iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

CHAOTIC MAP DRIVEN IMAGE ENCRPTION FOR ENHANCED SECURITY

Ms. N. SUGIRTHAM,
Assistant Professor, Department of Electronics and Communication Engineering,
Dr. Mahalingam College of Engineering and Technology, Pollachi, Tamilnadu, India
nsugirtham@gmail.com

A E HEMALATHA,
Student, Department of Electronics and Communication Engineering,
Dr. Mahalingam College of Engineering and Technology, Pollachi, Tamilnadu, India
hemachezhiyan@gmail.com

ABSTRACT
In order to improve security, the project focuses on chaotic map-driven image encryption, which uses Arnold's Cat Map in conjunction with the 2D Sine Map to create confusion and pixel scrambling. While Arnold's Cat Map offers a non-linear distortion that further jumbles the image pixels to fortify encryption, the 2D Sine Map, which is notorious for its chaotic character, produces random values that are essential for the first transformation. To provide strong data protection, the encryption algorithm SEME-TDHM (Secure Enhanced Modified Encryption - Time-Dependent Hybrid Mapping) integrates both of these chaotic maps in a time-dependent way. Multiple rounds of transformations and substitutions are incorporated into the SEME-TDHM algorithm to guarantee a high level of complexity, which strengthens the encryption against a variety of assaults. The image's security is further increased by the combination of chaotic maps and the SEME-TDHM algorithm, which guarantees that the encrypted output is extremely difficult to decipher without the right keys, providing a cutting-edge method for secure image transmission.

INTRODUCTION

Since digital photographs are becoming more and more susceptible to harmful attacks and illegal access, the field of image encryption is essential to maintaining their security and privacy. Effective encryption methods are becoming more and more necessary due to the extensive usage of image-based data transmission in a variety of applications, including personal data sharing, security surveillance, and medical imaging. Because they may not take into consideration the complexity of image data and are susceptible to a variety of cryptographic attacks, traditional encryption techniques like symmetric and asymmetric algorithms are frequently insufficient to guarantee a high level of security for images. Because of its intrinsic unpredictability and sensitivity to initial conditions, chaotic maps have drawn a lot of attention as a solution to this problem in picture encryption. Chaotic systems, such as Arnold's Cat Map and the 2D Sine Map, provide a reliable way to produce incredibly intricate transformations that make it very difficult for unauthorized parties to decode the encrypted data. Arnold's Cat Map works well for changing pixel placements, improving the image's diffusion and confusion qualities, while the 2D Sine Map offers a pseudo-random sequence that adds chaotic behavior. To greatly improve the security of image encryption, we provide a unique encryption technique in this project called Secure Enhanced Modified Encryption-Time Dependent Hybrid Mapping (SEME-TDHM), which integrates the 2D Sine Map and Arnold's Cat Map in a time-dependent manner. The algorithm's multi-phase encryption procedure, which includes both pixel replacement and scrambling, guarantees a high level of security and makes it impervious to cryptanalysis and brute force attacks. SEME-TDHM guarantees that every encrypted image is distinct by fusing chaotic maps with a time-dependent technique. This offers strong defense against unwanted decryption and a dependable solution for secure image transmission in contemporary communication systems.

LITERATURE SURVEY

The study of dynamical systems with deterministic unpredictability, nonlinearity, and sensitive dependence on initial conditions is known as chaos theory. It is very desirable in encryption to ensure unpredictability, and a small change in the initial parameters of such systems can produce entirely different results.Large key spaces,

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

nonlinear behavior, and high entropy are characteristics of pseudo-random sequences produced by chaotic systems. Because they can work directly on two-dimensional image matrices, two-dimensional (2D) chaotic maps provide more complex and nonlinear behavior than their one-dimensional counterparts. This makes them especially helpful in image encryption.The main application for Arnold's Cat Map, a periodic, deterministic map, is image permutation. Using a mathematical transformation, it jumbles pixel positions across iterations while preserving decryption reversibility.Compared to the 1D Logistic map, the 2D Sine Map provides better randomness and more robust chaotic behavior. It is frequently used to generate substitution keys as well as to cause confusion (pixel permutation). These maps have been used in numerous studies to achieve notable statistical improvements in encryption strength (e.g., Chen et al., 2014; Wang et al., 2012). However, because of their limited key variation and periodicity, they can occasionally be subject to brute-force and known-plaintext attacks when used independently. In hybrid encryption models, both 2D Sine Map and Arnold's Cat Map are commonly included. Typically, a 2D Sine Map is used to create a pseudo random sequence for changing pixel values (diffusion phase) after Arnold's Cat Map is used to jumble pixel positions (confusion phase). By rendering both pixel locations and values unidentifiable to an attacker, this two-layer technique greatly increases security.

