

# An image steganography using improved hyper-chaotic Henon map and fractal Tromino

Shyla Nagarajegowda, Kalimuthu Krishnan

Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Kattankulathur, India

## Article Info

### Article history:

Received May 9, 2023

Revised Jun 28, 2023

Accepted Jul 3, 2023

### Keywords:

Hyper-chaotic improved Henon map

Integer wavelet transform

Integer wavelet transform

Least significant bit

Steganography image

## ABSTRACT

Steganography is a vital security approach that hides any secret content within ordinary data, such as multimedia. First, the cover image is converted into a wavelet environment using the integer wavelet transform (IWT), which protects the cover images from false mistakes. The grey wolf optimizer (GWO) is used to choose the pixel's image that would be utilized to insert the hidden image in the cover image. GWO effectively selects pixels by calculating entropy, pixel intensity, and fitness function using the cover images. Moreover, the secret image was encrypted by utilizing a proposed hyper-chaotic improved Henon map and fractal Tromino. The suggested method increases computational security and efficiency with increased embedding capacity. Following the embedding algorithm of the secret image and the alteration of the cover image, the least significant bit (LSB) is utilized to locate the tempered region and to provide self-recovery characteristics in the digital image. According to the findings, the proposed technique provides a more secure transmission network with lower complexity in terms of peak signal-to-noise ratio (PSNR), normalized cross correlation (NCC), structural similarity index (SSIM), entropy and mean square error (MSE). As compared to the current approaches, the proposed method performed better in terms of PSNR 70.58% Db and SSIM 0.999 respectively.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



## Corresponding Author:

Kalimuthu Krishnan

Department of Electronics and Communication Engineering, SRM Institute of Science and Technology

Kattankulathur, India

Email: kalimutk@srmist.edu.in

## 1. INTRODUCTION

Technology has blitz scaled over the past years leading to wide usage of multimedia for transferring data, especially the internet of things (IoT) [1]. However, today, numerous attackers and hackers can intercept communications using some strategies, therefore protecting transmissions is still required to ensure information security [2]. Steganography is an important technology for secret information that can be disseminated across open networks [3]. The purpose of image steganography is to incorporate secret data while preventing its existence in personal communication [4]. The stego image is created by embedding the secret data in the carrier image, and one of the main goals of image steganography is to reduce the difference between the stego and carrier images [5]. Image steganography successfully extracts personal information and achieves error-free recovery of the original image containing secret information [6], [7]. Image steganography is primarily utilized to reconstruct the original image without distortion in medical, military, and other domains [8]. Image steganography has advantages like maintaining secret information content [9] and hiding transmission with more security [10] and privacy [11].

Steganography employs machine learning (ML) [12] and deep learning (DL) [13] approaches to increase hiding capacity, robustness, and security, that performed together in stego image to human vision [14], [15]. Ahmad *et al.* [16] created an enhanced medical image steganography technique to hide patients' information in their medical images. However, the proposed techniques for integrating the system within the medical cover image may not guarantee to give a decent better image. Rahman *et al.* [17] implemented a least significant bit (LSB) substitution method to accomplish the consistency between the basic measures of steganography images. However, LSB contains an unacceptably large number of embedding messages, resulting in increased processing costs and poor image quality. Durafe *et al.* [18] designed a hybrid steganography scheme based on the fractal cover, integer wavelet transform (IWT), singular value decomposition (SVD) and discrete wavelet transform (DWT) approaches for hiding the data. However, the information will not be changed since changing the single value elements directly will affect the image's lighting. Lin *et al.* [19] created a steganography structure for neural style transmission by presenting the Y channel data to avoid steganographic attacks. However, the planned Y-channel still requires a big space for optimization. Liu *et al.* [20] created a mapping module to increase the quality of the steganography image and its antidetection capabilities. However, the mapping module has different networks for encoding and decoding, which caused resulted in color distortion and artefacts in stego images. After examining every accessible framework, it is clear that traditional approaches are less secure because it is merely a matter of determining whether the secret message is present or not. Since a statistical method was employed to embed the data, the hidden message may be simply recovered. The stego image must be sent to the receiving end across an untrusted channel in order to implement the trained model for carrying out steganography and steganalysis. Images produced by the trained model contains noise, skewing, and blurring. Consequently, it is yet undefined whether to implement the model for image steganography. In order to overcome the above-stated issue, the major contributions are given below.

- The hyper-chaotic improved Henon map and fractal Tromino is developed to enhance the embedding capacity, computing efficiency and security.
- The grey wolf optimizer (GWO) is used to choose the image pixels that would be utilized to integrate the hidden image in the cover image.
- The least significant bit is used to locate the tempered region and to deliver self-recovery features in the digital image.

The overall organization of this study is given as follows: the process of the proposed method is described in section 2. Section explains the steps involved in improved Henon map. Section 4 describes the experimental results of the proposed and existing models. The conclusion of this research is given in section 5.

## 2. PROPOSED METHOD

Figure 1 depicts the workflow of the proposed image steganography, and comprehensive explanations of the suggested method are described below. In recent years, technology like video, audio, text, and image were low in complexity and cost-effective. Furthermore, the expediency of image processing implements data transfer, which was a relatively simple way to view and download digital images. An image steganography technique was presented in this study to increase data transmission security. Here, in this block, there are two stages are presented, (i.e.,) transmitter side and receiver side. Initially, the stego image is transferred to receiver side through the channel. Therefore, the stego image is mentioned twice in the block diagram. After passing through it, the same stego image is processed with lifting wavelet transform (LWT) for dividing the images into various sub-bands. Due to that divisions, the security level gets increased in that image.

