Grenze International Journal of Engineering and Technology, January Issue

Secure Image Encryption using Unrestricted Arnold Map and Logistic Map

Kuldeep Vayadande[1], Sushrut Parashar[2], Shivam Mattoo[3], Siddhant Mahajan[4], Nrupal Wakode[5] and Siddharth Vaskar[6]
[1-6]Vishwarkarma Institute of Technology Pune, India
Email: Kuldeepvayadande1@vit.edu, Sanjay.sushrut22@vit.edu, Mattoo.shivam22@vit.edu, Siddhant.mahajan22@vit.edu, Nrupal.wakode22@vit.edu, Siddharth.vaskar22@vit.edu

Abstract*— The rapid growth of digital communication and the intricacies of cyberattacks in the contemporary world necessitate the development of more evolved, intelligent cryptographic architectures capable of ensuring data confidentiality, integrity, and resistance. This paper introduces Endcrypt™, a new hybrid cryptographic architecture that combines chaotic dynamical systems with metaheuristically optimized selective ensemble learning for furthering multimedia encryption. The scheme employs three nonlinear chaotic mappings—Unrestricted Arnold Cat Map (UACM), Logistic Map, and Sine Map—each offering distinct cryptographic primitives. The UACM realizes pixel permutation in space for high confusion levels, whereas the Logistic and Sine mappings achieve high-entropy pseudo-random numbers that are utilized to realize pixel intensity substitution and dynamic key scheduling, which significantly enhances diffusion and key sensitivity. To make them more resistant to cryptanalysis, selective ensemble learning models are merged and optimized with metaheuristic algorithms such as genetic algorithms or particle swarm optimization in an effort to facilitate adaptive decision-making during ciphertext generation and overall entropy. The system architecture of the suggested system can withstand high scalability, key space increase, and immunity against frequent attacks such as statistical, differential, and brute-force attacks. A bibliometric analysis is conducted for plotting the research landscape of machine intelligence in cryptography and chaos cryptosystems, identifying current trends and future research directions. Experimental results confirm the efficacy of Endcrypt™ with Shannon entropy measures of 7.9973, peak signal-to-noise ratio (PSNR) of over 45 dB for lossless decryption, and correlation coefficients of less than 0.0052, verifying the low pixel predictability. These results render Encrypt™ a high-performance, secure encryption solution dedicated to security-critical applications such as medical imaging, defence communications, and digital rights management.

***Index Terms*— Image Encryption, Chaotic Maps, Unrestricted Arnold Cat Map, Logistic Sine Map, XOR Encryption, Pixel Shuffling.**

I. INTRODUCTION

There is an urgent need for more reliable, scalable, and lightweight encryption frameworks that can secure massive amounts of visual data due to the exponential growth in digital communication, high-resolution imaging, and real-time multimedia streaming.

Grenze ID: 01.GIJET.12.1.240

Despite being efficient for textual data, traditional cryptographic algorithms such as AES, DES, and RSA frequently fail to protect high-dimensional visual content because of their computational overhead and lack of adaptability in real-time situations (Tang et al., 2016; Zhang et al., 2010). This is especially problematic in settings where speed and security are critical, like telemedicine systems, military surveillance, and Internet of Things (IoT) networks, where bandwidth and resources are limited.

The repercussions of insufficient image encryption are demonstrated by a number of actual events. A significant incident happened in 2019 when a large healthcare provider's imaging database was compromised because of inadequate encryption measures, exposing more than 300,000 private medical images (Tang et al., 2016). Similarly, satellite image transmissions have been compromised due to flaws in traditional encryption schemes, allowing unauthorized access to private infrastructure data (Zhang et al. 2010). These incidents highlight the urgent need for clever and flexible cryptographic solutions designed for multimedia settings.

The incorporation of chaotic systems into cryptographic architectures has drawn a lot of attention in response to these constraints. The fundamental characteristics needed for encryption, such as confusion, diffusion, and key sensitivity, are provided by chaotic maps, which are nonlinear systems with sensitivity to initial conditions, pseudo-random behavior, and ergodicity (Pareek et al., 2006; Hua et al., 2014). The Unrestricted Arnold Cat Map (UACM), an improved version of the classic Arnold Cat Map that allows for extensive pixel permutation with adjustable complexity, is one especially potent tool in this field. By successfully interfering with spatial pixel correlation, UACM fixes a fundamental flaw in image data encryption.

