An Analytical Comparison of Image Encryption Techniques Utilizing Hyperchaotic Maps

Sourudra Nag, Akhul Murali, Aswathy.M, Sandra Sajeev, Shahana.T.K

[1]*School of Digital Sciences, Digital University Kerala, Thiruvananthapuram, PIN 695317, Kerala, India*

1. Abstact

In this paper, the authors explore two-dimensional and three-dimensional hyperchaotic maps to improve image encryption for secure and better image protection. Cryptographic techniques such as DES, AES, and Blowfish currently possess weaknesses, and as a result, chaotic systems being dynamic are the best for application.We compare predicted performance of 2D chaotic maps comparing efficiency with simplicity while 3D chaotic maps are compared about their enhanced security because of the higher degree of complexity. Encryption is another essential step which involve procedures such as making state signals that are chaotic to perform XOR on pixel values and thus make the picture less identifiable.Values of PSNR and SSIM have been examined in the experiments and it has been made a conclusion that 3D chaotic systems ensure better security as compared to 2D systems. 3D structure provides higher level of protection against attacks for data that is most vulnerable and require reliable protection, while more efficient encryption and decryption is provided by previously described 2D system.Therefore, this research coordinates on choosing the chaotic system for achieving particular security necessities and for the given computing capacity which will enhance the construction of sound and elastic image encryption methods.

2. Introduction

Our research compares various chaotic system methods[25] for image encryption[8]. To safeguard the confidentiality and integrity of a digital picture, image encryption converts the pixel values into an incomprehensible or unreadable format. Chaotic systems play a variety of roles in picture encryption, providing several advantages that improve the security, intricacy, and resilience of the encryption procedure [6]: In this study, we want to analyze and compare the effectiveness of using 2D and 3D chaotic systems for picture encryption[10].

In today's digital world, image encryption is essential for protecting sensitive visual data. Safeguarding photographs against unwanted access or alteration is becoming increasingly crucial as technology develops and our dependence on digital communication and storage grows. To make a picture unreadable without the matching decryption key[15], image encryption techniques employ intricate algorithms on the pixel values of the image. Usually, these methods use cryptography concepts[31] and mathematical procedures to efficiently jumble the picture data.Before chaotic systems, popular picture encryption algorithms included conventional techniques such as block ciphers like DES, AES, or Blowfish. These cryptosystems separated the picture into blocks of a set size and then jumbled the pixel values using different mathematical operations. The primary drawback of

these techniques was that block ciphers were insensitive to even minute modifications in the data or the key; this made block encryption vulnerable to a wide range of attacks. Stream ciphers were employed in addition to block ciphers to encrypt images. Using XOR operations, the keystream produced by the ciphers RC4 or ChaCha20 pseudorandomly mangled an image or the elementary values of bytes. Common techniques included the use of substitution-permutation networks, such as IDEA and Serpent, to alter image data by applying a combination of linear permutation operation and nonlinear S-boxes. The processes produced algorithmic computational complexity even though they aimed to produce confusion and diffusion characteristics resistant to analysis. Systems of visual cryptography, like the ones developed by Naor and Shamir, printed translucent sheets with divided images into shares. Together, they can create the original image without a computer, but the methods usually show limitations in sharing generation and image quality.

Chaotic systems have become a potent tool for picture encryption in recent years, providing several benefits over conventional techniques. For photo encryption, chaotic systems offer an extremely high level of security. It is almost impossible for hackers to decode the encryption process since chaotic systems are naturally unpredictable and susceptible to beginning conditions. This provides strong protection against brute-force attacks and illegal access. Techniques for encrypting chaotic images are extremely sensitive to any minor change to the input image or the encryption keys. Because even a single pixel alteration in the input image or a little modification in the key could result in an altogether different encrypted output, it becomes highly challenging for adversaries to obtain any valuable information from the data that was encrypted.

Quick image encryption and decryption are possible with the effective implementation of chaotic systems in software as well as hardware. They are therefore perfect for applications requiring quick data processing, such as Internet banking, secured video transfer, and real-time monitoring. Because chaotic image encryption techniques[7] are easily adaptable to work with different picture forms, resolutions, and color schemes, they are quite versatile and helpful for a wide range of imaging applications. Their flexibility allows for their smooth integration into a wide range of applications and systems, which further increases their usefulness and usage.