METHODOLOGY

Preprocessing images Image preparation is the initial stage of the SEME-TDHM image encryption technique. In this stage, the input image is loaded and, if necessary, converted to grayscale format. Each color channel (Red, Green, and Blue) can be processed independently if the image is RGB. In order to guarantee compatibility with the chaotic systems that will be utilized later, the image's pixel values are then normalized to a range of [0, 1]. If necessary, some chaotic maps, such as Arnold's Cat Map, may additionally scale the image to a square dimension. The image will be in the correct format for the next encryption phases thanks to this preparation. Initialization of Keys Key initialization is the following stage, during which a secret key is manually generated or supplied. Since it will be used to initialize the chaotic maps during the encryption process, this key is crucial. The key guarantees that the encryption procedure is distinct for every image and affects the chaotic system's beginning circumstances. The encrypted image's security depends on a correctly configured key. After initialization, the key is utilized to set the initial values of Arnold's Cat Map and the 2D Sine Map, which will be in charge of pixel diffusion and permutation in subsequent stages. Generation of Chaotic Key Stream Using 2D Sine Map This stage uses the 2D Sine Map to create a chaotic key stream. A non-linear, deterministic system that is sensitive to initial conditions, the 2D Sine Map can produce pseudo-random sequences. The secret key affects the parameters a, b, c, and d, while the resulting key stream's unpredictability is determined by the number of iterations. During the encryption process, the pixel values are then altered using this chaotic sequence. The encryption is unpredictable and extremely sensitive to even slight modifications in the beginning conditions or key thanks to the chaotic key stream. Scrambling of Image Pixels Using Arnold’s Cat Map Arnold's Cat Map is then used to jumble the image's pixels. A popular example of a chaotic map that permutes the image pixels is Arnold's Cat Map. A matrix-based transformation is used to rearrange the image's pixels, combining their locations in a deterministic but chaotic way. To create a high degree of pixel scrambling, this operation is repeated multiple times.Pixel positions become jumbled as a result of this transformation's iteration, confusing the image. Diffusion of Pixel Values Using Chaotic Key Stream The algorithm proceeds to diffusion after scrambling. In this stage, the chaotic key stream produced by the 2D Sine Map is used to alter the pixel values of the jumbled image. Using the chaotic key stream and operations like XOR or modular addition, diffusion is accomplished. In order to guarantee that small changes in the input image result in significant changes in the encrypted image, this stage modifies each pixel in a non-linear fashion. The encryption is extremely sensitive to beginning conditions because to the chaotic nature of the key stream, which makes it impervious to attacks. Entropy-Based Control (SEME) An adaptive technique that improves encryption security is the entropy-based control (SEME) step. This phase involves calculating the intermediate image's Shannon entropy. Entropy, which quantifies the image's randomness or unpredictability, is crucial in determining how many repetitions are needed for pixel scrambling and diffusion. An image is more secure if its entropy is larger since it is more unexpected. The main benefit of SEME is that it adjusts the encryption procedure according to the intrinsic complexity of the image. For images with higher entropy, the approach guarantees stronger encryption by varying the number of iterations or map parameters. Generation of Final Encrypted Image After performing pixel scrambling and diffusion, the final encrypted image is generated. If the image is in color (RGB

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

format), the encryption process is applied separately to each color channel, and then the channels are recombined to form the encrypted color image. At this stage, the image is fully encrypted, with both confusion (from pixel scrambling) and diffusion (from chaotic value modification) applied to make the image nearly impossible to decipher without the correct key. Decryption Process The opposite of the encryption process is the decryption procedure. The same secret key that was used to encrypt the image must be used to decrypt it. Reversing the encryption process's actions is part of the decryption procedures. First, the inverse of the chaotic key stream is applied to reverse the diffusion stage. The original pixel coordinates are then restored by using the inverse of the Arnold's Cat Map transformation, which reverses the scrambling step. The original image is then recovered after the image has been rebuilt.

