

## Chapter

# Encryption Scheme for the Security of Digital Images Based on Josephus Traversal and Chaos Theory

*Manzoor Ahmad Lone*

## Abstract

A synergistic approach based on the Josephus traversal and chaos theory is suggested for the security of digital images. To encrypt the digital images, a combination of the Josephus Traversal principle and the 2-dimensional Hénon map is employed for the secure transmission of digital data. The two distinct key matrices are used in the Josephus principle to cause bit-level shuffling throughout the image. These two distinct key matrices are effectively formed by the chaotic streams generated by the two-dimensional Hénon map. The system becomes more unpredictable because the Josephus traversal employs a different key set for every individual pixel to scramble it at the bit level. Moreover, the image is shuffled and diffused at the pixel level using the same streams produced by chaotic structure. The test images are used to determine the strength of the suggested system. The numerical results and comparative findings of the various quality parameters such as key space, information entropy, correlation coefficient, histogram analysis, differential attack indicators (NPCR and UACI) verify the strength of the encryption system. The acceptable key space, numerical values of entropy approaches to ideal value, correlation coefficient values close to 0, and satisfactory results of theoretical value tests verify the robustness of the employed scheme to resist various types of cryptanalytical attacks.

**Keywords:** security, Josephus traversal, encryption, 2D Hénon map, confusion, diffusion

## 1. Introduction

Encryption process transforms the information (plain-text) into a non-readable format (cipher-text) using some well-defined encryption method. The unauthorized persons without the prior knowledge of secret keys used in the encryption process are unable to recover the original information [1]. The digital data communicated over the internet always experience the risk of security. Thus, for a smooth and effective delivery system, sensitive and private data always needs to be masked and protected before transmission over the internet [2]. Multimedia content, such as digital images, plays an important role in the e-healthcare system, e-governance, e-commerce, e-education, e-banking, and in other fields of human life. Therefore, to ensure the safe

communication of data, a secure transmission method needs to be designed and developed. The security paradigms, such as watermarking, cryptography, steganography, and so forth, are applied to impart security to the data communicated over insecure internet channels. A large number of encryption algorithms have been fabricated by researchers using techniques such as wavelet transform, chaos theory, DNA encoding, cellular automata, and others. Among them, the encryption methods based on chaos theory for the fabrication of data security algorithms is a fundamental alluring option used by researchers. In recent years, various encryption schemes for digital images based on chaotic maps have been suggested [3–14]. These schemes either use low-dimensional and high-dimensional chaotic maps, or a mixture of them, or enhance the existing chaotic structures, or combine them with other techniques to encrypt the digital images. In [10], the suggested encryption scheme uses a single chaotic map, the Arnold map, to generate the final cipher image. In the encryption scheme, the scrambling and diffusion of pixels are achieved by using the Arnold map. In [15], the encryption method first uses the Chebyshev map to diffuse and shuffle pixels, and then, it applies the modified Logistic map to mask and confuse the pixels simultaneously. This scheme has fine pseudorandomness and is resistant to different types of attacks. In [16], the encryption scheme combines chaos theory and elliptic curve ElGamal (EC-ElGamal) to secure digital image communication. The scheme not only enhances the security of the encryption system but also addresses key management problem. In [17], a new 2D cosine map is proposed that has fine ergodicity, a more perplexing nature, more randomness, and a large chaotic range compared to the existing 2D chaotic map. In [11], the proposed encryption method uses the 1D logistic map and Josephus traversal principle to produce a reliable cipher image. The scheme is highly sensitive to initial value conditions that boost the security of the system.

In [18], the encryption method uses chaotic structures and DNA encoding with a one-time pad to confuse and diffuse the digital images. First, the image is shuffled, and the shuffled image is divided into four sub-images of equal sizes, and DNA rules encode these sub-images and diffuse them, respectively. The diffusion process is obtained by DNA XOR operations, and at last, these sub-images are joined to form the cipher image. The algorithm provides resistance to typical attacks and has good security. In [19], the suggested scheme uses variable step Josephus traversal and a Y-index Space Filling Curve (SFC) to provide an effective and enhanced image encryption security algorithm. The numerical findings and the comparison results of the proposed algorithm depict that this scheme has good security than others. In [2], the encryption scheme uses a combined approach of chaotic maps and the Affine Hill Cipher method to generate a secure cipher. In the first two stages of encryption, the input image is shuffled and diffused by the application of the 2-dimensional Hénon map and the 3-dimensional logistic map, respectively. Finally, the application of the AHC technique produces a strong cipher image. In [20], authors proposed an encryption scheme based on chaotic systems, hash function, and Josephus traversal concept. The encryption method applies chaotic system initialization, pixel shuffling, and pixel diffusion to form a cipher image. The system has effective security and efficiently combats against various attacks.