Symmetric-key encryption[3], in which the encryption and decryption processes share a single key, is a popular method for picture encryption. Another technique is asymmetric encryption, which uses a pair of keys—public and private—for encryption as well as decryption, respectively. Both strategies are appropriate for various use cases and provide varying degrees of security. People and organizations can reduce the possibility of important visual data being stolen, tampered with, or unauthorized access by encrypting their photos. This is especially important for sectors that value privacy and secrecy the most, including healthcare, banking, and government. But one must always keep in mind that encryption is but a single component of an all-encompassing security plan. To guarantee the general security of digital assets, additional precautions like access control, authentication, as well as safe communication protocols are required in addition to encryption. Furthermore, given how quickly cybersecurity is developing, it is essential to keep up with new threats and update encryption methods[1] regularly. The need to secure sensitive visual data in the digital age has led to the development of complex picture encryption methods. This paper explores two state-of-the-art techniques: the 2D chaos map and the 3D chaotic map. These methods, which make use of the complex dynamics of unpredictable systems, guarantee the integrity and privacy of digital pictures in an ever more precarious digital environment. The intricacy of three-dimensional chaotic systems[27][19], which are known for being sensitive to beginning circumstances and parameters, is harnessed by the 3-D chaotic map approach. This approach ensures an extremely high degree of security by producing distinct encryption keys for every image by creating a 3D chaotic

map[4][20]. This map may be used to jumble up pixel values such that the original image is almost indistinguishable preventing unwanted access attempts. The 3D chaotic system's starting circumstances and settings are used to produce unique encryption keys. After applying the produced key to the original picture, the encrypted image becomes unidentifiable due to the very complicated and random disruption of pixel values. The original pixel numbers are recovered using an identical 3D chaotic map and beginning circumstances in reverse, revealing the unencrypted image. By making use of the characteristics of two-dimensional chaotic systems, the 2D chaotic map approach[9], albeit simpler than its 3D equivalent, nevertheless provides strong encryption. It creates encryption keys to jumble pixel values, much like the 3D approach, providing security by unpredictability. The 2D chaotic system's characteristics and starting circumstances are used to create encryption keys. When the created key is put in place to the original picture, it obscures the content of the image by causing complicated and unexpected pixel value disruptions. The unencrypted image may be seen by repeating the procedure with a similar 2D chaotic map and starting circumstances to recover the original pixel values. Strong encryption solutions with distinct advantages and uses are provided by both methods. Although it may require more processing power, the 3D chaos map approach offers increased security. On the other hand, albeit a little less sophisticated, the 2D chaos map method provides effective encryption that may be used for a variety of purposes. While the 2D method is more straightforward but still reliable, the 3D method is more intricate and provides a greater level of protection. Because the 2D method uses less processing power, it is perfect for settings with limited resources. Both methods enable beginning circumstances and parameters to be changed to suit particular requirements. We are encrypting images in our project utilizing two-dimensional as well as three-dimensional chaotic systems. Our goal is to identify which of these two techniques provides the best safe image encryption. Our code shows how we can use two-dimensional and three-dimensional chaotic maps for photo encryption by offering a method that depends on chaotic behavior to generate surprising encryption patterns. Our technique encrypts grayscale or black-and-white images using these maps. It generates arbitrary patterns, encrypts each pixel of the image, and then saves the encrypted copy. Since the method is sensitive to these factors, it is difficult to analyze the encryption process without understanding its initial circumstances and settings. This approach mainly employs confusion instead of diffusion for picture encryption. This code uses the 'exclusive OR' (XOR) [13] operator to change the pixel values to hide the original image.To sum up, both the 2D and 3D chaotic map approaches offer novel approaches to picture encryption, each meeting distinct needs. By being aware of the trade-offs involved, security experts may make well-informed judgments that guarantee the creation of efficient encryption techniques in a constantly changing digital environment. A crucial factor to take into account when choosing between 2D and 3D chaotic maps for picture encryption is striking a balance between computing efficiency and security. Despite its simplicity, the 2D chaotic map has advantages in situations requiring speedier encryption and decryption or where computational resources are few. Because of its effectiveness, it may be used in real-time scenarios where speed is essential, including live video streaming or rapid data transfers. In contrast, a higher level of security is provided by the intrinsic complexity of the 3D chaotic map, which is essential for situations requiring extremely sensitive data, such as private financial information, government communications, and medical records. Because 3D maps are more dimensional, it is harder for outside parties to guess or decipher the encryption keys, adding an extra degree of protection to the system. As a result, the 3D chaotic technique is more resistant to advanced cyberattacks like differential or brute force cryptanalysis[34].

Furthermore, the flexibility of both 2D and 3D chaotic maps makes it possible to modify the encryption settings to satisfy certain security requirements. To guarantee that every encryption

instance is unique, for example, changing the chaotic system's beginning circumstances and settings might provide a wide variety of unique keys. This adaptability is crucial in dynamic security contexts where threats are ever-evolving and encryption systems must be updated regularly. Furthermore, the resilience and unpredictability of the encryption process are increased by the sensitivity of chaotic maps to beginning circumstances, which guarantees that even little changes in the input result in noticeably different encrypted outputs. The sophistication of cyber threats is growing along with the expansion and evolution of the digital realm. Thus, it's critical to keep your encryption technique current and strong. Chaotic map integration[35] improves security and shows that creative cryptographic methods are possible to keep up with the quick speed at which digital technology is developing. Our ability to combine the advantages of 2D and 3D chaotic systems allows us to create robust and adaptable encryption techniques that safeguard sensitive visual data in a wide range of applications and sectors.

