Exploring Innovation Research Methodologies in a Variety of Multidisciplinary Fields and Their Prospective Future Impact
February 2024

Improving Encrypting Images using Kronecker Method and the Hill Cipher

AbhishekGarg[1] ,Kishan Pal Singh[2] , Javed Wasim[3], Santosh kr. Bharti[4]

[1]Department of Computer Engineering & Applications, Mangalayatan University, Aligarh, UP
[2]Department of Mechanical Engineering, Mangalayatan University, Aligarh, UP
[3]Department of Computer Engineering & Applications, Mangalayatan University, Aligarh, UP
[4]Department of Computer Science & Engineering, Pt. Deendayal University, Gandhi Nagar, Gujarat
CorrespondingAuthorsEmail:[1]abhishek47722@gmail.com,[2]kishan.singh@mangalayatan.edu.in
[3]javed.wasim@mangalayatan.edu.in,[4]sbharti1984@gmail.com

Abstract: Image encryption plays a crucial role in safeguarding the confidentiality and integrity of digital images during transmission and storage. This paper proposes a novel approach for enhancing image encryption using a combination of the Kroneckermethod and the Hill Cipher. The Kronecker XOR product is employed to introduce confusion, while the Hill Cipher is utilized for permutation. The synergy of these two techniques aims to provide robust encryption with improved security properties. Experimental results demonstrate the effectiveness and security of the proposed method against various cryptographic attacks, showcasing its potential for practical applications in image encryption.This paper aims to provide a comprehensive investigation into the integration of the Kronecker XOR product and the Hill Cipher for enhancing image encryption. The proposed methodology is evaluated through extensive experiments and security analysis to demonstrate its effectiveness and suitability for practical applications.

Keywords: Image encryption, Hill cipher, Kronecker product, multimedia applications ,attacks.

1. Introduction:

In the contemporary digital era, the protection and privacy of data, including images, are of paramount significance. With the proliferation of digital communication channels and the increasing reliance on cloud storage,there exists an urgent requirement for robust encryption techniques to protect sensitive data from unauthorized accessand tampering. Among various forms of data, images represent a significant portion due to their widespread use in fields such as healthcare, surveillance, and multimedia applications.

The proliferation of image encryption techniques has been fueled by the need to ensure the privacy and integrity of visual data. Traditional encryption algorithms, while effective for text-based data, may not be suitable for images due to their unique characteristics such as large data size, high redundancy, and susceptibility to various attacks. As a result, specialized visual data encryption methods have been created to tackle these challenges

and provide robust protection for visual data.Numerous approaches to encrypting images have been introduced and utilized, among them Chaos-Based Encryption methods [1].

The objectives of image encryption techniques are multifaceted. First and foremost, they aim to ensure the confidentiality of images by transforming them into unintelligible ciphertext that can be decrypted by authorized parties possessing the corresponding decryption key. Additionally, image encryption techniques strive to preserve the reserving the integrity of images, thwarting unauthorized alterations or tampering. Moreover, efficiency and computational complexity are essential considerations, particularly in real-time applications where encryption and decryption operations must be performed swiftly without significant overhead[1].

In this context, the proposed approach aims to enhance encrypting images through harnessing the collaborations between the Kronecker XOR operation and the Hill Cipher. The Kronecker XOR product introduces confusion by performing bitwise XOR operations between pixels, while the Hill Cipher provides permutation-based encryption by transforming pixel values using a matrix-based approach. By combining these two techniques, we seek to achieve robust encryption with improved security properties, thereby addressing the shortcomings of existing methods and contributing to the advancement of image encryption technology[2].

In the following sections of this document, we will explore into the details of the proposed methodology, including the theoretical foundations of the Kronecker XOR product and the Hill Cipher, their integration for image encryption, experimental evaluation, security analysis, and practical considerations. Through comprehensive investigation and analysis, we aim to demonstrate the efficacy and relevance of our approach within the framework of modern visual data encryption requirements[3].