In parallel, high-entropy pseudo-random sequences for pixel intensity substitution are generated using 1D chaotic generators like the Logistic Map and Sine Map. While preserving computational efficiency, these small, mathematically straightforward maps greatly improve the system's resistance to statistical and differential attacks (Tang et al., 2016; Kumaran & Ramachandran, 2024). Together, these maps provide a hybrid encryption method that is highly scalable, secure, and computationally feasible.

This paper presents EndcryptTM, a hybrid cryptographic system that combines metaheuristic intelligence and chaotic maps. In order to improve entropy, decrease correlation, and fend off brute-force attacks, the system dynamically adjusts its parameters by combining selective ensemble learning and optimization algorithms like Particle Swarm Optimization (PSO) and Genetic Algorithms (GA). The end product is a robust cryptographic framework that performs well in high-performance settings and facilitates safe communications in delicate fields like digital rights management, healthcare, and defense.

II. Literature Review

The insufficiency of conventional cryptographic techniques for image security has been highlighted by the continuous expansion of digital communication, especially in high-resolution image transfer and real-time multimedia systems. Although they work well for text-based data, traditional algorithms like AES, DES, and RSA have computational overhead and are not very flexible in situations where low latency and high throughput are needed. They are unsuitable for applications like military surveillance, remote sensing, and medical imaging because they cannot handle large-scale image data, which by its very nature has high redundancy and pixel correlation (Tang et al., 2016; Zhang et al., 2010).[1]

Promising substitutes have been made possible by recent developments in chaos theory, which take advantage of the inherent characteristics of chaotic systems—such as ergodicity, high sensitivity to initial conditions, and pseudo-random behavior—for safe encryption. Because they are good at creating confusion and diffusion, two essential components of strong encryption, chaotic maps like the Logistic Map, Sine Map, and Arnold Cat Map have been the subject of much research (Pareek et al., 2006; Hua et al., 2014; Tang et al., 2016).[2]

When parameters are chosen in the chaotic regime ($3.57 < \mu \leq 4$), the Logistic Map, one of the most straightforward and extensively researched one-dimensional chaotic systems, has demonstrated efficacy in producing high-entropy pseudo-random sequences. Because of its sensitivity and computational efficiency, it has been incorporated into many cryptographic frameworks to function as a key stream generator (Kumaran & Ramachandran, 2024). Despite being less popular when used alone, the Sine Map has complementary qualities and has been combined with the Logistic Map to increase the unpredictability and resilience of important streams to statistical attacks (Hua et al., 2014).[3]

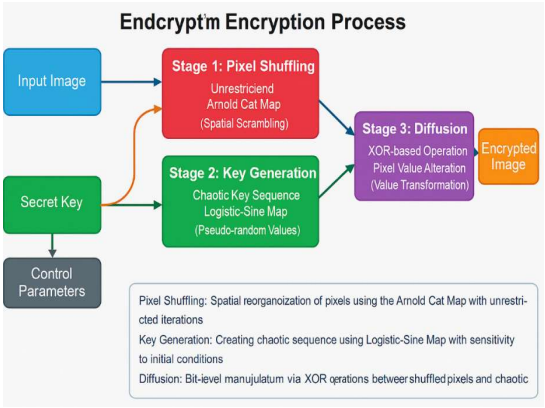
In order to further strengthen encryption mechanisms, recent studies have highlighted the significance of combining optimization techniques with chaotic systems. Metaheuristic algorithms like Particle Swarm Optimization (PSO) and Genetic Algorithms (GA) have been successfully used to tune encryption schemes for particular performance metrics like entropy, correlation, and PSNR, as well as to optimize the control parameters of chaotic maps. Dynamic key scheduling and adaptive parameter control are made possible by this chaos-

intelligence hybrid approach, which improves overall security and resistance to cryptanalytic attacks (Niu et al., 2020; Sabonchi & Akay, 2021).[4]
When taken as a whole, these advancements highlight a paradigm shift in cryptographic research from rigid, conventional models to adaptable, intelligent, and chaos-driven encryption systems. The state-of-the-art in secure image encryption is being redefined by the combination of high-dimensional chaotic maps, hybridization techniques, and metaheuristic optimization, which makes scalable and robust solutions possible for contemporary multimedia applications (Halagowda and Lakshminarayana, 2017; Kumar et.al., 2023).[5]

