Protecting Sensitive Images with Improved 6-D Logistic Chaotic Image Steganography

Mandeep Sandhu
Department of Computer Science
Guru Nanak Dev University College
India
gimeti4@gmail.com

Mohammad Ahmed
Department of Computer Science
King Khalid University
Saudi Arabia
monaahmed@kku.edu.sa

Mohammad Hussain
Department of Business Informatics
King Khalid University
Saudi Arabia
humohammad@kku.edu.sa

Surender Head
Career Programs, CodeQuotient Pvt. Ltd., India
surendahiya@gmail.com

Imran Khan
Department of Computer Engineering, King Khalid University
Saudi Arabia
imkhan@kku.edu.sa

Abstract: *In the digital age, strong methods for safeguarding sensitive data are essential. Image steganography is a practical technique for data protection that hides information inside seemingly authentic images. The proposed method increases security by using chaotic based image encryption and decryption. Encryption approaches based on chaotic logistic theory present an abundance of attractive and novel opportunities for developing secure image encryption methods. Nevertheless, these maps are frequently used for specific, unpredictable starting parameters. This problem is addressed by the research's Tabu search optimisation method. This method optimises chaotic map initial settings using a fitness function with numerous objectives. For image encryption, the most efficient methods are used to produce confidential keys. The input picture undergoes horizontal and vertical diffusion and permutation during encryption. These operations further scramble the image data, making it even more difficult to detect the hidden information. The primary goal is to develop a safe method for encrypting both color and grayscale images. Two common grayscale and color images that are accessible to the public were used to test the suggested strategy. Compare our method with key existing works, specifically on the basis of Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), Peak Signal-to-Noise Ratio (PSNR) and speed, respectively, our approach improves upon these studies. Our results demonstrate that 7.9981, 99.8245, 35.6507, and 78.871 are the greatest values of entropy, NPCR, UACI, and PSNR, respectively. Whereas the respective speeds of encryption and decryption increase to 0.8433 and 1.4387 seconds. This innovative approach presents a powerful tool for applications requiring secure image steganography.*

Keywords: *Image encryption, logistic chaotic map, steganography, optimization.*

Received June 21, 2024; accepted September 21, 2024
https://doi.org/10.34028/iajit/21/6/10

1. Introduction

Multimedia applications are now widely used in all sectors of engineering [4]. Globally, photographs, videos, and audios are conveniently able to convey the information [6]. Images are used in a wide range of applications, including telemedicine, military communication, remote sensing, image processing, and more [22]. In the context of security and secrecy, the information that images provide can occasionally be crucial. As a result, it's essential to conceal the image data so that only the intended user may access it [25]. Cryptography and information concealment techniques make up the majority of information security techniques. Watermarking and steganography are two methods of information concealment [14]. The original information is decoded using cryptography [24].

Steganography is a technique that conceals information by encoding confidential data into an image [38]. Information authentication uses watermarking. The main objective in our research is the application of cryptography to steganographyPicture cryptography uses encryption to make a significant image look chaotic. With decryption technology, a noisy image becomes meaningful [37].

Image steganography is a useful data protection method that conceals data within what appear to be normal photographs [37]. The technique uses chaotic picture encryption and decoding to gain higher security. There are three categories for image encryption techniques: spatial-based, transform-based, and hybrid [31]. Spatial-based approaches analyse the entire image, unlike transform-based methods, which partition input images into the frequency domain. Every technique has advantages and disadvantages [26].

Techniques based on spatial are straightforward and simple to use. In contrast, transform-based techniques are a little more difficult to use but offer more security against security breaches when compared to spatial-based strategies [17]. To create a more secure algorithm, both approaches are typically used in image encryption. To produce the random keys, chaotic maps are often

used [18]. As time has gone on, numerous chaotic map variations have been documented. Basically, chaotic maps are categorized into two types one-dimensional and multi-dimensional. Multiple-dimensional chaotic maps are more complex and challenging to interpret [27].

Sandhu *et al*. [28] used tent cubic maps in a hyper-chaotic system to generate a secret key that is more complex and random. After that, permutation and diffusion procedures are used to encrypt the images. A 3-D space-based image encryption approach was proposed [19]. The secret keys are created using a 3D modular chaotic system, which also contributes to the expansion of the key space. Nevertheless, hyper-parameter tuning is a problem with the aforementioned strategies. The hyper-parameters in the most of the literature is done via trial and error [13]. The values that were obtained might only be appropriate for a certain kind of image and not for another. Consequently, it is necessary to optimize or adjust the hyper-parameters of chaotic maps.

Hyper-parameters can be tuned using meta-heuristic methods [10]. However, there are a number of problems with meta-heuristic approaches, making the process of choosing an effective meta-heuristic difficult [11]. A steganography technique is used to first convert a color plain image into a grayscale image. Then, the resulting grayscale image is encrypted, lowering the encryption's dimension [34]. Two multi-image steganography approaches using Least Significant Bit (LSB) and classical gray code methods were examined [35]. The results favored the LSB technique because of its higher performance despite having a lower embedding capacity. A steganography approach that targets particular pixels to create the stego image while embedding data using the bit plane method [21]. A steganography technique that uses chaos theory and Particle Swarm Optimization (PSO) to conceal sensitive information from view while maintaining image quality [8]. Ant Colony Optimization (ACO) was taken into consideration by Sreelaja and Pai [30] to create the best secret keys. Nevertheless, its convergence speed is not very fast. In order to encrypt images more effectively, Abdullah *et al*. [1] used a Genetic Algorithm (GA). Other techniques, such as those by Shao *et al*. [29], Wu *et al*. [32], Abed *et al*. [2], and Sandhu *et al*. [28], integrate with encryption methods. While these approaches offer advancements in reducing computation time and achieving high compression ratios, there may be gaps in terms of addressing security vulnerabilities, ensuring robustness against attacks, and scalability for large-scale image encryption tasks.

Kaur and Singh [16] aims to create a steganography algorithm that gives equal weight to payload capacity and stego-image quality. It incorporates several methods, such as Ebola optimization, Huffman encoding, and Discrete Wavelet Transform (DWT). However, these methods still have a limited capacity for embedding and have slow computing speeds, especially for larger images.

