Optimized Image Encryption Model based on Hybridization of Chaotic Maps with Metaheuristic OOBO Algorithm

[1]Abhinaya Srivastava* and [2]Shano Solanki
[1,2]Department of Computer Science and Engineering, National Institute of Technical Teachers Training and Research Sector-26, Chandigarh, India
[1]abhi.askcha@gmail.com, [2]shano@nitttrchd.ac.in

Abstract: Chaotic maps have gained popularity in image encryption models due to their ability to secure images with a random key. Further, the randomness of the key is highly dependent on the initial parameter values of the chaotic map. Therefore, the literature employs metaheuristic algorithms to find the optimal parameter values for generating a completely random key. Two chaotic maps—the 1-D chaotic logistic map (CLM) and the chaotic tent map (CTM)—along with the metaheuristic algorithm known as one-to-one-based optimization (OOBO) were used to create an optimized image encryption (IE) model in this study. We utilize the 1-D CLM algorithm for random key generation, while the 1-D CTM algorithm generates the shuffling sequence for image shuffling. We use the metaheuristic OOBO algorithm in both chaotic maps to generate completely random keys and random shuffling sequences based on the objective function. In this research, we design the objective function using security parameters such as entropy (E) and correlation coefficient (CC). After determining the optimal parameter values for chaotic maps, we perform an exclusive-OR operation between the random key and the secret image. After that, shuffling of the secret image is done based on the shuffling sequence given by the 1-D CTM algorithm. We evaluate the proposed IE model through simulation using images from the primary and secondary datasets. Using various parameters, we compare the visual quality of the encrypted image with the secret image in this evaluation. The results illustrate that the proposed IE model outperforms in terms of entropy and correlation coefficients and provides better encryption than the existing IE models. The proposed model achieves an entropy of 7.99648 for the cameraman, 7.99688 for Elaine, and 7.99704 for the pepper image. Further, a correlation coefficient of 0.00021 for the cameraman, -0.00012 for Elaine, and -0.00161 for the pepper image.

Keywords: Chaotic Map, Encryption, Logistic Map, Metaheuristic, Objective Function, OOBO, Security, Tent Map

1. Introduction

In the present scenario, there is a substantial growth in the internet and modern communication, which increases the significant data communication on it [1]. In the literature, data communication is done in various forms, whereas images have gained popularity in social, defense, and healthcare applications [2]. Further, images are prone to various attacks, such as statistical, differential, brute force, and noise attacks on the communication channel [3]. Thus, images are secured before communicating from the transmitter. In the literature, encryption, steganography, and watermarking are the popular security approaches [4]. In this research, a security approach based on encryption is explored. This approach scrambles the image using a private key so it looks like a noisy image, and it is difficult for the attacker to intercept the original information. In the literature, AES and chaotic maps are some population image encryption algorithms [5-7]. The AES provides better security but has a high time complexity because it processes the image into the form of blocks and is prone to differential attack [5]. On the other hand, a chaotic map quickly encrypts the images when compared to the AES algorithm and withstands various attacks that are feasible on the image [8]. Further, the security of the chaotic map algorithm is sensitive to the input parameters. Thus, fine-tuning of the parameters is done using the metaheuristic algorithms [9]. These algorithms come under the category of optimization, and their motive is to maximize/minimize the solution according to the given problem [10]. Further, these algorithms are categorized into various classes based on their source of inspiration to find the solution. These classes are evolutionary, swarm, physical, and chemical. In the literature, several metaheuristic algorithms are available and differentiated on how it searches the optimal solution, how many parameters need to initialize for search the solution and providing single/multiple solution in the output [11]. Therefore, the main motive of this research is to choose the most optimal metaheuristic algorithm to fine tune the chaotic maps are considered in this research to optimized IE model. The main contribution of this research is summarized below.

N. Vyas et al. (eds.), *Proceedings of the International Conference on Advancements in Computing Technologies and Artificial Intelligence (COMPUTATIA 2025)*, Advances in Intelligent Systems Research 189,
https://doi.org/10.2991/978-94-6463-700-7_10

- This paper presents an optimized IE model by hybrid the two chaotic maps. Followed by, fine tuning of the chaotic maps using the metaheuristic algorithm.
- In this research, we have developed an objective function by considering the multiple security parameters.
- In this research, we have employed the most optimal metaheuristic algorithm which required minimum parameter tuning and provides better convergence rate to find the best solution for the IE model.
- The evaluation of the proposed IE model shows that the proposed model achieves the desired security parameter values which is required in the image encryption.