Inspired by the above literature study, the suggested scheme couples chaotic structure 2D Hénon map with Josephus traversal principle to form an encryption framework. The suggested scheme first brings bit-shuffling in all the pixels of the plain image with help of the Josephus traversal. After it, the confusion and diffusion in the pixels of the image is carried by using the two chaotic streams  $R_x^c$  and  $R_y^c$ , respectively, generated by the 2D Hénon map. Further, the two chaotic sequences generated by the 2D Hénon map are used in a novel way to generate the key matrices for Josephus

traversal. The Josephus traversal is operated on each individual pixel at the bit level. It uses a distinct key set for every pixel to trigger the bit-level scrambling in the image data. The key set used for the shuffling of bits in each individual pixel by the Josephus traversal is derived from the two chaotic sequences generated by the 2D Hénon map. The variable key set notion used in the Josephus traversal improves the overall randomness and unpredictability, thus enhancing the performance and security of the proposed system. The initial key parameter of the chaotic system is related to the plain image, which greatly increases the security of the system. The small change in such dependencies brings an avalanche in the output of a cryptosystem. Further, the favorable key space, satisfactory results of correlation coefficient, entropy results, differential attack indicator (NPCR and UACI) results, and uniform histograms of cipher images determine the strength of the proposed image encryption system.

## 2. Preliminaries

### 2.1 Two-dimensional Hénon map

Michel Hénon in 1976 introduced the concept of the 2-dimensional Hénon map in [21]. It is a model of a nonlinear discrete-time dynamical system showing chaos defined on a 2D plane. The 2D Hénon map is employed in various image security approaches [22–24]. Following is the mathematical relation of the map:

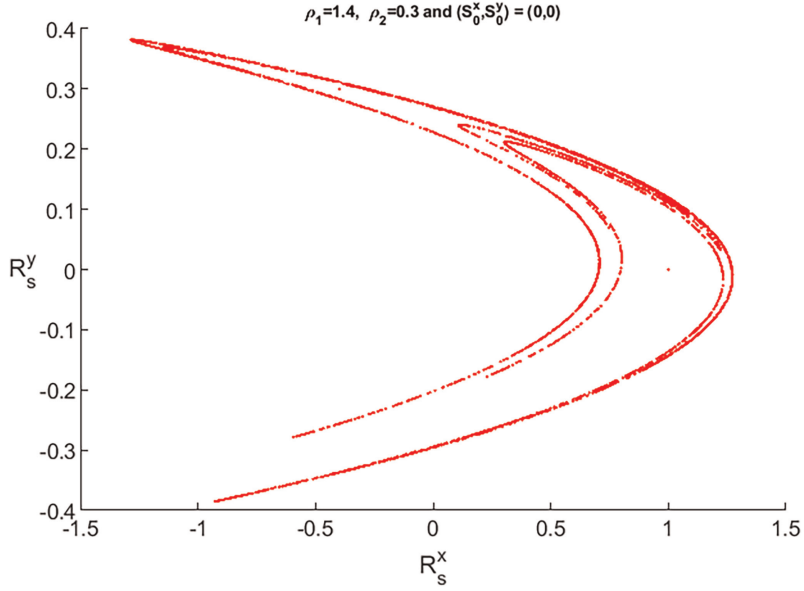
$$\begin{cases} R_{s+1}^x = 1 - \rho_1 \times R_s^x + R_s^y, \\ R_{s+1}^y = \rho_2 \times R_s^x, \end{cases} \quad (1)$$

where represent the initial conditions, and parameters  $\rho_1$  and  $\rho_2$  are known as bifurcation parameters. For  $\rho_1 \in [0, 1.4]$ ,  $\rho_2 = 0.3$ , the bifurcation characteristic nature of the Hénon map can be observed and is generally investigated at  $\rho_1 = 1.4$  and  $\rho_2 = 0.3$  as shown in **Figures 1** and **2**. The extent of thickness and stretching is governed by the bifurcation parameters  $(\rho_1, \rho_2)$  also named as chaotic attractors.

