International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 13, No. 6, December, 2023, pp. 1117-1125
Journal homepage: http://iieta.org/journals/ijsse

Chaotic Map Based Raster Data Encryption for Geospatial Data

Prajakta Bhangale[1,2*], Shubhangi Vaikole[3]

[1] Department of Computer Engineering, DMCE, Navi Mumbai, Mumbai University, Maharashtra 400708, India
[2] Department of Electronics and Computer Science, Fr. Conceicao Rodrigues College of Engineering, Mumbai University, Mumbai 400050, India
[3] Department of Information Technology, Fr. Conceicao Rodrigues Institute of Technology, Navi Mumbai, Mumbai University, Mumbai 400703, India

Corresponding Author Email: prajakta.bhongale@fragnel.edu.in

https://doi.org/10.18280/ijsse.130615

Received: 4 October 2023
Revised: 28 November 2023
Accepted: 5 December 2023
Available online: 25 December 2023

Keywords:
Chirikov chaotic map, Chebyshev chaotic map, continuous raster scan, encryption, shuffling, security, Unified Average Changing Intensity, Number of Pixels Change Rate

ABSTRACT

Data confidentiality, security authentication are just some of the many uses for image encryption, making it one of the most effective methods for safeguarding geospatial data. However, even with advancements in an encryption algorithms still face challenges in terms of both security and speed. However, limitations in key space, complexity of algorithms, make it susceptible to assaults plague present in image encryption methods. Considering the restrictions of past strategies, we've formulated a brought together way to deal with raster data encryption by consolidating shuffled raster Output, Chirikov and Chebyshev chaotic map. At the point image is the constant raster is first shuffled by shuffling method to muddle the pixels of each block. The randomization characteristic in keys generated by Chirikov and Chebyshev Chaotic maps will be used to encode raster data. Encryption is performed rapidly utilizing the recommended approach. The re-enactment results exhibit the adequacy and reasonableness of the method for safeguarding raster geospatial data.

1. INTRODUCTION

In the current climate of information security, an escalating array of threats to sensitive data has catalyzed a surge in the demand for sophisticated encryption methodologies. Within this sphere, chaotic maps are gaining recognition for their potential to underpin cryptographic algorithms, prized for their intricate complexity, high sensitivity to initial conditions, and pseudo-random characteristics. The present technical paper scrutinizes the deployment of chaotic maps in encryption, endeavoring to exploit their dynamic properties to fortify the efficacy and robustness of data protection strategies. A meticulous examination of diverse encryption schemes based on chaotic maps is undertaken, elucidating their theoretical foundations, algorithmic details, and the consequential benefits in the defense against unauthorized data breaches and malevolent activities. The architecture of this paper commences with an exposition on the rudimentary principles of cryptography and chaotic maps, progressing to a review of the related literature, an elucidation of the methodology, and an evaluation of the significance of the study's findings through results and discussion.

The application of image processing is widespread across various computer systems [1, 2], and the domain of cryptography has been enriched by the assimilation of novel technologies and conceptual paradigms. These advancements pertain to domains such as information theory [3], quantum computing [4], neural networks [5], Very Large Scale Integration (VLSI) technology [6], and, notably, chaos theory [7]. The intersection of image encryption with chaos theory is particularly salient and forms the crux of the ensuing discourse.

The work of Wang et al. [8] is acknowledged for its contributions within the spatio-temporal domain, where the authors have pioneered strategies for Dynamic Chaotic Image Encryption. Figure 1 shows Basic encryption using chaos.

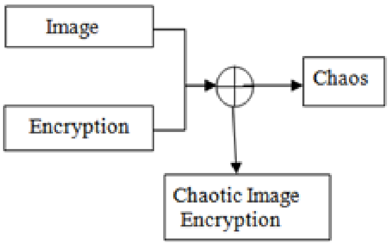


Figure 1. The meeting ground of image encryption using chaotic map

2. RELATED WORK CHAOTIC IMAGE ENCRYPTION

Research on tumultuous picture encryption is happening in three angles; turmoil, picture, and encryption. These perspectives are displayed in Figure 2. The cutting edge in every one of the referenced perspectives is explored underneath.

2.1 Current status of chaos consideration

Scientists zeroing in on the bedlam viewpoint have attempted different tumult spaces, sources, and aspects. These ideas are concentrated beneath alongside related research works. As found in Figure 2, the tumult angle is about disorder spaces, sources, and aspects.

2.1.1 Chaos domains

Spatial chaos, temporal chaos, and spatio-temporal chaos are the three primary categories of chaotic research. Every one of these fields is significant during the time spent scrambling a tumultuous picture. This section discusses these functions;

Turbulent Spaces: Both spatially tumultuous frameworks and guides are instances of capabilities whose state still up in the air by the information esteem. The use of a 2D spatial guide in a remarkable picture encryption strategy that shows great security in the wake of exposing it to key responsiveness tests, adjoining pixel relationship examination, key space examination, and testing against various assaults is only one illustration of their various applications in the field of picture encryption. The convenience of various tumultuous guides, including the Arnold feline guide, the dough puncher map, and the strategic guide, in the spatial space was explored in a paper distributed by Faragallah et al. [9].

Worldly Confusion: To learn the current situation with a fleeting framework, all you want is a period record and the condition of the framework at the earlier file. Wang and Chen [10] presented a picture encryption procedure that showed solid security characteristics like a wide key space, high key responsiveness, and measurable examination opposition by utilizing an arrangement of unadulterated worldly disarray known as a "super-tumultuous" map.

Jumble in Reality: Both the spatial space (the info) and the time file are significant to a spatiotemporal tumultuous framework. The Discrete Cosine Change (DCT) has been utilized in the proposed encryption methods of Ge et al. [11] and Luo et al. [12], which utilize spatiotemporal mayhem. The previous works by utilizing the Proliferating Code Block Anchoring (PCBC) mode not with standing the standard Code Block Tying (CBC) mode to scramble pictures, while the last option depends on the last alone. While inspected utilizing cryptographic examination instruments, each of the three calculations end up being very protected. Coupled Calculated Guide Cross section (LDCML) is a one of a kind spatiotemporal tumultuous model recommended in their examination. The suggested map was shown to have significant chaotic qualities via analysis, and it was shown through subsequent experimental study to be very successful when used to picture encryption.