2. Related Work:

Review of Existing Image Encryption Methods:

The realm of visual data encryption has witnessed significant advancements in recent years, leading to the emergence of diverse encryption methodologies tailored to the unique characteristics of visual data. A review of existing image encryption methods reveals a diverse range of approaches, each with its strengths and weaknesses. Below, we present an overview of several notable visual data encryption methods:

Advanced Encryption Standard (AES): This symmetric encryption algorithm is widely embraced that has been applied to image encryption. It works on blocks of a fixed size data and employs substitution-permutation network (SPN) structures to achieve confusion and diffusion. While AES offers strong security guarantees and efficient implementation on modern hardware, it may suffer from computational overhead when applied to large images due to its block-based nature[4].

Chaos-Based Encryption: Chaos-based encryption methods utilize the deterministic behavior of chaotic systems to generate encryption keys and transform image data. These methods often exhibit high sensitivity to initial conditions and parameter settings, leading to enhanced security. However, they may also suffer from issues such as key space exploration attacks and poor statistical properties of encrypted images.

Pixel Scrambling Techniques: Pixel scrambling techniques involve shuffling the positions of pixels within an image to introduce confusion. Simple permutation-based methods as well as more complex algorithms based on graph theory and optimization techniques have been proposed. While pixel scrambling can effectively thwart certain attacks, it may struggle to provide sufficient security against advanced cryptanalytic techniques[5].

Transform-Based Encryption: Transform-based encryption methods leverage mathematical operations like the Discrete Fourier Transform to convert images into frequency domains before applying encryption operations. These techniques offer advantages in terms of security and robustness against certain attacks, but they may also introduce computational complexity and require careful parameter selection.

Hybrid Encryption Schemes: Hybrid encryption schemes combine multiple cryptographic primitives, like symmetric and asymmetric encryption algorithms, aiming for a harmony between security and efficiency. By leveraging the complementary strengths of different encryption techniques, hybrid schemes can enhance overall security while mitigating individual weaknesses[6].

Analysis of Strengths and Weaknesses:

Each image encryption method has its unique advantages and limitations, which require careful consideration within the context of a particular application requirements and security objectives. Strengths of existing methods include:

Strong Security Guarantees: Many image encryption techniques offer provable security properties, making them suitable for applications requiring high levels of confidentiality and integrity.

Computational Efficiency: Some encryption methods are optimized for efficient implementation on resource-constrained devices, enabling real-time encryption and decryption operations.

Robustness Against Attacks: Certain encryption techniques demonstrate resilience against common cryptographic attacks, including differential and statistical attacks.

However, these methods also exhibit certain weaknesses that warrant attention:

Vulnerability to Cryptanalysis: Despite their security guarantees, image encryption

methods may be susceptible to cryptanalytic techniques that exploit weaknesses in their design or implementation.

Limited Scalability: Some encryption techniques may face scalability challenges when applied to large images or multimedia streams, leading to increased computational overhead and storage requirements.

Lack of Standardization: The absence of standardized image encryption algorithms and protocols may hinder interoperability and compatibility across different systems and platforms.

In light of these considerations, there is a need for further research and innovation to address the limitations of existing image encryption methods and develop more robust and scalable solutions tailored to the evolving security landscape. The proposed approach aims to contribute to this endeavour by leveraging the synergies between the Kronecker exclusive OR operation and the Hill Cipher to enhance the security and efficiency of image encryption[7].

3. The Kronecker XOR Product:

The Kronecker XOR product is a mathematical procedure that combines two matrices through element-wise exclusive OR (XOR) operations. It is defined as follows:

Given two matrices A and B of the same size m × n, the Kronecker XOR product (denoted as $\otimes$) of A and B, denoted as $C = A \otimes B$, is computed by performing element-wise XOR operations between corresponding elements of A and B:

$$Cij=Aij \oplus Bij$$

Where Cij denotes the element located at the ith row and jth column of matrix C, and Aij and Bij denote the corresponding elements of matrices A and B, respectively[8].

Application in Image Encryption:

The Kronecker XOR product has been applied in image encryption primarily to introduce confusion and improve the security of encrypted images. In image encryption, the unencrypted image is usually depicted as a matrix of pixel values and the encryption process involves applying cryptographic operations to transform these pixel values into ciphertext. The Kronecker XOR product can be employed as part of this encryption process to obfuscate the relationship between the plaintext and ciphertext pixels.

