How to Cite:
Suresh, K. S., & Kamalakannan, T. (2022). Image steganography based on LSB using various scanning methods in spatial domain. *International Journal of Health Sciences*, *6*(S3), 6820–6834. https://doi.org/10.53730/ijhs.v6nS3.7552

Image steganography based on LSB using various scanning methods in spatial domain

K. S. Suresh
Dept. of Computer Science, Rajeswari Vedachalam Government Arts College, Chengalpattu, Research Scholar, VISTAS, Chennai, India
*Corresponding author email: ksampathsuresh@gmail.com

Dr. T. Kamalakannan
[2]Head, Department of Information Technology, School of Computing Sciences, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India.
Email: kkannan.scs@velsuniv.ac.in

***Abstract*---**Data security plays a vital role in the field of Information Technology. Cryptography and Steganography methods are widely used to enforce security efficiently. In Spatial Domain, many steganography methods are available such as LSB, PVD etc. These existing methods always suffer from the quality, security trade off. In this paper, we proposed an enhanced LSB method to deal with such tradeoffs. The proposed method achieves the goal by employing variable embedding patterns and the results with optimized PSNR, MSE and entropy values evidently show that the quality and security are well balanced by the proposed method.

***Keywords*---**steganography, LSB, PVD, stego-image, PSNR, MSE.

Introduction

In this fast generation world, data transferring from one end to another is not accessible. Cryptography algorithms [1] are used to solve these issues in the early stage, but ethical hackers easily compromised these methods. After the cryptographic algorithms, a new ideology was introduced as steganography [2] to take care the data security. The model of steganography is shown in figure 1.

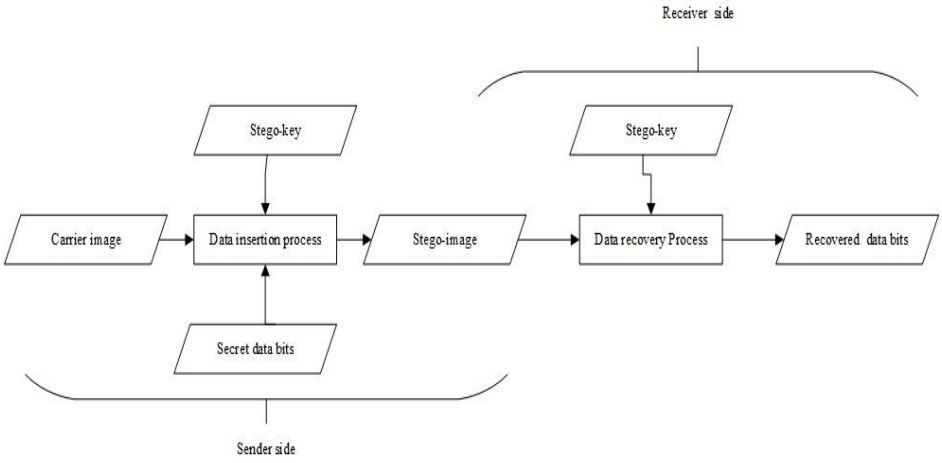

Figure 1. Steganography model

The steganography method has a very long history with different variations [3]. It has been utilised in ancient Greeks in a different version, two decades before this technology slowly entered into digital era and produced the several types as follows in figure 2.

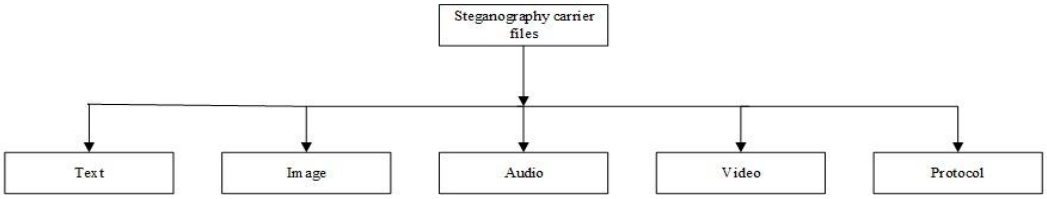

Figure 2. Steganography carrier file types

Digital steganography is classified into five different ways: text, image, audio, video, and network protocol [4]. These five variants are utilised as data carriers. The text-based steganography method is comparably easy to drive with another four ideas, but this method is easily eve-dropped by any hacker. The highly non compromised process is a network protocol based steganography [5]. The other three methods are used in a very often manner. In this field of research, for data security, more budding researchers have produced their new views on the image, audio, and video files as data carrier [6]. Every research article has its view and new developing part, so it has a long-life span when compared with cryptographic algorithms. In the era of the cryptographic algorithm, the developers were in very few numbers, but the users were in large numbers. Nowadays, every user is able to create their own algorithms. In these three predominant areas, image files as a carrier file are focused much more than the others [7]. The image steganography model is easier to implement their ideas [8] comparatively. The audio and video files complex when compared with the image files. This paper also specially focused on the image steganography model. There are many more unique models available under steganography method. The proposed method uses the traditional LSB method for data embedding.