2.1.2 Chaos sources

Mathematical or physical processes may generate chaos. Following, academics analyse the impact of mathematical literature. Typical mathematical chaos generators used for picture encryption are examined here.

A Chaotic System with a Fractional Order: Modern research has focused on systems like the Chen, Lorenz, and Liu fractional-order systems [13], albeit partial math has a set of experiences extending back over 300 years.

Hou [14] proposed another partial request bedlam framework that utilizations controlling changes to flip between its sub-structures and give areas of strength for a source to playing out the particular Or (XOR) method on the plaintext picture.

Wei [15] recommended an elective method that utilizes partial request frameworks, and it accomplishes ideal encryption includes and is impervious to famous attacks by utilizing a more regular third-request fragmentary framework, a special Josephus scrambling calculation, and round dispersion.

"Arnold's Guide of Felines": George and Gopakumar [16], Zhang et al. [17] have created encryption methods that utilize Arnold planning, a notable rendering tumultuous guide, to permute and de-relate adjoining pixels. The two calculations were demonstrated to be secure against savage power, entropy, CPT, and KPT assaults, and to have a wide keyspace with high key responsiveness.

Lattice of coupled maps: The production of random number streams may be facilitated by using a Coupled Map Lattice (CML), a kind of spatiotemporal chaos map. To build encryption streams that are reliant on both the starting values and intermediate cipher pictures, Wu [18] suggested a unique implementation of the CML that uses intermediate cipher images to adjust the CML parameters. This increases protection against many attacks by making plaintext use a prerequisite.

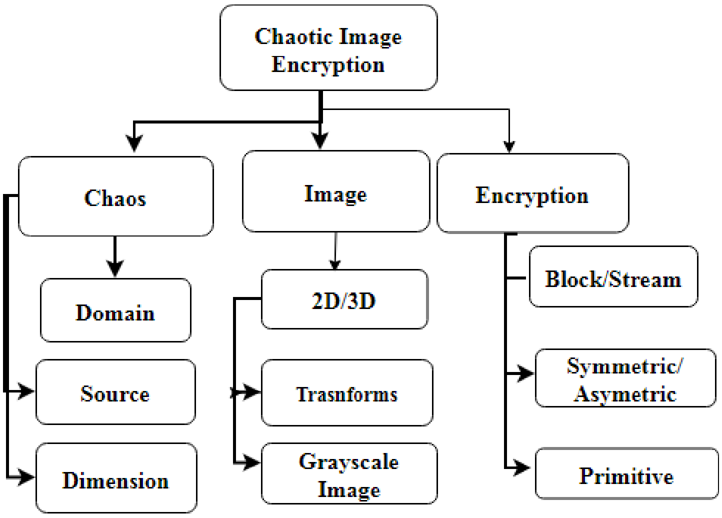


Figure 2. Studies on encrypting chaotic images

Lorenz diagram: When it comes to beginning circumstances, a differential equation is as sensitive as a Lorenz system. A picture encryption method described by Jiang and Fu [19] uses the chaotic nature of a 3D Lorenz system as inputs to generate a key, making use of its security.

Logistical diagram: When subjected to the impact of certain control variables, the relatively straightforward mathematical mapping function known as a logistic map displays chaotic behaviour. Sharma and Bhargava [20] proposed a strategy that involves a two-step intuitive calculated map as a wellspring of bedlam, with the following info relying upon the past two results. In a connected report, Lei et al. [21] improved the productivity of key age by consolidating a regular strategic guide with a hyper-tumult framework. Key creation utilizing the calculated guide was in like manner fruitful for Mu and Lui [22].

Tent layout: After Wu et al. [23] published a CTM-based picture encryption technique; Zhu and Sun [24] examined the transform's properties and offered enhancements to make it more resistant to plaintext assaults like CPT and KPT. When given a certain set of parameters, the Chaotic Tent Map (CTM) mapping function exhibits chaotic behaviour.

Strong cryptography was proved by the application of the Lotka-Volterra, Henon map, Logistic-sine system, Baker map, Tinkerbell map, Cubic map, Gingerbredman map, and Tangent map technique by a large group of researchers.

Different maps: There are several applications for picture encryption methods that combine different mapping functions. For instance, Bisht et al. [25] used a number of maps to accomplish goals such increased chaos in permutation, diffusion, and random number generation. Wang et al. [26] also presented a similarly conceived method, however theirs made use of many maps at various points in the encryption process. A unique keystream generation approach was developed by Fu et al. [27] that uses several chaotic maps to include the plaintext into the stream. The need of preventing CPT and KPT assaults inspired the algorithm, and an evaluation of the method demonstrated its efficacy in stopping such attacks. Multiple chaotic maps may be used to impose stronger algorithms, which have many practical applications. Choi et al. [28] suggested a method for encrypting colour medical pictures, which are special because of their size and sensitivity, by employing a set of maps. Statistical and experimental evaluation of the resultant process confirmed its safety for usage with medical pictures.

2.1.3 Chaos dimension

The number of functions (x(t), y(t), etc.) that make up a chaotic map is its "dimension." Multidimensional chaotic functions are often used in picture encryption methods. In chaotic image encryption, the chaotic functions utilised fall into the following broad classes.

One-dimensional: Wang and Lui [29] have done some interesting work with one-dimensional chaos by proposing the 1D Sine Chaotic System (1DSCS). When compared to its foundational standard sine map, this system's parameter interval is rather big.

Two-dimensional: Yang and Tong [30] presented another image encryption method in view of tumultuous elements in two aspects. This approach utilizes another block picture encryption strategy related to the 2D calculated turbulent framework. The algorithm's high key sensitivity, minimal pixel correlations, and strong randomization were all proven by experimental findings.