This remaining paper has five sections. Section 2 shows the related work is done in the IE model. Followed by purpose and methodology of this manuscript in Section 3. Further, Section 4 illustrates the proposed optimized IE model. Next, Section 5 shows the results and discussion. Finally, the manuscript is concluded, and future scope is defined in Section 6.

2. Related Work

In this part, we look at image encryption models that are based on chaotic maps and metaheuristic algorithms that have been written about by different authors. It was described in [12] as an IE model where the TLBO algorithm is used to finetune the parameters of the chaotic logistic map algorithm based on the entropy parameter. In [13], the authors combined several chaotic map algorithms with various metaheuristic algorithms to fine-tune the parameters, thereby enhancing the performance of the IE model. Even more, a number of image encryption models that combine the chaotic tent map, the Henon map, the logistic map, and optimization algorithms like the JAYA and TAO algorithms are proposed [14-16]. In all models, they have used a single objective function such as entropy. Next, the chaotic map is fine-tuned using the BWO and PSO algorithms based on the entropy function by various authors [17-18]. Moreover, two metaheuristic algorithms, namely, GA and PSO with a chaotic map, are used by authors [19]. The GA algorithm is used to generate different encryption images, whereas PSO is utilized to determine which encryption image gives the best performance over others. Finally, the 3-D logistic map is fine-tuned using the Osprey optimization algorithm by considering the two parameters in the objective function, namely, entropy and SSIM [20].

3. Purpose and Methodology

The main purpose of this research is to enhance the image encryption model by considering the multiple chaotic maps and security parameters. In this research, 1-D CLM and CTM algorithms are considered, and a multi-objective function is designed using the entropy and correlation coefficient to enhance the security parameters of the IE model. Further, in this research, we have considered a recent metaheuristic OOBO algorithm that provides a better exploration rate in order to fine-tune the 1-D CLM algorithm. Next, we have explained the methodology of this research.

- **Dataset:** In this research, the primary and secondary datasets are considered in evaluating the proposed IE model. In the primary dataset, real-time images are considered, whereas in the secondary dataset, the images that are utilized in the literature are taken into consideration. The literature utilized images from the USC-SIPI Image database [21].

- **Chaotic Maps:** In this research, two one-dimensional chaotic maps are considered for the design of the IE model [14-15]. The 1-D CLM algorithm is used for key generation purposes, whereas the CTM algorithm is used to shuffle the image matrix by determining the shuffling sequence index from it. The basic equations of these algorithms are given below.

$$CLM: x_{n+1} = \mu x_n(1 - x_n) \tag{1}$$

$$CTM: \begin{cases} f(x_{i+1}, \mu) = \mu x_i & if\ (x_i < 0.5) \\ f(x_{i+1}, \mu) = \mu(1 - x_i) & Otherwise \end{cases} \tag{2}$$

In Eq. (1-2), x_i, x_{i+1}represents the present and next state. On the other hand, μ denotes the control parameter. In this research, Eq. (1), control parameter is fine-tuned using the metaheuristic OOBO algorithm.

- **Metaheuristic OOBO Algorithm:** OOBO is a recent metaheuristic algorithm and has a different idea for searching the optimal solution over existing algorithms. In the earlier algorithms, a specific population is

chosen as the best/worst population in the initial stage of the searching process; after that, based on it, an optimal solution is explored, whereas in the OOBO algorithm, all population knowledge is considered while exploring the optimal solution [22]. Further, in this algorithm, the one-to-one correspondence principle is used, which means that a guide member is used to update the other member. Next, in this algorithm, only a few parameters need to be initialized in order to search the solution space over the existing algorithms. The basic steps of the OOBO algorithm are given below.

