International Journal of Engineering Research and Science & Technology

ENHANCED IMAGE SECURITY VIA TWO-LAYER ENCRYPTION WITH SWITCHED SYSTEM DYNAMICS

VANGALA SWATHI [1], GANGAPURAM NANDINI [2], MANNEM AKHILA[3], NARRA BHARGAVA SAI [4], MARKANTI BHANU PRASAD [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— Traditional image encryption techniques generally rely on single-layer security mechanisms such as standard cryptographic algorithms (e.g., AES, DES), chaotic maps, or pixel shuffling methods. These systems often face challenges in balancing computational efficiency with robust security. Many existing methods either lack resistance to differential and statistical attacks or have high computational overhead. Additionally, most conventional approaches do not incorporate control-theoretic principles or dynamic system behavior, which limits their adaptability and complexity. As a result, attackers with access to known-plaintext or cipher-plaintext pairs may exploit predictable encryption structures, making these systems more vulnerable to sophisticated cryptanalytic attacks. The proposed image encryption-decryption scheme introduces a novel two-layer security framework that integrates control theory and dynamic system modeling to significantly enhance image security. In the first layer, a switched system—a type of dynamic system that switches between multiple subsystems—is employed to encrypt the image and simultaneously generate a random key matrix. This matrix serves as the foundation for the second layer of security, where a pixel-level diffusion process is applied using the generated key. The decryption process utilizes an optimization technique to reverse the diffusion, and the flatness property of the switched system ensures accurate reconstruction of the original image. This dual-layer approach increases resistance to cryptanalytic attacks such as differential analysis and adjacent pixel correlation, while maintaining computational efficiency. The scheme is thoroughly evaluated through simulations and validated using key metrics

like entropy, pixel correlation, NPCR, UACI, and histogram analysis, all of which demonstrate its effectiveness and superiority over traditional methods.

Index Terms – Image encryption, image decryption, switched systems, control theory, dynamic systems, pixel diffusion, cryptography, optimization techniques, entropy analysis, NPCR, UACI, histogram analysis, secure image transmission, differential attack resistance.

I. INTRODUCTION

In the era of information explosion, we are currently facing risks and dangers from information loss; there fore, information security in the digital age is becoming increasingly important. Especially, the data and information, including confidential information, medical records, or even military secrets can be disclosed via the Internet. Therefore, information security in transmission and storage is an important concern for governments and the military. Many studies and work have been conducted by leading experts in this field in recent years. Several decades ago, the first traditional encryption methods, such as DES (Data Encryp tion Standard) and AES (Advanced Encryption Standard) were used in information encryption [1]. However, when applying these methods to image encryption, there are some drawbacks such as important information being overlooked, high redundancy, and correlation between adjacent pixels mentioned in [2]. To overcome these shortcomings, many image encryption techniques have been researched and developed based on nonlinear dynamical systems. Espe cially, some techniques related to chaotic systems have been proposed to enhance the security level [3], [4], [5]. Chaotic systems exhibit the characteristic of sensitivity to initial conditions to develop the random generator, which is the need for encryption systems. Nevertheless, the complexity in chaotic encryption, due to floating point calculations, can introduce drawbacks in practical hardware implementation, leading to a degradation in signal reconstruction [6], [7]. Moreover, a hybrid chaotic method is developed to enhance the security level of information or image in some applications such as attack resistance in communications channel [8] or medical image ciphering [9], [10]. Besides, a combination between deep learning and chaotic systems has significantly increased the security level of the information encryption schemes [11]. Additionally, the fusion of DNA subsequence operations with