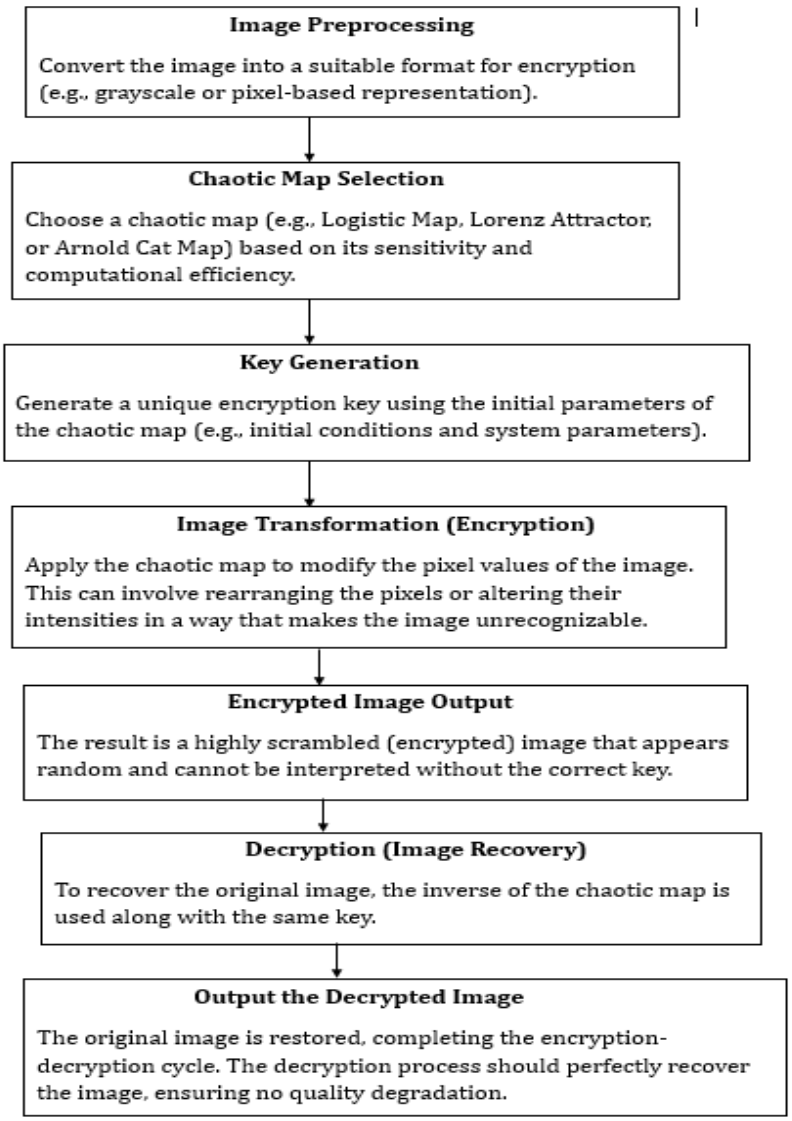

Figure 6.1 Workflow Block Diagram

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

APPLICATIONS

The proposed chaotic map-based image encryption system finds wide applicability in domains where secure image transmission and storage are critical. One of the most significant applications is in **secure image communication**, particularly in military, aerospace, and government operations where satellite images, surveillance footage, or intelligence data must be protected from interception. In the field of **medical imaging**, the method can be used to encrypt sensitive diagnostic images such as MRIs, CT scans, and X-rays, ensuring patient confidentiality and compliance with regulations like HIPAA and GDPR. Furthermore, the system is highly beneficial for **cloud storage and sharing**, enabling individuals and organizations to store encrypted images on cloud platforms without risking data breaches or unauthorized access.

Another important application lies in **digital forensics and surveillance**, where encrypted CCTV footage and drone images can help preserve the integrity of evidence. The algorithm also supports **copyright protection and digital watermarking**, safeguarding artistic and commercial media from piracy by embedding and protecting content before distribution. In **financial and legal sectors**, scanned documents, signatures, and identity proofs can be securely stored and transmitted using this encryption method, reducing the risk of forgery or data leakage. Additionally, the system is suitable for **IoT and smart devices**, including smart cameras and medical wearables, where images must be encrypted in real time before being processed or transmitted to the cloud. Lastly, as AI and deep learning models become capable of reconstructing image content, this encryption technique serves as a robust defense mechanism, ensuring that visual data remains unintelligible even to advanced analytical tools.

