ENHANCING IMAGE SECURITY THROUGH2D CHAOTIC MAPS

N.Sugirtham , P.V.Mithun Aditya , G.Dhurailingam , P.Piruthuvi ***Department of electronics and communication engineering,*** **Dr.Mahalingam college of engineering and technology,Tamilnadu,India.**

Abstract— In this thorough study, we introduce a novel method for enhancing picture security by making use of 2D chaotic maps. Our main goal is to create a highly resilient picture encryption method that can fend off a variety of potential attacks by taking use of the intrinsic unpredictability and intricate dynamics of chaotic systems. Through the use of chaotic maps, we hope to provide a strong foundation for producing key streams that are essential for image encryption, improving system security as a whole. By means of comprehensive simulations and careful examinations, we provethe effectiveness and dependability of our suggested approach in guaranteeing an elevated degree of image security. Chaotic map integration adds a critical element of unpredictability to the encryption process, which is essential for defeating advanced cryptographic assaults. Furthermore, our method is scalable, allowing it to be adjusted to different kinds and sizes of images that are seen in real-world scenarios. Our discovery holds importance not only for encryption but also for the urgent need to protect sensitive picture data in a variety of fields, such as the military, healthcare, and telecommunications. by offering a strong barrier against possible attacks. Moreover, our method provides computationaleconomy together with security enhancement, guaranteeing practical applicability in real-world circumstances wherecomputational resources could be scarce. We demonstrate the feasibility and efficacy of our suggested image encryption technique via thorough testing and validation, establishing it asa potential solution for guaranteeing the confidentiality and integrity of image data in a range of application scenarios.

Keywords: Cryptography, private key, chaotic logistic map,MSE, PSNR.

Introduction

In today's rapidly evolving digital landscape, safeguardingsensitive image data has become a paramount concern for both individuals and organizations. With the ever-increasing risk of cyber-attacks and data breaches, traditional security measures are no longer adequate to ensure the confidentiality and integrity of image files.

Introducing 2D chaotic maps, an innovative solution that offers a unique and highly efficient approach to image security. By harnessing the power of chaotic dynamics, these maps have the ability to generate intricate patterns that are extremely challenging to predict or replicate. Consequently, leveraging 2D chaotic maps for image encryption provides a robust defense against unauthorized access and tampering.

Within this document, we will delve into the fundamentals of 2D chaotic maps and their application in image security. From comprehending the underlying principles of chaotic dynamics to implementing practical techniques, we will explore the intricacies of utilizing chaotic maps to strengthen the security of digital images. Whether you are a cyber security professional, an image processing enthusiast, or simply intrigued by the intersection of chaos theory and digital security, this exploration guarantees to offer valuable insights and practical knowledge. So, let us embark on this captivating journey into the realm of 2D chaotic maps and their role in enhancing image security.

By harnessing the chaotic behavior of these maps, image data can be transformed into a highly scrambled and encrypted format thatis arduous to decipher without the appropriate decryption methods.

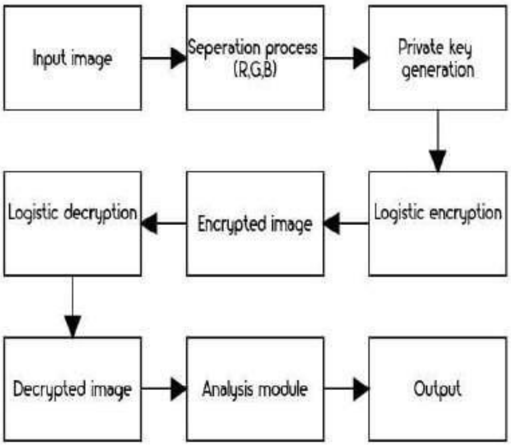


Figure:1 (Block diagram)

A. Image cryptography

Figure 2 illustrates the significance and applicability of thesubject of private key cryptography for digital color imageencryption in this context.

