



Enhancing Image Security using Henon and Tinkerbell Map

Umber Bashir¹, Nasir Siddiqui¹, Saba Inam², Shamsa Kanwal²

¹Department of Mathematical Sciences, University of Engineering and Technology Taxila, Pakistan

²Department of Mathematical Sciences, Fatima Jinnah Women University, The Mall, Rawalpindi

*Email: saba.inam@fjwu.edu.pk

DOI: <https://doi.org/10.55248/gengpi.5.0624.1417>

ABSTRACT

With the latest developments in technology, data security has become a more critical concern. One of the most important tools for protecting data during transmission from unauthorised access is encryption. Encryption protects a wide range of sensitive data against breaches, including financial transactions and email correspondence. This contains data in a range of types, including text, pictures, audio, and video. In this paper, we suggest a new method that incorporates chaotic maps: Henon map and the Tinkerbell map, in particular into the colour RGB picture encryption procedure. Our solution, in contrast to conventional approaches, makes use of the Hill cipher algorithm using a matrix key made up of several colour key codes. Careful consideration goes into choosing these key codes in order to improve security. Using chaotic maps, we produce numerical sequences that fill the Hill key matrix. These sequences are inherently unpredictable, which makes them difficult to interpret. In order to verify the efficacy of our suggested solution, we ran MATLAB simulations. A test picture was successfully encrypted and decrypted using our methods, demonstrating the reliability and effectiveness of our approach in practical settings.

Keywords: Henon map, Tinkerbell map, Histogram, Entropy, Correlation

1. INTRODUCTION

Digital data traffic has been expanding quickly in harmful transmission lines in recent years. For a variety of reasons, including integrity and secrecy, the security of digital data, and particularly digital picture protection, is becoming more crucial [1]. Thus, encryption is the most often used solution to security issues. In the study of dynamic nonlinear systems, chaotic maps are common. Mathematical formulae control its behaviour; even a small shift in the starting point can produce a noticeably different result. Although it may look random and chaotic, it really follows some patterns [2]. In a cryptosystem, chaotic output signals—which have unpredictable statistical characteristics—are employed for the purposes of diffusion and confusion.

Shannon [3] claims that there are two primary categories into which an encryption system's fundamental approaches may be divided: confusion and diffusion. Additionally, it is feasible to combine the two classes. Because chaos and cryptography are closely related, various research based on chaotic systems have been realised in the last few years. The pseudo-randomness, ergodicity, and sensitivity to beginning circumstances of the chaotic system-based approach assure its security [4].

The authors of [5] provide a single chaotic map and bit-level permutation as the foundation for a pure picture permutation technique. In [6], an Arnold cat map and chaotic sequence sorting are used to suggest a two-stage bit-level permutation method. The permutation-only encryption techniques are susceptible to several strong attacks, though. Li et al. suggested in [7] the quantifiable cryptanalysis of a permutation-only cypher against a known or chosen plain-text attack. For the diffusion-only image cypher, Zhu [8] suggested a hyperchaotic sequences-based picture encryption method requiring just two rounds of diffusion operation. But when Li et al. [9] reevaluated [10's security, they found that it may be vulnerable to a single known plain-image compromise.

Mohamed et al. [11] have developed a novel approach for confusion and diffusion that use a skew tenet map. The method involves dividing the plain picture into sectors, each with a size of 1×256 pixels. The MSE and PSNR indicate satisfactory results after encryption. In conclusion, [12] proposed a novel approach to picture encryption in which she creates a new chaotic An acceptable chaos-based picture encryption technique should include two steps, as suggested by Fridrich in [12], the first stage involves using chaotic map(s) to permute the order of the image pixels, and the second stage involves using chaotic map(s) to change the numerical values that represent each pixel's colour.

Many of the current chaos-based picture encryption techniques are built upon these two phases, which are also known as the confusion phase and the diffusion phase [13]. Both Fridrich's chaotic picture encryption system and other image encryption methods with a similar structure, such as Chen et al.'s image encryption algorithm [14], were cryptanalyzed in [12]. There have been other encryption methods proposed that resemble Fridrich's.