Chaos maps, also known as logistic maps, Chebyshev maps, tent maps, and so on, are evolution functions that, depending on the initial condition and the time domain (continuous or discrete), produce a deterministic bounded series of random integers. Furthermore, since chaos maps are non-periodic, non-converging, and random-like for parameter adaptation, they can be used in place of the metaheuristic's random sequence generator. These days, chaos-based metaheuristics-like chaotic particle swarm optimization, chaotic harmony search, chaotic genetic algorithm, chaotic league championship algorithm, etc.-are widely used because of their high rate of convergence and increased use of randomness [15].

Thus, the primary goal of this research project is to resolve these problems. In this study, an encryption-based image steganography algorithm is suggested to address the above-mentioned issues. The main contributions of this research work are:

- A local chaotic search based Tabu search algorithm is used to tune the initial parameters of 6-D chaotic map.
- Using the correlation coefficient and entropy to formulate a multi-objective fitness function.
- To encrypt the secret image applying permutation and diffusion processes using secure secret keys derived from the chaotic map.
- Embedding process to embed secret cipher image in cover image.
- Carrying out a thorough comparative study to assess the suggested image encryption method's performance in comparison to established meta-heuristic and revolutionary image encryption techniques.

The remaining article is arranged as follows: Section 2 discusses the preliminary. Section 3 provides a description of the suggested methodology. In section 4, the experimental setup, findings, and comparative analyses are presented. Section 5 concludes up the proposed methodology.

2. Preliminaries

2.1. 6-D logistic chaotic map

The easiest method for creating chaos is the logistic map, which was provided by Equation (1).

$$i_{n+1} = r i_n (1 - i_n) \tag{1}$$

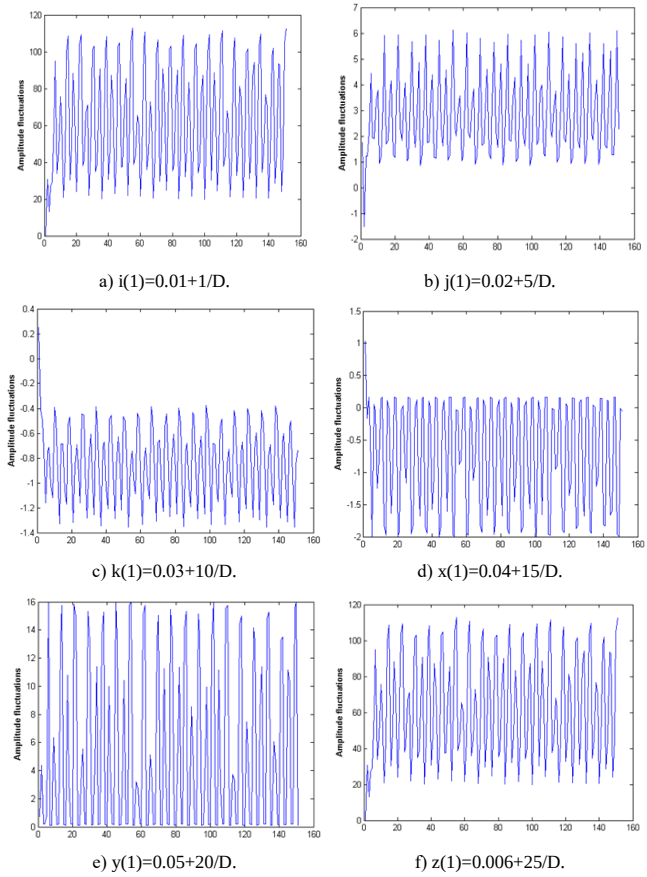
For this equation to be chaotic, $0<i_n<1$, and $r=4$ are necessary [33]. To improve security, Liu *et al*. [20] propose a 2D logistics map with quadratic coupling. For increased safety, Hossain *et al*. [7] propose a 3D logistics map utilizing quadratic-cubic coupling. Equation (2) suggests the extended 6-D form, as proposed by Rashid

et al. [23].

$$
\begin{aligned}
&i_{n+1} = \\
&ai_1(1-i_n) + \mathrm{b}z_n^2 i_n + \mathrm{c}y_n^3 + \mathrm{Q}x_n^4 i_n + \mathrm{P}k_n^5 + \mathrm{T}\, j_n^6 i_n \\
&j_{n+1} = \\
&aj_1(1-j_n) + \mathrm{b}i_n^2 j_n + \mathrm{c}z_n^3 + \mathrm{Q}y_n^4 j_n + \mathrm{P}x_n^5 + \mathrm{T}\, k_n^6 j_n \\
&k_{n+1} = \\
&ak_1(1-k_n) + \mathrm{b}j_n^2 k_n + \mathrm{c}i_n^3 + \mathrm{Q}z_n^4 k_n + \mathrm{P}y_n^5 + \mathrm{T}\, x_n^6 k_n \\
&x_{n+1} = \\
&ax_1(1-x_n) + bk_n^2 x_n + cj_n^3 + Qi_n^4 x_n + Pz_n^5 + T\, y_n^6 x_n \\
&y_{n+1} = \\
&ay_1(1-y_n) + \mathrm{b}x_n^2 y_n + \mathrm{c}k_n^3 + \mathrm{Q}j_n^4 y_n + \mathrm{P}i_n^5 + \mathrm{T}\, z_n^6 y_n \\
&z_{n+1} = \\
&az_1(1-z_n) + by_n^2 z_n + cx_n^3 + Qk_n^4 z_n + Pj_n^5 + T\, i_n^6 z_n
\end{aligned}
\tag{2}
$$

where 3.57<*a*<4, 0<*b*<0.14*10-11, 0<c<0.045*10-11, 0<*Q* <0.061*10-11, 0<*P*<0.012*10-11, 0<*T*<0.0021*10-11 and the initial values of i, j, k, x, y, and k between 0 and 1 exhibit the chaotic behavior shown in the previous equations.

The 6-D logistic map is made more complex and secure by the inclusion of six constant terms and hexagonal quadratic coupling. The 6-D logistic map is made more complex and secure by the inclusion of six constant terms and hexagonal quadratic coupling.



a) i(1)=0.01+1/D. b) j(1)=0.02+5/D.

c) k(1)=0.03+10/D. d) x(1)=0.04+15/D.

e) y(1)=0.05+20/D. f) z(1)=0.006+25/D.