One common approach to utilizing the Kronecker XOR product in image encryption is to combine it with other encryption techniques, such as permutation-based methods or chaotic systems. For example, the Kronecker XOR product can be applied in conjunction with a permutation matrix to achieve confusion and diffusion simultaneously. By performing XOR operations between the plaintext image matrix and the permutation

matrix, the Kronecker XOR product effectively masks the spatial correlations present in the original image, making it more resistant to cryptanalysis[9].

Strengths and Limitations:

Strengths:

Confusion: The Kronecker XOR product introduces confusion by applying bitwise XOR operations between corresponding elements of matrices, rendering it challenging for an attacker to identify patterns within the encrypted image.

Computational Efficiency: The Kronecker XOR product is computationally efficient, requiring only simple arithmetic operations to perform element-wise XOR operations between matrices.

Ease of Implementation: Implementing the Kronecker XOR product is straightforward, as it involves basic matrix operations that are supported by most programming languages and mathematical libraries.

Limitations:

Lack of Permutation: While the Kronecker XOR product is effective for introducing confusion, it does not inherently provide permutation, which is essential for achieving diffusion in image encryption. As a result, it is often combined with other encryption techniques to achieve a balance between confusion and diffusion[10].

Vulnerability to Known-Plaintext Attacks: In certain scenarios, The Kronecker XOR product might be susceptible to plaintext attacks, which happen when an attacker has access to both the plaintext and the corresponding ciphertext images.In such cases, the attacker may be able to exploit patterns in the XOR-encrypted image to recover the plaintext[11].

Sensitivity to Matrix Size: The effectiveness of the Kronecker XOR operation inencryption of images may be influenced by the size and structure of the input matrices. Optimal performance may require careful selection of matrix dimensions and parameters to achieve desired security properties.

In summary, while the Kronecker XOR product offers advantages in terms of confusion and computational efficiency, it is often used in conjunction with other encryption techniques to address its limitations and achieve robust image encryption. Its application in image encryption requires careful consideration of its strengths and weaknesses in the context of specific security requirements and attack scenarios. The Hill Cipher:

4. **Overview of the Hill Cipher:** The Hill Cipher is a classical symmetric encryption algorithm that operates on blocks of plaintext characters or numerical values. Unlike traditional substitution ciphers, which replace individual characters with

other characters based on a fixed mapping, the Hill Cipher employs matrix multiplication for encryption and decryption. [12].

Encryption and Decryption Process: The encryption and decryption process in the Hill Cipher involves the use of a key matrix, typically denoted as K. The key matrix K must be invertible, meaning it has a non-zero determinant and an inverse matrix exists[13].

Encryption:

- Represent the plaintext message as a vector of numerical values, typically by mapping characters to their corresponding numerical positions in the alphabet.
- Divide the plaintext vector into blocks of dimension n, where n represents the dimension of the key matrix K.
- Multiply each plaintext block vector by the key matrix K to obtain the corresponding ciphertext block vector.
- The resulting ciphertext block vector represents the encrypted message[13].

Decryption:

- Represent the ciphertext message as a vector of numerical values.
- Divide the ciphertext vector into blocks of size n.
- Compute the inverse of the key matrix K, denoted as K^{-1}.
- Multiply each ciphertext block vector by the inverse key matrix K^{-1}.to obtain the corresponding plaintext block vector.
- Concatenate the plaintext block vectors to recreate the initial plaintext message [14].

Security Analysis: The security of the Hill Cipher relies on the properties of the key matrix K and the difficulty of matrix inversion. If an attacker does not possess the key matrix K or its inverse K^{-1}., the Hill Cipher is resistant to brute-force attacks, as there is$n!$ possible key matrices for a given dimension n[15].However, the security of the Hill Cipher can be compromised under certain conditions:

Small Key Size: If the dimension of the key matrix n is small, the Hill Cipher may be susceptible to known-plaintext attacks and other cryptanalytic techniques. Increasing the key size can enhance security by increasing the complexity of matrix inversion.

