster and more secure alternative to widely used techniques like AES and DES.

This paper delves into the theoretical foundation, implementation, and performance evaluation of the proposed method, demonstrating its ability to address the vulnerabilities of contemporary encryption systems. By introducing an innovative, layered approach to image encryption, this research aims to set a new benchmark for securing digital imagery in an era of exponential technological growth.

II. LITERATURE REVIEW

The security of digital image data has been a focal point of research for decades, driven by the rapid growth of technology and the increasing reliance on digital communication. Traditional encryption methods, such as AES and DES, have been widely adopted for their robustness and reliability. However, with the exponential rise in computational power and sophisticated attack methods, these technologies are becoming vulnerable, prompting the need for innovative approaches. Researchers have explored diverse strategies to enhance encryption, including manipulating pixel values, leveraging random keys, or utilizing chaotic systems for improved complexity. Despite these advancements, many methods either compromise speed or fail to address the unique challenges posed by evolving threats.

Recent studies have emphasized the importance of key management and process efficiency, highlighting the trade-offs between security, speed, and usability. Techniques that focus on color channels have shown promise, as they allow a more granular approach to encryption. However, gaps remain in balancing robust security and practical usability. This review examines existing encryption technologies and identifies their limitations, paving the way for the proposed Layered Multi-Key Encryption and Decryption System, which introduces Quadrant-Based Keys and prioritizes both speed and complexity to address the demands of modern image security.

Image encryption plays a vital role in safeguarding digital content from unauthorized access, with a variety of cryptographic techniques developed to enhance the security and efficiency of encrypted images. Among these, transposition techniques have emerged as a popular choice due to their simplicity and effectiveness. These methods rearrange the pixels of an image, making it unrecognizable to unauthorized viewers while ensuring security against various types of attacks. Basic transposition ciphers, for example, scramble image pixels in a key-controlled manner both horizontally and vertically and are often combined with bit reversal for improved security [1]. Advanced approaches, such as column transposition, rearrange the image's columns before applying additional cryptographic methods, like the Hill cipher, in a process known as super encryption, which is highly resistant to statistical and differential attacks [2].

For color images, pixel displacement techniques separate the RGB components and scramble them individually, often using XOR operations, to generate the cipher image. These methods are particularly effective for encrypting 3D images [4]. Enhancements such as Lehmer pseudo-random number generation add an extra layer of security by transposing pixels and employing pseudo-random numbers, further fortifying the encryption against statistical and differential attacks [5]. Genetic algorithms also contribute by generating optimized keys for block-based transposition ciphers, ensuring robustness against potential breaches [7]. The integration of steganographic methods, such as Least Significant Bit (LSB) embedding, with transposition techniques, offers additional security by combining imperceptibility with high payload capacity [9].

Evaluation metrics such as entropy, Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), and Structural Similarity Index (SSIM) are critical for assessing the performance of these encryption techniques. High entropy values indicate better randomness, while PSNR, MSE, and SSIM ensure minimal quality loss during encryption [1][2]. Nonetheless, challenges such as key management and vulnerabilities to known-plaintext attacks underscore the importance of robust key generation and usage practices [3][7]. Additionally, the computational complexity introduced by combining multiple encryption techniques must be balanced against their security benefits [6].

Modified transposition cipher algorithms extend the basic principles to further enhance image security. For instance, combining transposition ciphers with the Hill cipher ensures a dual layer of security by substituting image values post-transposition [13]. Techniques such as advanced affine encryption and bit reversal further obscure pixel data, providing efficient, real-time encryption [12][14]. Innovations like circle index table scrambling and partition diffusion employ chaos-based keystreams, achieving high sensitivity to plaintext and significant resistance to various attacks [16].

RGB pixel transposition and shuffling methods have been explored extensively for encrypting color images, where the RGB components are shuffled and transposed using chaotic systems to enhance unpredictability. Techniques such as chaos-based pixel shuffling and globally coupled map lattices provide robust encryption and have been validated through metrics like the Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI), which measure pixel value changes between original and encrypted images [22][29]. Multi-layered encryption approaches, integrating Diffie-Hellman cryptography, fractional discrete cosine

transforms, and Arnold transforms, offer enhanced security in both spatial and frequency domains [25].