Figure 1. Chaotic sequences of the 6-D logistic chaotic map created with different initial values.

In Figure 1-a) shows the chaotic sequences of the 6-D logistic chaotic map. Chaotic sequences are created using the beginning value, of i(1)=0.01+1/D; and b)) shows the chaotic sequences of the 6-D logistic chaotic map. Chaotic sequences are created using the beginning value, of j(1)=0.02+5/D, in c) shows the chaotic sequences of the 6-D logistic chaotic map. Chaotic sequences are created using the beginning value, of k(1)=0.03+10/D; and in d) shows the chaotic sequences of the 6-D logistic chaotic map. Chaotic sequences are created using the beginning value, of x(1)=0.04+15/D, in e) shows the chaotic sequences of the 6-D logistic chaotic map . Chaotic sequences are created using the beginning value, of y(1)=0.05+20/D; and in f) shows the chaotic sequences of the 6-D logistic chaotic map. Chaotic sequences are created using the beginning value, of z(1)=0.006+25/D and the number of iterations is 160.

The primary goal is to create secure stego images. First, the secret image is encrypted using image encryption; the secret key is primarily responsible for the security. This paper generates the secret key using a 6-D hyper-chaotic map. This map requires six initial state variables such as *i*, *j*, *k*, *x*, *y* and *z* and six control parameters i.e., *a*, *b*, *c*, *Q*, *P*, , and *T*. These parameters affect the map's chaotic behavior. If the values of these parameters are chosen incorrectly, the chaotic map could become non-chaotic, which could compromise the security of the image cryptosystem. For this reason, it is desirable to tune these parameters. To do this, the Tabu Search optimization function is used. Here, we use two objectives, such as Entropy (E) and Correlation Coefficient (Cr) for optimization function. This is because, simultaneously, better encrypted images require the minimum correlation coefficient and maximum entropy. The value of the entropy for gray scale images should be equal to or close to 8 for an encrypted image. The maximum entropy indicates the presence of a more uniform distribution of pixels in the encrypted image.

2.2. Tabu Search

The Tabu search algorithm was employed in this paper to identify the best solutions for the 6-D hyper-chaotic map. When it comes to convergence, Tabu Search outperforms local search. The near-optimal solution is found by escaping from the local solution using the very effective Tabu search technique. The Tabu Search (TS) metaheuristic employs memory structures and local search algorithms to find a promising answer by investigating its neighbours [7]. Examining adjacent solutions yields this solution. Local searches often get stuck in unsuitable locations. TS improves search by preventing revisiting solutions once they've been thoroughly studied. SA and TS are very similar in that they both entail exploring and hill climbing. A collection of guidelines for removing solutions from the neighbourhood search are defined by the memory structure. Typically, a Tabu list is made up of solutions that are categorized by the number of Tabu tenure iterations during which the solution is kept in the solution bucket. Three categories can be used to group the memory structures employed in TS [9]:

- Short-term memory: a possible fix that makes it onto the Tabu list.
- Intermediate memory: to enhance the search spaces, intensification criteria are applied.
- Long-term memory: the hunt for new areas is guided by diversification criteria. If the solution finds itself on a plateau or less-than-ideal area, a reset is implemented.

Algorithm 1: Tabu Search Algorithm.

1. *Initialize parameters: tolerance, initial seed, max_iterations.max_Tabu_Size*
2. *SBest ← So*
3. *best_Candidate ← s0*
4. *tabu_list ← empty*
5. *tabu_list.push(s0)*
6. *while iterations < max_iterations do*
   s_Neighborhood ← get_Neighbors(best_ Candidate)
   best_Candidate ← s_Neighborhood[0]
   for s_Candidate in s_Neighborhood do
   if (not tabulist.contains(s_Candidate)) && (fitness(s_Candidate) > fitness(best_Candidate)) then
   best_Candidate ← s_Candidate
   (end if)
   (end for)
   if fitness(best_Candidate) > fitness(s_Best) then
   S_Best ← best_Candidate
   (end if)
   tabu_list.push(best_Candidate)
   if tabu_list.size > max_Tabu_Size then
   tabu_list.remove_First()
   (end if)
   (end while)
7. *return S_Best*
8. *Print the objective value*

3. Proposed Technique

Figure 2 represents the flow plan of the encryption process of the image encryption technique depends on 6-D chaotic systems. As in process firstly we optimized the parameter of 6-D chaotic map by using Tabu search algorithm. Afterwards secret key is generated by using 6-D chaotic map. The secret key is used to encrypt the secret image.

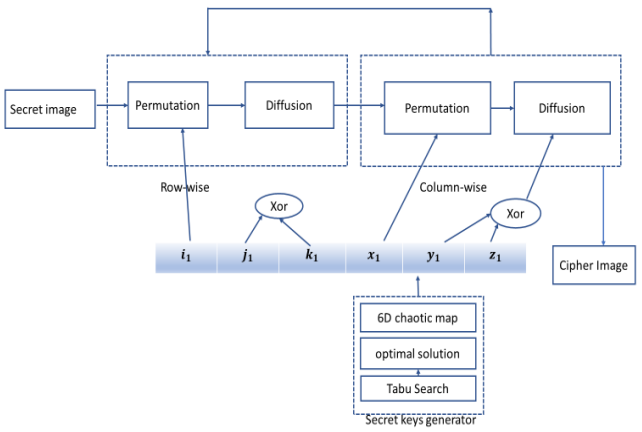


Figure 2. Shows the encryption process of secret image.

Decryption process: the same encryption procedures are used for decryption but in reverse. Utilize the parameters with the Tent-cubic chaotic map to generate the identical random numbers used in the encryption phase. Using the same secret key is necessary to reverse the diffusion of the image and get the original image before the encryption process.