chaotic sequences offers a novel encryption technique and provides a high security level for color images [12]. An image encrypted based on the hyperchaotic maps combined with a single neuron model has provided a larger key space and higher encryption efficiency than traditional chaotic encryption methods [4], [13]. In general, these approaches highlight the convergence of chaotic systems, deep learning and neural networks in the security applications. Hybrid systems have stimulated extensive investigation within the realms of control theory and theoretical com puter science, offering a robust theoretical framework that integrates discrete time and continuous time systems. This integration enables the unified modeling of both software logic and physical dynamics, presenting a versatile approach for addressing various challenges. Among the diverse applications, switched systems, a notable subset of hybrid systems, garner considerable attention in research. Switched linear systems refer to a set of linear subsystems alongside a switching function that dictates the active subsystem at any given moment in time. Over time, a multitude of methods for analyzing stability and designing controls have emerged, related to switching control [14], stability [15], observability [16] and identification [17]. Moreover, the characteristic of left invertibility, which recovers the input sequences from those output, makes it attractive. The switching function is considered in real-time, the findings in [18] and [19] enable the retrieval of input sequences through an inverse system. Also, the flatness property significantly contributes to the derivation of the input and output relationship [18]. Consequently, the contributions of the invertibility and flatness from switched systems prove beneficial in developing cryptographic algorithms. Encryption and decryption using a certain matrix is a common method that uses a matrix to encrypt an image or a signal and it can only be decrypted using that matrix [2], [20], [21]. Encryption methods using key matrix typically involve applying matrix algorithms and operations to modify the pixel values in the original image [22], [23]. The key matrix is usually chosen as a random matrix since it can enhance security and resistance to attack [24]. By using a random matrix in the encryption process, it is more difficult for attackers to analyze and predict the key space of the algorithm. Moreover, cryptographic attacks such as statistical analysis, brute-force, and differential cryptanalysis can be resisted by random matrix encryption [25]. When the key matrix is generated randomly

by an encryption scheme, the resulting ciphertext will differ with different times of encrypting the same image/signal, enhancing the security of the encryption scheme. Another advantage of using the random key matrix is that if a random key matrix can be detected by eavesdroppers, the security of the encryption system may remain intact due to the number of possible key combinations. This contrasts with deterministic matrices or patterns, where exposure of the key could compromise all encrypted data [26]. Random key matrices also offer flexibility and scalability regarding encryption strength. The random matrix can be adjusted for its size and properties, which makes the encryption scheme adapting to many security requirements [29]. Nevertheless, some disadvantages can be considered while using random key matrix for encryption such as high computational resource requirements and vulnerability of encryption scheme in statistical analysis-based attacks [25]. Borrowed from control theory, several studies have proposed methods for generating random matrices from chaotic systems [11], [30], [31]. The chao-based random matrix for encryption has advantages of complexity, non-repeatability, speed and resistance to attacks [32], [33]. The reasons to achieve these benefits are the complex and unpredictable behavior of the chaotic system. Moreover, with simple circuits, the chaotic system can provide a random matrix relatively fast and is suitable for real time applications. Nevertheless, they also face challenges such as control, synchronization, robustness, and computational complexity.

II. RELATED WORK

A. Image encryption algorithms: A survey of design and evaluation metrics

Ensuring confidentiality and privacy is critical when it comes to sharing images over unsecured networks such as the internet. Since widely used and secure encryption methods, such as AES, Twofish, and RSA, are not suitable for real-time image encryption due to their slow encryption speeds and high computational requirements, researchers have proposed specialized algorithms for image encryption. This paper provides an introduction and overview of the image encryption algorithms and metrics used, aiming to evaluate them and help researchers and practitioners starting in this field obtain adequate information to understand the current state of image encryption algorithms. This paper classifies image encryption into seven different approaches based on the techniques used and analyzes the strengths and weaknesses of

each approach. Furthermore, this paper provides a detailed review of a comprehensive set of security, quality, and efficiency evaluation metrics for image encryption algorithms, and provides upper and lower bounds for these evaluation metrics. Finally, this paper discusses the pros and cons of different image encryption approaches as well as the suitability of different image encryption approaches for different applications.