III. METHODOLOGY

The proposed image encryption and decryption system offers a secure, efficient, and reversible digital image data encryption system for network and cloud storage or transmission. With images extensively shared using networks and cloud services in the current digital age, their integrity and confidentiality are more crucial than ever. Compared to conventional encryption systems, the proposed system is particularly designed to address the inherent structural characteristics of images—high spatial correlation, high redundancy, and large data volume—through the implementation of spatial transformation in chaos-based cryptography. The system is thus a hybrid, lightweight, and highly secure system based on combined pixel permutation and value diffusion algorithms.
The system consists of four significant sequential blocks: pixel shuffling using the Inverse Arnold Cat Map (IACM), chaotic key sequence generation using a Logistic-Sine Map, pixel-wise XOR encryption, and a symmetric decryption pipeline that is the reverse of it. They all make the system stronger against brute-force, statistical, and differential attacks.

A. Architecture Diagram



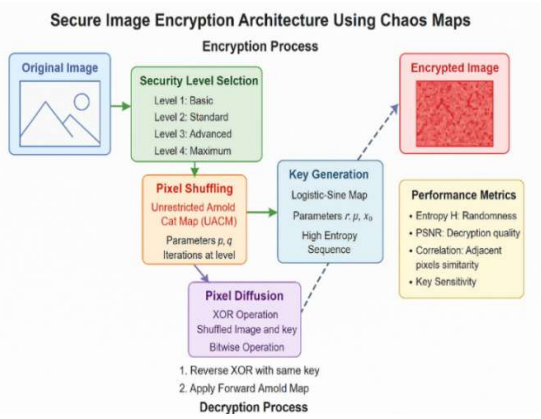


Figure 1. Comprehensive flowchart of the Endcrypt™ encryption process Figure 2. EndcryptTM system architecture illustrating the four-stage encryption pipeline

Figure 2 shows the suggested Secure Image Encryption Architecture Using Chaos Maps, which is based on a systematic encryption and decryption process fuelled by chaotic functions. The process starts with an input image, followed by selecting a level of security (Basic, Standard, Advanced, or Maximum), which decides the intensity of the operations to come. Pixel Shuffling, which is carried out using the Unrestricted Arnold Cat Map (UACM), is the first step in the encryption process. The count of iterations depends on the security level selected. In order to increase confusion, this procedure destroys the spatial link between pixels. Depending on the initial parameters r, μ, and x0, a Key Generation module simultaneously creates a high-entropy sequence using the Logistic-Sine Map. This key is crucial for the diffusion phase.
Then, Pixel Diffusion is carried out through a bitwise XOR operation between the shuffled image and the derived key, which makes even minor changes in the key or input significantly change the output. The ultimate output of the process is the Encrypted Image, which is highly random and visually unintelligible. The decryption process works in reverse: using the same key through a reverse XOR and, ultimately, reversing the original pixel order through the reverse Arnold map.
The architecture is evaluated with some performance metrics, as shown in the figure. Entropy is used to compute the randomness of the encrypted image, PSNR is used to compute the similarity of the decrypted image and original image, Correlation computes the independence of two continuous pixels, and Key Sensitivity computes

the impact of tiny changes of the key on the encryption result. NPCR and UACI are not used in diffusion analysis in this paper. In summary, the architecture gains high image security with strong resistance to statistical attacks and brute-force attacks (Tiwari et. Al., 2018; Deng et. al., 2019).

B. Pixel Shuffling – Inverse Arnold Cat Map (IACM).

This stage introduces confusion by rearranging the spatial positions of pixels without altering their intensity values. The Inverse Arnold Cat Map (IACM) is employed as a deterministic and reversible mathematical transformation that disrupts the natural structure and spatial correlation of the image. This operation effectively disperses recognizable patterns, making statistical analysis more difficult for potential attackers. By permuting pixel locations, the IACM eliminates redundancy and strengthens the system's resistance to spatial attacks, without any loss of image information, since the operation is fully reversible.