Table 1
LSB & MSB table

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
MSB							LSB

The secret data bits were embedded into the least significant bit position of the pixel value of the input image [9]. The primary reason for that is, if it is embedded into the LSB, it may affect significantly less in numbers; either it goes plus or minus of one or two in numerals [10]. It may only affect the output image quality in a minor difference [11]. If the same data insertion happens in the MSB bit in the image pixels, the changes in the pixel value are substantial in numerals, so it affects the quality of the image in the worst way. Table 1 shows the LSB & MSB bits. Due to the above valid points, all the conventional LSB algorithms only used the least significant bit [12]. Generally, the LSB methods are used to insert the personal data into image in their pixel value in a sequential manner, so these methods are easily eve dropped by anyone [13]. To overcome the common issues in the LSB methods, the proposed method is embedding the secret data differently; it has been clearly explained in the following section.

Background studies

Image steganography is classified into two domains: spatial and frequency. In the frequency-domain, there are many mathematical differential formulas used to insert the data bits into the carrier image [14]. In this case, the image is compressed from the original size to a minimal one so the user can embed one image into another one. The transformation formulas are used to do the same.These methods are executed in discrete structures; they use various algorithms are named Cosine transformation, Fourier transformation and Wavelet transformation [15]. The transformation above plans DFT serves better than the other models [16]. In the case of spatial domain, it works in a different way to compare with transformation domain, it embeds the data forum is pixel values of the carrier image. The standard methods in the spatial domain are LSB & PVD [17]. In LSB, the secret data embeds in the least significant bits [18]. PVD methods insert the data bits based on the difference between the pixel values [19]. The spatial domain can embed more data with minimum distraction in the image [20]. The LSB methods data insertion tenacious taken by stego-key. LSB method for data insertion uses different ideas as follows: The authors [18] have proposed that the data embedded in the edge area in the image because the positions of the edges showed huge difference between the two pixels. [21] Wang, Zhi Hui proposed a new ideology swarm scanning that was used to embed the private data bits into the carrier picture. In the spatial domain, they proposed a mathematical interpolation model in LSB substitutions [22]. The interpolation ideas are implemented in the transform domain, the authors implemented the same method into the spatial environment, it produced a positive result. [23] uses the reverse encrypted image files to insert the secret data bits.

The main objective of the image steganography method is to improve image quality as much as possible with a high payload. If it produces low-quality images, it can be identified easily. To attain this motto, plus or minus 1 LSB

model is introduced with nominal payload [24] Sarreshtedari approaches in a statistical way to insert the data into an image. Qazanfari, Kazem [25] improved the conventional LSB models with their ideas named LSB + identify the good pixels to embed more data. This method can embed more bits in random pixels in the image. J. Zhang and D. Zhang [23] got their idea in solving the puzzle, the same logic was implemented in their paper. Multilevel data encryptions are done in the works [26] the plain text is converted into cipher text with cryptographic algorithms, then it is converted into bits embedded into the image [27]. If an intruder hacks and gets the data in the middle of sender and receiver, the sender sends the encrypted data so the intruder cannot access the secured data.

Proposed method

The conventional LSB steganography methods insert the data bits into carrier image pixel LSB. The proposed method works as follows; select the carrier image size in a 256 x 256 or 512 x 512 based on the secret message needs. The proposed method gives four different scanning methods to the user named as follows; a. row-major scanning, b. column-major scanning, c. in spiral scanning, and d. out spiral scanning and it denoted by binary bits 00 / 01 / 10 / 11 respectively. Figure 3 and Table 2 depict the same.

1	2	3	4	5	6	7	8	9	10
20	19	18	17	16	15	14	13	12	11
21	22	23	24	25	26	27	28	29	30
40	39	38	37	36	35	34	33	32	31
41	42	43	44	45	46	47	48	49	50
60	59	58	57	56	55	54	53	52	51
61	62	63	64	65	66	67	68	69	70
80	79	78	77	76	75	74	73	72	71
81	82	83	84	85	86	87	88	89	90
100	99	98	97	96	95	94	93	92	91

(a) Row major scanning

1	20	21	40	41	60	61	80	81	100
2	19	22	39	42	59	62	79	82	99
3	18	23	38	43	58	63	78	83	98
4	17	24	37	44	57	64	77	84	97
5	16	25	36	45	56	65	76	85	96
6	15	26	35	46	55	66	75	86	95
7	14	27	34	47	54	67	74	87	94
8	13	28	33	48	53	68	73	88	93
9	12	29	32	49	52	69	72	89	92
10	11	30	31	50	51	70	71	90	91

(b) Column major scanning

1	2	3	4	5	6	7	8	9	10
36	37	38	39	40	41	42	43	44	11
35	64	65	66	67	68	69	70	45	12
34	63	84	85	86	87	88	71	46	13
33	62	83	96	97	98	89	72	47	14
32	61	82	95	100	99	90	73	48	15
31	60	81	94	93	92	91	74	49	16
30	59	80	79	78	77	76	75	50	17
29	58	57	56	55	54	53	52	51	18
28	27	26	25	24	23	22	21	20	19