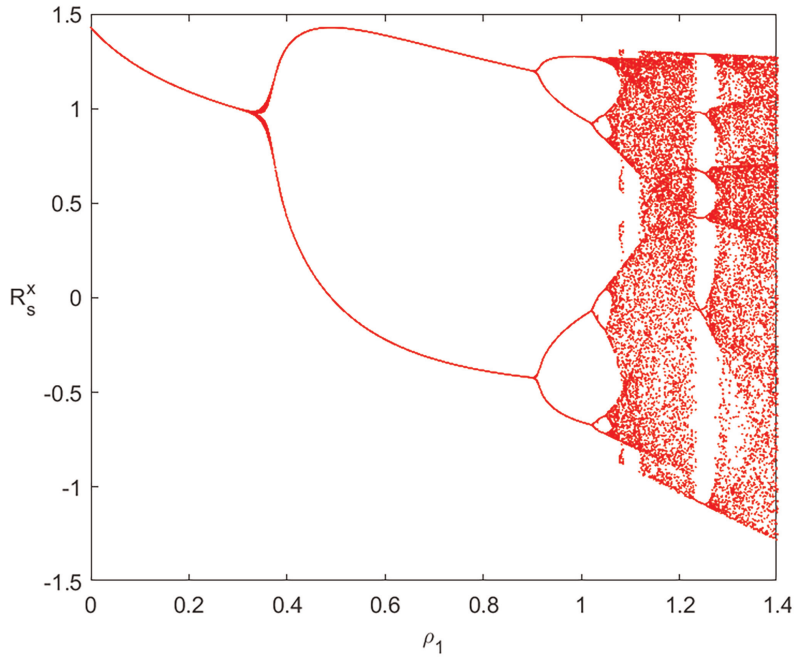
### 2.2 Josephus problem

The Josephus traversal is a famous problem in Computer Science and Mathematics [13, 25–28]. The problem is named after a Jewish historian Flavius Josephus. It represents a theoretical problem that is similar to a counting-out player game. In this game, there are  $n$  players in a circular pattern. Traverse the circle in a predetermined direction and start at a pre-specified first  $x^{th}$  person, eliminating the first person. After the first person is eliminated, then a predefined step count is used to skip a certain number of persons in the already predefined direction and eliminate the second person. The procedure continues, starting with the next person, following the same direction and using the same step count to skip persons till the last person is left. In the end, the persons eliminated from the circle, starting at a specified position, in a predetermined order and with a predetermined step count form a sequence known as the Josephus traversal sequence. Hence, the Josephus traversal contains three parameters  $n$ ,  $x$ , and  $c$ , where  $n$  is the total number of players in the game,  $x$  is starting person, and  $c$  is the step count to skip the certain number of persons in a pre-specified direction. Thus, the Josephus traversal is represented by function  $\mathcal{R}_{\odot} = J(n, x, c)$ ,

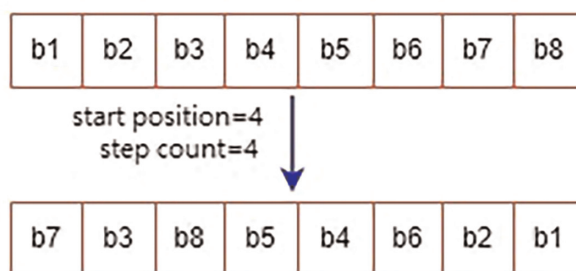
where  $\mathcal{R}_\odot$  represents the Josephus traversal sequence. For example, the solution to  $\mathcal{R}_\odot = J(7,1,2)$ , where  $n = 7$  with 1, 2, 3, 4, 5, 6, 7 makes a circle,  $x = 1$  and  $c = 4$ , we obtain the Josephus traversal sequence  $\mathcal{R}_\odot = 4, 1, 6, 5, 7, 3, 2$ .



**Figure 1.**  
*2D Hénon attractor.*



**Figure 2.**  
*2D Hénon map's bifurcation plot.*



**Figure 3.**  
 Bit shuffling using Josephus traversal, when starting position = 4 and step count = 4.

To enhance the randomness and unpredictability in the Josephus traversal sequence, the literature [11–13, 20, 29, 30] motivated to exploit a similar type of pattern to raise the degree of randomness in the Josephus traversal. The distinct starting positions and the distinct step counts for the Josephus traversal are determined from  $R_s^x$  and  $R_s^y$  chaotic sequences, respectively, generated by the two-dimensional Hénon map. The two chaotic sequences  $R_s^x$  and  $R_s^y$  are scaled in the range of [1–8] and transformed into two matrices  $[M_s]$  and  $[M_c]$  of the same dimensions as the original image.  $[M_s]$  work as the starting position key matrix, and  $[M_c]$  act as the step count key matrix. In the proposed scheme, the element from  $[M_s]$  and  $[M_c]$  frame the key set for Josephus traversal to operate the bit shuffling in one pixel of the plain image. Likewise, to bring the bit shuffling in all pixels, key sets are derived for Josephus traversal from  $[M_s]$  and  $[M_c]$ . Thus, distinct key sets for all individual pixels of the image are framed and applied to cause bit shuffling in each pixel, as demonstrated in **Figure 3**, respectively. This feature enhances the security of the proposed scheme system.