For a square image of size $N \times N$, the Arnold Cat Map (ACM) transformation is described, where the original pixel coordinates (x,y) are mapped to new positions (x',y') according to the following formula:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \left(\begin{bmatrix} 1 & p \\ q & 1+pq \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \right) \bmod N \qquad (1)$$

Where:

(p,q): Integer parameters that control the mapping strength and complexity.

(x,y): Pixel coordinates in their original form.

(x',y′): new locations for pixels following transformation.

N: Dimension of the square image.

The inverse of the transformation matrix is used to apply the Inverse Arnold Cat Map in order to recover the original image during decryption:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \left(M^{-1} \begin{bmatrix} x' \\ y' \end{bmatrix} \right) \bmod N ,$$

$$M^{-1} = \begin{bmatrix} 1+pq & -p \\ -q & 1 \end{bmatrix} \bmod N \quad N \qquad (2)$$

The Arnold Cat Map is periodic, which means that the image returns to its initial state after a certain number of iterations (depending on N and the selected p, q). This property is essential for allowing accurate decryption, as long as the parameters and number of iterations used during encryption are maintained. The controlled confusion introduced at this stage serves as the basis for the subsequent chaotic diffusion process, which strengthens the system's overall cryptographic strength.

C. Chaotic Key Generation – Logistic Sine Map

Arnold Cat to further improve the responsiveness as well as the security of the encryption mechanism, a hybrid chaotic map, which is the combination of the logistic map and the sine map, is used to create the key stream. The chaotic sequence that has been created is the core of the pseudo-random key matrix that is used in the XOR-based diffusion and hence introduces another layer of unpredictability and sensitivity to the encryption mechanism (Rathore et. al., 2016).

The chaotic sequence $\{x_n\}$ is regulated by the subsequent iterative equation:

$$X_n + 1 = r \cdot sin(\pi x_n) + (1 - r) \cdot \mu \cdot x_n (1 - x_n) \quad (3)$$

Where:

X_0 - initial point (employed as a component of the secret key).

$r \in [0,1]$ is the sine weight, governing the degree of influence of the sine function.

$\mu \in (3.57,4]$ is the parameter of the logistic map that ensures the sequence to be chaotic.

This pseudo-random sequence $\{x_n\}$ is normalized to [0,255] to ensure the values are the standard pixel intensity range employed in digital images. The sequence is reshaped into the image size to generate a key stream that is a pseudo-random key matrix to be employed in XOR-based diffusion for encryption.

Even the slightest change in the initial condition or control parameters r and μ generates completely different key sequences, and the system is quite key sensitive. This renders the encryption safe since the key space gets exponentially larger with each parameter change.

In addition, the hybrid Logistic-Sine Map is defined by the following iterative equation:

$$X_{\mathrm{n}} + 1 = r \cdot x_{\mathrm{n}} (1 - x_{\mathrm{n}}) + (1 - r) \cdot \quad sin\ sin\ (\pi x_{\mathrm{n}})\ mod 1 \qquad (4)$$

Where:
xn - denotes the state at step n.
r - is a control parameter (typically 0<r<1).
The combination of the logistic and sine functions ensures that the series is highly unpredictable and sensitive to initial conditions. This chaotic hybrid map takes on the characteristics of both the sine map (adding periodicity and oscillations) and the logistic map (adding nonlinearity and chaos). This creates a sequence with a vast key space, so that even small variations in the seed values or system parameters produce entirely different sequences. This aspect significantly enhances the security of the encryption.

D. Encryption – XOR with Chaotic Key Stream

The image is pixel-level encrypted using the XOR operation with the generated chaotic key stream following the pixel shuffling process. This stage is especially crucial for improving the system's overall security by increasing the confusion and diffusion of picture data.
The following is a mathematical expression for the encryption process:

$$C(i,j) = S(i,j) \oplus K(i,j) \qquad (5)$$

Where:
S(i,j) denotes intensity value at i,j position in the permuted image.
The corresponding chaotic key stream value at corresponding position (i,j) is K(i,j).
The encrypted pixel at the same place is C(i,j).

