

Textual Data Hiding in Digital Images Using Chaotic Maps

Vipul Sharma

Research Scholar, Department of Computer Science & Engineering, National Institute of Technology, Srinagar, India.

vipul_1phd17@nitsri.net

Roohie Naaz Mir

Department of Computer Science & Engineering, National Institute of Technology, Srinagar, India.
naaz310@nitsri.net

Published online: 30 December 2018

Abstract – In this research paper, another methodology for covering up literary information in computerized hues pictures has been proposed. Digital colored pictures will simply be used as a canopy media in steganography as a result of numerous deficiencies rumored in sensory system of mortals. In the proposed system we have utilized two non-subordinate disordered arrangement, for distinguishing the fundamental pixel positions where the bits relating to the mystery message must be inserted in the computerized cover picture. For implanting the message bits in the clamorously chosen pixels a 3-3-2 Least Significant Bit (LSB) addition strategy has been utilized. The proposed technique also provides a sufficient level of security because of the fact that same series of chaotically generated pixel locations for embedding the message bits is very difficult to be reproduced, till and unless the initial conditions of the 2 chaotic maps used for pixel selection method are well known. Additionally, the arranged method gives higher leads as far as PSNR (Peak Signal to noise ratio) and MSE (Mean squared error) values when contrasted, with optional existing strategies, subsequently guaranteeing that meddlers won't have any doubt that there is a message covered up inside the sent cover picture.

Index Terms – Steganography, LSB, PSNR, MSE, Chaotic Maps, Cover Image, Stego Image, Histogram.

Nomenclature

Symbol	Meaning
LSB	: Least Significant Bit.
MSE	: Mean Square Error.
$[A(i,j)]$: Cover image.
$[B(i,j)]$: Stego image.
A_i	: Chaotic sequence component of cover image.
B_i	: Chaotic sequence component of stego image.
P	: Total number of rows in cover image.
Q	: Total number of columns in cover image.

$(N_r \times N_c \times 3)$: Cover Image Size.
$\sim A_i$: Horizontal pixel index.
$\sim B_i$: Vertical pixel index.
PSNR	: Peak Signal to Noise Ratio.
R	: Control parameter in chaotic mapping.

1. INTRODUCTION

In this time of correspondence and systems administration, security has turned into a basic issue for flourishing systems. One of the fundamental necessities to keep the burglary of information is to anchor the data. There are different methods to anchor the data, however the outstanding and broadly utilized are "cryptography" and "steganography". These two procedures are for the most part utilized and have numerous applications like anchoring individual records, corporate information, sending secret and mission-basic messages and so on. [1][2][24] "Cryptography" has been derived from an attempt of Greek words "Kryptos" that signifies "covered up" and "graphein" which signifies "to compose". [21][24] So, cryptography can be characterized as the investigation of changing over the instant message or data from a clear organization into an indiscernible configuration without utilizing any mystery learning. Cryptography plans to scramble the genuine message that is being sent. This message can be encoded or mixed by utilizing different instruments including scientific strategies and calculations to clutter up the information into a non-clear, unlimited configuration rendering it un-open with no mystery learning. [2][3][4][21][24] The generalized cryptographic scheme is depicted in Figure 1.

The scrambled message created by cryptography must be decoded or unscrambled by the gathering that has the mystery key.[24] Steganography then again, is characterized as the craftsmanship and investigation of composing the shrouded messages so that nobody else, aside from the planned

RESEARCH ARTICLE

beneficiary knows the presence of the message. "Steganography" is extensive of Greek inception, which signifies "concealed composition". [25] "Steganography" is normally pondered almost like "Cryptography" and "Watermarking", while watermarking guarantees message honesty and cryptography scrambles the message, steganography conceals it. [22][23][24] It has been seen that the objective of "cryptography" and "steganography" is the equivalent, yet the manner in which this objective is accomplished is extraordinary. [2][3][4][24] In steganography the message to be conveyed subtly, is implanted inside a medium called a cover question or a stego protest so that the presence of the message is hidden. [23] Clearly, it can be observed that "steganography" is much more advantageous than "cryptography", because of the fact that steganography not only conceals the secret message contents but also conceives the third party who can no longer detect the secret transmission of data. The generalized steganographic scheme is depicted in Figure 2.