### 3. Initialization and encryption process

The assignment process of initial conditions of the 2D Hénon map and the proposed encryption algorithm are elaborated in this section.

#### 3.1 Initialization of chaotic structure

The initial value conditions of the 2-dimensional Hénon map are made dependent on the plain image data. In such relations, a small change produces an avalanche in the cipher, hence ensuring protection against cryptanalytical attacks. The key generation pattern discussed in [31] inspired author to initialize the initial values of the 2-dimensional Hénon map shown as follows:

```

 $k = (1/(\text{row} * \text{col} * 255)) * (\sum \text{img});$ 
if ( $k \geq 1$ )
 $R_0^x = \text{mod}(k, 1);$ 
else.
 $R_0^x = k;$ 
end if
 $R_0^y = (R_0^x/2);$ 
    
```

### 3.2 Encryption process

The proposed algorithm are elaborated in this section. The values of  $R_0^x$ ,  $R_0^y$ ,  $\rho_1$ , and  $\rho_2$  represent the secret key parameters in the suggested system. The steps followed in the suggested encryption system are listed below:

---

#### Algorithm-I

---

- Step 1:** Transform the input image  $[img_o]$  into the binary form image, say  $[img^{Bin}]$ .
- Step 2:** Apply Hénon map using Eq. (1) and generate two chaotic sequence  $R_s^x$  and  $R_s^y$ .
- Step 3:** Scale both the sequences  $R_s^x$  and  $R_s^y$  in the range of [1–8] and transform them into matrices, say  $[M_s]$  and  $[M_c]$ , respectively.
- Step 4:**  $[M_s]$  and  $[M_c]$  are employed as distinct key set matrices for the Josephus traversal technique.
- Step 5:** Apply the Josephus traversal process as discussed in subsection 2.2 on the binary image produced in step 2.
- $$[img^{BinScrm}] \xleftarrow[\text{Traversal}]{\text{Josephus}} [img^{Bin}]$$
- Step 6:** Transform  $[img^{BinScrm}]$  into decimal form, say  $[img']$ .
- Step 7:** In this step, apply **Sort** index function to  $[R_s^x]$  sequences generated in step 3 and shuffle all the pixels of the image as shown in the following pseudo-code:  $[val \quad inx] := \text{sort}(R_s^x)$ ;  $[img''] = [img'](inx)$ ; Transform  $[img'']$  into a matrix.
- Step 8:** Select the  $[R_s^y]$  sequences generated in step 3 and scale it in the range of [0–255] and transform the scaled output into a matrix of  $row * col$  dimension, say  $[R^y]_{row * col}$ .
- Step 9:** Perform XOR operation between  $[img'']$  and  $[R^y]$ . This causes diffusion in the final image, and at the end, an encrypted image  $img^C$  is acquired.

Thus, at the end of the procedure, we obtain a cipher image  $img^C$ . The reconstruction of the original in the decryption process is obtained by following the inverse of all the steps followed in the encryption process.

---

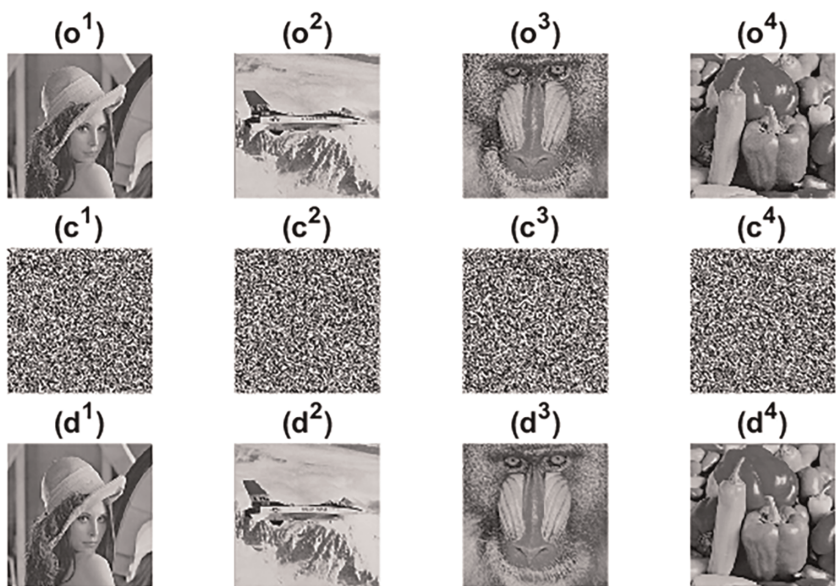
## 4. Result analysis

The results of the proposed system for various indicators are calculated using grayscale images shown in **Figure 4**. The size of the images is  $256 \times 256$ . MATLAB tool with a machine having Windows 10 and IntelR, CoreTM i7 CPU 2.40GHz and 16GB is used for the simulation purpose.

