International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Image Encryption Model based on Chaotic Henon Map and Termite Alate Optimization Algorithm

Naveen Kumar*[1], Satish Saini[2]

Submitted: 30/12/2023 **Revised**: 06/02/2024 **Accepted**: 14/02/2024

Abstract: In the present era, data communication in the form of multimedia images is increasing on the internet. To secure it, an image encryption model is designed in this paper. To accomplish this goal, multimedia images are encrypted using random keys. The random keys are generated using the chaotic Henon map algorithm.It is a two-dimensional signal. Hence, 2-D key generation is possible from it. The chaotic henon map is sensitive to input parameters, and the determination of its optimal value generates a completely random key. However, it is a complex process to search the values in the lower and upper bounds of the parameter value. To accomplish this goal, metaheuristic algorithms are used in the literature. Metaheuristics is a field of optimization. Thus, these algorithms, based on a given problem, find the optimal solution. In this paper, we have used a recent termite alate optimization algorithm based on the photoactivity of the termites that is characterized according to the requirements in the proposed model. After key generation, exclusive-OR and permutation steps are performed for final encryption. The simulation evaluation of the proposed model is based on the different gray-scale images. Further, subjective, and objective parameters are determined for it. The result shows that the proposed model achieves high entropy near 8 values, a low correlation coefficient near 0 values, and a low PSNR.

Keywords: *Chaotic Map, Encryption, Henon Map, Metaheuristic, Security, TAO.*

1. Introduction

In the present time, the Internet of Things (IoT) is the most popular network for communicating information between IoT devices. Moreover, the data is communicated in the form of multimedia data. Further, as computing power and storage capacity increase, more and more multimedia content is being created and shared online [1]. Digital images are one kind of multimedia data that may convey data in a visually appealing style. Many of the digital images that are being sent over networks are confidential. Images of a person's medical history, for instance, are often kept confidential since they reveal sensitive information about the patient's health. Serious security emergencies may occur if these confidential images are accessed in an unauthorized manner [2-4]. To safeguard these images, image encryption is the useful tool [5-8].

Using existing data encryption techniques to encrypt a binary data stream is one method of image encryption. The popular DES [9] and the AES [10] are two examples of such methods. On the other hand, unlike other types of data, data from pictures has some interesting characteristics of its own [11, 12]. These details will be lost if an image is processed as a binary stream, which might lead to ineffective encryption. To secure images, chaos theory [13-16], quantum theory, DNA encoding, compressive sensing, and certain mathematical models have been presented in the literature [17-24]. The most widely used of these tools is chaos theory. This is because the fundamentals of image encryption are very similar to those of chaotic behavior [25–27]. Encryption has several characteristics in chaos theory, including ergodicity and sensitivity to beginning conditions [28]. Here are some examples of encryption algorithms that rely on chaos. In the literature, chaotic logistic maps, tent maps, henon maps, and sine maps are successfully deployed for key generation in image encryption methods [29–32]. Further, to enhance the security, metaheuristic algorithms are hybrid with chaotic map [33-35]. In mathematics, optimization is the study of finding the best possible solution to a problem by minimizing or maximizing a fitness function according to certain restrictions. From product development to rocket launches, optimization has become more prevalent in the real world. Meta-heuristics are perhaps the most important tool in the optimization field. Meta-heuristics are used for optimization for the most part because they may be applicable to real-world issues despite their great complexity and nonlinearity. These methods also have the additional benefit of providing a somewhat excellent answer in a fair amount of time.

The main contribution of this paper is to secure images on the internet using the encryption method. In the encryption method, a random key is generated using the

[1]*Department of Electronics and Communication Engineering, RIMT University, Mandi Gobindgarh, Punjab*
ORCID ID : https://orcid.org/0009-0002-6459-8868.
[2]*Department of Electronics and Communication Engineering, RIMT University, Mandi Gobindgarh, Punjab*
ORCID ID : https://orcid.org/0000-0002-9194-3068
** Corresponding Author Email: goyal.naveen2020@gmail.com*

chaotic Henon map. The chaotic henon map algorithm generates a completely random key if its parameter values are appropriately determined. To accomplish this goal, we have deployed the termite alate optimization algorithm [36]. This algorithm determines the parameter values based on the objective function. Further, simulation evaluation is performed on different images, and various performance parameters are determined. The encrypted images are noisy, the histogram is equally distributed, and a high value of entropy, and a low value of PSNR, SSIM, and CC are achieved.