The report is arranged as follows: In Section 2, we provided a comprehensive introduction to image encryption, including its uses, methods, and tenets. In Sections 3,4 and 5, we looked at the importance of using chaotic systems for picture encryption. We also explored two types of chaotic systems: two- and three-dimensional. In Section 5, we also covered the benefits of chaotic systems in photo encryption [36], such as their high security, resilience, and complexity. We have also discussed the advantages and disadvantages of using 2D and 3D chaotic systems for photo encryption[11]. The findings of our research are presented in Section 6, where we have emphasized the key findings and insights from the data. The findings of our research are presented in Section 6, where we have emphasized the key findings and insights from the data. We have investigated the behavior of chaotic systems in both color and grayscale image formats. We have given a comprehensive overview of our study's conclusions and ramifications in Section 7. We have also discussed potential future directions for this sort of research, such as employing hybrid encryption techniques and utilizing machine learning algorithms to increase the security of photo encryption.

article graphicx

3. Chaotic Systems and Image Encryption

Encryption [30]benefits greatly from chaotic systems with complex non-linear dynamics and significant sensitivity to beginning circumstances. Despite predictable principles, they provide seemingly random outputs, which is important for picture encryption. Existing in both 2D (Logistic, Henon maps)[33][28] and 3D (Lorenz, Rossler systems) forms[2][16], the 2D forms are more straightforward while the 3D forms provide more security. For encryption, their sensitivity guarantees that even little alterations result in radically different outcomes. Ergodicity [5]provides a comprehensive investigation of phase space, which is necessary for uniform data distribution. They are ideal for cryptography applications because of their pseudo-randomness, which allows for predictable yet supposedly random sequences. These characteristics make chaotic systems effective instruments for encrypting sensitive data in the current era.

A bifurcation is a period-doubling that happens when the control parameter is altered. It is the transition from an N-point attractor to a 2N-point attractor. An illustration of the series of period-doublings that are created as r grows is called a bifurcation diagram. It can learn more about the behavior of intricate dynamical systems and how adjustments to their parameters affect them.

3.1. 2D Chaotic System

2D chaotic systems, which make use of the complexity and unpredictable nature of chaotic dynamics, are powerful instruments for picture encryption. For increased security, they use maps or equations to create chaotic sequences that jumble picture pixels. Their primary benefit is that they are sensitive to the system's characteristics and starting circumstances. Slight modifications result in remarkably distinct paths, making encrypted pictures unrecognizable from their originals. 2D chaotic encryption is resistant to assaults because it combines natural randomness. Maps such as Logistic, Henon, and Sine are often used to generate pseudorandom sequences that permute and diffuse pixel values, so preventing unwanted access to visual information.The equation of a 2nd order chaotic system is given below.

$$X_n = k\left(\left(Q^2 - 1\right)X\right)$$
$$Q_n = Q + X$$

X and Q are the state variables of the system at a given iteration.The interplay between the linear and non-linear components in these equations can generate complex, unpredictable behavior over time, characteristic of chaotic systems. The non-linear term Q^2 in the first equation is essential for chaos because it introduces sensitivity to initial conditions and complex interactions between the variables X and Q.