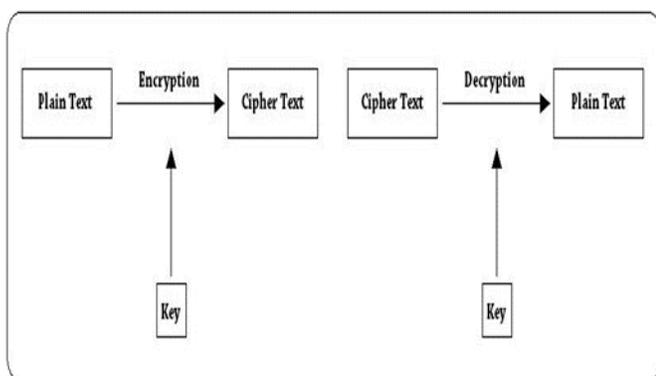


Figure 1: Generalized Cryptographic Approach

In this paper, we have proposed another strategy for concealing the literary data in an advanced shaded picture [23][24]. This proposed procedure includes the utilization of a mystery key, along these lines consolidating the highlights of steganography. Even if, the third party by some means detects the presence of the hidden message, he would not be able to predict the secret key used for the embedding purpose because of chaotic mapping, making this scheme more robust and secure.

Whatever is left of the paper is sorted out as, In segment II, literature identified with the proposed method has been looked into. Least Significant bit (LSB) strategy and disorganized maps (Chaotic maps) are examined in segment III. Segment IV incorporates different execution assessment measures for information concealing system. The proposed algorithm is incorporated into segment V. Usage and results got are talked about in segment VI. Correlation of the proposed system with different plans showed in writing

survey is displayed in segment VII lastly, segment VIII incorporates the closing comments.

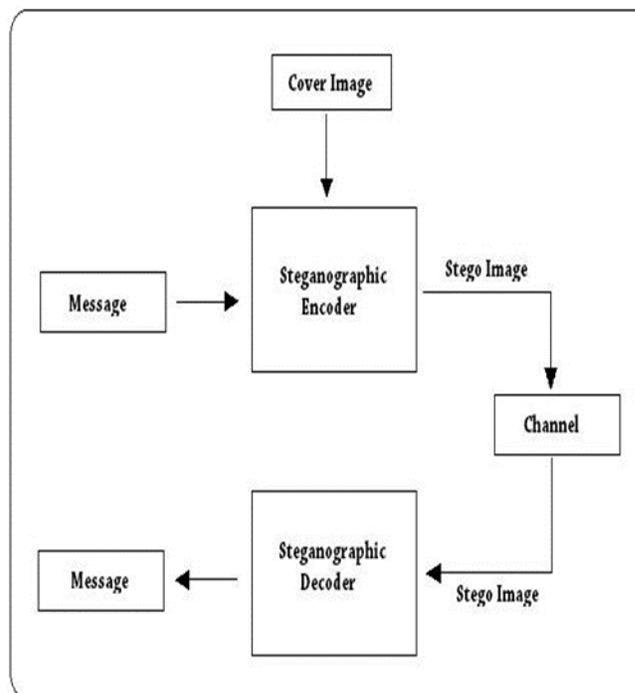


Figure 2: Generalized Steganographic Approach

2. LITERATURE REVIEW

Over the years, a number of efficient and highly secure steganographic techniques have been developed and implemented successfully. Basically, all of the steganographic techniques that have been proposed to date can be classified into four major categories. These are the Spread Spectrum Technique, wherein the information to be transmitted is divided into small pieces. Factual (Statistical) Techniques, wherein the data or message to be transmitted is encoded by modifying the measurable properties of the hidden cover picture and information is recuperated by utilizing speculation testing. [23][24][25] Patchwork is a case of the factual method. Substitution Technique is a plan in which pixel bits of the cover picture is supplanted with the character bits of the message to be transmitted. LSB (Least Significant Bit) method is an example of this technique. Transform Domain Technique hides information to be transmitted in the transform space of the signal. DCT (Discrete Cosine Transform) is an example of this technique. [28]