The paper is organized into five sections. Section 2 shows the related work. This section explains the algorithms taken into consideration for the proposed image encryption model. Section 3 explains the proposed image encryption model, in which the complete procedures of data collection, key generation, encryption, and performance metrics are used for evaluation purposes. Section 4 shows the simulation evaluation, in which simulation software, system and proposed model setup configuration, simulation results, and comparative analysis is shown. Finally, the proposed image encryption model is concluded in Section 5. Further, in this section, future work is defined to enhance the presented model in this paper.

2. Related Work

This section explains the chaotic henon map and metaheuristic TAO algorithm to understand the proposed model.

2.1 Chaotic Henon Map

In the image encryption method, the chaotic map gains popularity over the other encryption methods because it provides better confusion and diffusion and is used for key generation purposes. Further, the output response of chaotic map algorithms is highly sensitive to the input conditions of the input parameter. Therefore, in the literature, the parameter values are determined carefully for better encryption. Further, in the literature, numerous types of chaotic maps, such as logistic maps, henon maps, tent maps, logistic sine maps, etc., are deployed for image encryption [28]. In this work, we have taken the Henon map algorithm into consideration. The detailed description is given below.

Chaotic Henon map algorithm is highly sensitive to input parameters. Thus, when the optimal value of these parameter is given to it, it exhibits good chaotic features. The chaotic henon map is determined using Eq. (1).

$$X_{n+1} = 1 - \alpha(X_n^2) + Y_n$$
$$Y_n = \beta X_n \quad (1)$$

where α, β are the control parameters. The α β value varies in between [1.3-1.5] and [0.25-0.35], respectively. In the proposed encryption model, the α β optimal value is determined using the termite alate optimization algorithm based on the objective function.

2.2 Termite Alate Optimization Algorithm

In the present time, artificial intelligence gains popularity in different fields [37-39]. In this work, we have worked on the sub-field of it known as metaheuristic algorithm for determine the optimal parameter value of Henon map algorithm. In this work, a novel swarm-based approach called the Termite Alate Optimisation approach (TAOA) is considered in this paper. The algorithm is built by mimicking the behaviour of a colony of termite alates exposed to different intensities of light. The algorithm's strengths are as follows:

(i) it converges more quickly,
(ii) its exploration and exploitation approach is effective, and
(iii) its computing complexity and number of algorithm-specific parameters are both manageable. Subsequently, the method is put through its paces by being applied to 30 benchmark examples, 5 real-world situations, and permutation flow shop scheduling challenges. Results from TAOA are compared to those from other algorithms to ensure their efficacy.

2.2.1 Background

Termites, a widespread kind of insect, are important in decomposing wood. They have a strong need for community and like to reside in groups known as colonies. There are male termites, a queen termite, workers, soldiers, and reproductive termites in each of these colonies. Reproduction is the primary purpose of both the male and female termites. The soldiers defend the colony from any potential attackers. It was the worker termite's job to bring in food and help the colony grow. When the reproductive reach adulthood and gain flight, they disperse from the present colony to start a new one somewhere. The reproductive life cycle has six stages: “egg”, “larva”, “nymph”, “alate”, “de-alate”, and “king or queen” [17]. In the alate stage, the females and males develop wings and depart the nest. As many as a thousand young ones may emerge from a nest all at once. In most cases, an alate's battle will last little more than a few minutes until it gives up and stops trying to defend itself. Later, the wingless alate starts looking for the opposite sex in order to mate. Most species' alate swarming occurs at night. These alates are drawn to light and endeavour to find a brighter environment [18]. But many of the alates never make it to the better realm because they are eaten by birds or lose their wings too soon.

2.2.2 Termite Alate Optimization Algorithm

This research offers an optimisation method called the Termite Alate Optimisation method (TAOA), which is based on the phototactic behavior of the termite alate group. The foundation of this suggested algorithm is based on two rules [36]:

- When it comes to termites, the alate in the brightest position attracts them, while the alate in the darkest position repels them.
- The remaining population of termite alates looking for the best light source remains constant. The alates in the shadows are either eaten by birds or suffer wing damage on the way to the sun. Thus, new alates are constantly being swapped into more illuminated locations to replace the old ones.

Above two rules, helps the TAO algorithm to search the space and provides better convergence speed by overcoming the local optima problem by preventing the termite alates to stuck in the dark position.

3. Material and Method

In this section, we have designed an image encryption method using a hybrid chaotic henon map and metaheuristic termite alate optimization algorithm. The chaotic henon map algorithm generates a completely random key based on its optimal parameter values. The optimal parameter values for it are determined using the TAO algorithm. The benefit of the proposed method is that a random key is determined for different images because the TAO algorithm determines the optimal parameter value based on the secret image characteristics. The flowchart of the proposed method is shown in Figure 1.