### 2.1. Collection of images

Steganography involves two types of images in image collections: hidden images and cover images, which are utilized to get better accuracy. The cover image was used to insert the hidden image, to get a noiseless image and a suitable size. MATLAB is used to represent the hidden secret image to cover the image.

### 2.2. Encryption scheme

After collecting the MATLAB images, encryption was used to modify the secret image. It works by encoding through the use of cryptographic images. Decoding the data requires the usage of a decryption tool and string values.

- Step 1: To split and load the channels, the red, green and blue (RGB) for secret images was required.
- Step 2:  $k_1$  and  $k_2$  are the keys introduced and L- shaped fractal Tromino is evaluated using the article by utilizing the procedure.
- Step 3: The 3-fractional Tromino was XORed with the image of particular parts

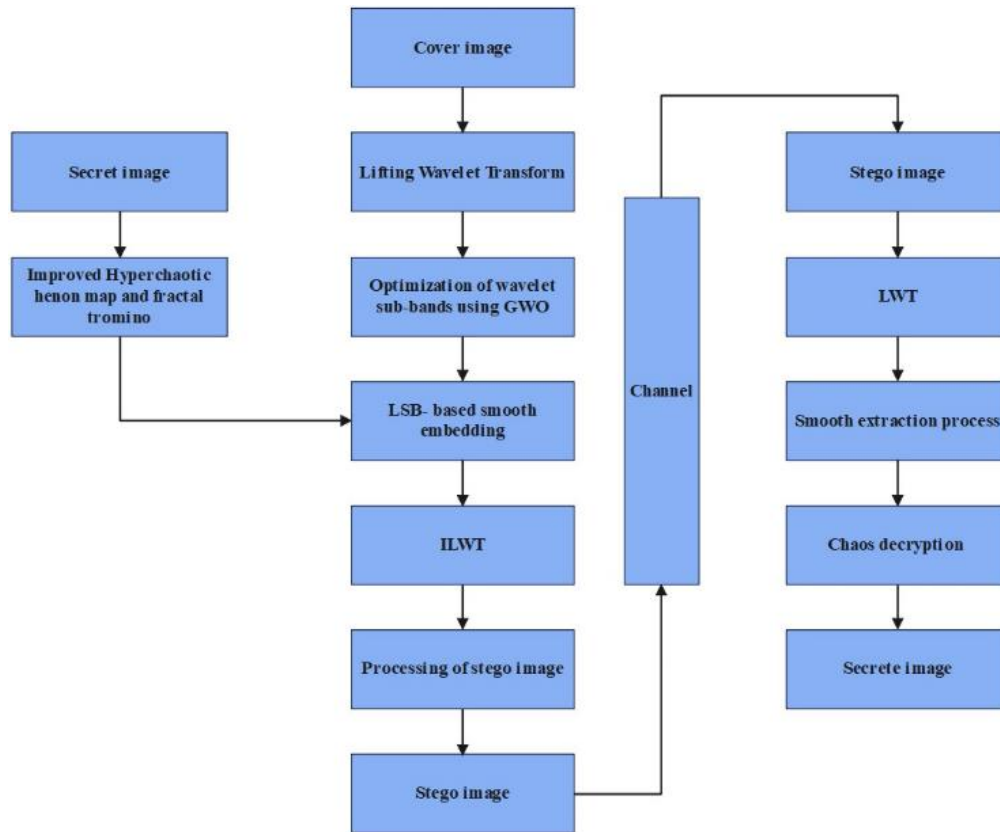


Figure 1. Workflow of the proposed method

### 2.3. Fractal Tromino

The encrypted image is given to fractal Tromino to achieve the most fundamental characteristics of steganography between confusion and diffusion matrix [21]. For confusion matrix, it has highly pre-defined and non-linear data to process [22]. The dimension  $M \times 3$  matrix of  $N$  was evaluated where  $M \times N \times 3$  is the dimension of the plain image. The length of 8-bits was utilized by producing two random keys  $K1$  and  $K2$ . By using the following rule in (1), the matrix values are generated in step 1.

$$R(ii, jj) = \begin{cases} \text{mod}(jj, ff) \text{ iff } \text{mod}(ii, k_2 \times c) < k_1 \times c \text{ mod}(ii, ff) \\ \text{iff } \text{mod}(jj, k_2 \times c) > k_1 \times c \text{ mod}(c - ii, c) \end{cases} \text{ otherwise} \quad (1)$$

where  $c$  was evaluated by utilizing (2).

$$c = \sqrt{(255 - m) \times m} \quad (2)$$

The range of  $c$  is curved in adjacent value, where  $m$  in (2) is the matrix generated in step 1 for mean value. The updated matrix in stage 3 was redesigned  $M \times N \times 3$ . This is the preferred fractal Tromino. The evaluated fractal has represented in the Figure 1.

### 3. IMPROVED HENON MAP

After fractal Tromino, the improved Henson map was also encrypted with a secret image and showed the most significant chaotic characteristics. However, the two-dimensional chaotic Henon map (2D-CHM) has some drawbacks like discontinuous chaotic intervals and simple chaotic characteristics [23]. To overcome the above limitations, 2D-CHM to two-dimensional improved chaotic Henon map (2D-ICHM) was suggested and the mathematical expressions were shown in (3). Where  $a$  and  $b$  are control parameters.

$$\{x(n + 1) = \cos(1 - ax(n)^2 + by(n)^2), y(n + 1) = \sin \sin(x(n)^2) \quad (3)$$

### 3.1. Lifting wavelet transform

The input secret image is given to the LWT to disguise the image multi-scale analysis for signals and purposes by scaling operations. Hence, it is used for image compression and processing [24]. Furthermore, the lifting wavelet transform constants are floating points and it is difficult to evaluate [25]. As the basics of lifting wavelet transform, it can be separated into three stages: prediction, update, and splitting which are demonstrated below.