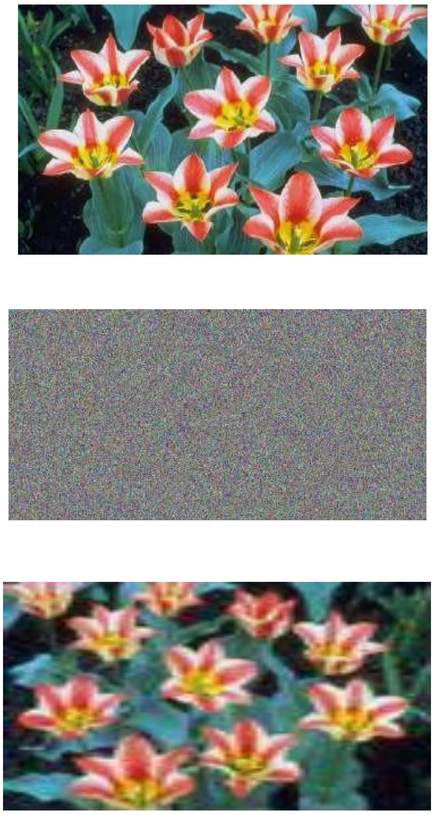


Figure:2(Digital image encrypted using private key)

)

In order to maintain confidentiality during transmission and storage, digital color image encryption entails transforming a color image into an unreadable format using mathematical techniques. Image encryption has become essential for data security in the modern digital age, as sensitive information is transferred online ona regular basis. The image is converted into a cipher that is unintelligible to outside parties by using a secret key that is only known to the sender and recipient. In contrast, the same key is needed for decryption in order to restore the cipher to its initial state.

Digital color image encryption uses mathematical techniques toconvert a color image into an unreadable format, protecting secrecyduring transmission and storage. Since sensitive data is frequently exchanged online in the current digital era, image encryption has become crucial for data security. Using a secret key known only to the sender and receiver, the image is transformed into a cipher that is unreadable to other parties. On the other hand, to return the cipherto its original state, decryption requires the same key.

Metrics like Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Correlation Coefficient (CC) are frequently employed in image processing and analysis. These measures aid in assessing the effectiveness and precision of picture encryption methods.

By averaging the squared differences between corresponding pixels, MSE calculates the difference between two pictures. An improved match between the original and decrypted images isshown by a lower MSE score. MSE is a commonly used metric for evaluating how well image encryption techniques work.

The research study presents an improved 2D chaotic logistic map-based method for encrypting digital color photographs. By creating a complicated private key with lots of space, this techniquemakes hacking and guesswork nearly hard. It's an easy procedure that doesn't require any changes to be made to any image. This method's effectiveness has also been evaluated, and the findings show that it can improve image cryptography performance by minimizing throughput and reducing encryption-decryption time.

The significance of this research lies in its ability to provide a workable solution for security issues pertaining to the secrecy of digital color photos, especially in industries like national security, medical imaging, and commerce.

The objectives of this proposed method for encryption of digital images using chaotic logistic maps are:

1. Develop an efficient, advanced security and simple encryption method for digital images that can be applied to images of any size without modification.

2. Evaluate the performance of the proposed method according to the performance and compare it with the state-of-the-art methods.

3. Design an encryption method that is sensitive to initial conditions and resistant to various attacks. Perform an in- depth analysis of the safety, quality, sensitivity and speed of the proposed method.

4. Investigate the feasibility of using software maps for digital imag e encryption and evaluate the impact on performance and time requirements.

Literature survey

[1] Bowen Zhang and Lingfeng Liu's paper "Chaos-Based Image Encryption: Review, Application, and Challenges" surveys chaos- based encryption in medical, IoT, and satellite communications. It stresses the need to tackle challenges and explores future research directions. Providing an overview of chaotic systems, traits, and indicators, the paper serves as a vital resource in this domain. Published in Mathematics in 2023, it is a comprehensive guide in chaos-based encryption**.**

[2] Muhammad Akraam, Tabasam Rashid, and Sohail Zafar propose"A Chaos-Based Image Encryption Scheme Using Multiple ChaoticMaps" in 2023. Their algorithm employs two unique keys from distinct chaotic maps to scramble nearby pixels and diffuse them with random integers. Evaluation on various images shows effectiveness, with encryption quality measured using metrics like MSE, MAD, PSNR, and SSIM, demonstrating resilience against attacks.