B. A new encryption algorithm utilizing DNA subsequence operations for color images

The computer network has fundamentally transformed modern interactions, enabling the effortless transmission of multimedia data. However, the openness of these networks necessitates heightened attention to the security and confidentiality of multimedia content. Digital images, being a crucial component of multimedia communications, require robust protection measures, as their security has become a global concern. Traditional color image encryption/decryption algorithms, such as DES, IDEA, and AES, are unsuitable for image encryption due to the diverse storage formats of images, highlighting the urgent need for innovative encryption techniques. Chaos-based cryptosystems have emerged as a prominent research focus due to their properties of randomness, high sensitivity to initial conditions, and unpredictability. These algorithms typically operate in two phases: shuffling and replacement. During the shuffling phase, the positions of the pixels are altered using chaotic sequences or matrix transformations, which are simple to implement and enhance encryption. However, since only the pixel positions are modified and not the pixel values, the encrypted image's histogram remains identical to the original, making it vulnerable to statistical attacks. In the replacement phase, chaotic sequences alter the pixel values. This research introduces a novel encryption technique for color images (RGB type) based on DNA subsequence operations to secure these images, which often contain critical information, from potential cyber-attacks. The suggested method includes two main components: a high-speed permutation process and adaptive diffusion. When implemented in the MATLAB software environment, the approach yielded promising results, such as NPCR values exceeding 98.9% and UACI values at around 32.9%, demonstrating its effectiveness in key cryptographic parameters. Security analyses, including histograms and Chi-square tests,

were initially conducted, with passing Chi-square test outcomes for all channels; the correlation coefficient between adjacent pixels was also calculated. Additionally, entropy values were computed, achieving a minimum entropy of 7.0, indicating a high level of randomness. The method was tested on specific images, such as all-black and all-white images, and evaluated for resistance to noise and occlusion attacks. Finally, a comparison of the proposed algorithm's NPCR and UAC values with those of existing methods demonstrated its superior performance and suitability.

C. A new attack resistant encryption method based on hybrid chaotic-quantum key distribution (CQKD)

In this paper, a new hybrid chaotic-quantum encryption model is investigated aiming to solve the interception trouble of information transmission through insecure environment. In this model, the image encryption method is studied using block diagonal chaotic (BDC) matrix and quantum based private key. The block diagonal chaotic model is designed with structured matrix based on two different nonlinear chaotic sequences and private key bits combined with quantum walks (QWs) path. At sender, the key bits convert to QWs states to increase tamper resistant of quantum key distribution in noisy communication channel. At the receiver side, the received data is retrieved merely by both initial key bits and states as similar as the sender initial key bits and states. If the eavesdropper attempts to measure quantum based private key, the key bits change to different states compared to real sender states and drops the bits eavesdropped in quantum channel. We call the hybrid chaotic image encryption method with private key based on quantum states as chaotic quantum key distribution (CQKD) method. The key space is evaluated using CQKD model rather than chaotic based encryption method without quantum distributed states over impure channels. Considering the sensitivity of block diagonal chaotic-based encryption BDC method with accuracy of 10(-32), the key space is increased from 10111 to 10142×10a×f(ΔΦ)×(1Δpe)Ne with phase-shifted QWs. It guarantees no information access by attackers considering high security against brute-force attacks and outperforms rather than the conventional chaotic encryption schemes.