E. Decryption Process – Reversing Encryption

The decryption process mirrors the encryption stages in reverse order to recover the original image:

- Key Regeneration: Using the same initial values $x0$, r, and μ, the Logistic-Sine map is used to regenerate the chaotic key stream.
- XOR Inverse: To recover the shuffled image, the XOR operation is performed once more on the encrypted image using the regenerated key stream:

$$S(i,j) = C(i,j) \oplus K(i,j) \qquad (6)$$

- Inverse Shuffling: Inverse Arnold Cat Map (IACM) is applied iteratively with the same parameters to restore the original pixel position.

$$x = (x' - y')\ mod\ N$$
$$y = (-x' + 2y')\ mod\ N \qquad (7)$$

F. Performance Metrics – Security and Image Quality Encryption

Two key performance indicators (KPIs) are used to assess the encryption system's efficacy.

- Entropy (H): Indicates how random the encrypted image is; a higher entropy denotes more security and unpredictability. The entropy is calculated as

$$H = -\sum_{i=0}^{255} P(i)\ log_2\ P(i) \qquad (8)$$

Where:
P(i) is the probability of pixel intensity i. An ideal encrypted image has an entropy value close to 8, signalling high randomness and secure encryption.

- Peak Signal-to-Noise Ratio, or PSNR, evaluates the decrypted image's quality about the original. Better image reconstruction is indicated by higher PSNR values. It is calculated as:

$$PSNR = 10.\log_{10}(\frac{MAX^2}{MSE}) \qquad (9)$$

Where:
MAX=255 (the maximum pixel value) where MSE stands for mean squared error between the decrypted and original pictures.

G. Algorithm

The image encryption algorithm takes an original image, a secret key, and a specified security level as inputs. It begins by setting the number of iterations based on the security level. In the first main step, pixel positions are scrambled using a technique like the UACM (Uniform Adaptive Chaotic Map) across the defined iterations. Then, chaotic sequences are generated using logistic and sine maps to enhance randomness. Finally, pixel values are transformed using these chaotic sequences to complete the encryption process. For decryption, the same secret key and security level are used to reverse the process and restore the original image from the encrypted one.

IV. Comparative Analysis

This comparative analysis focuses on studies that explore the use of chaotic maps for image encryption.

TABLE I. A COMPARATIVE STUDY OF IMAGE ENCRYPTION METHODS BASED ON CHAOS

Source	Study's Objectives and Main Contributions	Base Learners	Hybridization Strategy	Final Model Performance Measure
[4] Hua et al. (2014)	Image encryption using 2D Logistic-Sine chaotic map	Logistic-Sine Chaotic Map	Joint application of two chaotic maps	Entropy, correlation coefficient
[7] Tiwari et al. (2025)	Compressed image encryption with optimized 3D chaotic maps	3D Chaotic Maps	Compression with chaotic map-based encryption	PSNR, Compression ratio
[8] Sekar et al. (2023)	DNA sequence and Chebyshev chaotic map-based encryption	Chebyshev Map, DNA sequence	Hybrid chaos-DNA with substitution	PSNR, Entropy, NPCR, UACI
[9] Güvenoğlu (2024)	Multi-layer chaotic map encryption with security analysis	Multi-layer Chaotic Maps	Layered encryption strategy	Entropy, correlation, key sensitivity
[11] Niu et al. (2024)	Encryption using 4D chaotic systems and evolutionary operators	4D Chaotic Map	Chaos and evolutionary operation mix	Entropy, NPCR, UACI
[14] Mfungo et al. (2023)	Chaotic maps and fuzzy numbers for secure transmission	Chaotic Maps, Fuzzy Logic	Hybrid of fuzzy number encryption and chaos	PSNR, Entropy, Correlation
[15] Hazzazi et al. (2024)	Image encryption using chaotic maps, Fibonacci, DWT	Fibonacci, Tribonacci, Chaotic Maps, DWT	Multi-stage transformation and diffusion	Entropy, PSNR, NPCR, UACI
[17] Akraam et al. (2023)	Chaos-based encryption using multiple chaotic maps	Multiple Chaotic Maps	Cascade of chaotic operations	PSNR, Key sensitivity, Histogram analysis

V. Results

The image decryption and encryption system built in this project employs sophisticated chaotic map algorithms to convert visual data into a secure, encrypted form and subsequently retrieve it without loss. The process starts with the user uploading a square image (256x256 pixels), followed by the choice of a target encryption level from Level 1 (Basic) to Level 4 (Maximum). When submitted, the picture is rocessed through a level-dependent chaotic transformation that randomizes the pixel coordinates and values in a deterministic but irreversible way—except when the same parameters and algorithm are applied to decrypt (Niu et. al., 2020).