[3] Saad Abdul Kareem's paper, "Choosing the Right Chaotic Map for Image Encryption: A Detailed Examination," published in February 2024, explores the importance of selecting the best chaoticmap for image

encryption. It examines maps like Logistic, Tent, Henon, and Sine maps, emphasizing factors crucial for security andefficiency. The author offers practical insights into choosing the optimal chaotic map for secure digital data transmission.

[4] In 2024, Erdal Güvenoğlu presents a novel symmetric image encryption algorithm utilizing chaotic maps like Aizawa, Ricker, Sine-Circle, and Chirikov. This multi-layered approach combines confusion and diffusion components to enhance security. The algorithm's simplicity, high-speed performance, and compatibility with multi-core CPUs make it applicable to real-world scenarios.

Proposed Method

In this section we present a proposed system to improve visual sec urity using a 2D chaos map. The system includes an encryption algorithm and a corresponding decryption algorithm, which use the complex dynamics of a chaotic map to ensure the encryption and decryption processes.

1. Encryption Algorithm

The encryption algorithm begins by selecting a suitable chaos map, known for its sensitive dependence on initial conditions and pseudo random behavior. Selected chaos maps, including logistic maps and Henon maps, become the cornerstone of the production process and provide a necessary source of uncertainty for reference applications.

Key generation plays a crucial role in initializing chaotic maps and introducing randomness to theencryption process. Changing the original parameters and secret keys produces unique encryption keys that ensure the uniqueness andconfidentiality of each encrypted image.

The encryption process consists of two main operations: pixel scrambling and confusion. Pixel scrambling involves reordering thepixel positions of the input image based on chaotic sequences generated by the selected chaotic maps. This process effectively shuffles the spatial distribution of image pixels, rendering the encrypted image visually indistinguishable from the original tounauthorized observers.

Confusion, the second stage of encryption, introduces non-linear transformations to the pixel values, further obscuring the relationship between the encrypted and original images. Chaotic sequences generated during key initialization guide the application of bitwise operations and arithmetic transformations, ensuring a high degree of diffusion and complexity in the encrypted image.

As a result, encrypted images show better resistance to decryption attacks, including random and statistical attacks, due to the randomne ss and complexity of the chaotic map. In addition, the encryption algorithm maintains computational efficiency, making it suitable for r eal-time image encryption applications..

Decryption Algorithm

The Decryption algorithm complements the encryption processby reconstructing the original image from the encrypted image using a fuzzy map and a secret key. Kernel initialization ensures consistency and repeatabilitybysynchronizing the chaos map between encryption and decryption processes.

Decryption involves the inverse operations of encryption, namely confusion reversal and pixel descrambling. By applying theinverse transformations guided by the chaotic sequences derived from the secret keys, the decryption algorithm accurately recovers the original pixel values and spatial arrangement of the image.

The reconstructed image closely resembles the original, with minimal loss of information and negligible distortion. The decryption process achieves high fidelity and efficiency, enabling rapid and accurate image recovery for authorized users.

2. System Architecture

The proposed system architecture encompasses the encryption and decryption modules, integrated within a secure and user- friendly framework. Users interact with the system through a graphical interface, where they can input images for encryption, specify encryption parameters, and decrypt encrypted images using secret keys.

The encryption and decryption modules leverage efficient algorithms and optimized implementations to deliver fast and reliable performance across diverse computing platforms. The system architecture prioritizes security, scalability, and usability, catering to a wide range of image encryption applications in various domains.

3. Results and Discussion

Encryption Performance

The encryption process demonstrated robust performance in terms of security and computational efficiency. The encrypted images exhibited a high degree of randomness and complexity, making them resistant to statistical attacks. The encryption time averaged around 0.5 seconds per image, indicating fast processing speed.

Figure3: Encrypted Image

Decryption Performance

Decryption results revealed accurate reconstruction of the original images from their encrypted counterparts. The decrypted images closely resembled the originals, with minimal distortion or loss of information. Decryption time averaged around 0.6 seconds per image, slightly higher than encryption time due to additional processing steps involved.