In this article, we offer a key generator and a chaotic picture encryption technique. The last phase will employ the 3-D Tinkerbell map, and the resulting key may be used as a starting condition for the 2-D Henon map. In the encryption/decryption process, the suggested method uses m and n given an input

picture of any size, such as $m \times n \times 3$, where the RGB values are represented in the third dimension. efficacy and robustness of the suggested chaotic image encryption for a range of pictures are demonstrated by the experimental results utilising the image database. Finally, security analysis demonstrates that statistically random encrypted pictures may be produced using the suggested approach [15].

The following is the structure of the paper reminder: The evaluation of current encryption systems is covered in brief in Section 2, and the suggested encryption and decryption system architecture is covered in Section 3. The simulation results and security analysis of the encrypted photos are shown in Section 4 and the work is concluded in Section 5.

The nature of the issue, prior research, the paper's goal, and its contribution should all be included in the introduction. Each section's contents may be given for easy comprehension of the document.

Mathematical preliminaries

Our suggested encryption method makes use of the mathematical concepts of the Tinkerbell map, the self-invertible matrix, and the Henon map. Chaotic maps are the fundamental maps whose contents depend on their initial conditions. A minor adjustment to the initial parameters can provide a noteworthy effect on the outcome.

Henon map

As a simpler representation of the Poincare section for the Lorenz model [17], Michel Henon developed the two-dimensional discrete-time dynamical system known as the Henon map [16]. Equation (1) illustrates the meaning of the Henon map equation:

$$x_{p+1} = 1 - \alpha x_p^2 + y_p \quad (1)$$

$$y_{p+1} = b x_p$$

where a , b are two positive control parameters, x , y are state variables, and n is the number of iterations ($n = 0, 1, 2, \dots$). The Henon map, which has been thoroughly examined, revealed the chaotic behaviour at $a = 1.4$ and $b = 0.3$. In a traditional Henon map, the state variables, x and y , are continuous, but the time component is discrete. Henon map orbit diagram with $b = 0.3$. As seen in image 1, more density (darker) denotes a higher likelihood that the variable x will take on that value for the given value of a . The strong attributes of the Henon map were utilised by cryptologists in their cryptographic systems. This map provides homogeneity for the image encryption in the histogram and confusion. This chaotic map has near optimal randomization qualities and is computationally efficient. The Henon map sequence was subjected to pseudo randomness tests, such as the balance, run, and autocorrelation tests. The reported values were extremely near to the theoretical optimum [18].

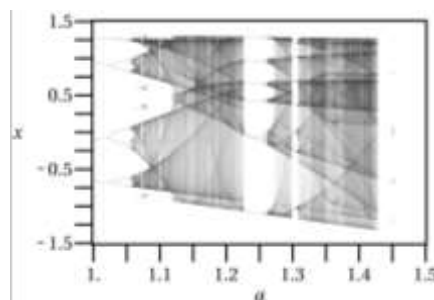


Figure 1: Orbit diagram for the Henon map

Tinkerbell map

Tinkerbell chaotic discrete-time system, which has the following form [22]:

$$q_{n+1} = z(n) 2 - q(n) 2 + \alpha z(n) + \beta q(n) \quad (2)$$

$$r_{n+1} = 2(n)q(n) + \gamma q(n) + \delta q(n) \quad (3)$$

where n is the discrete iteration step and α , β , η , and δ are system parameters. Given that the map's trajectory mimics Tinkerbell's appearance in the Cinderella movie, there is speculation that the map (1) gets its name from the well-known fairy tale. Numerous researchers have examined the Tinkerbell map because of its complex dynamics, which include a variety of periodic stages and chaotic behaviour. For example, the bifurcation of this issue under various starting conditions and circumstances has been examined in [19]. A more thorough investigation was conducted in [20].