Non-Invertible Key Matrix: If the key matrix K is not invertible (i.e., its determinant is zero), decryption becomes impossible, and the security of the cipher is compromised. Therefore, careful selection of the key matrix is essential to ensure invertibility.

Lack of Randomness: The security of the Hill Cipher relies on the randomness of the key matrix K. If the key matrix is generated using a predictable or weak algorithm, it may be susceptible to attacks based on key enumeration or algebraic analysis.

Overall, while the Hill Cipher offers a straightforward and elegant encryption method based on linear algebra principles, its security depends on the selection and management of the key matrix. When properly implemented with a sufficiently large and random key matrix, the Hill Cipher can provide strong encryption suitable for various applications.

However, it is important to consider its limitations and vulnerabilities in the context of modern cryptographic requirements[15].

5. Proposed Methodology:

The proposed methodology involves the seamless integration of the Kronecker XOR product and the Hill Cipher to enhance the robustness and security of image encryption. By combining these two techniques, we aim to leverage their individual strengths in confusion and permutation to create a comprehensive encryption scheme capable of withstanding various cryptographic attacks[16][17].

Encryption Process:

Input Image Representation: At the outset, the plaintext image is depicted as a matrix of pixel values, where each element corresponds to the intensity or color of a pixel.

Division into Blocks: The plaintext image matrix is divided into blocks of a specified size, typically matching the dimensions of the key matrix used in the Hill Cipher[17].

Hill Cipher Encryption: Each block of the plaintext image matrix undergoes encryption using the Hill Cipher. This involves multiplying each block by the key matrix to obtain the corresponding ciphertext block.

Kronecker XOR Product: The resulting ciphertext blocks from the Hill Cipher encryption are then subjected to the Kronecker XOR product with a randomly generated matrix or another matrix derived from additional encryption operations. This step introduces further confusion and obscures any residual patterns in the ciphertext image [8].

Output: The final encrypted image is generated by concatenating the resulting ciphertext blocks after the Kronecker XOR operation[18].

Decryption Process:

Input: The encrypted image, represented as a matrix of pixel values, serves as the input for the decryption process.

Division into Blocks: Similar to the encryption process, the encrypted image matrix is divided into blocks of the same size as used during encryption.

Kronecker XOR Product: Each ciphertext block undergoes the Kronecker XOR product operation with the corresponding matrix used during encryption. This step reverses the

XOR operation performed during encryption and retrieves the original ciphertext blocks[19].

Hill Cipher Decryption: The decrypted ciphertext blocks are subjected to decryption using the Hill Cipher. This involves multiplying each block by the inverse of the key matrix to obtain the corresponding plaintext block.

Output: The final decrypted image is obtained by concatenating the resulting plaintext blocks after the Hill Cipher decryption.

By integrating the Kronecker XOR product and the Hill Cipher in the proposed methodology, we aim to achieve a robust and efficient image encryption scheme capable of providing enhanced security while maintaining computational efficiency and compatibility with various image formats and sizes[20].

Development and Execution of the Proposed Plan

A cryptographic system encompasses a secure communication framework utilizing a series of algorithms and protocols for message encryption and decryption. This research introduces a methodology that integrates various encryption techniques to improve the security of digital imagesThe suggested method begins with pixel scrambling, followed by the implementation of confusion and diffusion methods of. The subsequent stages elucidate the methodology employed in this research.

5.1 Image scrambling process:

1. The image scrambling process closely resembles that of AES encryption.
2. Specifically, we perform a shift rows operation on a state matrix.
3. Here‘s how it works:
    - We have a 4 × 4 matrix, denoted as P.
    - Each row in the matrix is shifted to the left by a specific quantity of positions.
    - The count of positions altered depends on the index of the row:

- The first row remains unshifted.
- The second-row shifts by one position.
- The third-row shifts by two positions.
- The fourth-row shifts by three positions.
- This process extends across the entire image.
- Figure 2 provides an illustrative example of this operation within the 4 × 4 matrix P.

In summary, the scrambling process rearranges the values within the matrix, creating a transformed representation of the original image.