### 4.1 Key space

The key space of an encryption algorithm is a vital security parameter. It should be large enough to counter brute force attacks. According to the literature study [32], key space  $\geq 2^{128}$  is safe to resist exhaustive attacks. With a precision of  $2^{-15}$ , the total key space of the proposed algorithm is  $2^{199}$ , which is reliable to resist brute force attacks effectively.





**Figure 4.**  
 $o^1-o^4$  = plain images,  $c^1-c^4$  = cipher images,  $d^1-d^4$  = decrypted images.

## 4.2 Information entropy

The information entropy evaluation reflects the unpredictability and randomness of data. The values of entropy closer to the theoretical value of 8 for  $2^8$  gray-level image determine strong randomness in cipher data [33]. Eq. (2) represents the mathematical formula of information entropy:

$$\mathcal{IE}_{(S)} = - \sum_{v=0}^{255} p(S_v) \log_2 p(S_v), \quad (2)$$

where,  $S_v$  = source symbol, and  $p(S_v)$  = probability of source symbol. The numerical results of  $\mathcal{IE}_{(S)}$  listed in **Table 1** are close to the theoretical value 8, ensuring high randomness in the cipher data generated by the proposed encryption scheme.

Image	Entropy
Lena	7.9974
Jet	7.9969
Mandrill	7.9974
Pepper	7.9972

**Table 1.**  
 Information entropy results.

### 4.3 Differential attack

In this analysis, a little change is caused in the plain image, and then, the two images are encrypted by some predefined method. Through this investigation, the attacker attempts to know the link between plain image and cipher image. The two indicators, namely, NPCR (number of pixels change rate) and UACI (unified average changed intensity), are two basic parameters that decide the potential of an encryption system to withstand against differential attacks. Eq. (3) and Eq. (4) represent the two indicators, respectively [25].

$$NPCR = \frac{1}{row * col} \sum_{s_1, s_2} D_{(s_1, s_2)} * 100\% \quad (3)$$

$$D_{(s_1, s_2)} = \begin{cases} 1 & \text{if } img'_{(s_1, s_2)} \neq img''_{(s_1, s_2)} \\ 0 & \text{otherwise} \end{cases}$$

$$UACI = \frac{1}{(row * col)} * X * 100\%, \quad (4)$$

where,  $X = \sum_{s_1, s_2} \frac{|img'_{(s_1, s_2)} - img''_{(s_1, s_2)}|}{255}$

**Table 2** depicts the results of NPCR and UACI parameters and are in close proximity to their reference values. Hence, justify that the suggested scheme can resist differential attacks satisfactorily.

		$\mathcal{N}_{0.05}^*$	$\mathcal{N}_{0.01}^*$	$\mathcal{N}_{0.001}^*$ [34]
Image	NPCR	99.5693	99.5527	99.5341
Lena	99.6368	✓	✓	✓
Jet	99.6262	✓	✓	✓
Mandrill	99.6002	✓	✓	✓
Pepper	99.5804	✓	✓	✓
Avg.=	99.6110	✓	✓	✓
		$V_{0.05}^{*-}$	$V_{0.01}^{*-}$	$V_{0.001}^{*-}$ [20]
		$V_{0.05}^{*+}$	$V_{0.01}^{*+}$	$V_{0.001}^{*+}$
		33.2824	33.2255	33.1594
Image	UACI	33.6447	33.7016	33.7677
Lena	33.5372	✓	✓	✓
Jet	33.3475	✓	✓	✓
Mandrill	33.6070	✓	✓	✓
Pepper	33.4553	✓	✓	✓
Avg.=	33.4868	✓	✓	✓