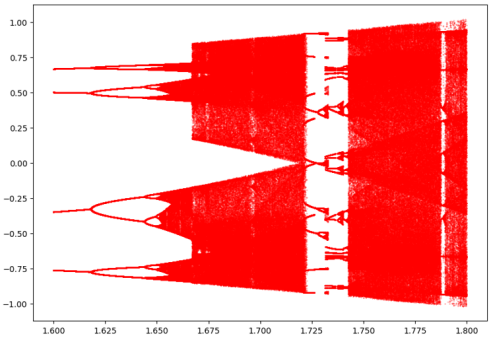

Figure 1: Bifurcation plot of 2D system

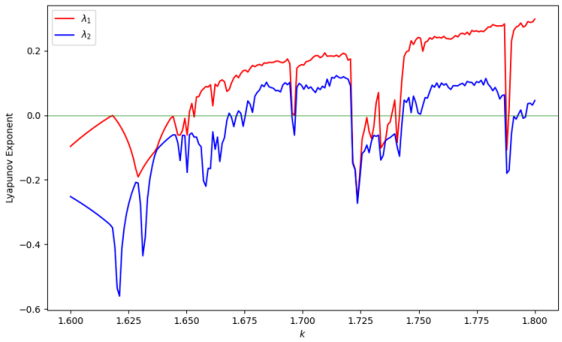

Figure 2: Bifurcation plot of 2D system

3.2. 3D Chaotic System

Compared to their 2D counterparts, 3D chaotic systems provide more complexity and security in image encryption[21]. By utilizing three-dimensional state variables like as acceleration, velocity, and location, they produce wildly unexpected patterns that make decryption difficult. By giving encryption keys another dimension, they make them more unpredictable and confusing, which deters hackers. They withstand brute-force attacks by expanding the key space through complex interactions. The "butterfly effect,"[12] which drives their complicated, irregular activity, strengthens resistance against differential and known-plaintext assaults. They also do a great job at hiding private information, giving encrypted photos a strong defense against a variety of attackers.Below is the equation for a third-order chaotic system.

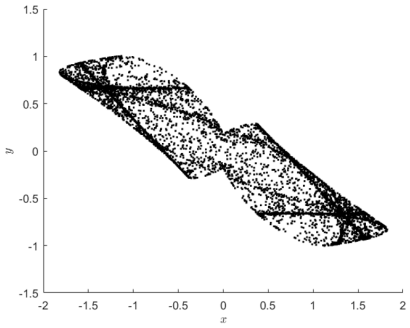

Figure 3: Phase plot of 2D chaotic map

$$X_n = a_1 x + a_2 y + a_3 y^2$$
$$Y_n = b_1 + b_2 z$$
$$Z_n = cx$$

These equations represent a simple yet potentially chaotic system where x, y, and z evolve over time based on their previous values and the specified coefficients. The non-linear nature and interdependencies of the variables are key features that can lead to chaotic dynamics.

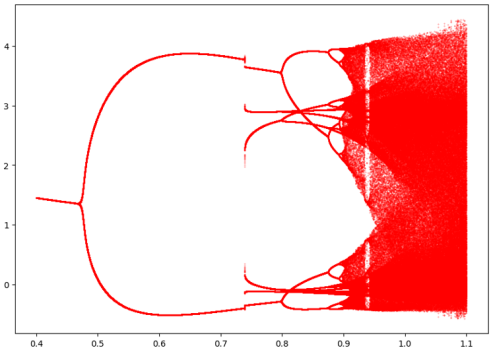

Figure 4: Bifurcation plot of 2D system

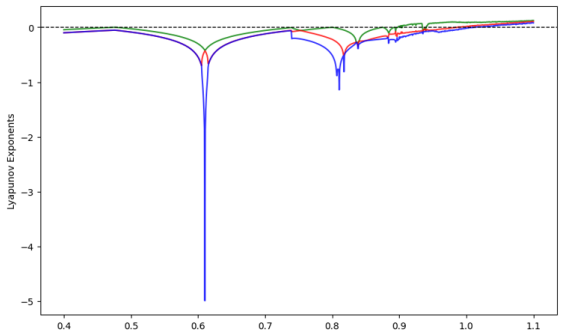

Figure 5: Bifurcation plot of 3D system

4. Method

This paper proposes a new image encryption algorithm based on chaotic systems. A byte signal of chaotic systems is used with the XOR operation for the bytes of the image to be encrypted in the proposed algorithm [6]. It elucidates the strength in encryption, which depends on itself and the initial conditions of the used chaotic systems. This would guarantee that only a person having full knowledge of both the parameters and initial conditions of the chaotic system will be able to decrypt the original image.

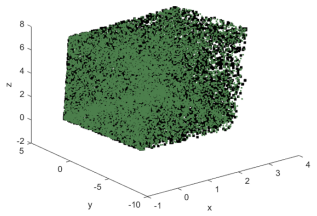

Figure 6: Phase plot of 3D chaotic map

Generation[17] First, generate chaotic signals from the X state variable of the 3D and 2D chaotic system. The chaotic data is normalized, further converted into a binary format, and used for the XOR operations with the image data. This process makes the encryption quite complex and secure. The chaotic system used is explained as follows: Chaotic System: In this system, a 3D and 2D chaotic map has been utilized with the X state variable as the key source for the chaotic signals. Normalization: The normalization is done into a 14-bit format for compatibility with the 8-bit image data.

Image Selection: The user selects an image that is to be encrypted. Read the Selected Image: Reads the selected image into MATLAB and returns the dimensions. Byte-wise encryption: Each byte of the transferred image will be encrypted by doing a byte-wise 'XOR' with bytes from the chaotic signal. A user selects an image to be encrypted. Image Read: Read the selected image into MATLAB, extract its dimensions. Byte-wise Encryption: Each byte of the image is encrypted by performing an XOR operation with corresponding bytes of the chaotic signal.