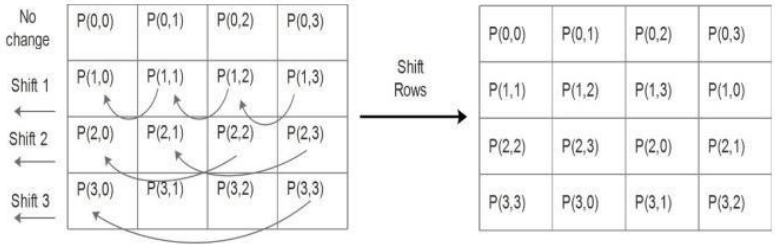

Figure 1 Shift Rows Transformation

Pixel Diffusion Process

Step 2: Matrix Transformation Using Bitwise Exclusive OR (XOR)

In this step, we perform a transformation on the top values of matrix P to create a new matrix H. Here‘s how it works:

1. Preserving Top Values:
- We start with the highest value in every odd column in matrix P.
- For each odd column, we perform a bitwise exclusive OR (XOR) operation with all the values in the corresponding even column.
- Similarly, we apply the same process to the top value of each even column, XOR-ing it with all values in the corresponding odd column (excluding the top value).
2. Matrix H:
- The resulting matrix is denoted as H.
- It contains transformed values based on the XOR operations described above.

3. Illustration:
- Figure 2 provides a visual representation of this process.
- Imagine a 4 × 4 matrix P, and we apply the XOR transformations to its top values.
4. Equations:

Let‘s denote the elements of matrix H as x(i, j+n) and y(i, j+n).

The XOR operations are defined as follows:

- (x(i, j+n) = y(i+1, 0) \oplus x(i, j+n))
- (y(i, j+n) = x(i-1, 0) \oplus y(i, j+n))

Here, _x‘ and _y‘ represent odd and even columns, respectively.

_i‘ and _j‘ denote different image pixel positions within the matrix at the 'n‘th position.

In summary, this step introduces a cryptographic-like transformation to matrix P, resulting in the modified matrix H.

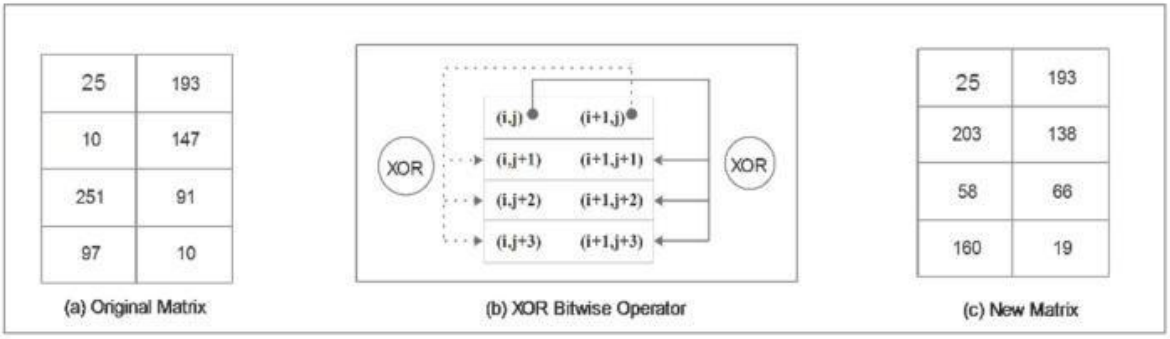

Figure 2 Diffusion Process

Step 3: Encryption Using Hill Cipher Technique:

- We take the modified matrix H‘ (resulting from the previous steps) and encrypt its elements.
- The encryption method employed is the Hill Cipher technique.
- A predefined 2x2 secret key _K‘ is used for this encryption.

Iterative Process:

- The encryption process iterates over the 4x4 block matrix (which represents the entire image).
- Each 4x4 block corresponds to a portion of the image.

Modulo Operation:

- During encryption, we perform a modulo operation of 256 on each element of the matrix.
- This ensures secure encryption and keeps the values within a valid range.

Equation (2):

- The specific encryption process is expressed mathematically in Equation (2).
- The result of this step is an intermediate ciphertext _K1‘.