(c) In spiral scanning

100	99	98	97	96	95	94	93	92	91
65	64	63	62	61	60	59	58	57	90
66	37	36	35	34	33	32	31	56	89
67	38	17	16	15	14	13	30	55	88
68	39	18	5	4	3	12	29	54	87
69	40	19	6	1	2	11	28	53	86
70	41	20	7	8	9	10	27	52	85
71	42	21	22	23	24	25	26	51	84
72	43	44	45	46	47	48	49	50	83
73	74	75	76	77	78	79	80	81	82

(d) Out spiral scanning

Figure 3. Scanning model

Table 2
Scanning model

Scanning model	Binary equivalence
row-major scanning	00

column-major scanning	01
in spiral scanning	10
out spiral scanning	11

The traditional LSB methods utilise RGB values to insert the data bits, but the proposed method has differed from the regular pattern. It offers five different embedding patterns to the user {RBG / GRB / GBR / BRG / BGR} and it is denoted in binary as follows {000 / 001 / 010 / 011 / 100}.

Table 3
Embedding pattern

R	G	B	Binary equivalence
R	B	G	000
G	R	B	001
G	B	R	010
B	R	G	011
B	G	R	100

Table 2
Encryption model

Encryption model	Binary equivalence
Triple DES	00
RSA	01
Blowfish	10
AES	11

The proposed method offers four different encryption models listed in Table 4 based on the user selection of the encryption model from Table 4. The hidden message text is encrypted into cipher text. In the second stage, it is converted into ASCII equivalent; finally, the secret message is converted into binary bits. Now it is ready to be embedded in the carrier image easily. The structure of the stego-key is 8 bits, and it is split as follows: 2 bits for scanning type, 3 bits allotted for data embedding pattern, encryption model needs 2 bits, and the final single bit assigned to k value. The stego-key is shown in Table 5 as follows;

Table 3
Stego-key structure

Stego –Key (8 bits)			
Scanning type (2 bits)	Data embedding pattern (3- bits)	Encryption model (2 bits)	Constant k value (1 bit)
00 / 01/10 / 11	000 / 001 / 010/ 011/100	00/01/10/11	0/1

Based on the secret message bit size, the constant k is determined in stego-key as follows; if the message bits can be sheltered in 256 x 256 size image, then the k

value is denoted as 0. Otherwise, it requires more pixels; then it chooses the 512 x 512 size image and assigns the k value as 1. The embedding procedure begins with choosing different values from the user based on the selections. After completing user selection and giving the k value, the embedding procedure starts as follows; initially, the constant k value is fixed based on the message bit size and the carrier image is selected as either 256 or 512 bits.

The second data embedding process begins with scanning the carrier image based on the user selection; the data embedding pattern has decided which method has been utilised to embed the bits in the cover image. Mainly the conventional LSB algorithms select the routine to embed the confidential data and the intruder can quickly identify the data without the sender and receiver knowledge. To overcome this issue, the proposed method uses a different type of embedding pattern, which is not an identical method. It gives good security to the confidential data bits at a higher level. The scanning method also differs from the conventional LSB methods; the proposed method offers four different scanning methods the user can select, strengthening the security at a higher level. The flow of the proposed method is pictorially clarified the same in Figure 4.

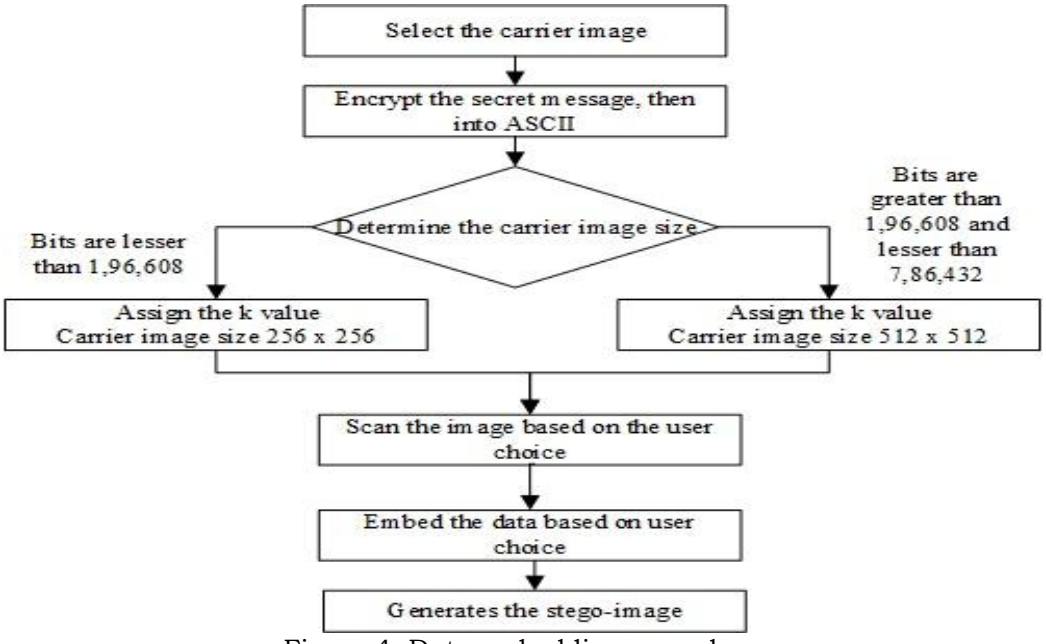

Figure 4. Data embedding procedure

The above procedures were on the sender's side. The final output of the process is stego-key and stego-image; it is transferred to another side through any transmission medium. Once the receiver gets the stego key and stego-image, they try to re-engineer the original message. The flow of the proposed method is explained with sample data in Figure 5.