CONCLUSION

This study successfully integrated the SEHE TDHM algorithm with Arnold's Cat Map and the 2D Sine Map to demonstrate a secure and reliable image encrypt on method exploiting chaotic systems. The technique uses chaos theory's main advantages sensitivity to initial conditions, pseudo randomness, and non-linearity— to encrypt images with good security. The method successfully hides the spatial and intensity i information of the original image by using Arnold's Cat M ap for pixel location scrambling (confusion) and the 2D S ine Map for key stream creation (diffusion). A wide range of picture formats and application cases can benefit from the encryption strength's dynamic adaptation-based o n image complexity thanks to the use of hybrid entropy c ontrol (SEHE). The performance of the suggested system was confirmed by experimental data. Encrypted images displayed consistent histograms, near-ideal entropy values (~8), and great sensitivity to input and key fluctuations (NPCR > 99%, UACI ≈ 33%). These findings show robust defense against differential and statistical attacks.

REFERENCES

1. U. Erkan, A. Toktas, S. Enginoğlu, E. Karabacak, and D. N. H. Thanh, "An Image Encryption Scheme Based on Chaotic Logarithmic Map and Key Generation using Deep CNN," arXiv preprint arXiv:2012.14156, Dec. 2020.
2. L. Li, Y. Luo, S. Tang, L. Cao, and X. Ouyang, "Image encryption algorithm using chaotic maps and cellular automata," EAI Endorsed Transactions on Security and Safety, vol. 7, no. 26, Oct. 2020. EUDL
3. P. Murali, G. Niranjana, A. J. Paul, and J. S. Muthu, "Domain-flexible selective image encryption based on genetic operations and chaotic maps," The Visual Computer, vol. 39, pp. 1057–1079, Mar. 2023. SpringerLink
4. M. Roy, S. Chakraborty, and K. Mali, "An optimized image encryption framework with chaos theory and EMO approach," Multimedia Tools and Applications, vol. 82, pp. 30309–30343, Aug. 2023. SpringerLink
5. A. A. Abdul-Kareem and W. A. M. Al-Jawher, "An image encryption using hybrid grey wolf optimisation and chaotic map," International Journal of Information and Computer Security, vol. 16, no. 2, pp. 188–213, Sep. 2024. Inderscience Publishers
6. V. Himthania, V. S. Dhakaa, and M. Kaurb, "A visually meaningful image encryption scheme based on a 5D chaotic map and deep learning," The Imaging Science Journal, vol. 69, pp. 164–176, Jan. 2023. Taylor & Francis Online

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

7. [7] W. A. Farooqui, J. Ahmad, N. Kureshi, F. Ahmed, A. A. Khattak, and M. S. Khan, "Image Encryption Using DNA Encoding, Snake Permutation and Chaotic Substitution Techniques," arXiv preprint arXiv:2503.09038, Mar. 2025. arXiv
8. [8] J. Sun, "Construction of Hyperchaotic Maps Based on 3D CCC and its Applications in Image Encryption," arXiv preprint arXiv:2503.23655, Mar. 2025. arXiv

[9] S. K. Sharma and S. K. Gupta, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," International Journal of Information Security, vol. 21, pp. 917–935, Apr. 2022. SpringerLink

[10] S. Wang, W. Zhao, and X. Zhou, "Remote sensing image encryption algorithm using chaos and differential coding," Proceedings of the 15th International Conference on Digital Image Processing, pp. 1–6, 2023.

[11] S. Patel, B. K. P., and R. K. Muthu, "Image Encryption Decryption Using Chaotic Logistic Mapping and DNA Encoding," arXiv preprint arXiv:2003.06616, Mar. 2020. arXiv

[12] V. Patidar and G. Kaur, "A Novel Conservative Chaos Driven Dynamic DNA Coding for Image Encryption," arXiv preprint arXiv:2207.05475, Jul. 2022. arXiv

[13] F. A. Farooqui, J. Ahmad, N. Kureshi, F. Ahmed, A. A. Khattak, and M. S. Khan, "Image Encryption Using DNA Encoding, Snake Permutation and Chaotic Substitution Techniques," arXiv preprint arXiv:2503.09038, Mar. 2025. arXiv

[14] H. Wen, L. Zhang, and Y. Zhang, "Image Encryption Using a New Hybrid Chaotic Map and Spiral Transformation," Entropy, vol. 25, no. 11, p. 1516, Nov. 2023. MDPI+1River Publishers Journals+1

[15] S. Murali, G. Niranjana, A. J. Paul, and J. S. Muthu, "Domain-Flexible Selective Image Encryption Based on Genetic Operations and Chaotic Maps," The Visual Computer, vol. 39, pp. 1057–1079, Mar. 2023. These references provide additional insights into recent advancements in image encryption utilizing chaotic maps and related techniques, further enriching the foundation for your project's research.