Image Encryption Algorithm

The colour picture of varying size encryption technique consists of three steps. The Henon map is used in the initial step of permutation to create a sequence for rearranging picture pixels. A colour key code is used to integrate the permuted pixels with the self-invertible matrix's key. The last stage, called diffusion, is a distinct sequence generated from an XORed Tinkerbell map with previously acquired results. The suggested scheme's resilience to attacker attempts is influenced by its density.

Stage 1. Pixel level permutation

1. Let us first examine the original image I , which is kept in an array of size $M = P \times Q \times 3$, where P denotes the image matrix I 's number of rows and Q its number of columns.
2. Using the Henon map and the key K_1 , create a sequence. To begin, make a chaotic sequence using the Henon map. Then, put the components in ascending order to create the desired order.
3. A permuted sequence is obtained by comparing the locations of the chaotic and sorted sequences.
4. This permuted sequence is then used to rearrange a 1-D array of plaintext in the substitution phase.

Stage 2. Substitution process

1. In the substitution process utilizing the Hill cipher, generate the key matrix using color key codes, subject to mod 256, with an order of 6×6 .
2. Subdivide the 1-D array into column matrices.
3. Transform the 1-D array E into submatrices of size 6×1 . Here, P_j denotes the j th matrix.
4. Utilize the following Hill Cipher formula for key mixing: $M_j = Ld \times P_j \pmod{256}$.
5. Concatenate all M_j 's into a 1-D array.

Stage 3. Diffusion process

1. In the diffusion phase, generate a random real sequence using the chaotic Tinkerbell map.
2. Convert the real sequence into an integer sequence.
3. Perform bitwise XOR operation between the scrambled 1-D image array and the integer sequence, along with the preceding points.
4. Reshape the 1-D diffused image array into a matrix.
5. To obtain the cipher picture OX , transform the resulting matrix as per step (4).

Image Decryption Algorithm

The original image is obtained by using the reverse encryption approach during the colour picture decryption process. The sequence of the Tinkerbell map is first XORed with the key K_3 . The Hill cypher is constructed using K_2 and the self-invertible matrix. After generating a random sequence with the Henon map, the inverse permutation is finished with the key K_1 . To reverse the permutation, use the inverse permutation. The previous array is converted into an image form in order to obtain the original image.

1. An array of size $I = p \times q \times 3$ contains the encoded image matrix.
2. The recipient uses the Tinker Bell map and their private key K_3 to create a sequence G of size I .
3. Each entry of OX from step 2 undergoes the following process: $D_j = OX_j \oplus F D_j \oplus D_{j-1}$, where $j = 1, 2, \dots, I$.
4. The receiver creates a matrix using K_2 , a self-invertible matrix, in accordance with algorithm 2.
5. Transform the 1-D array D into order 6×1 submatrices, which are referred to as W_j .
6. Employ the given formula to reverse key mixing: $O_j = Ld \times W \pmod{256}$, where $j = 1, 2, \dots, I$.
7. Adjust the 1-D array accordingly.
8. Utilizing the shared secret key K_1 , iterate the Henon map to obtain a sequence.
9. Employ the inverse transform position to create the permuted array.
10. Resize V into a matrix of size $I = p \times q \times 3$ and convert it into the image M .

EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

This section contains performance analysis and simulation results for the suggested picture encryption technique. The suggested design has undergone some security study, including crucial ones like statistical analysis, key sensitivity testing, and key space analysis. The outcomes demonstrate the suggested scheme's effectiveness. This section contains the results of several tests that were conducted on binary, grayscale, and RGB pictures. The experiments were performed using a Windows 10 PC equipped with an Intel(R) Core (TM) i7-10510U CPU operating at 1.80 GHz to 2.30 GHz, 32 GB of RAM, and MATLAB R2021a. The experiments (the usc-sipi image database) [21] employed the SC-SIPI 'Miscellaneous' picture dataset, which has 28 example images of unusual sizes, some of which are 256×256 and others which are 512×512 . Several earlier research have used this dataset to evaluate the security of suggested picture encryption techniques. The procedure of our suggested encryption method is shown in Figure 2.