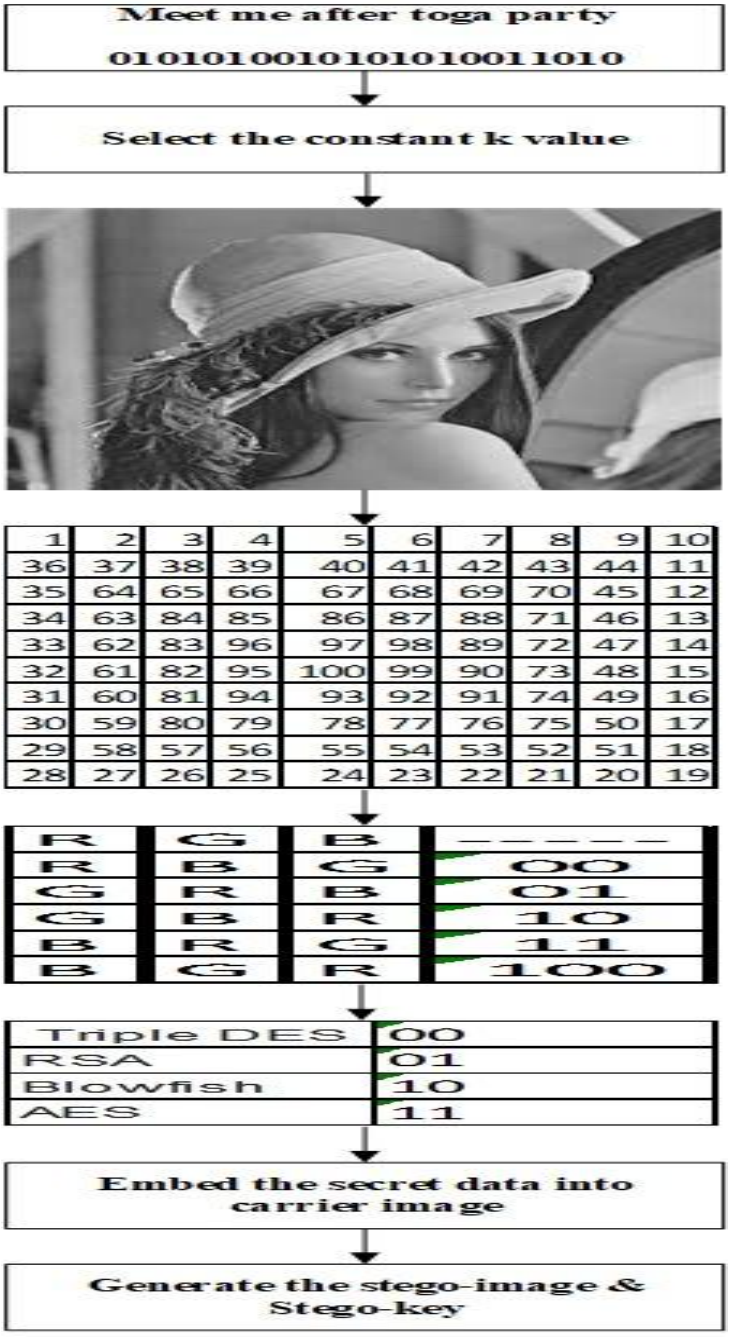

Figure 5. Flow of the proposed method

The data recovery process on the receiver side works as follows. The stego-key reveals the complete secret information to the receiver side. Initially, it starts from backward. The k value is used to identify the size of the carrier image, then scanning type binary equivalent is identified the scanning type. Based on that value the stego-image is scanned. The embedding style of binary number is used

to determine the embedding pattern of secret information into the stego-image. Finally, the data encryption method number decrypts the message bits recovered from the stego-image. After the process is done, the original secret information is successfully received at the receiver end. The proposed method performance is compared with the conventional methods and is described in the following section.

Results and Discussion

The quality of the stego-image is the representation of the excellent steganography method. The stego-image is compared with the source image. The proposed method test the quality of the stego-image under the three different ways, they are listed as follows;

- Statistical model – Entropy method
- Peak Signal Noise Ratio – denoted as PSNR
- Mean Square Error – represented as MSE

Entropy

This model uses a statistical way to identify the texture value of the stego-image [28] is formulated as follows;

$$H = -\sum_{i=0}^{2^N-1} P(S_i) log_2\, p(s_i) \quad (1)$$

In the above equation (1) N - number of bits represent the symbol, $P(S_i)$ – the probability of the symbol, and H – identifies the characteristic texture of the image.