- Splitting: Normally, the unique signal  $S$  was decayed by the odd signal  $S_{2jj+1}$  and even signal  $S_{2j}$ .
- Prediction: The odd signal  $S_{2jj-1}$ , remains unchanged while the even signal is  $S_{2jj+1}$  was projected by interpolation subdivisions. The transformation between the actual and predicted value is  $d_{jj}$  that has shown in (4),

$$d_{jj} = S_{2jj} + 1 - (S_{2jj}) \quad (4)$$

where  $P$  is represented as a prediction mechanism.

- Update: The update process is the data  $s_{2jj}$  with  $d_{jj}$  to preserve some characteristics of the original signal  $S$ . Then keeping the average value unchanged, and the operations were described in (5).

$$a_{jj} = S_{2jj} + (d_{jj}) \quad (5)$$

where  $U$  is the prediction operator.

### 3.2. Wavelet sub-bands using grey wolf optimization

The lifting wavelet transform is given to the suggested method to choose the embedding process in the optimal block. The GWO [26] can be classified into three segments hunting, attacking prey and encircling [27]. At the initial stage, GWO parameters were modified such as search agents  $G_s$ , variable size  $G_d$ , and the maximum number of iterations  $iterma$ , and vectors were described in (6) and (7).

$$A^{\rightarrow} = 2a^{\rightarrow} \cdot rand1 - a^{\rightarrow} \quad (6)$$

$$C^{\rightarrow} = 2 \cdot rand2 \quad (7)$$

where,  $rand1$  and  $rand2$  was described as random vectors between the ranges [0,1]. The generated arbitrarily of wolves based on the package was determined in (8). The initial range of the  $j^{th}$  pack of the  $i^{th}$  wolves can be represented by  $G_1$ . The fitness value utilization of each value was calculated in (9) and (10).

$$Wolves = [G_1^1 G_2^1 G_3^1 G_1^2 G_2^2 G_3^2 \cdot G_1^{G_s} \cdot G_2^{G_s} \cdot G_3^{G_s} \dots G_{G_d-1}^1 G_{G_d}^1 \dots G_{G_d-1}^2 G_{G_d}^2 \dots \dots \cdot G_{G_d-1}^{G_s} \cdot G_{G_d}^{G_s}] \quad (8)$$

The initial range of the  $j^{th}$  pack of the  $i^{th}$  wolves can be represented by  $G_j^1$ .

$$\vec{D} = |\vec{C} \cdot \vec{G}_p(t) - \vec{G}(t)| \quad (9)$$

$$\vec{G}(t+1) = \vec{G}_p(t) - \vec{A} \cdot \vec{D} \quad (10)$$

Based on the equations,  $C^{\rightarrow}$  and  $A^{\rightarrow}$  was act as coefficient vectors.  $G^{\rightarrow}$  act as the position vector of a grey wolf and  $G^{\rightarrow}$  act as a position vector of the prey. Demonstrate the better hunt agents  $G\alpha$ , Second and the third hunt agents  $G\beta$  and  $G\delta$  by utilizing (11)-(16).

$$\vec{D}_\alpha = |\vec{C}_1 \cdot \vec{G}_\alpha - \vec{G}| \quad (11)$$

$$\vec{D}_\beta = |\vec{C}_2 \cdot \vec{G}_\beta - \vec{G}| \quad (12)$$

$$\vec{D}_\delta = |\vec{C}_3 \cdot \vec{G}_\delta - \vec{G}| \quad (13)$$

$$\vec{G}_1 = \vec{G}_\alpha - \vec{A}_1 \cdot (\vec{D}_\alpha) \quad (14)$$

$$\vec{G}_2 = \vec{G}_\beta - \vec{A}_2 \cdot (\vec{D}_\beta) \quad (15)$$

$$\vec{G}_3 = \vec{G}_\delta - \vec{A}_3 \cdot (\vec{D}_\delta) \quad (16)$$

$G\alpha$ ,  $\beta$  and  $G\delta$  values are updated. The possible outcomes can be taken by utilizing the best values  $G\alpha$ ,  $\beta$  and  $G\delta$ . The ending values can be checked, whether the *Iteration* reaches *Iterationmax* or not, if else again go to step 5 or if yes, print the current best value. Hence, LSB [28] was utilized to hide the cover image after encryption. Then, LWT was smoothly embedded and used for processing the stego image for the cover image. The position was updated to the existing hunt agent by using (17). The fitness for hunt ranges was utilized in (18).

$$\vec{G}(t+1) = \frac{G_1 + G_2 + G_3}{3} \quad (17)$$

$$Fitness = \sum_{i=1}^n G_{ii}^2 \quad (18)$$

### 3.3. Decryption phase

The decryption phase was used to process the embedding secret image for cover image transformation, where the embedding process of LSB was utilized as integer unit values. The binary values are then converted to decimal points, LWT is applied to the output image, and the decimals are represented as stego images. Hence, the secret image was extracted without no loss of data, therefore, the retained secret image has the original secret image.

## 4. RESULTS AND DISCUSSION

Here in this section, the experimental results of the proposed method were analyzed using MATLAB. For evaluating the system, the following system specifications was essential such as 8 GB RAM, 3 TB storage, and i9 3.0 GHZ processor. The suggested method performances were authenticated in terms of peak signal-to-noise ratio (PSNR), normalized cross correlation (NCC), structural similarity index (SSIM), entropy, mean average error (MAE), and mean square error (MSE) values.