Out of all these major steganographic techniques, the algorithm that we have proposed comes under the category of Substitution Scheme and employs the Least Significant Bit methodology for hiding the data. The majority of the steganographic procedures that have been proposed till date

RESEARCH ARTICLE

depend on LSB (Least Significant Bit) system wherein, the character bits of the mystery message is implanted inside the slightest critical bits of pixels of the fundamental advanced cover picture. [28] In [6], the authors have proposed an amateur information concealing system wherein, the pixels of the cover picture is deteriorated as a whole of prime numbers. [31] The authors of [7] have used an enhanced adaptation of the LSB procedure wherein, the concealing limit has been expanded by utilizing clamorous maps. Another methodology dependent on LSB has been exhibited in [8]. Here authors have utilized a four-pixel differencing procedure dependent on the adjusted LSB substitution strategy. This technique enhanced the information implanting limit and furthermore giving better visual quality. [23][31]

In [9], a picture steganographic procedure dependent on 1-dimensional tumultuous maps has been proposed to deliver an arbitrary arrangement of pixel positions which are then utilized for inserting the mystery message inside a computerized cover picture. [42] Besides, authors in [10] have utilized a disordered mapping method to guarantee security amid the implanting procedure. Here the irregular succession of pixel positions is produced by separating the advanced cover picture into (3x3) squares. [29]

In [12] a more secure advanced picture steganographic strategy dependent on 3-dimensional tumultuous feline maps and discrete wavelet change (DWT) has been displayed.[26] Here, the yield of the riotous maps is utilized for implanting the mystery message inside the cover picture.[25][28] Authors in [13] have exhibited a spatial space steganographic strategy dependent on 1-dimensional riotous maps for deciding the pixel positions in which the comparing bits of the mystery message must be inserted. While in [14] authors have exhibited a modified algorithm for implanting scrambled content in arbitrary pixel positions in edges and smooth zones of the cover picture by utilizing enhanced edge recognition channels. Message bits are then installed utilizing LSB strategy. [28]

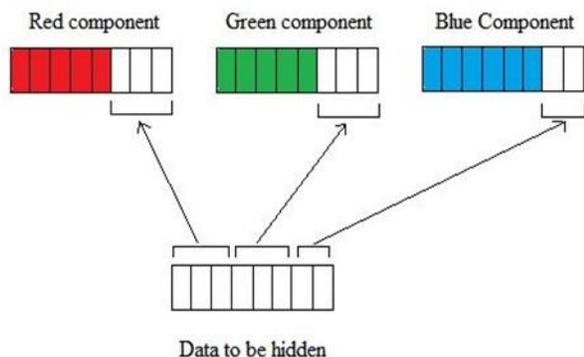


Figure 3: 3-3-2 LSB Embedding Technique

In [15] 3-3-2 LSB addition strategy has been used for picture steganography and this is further being utilized in our proposed method. [26] Figure 3 delineates the 3-3-2 LSB inclusion approach.

3. CONCEPTS USED IN PROPOSED SCHEME

3.1. Chaotic Maps for Data Hiding

Chaos can be defined as a process that is closely related to the non-linear dynamical system. The systems based on chaos mechanism are very sensitive to the parameters that are set initially. Any minor differences in the initial parameters may lead to extreme modifications of the final results. Over the years, a lot of research has been done in this field and many characteristics of the chaotic maps have been exploited and could be employed to secure the information hiding process. To the extent data stowing away is concerned, riotous maps can be utilized for choosing the pixels of the hidden cover picture that ought to be adjusted by the strategy for addition. [17][26]

One of the most straightforward types of a confused map is the logistic map. It is fundamentally a one-dimensional mapping system, utilized for extraction of numbers from a recursive connection. [42]

Recursive connection for the logistic map is as characterized underneath: -

$$A_{i+1} = r[(A_i)(1 - A_i)] \tag{1}$$

Where $0 <= r <= 4$, $A_i \in (0,1)$.