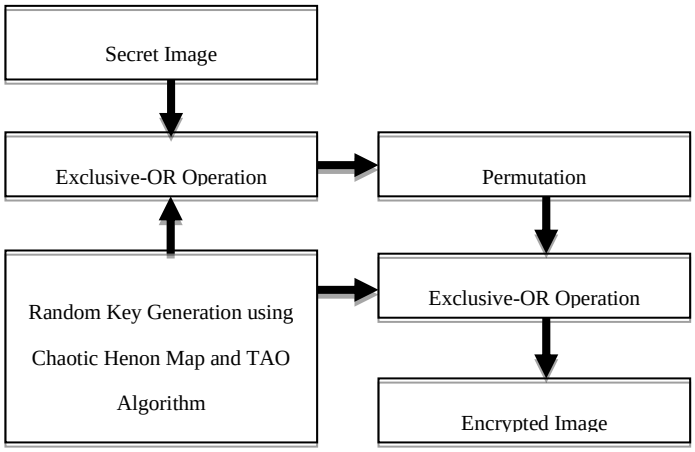


Fig.1 Flowchart of the Proposed Image Encryption Model

3.1 Secret Image

In this work, we have taken the different standard dataset images for the proposed method. In the literature, numerous dataset images are available. Out of these, the USC-SIPI image database is the most preferred. In this work, gray-scale images are used for image encryption. Further, image resolution 256×256 is taken into consideration.

3.1 Key Generation using Hybrid Combination of Chaotic Henon Map and TAO Algorithm

In the proposed model, a chaotic henon map algorithm is used for key generation. Therefore, optimal parameter values for it are determined using the metaheuristic termite alate optimization algorithm. This algorithm determines the value based on the objective function. In this work, the entropy parameter is taken into consideration while designing the objective function.

3.3 Image Encryption

In the encryption process, two keys are generated using the chaotic henon map algorithm. Initially, exclusive-OR operation performed pixel-wise between secret image and first key. After that, permutation is performed by circular shifting the secret image matrix. Finally, to achieve the final encrypted image, an exclusive-OR operation is performed with the second key.

3.4 Performance Metrics

The proposed model is evaluated using subjective and objective performance metrics. The visual quality of the input and encrypted image and their histogram is measured in the subjective, whereas in the objective analysis, various security performance metrics such as MSE, PSNR, structural similarity index measure, correlation coefficient (CC), and entropy are determined. A detailed description of these metrics is given below [40–41].

- Mean Square Error: It compares the pixel values of two images and provides an average of the differences. It is mathematically expressed using Eq. (2).

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(S_{ij}-E_{ij})^2}{MN} \quad (2)$$

  In Eq. (2), MN denotes the resolution of the confidential image. On the other hand, SE denotes the secret and encrypted image.
- Peak Signal to Noise Ratio (PSNR): This statistic compares the plain and cipher images in terms of the noise ratio. The PSNR between the plaintext image and the cipher picture may be expressed mathematically as follows:

$$PSNR = 20\log_{10}\frac{Max}{MSE} \quad (3)$$

  In eq. (3), Max denotes the maximum possible value in the grey scale image.
- Structural Similarity Index Measure (SSIM): This parameter measures the similarity between secret and encrypted image. The high value of it represents the strong interdependencies between

both images. In the encryption process, a low value of SSIM is required and it is determined using Eq. (4).

$$SSIM(SE) = \frac{(2\mu_S\mu_E+C_1)(2\sigma_{SE}+C_2)}{(\mu_S{}^2+\mu_E{}^2+C_1)(\sigma_S^2+\sigma_E^2+C_2)} \quad (4)$$

In Eq. (4), $\mu_S\mu_E$ denotes the average value of secret and encrypted image, σ_{SE} denotes covariance.

- Correlation Coefficient Analysis (CCA): Similar pixels in the original and encrypted images may be matched up using CCA. The pixels in the source image are closely linked in the horizontal, vertical, and diagonal axes. However, the encrypted image's neighboring pixels must be completely unrelated to one another. Increased susceptibility to statistical assault is associated with the increased correlation between neighboring pixels. Therefore, efficient encryption methods have a tendency to reduce the coefficient value. It is mathematically expressed using Eq. (5).

$$r_{SE} = \frac{C(S,E)}{\sqrt{D(S)}\sqrt{D(E)}} \quad (5)$$

The covariance between two samples, denoted as C(S,E), is the product of their coordinates, S, and E. $D(S)$ ad $D(E)$ denotes the standard deviation.

- Entropy (E): Average information per bit in an image is represented by E, making it a measure of how unpredictable the image is. A suitable encryption method has an information entropy range of [0, 8]. The formula for calculating entropy of information is:

$$H(S) = -\sum P(S_i) \times \log_2 P(S_i) \quad (6)$$

4. Result and Discussion

The proposed model evaluated in MATLAB 2018a. The simulation evaluation for 10 images are presented in this paper.