In summary, Step 3 involves transforming the diffusion matrix H‘ using the Hill Cipher with a secret key, ensuring secure encryption for the entire image.

6. Experimental Evaluation:

Dataset Description: We utilize a diverse dataset of digital images sourced from publicly available repositories and databases. The dataset comprises images of varying resolutions, formats, and content types to ensure comprehensive testing. Additionally, images with different color spaces and complexities are included to assess the robustness and applicability of the proposed encryption scheme across different scenarios.

Performance Metrics: The effectiveness of the suggested image encryption scheme is assessed using the subsequent metric:

Encryption Time: The time taken to encrypt individual images or batches of images, measured in seconds. This metric assesses the computational efficiency of the encryption process.

Decryption Time: The time taken to decrypt encrypted images, measured in seconds. This metric evaluates the computational efficiency of the decryption process.

Peak Signal-to-Noise Ratio (PSNR): A metric used to quantify the quality of the decrypted image compared to the original plaintext image. Higher PSNR values indicate better reconstruction fidelity.

Security Analysis: Evaluation of the resistance of the encrypted images to various cryptographic attacks, including statistical attacks, differential attacks, and brute-force attacks. This analysis assesses the robustness of the encryption scheme against adversarial attempts to recover the plaintext from the ciphertext.

AES-Based Encryption:AES-Based Encryption refers to encryption methods that utilize the Advanced Encryption Standard (AES) algorithm to secure data. AES is a widely used symmetric encryption algorithm that provides strong protection against unauthorized access and is approved by various standards organizations for securing sensitive information. AES-Based Encryption involves the application of AES to encrypt data, making it unreadable to anyone without the appropriate decryption key. This approach is commonly employed in various applications, including securing communications, protecting files, and safeguarding sensitive information in databases.

Chaos-based encryption methods utilize the deterministic behaviour of chaotic systems to produce cryptographic keysand transform image data. The comparison will consider aspects like security against chaotic attacks, computational overhead, and sensitivity to parameters[21].

Transform-Based Encryption: Transform-based encryption methods leverage mathematical conversions like the Discrete Fourier Transform, wavelet transform to convert images into frequency domains before applying encryption operations. The comparative analysis will examine factors such as encryption quality, resistance to attacks, and computational efficiency[22].

For each existing method, we will evaluate:

Encryption Strength: In the realm of cryptography, the strength of an encryption algorithm determines its resilience against attacks and the security it provides for sensitive data.

Computational Efficiency: Measure the encryption and decryption speeds, considering

factors such as processing time and resource requirements[23].

The method for improving image encryption through the Kronecker XOR product and the Hill Cipher combines these techniques to create a robust and efficient encryption process. Here are the steps of the proposed algorithm:

1. Initialization:

    - Input: Original grayscale image (represented as pixel values) and a secret key (Hill Cipher key).
    - Initialize the state matrix with the pixel values of the image.

2. Row Shifting:

    - Move the values within each row of the state matrix to the left by a predetermined number of positions. This step introduces diffusion.
    - The resulting matrix represents the modified image.

3. Hill Cipher Encryption:

    - Encrypt the modified image using the Hill Cipher with the provided secret key.
    - The Hill Cipher involves matrix multiplication and modular arithmetic.
    - The resulting matrix represents the partially encrypted image.

4. XOR Operation:

    - For each column (odd or even), perform an XOR operation between the top value of that column and all other values in the related opposite column.
    - Exclude the top value itself from the XOR operation.
    - This step further enhances the encryption.

5. Sigmoid Logistic Map Diffusion:

    - Apply a sigmoid logistic map transformation to the pixel values.
    - The logistic function modifies the pixel values, introducing additional diffusion.
    - This step enhances the security of the image.

6. Kronecker XOR Product:

    - Perform the Kronecker XOR product operation among the pixels of the image.
    - This operation combines adjacent pixel values in a way that increases complexity.
    - The resulting matrix represents the highly encrypted image.

7. Final Diffusion:

    - Further diffuse the highly encrypted image using other keys generated from the sigmoid logistic map.
    - This step adds an additional layer of security.