1. Initialize the OOBO algorithm. In this step, the problem is taken into consideration, and its lower (LB) and upper bounds (UB) are defined to search the solution space. Further, the desired objective function is defined.
2. In the second step, OOBO parameters are initialized. In the OOBO algorithm, two parameters, N and T, are initialized. The N denotes the population, whereas T denotes the iteration.
3. In the third step, the N is randomly generated in the LB and UB according to the given problem and evaluated using the objective function.
4. In the fourth step, according to the T parameter, a loop is executed in which a set of guiding members are determined, and a new population is generated and evaluated using the objective function. If the new population is superior to the previous population, then the population is updated.
5. In the final step, the population that gives the best solution is chosen as the optimal solution.

- **Performance Evaluation Parameters:** The proposed IE model is evaluated using the various parameters to show its robustness against attacks. In this research, statistical attack parameters are taken into consideration. The parameters are determined to evaluate the statistical attack: entropy, MSE, RMSE, PSNR, CC, SSIM, MD, and time complexity [13].

4. Proposed Image Encryption Model

In this section, we have presented an optimized image encryption model based on the chaotic maps. The proposed IE model works better when the parameter values of the chaotic maps are optimized using the metaheuristic OOBO algorithm to make random keys and shuffling sequences. Figure 1 shows the block diagram of the proposed IE Model. Initially, the OOBO algorithm receives a secret image and applies the CLM algorithm. The OOBO algorithm finds the best parameter values by randomly searching the value in the lower and upper bounds of the parameter based on the objective function. Similarly, the chaotic tent map algorithm generates a random shuffling sequence. To accomplish this, the OOBO algorithm obtains the secret image following the exclusive-OR operation. This research utilizes entropy and correlation coefficient as the objective function. In this research, the entropy parameter is maximized whereas the correlation coefficient function is minimized. The designed multi-objective function for the proposed IE model is shown below.

$$Multi - Objective\ Function = \frac{E/8+(1-abs(CC))}{2} \quad (1)$$

Based on the objective function, which population value of CLM and CTM gives the minimum value of the objective function based on those parameter values, encryption is performed in the proposed IE Model. After determining the parameter value, we generate a random key and perform an exclusive-OR operation with the secret image. Next, shuffling of the image matrix is done. Finally, the encryption is achieved by performing the exclusive OR between the random key and the shuffled image matrix.

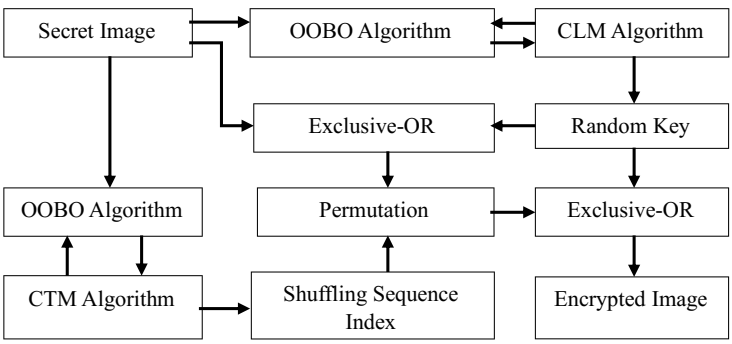

Figure 1. Flowchart of the Proposed IE Model

5. Results and Discussion

This section shows the simulation results of the proposed IE model and comparative analysis with the existing IE models. We design and simulate the proposed IE model using MATLAB 2018a software. Table 1 illustrates the system configuration and parameter setup values used for simulation purposes.

Table 1. Simulation Setup Configuration

Parameter	Value
System Configuration	i7 Processor, 8GB RAM, 64-bit Operating System
Image Resolution	$[256 \times 256]$
Total Images	5
Population	10
Iteration	100
Objective Function	E and CC
Logistic Map Parameter r	$[3.57 - 3.99]$
Tent Map Parameter r	$1.4 - 2$

Table 2-4 presents the visual quality analysis of the encrypted image and its histogram in comparison to the secret image and its histogram for the primary and secondary database. When comparing the encrypted image and its histogram to the original secret image and its histogram, the IE model requires the encrypted image to be noisy and its histogram to have an equal distribution. Furthermore, Table 5-6 demonstrates the evaluation of parameters for the proposed IE model, which analyzes the encrypted image in relation to the secret image. To accomplish this goal, the average value of the parameters is determined by executing the proposed model five times. Initially, we found the average correlation coefficient. The result shows that the proposed model achieves a low value of correlation coefficient. In a similar way, the proposed IE model achieves a low value of SSIM for different images. Further, analysis based on entropy analysis shows that the proposed model achieves high entropy near to 8. Next, the analysis based on MD, MSE, and RMSE parameters shows that the proposed model achieves a high value and low value of PSNR.