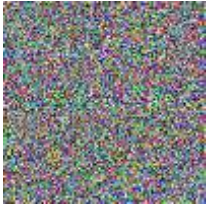






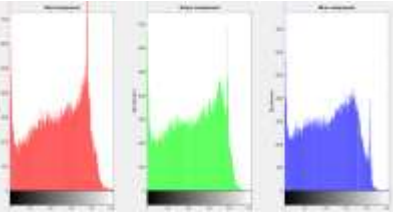
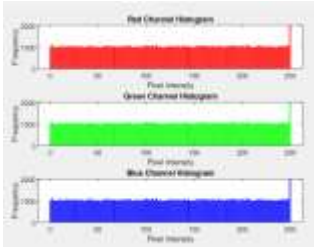


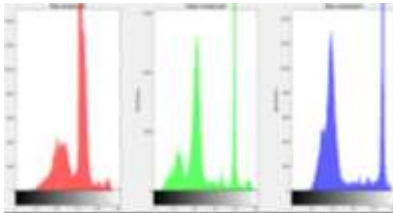
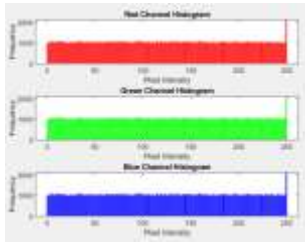
Original	Encrypted	Decrypted
 (a)	 (e)	 (i)
 (b)	 (f)	 (j)
 (c)	 (g)	 (k)
 d(d)	 (h)	 (l)

Figure. 2 Encryption/decryption results: (a-b) original image of size 512×512 . (c-d) original image of size 256×256 . (e-h) encrypted image. (i-l) decrypted image.

Histogram analysis

The frequency distribution of a picture's pixel intensity is shown by a histogram. An encrypted image's histogram should never match the original [22]. The original image's pixels exhibit non-uniform distribution, but the encrypted image's histogram displays uniform distribution. Table 1 illustrates the homogeneous cypher images. Regarding the original image's pixel distribution, there is no proof.

Table 1 Histogram Analysis of plain and encoded images

Sr.no	Original Image	Cipher Image
Img(a)		
Histogram		
Img(b)		
Histogram		

Img (a) represents cipher image histogram analysis of baboon (colored 512 × 512 pixels) and img (b) represent cipher image histogram analysis of girl (colored 256 × 256 pixels).

Entropy

When two chaotic maps are used for picture encryption, the entropy and unpredictability are increased, strengthening the encryption's security. This method makes use of chaotic systems' innate unpredictability and sensitivity to beginning circumstances. Equation (4) provides the calculated value of entropy for the encrypted image *g*.

$$k(g) = -\sum_{i=1} r(ni) \log_2 r(ni) \tag{4}$$

Let each element's probability be represented by *r*(*ni*), so that the sum of these probabilities equals 1. In an 8-bit picture made up of three 8-bit colour planes, a pixel can have *L* = 256 values. Therefore, the optimal Signal-to-Interference-plus-Noise Ratio (SIE) for a flawless cypher image is anticipated to be 8. The results displayed in Table 1 illustrate the efficacy of this tactic and offer comparisons with other methods. All SIE test scores, however, are

more than 7.99, indicating that each encrypted plain image closely resembles the optimal cypher image. Consequently, our system shows resilience to SIE analysis-based attacks, much as its rivals.

Table 2 Entropy values of Cipher Images

Image Encryption Schemes	Entropy Values
Baboon	7.9998
Girl	7.9992
Tree	7.9992
Splash	7.9990

Correlation

Along with the histogram analysis, we also looked at the connection between two neighbouring pixels in the numerous pictures, both their encrypted versions and their vertical and horizontal orientations.

Strong correlations between neighboring pixels in several directions characterize plain pictures. Equation (5) contains the formula that may be used to compute it.