3.1. The LSB (Least Significant Bit)

In order to encode hidden data, the Least Significant Bit (LSB) embedding technique modifies the least significant bits of pixel values in an image covertly [35]. First, the secret data-which is frequently taken from text or other sources-is encoded into binary format. A carrier image is selected and then partitioned into smaller pieces, like blocks or pixels [3]. The LSBs of the pixel values are successively replaced with matching bits of the secret data during the embedding process. The least significant bits of the cover image's pixel values are swapped out for the matching bits of the secret data during the LSB embedding procedure.

As shown in Figure 3 pixels of cover image is taken; secret image is taken in binary form. Then in embedding process, the LSB is altered to '0' if the secret bit is '0' and the pixel's LSB is '1'. When the secret bit is set to '1', the LSB stays at '1' if it is already at that value and changes to '1' if it is at '0'. Minimal alterations are made to maintain the cover image's aesthetic appeal and make it invisible to the naked eye. Once all units have been finished, the altered image becomes the stego image, hiding the cover image's secret data. Even though the LSB methodology is straightforward, if the changes to the LSBs are statistically significant, it can be vulnerable to detection by sophisticated steganalysis techniques.

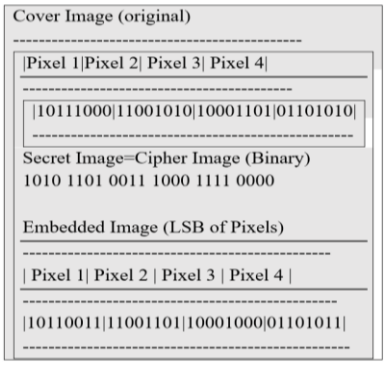


Figure 3. Shows the working process of LSB algorithm.

3.2. Embedding Process

In Image steganography, the embedding procedure entails concealing sensitive information inside an image while maintaining its visual imperceptibility. An outline of the embedding procedure is provided below:

The first step is choosing the cover image for the covert data carrier. Next, chaotic encryption should be used to create the cypher image from the confidential image. Before encoding, the cypher image must be converted to an embeddable format. Visual data may

need to be converted to binary. The cover and cypher images must be divided into pixels to improve embedding. The LSB method embeds the cypher picture into the cover image. Combined with steganographic technology, this method hides encrypted data. LSBs of pixel values should be changed to minimise noticeable changes during data embedding. To avoid detection, the fake image must closely resemble the cover image. Figure 4 shows the suggested method.

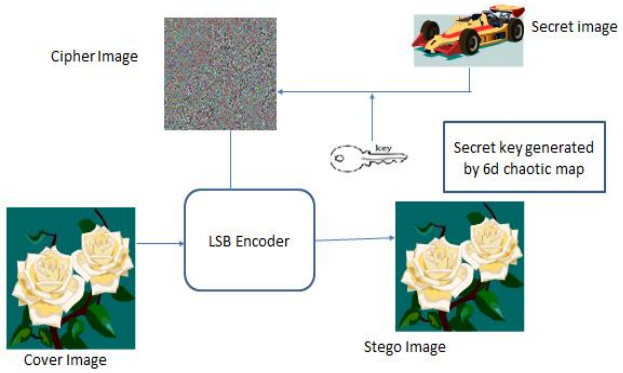


Figure 4. Shows the working process of proposed technique.

4. Simulation Results and Security Analysis

This section presents the methods and techniques to gauge the effectiveness and performance of the proposed encryption and steganography technique through several tests. To evaluate image steganography techniques, a range of metrics are employed, including payload capacity, Peak Signal-to-Noise Ratio (PSNR), Structured Similarity Index Measure (SSIM), and Correlation Coefficient. These metrics offer insights into different aspects of steganographic performance [36].

This method uses as inputs the color Lena picture, Baboon, and aerial photos of "Miramar NAS". A laptop running Windows 10 with 4 GB of RAM and MATLAB R2019a is used for security analysis and simulation. The 6D chaotic map's beginning circumstances and control settings are the keys that this algorithm uses. The simulation's outcomes are listed below.

4.1. Key Space Analysis

The number of keys required for encryption is termed as the key space [14] to thwart brute-force attacks, an algorithm's key space should exceed2^{128} [12]. In our case, considering control parameters and initial state variables, the 6D chaotic based employs a key space of 2^{765} to prevent attacks. This underscores the robustness of our proposed technique against brute-force assaults. Key space depends on the combination of control parameters and initial state variables such as *i, j X or k, x, y Xor z* are used for encryption procedure. Secret keys are the same size as the input image. Therefore, for image size 256 the key space is given below:

- Key space=(256!)3.
- Power of 2 in $(256!)^3$=3×255=765.

4.2. Peak Signal to Noise Ratio (PSNR)

Peak Signal to Noise Ratio (PSNR) assesses the quality of the stego-image by quantifying the difference between it and the original cover image. When embedding secret information into the host image, alterations occur in the pixel values, impacting the quality of the resulting stego image, particularly its imperceptibility [5]. Table 1 shows the comparison analysis based on PSNR by the proposed technique. Table 2 shows the PSNR and MSE values of several images by the proposed technique. MSE refers to the sum of errors in the values of host and cipher images [2].

Table 1. PSNR comparisons of proposed technique with related work.

Ref. [34]	Ref. [35]	Ref. [16]	Proposed approach
74.6	58.62	75.8	78.871
79.68	57.53	78.13	80.855
80.24	50.00	79.85	80.547

Table 2. PSNR and MSE the proposed technique with different images.

Name of image	PSNR	MSE
Boat	78.565	0.00175
Aeroplane	79.12	0.00191
Lena	78.871	0.00019
Baboon	80.5472	0.000187
Miramar NAS	80.855	0.004285

Equation (3) for calculating MSE defined as follows:

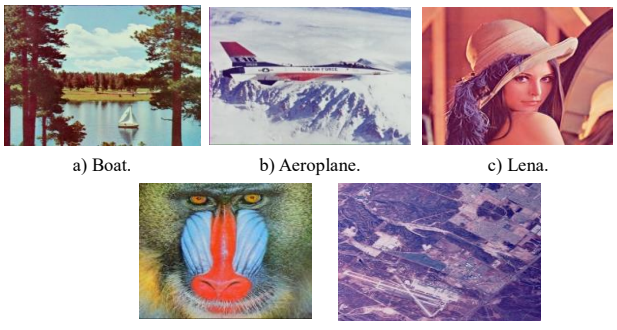
$$MSE=\frac{1}{MN}\sum_{\substack{0<i\le m\\0<j<n}}(O(i,j)-C(i,j)) \quad (3)$$

For calculating the value of PSNR the Equation (4) is given below:

$$\text{PSNR} = 10\log_{10}\left[\frac{I^2}{\text{MSE}}\right] \quad (4)$$

Here *I* is representing the largest value that is possible for the pixel of gray scale image i.e., I=255.