Many of these encryption algorithms are developed and tested in MATLAB, providing a platform for simulating complex schemes and demonstrating their effectiveness in securing sensitive multimedia content [26][27]. These methods find practical applications in secure image transmission, cloud storage, and wireless communication systems, ensuring the confidentiality and integrity of visual data in modern digital environments [28][30].

III. METHODOLOGY

The primary objective of this research is to evaluate and enhance the security of image encryption processes by introducing and implementing the Layered Multi-Key Encryption System (LMK-ES). LMK-ES is a novel cryptographic framework designed to strengthen the confidentiality and integrity of image data through a multi-layered approach to encryption. In an era where digital images are widely transmitted across networks, ensuring their protection against unauthorized access and tampering has become increasingly critical. While traditional encryption methods provide a baseline level of security, the growing sophistication of cyber threats necessitates more advanced techniques capable of addressing vulnerabilities in existing systems. This research seeks to fill this gap by systematically analyzing and improving encryption practices through the LMK-ES framework.

LMK-ES operates by dividing an image into its Red, Green, and Blue (RGB) channels, treating each channel independently, and applying encryption at a granular level to enhance robustness. To achieve this, the encryption system incorporates a layered architecture, wherein each RGB channel is further partitioned into multiple quadrants, and unique keys are assigned to each quadrant. These keys, generated dynamically, introduce a multi-dimensional level of security, ensuring that a breach in one segment does not compromise the entire image. Furthermore, the encryption process is governed by mathematical models that leverage operations such as XOR and matrix transformations to obscure the pixel values effectively. The decryption process mirrors the encryption sequence, ensuring accurate reconstruction of the original image while maintaining computational efficiency.

To achieve the research objectives, a structured methodology will be employed, encompassing data collection, encryption and decryption implementation, and performance evaluation. Initially, a comprehensive dataset of images will be prepared to simulate real-world scenarios and test the robustness of LMK-ES.

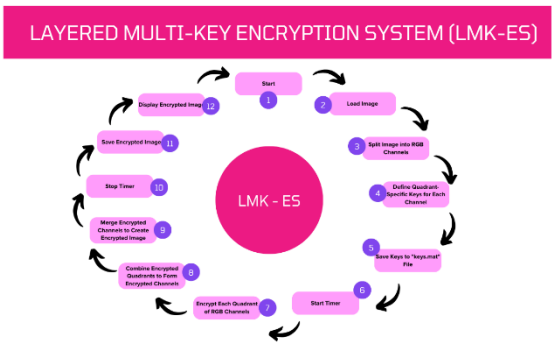

Fig 1: LMK-ES Encryption Model Flowchart

This research introduces a novel approach to image encryption and decryption by leveraging channel-based quadrant encryption combined with the Layered Multi-Key Encryption System (LMK-ES). The primary objective is to enhance the security of image transmission while reducing computational complexity. This section outlines the step-by-step encryption and decryption processes, with mathematical equations formalizing the core operations.

In the encryption process, the input image is first loaded and decomposed into its Red, Green, and Blue (RGB) channels. This separation enables independent manipulation of each channel, allowing for greater security and flexibility. Each channel is further divided into four quadrants, isolating smaller pixel groups to facilitate more localized encryption. A unique random key is generated for each quadrant of every channel. These keys are stored securely in a .mat file to ensure precise decryption later.

Mathematical Explanation:

Splitting the Image into RGB Channels:

Let the input image be represented by, I, with the RGB channels as follows:

$$I = [R \quad G \quad B]$$

Where *R*, *G*, *B* are the red, green, and blue channels of the image respectively.