### 4.1. Quantitative analysis for color image

The quantitative analysis is given to the color image, which was used for the image steganography process. Figures 2 and 3 show the color vision of the sample image 1 and sample image 2. In the Figures 2 and 3, the following images (i.e.), Figures 2(a) and 3(a) cover image, Figures 2(b) and 3(b) secret image, Figures 2(c) and 3(c) encrypted image, Figures 2(d) and 3(d) Fractal Tromino, Figures 2(e) and 3(e) stego image, Figures 2(f) and 3(f) reconstructed secret image, and Figures 2(g) and 3(g) decrypted secret image are displayed correspondingly.

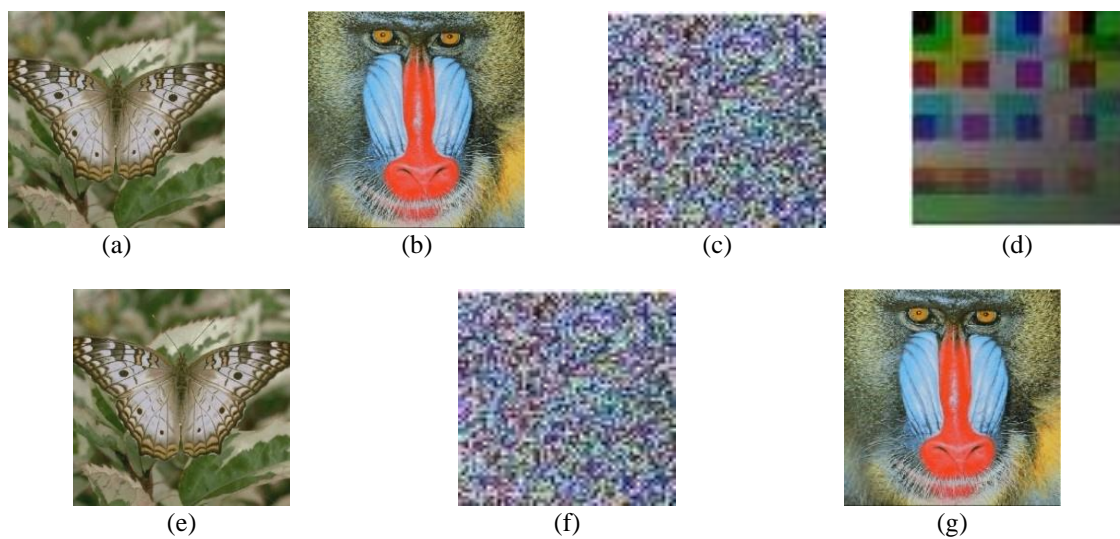


Figure 2. Representation of color images for sample image 1 (a) cover image, (b) secret image, (c) encrypted image, (d) fractal Tromino, (e) stego image, (f) reconstructed secret image, and (g) decrypted secret image

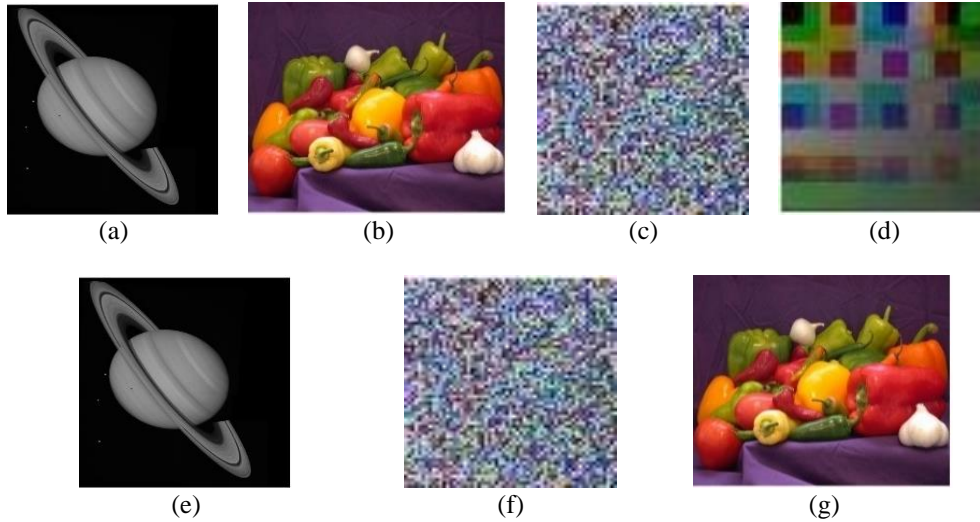


Figure 3. Representation of color images for sample image 2 (a) cover image, (b) secret image, (c) encrypted image, (d) fractal Tromino, (e) stego image, (f) reconstructed secret image, and (g) decrypted secret image

The quantitative analysis was used for statistical, mathematical, and measurement to understand the characteristics for performing in numerical values. Table 1 describes the features of suggested steganography for images. Furthermore, the performance evaluation was carried out in five conditions.

Table 1 describes the performance analysis of color images for SSIM, PSNR, NCC, Entropy, and MSE. In the color image, butterfly as cover image and baboon as secret image achieved PSNR of 69.11 and 40.58, SSIM of 0.999 and 0.999, NCC of 0.985 and 0.972, Entropy of 6.532 and 6.51, and MSE of 0.134 and 0.064 respectively. For the histogram equalization, PSNR, SSIM, NCC, entropy, and MSE of 69.15 dB, 0.956, 0.925, 6.325, and 0.104 respectively in the cover image. Similarly, for the secret image, PSNR as 43.47 dB, SSIM as 0.978, NCC as 0.97, entropy as 6.285 and MSE as 0.134 respectively. The analysis of MAE for color image was illustrated in Tables 2. To prove the embedding capacity of the secret image, Table 3 shows the analysis of secret image (Baboon) with different sizes such as  $16 \times 16$ ,  $32 \times 32$ ,  $64 \times 64$ ,  $128 \times 128$  in terms of PSNR, SSIM, NCC, entropy and MSE.