The permutation process is a better way to disrupt this association. As a result, the strong permutation causes the weak association. This methodology suggests a novel permutation strategy based on the perturbed logistic map. Table 3 displays the CC results for the suggested picture method.

$$Cr = \frac{m(\sum_{j=1}^n p_j q_j - \sum_{j=1}^n p_j \sum_{j=1}^n q_j)}{(m \sum_{j=1}^n (p_j)^2 - (\sum_{j=1}^n p_j)^2)(m \sum_{j=1}^n (q_j)^2 - (\sum_{j=1}^n q_j)^2)} \quad (5)$$

where N is the total number of pixels required to calculate the coefficient, and p and q are the values of two neighbouring pixels. When the correlation coefficient is 1, there is a significant degree of connectivity between adjacent pixels. Consequently, we must use our encryption approach, where p and q are the values of two nearby pixels, and y is the total number of pixels required to compute the coefficient. Figures 3 and 4 display the distribution of the original and encrypted image pixels in RGB components.

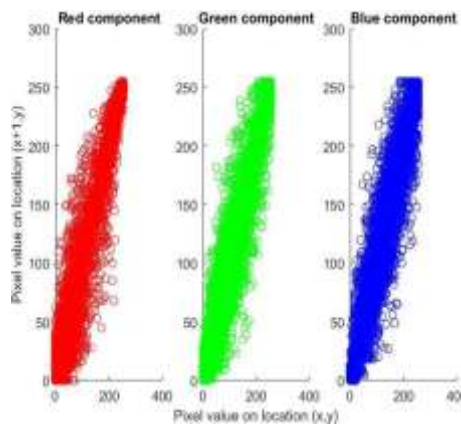


Figure 3. Correlation (row-wise) of the cipher image of baboon 512*512 pixel

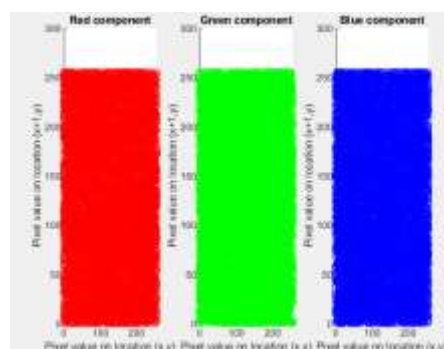


Figure 4. Correlation (row-wise) of the cipher image of baboon 512*512 pixel

Table 3 displays the correlation distribution values in three directions for the original and cypher pictures.

Table 3 The baboon (512 × 512) cipher image's correlation coefficient values.

Directions\Colors	Red	Green	Blue
Horizontal	0.0237	-0.0051	0.0095
Vertical	0.865538	0.0116	0.0093
Diagonal	0.0091	0.0152	-0.0048

Conclusion

This work introduces a chaotic map-based digital picture encryption technique. The algorithm is examined conceptually. The technique can successfully maintain the security of encrypted pictures because it has vast key space, a sensitive key, and uniform pixel distribution after encryption. However, the technique is ineffective in thwarting the selection of a plaintext assault since it uses picture scrambling rather than taking the choice of attack into account. Considering the above-mentioned factors, we provide an image replacement technique based on chaos that can withstand specific plaintext assaults. Results from the experimental simulation are also provided. The outcomes suggest that the technique is extremely sensitive to even the smallest changes in the plaintext and can effectively withstand selection assaults. Additionally, the encrypted picture entirely replaces the original image.