4.1 Setup Configuration of the Proposed Image Encryption Model

Table 1 and 2 shows the system configuration and simulation setup configuration of the proposed image encryption model.

Table 1. System Configuration for the Proposed Model

System Parameter	Values
Processor	Intel Core i7 Processor
RAM	16GB
Operating System	64-bit
Hard Disc	1TB

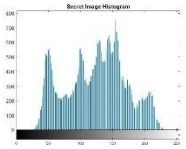
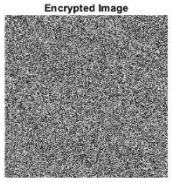
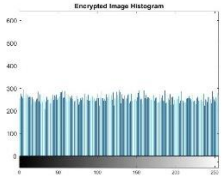
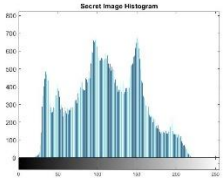
Table 2. Simulation Setup Configuration for the Proposed Model

Parameter	Values
α	[1.3-1.5]
β	[0.25-0.35]
Population	30
Iterations	50
Objective Function	Entropy

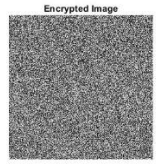
4.2 Subjective Analysis

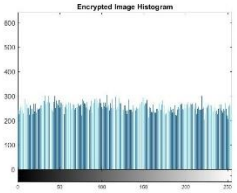
Table 3 shows the visual quality of the input and encrypted image, along with their histogram. In the encryption method, the encrypted image should be noisy, and histograms of it that are equally distributed show the best security. To accomplish this goal, we have simulated the proposed model for different images. The result shows that the encrypted image is completely noisy, and it is difficult to distinguish the secret image from it. On the other hand, the encrypted histogram is equally distributed over the input histogram of any distribution.

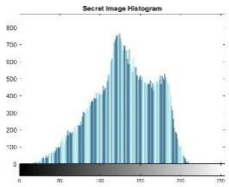
Table 3. Subjective Analysis of the Input and Encrypted Image