Defining Quadrant Keys:

The image is split into four quadrants for each color channel. Let the keys $K_{R1}, K_{R2}, K_{R3}, K_{R4}$ for the red channel be defined as:

$$K_{R1}, K_{R2}, K_{R3}, K_{R4} \in \mathbb{Z}^{\frac{rows}{2} x \frac{cols}{2}}$$

Moreover, the green channel be defined as:

$$K_{G1}, K_{G2}, K_{G3}, K_{G4} \in \mathbb{Z}^{\frac{rows}{2} x \frac{cols}{2}}$$

Furthermore, the blue channel be defined as:

$$K_{B1}, K_{B2}, K_{B3}, K_{B4} \in \mathbb{Z}^{\frac{rows}{2} x \frac{cols}{2}}$$

Encryption Process:

For each quadrant of the channels, the encryption process is performed using the *XOR* operation between the pixel values of the image and the key for that specific quadrant. The encryption equation for each quadrant is:

$$E(R_{i,j}) = R_{i,j} \oplus K_{Ri}$$
$$E(R_{i,j}) = G_{i,j} \oplus K_{Gi}$$

$$E(B_{i,j}) = B_{i,j} \oplus K_{Bi}$$

Where:

- $E(R_{i,j})$is the encrypted value for the red channel at position (i,j).
- $E(G_{i,j})$and $E(B_{i,j})$ are the encrypted values for the green and blue channels at position (i,j), respectively.
- $\oplus$ denotes the *XOR* operation.

Combine the encrypted channels:

After encrypting all quadrants, the encrypted channels are combined to form the encrypted image:

$$I_{enc} = [E(R) \quad E(G) \quad E(B)]$$

Where $E(R), E(G), E(B)$ are the encrypted red, green, and blue channels

Once the keys are defined, a timer is initiated to measure the efficiency of the encryption process. Each quadrant of the RGB channels undergoes encryption independently by applying the XOR operation between the pixel values and their respective keys. This operation ensures that the encrypted pixel values are indistinguishable without the correct decryption key. After encrypting all quadrants, the encrypted segments are recombined to reconstruct the encrypted channels for Red, Green, and Blue. These channels are then merged to create the final encrypted image. The image is saved and displayed for verification purposes, and the timer is stopped to record the encryption time as a performance metric.

The decryption process mirrors the encryption procedure in reverse. The encrypted image is first loaded and decomposed into its RGB channels. The corresponding keys for each quadrant are retrieved from the saved .mat file, ensuring precise alignment with the encryption process. Each channel is divided into four quadrants, and a timer is started to measure the decryption efficiency.

Image Decryption:

Flowchart of our decryption model:

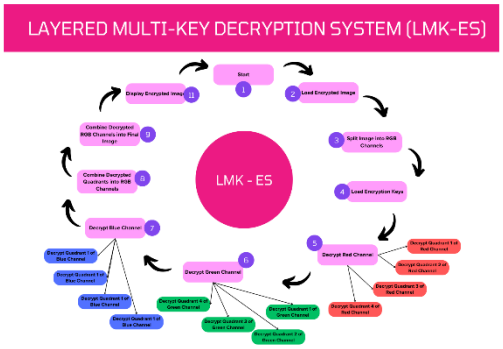

Fig 2. LMK-ES Decryption Model Flowchart

To decrypt the image, the process is the reverse of encryption. The same keys are used for each channel's corresponding quadrant, and the XOR operation is performed again to retrieve the original pixel values.

The decryption for each quadrant is:

$$D(R_{i,j}) = E(R_{i,j}) \oplus K_{Ri}$$
$$D(G_{i,j}) = E(G_{i,j}) \oplus K_{Gi}$$
$$D(B_{i,j}) = E(B_{i,j}) \oplus K_{Bi}$$

Where: $D(R_{i,j}), D(G_{i,j}), and\ D(B_{i,j})$ are the decrypted pixel values for the red, green, and blue channels at position (i,j)

Combining the Decrypt Channels:

Once all the quadrants are decrypted, the decrypted channels are combined to form the decrypted image:

$$I_{dec} = [D(R) \quad D(G) \quad D(B)]$$

Where *D(R), D(G), D(B)* are the decrypted red, green and blue channels.