References

- [1] D. Ravi, S. Ramachandran, R. Vignesh, V.R. Falmari, & , M. Brindha " Privacy preserving transparent supply chain management through Hyperledger Fabric." *Blockchain: Research and Applications*, Vol. 3, (2022),100072.
- [2] S. Inam, S. Kanwal, R. Firdous, K. Zakria, F. Hajje "A new method of image encryption using Advanced Encryption Standard (AES) for network security", *Physica Scripta*, Vol. 98, (2023), 126005.
- [3] C.E. Shannon, "Communication theory of secrecy systems." *Bell Syst Tech J*, Vol 28, (1945) pp. 656–715.
- [4] S. Kanwal, S. Inam, O. Cheikhrouhou, K. Mahnoor, A. Zaguia, H. Hamam "Analytic study of a novel color Image Encryption Method Based on the chaos System and color codes." *Complexity*, 2021, 5499538.
- [5] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," *Pattern Recogn. Lett.*, Vol.331, 2010, pp.347-354.
- [6] C. Fu, B. B. Lin, Y. S. Miao, "A novel chaos based bit-level permutation scheme for digital image encryption" *Opt. Commun.*, Vol.284, 2011, pp.5415-5423.
- [7] C. Li, K. T. Lo, "Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal Process.*, Vol.91, 2011, pp.949-954.
- [8] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Opt. Commun.*, Vol.285, 2012, pp.29-37.
- [9] C. Li, Y. Liu, T. Xie, M. Z. Q. Chen, "Breaking a novel image encryption scheme based on improved hyperchaotic sequences," *Nonlinear Dyn.*, Vol.73, 2013, pp.2083-2089.
- [10] Z. L. Zhu, W. Zhang, K. W. Wong, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Inform. Sciences*, Vol.181, 2011, pp.1171-1186.
- [11] M. Mahmoud, Maqableh "secure hash functions based on chaotic mapsfor e-commerce applications" *International Journal of Information Technology & Management Information System*, Vol.1, (2010), pp. 12-22
- [12] Fridrich Jiri "Symmetric ciphers based on two dimensional chaotic maps," *Int. J. Bifurcat Chaos*, Vol. 8, (1998), pp. 1259–1284.
- [13] K.A.K. Patro, B. Acharya, "An efficient dual-layer cross-coupled chaotic map security-based multi-image encryption system." *Nonlinear Dyn*, Vol. 104, 2021, pp. 2759–2805
- [14] G. Chen, Y. Mao, C.K. Chui, "A symmetric image encryption based on 3D chaotic maps." *Chaos Solitons Fractals*, Vol. 21, 2004,pp. 749–761.
- [15] A.K. Mandal, C. Parakash, A. Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES." In *Proceedings of the IEEE Students' Conference on Electrical, Electronics and Computer Science, Bhopal, India*, Vol. 2, 2012, pp. 1–5.
- [16] J. Khan, J. Ahmad, and S. O. Hwang, "An efficient image encryption scheme based on: Henon map, skew tent map and S-Box," in *Proc. 6th Int. Conf. Modeling, Simulation, Appl. Optima. (ICMSAO)*, 2015, pp. 1–6.
- [17] B. W. Shen, "A Review of Lorenz's Models from 1960 to 2008." *International Journal of Bifurcation and Chaos*, Vol. 33, (2023), 2330024.
- [18] B. Song and Q. Ding, "Comparisons of typical discrete logistic map and henon map," in *Intelligent Data analysis and its applications*, vol. 1, 2014, pp. 267–275.

-
- [19] T A. Dhivakar, S K. Nayak, S. Roy "A novel image encryption technique using Tinkerbell map and Duffing map for IoT applications." *Multimedia Tool and Applications*, Vol. 81, (2022), pp. 43189-43228
- [20] B. Zhang, L. Liu "Chaos-Based Image Encryption: Review, Application, and Challenges", *Mathematics*, Vol.11, (2023), pp.25-85.
- [21] Usc-Sipi Image Database for Research in Image Processing, Image Analysis, and Machine Vision. Available online: <http://sipi.usc.edu/database/> (accessed on 19 September 2017).
- [22] S. Kanwal, S. Inam, M. T. B. Waqar, M. Ibrahim, F. Nawaz, H. Hamam, "An Effective Color Image Encryption Based on Henon Map, Tent Chaotic Map, and Orthogonal Matrices." *Sensors*, Vol. 22, (2022),4359