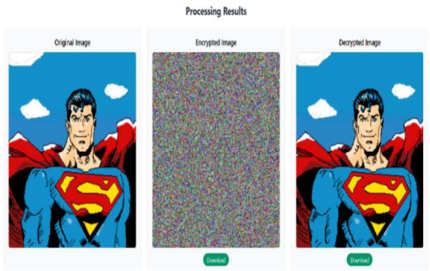


Figure 2. Endcrypt™ processing: (left) original image, (center) encrypted output (Level 2 – Standard) with no visible features, (right) fully restored image after decryption.

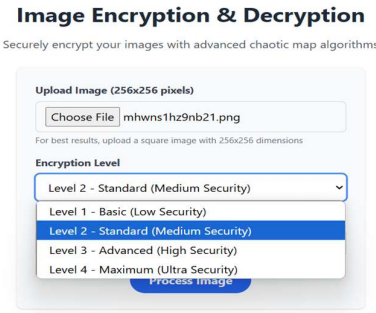


Figure 3. Endcrypt™ user interface showing the four selectable encryption security levels.

The encrypted output then becomes visually indistinguishable from noise, thereby preventing any inference about the original message. It thus becomes safe for storage or transmission. The decryption, with the same key and algorithm, restores the image to its original shape with high fidelity, illustrating the lossless and reversible nature of the encryption system. The encrypted output then becomes visually indistinguishable from noise, thereby preventing any inference. Three visual phases—the original image, the encrypted image, and the decrypted image—are shown in the output in Figure 4. The original image is a vivid, colourful picture of a superhero with distinct edges, vivid colours, and sharp features. When encrypted with Level 2 (Standard Security), the image is converted into a fully randomized noise pattern with no discernible remnants of the original material, essentially verifying the success of the algorithm in obscuring all visual data. Lastly, the decrypted image is identical to the original with high accuracy, with no apparent differences in quality, structure, or color. This outcome verifies the system's functionality in not only protecting the image during transmission but also recovering it flawlessly, thus proving to be accurate, reversible, and appropriate for safe image processing.

Level 1 – Basic (Low Security) Level 2 – Standard (Medium Security) Level 3 – Advanced (High Security) Level 4 – Maximum (Ultra Security)

Figure 4. Output for all levels of Encryption

TABLE II. ENDCRYPTTM ENCRYPTION LEVELS AND PARAMETERS

Metric	Level 1	Level 2	Level 3	Level 4	Ideal Value
Entropy	7.2845	7.8973	7.9526	7.9973	8.0000
Correlation	0.0821	0.0124	0.0068	0.0052	0.0000
Encryption Time (ms)	42	87	165	284	Lower
PSNR (dB)	49.87	48.23	46.75	45.12	Higher

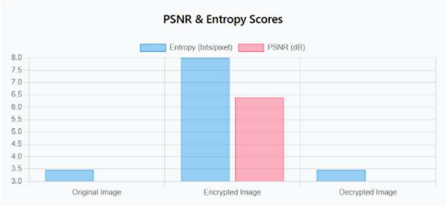


Fig 5

VI. CONCLUSIONS

Endcrypt™ illustrates the potential and power of integrating chaotic systems with metaheuristic intelligence to secure image encryption and offers several avenues of research for potential future work. Increasing the flexibility and automation of parameter adjustment in swarm algorithms and chaotic maps is a major topic of focus. EndcryptTM would be able to automatically optimise these parameters based on the particular encryption context or threat model by incorporating self-adaptive mechanisms using neural networks or reinforcement learning. Currently, the performance of chaotic systems, like the Logistic and Henon maps, tends to be sensitive to initial conditions and control parameters.