[22][23]: This proposed technique is very secure in its three-way mechanism. Chaotic Signal Dependency: The encryption relies on the chaotic system's signals, which are highly sensitive to initial conditions. The signal depends on a chaotic system that demonstrates a high degree of sensitivity to initial conditions, where the encryption will heavily depend on them. XOR Operation: This is a reversible XOR operation, thus guaranteeing very high security of the image and avoiding different procedures to be used for encryption and decryption. Pixel complexity: The byte values in each pixel's RGB channels for an RGB image, or the grayscale values, are encrypted to make the image too complex and secure to be decrypted.

Experiment results and image quality assessments, like PSNR and SSIM [18], prove the effectiveness of the proposed method. These metrics indicate that the encryption method is competent in resisting several attacks efficiently and changing the pixel information so that the original image cannot be recognized.

5. Mathematical Explanation

5.1. Chaotic System and Signal Normalization

This chaotic map creates a series of chaotic signals denoted by the state variable X. In this study, a 3D and 2D chaotic map is used, and then the state variable X is normalized. This is done to ensure compatibility with 8-bit image data. The normalization process includes scaling and rounding off of the chaotic values:

$$X_{\text{normalized}} = \left|\text{round}\left(2^{k_{\text{acBit}}-1} \cdot X\right) + 2^{k_{\text{acBit}}-1}\right|$$

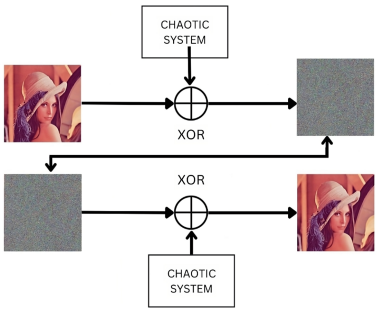

Figure 7: Method for encryption

here kacBit=14. After this the data will be suitable for binary conversion and XOR operation.

5.2. Binary Conversion

The The normalized chaotic data is converted into a binary format data.

$$X_{\text{binary}} = \text{dec2bin}(X_{\text{normalized}}, 15)$$

Now, the data is suitable for XOR operation.

5.3. Image Encryption Process

5.3.1. Reading the Image:

The image is read then it is converted into an 8-bit binary format. The Original image with pixel values represented as

Iij , where I is Original image with pixel values and i is row and j is column.

5.3.2. XOR:

XOR operation is done between each byte of image and corresponding chaotic data got from 2D or 3D equation map.

X_k = Corresponding Chaotic Signal, k denotes the index of Chaotic Signal

Here for every byte b the I is the pixel value:

$$I_{ij}^{(b)} = \text{dec2bin}(I_{ij}, 8)$$

XOR operation is executed for every bit of a byte, where $\oplus$ denotes the XOR operation :

$$I_{ij}^{(b,k)} = I_{ij}^{(b)} \oplus X_k$$

Then the encrypted byte is added together, and it will form a encrypted image:

$$I_{\text{enc}} = \text{bin2dec}(I_{ij}^{(b,k)})$$

6. Result

All results of this algorithm were proved by several methods, such as histogram analysis, correlation of adjacent pixels, information entropy, UIQ, and NCC. PSNR—Peak Signal-to-Noise Ratio, SNR—Signal-to-Noise Ratio, SSIM—Structural Similarity Index Measure; for checking the decryption accuracy, UIQ, and NCC.

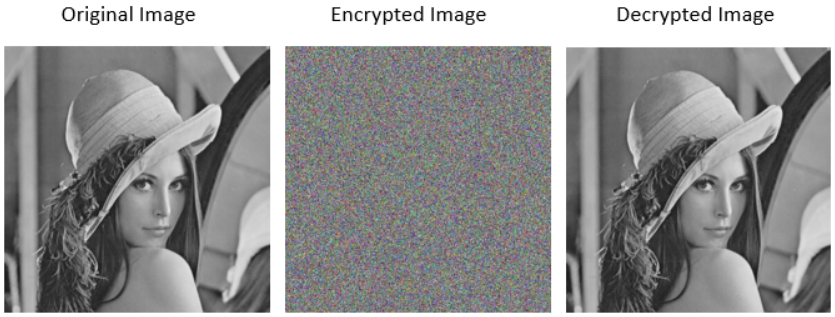

Figure 8: Comparison between original, encrypted and decrypted grayscale image using 2D map

Figure 9: Comparison between original, encrypted and decrypted rgb image using 2D map

7. Image Encryption using 2 Dimensional and 3 Dimensional Chaotic Map

Effective comparison of the image encryption algorithm based on the proposed chaotic system with existing systems has to be based on major metrics of consideration: quality of encryption expressed by PSNR and SSIM; security features including sensitivity to the key, resistance to attacks of differential and statistical types, entropy; computational efficiency indicated in time of encryption and decryption, memory usage; and complexity, specifically algorithmic and implementation-related. This would be drawn on available image encryption methods like AES, DES, RSA [26],