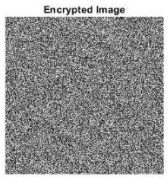
	Image	Histogram
Lena		
		
Barbara		

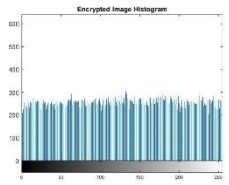
Baboon



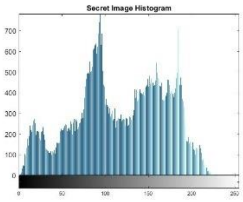


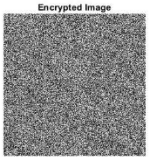


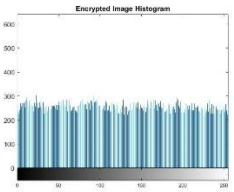




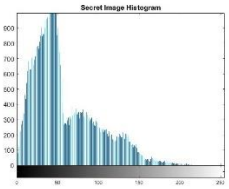
Pepper

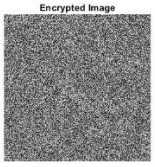


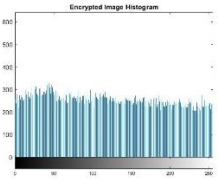




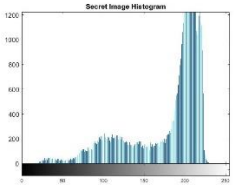
Female



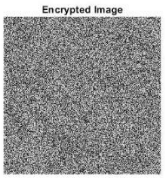


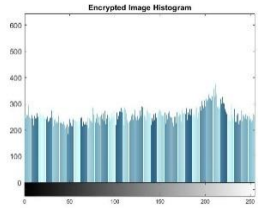


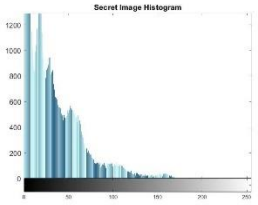
Aeroplane

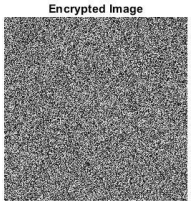


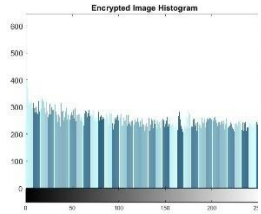
Couple



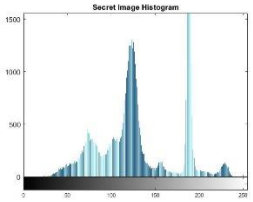


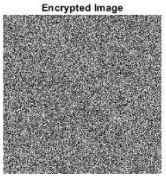


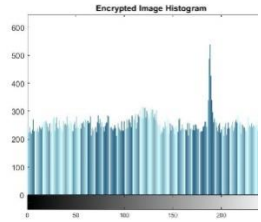




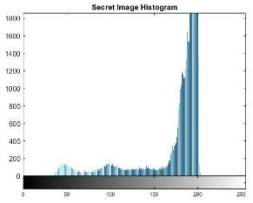
House

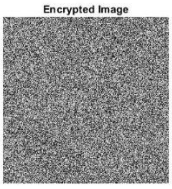


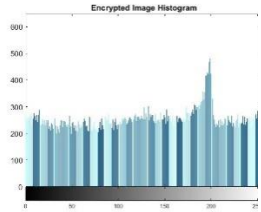




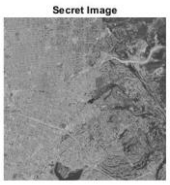
Jellybeans

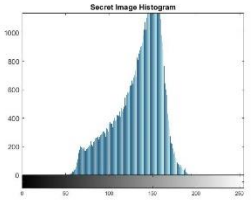


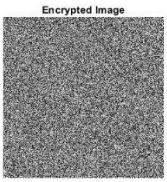


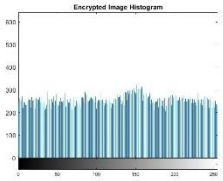


Oakland









4.3 Objective Analysis

Table 4 shows the various performance metrics (MSE, PSNR, CC, SSIM, and Entropy) are determined in the objective analysis for the proposed model.

Table 4. Performance Metrics for the Objective Analysis

Images	MSE	PSNR	CC	SSIM	Entropy
Lena	3.6110e+03	12.5546	0.0014	0.0106	7.9973
Barbara	2.7007e+03	13.8161	8.1743e-04	0.0107	7.9961
Baboon	3.5114e+03	12.6760	0.0012	0.0126	7.9971
Pepper	3.4205e+03	12.7899	-0.0041	0.0099	7.9968
Female	775.6935	19.2339	0.0033	0.0072	7.9933
Aeroplane	8.4141e+03	8.8808	0.0047	0.0096	7.9918
Couple	282.8954	23.6145	1.1460e-04	0.0055	7.9917
House	4.5073e+03	11.5916	-0.0059	0.0111	7.9892
Jellybeans	7.5914e+03	9.3276	-0.0096	0.0101	7.9849
Oakland	3.3409e+03	12.8921	0.0062	0.0130	7.9950

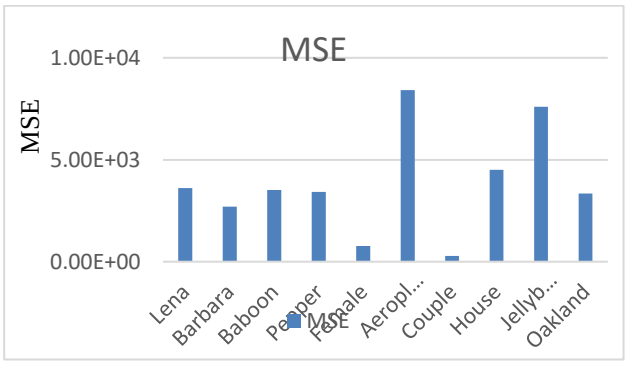


Fig 2. MSE for Different Images

Figure 2 shows the MSE analysis for different images. The MSE value for different images varies from 282.8954 to 8.4141e+03. The result shows that aeroplane image achieves the highest MSE over the other. This reflects that there is maximum error between secret and encrypted image.

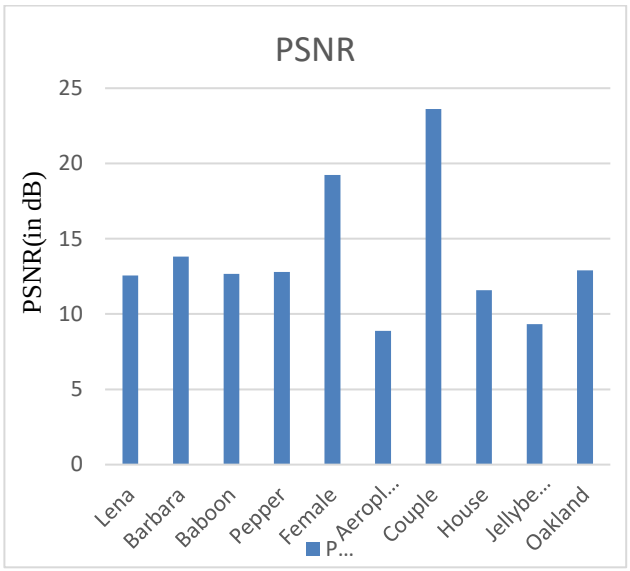


Fig. 3. PSNR for Different Images

Figure 3 shows the PSNR analysis for different images. The PSNR value for different images varies from 8.8808 to 23.6145dB. The result shows that aeroplane image achieves the lowest PSNR over the other.