Numerous specialists have recommended that the logistic map is in a tumultuous state when $3.569 < r < 4$, which implies that the arrangement A_1, A_2, A_3, \dots created by confused maps is non-focalized in nature. [23] We in our proposed method have used the coordination map to arbitrarily create the pixel areas where the mystery message ought to be installed. [42]

3.2. LSB (Least Significant Bit) Insertion Method

A standout amongst the most well-known systems utilized for picture steganography is LSB. In this strategy, bit-outline are utilized for concealing the information, wherein every pixel bit of the picture is supplanted with the character bit to be covered up. In the proposed approach we have utilized 3-3-2 LSB inclusion strategy. Here in this system, the initial 3 bits of the mystery message is disguised inside the 3 LSB's of the red part of the pixel. The following three bits inside the 3 LSB's of the green part and the rest of the 2 bits inside the 2 LSB's of the blue segment. [23][29] The subtleties of 3-3-2 LSB procedure is shown in Figure 3.

4. VARIOUS PERFORMANCE EVALUATION METRICS OF HIDING TECHNIQUE

So as to assess the nature of the concealing procedure, various

RESEARCH ARTICLE

assessment measurements have been proposed which are utilized for contrasting the stego picture and the first transporter or cover picture. [39][40] The most conspicuous measurements are an investigation dependent on picture histograms, Mean squared error, Peak signal to noise ratio and so forth. Concealing limit of the cover picture can likewise be considered as a viable execution metric. [33]

4.1. Analysis of Images Using Histograms

A histogram is essentially a graphical portrayal of the conveyance of numerical information. [26] To the extent pictures are concerned, a histogram can be characterized as a portrayal of pixel esteem appropriation. Variety in the quantity of pixels regarding the shading powers of a picture can without much of a stretch be spoken to utilizing histograms. [23][46] In computerized picture handling, histograms can be utilized to assess the information concealing procedure. The hidden strategy is viewed as effective if stego picture and cover picture has comparative histograms. [26]

4.2. Analysis Based on Peak Signal to Noise Ratio

Another assessment metric is the PSNR (Peak Signal to Noise Ratio). It is fundamentally a measure to compute the bending caused by information covering up in stego picture. [29]

It is likewise utilized for estimating the deviation between the basic cover picture and delivered stego picture. It is as spoken to beneath [38]: -

$$PSNR = 10 \log_{10} \frac{MAX^2}{MSE} \tag{2}$$

The maximum possible number of pixels is represented by MAX. This MAX value comes out to be “255” if pixels are spoken to utilizing 8 bits for every example. [38]The description of PSNR remains exactly the same except the MSE in the denominator for colored images with 3 RGB components per pixel. Here, in this case, the sum of all the squared value differences divided by the size of image multiplied by a factor 3 is represented by MSE.

The hiding process is considered successful if the value of PSNR is high.

4.3. MSE (Mean Square Error)

MSE (Mean Square Error) is essentially a signal constancy measure. The objective of signal constancy is to think about two signals by giving a quantitative score that can be utilized for depicting the level of likeness or the level of twisting between them. [4][7][20]

Assume $x = \{x_i \mid i = 1,2,3, \dots, N\}$ and $y = \{y_i \mid i = 1,2,3, \dots, N\}$ are two limited length discrete signals, where N is the quantity of signal samples and x_i and y_i are the estimations of the i th sample in x and y individually at that

point, MSE between the signals is given as: [20]

$$MSE(x, y) = \frac{\sum_{i=1}^N (x_i - y_i)^2}{N} \tag{3}$$

As far as images are concerned, MSE is given as:

$$MSE = \frac{\sum_{i=0}^{P-1} \sum_{j=0}^{Q-1} [A(i,j) - B(i,j)]^2}{P \times Q} \tag{4}$$

Where A(i,j) and B(i,j) are cover image and stego image respectively and P&Q is the number of rows and columns in the cover image.[23]

4.4. Hiding Capacity of the Cover Image:

Information installing limit can likewise be considered as a viable method to gauge the proficiency of the concealing procedure. [41] The concealing procedure is viewed as effective if countless bytes can be covered up inside a cover picture without disintegrating it. [37] Consequently the limit of an inserting strategy relies on the aggregate number of bits per pixel and the quantity of bits implanted in every pixel. [26]

Capacity ratio is as given below:

$$Capacity\ Ratio = \frac{Number\ of\ bytes\ to\ be\ embedded}{Total\ number\ of\ bytes\ per\ channel} \tag{5}$$