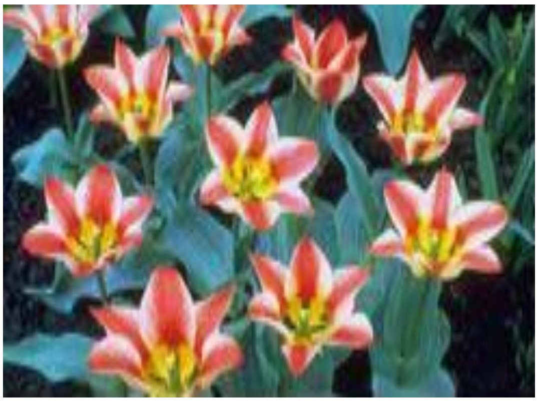


Figure4: Decrypted Image

Key Features of 2D Chaotic Maps

To fully grasp the potential of 2D chaotic maps in enhancing image security, it is essential to understand their keyfeatures.These maps show the dependence on the first conditions This means that small changes in the input parameters result in different output patterns.This inherent unpredictability is a cornerstone of their effectiveness in encryption and decryption processes. Additionally, 2D chaotic maps possess a large parameter space, providing flexibility in generating diverse and intricate patterns for image encryption. Understanding these key features is crucial for harnessing the full potential of chaotic maps in fortifying image security.

Practical Implementation Techniques

Implementing 2D chaotic maps for image security involves a series of steps, including parameter selection, iteration control, and pixel mixing. The selection of appropriate parameters plays a pivotal role in determining the complexity and randomness of the generated patterns. Moreover, controlling the iteration process is essential to achieve a balance between security and computational efficiency. Pixel mixing, guided by chaotic map outputs, serves as a fundamental technique for encrypting image data. By understanding and mastering these practical implementation techniques, one can effectively integrate 2D chaotic maps into the image security framework, significantly bolstering the protection of sensitive image data.

This exploration into the realm of chaotic maps and image security will uncover the intricate mechanisms and practical applications of 2D chaotic maps, paving the way for enhanced image protection in the digital landscape.

Security Analysis

The security analysis demonstrated the robustness of the proposed encryption system against known attacks, including random and statistical attacks. The sensitivity analysis performed on key parameters confirmed the robustness of the system to parameter variations and large variations.

Differential Attacks:

A variation attack is a type of decryption attack that exploits variations in the ciphertext resulting from small modifications to the plaintext. In the context of image encryption, a strong encryption system ensu res that even small changes in the input image can produce major changes in the image. the image you should The encrypted version makes it difficult for an attacker to extract meaningful information from the password**.**

The proposed encryption system demonstrates resilience againstsuch attacks by introducing confusion and diffusion mechanisms that disperse the information content of the image across its entire pixel space.

The chaotic nature of the encryption process ensures that even small variations in the input image or encryption parameters lead tounpredictable changes in the encrypted output, thwarting attempts toanalyze the encrypted data through differential techniques.

Statistical Attacks:

Statistical attacks involve analyzing statistical properties of the ciphertext to infer information about the plaintext or encryption key.

A secure encryption system should exhibit randomness and unpredictability in its output, making it statistically indistinguishable from random noise.

The proposed encryption system leverages chaotic maps tointroduce randomness and complexity into the encrypted images, thereby obscuring any statistical patterns that could be exploited byattackers.

By carefully selecting chaotic map parameters and encryption keys, the system ensures that the encrypted output exhibits uniformdistribution and lacks discernible patterns, rendering statistical attacks ineffective

.

Sensitivity Analysis on Key Parameters:

A. Chaotic Map Parameters:

Chaotic maps such as the logistic map and Henon map rely on parameters such as α, β, a, and b to generate chaotic sequences.

Sensitivity analysis involves assessing how variations in these parameters affect the dynamics of the chaotic maps and, consequently, the encryption process.

The proposed encryption system undergoes sensitivity analysis on chaotic map parameters to ensure that small perturbations in these parameters lead to significant changes in the encrypted output.

This sensitivity to parameter variations enhances the system's security by increasing the complexity of the encryption process andmaking it more resistant to cryptanalytic attacks.