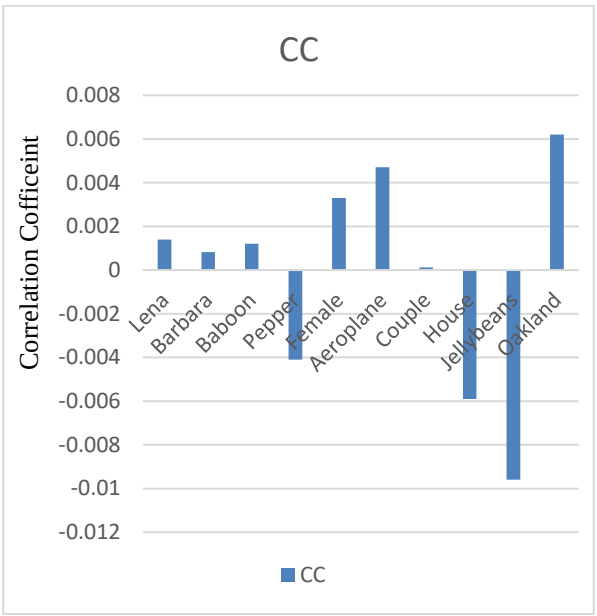


Fig 4. Correlation Coefficient Analysis for Different Images

Figure 4 shows the correlation coefficient analysis for different images. The result shows that correlation varies from -0.0059 to 0.006. This reflects that there is minimum correlation between secret and encrypted image.

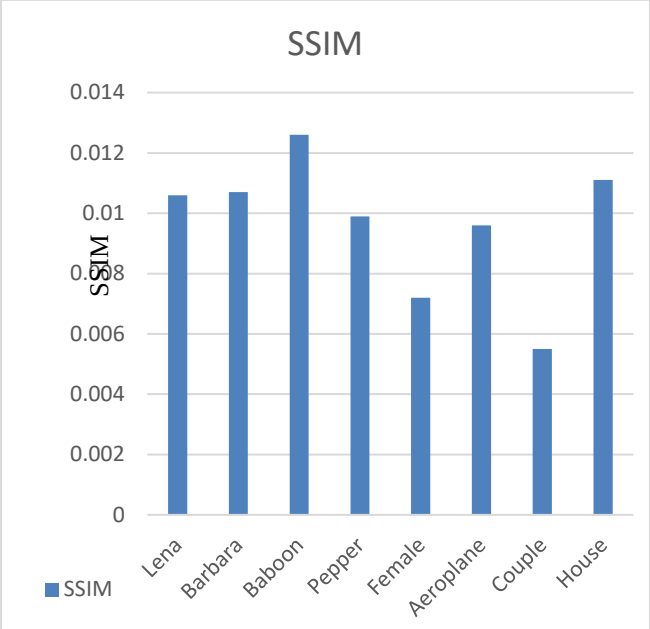


Fig 5. SSIM Analysis for Different Images

Figure 5 shows the structural similarity index measure analysis for different images. The result shows that SSIM varies from 0.0055 to 0.0126. This reflects that there is minimum SSIM between secret and encrypted image.