Mean Square Error

It calculates the squared difference of the carrier image with the stego-image. The calculated MSE value is considered when it shows the varying minor differences; the steganography method is not a appropriate one[14][29]. The following equation (2) represents the same.

$$MSE = \frac{1}{w \times h} \sum_{r=0}^{w-1} \sum_{c=0}^{H-1} (CI(r,c) - SI(r,c))^2 \quad (2)$$

In the above equation, w & h – represents the width & height of the source image, r & c denotes the row and column of the pixel matrix of the image, CI is referred to as carrier image and SI is known as stego-image.

Peak Signal Noise Ratio

This method is used to identify the noise ratio between the input image and output image of the proposed approach; the calculated value from equation (3) is only taken as an account when it produces the higher value [30]–[32].

$$PSNR\ (db) = \ 10\ log_{10}\ \frac{(R)^2}{MSE} \quad (3)$$

Figure 6 depicts the sample images used to test the proposed method in the size of 256 x 256 grayscale images. If the secret message can accommodate the 256 x 256, then k is assigned as 0. If size of message bits are more significant than 1,96,688, it uses the 512 x 512 and k is assigned as 1. Every image is a collection of pixels, and each pixel may vary in its colour. The colour value is between 0-255; it can easily represent the eight-bit binary number. The proposed method embeds the three-bit binary data in each pixel in the source image, the constant k value is calculated with following expression; number-of-bits = 256 x 256 x 3 = 1,96,608 / 512 x 512 x 3 = 7,86,432 based on this value, k is assigned either 0 or 1 in the structure of stego-key. The proposed method's statistical analysis is depicted in table 5, and it uses eight different sample images of the same size. The private data is embedded into the carrier image in the size of 25,387 bits. The secret data can be accommodated in 256 x 256 grayscale images, and the sample images are listed in figure 6.

Table 6
Statistical analysis of proposed method

Statistical analysis (Entropy)						
Image name	Source image			Stego-image		
	R	G	B	R	G	B
Baboon	7.8457	7.7842	7.5144	7.8458	7.7846	7.5147
Lena	7.2477	7.5883	6.9232	7.2478	7.5887	6.9235
Peppers	7.3857	7.6658	7.1614	7.3858	7.6662	7.1617
Barbara	7.4892	7.4859	7.2022	7.4893	7.4863	7.2025
Lake	7.2756	7.2564	7.3101	7.2757	7.2568	7.3104
Cameraman	7.4321	7.4765	7.4123	7.4322	7.4769	7.4126
City	7.1345	7.2001	7.2011	7.1346	7.2005	7.2014
Plane	7.5234	7.5231	7.5432	7.5235	7.5235	7.5435

Table 6 clearly shows the minimal divergence between the source and stego images. The comparative analysis is done based on the random manner. The

illumination value of pair of pixels checked from the two images, one from the source image and another from the stego-image. These pixels are compared with R, G, and B values. The proposed method shows better results by testing the statistical entropy method with eight different sample images in the same size as 256 x 256. The sample images are listed in figure 6 and arranged clockwise left to right as follows;

- Baboon
- Lena
- Peppers
- Barbara
- Lake
- Cameraman
- City
- Plane
- Elaine respectively.