Figure 5 shows cover images standard the color Lena picture, Baboon, and aerial photos of "Miramar NAS" which have been used in the experimentations. Table 2 shows the PSNR and MSE values of experimentation for different cover images.



a) Boat. b) Aeroplane. c) Lena.

d) Baboon. e) Miramar NAS.

Figure 5. Sample cover images.

4.3. The Number of Pixel Changes Rate

Number of Pixel Changes Rate (NPCR) measures the percentage of differing pixel values between two

encrypted images resulting from a single-pixel change in the input image. A higher NPCR indicates greater resistance against differential attacks. It is calculated as Equation (5) as follows:

$$NPCR=\frac{1}{w*h}\sum_{\substack{1\le i\le w\\ 1\le j<h}} D(i,j)*100$$
$$D(i,j)=0 \text{ when } C1(i,j)=C2(i,j) \text{ and} \quad (5)$$
$$D(i,j)=1 \text{ when } C1(i,j)\neq C2(i,j)$$

Where the image height is represents by h and its width by w. The variation between corresponding pixels in the original encrypted image is shown by $D(i, j)$. NPCR ϵ range: [0,100].

4.4. Unified Average Changing Intensity

Unified Average Changing Intensity (UACI) quantifies the average change in intensity between two encrypted images originating from original images with only a single-pixel difference. It is calculated as below Equation (6):

$$UACI=\left[\sum_{\substack{0\le i\le w\\ 0<j<h}}\frac{|C1(i,j)-C2(i,j)|}{255}\right]*\frac{100}{w*h} \quad (6)$$

Where $C1$ and $C2$ is the encrypted images that has been altered by altering a single pixel in the original image. Table 3 shows the NPCR and UACI values of several images by the proposed encrypted technique.

Table 3. Comparison of average NPCRR, G, B and UACIR, G, B of "Lena" image.

Lena images		NPCR (%)	UACI (%)
Ref. [25]	Avg.	99.60	33.62
Ref. [26]	Avg.	99.606	33.466
Ref. [27]	Avg.	99.78	30.62
Proposed technique	Avg.	99.8245	35.6507

4.5. Entropy

It quantifies the level of uncertainty and randomness of pixels in encrypted images [25]. It is computed as Equation (7):

$$H_E=\sum_{i=0}^{255} p(i)log_2 p(i) \quad (7)$$

Where H_E is the entropy, $P(i)$ determines the possibility of existence of symbol i.

The ideal entropy value for a perfectly random grayscale image is 8 [36]. In Table 4, the algorithm's computed information entropy is 7.9981, indicating a uniform distribution of gray values and a minimal variance in the probability of each pixel value occurrence. This establishes the algorithm's robust resistance to attacks, its capacity to withstand exhaustive attacks, and its successful encryption. Table 5 presents a comparative analysis of information entropy with recent sources.

Table 4. The entropy of the cipher image.

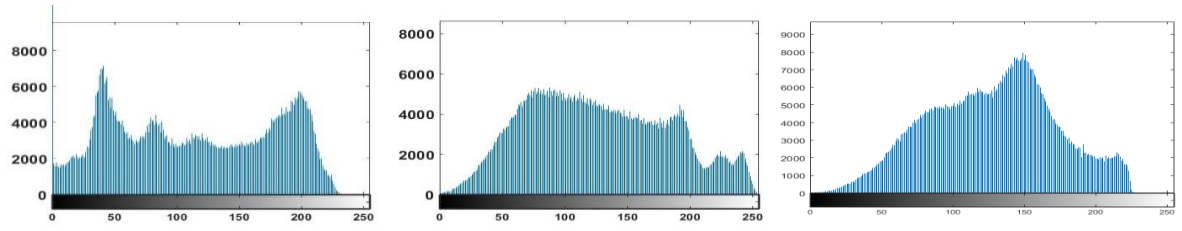
Image Name	Entropy
Baboon	7.9980
Boat	7.9981
Cameraman	7.9983
Peppers	7.9979
Lena	7.9981

Table 5. Compares information entropy.

Lena image	Entropy value of encrypted images			
	R	G	B	RGB
Ref. [29]	-	-	-	7.9993
Ref. [32]	7.9971	7.9974	7.9972	7.9972
Ref. [2]	-	-	-	7.9983
Proposed technique	7.9979	7.9982	7.9980	7.9981

4.6. Visual Effects

Visual analysis in steganography involves carefully scrutinising photographs to find small changes or anomalies that may indicate concealed data. Analysis of pixel intensity distributions, colour channel variances, texture patterns, and spatial correlations are some method used in visual analysis. In this study pixel intensity is used. Pixel intensity refers how pixel values are distributed across an image. Histograms are often used to visualize these distributions, providing insights into the overall brightness and contrast of an image. Steganographic algorithms alter stego pictures, therefore histogram analysis and eye examination are often employed to detect them. Steganography relies on visual inspection to maintain digital content authenticity and privacy. This is possible because it detects and reduces hidden communication routes. Figure 7 shows secret images (Girl, Car, CT scan image) that are used for experimentation. Figure 6, 7, and 8 show histogram of cover images, the secret key images, and their histograms respectively. Figures 9 and 10 show the result obtained by applying chaotic maps using cover images and secret images into cipher images, with their histograms.