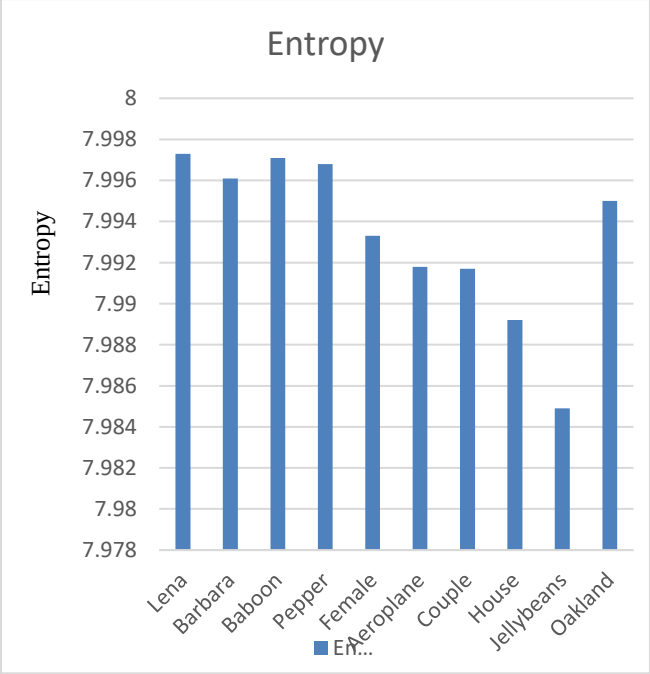


Fig 6. Output Entropy Analysis for Different Images

Figure 6 shows the output entropy analysis for different images. The result shows that entropy varies from 7.9849 to 7.9973. This reflects that output entropy near to ideal value.

5. Conclusion and Future Work

In this work, we have designed an encryption model using the chaotic henon map and termite alate optimization algorithm. These algorithms are in the proposed model generates a completely random key. After that, to accomplish final encryption, exclusive-OR and permutation steps are performed. The simulation evaluation shows that the proposed model achieves low PSNR, correlation and high value of entropy parameter. In the future, we will design multi-objective function for the presented image encryption model. Further, we will explore the other chaotic map and metaheuristic algorithms.

Conflict of Interest

All authors declare that they have no conflict of interest.

References

[1] John, S. and Kumar, S.N., 2023. IoT based medical image encryption using linear feedback shift register–Towards ensuring security for teleradiology applications. *Measurement: Sensors*, *25*, p.100676.

[2] X.-W. Li, I.-K. Lee, Robust copyright protection using multiple ownership watermarks, Optics Express 23 (3) (2015) 3035–3046.

[3] L. Y. Zhang, Y. Liu, F. Pareschi, Y. Zhang, K.-W. Wong, R. Rovatti, G. Setti, On the security of a class of diffusion mechanisms for image encryption, IEEE Transactions on Cybernetics, DOI: 10.1109/TCYB.2017.2682561.

[4] X. Wang, Q. Wang, Y. Zhang, A fast image algorithm based on rows and columns switch, Nonlinear Dynamics 79 (2) (2015) 1141–1149.

[5] W. Liu, K. Sun, C. Zhu, A fast image encryption algorithm based on chaotic map, Optics and Lasers in Engineering 84 (2016) 26–36.

[6] G. Ye, X. Huang, L. Y. Zhang, Z.-X. Wang, A self-cited pixel summation based image encryption algorithm, Chinese Physics B 26 (1) (2017) Article ID. 010501.

[7] X. Li, D. Xiao, Q.-H. Wang, Error-free holographic frames encryption with ca pixel-permutation encoding algorithm, Optics and Lasers in Engineering 100 (2018) 200–207.

[8] Z. Hua, S. Yi, Y. Zhou, Medical image encryption using high-speed scrambling and pixel adaptive diffusion, Signal Processing 144 (2018) 134–144.

[9] FIPS PUB 46, Data encryption standard (DES) (1999).

[10] Subashini, A. and Raju, P.K., 2023. Hybrid AES model with elliptic curve and ID based key generation for IOT in telemedicine. *Measurement: Sensors*, p.100824.

[11] Y. Zhang, D. Xiao, An image encryption scheme based on rotation matrix bit-level permutation and block diffusion, Communications in Nonlinear Science and Numerical Simulation 19 (1) (2014) 74–82.

[12] Y. Zhang, D. Xiao, Y. Shu, J. Li, A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations, Signal Processing: Image Communication 28 (3) (2013) 292–300.

[13] C. Fu, J. Chen, H. Zou, W. Meng, Y. Zhan, Y. Yu, A chaos-based digital image encryption scheme with an improved diffusion strategy, Optics 385 Express 20 (3) (2012) 2363–2378.

[14] G. Ye, X. Huang, Spatial image encryption algorithm based on chaotic map and pixel frequency, Science China-Information SciencesDOI: 10.1007/s11432-017-9191-x, to be published.

[15] Y.-Q. Zhang, X.-Y. Wang, A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice, Information Sciences 273 (2014) 329–351.

[16] Y.-Q. Zhang, X.-Y. Wang, A new image encryption algorithm based on non-adjacent coupled map lattices, Applied Soft Computing 26 (2015) 10–20.

[17] R. Enayatifar, H. J. Sadaei, A. H. Abdullah, M. Lee, I. F. Isnin, A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata, Optics and Lasers in Engineering 71 (2015) 33–41.

[18] J. Chen, Z.-L. Zhu, L.-B. Zhang, Y. Zhang, B.-Q. Yang, Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure 395 and efficient image encryption, Signal Processing 142 (2018) 340–353.