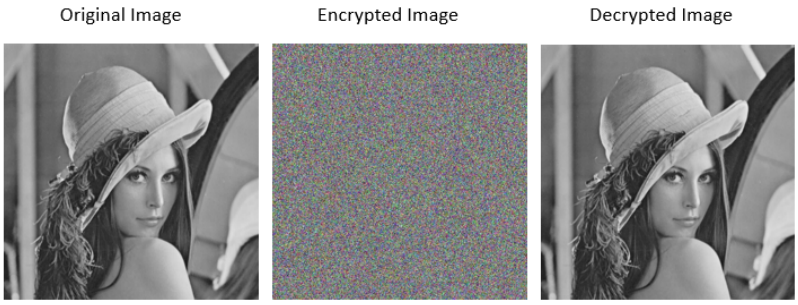

Figure 10: Comparison between original, encrypted and decrypted grayscale image using 3D map

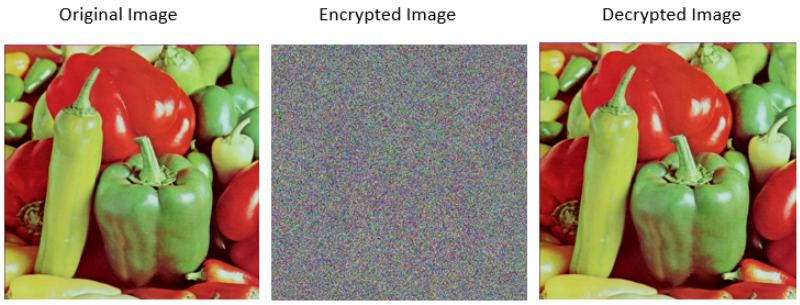

Figure 11: Comparison between original, encrypted and decrypted rgb image using 3D map

Metric	2D map	3D map
BER	0.9947	0.9945
NCC	-0.0296	0.0039
Information Entropy	7.99	7.99
UIQ	-0.0295	0.0039
Correlation of adjacent pixels (RGB)	1.0	1.0

Figure 12: Evaluation metrics of Encryption

Metric	2D map	3D map
BER	0.0005	0.0005
NCC	1.0	1.0
PSNR (dB)	76.02	76.02
SNR (dB)	48.16	48.16
SSIM	1.0	1.0
UIQ	1.0	-

Figure 13: Evaluation metrics of Decryption

image scrambling techniques such as Arnold Transform [24], and other chaotic systems, which include the Logistic Map [29] or Lorenz System [14]. The quality of encryption, security, efficiency, and complexity fundamentally differ in each methodology: AES is highly secure but has high moderating complexity and is slower for larger images; DES is much less secure and simpler; RSA is highly secure but quite impractical for large data; image scrambling is a fast approach but less secure without iteration secrecy; and other chaotic systems, as has been noted, hold similar advantages and challenges to your proposed method.

The methods of the proposed system ensures the quality of the encrypted system, manifested through high PSNR and SSIM values, high key sensitivity, resistance against several kinds of attacks, and very efficient utilization of the XOR operation, which makes it suitable for real-time applications. The scheme offers a superior trade-off between security and computational efficiency compared to AES, which is itself secure but highly complex, along with other chaotic systems; hence, it is more advantageous in image encryption applications. This balance of quality, security, and efficiency identifies the methods of the proposed system as a very enabling complement or even alternative to the many existing methods, especially in applications where high security is required as well as high speeds.

8. Future Works

1.Enhancement in Chaotic Systems:

• Investigation of Different Chaotic Maps: Analyse different types of chaotic systems over 3D and 2D maps, like higher-dimensional chaotic systems or chaotic oscillators. The levels of security and computational efficiency may vary for different systems.

• Optimization of Parameter: By maintaining computational feasibility adjust parameters of existing chaotic systems to improve encryption power.

2.Improvements in algorithm:

• Management of adaptive Key: Create ways for the management of adaptive key that can adjust parameters of encryption dynamically based on the features of the image or data being encrypted.

• Multilevel Encryption: Execute multilevel encryption techniques where different chaotic algorithms or signals are used serially to further improve security.

3.Optimization of Performance :

• Parallelization: Check methods to parallelize encryption and decryption processes to increase computational efficiency, particularly for large-scale image data.

• Hardware Acceleration: To attain encryption and decryption speeds faster execute encryption algorithms using hardware acceleration techniques (e.g., GPUs or specialized processors).

4.Analysis of security:

• Blocking of Advanced Attacks: Attacks like differential cryptanalysis, statistical attacks, or machine learning-based attacks are resisted by conducting in-depth examinations.