Dimensional in three space-time dimensions: Three-dimensional chaos is used in several picture encryption methods. Using 3D logistic and cat maps, Qian et al. [31] suggested one such approach. The innovative use of image reconstruction methods contributed to the algorithm's enhanced performance.

*Dimensional in four space-time dimension*s: Based on "shape synchronisation" and "driver-response" principles, Huang et al. [32] suggested a unique four-dimensional chaotic system. Experimental testing in the use of picture encryption revealed encouraging results, and the algorithm's complexity mathematical foundations make it incredibly tough to crack.

Dimensional in five ways: Consolidating the 2D calculated map with the 3D discrete Lorenz map, Zhu and Zhu [33] made another 5D tumultuous guide. When tested in a variety of standard encryption strength evaluations, experimental simulations of the system's application to picture encryption achieved excellent results.

Several dimensions: Mixing maps of different dimensions has also been investigated for use in picture encryption. Utilizing the 1D strategic guide with the 3D Lorenz framework, for example, Qui and Yan [34] recommended a picture encryption strategy. The thorough security of the calculation was affirmed by exploratory discoveries.

2.2 The present image technology state

The security of raster data can be enhanced through the utilization of watermarking techniques. Specifically, a method involves embedding watermarks into the low-frequency coefficients of wavelet transforms, employing Arnold's permutation for the embedding process [35]. The procedure includes applying 2-D Discrete Wavelet Transform (DWT) on each channel of the host raster image up to the third level. From these third-level components, LL3 and HH3 coefficients are selected for watermark embedding. The watermarked raster is obtained by applying the inverse DWT as the final step. This method yields efficient results compared to previous approaches when subjected to various geometric and non-geometric attacks on raster images containing geospatial data.

Another research effort focuses on securing Geographic Information System (GIS) data using the Visual Cryptography (VC) technique applied to raster images, generating two shares from the original image [36]. The primary emphasis is on the secure transmission of raster maps and a computation-free encryption scheme for raster maps. The encoding process occurs block-wise, generating shares on a block-by-block basis and imposing them with equally sized secret blocks. This approach eliminates pixel expansion, thereby enhancing the quality of visual perception. However, it's crucial to acknowledge that this method exclusively addresses grayscale images.

In a different study by Ren [37], a digital watermarking algorithm based on Discrete Cosine Transform (DCT) and DWT is proposed. However, it's worth noting that these algorithms are susceptible to compression and deletion attacks.

Colour picture encryption algorithms use a broad variety of methods, including matrix convolution [38]. Multiple colour picture encryptions [39] and an innovative colour image encryption and transmission mechanism based on auditory cues [40] have also been presented.

In chaotic image encryption, picture transformations play a vital role. We'll take a look at a few of them here.

Wavelet: The wavelet change is in many cases used to rearrange the cells of a 2D lattice, which may extraordinarily work on the viability of encryption [41]. An improved 3D feline guide [42], a 1D strategic guide [43], a 3D calculated map [44], the Arnold map [45, 46], and a strategic succession [46] are just a portion of the turbulent sources that have been joined with the wavelet change to meet the turmoil basis of phenomenal encryption. There have been a few recommended techniques that utilization varieties of the standard wavelet change, for example, the Number Wavelet Change (IWT) [47].

Crisscross Change: One of the most valuable properties of the crisscross change for picture encryption is its capacity to revamp the phones of a 2D grid so as to decrease the connection between's adjoining pixels definitely. Gao and Wang [47] recommended an image encryption method that utilizes a more elaborate execution of the change, which gives expanded security.

Cosine Transform: As an alternative to the more often used Discrete Cosine Transform (DCT), Zhang et al. [48] suggested the use of the Discrete Fraction Cosine Transform (DFrCT) in an image encryption technique.

Change to a Contourlet: The disadvantages of the wavelet change while working with veritable pictures were supposed to be watched out for by the improvement of the contourlet change, which offers a way to deal with de-correlating the cells of a 2D system. A picture encryption procedure utilizing the change was presented by Jiang et al. [49], and it has a couple of needed attack securities, for instance, against JPEG pressure.

LCT, or Linear Canonical Transform: In order to prevent brute-force assaults, Li and Dai [50] devised a picture encryption technique that makes use of LCT and is both fast to execute and has a large key space.

3. METHOD

Explaining from the discussion so far we reached a decision that blending numerous planning capabilities in encryption calculations can fill various needs. Utilization of chaotic maps is used to achieve randomization safeguard against attacks. Chebyshev and Chirikov Chaotic are in this way chosen for the proposed framework. Figure 3 shows the functioning methodology of the proposed methodology.

The fundamental standard of encryption depends on the capacity of a few unique frameworks to create grouping of numbers that are sporadic in nature. Messages might be scrambled using this string. The recipe for the image encryption utilizing a Chebyshev Chaotic Map is as given by Eq. (1).

$$X_{n+1}=\cos(d*\cos^{-1}(X_n)) \tag{1}$$

where, $X_n \in [-1, 1]$

X_n is the current value.

X_{n+1} is the next value.

n is the iteration index.

For two sanctioned unique factors (x, p), the Chirikov map is an unyielding region saving turbulent guide. Eqns. (2) and (3) gives a portrayal of this

$$Pn+1=Pn+K*\sin(Xn) \tag{2}$$

$$Xn+1=Xn+Pn+1 \tag{3}$$

P_n is the momentum at iteration n.

X_n is the position at iteration n.

K is a parameter that influences the strength of the nonlinearity and chaotic behaviour.

K is a non-metric quantity that modifies the level of disorder. Confusion may be unlocked with the correct k value. The image's dimensions are N by N.