Table 1. Performance analysis for color image for SSIM, PSNR, NCC, MSE, entropy and MAE

Color Images	Performance measure	Normal	Histogram equalization	Noise attacks	
				SP noise 5%	Gaussian 5%
Butterfly as cover image	PSNR (dB)	69.11	69.15	42.25	42.24
	SSIM	0.999	0.956	0.80	0.83
	NCC	0.985	0.925	0.86	0.85
	Entropy	6.532	6.325	3.34	3.11
	MSE	0.134	0.104	1.15	1.22
Baboon as secret image	PSNR (dB)	40.58	43.47	36.06	39.07
	SSIM	0.999	0.978	0.75	0.71
	NCC	0.972	0.97	0.79	0.68
	Entropy	6.51	6.285	5.30	5.31
	MSE	0.064	0.134	0.95	0.94

Table 2. Analysis of MAE for color images

Color Images	MAE		
	R	G	B
Butterfly as cover image	84.25	87.63	82.99
Baboon as secret image	89.96	85.86	85.50

**4.1.1. Encryption quality**

The analysis of encryption quality for color image was tabulated in Tables 4. After encryption, the pixels of cover image change have greater image pixels, and overall encryption quality (*EEElty*). As a result, the encryption quality can be expressed as the overall alteration of image pixels in both plain and ciphered images. It can be described as an average amount of changes to each grey level. Let *Hp* described the amount



of pixels has  $jj$  gray levels in the  $ii^{th}$  plain image and  $He$  described the amount of  $ii, jj$  pixels has  $jj$  gray levels in the  $ii^{th}$  encrypted image. Then, it gives the results as  $jj = (0, 1, 2, 3, \dots, 255)$  and  $ii = (1, 2, 3)$  in the encryption efficiency of a color image can be explained in (19).

$$Qty = \frac{\sum_{i=1}^3 \sum_{j=0}^{255} |H_{i,j}^p - H_{i,j}^e|}{3 \times 256} \quad (19)$$

Table 3. Analysis of secret image with different sizes

Color image	Metrics	16×16	32×32	64×64	128×128
Baboon as secret image	PSNR (dB)	40.98	43.42	40.58	41.13
	SSIM	0.975	0.981	0.999	0.97
	NCC	0.972	0.965	0.972	0.987
	Entropy	5.879	5.35	6.51	5.97
	MSE	0.0987	0.145	0.064	0.114

Table 4. Analysis of encryption quality for color images

Methods	Encryption quality
Butterfly as cover image	893.93
Baboon as secret image	970.97

#### 4.1.2. Quantitative analysis for greyscale image

The quantitative analysis given to the greyscale image was used for image steganography process. Figures 4 and 5 show the representation as greyscale images 1 and 2 respectively. From Figures 4 and 5, the following images such as Figures 4(a) and 5(a) cover image, Figures 4(b) and 5(b) secret image, Figures 4(c) and 5(c) encrypted image, Figures 4(d) and 5(d) fractal Tromino, Figures 4(e) and 5(e) embedded image, Figures 4(f) and 5(f) reconstructed secret image, Figures 4(g) and 5(g) decrypted secret images are displayed correspondingly. Figure 6 shows the representation of pixel values using proposed method.

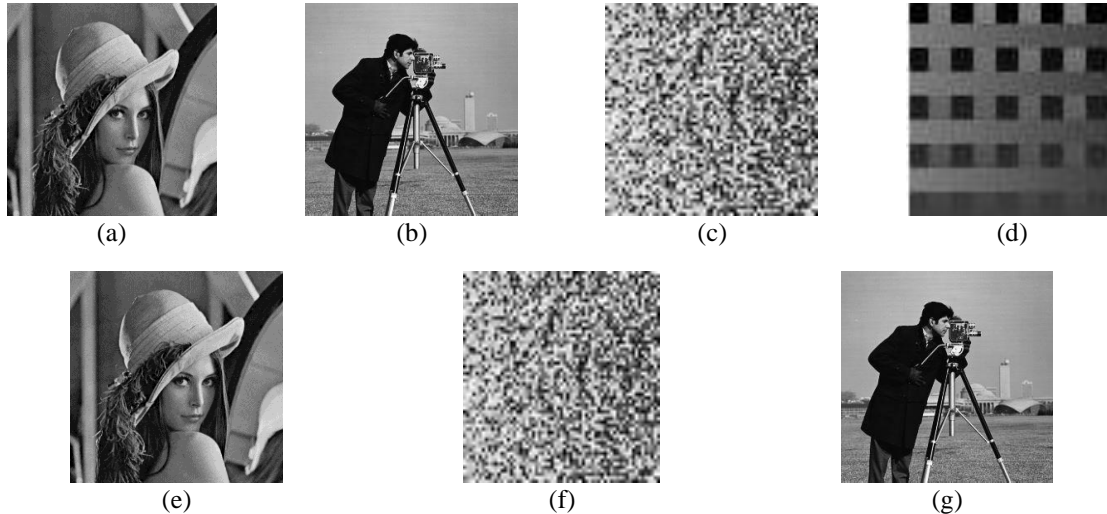


Figure 4. Representation of greyscale image 1 for (a) cover image, (b) secret image, (c) encrypted image, (d) fractal Tromino, (e) embedded image, (f) reconstructed secret image, and (g) decrypted secret image

Table 5 describes the performance analysis of greyscale image for SSIM, PSNR, NCC entropy, unified average changed intensity (UACI) and MAE. In greyscale images, Lena as the cover image and the cameraman as secret image achieved PSNR of 65.58 and 66.58, SSIM of 0.97 and 0.90, NCC of 0.98 and 0.99, entropy of 6.69 and 7.65, UACI of 32.66 and 51.81 and MAE achieved 85.79 and 85.65 respectively. Additionally, the suggested system obtained better results in the condition of network lifetime, throughput, delay, energy consumption and packet delivery ratio respectively. Table 6 illustrated the encryption quality analysis of greyscale images achieved Lena as cover image achieved 902.86 and Cameraman as secret image achieved 918.93 respectively.