• Side-Channel Attacks:Side-channel attacks (e.g., timing analysis, power analysis) that could deal with the encryption security are examined and reduce its risks.

5.Applications and Integrations:

• Real-Time Applications: Encryption algorithm for real-time applications like secure communication channels or video streaming are adapted.

• Cloud-Cambatible Solutions: Develop cloud-based encryption solutions that make sure transmission and storage security of encrypted images on cloud platforms.

9. Conclusion

In this study, we investigated the use of 2D and 3D chaotic maps for picture encryption using chaotic systems. These maps are especially well-suited for encryption because of their intrinsic complexity and sensitivity to beginning circumstances, which result in hyper-chaotic behavior. The main steps in the process include creating chaotic values, normalizing, translating to binary, and bitwise XORing[32] the chaotic and picture data. This method's resilience was confirmed by several indicators, proving how well it protects digital photos from unwanted access. With at least one positive Lyapunov exponent confirming their hyper-chaotic characteristics, the chaotic maps employed in this investigation were carefully chosen. From 2D and 3D systems, we produced 256 chaotic values. We then processed them to remove negative values, rounded them to the closest integer, and raised them to the power of 2 to normalize them. After that, these numbers were transformed into a 14-bit binary format, which struck a compromise between accuracy and computing speed. The picture bytes and the chaotic data were subjected to a byte-by-byte XOR operation throughout the encryption process, which was made more complicated and secure by nonlinear transformations.

Our study demonstrates that image encryption using 2D and 3D chaotic maps provides a robust and effective means of securing digital images. The high entropy, low pixel correlation, and excellent quality of decrypted images underscore the strength of this encryption approach. In conclusion, the 2D system's behavior may be less complex than that of higher-dimensional systems because of the phase space's reduced dimensionality. This could have an impact on the system's capacity to produce encryption keys that are complicated enough for reliable picture encryption. Therefore, a 3D chaotic system is much better and more efficient in generating unpredictable encryption keys due to its complexity, which in turn results in more robust image encryption.

References

[1] Ayman Alfalou and C Brosseau. Optical image compression and encryption methods. *Advances in Optics and Photonics*, 1(3):589–636, 2009.

[2] Nashwan Alsalam Ali, Abdul Monem S Rahma, and Shaimaa H Shaker. Multi-level encryption for 3d mesh model based on 3d lorenz chaotic map and random number generator. *International Journal of Electrical & Computer Engineering (2088-8708)*, 12(6), 2022.

[3] Mohammad Ubaidullah Bokhari and Qahtan Makki Shallal. A review on symmetric key encryption techniques in cryptography. *International journal of computer applications*, 147(10), 2016.

[4] Belqassim Bouteghrine, Camel Tanougast, and Said Sadoudi. Novel image encryption algorithm based on new 3-d chaos map. *Multimedia Tools and Applications*, 80:25583–25605, 2021.

[5] Giuseppe Da Prato and Jerzy Zabczyk. *Ergodicity for infinite dimensional systems*, volume 229. Cambridge university press, 1996.

[6] Ali Durdu. Image transfer with secure communications application using a new reversible chaotic image encryption. *Multimedia Tools and Applications*, 83(2):3397–3424, 2024.

[7] Jiri Fridrich. Image encryption based on chaotic maps. In *1997 IEEE international conference on systems, man, and cybernetics. Computational cybernetics and simulation*, volume 2, pages 1105–1110. IEEE, 1997.

[8] Haojiang Gao, Yisheng Zhang, Shuyun Liang, and Dequn Li. A new chaotic algorithm for image encryption. *Chaos, Solitons & Fractals*, 29(2):393–399, 2006.

[9] Xiaohong Gao. Image encryption algorithm based on 2d hyperchaotic map. *Optics & Laser Technology*, 142:107252, 2021.

[10] Xinyu Gao, Miao Miao, and Xiaoyang Chen. Multi-image encryption algorithm for 2d and 3d images based on chaotic system. *Frontiers in Physics*, 10:901800, 2022.

[11] Gopal Ghosh, Sahil Verma, NZ Jhanjhi, MN Talib, et al. Secure surveillance system using chaotic image encryption technique. In *IOP conference series: materials science and engineering*, volume 993, page 012062. IOP Publishing, 2020.

[12] Étienne Ghys. The butterfly effect. In *The Proceedings of the 12th International Congress on Mathematical Education: Intellectual and attitudinal challenges*, pages 19–39. Springer International Publishing, 2015.

[13] Oded Goldreich. Three xor-lemmas—an exposition. *Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation: In Collaboration with Lidor Avigad, Mihir Bellare, Zvika Brakerski, Shafi Goldwasser, Shai Halevi, Tali Kaufman, Leonid Levin, Noam Nisan, Dana Ron, Madhu Sudan, Luca Trevisan, Salil Vadhan, Avi Wigderson, David Zuckerman*, pages 248–272, 2011.