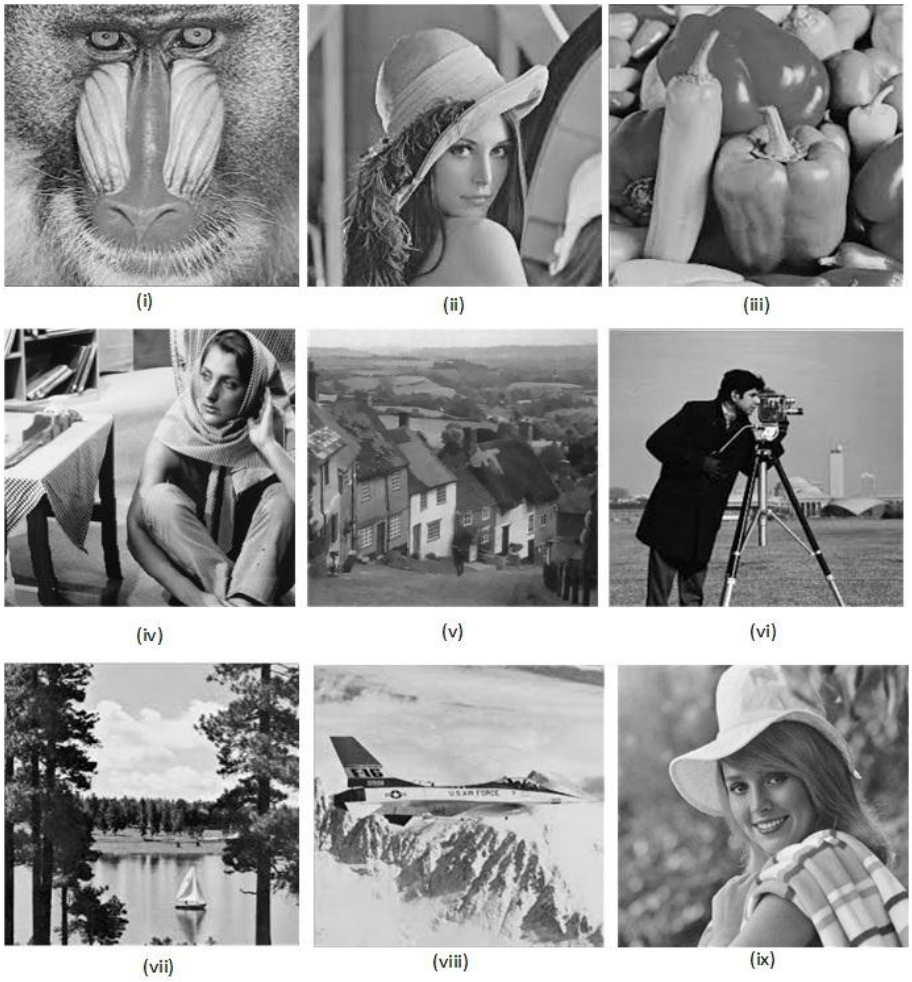

Figure 6. Testing sample pictures

The output of the proposed method depicts Table 7, and the proposed method compares with five conventional methods with two different parameters PSNR and MSE. The capacity slightly increased with the previous methods.

Table 7
PSNR & MSE value comparative table

Image name	Proposed by	Capacity	PSNR	MSE
Baboon	Tasi et al.	25,462	48.92	7.41
	Luo et al.	27,687	49.73	8.21
	Kim et al.	21,965	49.63	7.91
	Hong et al.	27,194	49.74	8.23
	Tian et al.	28,658	48.28	8.01
	Proposed Method	**29,453**	**48.41**	**7.02**
Lena	Tasi et al.	26,567	48.77	7.53
	Luo et al.	27,765	48.34	8.13
	Kim et al.	22,765	48.43	8.02
	Hong et al.	27,145	49.52	9.02
	Tian et al.	28,678	47.23	8.91
	Proposed Method	**29,721**	**48.76**	**7.02**
Peppers	Tasi et al.	32,186	48.99	9.623
	Luo et al.	33,783	49.8	8.934
	Kim et al.	27,045	49.68	9.83
	Hong et al.	34,758	49.87	8.34
	Tian et al.	35,767	46.72	9.62
	Proposed Method	**36,102**	**47.54**	**8.02**
Barbara	Tasi et al.	36,361	49.63	10.34
	Luo et al.	39,338	49.92	10.67
	Kim et al.	30,764	49.22	11.92
	Hong et al.	39,475	50.77	11.56
	Tian et al.	37,568	49.46	11.67
	Proposed Method	**39,623**	**50.02**	**10.49**
Boat	Tasi et al.	25,788	48.92	11.45
	Luo et al.	28,041	49.74	12.68
	Kim et al.	22,480	49.63	12.62
	Hong et al.	28,739	50.11	13.56
	Tian et al.	28,875	49.53	12.97
	Proposed Method	**29,754**	**50.12**	**11.04**
Elaine	Tasi et al.	25,462	48.92	13.36
	Luo et al.	27,687	49.73	13.95
	Kim et al.	21,965	49.63	14.05
	Hong et al.	27,194	49.74	14.38
	Tian et al.	28,658	48.28	15.21
	Proposed Method	**32,145**	**49.32**	**12.89**
Cameraman	**Proposed Method**	**23,783**	**51.87**	**15.34**
City	**Proposed Method**	**24,687**	**52.02**	**12.67**
Plane	**Proposed Method**	**27,145**	**48.56**	**15.84**

$$\text{Percentage} - \text{wise comparison} = \left(\frac{\text{newvalue} - \text{oldvalue}}{\text{oldvalue}}\right) \times 100 \quad (4)$$

Equation 4 calculates the difference between the proposed method value and the output of the existing method. The proposed method increases the payload gradually higher than the other methods. The stego-image was applied to the testing to find the MSE and PSNR value with equations two and 3, respectively. In Table 7, the image Baboon used to hide the data using the proposed method and the output is compared with the previous method outputs of MSE and PSNR. The proposed method hides the 29,453 number of bits into the carrier image. It increases the data size compared with the existing practices; the minimum value of 2 % and the maximum of 34 % on average come to around 13.44 %. The MSE value shows a massive difference from 5 % to 14 % on average 11 %. The PSNR values show minor difference while comparing with an existing model. The first parameter payload size increases in the proposed method and produces the similar equivalent number to the previous model. The payload value is proportionate to the output values MSE and PSNR, respectively. If the payload increases, the output values automatically increase, but the proposed method improves the payload size and produces a similar output compared with existing methods. The more significant value is accepted as a sound output of PSNR, but in the case of MSE, the smaller value is taken. The proposed method produces 48.41 for PSNR and 7.02 for MSE. Comparatively, the proposed method output MSE shows a good number than other methods. The PSNR shows the nearby values with the previous model.