**Table 2.**  
*Results of NPCR and UACI indicators.*



#### 4.4 Correlation analysis

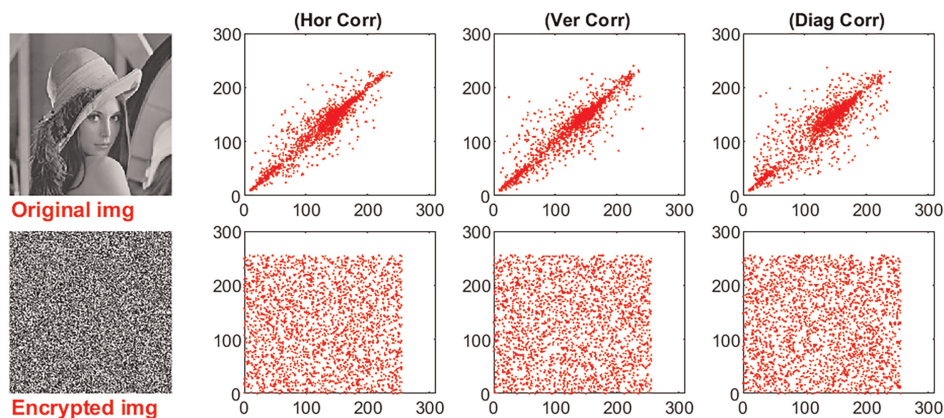
In an encrypted image, the correlation among the adjoining pixels in horizontal, vertical, and diagonal directions should be 0 or approaching to 0. If the correlation is mitigated, it is hard for an attacker to crack the cipher using statistical analysis. The correlation coefficient  $\psi_{s^x, s^y}$  [22] is used to conduct this analysis, represented by Eq. (5).

$$\begin{cases} \psi_{s^x, s^y} = \mathbb{C}_{(s^x, s^y)} / \left( \sqrt{D(s^x)}^* \sqrt{D(s^y)} \right), \\ \mathbb{C}_{(s^x, s^y)} = (1/N) * \sum_{i=1}^N F \\ F = (s_i^x - E(s^x)) * (s_i^y - E(s^y)) \\ D(s^x) = (1/N) * \sum_{i=1}^N (s_i^x - E(s^x))^2, \\ E(s^x) = (1/N) * \sum_{i=1}^N (s_i^x) \end{cases} \quad (5)$$

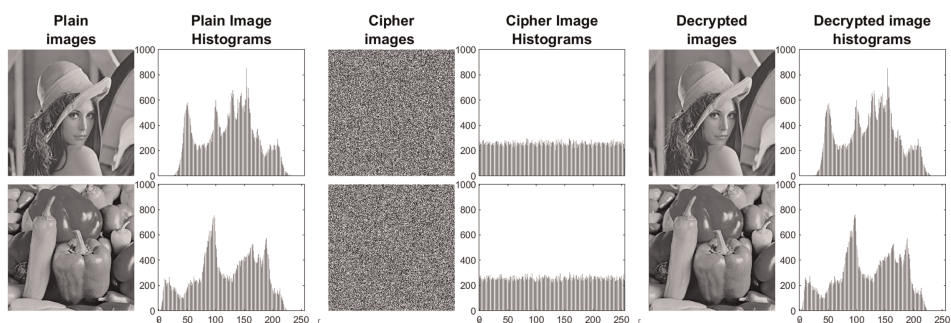
The correlation coefficient results of the encrypted image in **Table 3** are close to 0 along the horizontal (H), vertical (V), and diagonal (D) axis. **Figure 5** shows the correlation plots of plain and cipher images. It is obvious from **Figure 5** that the data is highly correlated in the plain image, and in contrast to it, the data in cipher image is strongly uncorrelated. Thus, it reveals that the proposed system is able to counter statistical attacks effectively.

Corr.	Lena	Jet	Mandrill	Pepper
VC	-0.0033	-0.0004	0.0002	0.0037
HC	-0.0054	-0.0064	0.0037	-0.0022
DC	0.0004	-0.0005	0.0045	-0.0002

**Table 3.**  
Correlation coefficient results.



**Figure 5.**  
Correlation plots.



**Figure 6.**  
*Histogram plots.*

## 4.5 Histogram analysis

The histogram distribution reveals important statistical information about an image. This information needs to be concealed in a cipher histogram, which is possible only if the encrypted image yields a flat histogram. If an encryption algorithm performs only pixel shuffling, the histogram of the image remains unaffected. Thus, the objective of the application of the bit-scrambling process and diffusion process in the proposed algorithm is to yield a uniform cipher histogram to counter the statistic attacks. Histogram plots of cipher and plain images are shown in **Figure 6**. It can be observed that histograms of cipher images are evenly distributed compared to the original images. Thus, the proposed algorithm masks the statistical information and results in an effective encryption system, which indicates that encrypted images yield uniform histograms. This ensures that the proposed security method can strongly counter the histogram based attacks.