D. Enhancing satellite image security through multiple image encryption via hyperchaos, SVD, RC5, and dynamic S-box generation

In this paper, a novel image encryption scheme is presented that leverages a combination of hyperchaotic systems, Singular Value Decomposition (SVD), RC5 operations, permutation techniques, and a custom S-box generated via the XORshift algorithm. Multiple satellite images are merged into a single augmented image prior to encryption by this algorithm, effectively protecting against traffic analysis attacks that could compromise individual encrypted images. Once the augmented image is created, it is split into RGB color channels, and each channel undergoes a four-stage encryption process. The encryption process is initiated by the generation of a chaotic sequence from a six-dimensional (6D) hyperchaotic system. This initial key sequence is then manipulated and transformed into a new key using SVD. The transformed key sequence is utilized to XOR the original image, providing an initial layer of encryption. Subsequently, the image is divided into blocks, and RC5 operations are applied to each block to enhance the security of the encryption process. Following this, a permutation operation is performed on the image using the chaotic sequence generated earlier. Finally, an S-box, created from a random sequence generated by the XORshift algorithm, is applied to the image to further obscure the pixel values. The robustness of the algorithm is validated by numerical tests, demonstrating its effectiveness against both statistical, differential attacks and brute-force attacks, making it extremely difficult for third parties, such as cloud service providers, to identify any relational patterns between the encrypted satellite images. Specific numerical values that demonstrated an enhanced security level include a key space of 27016, entropy exceeding 7.999, and a cross-correlation of ≈ 0. This encryption method not only strengthens the protection of satellite imagery against unauthorized access but also ensures the integrity and confidentiality of the images, which are crucial for applications ranging from national security to environmental monitoring in an increasingly data-driven world.

III. PROPOSED METHODOLOGY

In this paper, we propose an encryption-decryption scheme which has advantages in two-layer security from a switched system and a random key matrix (generated from that switched system). This scheme consists of two main encryption stages: encrypting by switched system, then encrypting by random key matrix. In the first stage, we build a switched system with initial parameters, these parameters are considered as the

cryptographic key for decryption. In the second stage, we continue to encrypt the output image by using a random key matrix, this matrix is generated by the switched system above and this matrix will also serve as a cryptographic key in the decryption stage. Additionally, the recovered image can be fully reconstructed using the designed cryptographic keys from both stages. The contribution of this design is to enhance the security by two-layer security.

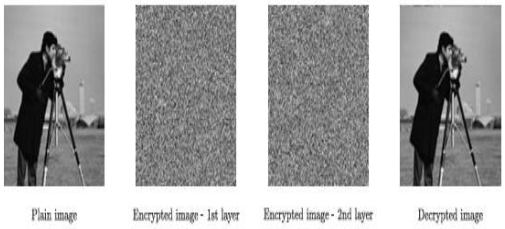
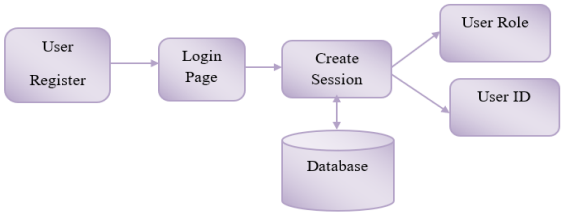


Fig. 1: System Overview

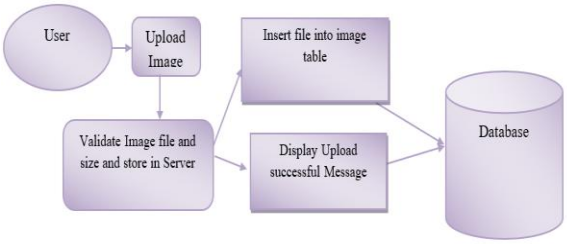
1. User Authentication Module

This module manages secure user access to the system. It allows users to register, log in, and log out using unique credentials. Passwords are encrypted before storing in the database to ensure data privacy. Once authenticated, the user session is created, enabling access to encryption and decryption features based on their role (user/admin).



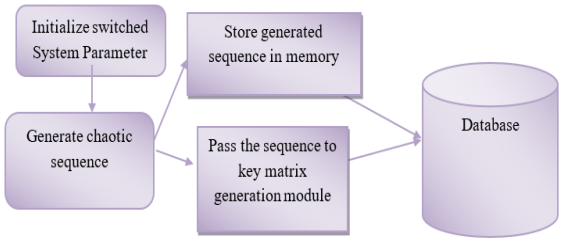
2. Image Upload Module

This module enables users to upload images (e.g., JPG, PNG) that need encryption or decryption. It performs file validation, saves the image on the server, and records details like file name, size, and upload time in the database. This module acts as the entry point for the encryption process.