[14] Ilia Grigorenko and Elena Grigorenko. Chaotic dynamics of the fractional lorenz system. *Physical review letters*, 91(3):034101, 2003.

[15] Fuchun Guo, Yi Mu, and Zhide Chen. Identity-based encryption: how to decrypt multiple ciphertexts using a single decryption key. In *International Conference on Pairing-Based Cryptography*, pages 392–406. Springer, 2007.

[16] Yasir Ahmed Hamza and Marwan Dahar Omer. An efficient method of image encryption using rossler chaotic system. *Academic Journal of Nawroz University*, 10(2):11–22, 2021.

[17] Simon Haykin and Xiao Bo Li. Detection of signals in chaos. *Proceedings of the IEEE*, 83(1):95–122, 1995.

[18] Alain Hore and Djemel Ziou. Image quality metrics: Psnr vs. ssim. In *2010 20th international conference on pattern recognition*, pages 2366–2369. IEEE, 2010.

[19] Kunal Kumar Kabi, Chittaranjan Pradhan, Bidyut Jyoti Saha, and Ajay Kumar Bisoi. Comparative study of image encryption using 2d chaotic map. In *2014 International Conference on Information Systems and Computer Networks (ISCON)*, pages 105–108. IEEE, 2014.

[20] A Kanso and M Ghebleh. A novel image encryption algorithm based on a 3d chaotic map. *Communications in Nonlinear Science and Numerical Simulation*, 17(7):2943–2959, 2012.

[21] Pawan N Khade and Manish Narnaware. 3d chaotic functions for image encryption. *International journal of computer science issues (IJCSI)*, 9(3):323, 2012.

[22] Chenghai Li, Fangzheng Zhao, Chen Liu, Lei Lei, and Jie Zhang. A hyperchaotic color image encryption algorithm and security analysis. *Security and Communication Networks*, 2019(1):8132547, 2019.

[23] Shiguo Lian, Jinsheng Sun, and Zhiquan Wang. Security analysis of a chaos-based image encryption algorithm. *Physica A: Statistical Mechanics and its Applications*, 351(2-4):645–661, 2005.

[24] Zhengjun Liu, Lie Xu, Ting Liu, Hang Chen, Pengfei Li, Chuang Lin, and Shutian Liu. Color image encryption by using arnold transform and color-blend operation in discrete cosine transform domains. *Optics Communications*, 284(1):123–128, 2011.

[25] Nikolai Aleksandrovich Magnitskii and Sergey Vasilevich Sidorov. *New methods for chaotic dynamics*, volume 58. World Scientific, 2006.

[26] Prerna Mahajan and Abhishek Sachdeva. A study of encryption algorithms aes, des and rsa for security. *Global journal of computer science and technology*, 13(15):15–22, 2013.

[27] Dania Saleem Malik and Tariq Shah. Color multiple image encryption scheme based on 3d-chaotic maps. *Mathematics and Computers in Simulation*, 178:646–666, 2020.

[28] Kapil Mishra and Ravi Saharan. A fast image encryption technique using henon chaotic map. In *Progress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2017, Volume 1*, pages 329–339. Springer, 2019.

[29] Narendra K Pareek, Vinod Patidar, and Krishan K Sud. Image encryption using chaotic logistic map. *Image and vision computing*, 24(9):926–934, 2006.

[30] Gerald J. Popek and Charles S. Kline. Encryption and secure computer networks. *ACM Comput. Surv.*, 11(4):331–356, dec 1979.

[31] Shivani Sharma and Yash Gupta. Study on cryptography and techniques. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 2(1):249–252, 2017.

[32] Jilei Sun. A chaotic image encryption algorithm combining 2d chaotic system and random xor diffusion. *Physica Scripta*, 96(10):105208, 2021.

[33] Yue Wu, Gelan Yang, Huixia Jin, and Joseph P Noonan. Image encryption using the two-dimensional logistic chaotic map. *Journal of Electronic Imaging*, 21(1):013014–013014, 2012.

[34] Ibrahim Yasser, Abeer T Khalil, Mohamed A Mohamed, Ahmed S Samra, and Fahmi Khalifa. A robust chaos-based technique for medical image encryption. *IEEE Access*, 10:244–257, 2021.

[35] Bedir Yousif, Fahmi Khalifa, Ahmed Makram, and Ali Takieldeen. A novel image encryption/decryption scheme based on integrating multiple chaotic maps. *AIP Advances*, 10(7), 2020.

[36] Yicong Zhou, Long Bao, and CL Philip Chen. A new 1d chaotic system for image encryption. *Signal processing*, 97:172–182, 2014.