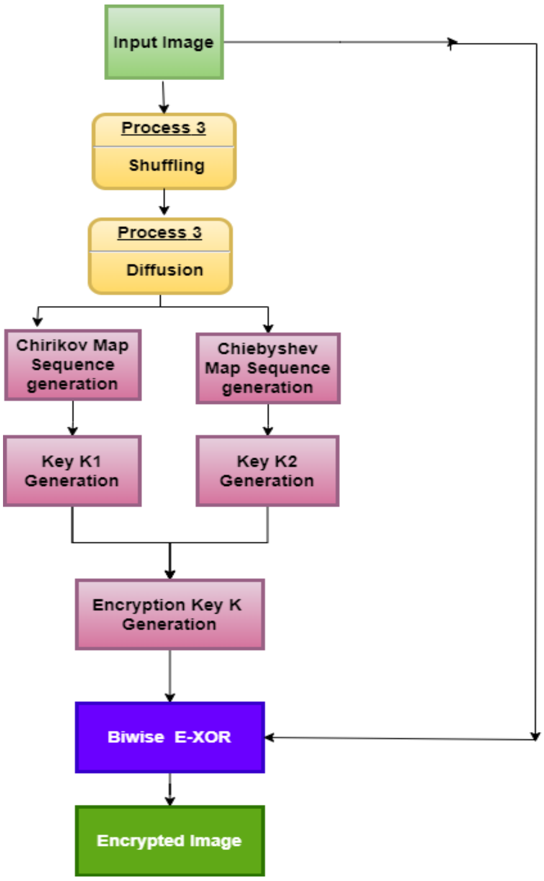


Figure 3. Chaotic map based encryption

The suggested approach has three key steps: a bitwise XOR activity, a persistent raster filter, and a non-covering block parcel. Utilizing the Chirikov map succession and the chebyshev map arrangement, the request for picture blocks not entirely settled. By partitioning the input picture using a secret key, we may produce non-overlapping blocks. The image's dimensions (256 pixels on each side) are used to construct a chaotic sequence (X_1, X_2). As shown in Eqs. (4), (5):

$$X_1= \text{Chebyshev map.} (X_1, a_1, b_1, c_1) \tag{4}$$

$$X_2 = \text{Chirikov map.} (X_2, a_2, b_2, c_2) \tag{5}$$

To create the chaotic sequences 1 and 2, X_1 and X_2 combine to construct a hidden matrix (map). Randomly rearranging the pixels in each non-overlapping picture block is achieved by using the continuous raster scans. Image encryption uses a variety of key combinations, including

X_1, X_2 = Range (0-1)
a_1, a_2 = Range (0-5)
b_1, b_2 = Range (0, 2)
c_1, c_2 = Range (0-1)

In order to produce 2 keys (Key1 and Key2), we use the

Chebyshev and Chirikov Chaotic Map. The decryption key is calculated using Key1 and Key2 as inputs and the product as output. Bitwise XORing the Key with the shuffled and diffusion of image yields the final encrypted image as Eq. (6):

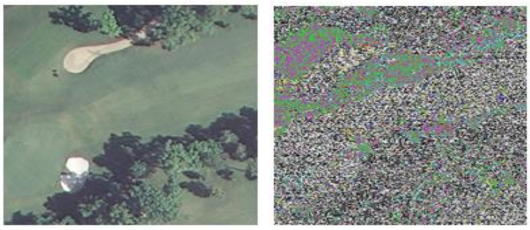
$$\text{Encrypted\_image} = \text{bitwise\_Ex-OR(Key, image)} \tag{6A}$$

Decryption is a backwards process; Eq. (6B) indicates decryption process:

$$\text{Decrypted\_image} = \text{bitwise\_Ex-OR(Key, encrypted image)} \tag{6B}$$

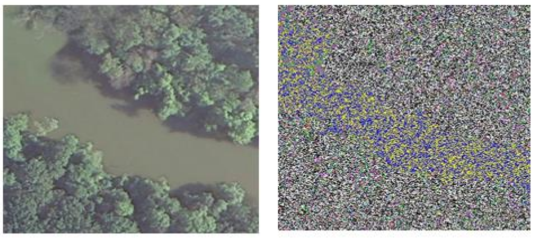
4. RESULTS AND DISCUSSION

The test pictures incorporate variety pictures and are chosen for approving the suggested encryption method aims. The suggested encryption method, plans are applied on these test pictures; then pictures as encoded pictures are recognized. The proposed conspire produced the scrambled pictures for two test pictures (for example golfcourse10, and river10), which is delineated in Figures 4, and 5 separately. Results show that the proposed technique is successful.



(a) (b)

Figure 4. (a) Golfcourse10 (original image), (b) Encrypted image



(a) (b)

Figure 5. (a) river10 (original image), (b) Encrypted image

To test the cryptographic system' security, differential attack is a capable strategy. The capacity of opposing differential assault is determined frequently by utilizing Unified Average Changing Intensity (UACI) and Number of Pixels Change Rate (NPCR). The mathematical expressions of UACI and NPCR are shown in Eqs. (7) and (8).

$$\text{UACI} = 1/(W\ X\ H)\ [(\sum|c1(i,j) - c2(i,\ j|)/255]X\ 100 \tag{7}$$

$$\text{NPCR} = (\sum\_(i,j)\ D\ (i,j))/(W\ X\ H)\ \text{X}\ 100\% \tag{8}$$

where, picture level and width is portrayed as H and w, the pixel worth of two scrambled pictures in the i^{th} line and j^{th} segment is addressed as c_1(i, j) and c_2(i, j). Suppose c_1(i, j) not equal to c_2(i, j) then the value of (i, j) is 1 or D(i, j) = 0.

Theoretically, NPCR should be set at 100%, whereas UACI should be set at 33.333%. At the point when the assessed numbers are nearer to the hypothetical qualities, the encryption method is more protected.

Key Sensitivity Analysis:

Table 1 shows the consequences of a key responsiveness examination, in which NPCR and not set in stone for a similar picture with two different keys (K1 and K2).

Differential Attack Analysis:

Each test picture has a randomly chosen pixel tweaked by one bit in order to ensure the suggested technique can withstand differential attacks. Table 2 exhibits the after effects of NPCR and UACI tests performed on the first and changed pictures utilizing a similar encryption key.