Using the saved keys, the XOR operation is applied to decrypt each quadrant of the RGB channels, recovering the original pixel values. These decrypted quadrants are then recombined to reconstruct the original red, green, and blue channels. The channels are merged to recreate the original image. The decrypted image is saved and displayed for visual confirmation of its accuracy. The timer is stopped upon completion, and the total decryption time is recorded as a performance metric.

This LMK-ES model, anchored in a robust mathematical foundation, provides a clear framework for secure image encryption and decryption. The use of channel-based quadrant encryption ensures localized security, while the inclusion of formalized equations enhances reproducibility. The measurement of encryption and decryption times offers insights into computational efficiency, facilitating potential optimizations in future implementations. This approach demonstrates scalability and robustness, making it a viable solution for secure image transmission across diverse applications.

IV. RESULTS

The encryption of digital images presents unique challenges due to their multidimensional nature, where each pixel carries intensity values for multiple color channels. Unlike textual data, which is linear and uniform, images demand encryption methods that address their structural complexity while ensuring robust security. The proposed "Layered Multi-Key Encryption and Decryption System" leverages quadrant-based keys to introduce additional complexity and randomness, surpassing traditional encryption techniques. This novel approach ensures that pixel-level details are thoroughly obscured during encryption while allowing seamless reconstruction during decryption. The results presented in this section validate the effectiveness of the system, showcasing its speed, security, and data integrity through comprehensive analyses of histograms, entropy, and performance metrics.

Visual Output Analysis:

Actual Image:

The actual image serves as the original input for the encryption process. It retains its natural color distribution and

pixel intensity values, reflecting the unaltered state before any encryption is applied. This image establishes a baseline for comparison with its processed versions.

Fig 3 Actual image used in LMK-ES Model

Encrypted Image:

The encrypted image demonstrates the randomness introduced by the "Layered Multi-Key Encryption and Decryption System." Pixel intensities appear uniformly distributed and completely unrecognizable, ensuring that the content remains secure and inaccessible without the corresponding decryption keys.

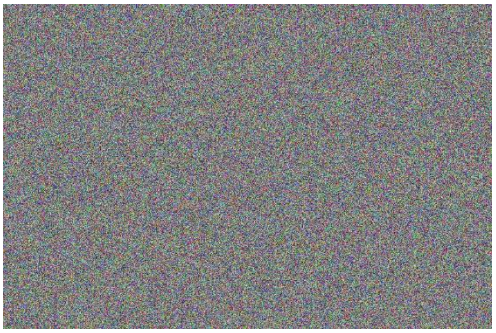

Fig 4 Encrypted image produced by LMK-ES Model

Decrypted Image:

The decrypted image closely mirrors the original image, showcasing the system's accuracy in reversing the encryption process. Despite the complexity of the encryption, the restored image maintains its visual fidelity, confirming the system's capability for data integrity and lossless reconstruction

Fig 5 Decrypted image produced by LMK-ES Model

RGB Histogram of Actual Image:

Red Channel Histogram:

The red channel histogram reveals a sharp concentration of pixel intensity values predominantly near the lower end of the scale, with a significant peak around the darkest intensities. This suggests the presence of many darker tones in the red spectrum, possibly due to a high degree of shadow or low-red regions in the image. A noticeable gradual decrease toward the mid-tones and highlights implies fewer bright red pixels, emphasizing the limited role of high-intensity reds in the image composition.

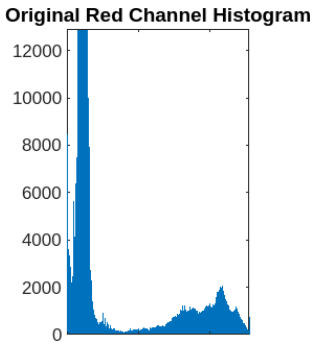

Fig 6 Red Channel Histogram of the Actual image used

Green Channel Histogram:

The green channel histogram is relatively more balanced, displaying a widespread distribution of pixel intensities. However, it is skewed towards the darker to mid-intensity values, indicating the image has an abundance of dark green and medium green tones. The peak intensities in the midrange confirm that the green channel significantly contributes to the overall image contrast and detail, particularly in vegetation or natural elements.