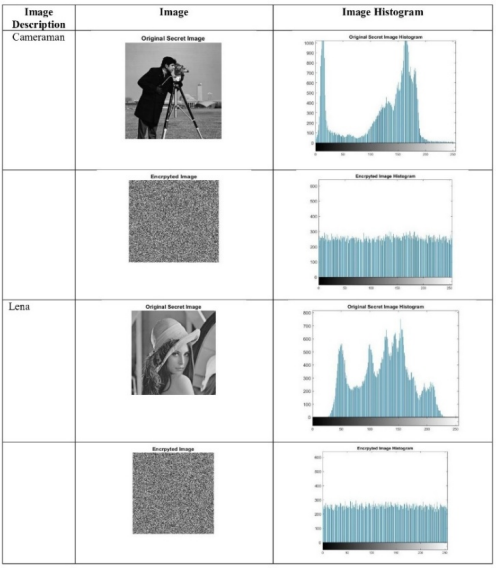

Figure 2. Visual Quality Analysis of Secret and Encrypted Image for Secondary Dataset Images (Cameraman and Lena)

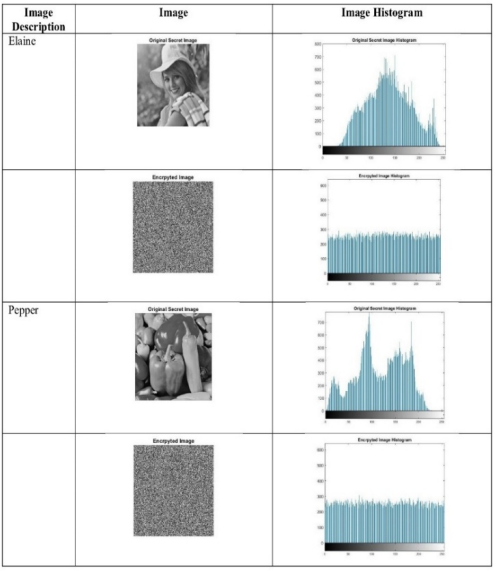

Figure 3. Visual Quality Analysis of Secret and Encrypted Image for Secondary Dataset Images (Elaine and Pepper)

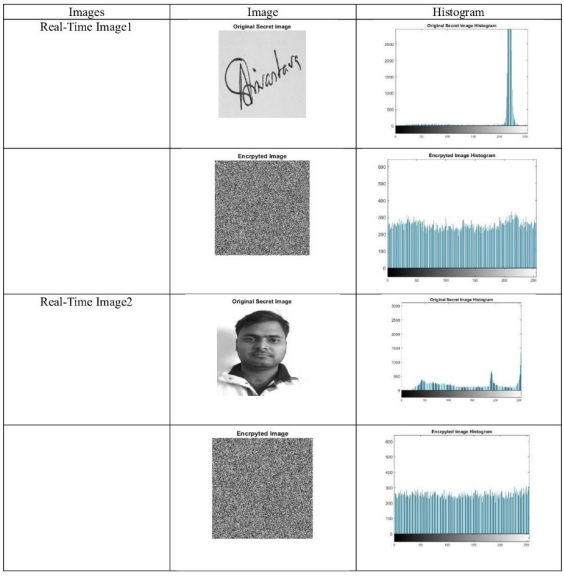

Figure 4. Visual Quality Analysis of Secret and Encrypted Image for Primary Dataset Images

Table 2: Performance Evaluation of the Proposed IE Model for Secondary Dataset Images