5. PROPOSED ENCODING & DECODING APPROACHES BASED ON CHAOTIC MAPS

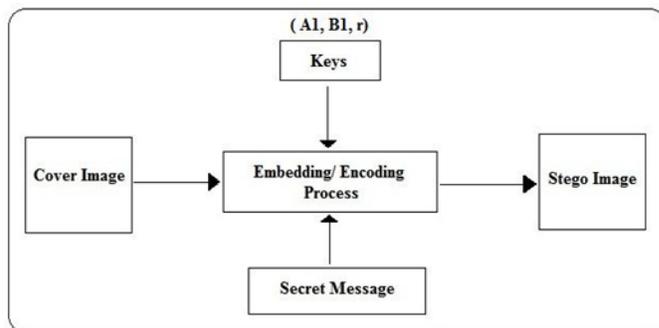


Figure 4: Proposed Encoding Scheme

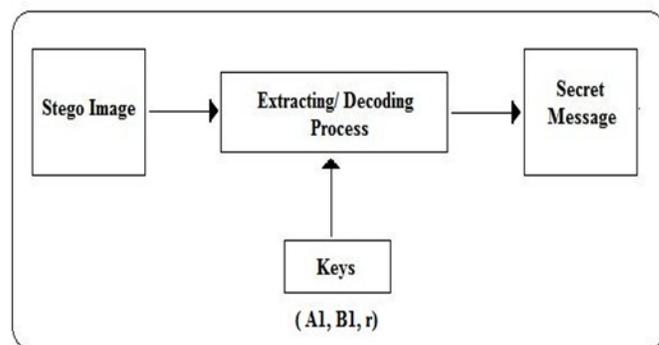


Figure 5: Proposed Decoding Scheme

RESEARCH ARTICLE

In this section proposed chaotic maps based encoding and decoding techniques are presented.

The block diagrams of proposed encoding and decoding processes are shown in Figure 4 & 5 respectively.

5.1. Proposed Insertion Process

The steps in proposed encoding scheme as given in Figure 6, are as illustrated below:

- i. Enter the secret message consisting of “L” characters to be embedded inside the cover image. Convert this mystery message into an arrangement of 8L paired bits. [23]
- ii. Input the image of size (N_r X N_c X 3) used for hiding purpose. This image is known as the cover image.
- iii. Extract the color channels corresponding to red, green and blue components of each & every pixel of the cover image separately.

- iv. Utilizing two-dimensional disorderly maps, produce the pixel areas where the mystery message bits are to be implanted inside the cover picture. The accompanying two capacities are utilized for this reason. [23]

$$A_{i+1} = r[A_i(1 - A_i)] \tag{6}$$

$$B_{i+1} = r[B_i(1 - B_i)] \tag{7}$$

Where the value of i varies from 1 to L.

- v. In request to precisely coordinate the quantity of lines and segments of the cover picture (N_r X N_c). [33] Use the following two formulas to update the chaotic sequences.

$$\sim A_i = [A_i \times N_r] \tag{8}$$

$$\sim B_i = [B_i \times N_c] \tag{9}$$

- vi. Embed each of the 8 bits corresponding to each character of the mystery message into LSB's of RGB parts of the pixels utilizing the 3-3-2 LSB inclusion technique.[7] Repeat step number 6 until all the “L” characters are embedded.

- vii. Output the stego image having exactly the same size (N_r X N_c X 3) as that of the cover image.

5.2. Proposed Extraction Process:

The steps in the proposed decoding scheme as given in Figure 6, are as illustrated below:

- i. Enter the stego image embedded with a secret message.

- ii. Separately extract the color channels corresponding to RGB components of each & every pixel of the stego image.
- iii. Using equation no. 6th & 7th generate the chaotic sequences (A₁,A₂,A₃,.....A_L) and (B₁,B₂,B₃,.....B_L).
- iv. Using equation no. 8th & 9th generate the pixel indices (~A₁,~A₂,~A₃,.....~A_L) and (~B₁,~B₂,~B₃,.....~B_L) where the hidden message bits are lying.
- v. Extract each of the 8 bits corresponding to each and every character of the concealed message from the LSB's of RGB segments of the stego pixels utilizing the 3-3-2 LSB extraction plot. [23]
- vi. Regenerate the corresponding secret message.