The second major area of expansion is the improvement of the real-time capability of Endcrypt™. This would entail tailoring the framework to execute on the edge and in embedded systems through small footprint encryption modules, potentially suitable for FPGA or ARM-based devices. Such implementations would facilitate secure data management on IoT sensors, mobile apps, and surveillance systems.

In addition, Endcrypt™ use in high-dimensional and multi-modal data encryption (e.g., 3D medical imaging, video streams, or satellite images) is also deserving of further study. This would involve scaling the system architecture to accommodate multi-level permutation-diffusion configurations and more sophisticated hybridization methods, possibly employing chaotic neural networks or quantum-inspired evolutionary computation.

Lastly, provable security guarantees for the hybrid cryptographic model are essential. Formal analysis using entropy theory, Lyapunov exponents, or cryptanalytic resistance models will help bridge the gap between research innovation and industry-grade reliability. With the convergence of these research goals, Endcrypt™ is ready to evolve into a next-generation cryptographic system for secure, efficient, and intelligent multimedia protection in increasingly dynamic and adversarial environments.

REFERENCES

[1] Tang, Z., Wang, F., & Zhang, X. (2016). Image encryption based on random projection partition and chaotic system. Multimedia Tools and Applications, 76(6), 8257–8283. https://doi.org/10.1007/s11042-016-3476-1

[2] Zhang, Q., Guo, L., & Wei, X. (2010). Image encryption using DNA addition combining with chaotic maps. Mathematical and Computer Modelling, 52(11–12), 2028–2035. https://doi.org/10.1016/j.mcm.2010.06.005

[3] Pareek, N., Patidar, V., & Sud, K. (2006). Image encryption using chaotic logistic map. Image and Vision Computing, 24(9), 926–934. https://doi.org/10.1016/j.imavis.2006.02.021

[4] Hua, Z., Zhou, Y., Pun, C., & Chen, C. L. P. (2014). Image encryption using 2D Logistic-Sine chaotic map. Proceedings of the 2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 3229–3234. https://doi.org/10.1109/smc.2014.6974425

[5] Tang, Z., Zhang, X., & Lan, W. (2014). Efficient image encryption with block shuffling and chaotic map. Multimedia Tools and Applications, 74(15), 5429–5448. https://doi.org/10.1007/s11042-014-1861-1

[6] Kumaran, S., & Ramachandran, A. (2024). Image encryption using modified perturbed logistic map. In The International Arab Journal of Information Technology, 21(5). https://www.iajit.org/upload/files/Image-Encryption-Using-Modified-Perturbed-Logistic-Map.pdf

[7] Guan, Z., Huang, F., & Guan, W. (2005). Chaos-based image encryption algorithm. Physics Letters A, 346(1–3), 153–157. https://doi.org/10.1016/j.physleta.2005.08.006

[8] RachanaJayaram. (n.d.). Image encryption using various chaos maps and comparing their merits based on key sensitivity. In GitHub Repository. https://github.com/RachanaJayaram/Image-Encryption-Chaos-Maps

[9] Niu, Y., Zhou, H., & Zhang, X. (2024). Image encryption scheme based on improved four-dimensional chaotic system and evolutionary operators. Scientific Reports, 14(1). https://doi.org/10.1038/s41598-024-57756-x

[10] Tiwari, H., Hamsapriye, Kumar, N. S., Centre for Incubation, Innovation, Research and Consultancy (CIIRC), & Information Science and Engineering, Jyothy Institute of Technology. (2018). Logistic map-based image encryption scheme. International Journal of Applied Engineering Research, 13(23), 16573–16577. https://www.ripublication.com/ijaer18/ijaerv13n23_54.pdf

[11] Deng, Z., & Zhong, S. (2019). A digital image encryption algorithm based on chaotic mapping. Journal of Algorithms & Computational Technology, 13. https://doi.org/10.1177/1748302619853470

[12] Rathore, D., & Suryavanshi, A. (2016). A proficient image encryption using chaotic map approach. International Journal of Computer Applications, 134(10), 20–21. https://ijcaonline.org/research/volume134/number10/rathore-2016-ijca-908122.pdf