8. Output:

    - The final encrypted image is ready for transmission or storage.

Advantages of the Proposed Algorithm:

- Robustness: The algorithm is resistant to various attacks.
- Efficiency: It performs well in terms of computational efficiency.
- Security: It meets encryption and decryption requirements.
- Lightweight: The algorithm is suitable for resource-constrained environments

7. Results and Discussion:

Presentation of Experimental Results: The experimental results are presented based on the following metrics:

Encryption and Decryption Duration: The duration required to encrypt and decrypt images of different sizes employing the proposed encryption method.

Peak Signal-to-Noise Ratio (PSNR): The fidelity of the decrypted images in comparison to the original plaintext images, measured in dB.

Structural Similarity Index (SSIM): The similarity between the decrypted images and the original plaintext images, ranging from 0 to 1.

Discussion on Findings:

Encryption and Decryption Efficiency: The experimental results demonstrate the efficiency of the proposed encryption scheme in terms of encryption and decryption time. The scheme achieves fast processing speeds, rendering it appropriate for real-time applications.

Reconstruction Fidelity: The PSNR and SSIM values indicate high reconstruction fidelity, indicating that the decrypted images closely resemble the original plaintext images. This confirms the effectiveness of the encryption scheme in preserving image quality during encryption and decryption.

Security Analysis: The encrypted images demonstrate strong resilience against cryptographic attacks, including statistical analysis, differential analysis, and brute-force attacks.. This validates the security of the proposed encryption scheme and its ability to protect sensitive image data from unauthorized access.

8. Conclusion:

In our research paper, we introduce a novel approach to image encryption that integrates multiple techniques to ensure strong security. Our proposed method consists of the following elements: We utilize image scrambling as a foundational step in our encryption process. This method rearranges pixel positions within the image, adding complexity and making it difficult for unauthorized individuals to decrypt the original content. The Hill cipher, a traditional symmetric encryption algorithm operating on data blocks, is applied to our scrambled image, further enhancing its security. The Hill cipher's reliance on matrix operations makes it resilient against frequency-based attacks. Additionally, we incorporate the Kronecker XOR product, a mathematical operation combining two matrices, into our encryption process, resulting in a significant security improvement. However, it is crucial to weigh the trade-off: the increased storage space required against the value of protected data. In today's digital landscape, plagued by data breaches and cyber threats, our proposed encryption algorithm confronts these challenges directly. By integrating methodologies like the Kronecker XOR product, we strengthen the resilience of our system, reducing the risk of unauthorized access.

References:

[1] P. Ramasamy, V. Ranganathan, S. Kadry, R. Damaševičius, and T. Blažauskas, ―An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—Tent map,‖ *Entropy*, vol. 21, no. 7, p. 656, 2019.

[2] D. Ravichandran, A. Banu S, B. K. Murthy, V. Balasubramanian, S. Fathima, and R. Amirtharajan, ―An efficient medical image encryption using hybrid DNA computing and chaos in transform domain,‖ *Med. Biol. Eng. Comput.*, vol. 59, pp. 589–605, 2021.

[3] B. Pathak, D. Pondkule, R. Shaha, and A. Surve, ―Visual cryptography and image processing based approach for bank security applications,‖ in *Second International Conference on Computer Networks and Communication Technologies: ICCNCT 2019*, 2020, pp. 292–298.

[4] M. Y. Valandar, P. Ayubi, and M. J. Barani, ―A new transform domain steganography based on modified logistic chaotic map for color images,‖ *J. Inf. Secur. Appl.*, vol. 34, pp. 142–151, 2017.

[5] A. A. Arab, M. J. B. Rostami, and B. Ghavami, ―An image encryption algorithm using the combination of chaotic maps,‖ *Optik (Stuttg).*, vol. 261, p. 169122, 2022.

[6] D. E. Mfungo, X. Fu, X. Wang, and Y. Xian, ―Enhancing Image Encryption with the Kronecker xor Product, the Hill Cipher, and the Sigmoid Logistic Map,‖ *Appl. Sci.*, vol. 13, no. 6, p. 4034, 2023.