## 5. Comparison results

The comparison results of the proposed scheme for entropy, NPCR, UACI, and correlation coefficient parameters are listed in **Table 4**. The comparative assessment shows that the outcomes of the suggested scheme are good, acceptable, and

Image	Algorithm	Entropy	NPCR	UACI	$H_{Corr}$	$V_{Corr}$	$D_{Corr}$
Lena	Proposed	7.9974	99.6368	33.5372	-0.0054	-0.0033	0.0004
	Ref. [35]	7.9972	99.6246	33.4226	0.0069	0.0479	0.0075
	Ref. [36]	7.9972	99.6124	33.4468	-0.0019	-0.00023	-0.00013
	Ref. [19]	7.9971	99.6337	33.6050	0.0071	-0.0052	0.0013
	Ref. [8]	7.9972	99.6262	33.4578	-0.0003	0.0016	0.0029
	Ref. [20]	7.9973	99.6117	33.4570	-0.0013	-0.0008	-0.0017
	Ref. [12]	7.9971	99.5989	33.4561	-0.0029	-0.0017	0.0004
	Ref. [37]	7.9975	99.6114	33.4636	-0.0223	-0.0084	-0.0086

**Table 4.**  
*Comparison results.*

concurrent with the results of the existing encryption schemes. Thus, the comparative analysis also favors the robustness, stalwartness, and effectiveness of the suggested encryption scheme.

## 6. Conclusion

The work in this article exploits chaotic system and the principle of the Josephus traversal to encrypt digital images. The suggested scheme makes efficient and effective use of the chaotic streams generated by the 2D Hénon map to shuffle and diffuse the image at the pixel level. Simultaneously, at the bit level, the same chaotic streams of the 2D Hénon map are employed to form the distinct keys in the Josephus traversal to shuffle the bits of the pixels in the whole image. The results of the key space, entropy, and correlation coefficient are favorable. The theoretical value test of differential attack indicators (NPCR and UACI) depicted in **Table 2** is satisfactorily. Thus, the simulation analysis verifies that the security level of the suggested method is good and thus can be used in image encryption.


## Author details

Manzoor Ahmad Lone  
Department of CSE, University of Kashmir (North Campus), India

\*Address all correspondence to: mahmadlone@gmail.com

## IntechOpen

---

© 2024 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

## References

- [1] Stinson DR. *Cryptography: Theory and Practice*. Boca Raton: CRC Press, Taylor & Francis Group; 2005
- [2] Lone MA, Qureshi S. Encryption scheme for rgb images using chaos and affine hill cipher technique. *Nonlinear Dynamics*. 2022;**11**:1-21
- [3] Belazi A, Talha M, Kharbech S, Xiang W. Novel medical image encryption scheme based on chaos and DNA encoding. *IEEE Access*. 2019;**7**: 36667-36681
- [4] Farah M, Farah A, Farah T. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. *Nonlinear Dynamics*. 2020;**99**(4):3041-3064
- [5] Li C, Luo G, Qin K, Li C. An image encryption scheme based on chaotic tent map. *Nonlinear Dynamics*. 2017;**87**(1): 127-133
- [6] Lone MA, Qureshi S. Rgb image encryption based on symmetric keys using Arnold transform, 3d chaotic map and affine hill cipher. *Optik*. 2022;**260**: 168880
- [7] Luo Y, Yu J, Lai W, Liu L. A novel chaotic image encryption algorithm based on improved baker map and logistic map. *Multimedia Tools and Applications*. 2019;**78**(15):22023-22043
- [8] Niu Y, Zhang X. A novel plaintext-related image encryption scheme based on chaotic system and pixel permutation. *IEEE Access*. 2020;**8**:22082-22093
- [9] Wu J, Cao X, Liu X, Ma L, Xiong J. Image encryption using the random frdct and the chaos-based game of life. *Journal of Modern Optics*. 2019;**66**(7): 764-775
- [10] Wu J, Liu Z, Wang J, Hu L, Liu S. A compact image encryption system based on Arnold transformation. *Multimedia Tools and Applications*. 2021;**80**(2): 2647-2661
- [11] Yang G, Jin H, Bai N. Image encryption using the chaotic Josephus matrix. *Mathematical Problems in Engineering*. 2014;**2014**:632060
- [12] Wang X, Zhu X, Zhang Y. An image encryption algorithm based on Josephus traversing and mixed chaotic map. *IEEE Access*. 2018;**6**:23733-23746
- [13] Yi G, Li-ping S, Lu Y. Bit-level image encryption algorithm based on Josephus and Henon chaotic map. *Application Research of Computers/Jisuanji Yingyong Yanjiu*. 2015;**32**(4):1-7
- [14] Zhou Y, Hua Z, Pun C-M, Chen CP. Cascade chaotic system with applications. *IEEE Transactions on Cybernetics*. 2014;**45**(9):2001-2012
- [15] Diab H. An efficient chaotic image cryptosystem based on simultaneous permutation and diffusion operations. *IEEE Access*. 2018;**6**:42227-42244
- [16] Luo Y, Ouyang X, Liu J, Cao L. An image encryption method based on elliptic curve elgamal encryption and chaotic systems. *IEEE Access*. 2019;**7**: 38507-38522
- [17] Hua Z, Jin F, Xu B, Huang H. 2d logistic-sine-coupling map for image encryption. *Signal Processing*. 2018;**149**: 148-161
- [18] Wang X, Wang Y, Zhu X, Unar S. Image encryption scheme based on chaos and DNA plane operations. *Multimedia Tools and Applications*. 2019;**78**(18): 26111-26128