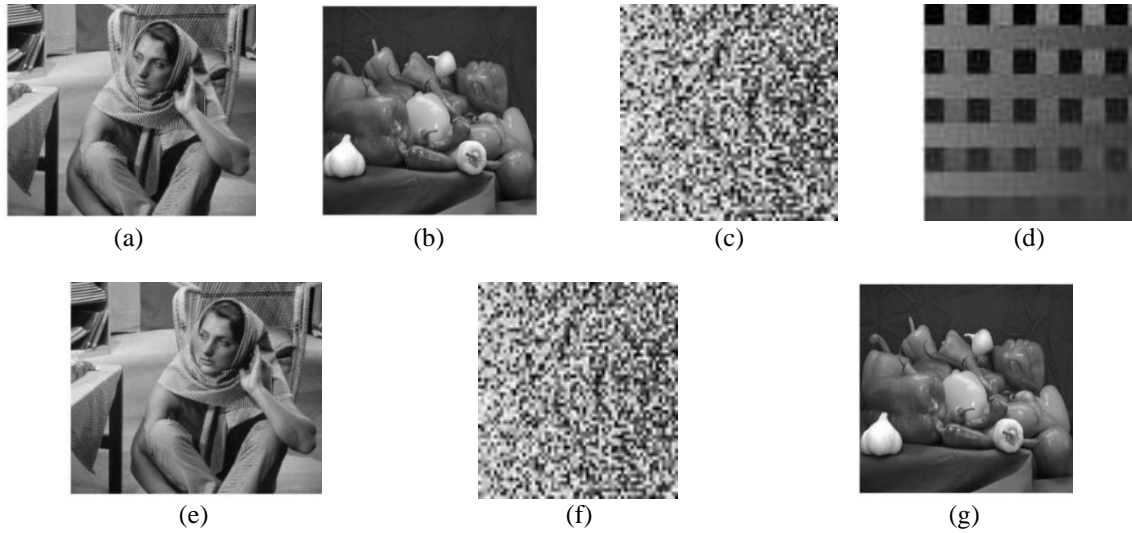


Figure 5. Representation of greyscale image 2 for (a) cover image, (b) secret image, (c) encrypted image, (d) fractal Tromino, (e) embedded image, (f) reconstructed secret image, and (g) decrypted secret image

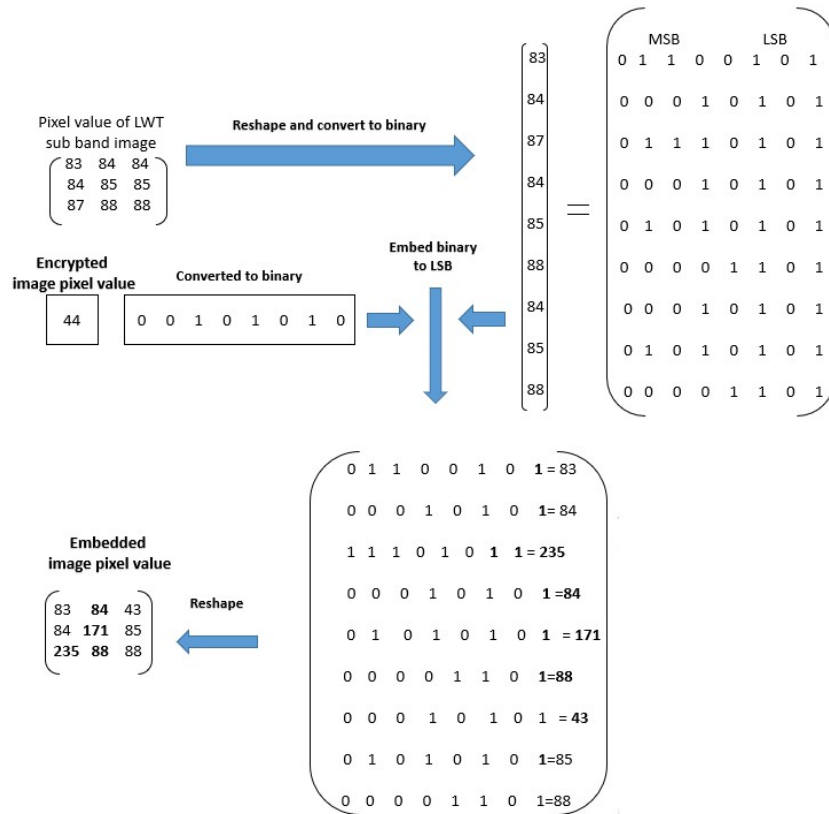


Figure 6. Representation of pixel values using proposed method

#### 4.2. Comparative analysis

Here, in this section, Table 6 illustrated the encryption quality analysis of greyscale images achieved Lena as cover image achieved 902.86 and Cameraman as secret image achieved 918.93 respectively. Further, the proposed method is analyzed with state-of-the-art methods (different encryption techniques) such as Henon map, logistic map and baker’s map which is tabulated in Table 7. From the Table 7, it clearly shows that proposed method outperforms the state-of-the-art methods in terms of PSNR (40.98%), SSIM (0.97), NCC (0.97), entropy (5.87) and MSE (0.09).