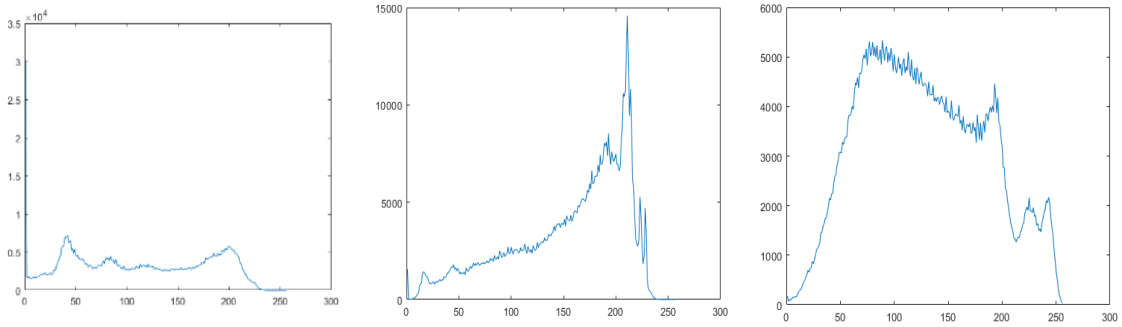


a) Lena. b) Baboon. c) Miramar NAS.

Figure 6. Histogram of cover images.

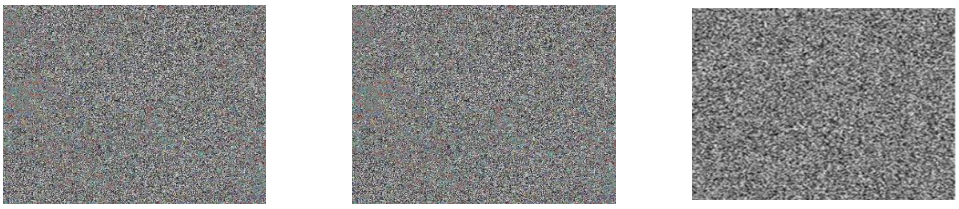
a) Girl. b) Car. c) CT Scan image.

Figure 7. Secret images.



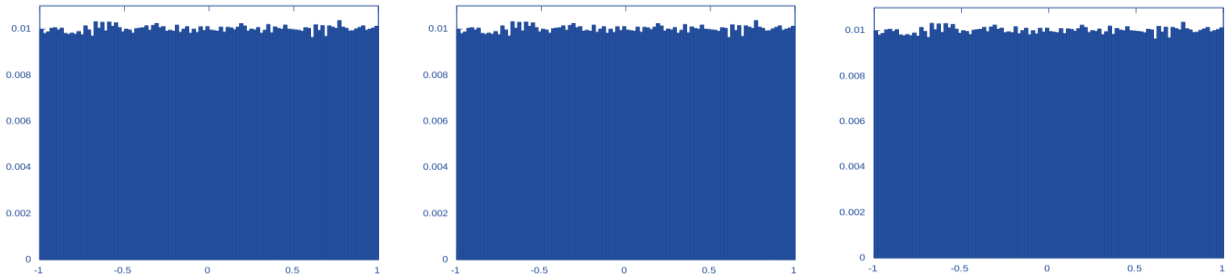
a) Girl. b) Car. c) CT Scan image.

Figure 8. Histogram of secret images.



a) Girl. b) Car. c) CT Scan image.

Figure 9. Histogram of cipher images.



a) Girl. b) Car. c) CT Scan image.

Figure 10. Histogram of stego images.

4.7. Speed Analysis

Speed analysis section examines the swiftness of the proposed cryptosystem and compares it with other cryptosystems for establishing it usecase for a real time system. A range of color photos of 512×512 and 1024×1024 pixels are captured to evaluate the speed of this method. The speed test is conducted on a Windows 10 PC with a 3.40 GHz processor, 4GB of RAM, and an operating system. Image size 1024×1024 results shown in Table 6.

Table 6. Comparison based on speed analysis of encryption and decryption process.

Process type	Ref. [34]	Ref. [35]	Ref. [16]	Proposed approach
Encryption	0.98	1.814	1.254	0.8433
Decryption	1.54	2.014	1.642	1.4387

5. Conclusions

This study presents a novel image steganography technique intended to improve data imperceptibility, data hiding ability, and assault resistance. The suggested approach makes use of chaotic image encryption and decoding to boost security. Chaotic logistic theory-based cryptographic techniques offer a number of fresh and exciting possibilities for creating safe image encryption techniques. Nevertheless, these maps frequently call for particular, arbitrary beginning parameters. The study presents a novel strategy that makes use of an optimization technique for Tabu search to overcome this difficulty. Using a multi-objective fitness function, this algorithm optimizes the chaotic maps' starting parameters. Next, secret keys for picture

encryption are generated using the optimum parameters. The input image is subjected to row- and column-wise diffusion and permutation operations during the encryption process. These processes further mix the image data, making it more challenging to find the hidden information. The main objective of this article is to develop a safe method for encrypting both color and grayscale images. The test results show that 7.9981, 99.8245, 35.6507, and 78.871 are the greatest values of entropy, NPCR, UACI, and PSNR, respectively. Whereas the respective speeds of encryption and decryption increase to 0.8433 and 1.4387 seconds. This novel method offers an effective tool for applications that need secure image steganography.

Acknowledgement

This research was supported by the Deanship of Scientific Research at King Khalid University for funding this work through Research Group Project under grant number RGP.1/96/45

References

[1] Abdullah A., Enayatifar R., and Lee M., "A Hybrid Genetic Algorithm and Chaotic Function Model for Image Encryption," *Aeu-International Journal of Electronics and Communications*, vol. 66, no. 10, pp. 806-816, 2012. DOI:10.1016/j.aeue.2012.01.015

[2] Abed Q. and Al-Jawher W., "An Image Encryption Method Based on Lorenz Chaotic Map and Hunter-Prey Optimization," *Journal Port Science Research*, vol. 6, no. 4, pp. 332-343, 2023. DOI:10.36371/port.2023.4.3

[3] Alanzy M., Alomrani R., Alqarni B., and Almutairi S., "Image Steganography Using LSB and Hybrid Encryption Algorithms," *Applied Sciences*, vol. 13, no. 21, pp. 11771, 2023. DOI:10.3390/app132111771

[4] Alawida M., "A novel Chaos-Based Permutation for Image Encryption," *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 6, pp. 101595, 2023. DOI:10.1016/j.jksuci.2023.101595