Image	**Parameter**	**Iterations**					**Average**
		1st	**2nd**	**3rd**	**4th**	**5th**	
Cameraman	CC	-0.0017	2.3762e-04	8.1889e-04	0.0030	-0.0013	**0.000211**
	SSIM	0.0064	0.0088	0.0108	0.0070	0.0093	**0.00846**
	MD	6.0547e+04	6.0519e+04	60372	60543	6.0515e+04	**6.05E+04**
	E	7.9966	7.9963	7.9959	7.9970	7.9966	**7.99648**
	MSE	3.7449e+03	3.7094e+03	3.7140e+03	3.7732e+03	3.6995e+03	**3.73E+03**
	RMSE	61.1954	60.9049	60.9429	61.4264	60.8237	**61.05866**
	PSNR	12.3964	12.4378	12.4323	12.3637	12.4493	**1.24E+01**
Lena	CC	4.8272e-04	0.0063	-0.0014	0.0024	6.9947e-05	**1.57E-03**
	SSIM	0.0102	0.0136	0.0103	0.0085	0.0098	**0.01048**
	MD	42173	4.2213e+04	4.1991e+04	4.2139e+04	4.1676e+04	**42038.4**
	E	7.9972	7.9970	7.9969	7.9971	7.9969	**7.99702**
	MSE	3.5751e+03	3.5635e+03	3.6294e+03	3.5394e+03	3.4990e+03	**3.56E+03**
	RMSE	59.7925	59.6953	60.2441	59.4927	59.1523	**59.67538**
	PSNR	12.5979	12.6120	12.5325	12.6415	12.6914	**12.61506**
Elaine	CC	-0.0047	-0.0018	0.0025	0.0012	0.0022	**-0.00012**
	SSIM	0.0097	0.0079	0.0120	0.0091	0.0126	**0.01026**
	MD	41096	4.1553e+04	41608	42000	41704	**41592.2**
	E	7.9965	7.9968	7.9972	7.9970	7.9969	**7.99688**
	MSE	4.3823e+03	4.3856e+03	4.4765e+03	4.4238e+03	4.3831e+03	**4.41E+03**
	RMSE	66.1993	66.2236	66.9064	66.5119	66.2047	**66.40918**
	PSNR	11.7137	11.7105	11.6215	11.6728	11.7130	**11.6863**
Pepper	CC	6.2088e-04	-0.0084	6.0670e-04	0.0042	-0.0051	**-1.61E-03**

	SSIM	0.0084	0.0099	0.0104	0.0114	0.0095	**0.00992**
	MD	3.5921e+04	36362	3.6118e+04	3.6305e+04	35815	**3.61E+04**
	E	7.9971	7.9970	7.9973	7.9968	7.9970	**7.99704**
	MSE	3.3265e+03	3.3990e+03	3.3092e+03	3.3311e+03	3.3109e+03	**3.34E+03**
	RMSE	57.6754	58.3009	57.5258	57.7153	57.5401	**57.7515**
	PSNR	12.9110	12.8173	12.9336	12.9050	12.9314	**1.29E+01**

Table 3: Performance Evaluation of the Proposed IE Model for Primary Dataset Images

Image	**Parameter**	**Iterations**					**Average**
		1st	**2nd**	**3rd**	**4th**	**5th**	
Real-Time Image1	CC	0.0022	0.0018	0.0036	0.0093	-0.0017	**0.00304**
	SSIM	0.0094	0.0107	0.0102	0.0116	0.0088	**0.01014**
	MD	1.0671e+05	1.0660e+05	106711	1.0669e+05	106601	**1.07E+05**
	E	7.9931	7.9945	7.9943	7.9932	7.9937	**7.99376**
	MSE	1.2920e+04	1.2758e+04	1.2509e+04	1.2920e+04	1.2759e+04	**1.28E+04**
	RMSE	113.6665	112.9496	111.8443	113.6668	112.9537	**113.0162**
	PSNR	7.0182	7.0731	7.1585	7.0181	7.0728	**7.07E+00**
Real-Time Image2	CC	0.0018	0.0026	-0.0091	-3.6920e-04	0.0027	**-0.00047**
	SSIM	0.0093	0.0100	0.0082	0.0095	0.0081	**0.00902**
	MD	3.9776e+04	40299	39971	39501	39724	**3.99E+04**
	E	7.9962	7.9965	7.9969	7.9971	7.9965	**7.99664**
	MSE	1.0860e+04	1.0770e+04	1.1020e+04	1.0952e+04	1.1005e+04	**1.09E+04**
	RMSE	104.2111	103.7763	104.9769	104.6531	104.9024	**104.504**
	PSNR	7.7725	7.8088	7.7089	7.7358	7.7151	**7.75E+00**

Finally, the proposed IE model is compared with the existing IE model based on two parameters, namely, Entropy and CC. Table 7 shows the entropy and correlation analysis of the proposed IE model with the recent existing IE model proposed by Sameh et al. [13]. The results shows that the proposed IE model achieves high entropy, as shown in Figure 2. Further, low correlation coefficient as compared to the existing model, as shown in Table 7.