Table 1. Key sensitivity analysis

Image	NPCR	UACI
River10.tiff (K_1)	99.569702	32.502447
River10.tiff (K_2)	99.006323	31.46831
Golfcourse10.tiff (K_1)	99.530029	28.864142
Golfcourse10.tiff (K_2)	99.571228	28.464142

Table 2. Differential attacks on NPCR and UACI

Image	NPCR	UACI
River10.tiff	99.569702	32.502447
Modified River10.tiff	99.006323	31.46831
Golfcourse10.tiff	99.530029	28.864142
Modified Golfcourse10.tiff	99.571228	28.464142

Table 3 indicates performance of proposed Encryption Technique for various images from UC Merced Land Use dataset.

Table 4 shows the outcomes acquired utilizing various encryption procedure. Parameters in table like Entropy, Correlation Coefficient, Execution Time, NPCR values are improved, hence making it more robust and secure system.

Table 5 contrasts the proposed strategy and existing techniques shows that execution time is least among all techniques which indeed makes it time efficient encryption system. Also, negative correlation coefficient indicates high randomness tend to high security.

Table 3. Chirikov_map Chebyshev_map with diffusion and shuffling

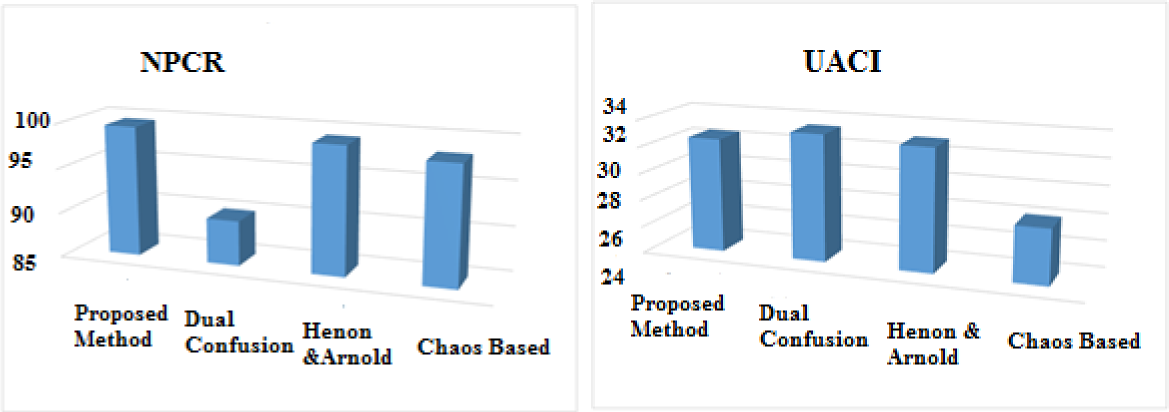
Image	NPCR	UACI	Entropy		Correlation Coefficient	
			Source Image	Encrypted Image	Red	Green
Tenniscourt00.tif	99.569702	32.502447	7.9436	7.9301	-0.001976	-0.000823
River10.tiff	99.606323	32.46831	7.937453	7.930186	-0.001976	-0.000823
Golfcourse10.tiff	99.530029	28.864142	7.887903	7.838825	-0.003349	-0.003981
Airplane18.tiff	99.571228	28.864142	7.914895	7.89767	-0.001899	-0.002488

Table 4. Comparative analysis of various chaotic maps

Image	NPCR	UACI	Entropy	Correlation Coefficient	Execution Time
Proposed method	99.569702	32.502447	7.9301	-0.0011	0.262454
Dual confusion [51]	90.0239	33.4269	6.62845	-0.0023	0.823455
Hennon and Arnold map combination [52]	99.23	33.0723	6.6337	0.0023	0.7655
Chaos based partial encryption scheme [53]	98.2354	28.1145	7.9989	0.00275	0.59375

Table 5. Comparison of existing encryption techniques

Encryption Technique	Entropy	Correlation Coefficient	Execution Time
Som et al. [53]	7.9968	0.00225	1.0825
Liu et al. [54]	7.989	0.00936	0.8753
Proposed Method	7.9301	-0.0011	0.262454



(a) NPCR

(b) UACI

Figure 6. Comparative representation of various chaotic map encryption method

Table 6. NPCR and UACI of respective channels

Channel	Entropy Source	Entropy Encrypted	NPCR	UACI	Correlation Coefficient
Red	7.930780	7.930917	99.586487	32.467454	-0.004568
Green	7.943494	7.943043	99.578857	32.502274	-0.004176
Blue	7.942184	7.941433	99.594116	32.480630	-0.004270

Following figure indicates Plots of NPCR and UACI are addressed in Figure 6 separately.

Table 6 shows the entropy, NPCR, UACI, and correlation coefficients for the singular red, green, and blue channels used to make the image showed in Figure 7. low correlation coefficient values between the original and encrypted images are generally considered desirable in image encryption to indicate effective randomization and increased security.