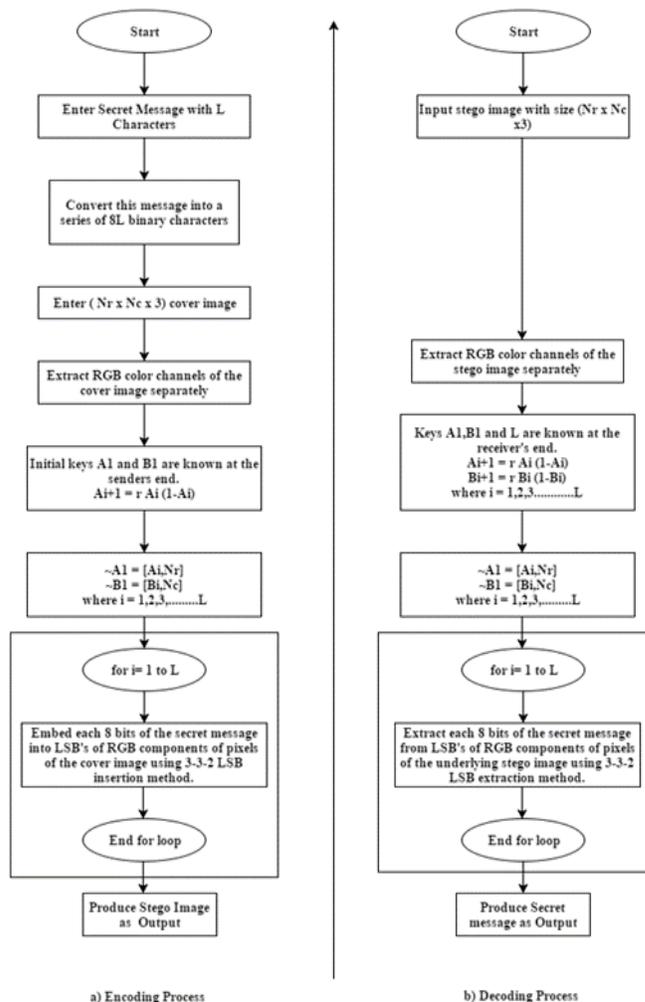


Figure 6: Flowchart of the Proposed Encoding & Decoding Algorithm

RESEARCH ARTICLE

6. IMPLEMENTATION & RESULTS

The proposed algorithms for encoding and decoding purposes have been implemented in MATLAB. For standardization, some standard digital colored images have been selected for experiment purpose from the USC-SIPI digital image database [19]. Some of the images used are shown in Table 2. Size of images selected is 512 x 512 x 3. Results are acquired in the wake of applying the proposed calculations on some standard pictures like Airplane (4.2.05) and Sailboat (4.2.06). The instant message to be covered up inside the pictures is 1 kilobyte in size [23] and is shown in Figure 7.

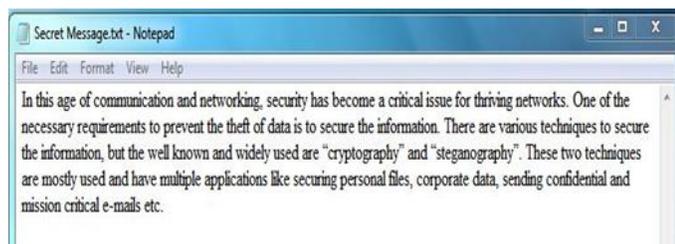


Figure 7: Mystery Message Record to be Inserted in the Picture

For directing the trial, the estimation of r has been set to "3.7688" and the underlying estimations of even and vertical disordered maps are set to $A1 = 0.7$ and $B1 = 0.6$ separately. Diverse assessment measurements have been utilized to survey the effectiveness of the proposed plans. [23][45] A portion of the measurements utilized are MSE, histogram examination, PSNR and so forth.

Image Name (Code)	Mean Squared Error			Peak Signal to Noise Ratio		
	Red component	Green Component	Blue Component	Red Component	Green Component	Blue Component
Airplane (4.2.05)	0.0269	0.0278	0.0082	65.3424	66.1546	72.6582
Sailboat (4.2.06)	0.0252	0.0267	0.0064	66.3151	64.6512	70.6576
Pepper (4.2.07)	0.0232	0.0252	0.0075	66.5645	63.7912	71.7357

Table 1: Experimental MSE & PSNR Values for Some of the Standard Images Embedded with 1KB Textual Data.