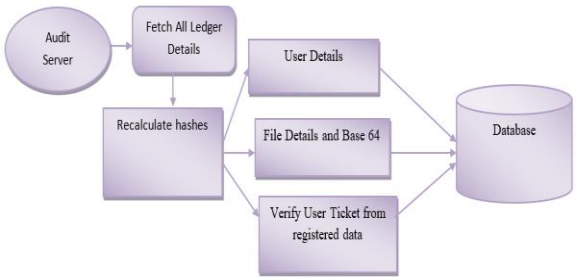
3. Switched System Generation Module

This module implements the control-theory-based switched system, which generates dynamic chaotic sequences by switching between multiple subsystems. These sequences serve as the foundation for random key matrix generation. The randomness and sensitivity of the switched system enhance the unpredictability of the encryption process.



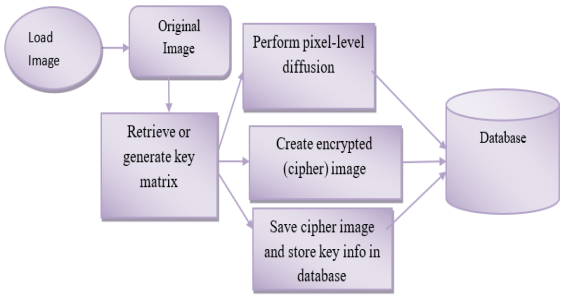
4. Random Key Matrix Generation Module

This module uses the chaotic sequences generated by the switched system to construct a random key matrix. The key matrix defines how each pixel will be encrypted or diffused. It ensures that each encryption process produces a unique cipher image even for the same input image. The key matrix is securely encrypted and stored in the database for later decryption.



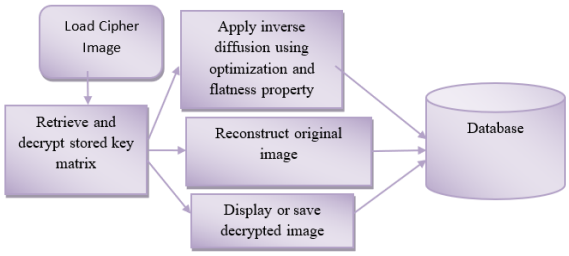
5. Image Encryption Module

This module performs the encryption operation using the random key matrix. It modifies pixel values based on matrix operations such as XOR or modular arithmetic to produce a cipher image. The encrypted image is saved on the server and linked to its key matrix record in the database. This step ensures strong protection against cryptanalytic attacks.



6. Image Decryption Module

This module reverses the encryption process to retrieve the original image. It fetches the encrypted key matrix from the database, decrypts it, and uses optimization and flatness-based techniques to restore the original pixel arrangement. The decrypted image is then displayed for verification.



7. Metrics and Evaluation Module

This module evaluates the encryption quality and robustness by calculating key performance metrics such as entropy, NPCR, UACI, pixel correlation, and histogram uniformity. These values help assess the

resistance of the encryption method against statistical and differential attacks.

8. Result Visualization Module

This module displays the output of encryption and decryption processes visually. It presents original, encrypted, and decrypted images side-by-side, along with numerical and graphical representations of performance metrics such as histograms and entropy charts.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed two-layer image encryption scheme provides strong security while maintaining computational efficiency. The method achieved high information entropy, low pixel correlation, excellent NPCR and UACI values, and uniform histogram distribution, indicating strong resistance to statistical and differential attacks. The switched system-based key generation and pixel diffusion process ensured accurate image reconstruction during decryption. Overall, the framework offers a robust and reliable solution for secure image encryption.