Table 4. Comparative Analysis

Images	**Sameh et al. [13]**		**Proposed IE Model**	
	E	**CC**	**E**	**CC**
Cameraman	7.9956	− 0.0039	7.99648	0.00021
Elaine	7.9951	− 0.0010	7.99688	-0.00012
Peppers	7.9961	− 0.0022	7.99704	-0.00161

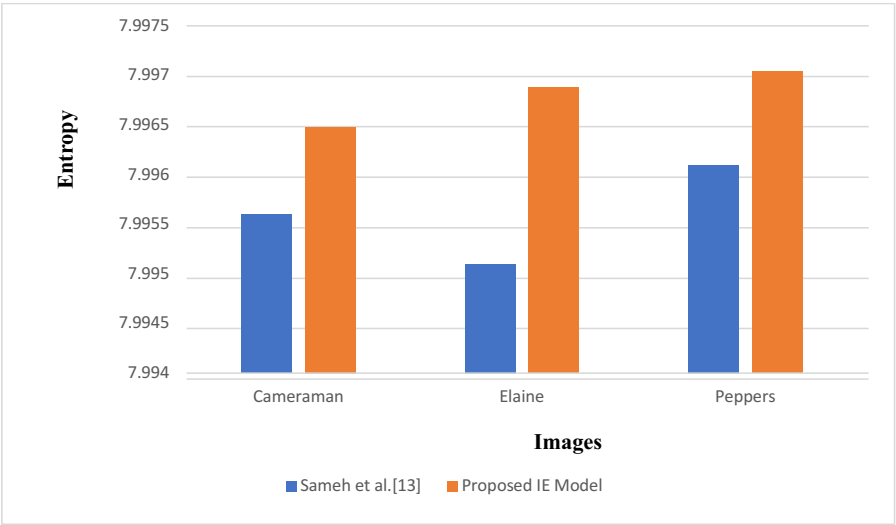

Figure 5. Comparative Analysis based on Entropy Parameter

6. Conclusion and Future Scope

In this study, we have presented an optimized image encryption model based on the chaotic maps and the metaheuristic OOBO algorithm. The proposed IE model benefits from using chaotic maps to generate random keys and shuffling sequences. However, to achieve this goal, we first employ the metaheuristic OOBO algorithm to fine-tune the parameters of the chaotic maps based on the objective function. In this research, we design the objective function using two parameters: E and CC. Moreover, we perform an exclusive-OR operation using a random key to achieve encryption and then shuffle the secret image according to the shuffling sequence. The simulation evaluation reveals that the encrypted image's visual quality is noisy, and its histogram exhibits an equal distribution across different secret images. Next, the comparative analysis based on the E and CC parameters shows that the proposed IE model achieves better values than the existing IE models. Finally, from this research, the following key points are drawn.

- In the proposed IE model, the fine-tuning of the chaotic map algorithms is done using the metaheuristic OOBO algorithm. Therefore, a number of parameters need to be communicated to the receiver for decryption purposes.
- In the proposed IE model, the initialization of parameters for the metaheuristic algorithm is a challenging task.

In the future, we will explore the high-dimensional chaotic maps to encrypt the secret color images. We generate multiple keys simultaneously in the higher dimension to encrypt the different planes of color images. Further, we will explore machine learning/deep learning based image encryption methods.

References

[1] Rehman, M.U., 2024. Quantum-enhanced chaotic image encryption: Strengthening digital data security with 1-D sine-based chaotic maps and quantum coding. *Journal of King Saud University-Computer and Information Sciences*, *36*(3), p.101980.