Table 2: Some Standard Images of Size (512 X 512 X 3) Taken from USC-SIPI Image Database.

6.1. Discussion of Results

- i. From Table 1 it is quite clear that the value of MSE (Mean square error) is relatively very small which shows that the proposed algorithm is effective in nature.
- ii. PSNR (Peak Signal to Noise Ratio) values as delineated in Table 1 for different standard pictures are moderately extensive, which again features the productivity of the proposed plan.
- iii. From Table 4 it has been seen there is no contrast between the histograms of the cover picture and the stego picture implanted with a 2KB information record. Henceforth nobody would have the capacity to make sense of the presence of the concealed message.
- iv. Using the proposed plan an implanting limit of half has been accomplished as appeared in Table 3, while the estimation of PSNR is still inside a worthy range.
- v. Quality of stego image is still satisfactory despite reaching an embedding capacity of 50% as evident from Table 5.

Size of Secret Message in KB (Kilo Bytes)	Capacity ratio	Capacity ratio %age	Peak Signal to Noise Ratio		
			Red Component	Green Component	Blue Component
1 KB	0.00213	0.2113 %	65.3424	66.1546	72.6582
2 KB	0.0042	0.42 %	62.1252	63.1657	69.1954
4 KB	0.0084	0.84 %	59.3421	60.2351	66.1633
8 KB	0.0169	1.69 %	56.1542	57.3451	63.1020
16 KB	0.0574	5.74 %	53.2308	54.3522	60.6213
32 KB	0.1276	12.76 %	50.3201	51.4512	57.3562

RESEARCH ARTICLE

64 KB	0.2552	25.52 %	47.1211	48.7621	54.3496
128 KB	0.5104	51.04 %	44.2109	45.8028	51.1415
180 KB	0.7045	70.45 %	40.2109	41.8028	47.1415

Table 3: Data Embedding Capacity Analysis for 512 x 512 x 3 “Airplane (4.2.05)” Image.

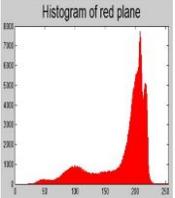
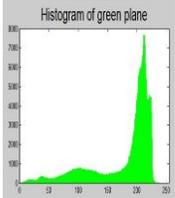
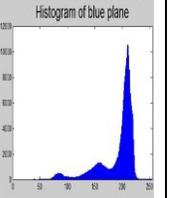
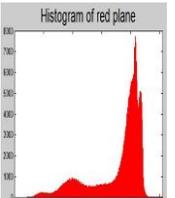
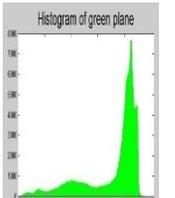
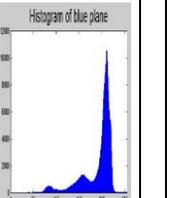
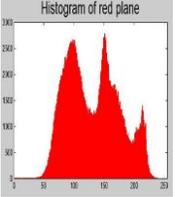
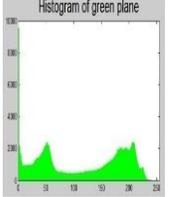
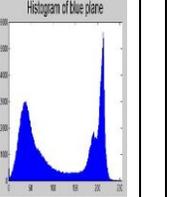
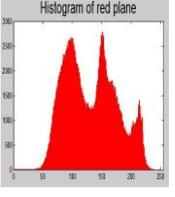
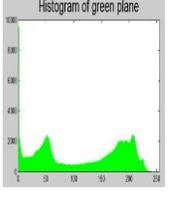
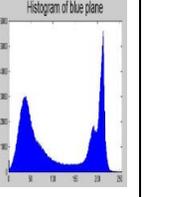
Image	Red Component	Green Component	Blue Component
Airplane.jpg (4.2.05)  (Cover Image)			
Airplane.jpg (4.2.05)  (Stego Image)			
Sailboat (4.2.06)  (Cover Image)			
Sailboat (4.2.06)  (Stego Image)			

Table 4: Histogram Examination of Cover Picture and Stego Picture Installed with 2 KB Information Document.