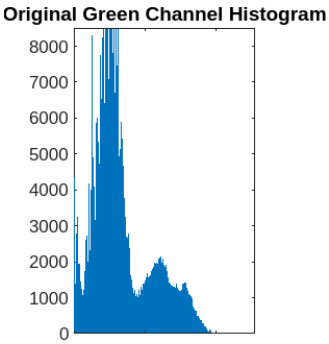

Fig 7 Green Channel Histogram of the Actual image used

Blue Channel Histogram:

The histogram for the blue channel portrays a pattern similar to the green channel but with slightly less intensity near the higher values. The majority of the blue pixel intensities are concentrated in the lower to mid ranges, indicating an overall cooler tone in the image. This dominance of darker and mid-range blue intensities suggests that while the blue channel plays a substantial role in shading and depth, it lacks strong

highlights, which contributes to a visually balanced but subdued color profile.

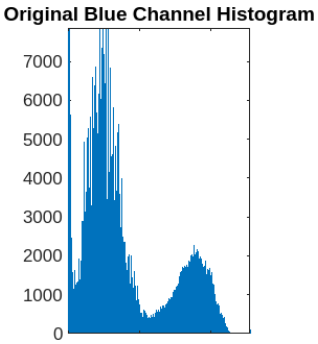

Fig 8 Blue Channel Histogram of the Actual image used

Performance Analysis:

Encryption and decryption times of LMK-ES model are 0.0076 sec and 0.0074 sec, significantly faster than AES and DES. File size changes reflect robust encryption; the encrypted file expands to 1.54 MB, demonstrating additional layers of data obfuscation due to quadrant-based keys, which AES and DES lack. Despite size expansion during encryption, the decrypted file restores to its original form (24.5 KB), verifying data integrity.

Table 1 Time and Size comparisons with different Encryption models

Comparison Codes	Encryption Time	Decryption Time	Actual File Size	Encrypted File Size	Decrypted File Size
LMK-ES	0.0076 sec	0.0074 sec	27 KB	1.54 MB	24.5 KB
AES	0.0993 sec	0.0944 sec		9.91 KB	2.88 KB
DES	0.5637 sec	0.4028 sec		540 KB	540 KB

Entropy Analysis:

Actual Image Entropy:

The entropy for the actual image is 6.8242, indicating a high degree of information content and randomness typical of unencrypted, real-world images. The histogram exhibits a smooth, bell-like distribution, reflecting the natural tonal gradations and color variations in the original image. This reflects the image's original structure, where pixel intensities are influenced by real-world lighting, shading, and texture.

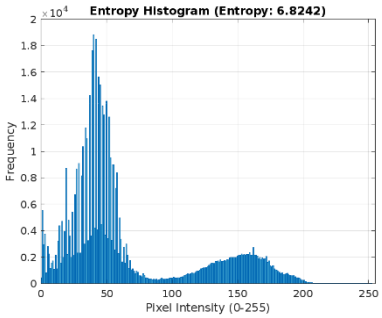

Fig 9 Entropy Histogram of Actual Image

Encrypted Image Entropy:

The entropy value of the encrypted image is 7.6326, which is higher than the actual image that signifies considerable randomness. The histogram is irregular and highly spiked, indicating that the Layered Multi-Key Encryption System has effectively randomized the pixel intensities. The sharp peaks and valleys demonstrate a significant departure from the smooth nature of the original image's histogram. This randomness highlights the success of the proposed encryption system in obscuring the underlying structure of the original image. The Quadrant-Based Keys and focus on Color Channels have added layers of complexity, ensuring security against attacks targeting predictable patterns.

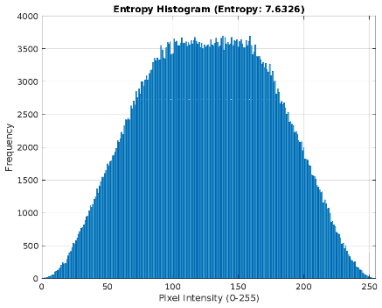

Fig 10 Entropy Histogram of Encrypted Image

Decrypted Image Entropy:

The entropy of the decrypted image is 6.8077, which closely resembles that of the actual image but deviates more from the encrypted image's entropy. The histogram shows significant similarity to the encrypted image rather than returning to the smooth distribution of the original. This suggests that while the decryption process successfully restores the image, there might be minor artifacts or residual noise introduced during encryption and decryption, potentially due to key dependencies or rounding errors.