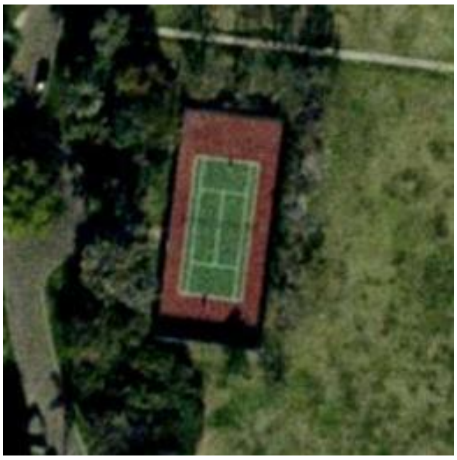


Figure 7. Original image Golf courses

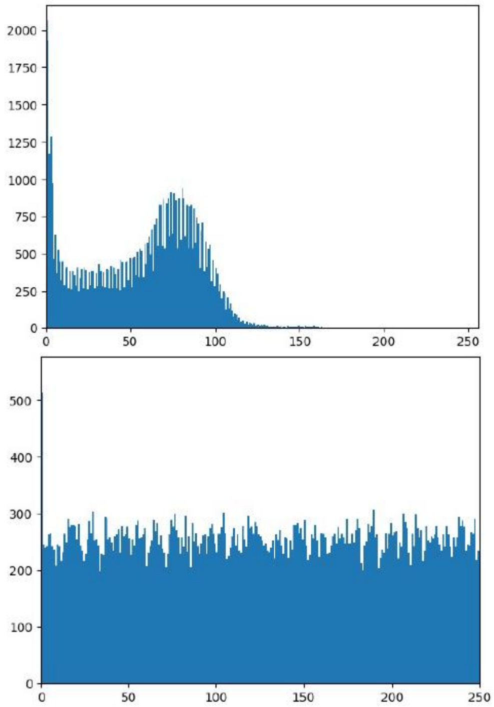


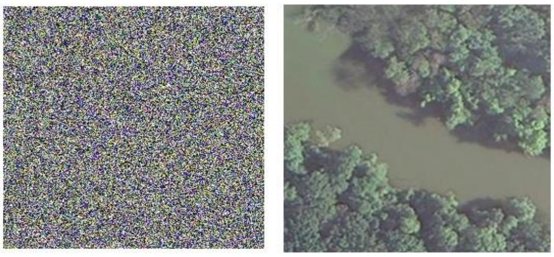
Figure 8. Histogram for original and encrypted image Golf course

In Figure 8, we see a histogram of the raw data and the encrypted version. This flat histogram of encrypted image indicates uniformly distributed pixels after encoding process which indicates that the encryption process has effectively randomized the pixel values, making it more challenging for an observer to discern any patterns or information about the original image.

A flat histogram implies that each intensity level is equally likely, and it can be an indication of a good diffusion property in the encryption method. Diffusion is a process in encryption that ensures that a change in one part of the input image affects the entire output image. This helps in spreading the information of the original image uniformly.

Decryption is a backwards process, Figure 9 displays river10's decryption.

Decrypted_image = bitwise_Ex-OR(Key, encrypted_image)



(a) (b)

Figure 9. (a) encrypted image (b) decrypted image (river10)

5. CONCLUSION

In this paper, we proposed an image encryption calculation in light of ceaseless raster Output utilizing Chirikov and Chebyshev chaotic maps. The pixels of image block are successfully mixed by shuffling and diffusion process, where the Chebyshev and the Chirikov is utilized to produce the keys. The proposed procedure ensures a high standard of results while maintaining efficiency in execution, with a notable reduction in processing time. The encryption method employed achieves a superior level of randomness and pixel value dispersion, contributing significantly to the security of the encrypted data. Additionally, the encryption and unscrambling processes are characterized by their straightforward execution, further emphasizing their essential nature. The results affirm the feasibility, robustness, and time efficiency of the system. Looking forward, potential enhancements include exploring different combinations of chaotic maps and implementing pixel shuffling as a post-processing step, with the aim of further optimizing the system's performance.

ACKNOWLEDGMENT

We are deeply grateful to Dr. Shubhangi Vaikole and Prof. Sangeeta Chaudhari for their unwavering guidance, expertise, and invaluable insights through her research work which greatly enriched the research and the quality of this paper.

REFERENCES

[1] Preishuber, M., Hutter, T., Katzenbeisser, S., Uhl, A. (2018). Depreciating motivation and empirical security analysis of chaos-based image and video encryption. IEEE Transactions on Information Forensics and Security, 13(9): 2137-2150. https://doi.org/10.1109/TIFS.2018.2812080

[2] Lin, C.M., Pham, D.H., Huynh, T.T. (2021). Encryption and decryption of audio signal and image secure communications using chaotic system synchronization control by TSK fuzzy brain emotional learning controllers. IEEE Transactions on Cybernetics, 52(12): 13684-13698. https://doi.org/10.1109/TCYB.2021.3134245

[3] Zolfaghari, B., Bibak, K., Koshiba, T. (2022). The odyssey of entropy: Cryptography. Entropy, 24(2): 266. https://doi.org/10.3390/e24020266

[4] Bibak, K., Ritchie, R., Zolfaghari, B. (2021). Never-ending security of quantum key conveyance with 1k-dwcdm and quadratic hash. Quantum Information and Computation, 21(3-4): 181-202. https://doi.org/10.26421/QIC21.3-4-1

[5] Dong, T., Huang, T. (2019). Neural cryptography based on complex-valued neural network. IEEE Transactions on Neural Networks and Learning Systems, 31(11): 4999-5004. https://doi.org/10.1109/TNNLS.2019.2955165

[6] Zolfaghari, B., Bibak, K., Koshiba, T., Nemati, H.R., Mitra, P. (2021). Statistical Trend Analysis of Physically Unclonable Functions: An Approach via Text Mining. CRC Press.

[7] Dai, J., Hao, X., Yan, X., Li, Z. (2022). Adaptive false-target recognition for the proximity sensor based on joint-feature extraction and chaotic encryption. IEEE Sensors Journal, 22(11): 1 0828-10840. https://doi.org/10.1109/JSEN.2022.3169746

[8] Wang, X., Feng, L., Wang, S., Chuan, Z., Zhang, Y. (2018). Spatiotemporal chaos in coupled logistic map lattice with dynamic coupling coefficient and its application in image encryption. IEEE Access, 6: 39705-39724. https://doi.org/10.1109/ACCESS.2018.2855726

[9] Faragallah, O.S., Afifi, A., El-Shafai, W., El-Sayed, H.S., Naeem, E.A., Alzain, M.A., Al-Amri, J.F., Soh, B., El-Samie, F.A. (2020). Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications. IEEE Access, 8: 42491-42503. https://doi.org/10.1109/ACCESS.2020.2974226

[10] Wang, J., Chen, G. (2015). Design of a chaos-based digitlal image encryption algorithm in time domain. In 2015 IEEE International Conference on Computational Intelligence & Communication Technology, Ghaziabad, India, pp. 26-29. https://doi.org/10.1109/CICT.2015.23