Fig. 2: User Registration



Fig. 3: Encryption



Fig. 4: Key Matrix



Fig. 5: Decryption



Fig. 6: Result

V. CONCLUSION

The proposed two-layer image encryption scheme effectively integrates hybrid system concepts, including switched systems and control theory, to enhance security and complexity in digital image protection. By leveraging the left inversion and flatness properties, the scheme ensures accurate reconstruction of images while providing robust encryption. Simulation results demonstrate that the scheme resists various cryptographic attacks, maintains high unpredictability, and achieves superior security compared to conventional single-layer encryption methods. Although minor synchronization transients may affect a few initial pixels during reconstruction, the overall decrypted image closely matches the original, confirming the efficiency and reliability of the proposed method. This indicates that the approach successfully balances computational efficiency with enhanced security, making it suitable for practical image encryption applications.

REFERENCES

[1] M.-L. Akkar and C. Giraud, ‘‘An implementation of DES and AES, secure against some attacks,’’ in Proc. 3rd Int. Workshop Cryptograph. Hardw. Embedded Syst., Paris, France, 2001, pp. 309–318.

[2] C. Zou, X. Wang, and H. Li, ‘‘Image encryption algorithm with matrix semi-tensor product,’’ Nonlinear Dyn., vol. 105, no. 1, pp. 859–876, Jul. 2021.

[3] S. Zhu, C. Zhu, and H. Yan, ‘‘Cryptanalyzing and improving an image encryption algorithm based on chaotic dual scrambling of pixel position and bit,’’ Entropy, vol. 25, no. 3, p. 400, Feb. 2023.

[4] W. Alexan, Y.-L. Chen, L. Y. Por, and M. Gabr, ‘‘Hyperchaotic maps and the single neuron model: A novel framework for chaos-based image encryption,’’ Symmetry, vol. 15, no. 5, p. 1081, May 2023.

[5] J. Tang, Z. Zhang, P. Chen, F. Zhang, H. Ni, and Z. Huang, ‘‘An image layered scrambling encryption algorithm based on a novel discrete chaotic map,’’ IET Image

Process., vol. 17, no. 2, pp. 518–532, Feb. 2023.

[6] E.Winarno, W. Hadikurniawati, K. Nugroho, and V. Lusiana, ‘‘Integrating quadratic polynomial and symbolic chaotic map-based feistel network to improve image encryption performance,’’ IEEE Access, vol. 12, pp. 106720–106734, 2024.

[7] M. Youssef, M. Gabr, W. Alexan, M. B. M. Mansour, K. Kamal, H. Hosny, and D. El-Damak, ‘‘Enhancing satellite image security through multiple image encryption via hyperchaos, SVD, RC5, and dynamic S-box generation,’’ IEEE Access, vol. 12, pp. 123921–123945, 2024.

[8] V. Mamandi, N. Ardalani, and B. Ghalamkari, ‘‘A new attack resistant encryption method based on hybrid chaotic-quantum key distribution (CQKD),’’ Quantum Inf. Process., vol. 23, no. 7, p. 265, Jul. 2024. [9] A. Yadav, B. Saini, V. K. Verma, and V. Pal, ‘‘A joint medical image compression and encryption using AMBTC and hybrid chaotic system,’’ J. Discrete Math. Sci. Cryptogr., vol. 24, no. 8, pp. 2233–2244, Nov. 2021.

AUTHORS Profile



Mrs. VANGALA SWATHI has received her B.Tech from JNTUH, Hyderabad in 2015, M.Tech degree in Computer science from JNTUH, Hyderabad in 2017. She is dedicated to teaching field from the last 7 years. Her research area Deep Learning. At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Ms. GANGAPURAM NANDINI pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. MANNEM AKHILA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Instit-utions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. NARRA BHARGAVA SAI pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. MARKANTI BHANU PRASAD pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.