In Table 7, the proposed method hides the 29,721 number of bits in the Lena image. It increases the data size compared with the existing practices; the minimum value of 3.63 % and the maximum of 30 % on average come to around 12.51 %. The MSE value shows a massive difference from 6.77 % to 22.21 %, an average 16.62 %. The PSNR values show a very minimal difference when compared with existing models. The proposed method produces 48.76 for PSNR and 7.02 for MSE. Comparatively, the proposed method shows the excellent output for the values. In Table 7, the proposed method increases the secret data bits to 36,102 in the Peppers image. While measuring up the data size with the previous models shows the minimum value of 0.9 % and the maximum of 12.92 % on average come to around 11.46 %. The MSE value shows an immense difference from 3.83 % to 18.41 % on average 13.41 %. The PSNR values show very minimal differences while comparing with existing models. The proposed method produces 47.54 for PSNR and 8.02 for MSE. Relatively, the proposed method yields an excellent value with this payload size.

In Table 7, the proposed method increases the secret data bits size to 39,623 in the Barbara image. While comparing the data size with previous models, the proposed method shows the increased value from 0.3 % to 28.79 % on average come to around 8.8 %. The MSE value shows an immense difference from 1.6 % to 11.99 %, on average 6.32 %. The PSNR values show a difference from 0.2 % to 1.6%, an average 0.4%. The proposed method produces 50.02 for PSNR and 10.49 for MSE. Relatively, the proposed method gives an excellent value with this payload size. In Table 7, the proposed method hides the 29,754 number of bits in the Boat image. The payload is increased as much as possible. Relatively, the proposed method shows impressive numbers as a result. The MSE value shows a massive difference from 3.58 % to 18.58 %, on average 12.49 %. The PSNR value shows the difference from 0.45 % to 1.19 on average 1.08 % better result than

existing models. The proposed method produces 50.12 for PSNR and 11.04 for MSE.

In Table 7, the proposed method hides the 32,145 number bits in the Elaine image. The payload is increased 23 % on average while compared with existing models. The MSE value shows a good result compared with all previous models, an average of 8.99 %. The PSNR value shows the minimal difference from 0.45 % to 1.19, an average 1.08 % better result than existing models. The proposed method produces 49.32 for PSNR and 12.89 for MSE. The proposed method produces outstanding results. The proposed method has also been tested with Cameraman, City and Plane images with different payloads 23,783, 24,687 and 27,145, respectively. The Cameraman produces the PSNR value of 51.87 and MSE value as 15.34. The city image results as 12.67 for MSE and 52.02 for PSNR. The Plane image with 27,145 data bits follows PSNR 48.56 and MSE as 15.84.

Conclusion

The main motto of the steganography model is to embed more data into the input image with minimal distraction, and the output is not to be traced by any intruder while transmitting from one end to another end. The proposed design in all the way gives better results with a high payload in all testing aspects. With the help of table 6 and above, the section clearly depicts that the proposed method achieved the goal successfully.

References

1. R. P. V.Tyagi, A.kumar, "Image Steganography Using Least Significant Bit With Cryptography," J. Glob. Res. Comput. Sci. Res. Pap. Available Online www.jgrcs.info IMAGE, vol. 3, no. 3, 2012.
2. S. Gupta,Ankur Goyal and B. Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography," Int. J. Mod. Educ. Comput. Sci., vol. 4, no. 6, 2012, doi: 10.5815/ijmecs.2012.06.04.
3. J. Silman, "Steganography and Steganalysis: An Overview," SANS Institute, no. May, 2001.
4. S. B. Sasi, N. Sivanandam, and Emeritus, "A survey on cryptography using optimisation algorithms in WSNs," Indian J. Sci. Technol., vol. 8, no. 3, 2015, doi: 10.17485/ijst/2015/v8i3/59585.
5. Y. F. Huang, S. Tang, and Y. Zhang, "Detection of covert voice-over Internet protocol communications using sliding window-based steganalysis," IET Commun., vol. 5, no. 7, 2011, doi: 10.1049/iet-com.2010.0348.
6. W. Mazurczyk, "VoIP steganography and its detection-a survey," ACM Computing Surveys, vol. 46, no. 2. 2013, doi: 10.1145/2543581.2543587.
7. V. Raja and S. Rajalakshmi, "Pearl pixel steganographic method for grayscale images using location-array method," Int. J. Eng. Adv. Technol., vol. 8, no. 6, 2019, doi: 10.35940/ijeat.F9049.088619.
8. H. Kayarkar and S. Sanyal, "A Survey on Various Data Hiding Techniques and their Comparative Analysis," Acta Tech. Corvininesis - Bull. Eng., vol. 5, no. 3, pp. 35-40., 2012, [Online]. Available: http://arxiv.org/abs/1206.1957.