Table 5. Performance analysis of greyscale image for SSIM, PSNR, NCC, and MSE

Gray scale Images	Performance measure	Normal	Histogram equalization	Noise attacks	
				SP noise 5%	Gaussian 5%
Lena as cover image	PSNR (dB)	65.58	52.28	43.08	43.08
	SSIM	0.97	0.96	0.85	0.85
	NCC	0.98	0.99	0.79	0.79
	Entropy	6.69	7.44	4.35	4.35
	UACI (%)	32.66	33.46	29.46	24.46
	MAE	85.79	75.98	84.25	77.25
Cameraman as secret image	PSNR (dB)	66.58	69.76	35.32	35.32
	SSIM	0.90	0.98	0.88	0.88
	NCC	0.991	0.94	0.76	0.80
	Entropy	7.65	7.87	5.19	5.19
	UACI (%)	51.81	33.46	30.37	30.37
	MAE	85.65	71.79	50.66	51.67

Table 6. Encryption quality analysis of greyscale images

Methods	Encryption quality
Lena as the cover image	902.86
Cameraman as secret image	918.93

Table 7. Comparison with state-of-the-art methods

Stats of art methods	PSNR (dB)	SSIM	NCC	Entropy	MSE
Henon map	38.56	0.90	0.92	4.63	0.14
Logistic map	32.67	0.81	0.83	3.98	0.45
Baker's map	29.01	0.72	0.73	2.73	0.98
Proposed method	40.98	0.97	0.97	5.87	0.09

Followed by that, the comparative analysis of the existing and proposed work was described in Table 8. Subramanian *et al.* [1] designed deep learning techniques which achieved a PSNR value of 64.7% respectively. Rustad *et al.* [8] implemented a least significant bit which achieved a PSNR value of 57.45% and SSIM of 0.999 respectively. Ahmad *et al.* [16] suggested medical images to hide the patient's data which achieved 59.50% and SSIM of 0.939 which are shown in Table 8 respectively.

Table 8. PSNR and SSIM values for comparative analysis

Methods	PSNR	SSIM
Subramanian - DL technique (2021)	64.7	-
Rustad - LSB method (2022)	57.45	0.999
Ahmad - EMIS technique (2022)	59.50	0.939
Proposed method	70.58	0.999

From the Table 8, it clearly shows that proposed method outperforms the existing methods in terms of PSNR (70.58) and SSIM (0.999) respectively. When compared to the existing methods, the proposed technique is efficiently avoiding the loss of data and gained the least computational time. Additionally, classifying the optical data of multiple factors was a critical challenge in image steganography which is efficiently solved by the GWO.





## 5. CONCLUSION

In this research, a GWO and IWT were utilized for real-time applications that have highly secured data transmission of network structure in digital images. Additionally, a hyper-chaotic map was utilized to guarantee the integrity and privacy of information in the secret image. For inserting the secret information in the cover image, LSB was utilized to hide the secret image. After the process of the embedding system, a hyper-chaotic Henson map was used with the cover image to get the secret image. The suggested scheme evaluated the feature measures such as SSIM, PSNR, MSE, and NCC. As compared to the existing approaches, the proposed method performed better in terms of PSNR 70.58% Db and SSIM 0.999 respectively. In the future, a new optimization technique can be combined with an improved Henon map to improve the image steganography performance.