[5] Aparna H. and Madhumitha J., "Combined Image Encryption and Steganography Technique for Enhanced Security Using Multiple Chaotic Maps," *Computers and Electrical Engineering*, vol. 110, pp. 108824, 2023. DOI:10.1016/j.compeleceng.2023.108824

[6] Benaissi S., Chikouche N., and Hamza R., "A Novel Image Encryption Algorithm Based on Hybrid Chaotic Maps Using a Key Image," *Optik*, vol. 272, pp. 170316, 2023. DOI:10.1016/j.ijleo.2022.170316

[7] Hossain M., Rahman M., Rahman A., and Islam S., "A New Approach of Image Encryption Using 3D Chaotic Map to Enhance Security of Multimedia Component," *in Proceedings of the International Conference on Informatics, Electronics and Vision*, Dhaka, pp. 1-6, 2014. DOI:10.1109/ICIEV.2014.6850856

[8] Jaradat A., Taqieddin E., and Mowafi M., "A High-Capacity Image Steganography Method Using Chaotic Particle Swarm Optimization," *Security and Communication Networks*, vol. 2021, pp. 1-11, 2021. DOI:10.1155/2021/6679284.

[9] Kaddouri Z. and Omary F., "Application of the Tabu Search Algorithm to Cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 7, 2017. DOI:10.14569/IJACSA.2017.080712

[10] Kalaiarasan D., Ahilan A., and Ramalingam S., "A Harris Hawk Optimization with Chaotic Map Based Image Encryption for Multimedia Application," *Journal of Intelligent and Fuzzy Systems: Applications in Engineering and Technology*, vol. 45, no. 6, pp. 11035-11057, 2023. DOI:10.3233/JIFS-213337

[11] Kaur M. and Kumar V., "Adaptive Differential Evolution-Based Lorenz Chaotic System for Image Encryption," *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 8127-8144, 2018. https://doi.org/10.1007/s13369-018-3355-3

[12] Kaur M., Sandhu M., and Singh S., "A New Hybrid Chaotic System and its Analysis," *International Journal of Advanced Computer Science and Applications*, vol. 23, no. 3, pp. 271-293, 2023. DOI:10.1504/IJICS.2023.10053890

[13] Kaur M., Singh D., Sun K., and Rawat U., "Color Image Encryption Using Non-Dominated Sorting Genetic Algorithm with Local Chaotic Search Based 5D Chaotic Map," *Future Generation Computer Systems-the International Journal of Escience*, vol. 107, pp. 333-350, 2020. DOI:10.1016/j.future.2020.02.029

[14] Kaur M., Singh S., and Kaur M., "Computational Image Encryption Techniques: A Comprehensive Review," *Mathematical Problems in Engineering*, vol. 2021, pp. 1-17, 2021. DOI:10.1155/2021/5012496

[15] Kaur M., Singh S., Kaur M., Singh A., and Singh D., "A Systematic Review of Metaheuristic-based Image Encryption Techniques," *Archives of Computational Methods in Engineering*, vol. 29, no. 5, pp. 2563-2577, 2022. DOI:10.1007/s11831-021-09656-w

[16] Kaur S. and Singh S., "A Digital Steganography Technique Using Hybrid Encryption Methods for Secure Communication," *in Proceedings of the International Conference on Information Technology and Applications*, Lisbon, pp. 481-489, 2023. DOI:10.1007/978-981-19-9331-2_41

[17] Kocak O., Erkan U., Toktas A., and Gao S., "PSO-based Image Encryption Scheme Using Modular

Integrated Logistic Exponential Map," *Expert Systems with Applications*, vol. 237, pp. 121452, 2024. DOI:10.1016/j.eswa.2023.121452

[18] Kumar S. and Sharma D., "Image Scrambling Encryption Using Chaotic Map and Genetic Algorithm: A Hybrid Approach for Enhanced Security," *Nonlinear Dyn*, vol. 112, pp. 12537-12564, 2024. DOI:10.1007/s11071-024-09670-0

[19] Li X., Cho S., and Kim S., "A 3D Image Encryption Technique Using Computer-Generated Integral Imaging and Cellular Automata Transform," *Optik*, vol. 125, no. 13, pp. 2983-2990, 2014. https://doi.org/10.1016/j.ijleo.2013.12.036

[20] Liu H., Zhu Z., Jiang H., and Wang B., "A Novel Image Encryption Algorithm Based on Improved 3D Chaotic Cat Map," *in Proceedings of the 9th International Conference for Young Computer Scientists*, Hunan, pp. 3016-3021, 2008. doi:10.1109/ICYCS.2008.449.

[21] Nguyen T., Arch-int S., and Arch-int N., "An Adaptive Multi Bit-Plane Image Steganography Using Block Data-Hiding," *Multimedia Tools and Applications*, vol. 75, no. 14, pp. 8319-8345, 2016. DOI:10.1007/s11042-015-2752-9

[22] Rajagopalan S., Sharma S., Arumugham S., Upadhyay H., Rayappan J., and Amirtharajan R., "YRBS Coding with Logistic Map-A Novel Sanskrit Aphorism and Chaos for Image Encryption," *Multimedia Tools and Applications*, vol. 78, no. 8, pp. 10513-10541, 2019. DOI:10.1007/s11042-018-6574-4

[23] Rashid A. and Hussein K., "Image Encryption Algorithm Based on the Density and 6D Logistic Map," *International Journal of Electrical Computer Engineering*, vol. 13, no. 2, pp. 1903, 2023. DOI:10.11591/ijece.v13i2.pp1903-1913

[24] Rezaei B., Ghanbari H., and Enayatifar R., "An Image Encryption Approach Using Tuned Henon Chaotic Map and Evolutionary Algorithm," *Nonlinear Dyn*, vol. 111, no. 10, pp. 9629-9647, 2023. DOI:10.1007/s11071-023-08331-y

[25] Sameh S., Moustafa H., AbdelHay E., and Ata M., "An Effective Chaotic Maps Image Encryption Based on Metaheuristic Optimizers," *The Journal of Supercomputing*, vol. 80, no. 1, pp. 141-201, 2024. DOI:10.1007/s11227-023-05413-x