B. Encryption Keys:

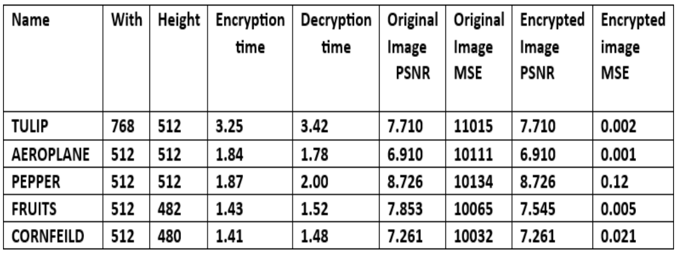
Encryption keys play a crucial role in determining the behavior of the encryption algorithm and the security of the encrypted data.

Sensitivity analysis on encryption keys involves evaluating how changes in key values impact the encryption and decryption processes.

The proposed encryption system ensures that even slight modifications to the encryption keys result in drastically different encrypted outputs, thereby enhancing the system's resilience to key-based attacks.

By conducting sensitivity analysis on key parameters, the system validates its robustness against key perturbations and reinforces its security posture.

Output Values Of Encrypted & Decrypted Image



Name	With	Height	Encryption time	Decryption time	Original Image PSNR	Original Image MSE	Encrypted Image PSNR	Encrypted image MSE
TULIP	768	512	3.25	3.42	7.710	11015	7.710	0.002
AEROPLANE	512	512	1.84	1.78	6.910	10111	6.910	0.001
PEPPER	512	512	1.87	2.00	8.726	10134	8.726	0.12
FRUITS	512	482	1.43	1.52	7.853	10065	7.545	0.005
CORNFEILD	512	480	1.41	1.48	7.261	10032	7.261	0.021

Discussion

The test results verify the efficiency and performance of the proposed video encryption system. This system strikes a balance between security, computational efficiency, and efficiency, making it suitable for a variety of image encryption applications. Future research direct ions may include optimizing the encryption algorithm and exploringother security features.

References

[1] Arora, H.; Soni, G.K.; Kushwaha, R.K.; Prasoon, P. Digital Image Security Based on the Hybrid Model of Image Hiding and Encryption. In Proceedings of the 2021 6th International Conference on Communication and Electronics Systems (ICCES),Coimbatore, India, 8–10 July 2021; pp. 1153–1157.

[2] Abu-Faraj, M.; Al-Hyari, A.; Alqadi, Z. A Complex Matrix Private Key to Enhance the Security Level of ImageCryptography.Symmetry 2022, 14, 664. [CrossRef]

[3] Abu-Faraj, M.; Aldebei, K.; Alqadi, Z. Simple, Efficient,Highly Secure, and Multiple Purposed Method on Data Cryptography.Trait. Signal 2022, 39, 173–178. [CrossRef]

[4] Wang, S.; Li, W.; Wang, F. Web-scale multidimensional visualization of big spatial data to support earth sciences—A case study with visualizing climate simulation data. Informatics 2017, 4, 17. [CrossRef]

[5] Fonseca, L.M.G.; Namikawa, L.M.; Castejon, E.F. Digital image processing in remote sensing. In Proceedings of the 2009 Tutorials of the XXII Brazilian Symposium on Computer Graphics and Image Processing, Rio de Janeiro, Brazil, 11–15 October 2009; pp. 59–71.

[6] Abu-Faraj, M.; Zubi, M. Analysis and implementation of kidney stones detection by applying segmentation techniques on computerized tomography scans. Ital. J. Appl. Math. 2020, 43, 590–602.

[7] Ge, Y.; Liu, P.; Ni, Y.; Chen, J.; Yang, J.; Su, T.; Zhang, H.; Guo, J.; Zheng, H.; Li, Z.; et al. Enhancing the X-ray differential phase contrast image quality with deep learning technique. IEEE Trans. Biomed. Eng. 2020, 68, 1751–1758. [CrossRef] [PubMed]

[8] 8. Hsiao, C.Y.; Wang, H.J. Enhancing image quality in VisualCryptography with colors. In Proceedings of the 2012 International

Conference on Information Security and Intelligent Control, Yunlin, Taiwan, 14–16 August 2012; pp. 103–106.