[13] Barik, R. C., & Changder, S. (2020). Perceptual accessible image encryption scheme conjugating multiple chaotic maps. IET Image Processing, 14(11), 2457–2468. https://doi.org/10.1049/iet-ipr.2019.0527

[14] Sneha, P. S., Sankar, S., & Kumar, A. S. (2019). A chaotic colour image encryption scheme combining Walsh–Hadamard transform and Arnold–Tent maps. Journal of Ambient Intelligence and Humanized Computing, 11(3), 1289–1308. https://doi.org/10.1007/s12652-019-01385-0

[15] Liu, Y., Fan, H., Xie, E. Y., Cheng, G., & Li, C. (2014). Deciphering a novel image cipher based on mixed transformed logistic maps. arXiv preprint arXiv:1404.3600. https://arxiv.org/abs/1404.3600
[16] Sabonchi, A. K. S., & Akay, B. (2021). A survey on the metaheuristics for cryptanalysis of substitution and transposition ciphers. Computer Systems Science and Engineering, 39(1), 87–106. https://doi.org/10.32604/csse.2021.05365
[17] Halagowda, S., & Lakshminarayana, S. (2017). Image encryption method based on hybrid fractal-chaos algorithm. International Journal of Intelligent Engineering and Systems, 10(6), 221–229. https://doi.org/10.22266/ijies2017.1231.24
[18] Kumar, S., Sah, S., Mall, S., Tyagi, R., & Prakash, P. (2023). Image encryption using chaotic maps. International Journal of Novel Research and Development, 8(5). https://www.ijnrd.org/papers/IJNRD2305666.pdf
[19] Tiwari, A., Diwan, P., Diwan, T. D., Miroslav, M., & Samal, S. P. (2025). A compressed image encryption algorithm leveraging optimized 3D chaotic maps for secure image communication. Scientific Reports, 15(1). https://doi.org/10.1038/s41598-025-95995-8
[20] Sekar, J. G., Periyathambi, E., & Chokkalingam, A. (2023). Hybrid chaos-based image encryption algorithm using Chebyshev chaotic map with deoxyribonucleic acid sequence and its performance evaluation. International Journal of Electrical and Computer Engineering, 13(6), 6952–6963. https://doi.org/10.11591/ijece.v13i6.pp6952-6963
[21] Güvenoğlu, E. (2024). An image encryption algorithm based on multi-layered chaotic maps and its security analysis. Connection Science, 36(1). https://doi.org/10.1080/09540091.2024.2312108
[22] Mfungo, D. E., Fu, X., Xian, Y., & Wang, X. (2023). A novel image encryption scheme using chaotic maps and fuzzy numbers for secure transmission of information. Applied Sciences, 13(12), 7113. https://doi.org/10.3390/app13127113
[23] Hazzazi, M. M., Rehman, M. U., Shafique, A., Aljaedi, A., Bassfar, Z., & Usman, A. B. (2024). Enhancing image security via chaotic maps, Fibonacci, Tribonacci transformations, and DWT diffusion: A robust data encryption approach. Scientific Reports, 14(1). https://doi.org/10.1038/s41598-024-62260-3
[24] Akraam, M., Rashid, T., & Zafar, S. (2023). A chaos-based image encryption scheme is proposed using multiple chaotic maps. Mathematical Problems in Engineering, 2023(1). https://doi.org/10.1155/2023/2003724
[25] Niu, Y., Zhou, Z., & Zhang, X. (2020). An image encryption approach based on chaotic maps and genetic operations. Multimedia Tools and Applications, 79(35–36), 25613–25633. https://doi.org/10.1007/s11042-020-09237-2
[26] Patro, K. A. K., Kumar, M. P., & Acharya, B. (2022). An efficient dual-stage pixel-diffusion based multimedia-image encryption using one-type 1D chaotic maps. Sādhanā, 47(3). https://doi.org/10.1007/s12046-022-01934-y
[27] Benlashram, A., Al-Ghamdi, M., AlTalhi, R., & Laabidi, P. K. (2020). A novel approach of image encryption using pixel shuffling and 3D chaotic map. Journal of Physics: Conference Series, 1447(1), 012009. https://doi.org/10.1088/1742-6596/1447/1/012009.