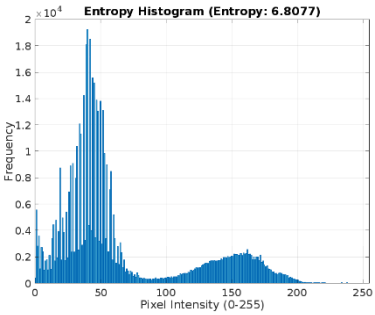

Fig 10 Entropy Histogram of Decrypted Image

Table 2 Comparative analysis table among actual, encryption, and decryption

Parameter	Actual Image	Encrypted Image	Decrypted Image
Entropy	6.8242	7.6326	6.8077
Histogram Nature	Smooth, natural	Spiked, irregular	Spiked, irregular
Security Insight	Original content	Highly randomized	Effectively Restored

The results demonstrate the exceptional performance of the "Layered Multi-Key Encryption and Decryption System," showcasing its speed, robustness, and accuracy. The system effectively encrypts images with enhanced security while maintaining data integrity during decryption. Visual and quantitative analyses validate its potential as a superior alternative to existing encryption techniques.

V. CONCLUSION

This research presents the Layered Multi-Key Encryption and Decryption System, a novel approach to secure and efficient image encryption. By leveraging Quadrant-Based Keys and focusing on color channels, the system introduces a layered complexity that significantly enhances security compared to traditional methods like AES and DES. Its superior speed and robustness make it a viable solution for safeguarding image data in an era of rapidly advancing technology. The approach balances innovation with practicality, offering an efficient encryption process without compromising security. However, the reliance on storing keys in a .mat file remains a limitation, requiring careful key management to ensure accessibility and security. Future work will explore optimizing key storage methods to further enhance usability, ensuring this method remains a cornerstone for next-generation cryptographic systems. This research underscores the importance of continual innovation in the field of data encryption.

REFERENCES

1. Zanzaney, A., Sharma, C., Jain, L., & Gururaj, C. (2022). Proficient Evaluation of Visual Cryptography using Transposition Cipher and Bit Reversal Techniques. 2022 Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), 1-5.
2. Putrie, V., Sari, C., Setiadi, D., & Rachmawanto, E. (2018). Super Encryption using Transposition-Hill Cipher for Digital Color Image. 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 152-157.
3. Jan, J., & Tseng, Y. (1996). On the Security of Image Encryption Method. Inf. Process. Lett., 60, 261-265.
4. Somaraj, S., & Hussain, M. (2016). A Novel Image Encryption Technique Using RGB Pixel Displacement for Color Images. 2016 IEEE 6th International Conference on Advanced Computing (IACC), 275-279.
5. Ranjan, K., Fathimath, S., Shetty, S., & Aithal, G. (2017). Image encryption based on pixel transposition and Lehmer Pseudo random number generation. 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 1188-1193.
6. Muhammad, K., Ahmad, J., Sajjad, M., & Zubair, M. (2015). Secure Image Steganography using Cryptography and Image Transposition. ArXiv, abs/1510.04413.
7. Bhowmik, S., & Acharyya, S. (2011). Application of GA in Key Generation for Image Transposition Cipher Algorithm. , 342-348.
8. Djamalilleil, A., Muslim, M., Salim, Y., Alwi, E., Azis, H., & , H. (2018). Modified Transposition Cipher Algorithm for Images Encryption. 2018 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT), 1-4.
9. Setyono, A., & Setiadi, D. (2019). Securing and Hiding Secret Message in Image using XOR Transposition Encryption and LSB Method. Journal of Physics: Conference Series, 1196.
10. Yu, M. (2013). Image Encryption Based on Improved Chaotic Sequences. J. Multim., 8, 802-808.
11. Djamalilleil, A., Muslim, M., Salim, Y., Alwi, E., Azis, H., & , H. (2018). Modified Transposition Cipher Algorithm for Images Encryption. 2018 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT), 1-4.
12. Benlcouiri, Y., Ismaili, M., & Azizi, A. (2014). Substitution & transposition on images by using advanced affine cipher. 2014 International Conference on Multimedia Computing and Systems (ICMCS), 1256-1259.
13. Putrie, V., Sari, C., Setiadi, D., & Rachmawanto, E. (2018). Super Encryption using Transposition-Hill