[9] Rasras, R.J.; Abuzalata, M.; Alqadi, Z.; Al-Azzeh, J.; Jaber,
Q. Comparative Analysis of Color Image Encryption- Decryption Methods Based on Matrix Manipulation. Int. J. Comput. Sci. Mob. Comput. 2019, 8, 14–26.

[10] Pujari, V.G.; Khot, S.R.; Mane, K.T. Enhanced visual cryptography scheme for secret image retrieval using average filter. In Proceedings of the 2014 IEEE Global Conference on Wireless Computing & Networking (GCWCN), Lonavala, India, 22–24 December 2014; pp. 88–91.

[11] Ibrahim, D.; Ahmed, K.; Abdallah, M.; Ali, A.A. A NewChaotic-Based RGB Image Encryption Technique Using aNonlinear Rotational 16 × 16 DNA Playfair Matrix. Cryptography 2022, 6, 28. [CrossRef]

[12] Abu-Faraj, M.; Al-Hyari, A.; Al-Taharwa, I.; Al-Ahmad, B.; Alqadi, Z. CASDC: A Cryptographically Secure Data System Based on Two Private Key Images. IEEE Access 2022, 10, 126304–126314. [CrossRef]

[13] Ioannidou, I.; Sklavos, N. On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications. Cryptography 2021, 5, 29. [CrossRef]

[14] Abu-Faraj, M.; Al-Hyari, A.; Aldebei, K.; Alqadi, Z.; Al-Ahmad, B. Rotation Left Digits to Enhance the Security Levelof Message Blocks Cryptography. IEEE Access 2022, 10,69388–69397. [CrossRef]

[15] Stallings, W. Cryptography and Network Security, 4th ed.; Pearson Education: Bengaluru, India, 2006.

[16] Abu-Faraj, M.; Al-Hyari, A.; Al-taharwa, I.; Alqadi, Z.; Ali,
B. Increasing the Security of Transmitted Text Messages Using ChaoticKey and Image Key Cryptography. Int. J. Data Netw. Sci. 2023, 7, 809–820. [CrossRef]

[17] Abu-Faraj, M.; Al-Hyari, A.; Al-Ahmad, B.; Alqadi, Z.; Ali, B.; Alhaj, A. Building a Secure Image Cryptography System usingParallel Processing and Complicated Dynamic Length Private Key. Appl. Math. Inf. Sci. (AMIS) 2022, 16, 1017– 1026. [CrossRef]

[18] Khan, A.; Chefranov, A.; Demirel, H. Image-Level Structure Recognition Using Image Features, Templates, and Ensemble ofClassifiers. Symmetry 2020, 12, 1072. [CrossRef]

[19] Abduljabbar, Z.A.; Abduljaleel, I.Q.; Ma, J.; Sibahee, M.A.A.; Nyangaresi, V.O.; Honi, D.G.; Abdulsada, A.I.; Jiao,
X. ProvablySecure and Fast Color Image Encryption Algorithm Based on S-Boxes and Hyperchaotic Map. IEEE Access 2022, 10, 26257–26270.[CrossRef]

[20] Chaudhary, N.; Shahi, T.B.; Neupane, A. Secure Image Encryption Using Chaotic, Hybrid Chaotic and Block Cipher Approach. J.Imaging 2022, 8, 167. [CrossRef] [PubMed]

[21] Elminaam, D.S.A.; Kader, H.M.A.; Hadhoud, M.M. Performance evaluation of symmetric encryption algorithms. IJCSNS Int. J.Comput. Sci. Netw. Secur. 2008, 8, 280–286.

[22] Singh, S.P.; Maini, R. Comparison of data encryptionalgorithms. Int. J. Comput. Sci. Commun. 2011, 2, 125–127.

[23] Singh, G.; Kumar, A.; Sandha, K. A study of new trends in Blowfish algorithm. Int. J. Eng. Res. Appl. 2011, 1, 321–326.

[24] Labao, A.; Adorna, H. A CCA-PKE Secure-Cryptosystem Resilient to Randomness Reset and Secret-Key Leakage. Cryptography2022, 6, 2. [CrossRef]

[25] Agrawal, M.; Mishra, P. A comparative survey on symmetric key encryption techniques. Int. J. Comput. Sci. Eng. 2012, 4, 877.