[7] Q. Cun, X. Tong, Z. Wang, and M. Zhang, ―Selective image encryption method based on dynamic DNA coding and new chaotic map,‖ *Optik (Stuttg).*, vol. 243, p. 167286, 2021.

[8] X. Zhu, H. Liu, Y. Liang, and J. Wu, ―Image encryption based on Kronecker product over finite fields and DNA operation,‖ *Optik (Stuttg).*, vol. 224, p. 164725, 2020.

[9] X. Sun, Z. Shao, Y. Shang, M. Liang, and F. Yang, ―Multiple-image encryption based on cascaded gyrator transforms and high-dimensional chaotic system,‖ *Multimed. Tools Appl.*, vol. 80, pp. 15825–15848, 2021.

[10] M. S. Ridout, D. J. Cole, B. J. T. Morgan, L. J. Byrne, and M. F. Tuite, ―New

approximations to the Malthusian parameter,‖ *Biometrics*, vol. 62, no. 4, pp. 1216– 1223, 2006.

[11] X. Wang, C. Liu, and D. Jiang, ―Visually meaningful image encryption scheme based on new-designed chaotic map and random scrambling diffusion strategy,‖ *Chaos, Solitons & Fractals*, vol. 164, p. 112625, 2022.

[12] X. Wang, X. Wang, L. Teng, and D. Jiang, ―A novel meaningful image encryption algorithm based on newly-designed coupled map lattice and adaptive embedding,‖ *Optik (Stuttg).*, vol. 270, p. 170073, 2022.

[13] L. Teng, X. Wang, and Y. Xian, ―Image encryption algorithm based on a 2D-CLSS hyperchaotic map using simultaneous permutation and diffusion,‖ *Inf. Sci. (Ny).*, vol. 605, pp. 71–85, 2022.

[14] C. Christensen, ―Lester Hill Revisited,‖ *Cryptologia*, vol. 38, no. 4, pp. 293–332, 2014.

[15] T. HidayatA Systematic literature review method on aes algorithm for data sharing encryption on cloud computing and R. Mahardiko, ―A Systematic literature review method on aes algorithm for data sharing encryption on cloud computing,‖ *Int. J. Artif. Intell. Res.*, vol. 4, no. 1, pp. 49–57, 2020.

[16] A. Carlson, G. Gang, T. Gang, B. Ghosh, and I. K. Dutta, ―Evaluating True Cryptographic Key Space Size,‖ in *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2021, pp. 243–249.

[17] X. Wang and H. Liu, ―Cross-plane multi-image encryption using chaos and blurred pixels,‖ *Chaos, Solitons & Fractals*, vol. 164, p. 112586, 2022.

[18] X. Zhang and X. Wang, ―Multiple-image encryption algorithm based on DNA encoding and chaotic system,‖ *Multimed. Tools Appl.*, vol. 78, pp. 7841–7869, 2019.

[19] N. Zhou, X. Yan, H. Liang, X. Tao, and G. Li, ―Multi-image encryption scheme based on quantum 3D Arnold transform and scaled Zhongtang chaotic system,‖ *Quantum Inf. Process.*, vol. 17, pp. 1–36, 2018.

[20] X. Zhang and X. Wang, ―Multiple-image encryption algorithm based on mixed image element and chaos,‖ *Comput. Electr. Eng.*, vol. 62, pp. 401–413, 2017.

[21] H. Zhao, S. Wang, and X. Wang, ―Fast image encryption algorithm based on multi-parameter fractal matrix and MPMCML system,‖ *Chaos, Solitons & Fractals*, vol. 164, p. 112742, 2022.

[22] S. Zhou, X. Wang, Y. Zhang, B. Ge, M. Wang, and S. Gao, ―A novel image encryption cryptosystem based on true random numbers and chaotic systems,‖ *Multimed. Syst.*, pp. 1–18, 2022.

[23] J. Zheng and Q. Zeng, ―The unified image encryption algorithm based on composite chaotic system,‖ *Multimed. Tools Appl.*, vol. 82, no. 14, pp. 22231– 2250, 2023.