[26] Sandhu M. and Singh S., "Review of Image Encryption and Compression Techniques," *in Proceedings of the 5th Scientific Conference for Electrical Engineering Techniques Research*, Mohali, pp. 040006, 2022. DOI:10.1063/5.0108517

[27] Sandhu M., Singh S., and Kaur M., "A New Hybrid Chaotic System and its Analysis," *International Journal of Electrical Computer Engineering*, vol. 23, no. 3, pp. 271-293, 2024. DOI:10.1504/IJICS.2024.138493

[28] Sandhu M., Singh S., and Kaur M., "Efficient Permutation and Diffusion Model based on TCMT for Image Encryption," *in Proceedings of the 2nd International Conference on Intelligent Technologies*, Hubli, pp. 1-8, 2022. DOI:10.1109/CONIT55038.2022.9848007

[29] Shao S., Li J., Shao P., and Xu G., "Chaotic Image Encryption Using Piecewise-Logistic-Sine Map," *IEEE Access*, vol. 11, pp. 27477-27488, 2023. DOI:10.1109/ACCESS.2023.3257349

[30] Sreelaja N. and Pai G., "Stream Cipher for Binary Image Encryption Using Ant Colony Optimization Based Key Generation," *Applied Soft Computing*, vol. 12, no. 9, pp. 2879-2895, 2012. DOI:10.1016/j.asoc.2012.04.002

[31] Wang X. and Yang L., "A Novel Chaotic Image Encryption Scheme Based on Magic Cube Permutation and Dynamic Look-Up Table," *International Journal of Modern Physics B*, vol. 26, no. 29, pp. 1250139, 2012.

[32] Wu X., Kurths J., and Kan H., "A Robust and Lossless DNA Encryption Scheme for Color Images," *Multimedia Tools and Applications*, vol. 77, no. 10, pp. 12349-12376, 2018. DOI:10.1007/s11042-017-4885-5

[33] Xiang H. and Liu L., "An Improved Digital Logistic Map and its Application in Image Encryption," *Multimedia Tools and Applications*, vol. 79, no. 41-42, pp. 30329-30355, 2020. DOI:10.1007/s11042-020-09595-x

[34] Yang Y., Wang B., Zhou Y., Shi W., and Liao X., "Efficient Color Image Encryption by Color-Grayscale Conversion Based on Steganography," *Multimedia Tools and Applications*, vol. 82, no. 7, pp. 10835-10866, 2023. DOI:10.1007/s11042-022-13689-z.

[35] Yao J., Yang H., Jiang D., Yan B., Pan J., and Wang M., "A Novel Quantum Image Steganography Algorithm Based on Double-Layer Gray Code," *International Journal of Theoretical Physics*, vol. 62, no. 3, pp. 52, 2023. DOI:10.1007/s10773-023-05303-1

[36] Zarebnia M., Pakmanesh H., and Parvaz R., "A fast Multiple-Image Encryption Algorithm Based on Hybrid Chaotic Systems for Gray Scale Images," *Optik*, vol. 179, pp. 761-773, 2019. DOI:10.1016/j.ijleo.2018.10.025

[37] Zhang X., Wang L., Zhou Z., and Niu Y., "A Chaos-Based Image Encryption Technique Utilizing Hilbert Curves and H-Fractals," *IEEE ACCESS*, vol. 7, pp. 74734-74746, 2019. DOI:10.1109/ACCESS.2019.2921309

[38] Zhou Y. and Agaian S., "Image Encryption Using the Image Steganography Concept and PLIP Model," *in Proceedings of the International Conference on System Science and Engineering*, Macau, pp. 699-703, 2011. DOI:10.1109/ICSSE.2011.5961993

Mandeep Sandhu is serving as an Assistant Professor, Department of Computer Science, Guru Nanak Dev University College, Pathankot and has teaching experience of 16 years. She has completed her Ph.D. from the Department of Computer Science and Engineering, Chandigarh University, Mohali in the field of Image Processing. She is a distinguished expert in the fields of image encryption, AI and cybersecurity. With a robust publication record exceeding 25 articles in prestigious national and international journals, 2 book chapters and one National Patent to her credit.

Mohammad Ahmed is working as an Assistant Professor in the Department of Computer Science, King Khalid University, Saudi Arabia, Abha. He has published several papers in, SCI indexed journal, SCOPUS, Web of Science, and in many conferences. He is having around more than 8 years of experience in teaching and Software industry. He is Cloud Certified, Java Certificate, Oracle Developer Certified and Big Data Certified. His area of interest is Bigdata, Machine Learning, Web Security, Object Oriented Programming, and Cloud Computing.

Mohammad Hussain Assistant Professor, Department of Business Informatics, College of Business, King Khalid University, Abha, Kingdom of Saudi Arabia, received his Master of Technology degree from the Department of Computer Science Engineering, Anna University, Chennai, India. After that he obtained his PhD degree from Bihar University, India. He was an Associate Professor in the Department of Computer Science Engineering, ABESIT Ghaziabad, India. He is currently working as an Assistant Professor in the department of Business Informatics, King Khalid University, Abha, Saudi Arabia. His research interests include Computer Networks, Information Technology, Artificial Intelligence, Machine Learning, IoT, and Operation Research.

Surender Singh is the Head of Career Programs at CodeQuotient Pvt. Ltd., Mohali, with over 27 years of teaching and administrative experience. He previously served as a Professor at Chandigarh University and holds a PhD in Digital Image Processing from UPES, Dehradun. He has published 90+ research papers, with expertise in Software Engineering, Machine Learning, and Computer Vision. Professor Singh is a certified Microsoft Networking Specialist and a Stanford Machine Learning professional, and has played key roles in academic committees and accreditation processes like IQAC, NAAC, and NBA.

Imran Khan graduated with a bachelor's degree in Computer Science from the K.N. Modi Institute of Engineering and Technology in India in 2009 and a Master's Degree in computer networks from Sheffield Hallam University in the United Kingdom in 2012. He is currently employed by King Khalid University in Abha as a Lecturer in the Computer Engineering Department. Developing Novel Approaches to improve DDoS Attack Detection, Software-Defined Networks, Intrusion Detection Systems, Cyberthreats, and Machine Learning are some of his research interests.