[11] Ge, X., Liu, F.L., Lu, B., Wang, W., Chen, J. (2010). An image encryption algorithm based on spatiotemporal chaos in DCT domain. In 2010 2nd IEEE International Conference on Information Management and Engineering, Chengdu, China, pp. 267-270. https://doi.org/10.1109/ICIME.2010.5477434

[12] Luo, Y., Du, M., Liu, D. (2012). Jpeg image encryption algorithm based on spatiotemporal chaos. In 2012 Fifth International Workshop on Chaos-fractals Theories and Applications, Dalian, China, pp. 191-195. https://doi.org/10.1109/IWCFTA.2012.49

[13] He, B., Zhang, F., Luo, L., Du, M., Wang, Y. (2009). An image encryption algorithm based on spatiotemporal chaos. In 2009 2nd International Congress on Image and

Signal Processing, Tianjin, China, pp. 1-5. https://doi.org/10.1109/CISP.2009.5301320

[14] Hou, J., Xi, R., Liu, P., Liu, T. (2016). The switching fractional order chaotic system and its application to image encryption. IEEE/CAA Journal of Automatica Sinica, 4(2): 381-388. https://doi.org/10.1109/JAS.2016.7510127

[15] Wei, J., Zhang, M., Tong, X. (2021). Image encryption algorithm based on fractional order chaotic system. In 2021 IEEE 12th international conference on software engineering and service Science (ICSESS), Beijing, China, pp. 72-75. https://doi.org/10.1109/ICSESS52187.2021.9522343

[16] George, R.T., Gopakumar, K. (2014). Spatiotemporal chaos in globally coupled NCA map lattices using 3-D Arnold cat map for digital image encryption. In 2014 First International Conference on Computational Systems and Communications (ICCSC), Trivandrum, India, pp. 203-208. https://doi.org/10.1109/COMPSC.2014.7032648

[17] Zhang, Y., Xie, J., Sun, P., Huang, L. (2010). A new image encryption algorithm based on Arnold and coupled chaos maps. In 2010 International Conference on Computer and Communication Technologies in Agriculture Engineering, Chengdu, pp. 308-311. https://doi.org/10.1109/CCTAE.2010.5543244

[18] Wu, X. (2013). A novel chaos-based image encryption scheme using coupled map lattices. In 2013 10th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Shenyang, China, pp. 1020-1024. https://doi.org/10.1109/FSKD.2013.6816345

[19] Jiang, H.Y., Fu, C. (2008). An image encryption scheme based on Lorenz chaos system. In 2008 Fourth International Conference on Natural Computation, Jinan, China, pp. 600-604. https://doi.org/10.1109/ICNC.2008.813

[20] Sharma, M., Bhargava, A. (2016). Chaos based image encryption using two step iterated logistic map. In 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Jaipur, India, pp. 1-5. https://doi.org/10.1109/ICRAIE.2016.7939535

[21] Lei, L.H., Bai, F.M., Han, X.H. (2013). New image encryption algorithm based on logistic map and hyper-chaos. In 2013 International Conference on Computational and Information Sciences, Shiyang, China, pp. 713-716. https://doi.org/10.1109/ICCIS.2013.193

[22] Mu, Z., Liu, H. (2020). Research on digital media image encryption algorithm based on logistic chaotic map. In 2020 International Conference on Robots & Intelligent System (ICRIS), Sanya, China, pp. 108-111. https://doi.org/10.1109/ICRIS52159.2020.00035

[23] Wu, X., Zhu, B., Hu, Y., Ran, Y. (2017). A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps. IEEE Access, 5: 6429-6436. https://doi.org/10.1109/ACCESS.2017.2692043

[24] Zhu, C., Sun, K. (2018). Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps. IEEE Access, 6: 18759-18770. https://doi.org/10.1109/ACCESS.2018.2817600

[25] Bisht, A., Jaroli, P., Dua, M., Dua, S. (2018). Symmetric multiple image encryption using multiple new one-dimensional chaotic functions and two-dimensional cat man. In 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, pp. 676-682. https://doi.org/10.1109/ICIRCA.2018.8597245

[26] Wang, X., Zhu, X., Zhang, Y. (2018). An image encryption algorithm based on Josephus traversing and mixed chaotic map. IEEE Access, 6: 23733-23746. https://doi.org/10.1109/ACCESS.2018.2805847

[27] Fu, C., Li, W.J., Meng, Z.Y., Wang, T., Li, P.X. (2013). A symmetric image encryption scheme using chaotic baker map and Lorenz system. In 2013 Ninth International Conference on Computational Intelligence and Security, Emeishan, China, pp. 724-728. https://doi.org/10.1109/CIS.2013.158

[28] Choi, U.S., Cho, S.J., Kang, S.W. (2020). Color image encryption algorithm for medical image by mixing chaotic maps. In 2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), Porto, Portugal, pp. 1-5. https://doi.org/10.1109/CSNDSP49049.2020.9249557

[29] Wang, X., Liu, P. (2020). A new image encryption scheme based on a novel one-dimensional chaotic system. IEEE Access, 8: 174463-174479. https://doi.org/10.1109/ACCESS.2020.3024869

[30] Yang, S., Tong, X. (2021). A block image encryption algorithm based on 2d chaotic system. In 2021 IEEE 12th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, pp. 61-64. https://doi.org/10.1109/ICSESS52187.2021.9522269

[31] Qian, X., Yang, Q., Li, Q., Liu, Q., Wu, Y., Wang, W. (2021). A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques. IEEE Access, 9: 61334-61345. https://doi.org/10.1109/ACCESS.2021.3073514

[32] Huang, Y., Huang, L., Wang, Y., Peng, Y., Yu, F. (2020). Shape synchronization in driver-response of 4-D chaotic system and its application in image encryption. IEEE Access, 8: 135308-135319. https://doi.org/10.1109/ACCESS.2020.3011524