## REFERENCES

- [1] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image steganography: a review of the recent advances," *IEEE Access*, vol. 9, pp. 23409–23423, 2021, doi: 10.1109/ACCESS.2021.3053998.
- [2] K. Ding *et al.*, "A novel steganography method for character-level text image based on adversarial attacks," *Sensors*, vol. 22, no. 17, Aug. 2022, doi: 10.3390/s22176497.
- [3] M. K. Shyla, K. B. S. Kumar, and R. K. Das, "Image steganography using genetic algorithm for cover image selection and embedding," *Soft Computing Letters*, vol. 3, Dec. 2021, doi: 10.1016/j.socl.2021.100021.
- [4] H. Ye, K. Su, X. Cheng, and S. Huang, "Research on reversible image steganography of encrypted image based on image interpolation and difference histogram shift," *IET Image Processing*, vol. 16, no. 7, pp. 1959–1972, May 2022, doi: 10.1049/ipr2.12461.
- [5] P. Pan, Z. Wu, C. Yang, and B. Zhao, "Double-matrix decomposition image steganography scheme based on wavelet transform with multi-region coverage," *Entropy*, vol. 24, no. 2, Feb. 2022, doi: 10.3390/e24020246.
- [6] A. AbdelRaouf, "A new data hiding approach for image steganography based on visual color sensitivity," *Multimedia Tools and Applications*, vol. 80, no. 15, pp. 23393–23417, Jun. 2021, doi: 10.1007/s11042-020-10224-w.
- [7] A. H. Mohsin *et al.*, "PSO-blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture," *Multimedia Tools and Applications*, vol. 80, no. 9, pp. 14137–14161, Apr. 2021, doi: 10.1007/s11042-020-10284-y.
- [8] S. Rustad, D. R. I. M. Setiadi, A. Syukur, and P. N. Andono, "Inverted LSB image steganography using adaptive pattern to improve imperceptibility," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 6, pp. 3559–3568, Jun. 2022, doi: 10.1016/j.jksuci.2020.12.017.
- [9] Y.-H. Chuang, B.-S. Lin, Y.-X. Chen, and H.-J. Shiu, "Steganography in RGB images using adjacent mean," *IEEE Access*, vol. 9, pp. 164256–164274, 2021, doi: 10.1109/ACCESS.2021.3132424.
- [10] P. D. Shah and R. S. Bichkar, "Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure," *Engineering Science and Technology, an International Journal*, vol. 24, no. 3, pp. 782–794, Jun. 2021, doi: 10.1016/j.jestch.2020.11.008.
- [11] M. Plachta, M. Krzemień, K. Szczypiorski, and A. Janicki, "Detection of image steganography using deep learning and ensemble classifiers," *Electronics*, vol. 11, no. 10, May 2022, doi: 10.3390/electronics11101565.
- [12] A. Jaradat, E. Taqieddin, and M. Mowafi, "A high-capacity image steganography method using chaotic particle swarm optimization," *Security and Communication Networks*, vol. 2021, pp. 1–11, Jun. 2021, doi: 10.1155/2021/6679284.
- [13] G. Peter, A. Sherine, Y. Teekaraman, R. Kuppusamy, and A. Radhakrishnan, "Histogram shifting-based quick response steganography method for secure communication," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–11, Mar. 2022, doi: 10.1155/2022/1505133.
- [14] N. Subramanian, I. Cheheb, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "End-to-end image steganography using deep convolutional autoencoders," *IEEE Access*, vol. 9, pp. 135585–135593, 2021, doi: 10.1109/ACCESS.2021.3113953.
- [15] A. H. S. Saad, M. S. Mohamed, and E. H. Hafez, "Coverless image steganography based on optical mark recognition and machine learning," *IEEE Access*, vol. 9, pp. 16522–16531, 2021, doi: 10.1109/ACCESS.2021.3050737.
- [16] M. A. Ahmad *et al.*, "Hiding patients' medical reports using an enhanced wavelet steganography algorithm in DICOM images," *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 10577–10592, Dec. 2022, doi: 10.1016/j.aej.2022.03.056.
- [17] S. Rahman, J. Uddin, H. U. Khan, H. Hussain, A. A. Khan, and M. Zakarya, "A novel steganography technique for digital images using the least significant bit substitution method," *IEEE Access*, vol. 10, pp. 124053–124075, 2022, doi: 10.1109/ACCESS.2022.3224745.
- [18] A. Durafe and V. Patidar, "Development and analysis of IWT-SVD and DWT-SVD steganography using fractal cover," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 7, pp. 4483–4498, Jul. 2022, doi: 10.1016/j.jksuci.2020.10.008.
- [19] W. Lin, X. Zhu, W. Ye, C.-C. Chang, Y. Liu, and C. Liu, "An improved image steganography framework based on y channel information for neural style transfer," *Security and Communication Networks*, vol. 2022, pp. 1–12, Jan. 2022, doi: 10.1155/2022/2641615.
- [20] L. Liu, L. Tang, and W. Zheng, "Lossless image steganography based on invertible neural networks," *Entropy*, vol. 24, no. 12, Dec. 2022, doi: 10.3390/e24121762.
- [21] M. Hussain, A. W. A. Wahab, Y. I. Bin Idris, A. T. S. Ho, and K.-H. Jung, "Image steganography in spatial domain: a survey," *Signal Processing: Image Communication*, vol. 65, pp. 46–66, Jul. 2018, doi: 10.1016/j.image.2018.03.012.
- [22] M. Khan, A. S. Alanazi, L. S. Khan, and I. Hussain, "An efficient image encryption scheme based on fractal Tromino and Chebyshev polynomial," *Complex & Intelligent Systems*, vol. 7, no. 5, pp. 2751–2764, Oct. 2021, doi: 10.1007/s40747-021-00460-4.
- [23] Y. Chen, S. Xie, and J. Zhang, "A hybrid domain image encryption algorithm based on improved Henon map," *Entropy*, vol. 24, no. 2, Feb. 2022, doi: 10.3390/e24020287.
- [24] M. Hussain, A. W. Abdul Wahab, A. T. S. Ho, N. Javed, and K.-H. Jung, "A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement," *Signal Processing: Image Communication*, vol. 50, pp. 44–57, Feb. 2017, doi: 10.1016/j.image.2016.10.005.
- [25] S. Wang *et al.*, "Optical image watermarking based on singular value decomposition ghost imaging and lifting wavelet transform," *Optics and Lasers in Engineering*, vol. 114, pp. 76–82, Mar. 2019, doi: 10.1016/j.optlaseng.2018.10.014.
- [26] M. Suresh and I. S. Sam, "Optimal wavelet transform using oppositional grey wolf optimization for video steganography," *Multimedia Tools and Applications*, vol. 79, no. 37–38, pp. 27023–27037, Oct. 2020, doi: 10.1007/s11042-020-09330-6.
- [27] J. Liu, X. Wei, and H. Huang, "An improved grey wolf optimization algorithm and its application in path planning," *IEEE Access*, vol. 9, pp. 121944–121956, 2021, doi: 10.1109/ACCESS.2021.3108973.
- [28] M. Hussain, Q. Riaz, S. Saleem, A. Ghafoor, and K.-H. Jung, "Enhanced adaptive data hiding method using LSB and pixel value differencing," *Multimedia Tools and Applications*, vol. 80, no. 13, pp. 20381–20401, May 2021, doi: 10.1007/s11042-021-10652-2.

**BIOGRAPHIES OF AUTHORS**

**Shyla Nagarajegowda**     received the bachelor's degree in Electronics and Communication Engineering from BCE, VTU Belgaum, in 2005, the master's degree in computer network engineering from VTU Belgaum, in 2013, and the Pursuing Ph.D. degree in Image processing from the Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Chennai, India. She is currently working as an Assistant Professor with the RNS Institute of Technology. Her areas of interests include signal processing, the internet of things, and sensor networks. She can be contacted at email: shylaashok@gmail.com.



**Kalimuthu Krishnan**     received the bachelor's degree in Electronics and Communication Engineering from MIT, Anna University, in 2003, the master's degree in communication system from SRM University, in 2007, and the Ph.D. degree in wireless communications from the Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Chennai, India. He is currently working as an Associate Professor with the SRM Institute of Science and Technology. His areas of interests include wireless communication, signal processing, the internet of things, and embedded systems. She can be contacted at email: kalimutk@srmist.edu.in.