9. Raja.V and Rajalakshmi.S, "An improved adaptive digital image steganography based on pixel value differencing by rotation of base pixels," Int. J. Pure Appl. Math., vol. 119, no. 15, pp. 649–659, 2018.
10. M. O. Islam, M. S. Hossain, M. S. H. Siddique, and D. K. Saha, "Improving the non-filtering steganographic algorithm using LSB verification method," 2014, doi: 10.1109/ICEEICT.2014.6919106.
11. J. C. T. Arroyo and A. J. P. Delima, "LSB image steganography with data compression technique using goldbach G0 code algorithm," Int. J. Emerg. Trends Eng. Res., vol. 8, no. 7, pp. 3259–3264, 2020, doi: 10.30534/ijeter/2020/62872020.
12. C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognit., vol. 37, no. 3, pp. 469–474, 2004, doi: 0.1016/j.patcog.2003.08.007.
13. V. Raja and S. Rajalakshmi, "Divide and Conquer Steganography Model," Int. J. Comput. Appl., vol. 91, no. 15, 2014, doi: 10.5120/15960-5356.
14. J. R. Jayapandiyan, C. Kavitha, and K. Sakthivel, "Enhanced Least Significant Bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimisation," IEEE Access, vol. 8, pp. 136537–136545, 2020, doi: 10.1109/ACCESS.2020.3009234.
15. J. Sang, H. Xiang, and H. Hu, "Discrete Fourier transform-based information steganography," Huazhong Keji Daxue Xuebao (Ziran Kexue Ban)/Journal Huazhong Univ. Sci. Technol. (Natural Sci. Ed., vol. 36, no. 8, 2008.
16. A. S. Khashandarag, A. H. Navin, M. K. Mirnia, and H. H. Agha Mohammadi, "An optimised color image steganography using LFSR and DFT techniques," in Communications in Computer and Information Science, 2011, vol. 176 CCIS, no. PART 2, doi: 10.1007/978-3-642-21802-6_40.
17. C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, "Varied PVD + LSB evading detection programs to spatial domain in data embedding systems," J. Syst. Softw., vol. 83, no. 10, 2010, doi: 10.1016/j.jss.2010.03.081.
18. C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," IEEE Trans. Inf. Forensics Secur., vol. 3, no. 3, 2008, doi: 10.1109/TIFS.2008.926097.
19. Z. Li and Y. He, "Steganography with pixel-value differencing and modulus function based on PSO," J. Inf. Secur. Appl., vol. 43, pp. 47–52, 2018, doi: 10.1016/j.jisa.2018.10.006.
20. 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 Process. Image Commun., vol. 65, 2018, doi: 10.1016/j.image.2018.03.012.
21. Z. H. Wang, C. C. Chang, and M. C. Li, "Optimising least-significant-bit substitution using cat swarm optimisation strategy," Inf. Sci. (Ny)., vol. 192, 2012, doi: 10.1016/j.ins.2010.07.011.
22. H. B. Kekre, A. A. Athawale, and U. A. Athawale, "Increased cover capacity using advanced multiple LSB algorithms," 2011, doi: 10.1145/1980022.1980029.
23. J. Zhang and D. Zhang, "Detection of LSB matching steganography in decompressed images," IEEE Signal Process. Lett., vol. 17, no. 2, pp. 141–144, 2010, doi: 10.1109/LSP.2009.2035379.
24. S. Sarreshtedari and M. A. Akhaee, "One-third probability embedding: A new ±1 histogram compensating image least significant bit steganography

scheme," IET Image Process., vol. 8, no. 2, 2014, doi: 10.1049/iet-ipr.2013.0109.
25. K. Qazanfari and R. Safabakhsh, "A new steganography method which preserves histogram: Generalisation of LSB++," Inf. Sci. (Ny)., vol. 277, pp. 90–101, Sep. 2014, doi: 10.1016/J.INS.2014.02.007.
26. P. Sallee, "MODEL-BASED METHODS for STEGANOGRAPHY and STEGANALYSIS," Int. J. Image Graph., vol. 5, no. 1, pp. 167–189, Jan. 2005, doi: 10.1142/S0219467805001719.
27. T. Zhang and X. Ping, "A new approach to reliable detection of LSB steganography in natural images," Signal Processing, vol. 83, no. 10, pp. 2085–2093, Oct. 2003.
28. Z. Gao, G. Tang, and S. Wang, "A Novel VoIP Steganography Method Based on Bayesian Network and Matrix Embedding," Jisuanji Yanjiu yu Fazhan/Computer Res. Dev., vol. 55, no. 4, 2018, doi: 10.7544/issn1000-1239.2018.20161042.
29. A. Alabaichi, M. A. A. K. Al-Dabbas, and A. Salih, "Image steganography using least significant bit and secret map techniques," Int. J. Electr. Comput. Eng., vol. 10, no. 1, pp. 935–946, 2020, doi: 10.11591/ijece.v10i1.pp935-946.
30. A. K. Sahu, G. Swain, M. Sahu, and J. Hemalatha, "Multi-directional block based PVD and modulus function image steganography to avoid FOBP and IEP," J. Inf. Secur. Appl., vol. 58, no. March, p. 102808, 2021, doi: 10.1016/j.jisa.2021.102808.
31. M. Khodaei and K. Faez, "New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing," IET Image Process., vol. 6, no. 6, 2012, doi: 10.1049/iet-ipr.2011.0059.
32. H. H. Liu, P. C. Su, and M. H. Hsu, "An Improved Steganography Method Based on Least-Significant-Bit Substitution and Pixel-Value Differencing," KSII Trans. Internet Inf. Syst., vol. 14, no. 11, pp. 4537–4556, 2020, doi: 10.3837/tiis.2020.11.016.