- [19] Niu Y, Zhang X. An effective image encryption method based on space filling curve and plaintext-related Josephus traversal. *IEEE Access*. 2020;**8**: 196326-196340
- [20] Niu Y, Zhou H, Zhang X, Qin L, et al. Hybrid encryption algorithm based on gray curve and Josephus permutation. *Computational Intelligence and Neuroscience*. 2022;**2022**:7076416
- [21] Hénon M. A two-dimensional mapping with a strange attractor. In: *The Theory of Chaotic Attractors*. New York, NY: Springer; 1976. pp. 94-102
- [22] Ibrahim S, Alharbi A. Efficient image encryption scheme using Henon map, dynamic s-boxes and elliptic curve cryptography. *IEEE Access*. 2020;**8**: 194289-194302
- [23] Liu Y, Qin Z, Liao X, Wu J. A chaotic image encryption scheme based on Hénon–Chebyshev modulation map and genetic operations. *International Journal of Bifurcation and Chaos*. 2020;**30**(06): 2050090
- [24] Mishra K, Saharan R. A fast image encryption technique using henon chaotic map. In: *Progress in Advanced Computing and Intelligent Engineering*. Singapore: Springer; 2019. pp. 329-339
- [25] Chai Z, Liang S, Hu G, Zhang L, Wu Y, Cao C. Periodic characteristics of the Josephus ring and its application in image scrambling. *EURASIP Journal on Wireless Communications and Networking*. 2018;**2018**(1):1-11
- [26] Halbeisen L, Hungerbühler N. The Josephus problem. *Journal de Théorie des Nombres de Bordeaux*. 1997;**9**(2): 303-318
- [27] Schumer PD. *Mathematical Journeys*. Hoboken, New Jersey: John Wiley & Sons, Inc.; 2004
- [28] Van Roy P, Haridi S. *Concepts, Techniques, and Models of Computer Programming*. Cambridge, Massachusetts London, England: The MIT Press; 2004
- [29] Hua Z, Xu B, Jin F, Huang H. Image encryption using Josephus problem and filtering diffusion. *IEEE Access*. 2019;**7**: 8660-8674
- [30] Zhang X, Wang L, Wang Y, Niu Y, Li Y. An image encryption algorithm based on hyperchaotic system and variable-step Josephus problem. *International Journal of Optics*. 2020; **2020**:1-15
- [31] Kamal ST, Hosny KM, Elgindy TM, Darwish MM, Fouda MM. A new image encryption algorithm for grey and color medical images. *IEEE Access*. 2021;**9**: 37855-37865
- [32] Ayubi P, Setayeshi S, Rahmani AM. Deterministic chaos game: A new fractal based pseudo-random number generator and its cryptographic application. *Journal of Information Security and Applications*. 2020;**52**:102472
- [33] Iqbal N, Hanif M, Abbas S, Khan MA, Almotiri SH, Al Ghamdi MA. DNA strands level scrambling based color image encryption scheme. *IEEE Access*. 2020;**8**:178167-178182
- [34] Hu X, Wei L, Chen W, Chen Q, Guo Y. Color image encryption algorithm based on dynamic chaos and matrix convolution. *IEEE Access*. 2020; **8**:12452-12466
- [35] Hosny KM, Kamal ST, Darwish MM, Papakostas GA. New image encryption algorithm using hyperchaotic system and fibonacci q-matrix. *Electronics*. 2021; **10**(9):1066
- [36] Murugan B, Nanjappa Gounder AG, Manohar S. A hybrid image encryption

algorithm using chaos and Conway's game-of-life cellular automata. *Security and Communication Networks*. 2016; **9**(7):634-651

[37] Zhang Y. The fast image encryption algorithm based on lifting scheme and chaos. *Information Sciences*. 2020;**520**: 177-194