[33] Zhu, S., Zhu, C. (2019). Plaintext-related image encryption algorithm based on block structure and five-dimensional chaotic map. IEEE Access, 7: 147106-147118. https://doi.org/10.1109/ACCESS.2019.2946208

[34] Qiu, W.C., Yan, S.J. (2019). An image encryption algorithm based on the combination of low-dimensional chaos and high-dimensional chaos. In 2019 3rd International Conference on Electronic Information Technology and Computer Engineering (EITCE), Xiamen, China, pp. 684-687. https://doi.org/10.1109/EITCE47263.2019.9094882

[35] Xu, J., Zhao, C., Mou, J. (2020). A 3D image encryption algorithm based on the chaotic system and the image segmentation. IEEE Access, 8: 145995-146005. https://doi.org/10.1109/ACCESS.2020.3005925

[36] Zope-Chaudhari, S., Venkatachalam, P. (2014). Robust copyright protection of raster images using wavelet based digital watermarking. In 2014 IEEE Geoscience and Remote Sensing Symposium, Quebec City, QC, Canada, pp. 3129-3132. https://doi.org/10.1109/IGARSS.2014.6947140

[37] Ren, L. (2021). A novel raster map exchange scheme based on visual cryptography. Advances in Multimedia, 2021: 3287774. https://doi.org/10.1155/2021/3287774

[38] Min, L., Yu, Q. (2007). A digital map watermarking algorithm based on discrete cosine transform. Computer Applications and Software, 24(1): 146-148.

[39] Yin, P., Min, L. (2010). A color image encryption algorithm based generalized chaos synchronization for bidirectional discrete systems for audio signal communication. In 2010 International Conference on Intelligent Control and Information Processing, Dalian, China, pp. 443-447. https://doi.org/10.1109/ICICIP.2010.5565244

[40] Wang, J. (2009). Image encryption algorithm based on 2-d wavelet transform and chaos sequences. 2009 International Conference on Computational Intelligence and Software Engineering, Wuhan, China, pp. 1-3. https://doi.org/10.1109/CISE.2009.5362955

[41] Zhang, Q., Shen, M., Li, B., Fang, R. (2014). Chaos-based color image encryption scheme in the wavelet domain. In 2014 7th International Congress on Image and Signal Processing, Dalian, China, pp. 330-334. https://doi.org/10.1109/CISP.2014.7003801

[42] Wang, Q., Ding, Q., Zhang, Z., Ding, L. (2008). Digital image encryption research based on dwt and chaos. In 2008 Fourth International Conference on Natural Computation, Jinan, China, pp. 494-498. https://doi.org/10.1109/ICNC.2008.105

[43] Zhang, S., Cai, R., Jiang, Y., Guo, S. (2009). An image encryption algorithm based on multiple chaos and wavelet transform. In 2009 2nd International Congress on Image and Signal Processing, Tianjin, China, pp. 1-5. https://doi.org/10.1109/CISP.2009.5301361

[44] Macovei, C., Răducanu, M., Datcu, O. (2020). Image encryption algorithm using wavelet packets and multiple chaotic maps. In 2020 International Symposium on Electronics and Telecommunications (ISETC), Timisoara, Romania, pp. 1-4. https://doi.org/10.1109/ISETC50328.2020.9301088

[45] Li, X., Zhang, Y. (2016). Digital image encryption and decryption algorithm based on wavelet transform and chaos system. In 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Xi'an, China, pp. 253-257. https://doi.org/10.1109/IMCEC.2016.7867211

[46] Karmakar, J., Mandal, M.K. (2020). Chaos-based image encryption using integer wavelet transform. In 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, pp. 756-760. https://doi.org/10.1109/SPIN48934.2020.9071316

[47] Gao, H., Wang, X. (2021). Chaotic image encryption algorithm based on zigzag transform with bidirectional crossover from random position. IEEE Access, 9: 105627-105640. https://doi.org/10.1109/ACCESS.2021.3099214

[48] Zhang, L., Wu, J., Zhou, N. (2009). Image encryption with discrete fractional cosine transform and chaos. In 2009 Fifth International Conference on Information Assurance and Security, Xi'an, China, pp. 61-64. https://doi.org/10.1109/IAS.2009.89

[49] Jiang, A., Yu, J., Cang, X. (2010). Image encryption algorithm based on chaos and contourlet transform. In 2010 First International Conference on Pervasive Computing, Signal Processing and Applications, Harbin, China, pp. 707-710. https://doi.org/10.1109/PCSPA.2010.176

[50] Li, X.M., Dai, L. (2010). Reality-preserving image encryption assosiated with the chaos and the LCT. In 2010 3rd International Congress on Image and Signal Processing, Yantai, China, pp. 2624-2627. https://doi.org/10.1109/CISP.2010.5648150

[51] Rehman, A.U., Liao, X. (2019). A novel robust dual diffusion/confusion encryption technique for color image based on Chaos, DNA and SHA-2. Multimedia Tools and Applications, 78(2): 2105-2133. https://doi.org/10.1007/s11042-018-6346-1

[52] Sankhe, P., Pimple, S., Singh, S., Lahane, A. (2018). An image cryptography using henon map and arnold cat map. International Research Journal of Engineering and Technology (IRJET), 5(4): 1900-1904.

[53] Som, S., Kotal, A., Mitra, A., Palit, S., Chaudhuri, B.B. (2014). A chaos based partial image encryption scheme. In 2014 2nd International Conference on Business and Information Management (ICBIM), Durgapur, India, pp. 58-63. https://doi.org/10.1109/ICBIM.2014.6970933

[54] Liu, L., Zhang, Q., Wei, X. (2012). A RGB image encryption algorithm based on DNA encoding and chaos map. Computers & Electrical Engineering, 38(5): 1240-1248. https://doi.org/10.1016/j.compeleceng.2012.02.007

NOMENCLATURE

UACI	Unified Average Changing Intensity
NPCR	Number of Pixels Change Rate