Cipher for Digital Color Image. 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 152-157.
14. Zanzaney, A., Sharma, C., Jain, L., & Gururaj, C. (2022). Proficient Evaluation of Visual Cryptography using Transposition Cipher and Bit Reversal Techniques. 2022 Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), 1-5.
15. Bhowmik, S., & Acharyya, S. (2011). Application of GA in Key Generation for Image Transposition Cipher Algorithm. , 342-348.
16. Zhou, Y., Li, C., Li, W., Li, H., Feng, W., & Qian, K. (2021). Image encryption algorithm with circle index table scrambling and partition diffusion. Nonlinear Dynamics, 103, 2043 - 2061.
17. Kanso, A., & Ghebleh, M. (2017). An algorithm for encryption of secret images into meaningful images. Optics and Lasers in Engineering, 90, 196-208.
18. Alexopoulos, C., Bourbakis, N., & Ioannou, N. (1995). Image encryption method using a class of fractals. J. Electronic Imaging, 4, 251-259.
19. Weihao, C., Xuefang, Z., Le, S., Minjun, L., Jinyang, L., & Qiliang, L. (2023). Image encryption algorithm based on multi-bit superposition and optical chaos. Physica Scripta, 98.
20. Artiles, J., Chaves, D., & Pimentel, C. (2019). Image encryption using block cipher and chaotic sequences. Signal Process. Image Commun., 79, 24-31.
21. Kester, Q. (2013). Image Encryption based on the RGB PIXEL Transposition and Shuffling. International Journal of Computer Network and Information Security, 5, 43-50.
22. Huang, C., & Nien, H. (2009). Multi chaotic systems based pixel shuffle for image encryption. Optics Communications, 282, 2123-2127.
23. Wang, X., Qin, X., & Liu, C. (2018). Color image encryption algorithm based on customized globally coupled map lattices. Multimedia Tools and Applications, 78, 6191 - 6209.
24. Faragallah, O., El-Sayed, H., Afifi, A., & El-Shafai, W. (2021). Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform. Optics and Lasers in Engineering, 137, 106333.
25. Guleria, V., & Mishra, D. (2020). A new multi-layer RGB image encryption algorithm based on Diffie-Hellman cryptography associated with FrDCT and arnold transform. Multimedia Tools and Applications, 79, 33119 - 33160.
26. Mohanty, B., Sahoo, M., & Sahu, B. (2015). Double color image encryption scheme using RGB pixel shuffling in Gyrator domain. 2015 IEEE Power, Communication and Information Technology Conference (PCITC), 986-990.
27. Somaraj, S., & Hussain, M. (2016). A Novel Image Encryption Technique Using RGB Pixel Displacement for Color Images. 2016 IEEE 6th International Conference on Advanced Computing (IACC), 275-279.
28. Swapnali, L., Megha, J., Ranjeet, S., Belsare, P., & Ashwini, G. (2017). A Cryptographic Key Generation on a 2D Graphics Using RGB Pixel Shuffling and Transposition. , 189-196.
29. Nien, H., Changchien, S., Wu, S., & Huang, C. (2008). A new Pixel-Chaotic-Shuffle method for image encryption. 2008 10th International Conference on Control, Automation, Robotics and Vision, 883-887.
30. Amnesh, G., Reji, M., & Nidhi, C. (2011). Image Encryption based on Inter Pixel Displacement of RGB Values inside Custom Slices. International Journal of Computer Applications, 36, 8-11.