[2] Es-sabry, M., El Akkad, N., Khrissi, L., Satori, K., El-Shafai, W., Altameem, T. and Rathore, R.S., 2024. An efficient 32-bit color image encryption technique using multiple chaotic maps and advanced ciphers. *Egyptian Informatics Journal*, *25*, p.100449.

[3] Kaur, M., Singh, D. and Kumar, V., 2020. Color image encryption using minimax differential evolution-based 7D hyper-chaotic map. *Applied Physics B*, *126*(9), p.147.

[4] Razzaq, M.A., Shaikh, R.A., Baig, M.A. and Memon, A.A., 2017. Digital image security: Fusion of encryption, steganography and watermarking. *International Journal of Advanced Computer Science and Applications*, *8*(5).

[5] Singh, D., Kaur, S., Kaur, M., Singh, S., Kaur, M. and Lee, H.N., 2024. A systematic literature review on chaotic maps-based image security techniques. *Computer Science Review*, *54*, p.100659.

[6] Singh, M. and Singh, A.K., 2023. A comprehensive survey on encryption techniques for digital images. *Multimedia Tools and Applications*, *82*(8), pp.11155-11187.

[7] Kaur, M. and Singh, D., 2021. Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption. *Multidimensional Systems and Signal Processing*, *32*, pp.281-301.

[8] Zhang, B. and Liu, L., 2023. Chaos-based image encryption: Review, application, and challenges. *Mathematics*, *11*(11), p.2585.

[9] Kaur, M., Singh, S., Kaur, M., Singh, A. and Singh, D., 2021. A systematic review of metaheuristic-based image encryption techniques. *Archives of computational methods in engineering*, pp.1-15.

[10] Rajwar, K., Deep, K. and Das, S., 2023. An exhaustive review of the metaheuristic algorithms for search and optimization: taxonomy, applications, and open challenges. *Artificial Intelligence Review*, *56*(11), pp.13187-13257.

[11] Abdel-Basset, M., Abdel-Fatah, L. and Sangaiah, A.K., 2018. Metaheuristic algorithms: A comprehensive review. *Computational intelligence for multimedia big data on the cloud with engineering applications*, pp.185-231.

[12] Abedzadeh, M., Rostami, M.J. and Shariatzadeh, M., 2023. Image encryption using a standard map and a teaching-learning based optimization algorithm. *Multimedia Tools and Applications*, *82*(19), pp.29199-29225.

[13] Sameh, S.M., Moustafa, H.E.D., AbdelHay, E.H. and Ata, M.M., 2024. An effective chaotic maps image encryption based on metaheuristic optimizers. *The Journal of Supercomputing*, *80*(1), pp.141-201.

[14] Kumar, N., Saini, S. and Garg, D., 2024. Color Image Encryption Model Based on 3-D Chaotic Logistic Map and JAYA Algorithm. *IETE Journal of Research*, pp.1-11.

[15] Kumar, N. and Saini, S., 2024, July. Image encryption model based on tent map and JAYA algorithm. In *AIP Conference Proceedings* (Vol. 3121, No. 1). AIP Publishing.

[16] Kumar, N. and Saini, S., 2024, July. Image Encryption Model based on Chaotic Henon Map and Termite Alate Optimization Algorithm. International Journal of Intelligent Systems and Applications in Engineering, 12(18s), pp. 428–436

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

[18] 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.

[19] Ferdush, J., Mondol, G., Prapti, A.P., Begum, M., Sheikh, M.N.A. and Galib, S.M., 2021. An enhanced image encryption technique combining genetic algorithm and particle swarm optimization with chaotic function. *International Journal of Computers and Applications*, *43*(9), pp.960-967.

[20] Kaur, G., Singh, Y., Bhadauria, P., Kumar, A. and Singh, J.P., 2024. Color Image Encryption Method based on Three-Dimensional Chaotic Map and Nature-Inspired Osprey Optimization Algorithm. *Power System Technology*, *48*(1), pp.306-321.

[21] sipi.usc.edu. (n.d.). *SIPI Image Database*. [online] Available at: https://sipi.usc.edu/database/.

[22] Dehghani, M., Trojovská, E., Trojovský, P. and Malik, O.P., 2023. OOBO: a new metaheuristic algorithm for solving optimization problems. *Biomimetics*, *8*(6), p.468.