[19] D. Jiang, Y. Chen, X. Gu, L. Xie, L. Chen, Efficient and universal quantum key distribution based on chaos and middleware, International Journal of Modern Physics B 31 (2) (2017) 1650264.

[20] N. Zhou, Y. Hu, L. Gong, G. Li, Quantum image encryption scheme with iterative generalized Arnold transforms and quantum image cycle shift operations, Quantum Information Processing 16 (6) (2017) 164.

[21] Zhou, N., Pan, S., Cheng, S. and Zhou, Z., 2016. Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing. *Optics & Laser Technology*, *82*, pp.121-133.

[22] Chai, X., Gan, Z., Chen, Y. and Zhang, Y., 2017. A visually secure image encryption scheme based on compressive sensing. *Signal Processing*, *134*, pp.35-51.

[23] Zhou, Y., Panetta, K., Agaian, S. and Chen, C.P., 2012. Image encryption using P-Fibonacci transform and decomposition. *Optics Communications*, *285*(5), pp.594-608.

[24] Hua, Z. and Zhou, Y., 2017. Design of image cipher using block-based scrambling and image filtering. *Information sciences*, *396*, pp.97-113.

[25] Zhang, B. and Liu, L., 2023. Chaos-Based Image Encryption: Review, Application, and Challenges. *Mathematics*, *11*(11), p.2585.

[26] Özkaynak, F., 2018. Brief review on application of nonlinear dynamics in image encryption. *Nonlinear Dynamics*, *92*(2), pp.305-313.

[27] Sharma, B. and Singh, J., 2022. Chaos Based Image Encryption Techniques: A Review. *International Research Journal of Engineering and Technology*.

[28] Kari, A.P., Navin, A.H., Bidgoli, A.M. and Mirnia, M., 2022. Image cryptosystem based on plain image correlation rate and selective chaotic maps. *Multimedia Tools and Applications*, *81*(15), pp.20483-20508.

[29] Pourjabbar Kari, A., Habibizad Navin, A., Bidgoli, A.M. and Mirnia, M., 2021. A new image encryption scheme based on hybrid chaotic maps. *Multimedia Tools and Applications*, *80*, pp.2753-2772.

[30] Wang, X. and Chen, S., 2023. An image encryption algorithm based on pixel bit operation and nonlinear chaotic system. *The Visual Computer*, *39*(7), pp.3123-3144.

[31] Kumar, N. and Jain, S., A Review of Performance Comparison on Chaos Based Image Encryption Technique.

[32] Kanwal, S., Inam, S., Othman, M.T.B., Waqar, A., Ibrahim, M., Nawaz, F., Nawaz, Z. and Hamam, H., 2022. An effective color image encryption based on Henon map, tent chaotic map, and orthogonal matrices. *Sensors*, *22*(12), p.4359.

[33] Rezaei, B., Ghanbari, H. and Enayatifar, R., 2023. An image encryption approach using tuned Henon chaotic map and evolutionary algorithm. *Nonlinear Dynamics*, *111*(10), pp.9629-9647.

[34] Wang, J., Song, X. and El-Latif, A.A.A., 2022. Single-objective particle swarm optimization-based chaotic image encryption scheme. *Electronics*, *11*(16), p.2628.

[35] Kumar, A., 2022. Improved Chaotic Logistic Map Algorithm based on Bio-Inspired Algorithm for Image Encryption. *Tobacco Regulatory Science (TRS)*, pp.1915-1928.

[36] Majumder, A., 2023. Termite alate optimization algorithm: a swarm-based nature inspired algorithm for optimization problems. *Evolutionary Intelligence*, *16*(3), pp.997-1017.

[37] Kaur, G., Saini, S. and Sehgal, A., 2022. Introduction to Artificial Intelligence. In *Artificial Intelligence* (pp. 1-20). Chapman and Hall/CRC.

[38] Kaur, G., Saini, S. and Sehgal, A., 2022. Machine Learning–Principles and Algorithms. In *Artificial Intelligence* (pp. 21-54). Chapman and Hall/CRC.

[39] Kaur, G., Saini, S. and Sehgal, A., 2022. Applications of Machine Learning and Deep Learning. In *Artificial Intelligence* (pp. 55-70). Chapman and Hall/CRC.

[40] Alghamdi, Y., Munir, A. and Ahmad, J., 2022. A lightweight image encryption algorithm based on chaotic map and random substitution. *Entropy*, *24*(10), p.1344.

[41] Zia, U., McCartney, M., Scotney, B., Martinez, J., AbuTair, M., Memon, J. and Sajjad, A., 2022. Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. *International Journal of Information Security*, *21*(4), pp.917-935.