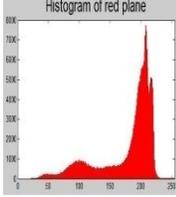
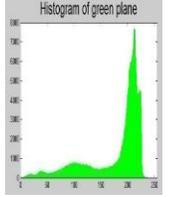
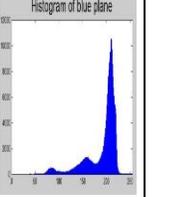
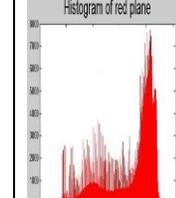
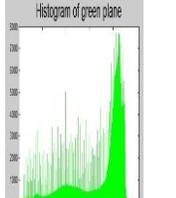
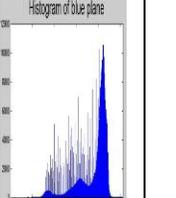
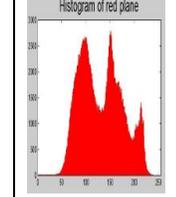
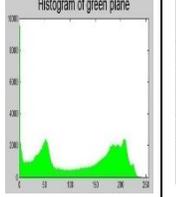
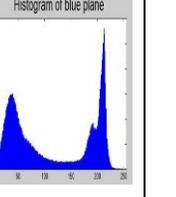
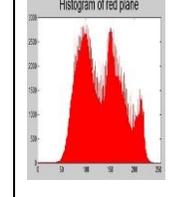
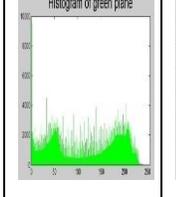
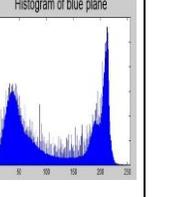
Image	Red Component	Green Component	Blue Component
Airplane.jpg (4.2.05)  (Cover Image)			
Airplane.jpg (4.2.05)  (Stego Image)			
Sailboat (4.2.06)  (Cover Image)			
Sailboat (4.2.06)  (Stego Image)			

Table 5: Histogram Examination of Cover Picture and Stego Picture Installed with 180 KB Information Document.

7. CORRELATION OF PROPOSED ALGORITHM WITH SOME OF THE OTHER TECHNIQUES FROM LITERATURE

The outcomes gotten by utilizing the proposed plan are very energizing. Yet at the same time, so as to additionally evaluate the effectiveness of the proposed calculation, It has been contrasted and different plans described in the writing review. Table 6 demonstrates the examination results. The measurements utilized for examination are Mean Square Error and PSNR. The correlation is performed by applying the proposed plan on standard picture Airplane.jpg (4.2.05) and

RESEARCH ARTICLE

contrasting the outcomes delivered and the best consequences of the other related plans talked about in the writing. The got outcomes demonstrate the extraordinary capability of the proposed method when contrasted with alternate strategies.

8. CONCLUSION

In this research paper, another and very productive methodology has been displayed for covering up literary records inside computerized hue pictures utilizing two-dimensional riotous mapping plan. The comparing bits of the mystery message are implanted inside the cover picture utilizing the 3-3-2 LSB addition strategy. The proposed calculation not just implants the mystery message inside the cover picture yet in addition gives an abnormal state of security inferable from the way that area of installed mystery message bits are obscure to the busybody and it is exceptionally hard to replicate the correct areas until the point when starting disorderly guide conditions are known. The proposed calculation has been connected and effectively tried on different standard pictures delivering results which are far superior to the outcomes created by other comparable methods.

REFERENCES

- [1] William Stallings, (2003) Cryptography and Network Security, Principles & Practices, third edition, Pearson Education, Singapore.
- [2] B. Dunba. (2002). A detailed look at steganographic techniques and their use in an open system environment, Sans institute.
- [3] C. Christian. An Information Theoretic Model for Steganography, Proceedings of 2nd Workshop on information Hiding, MIT laboratory.
- [4] Jhonson, January 2002. Survey of Steganography Software, technical report.
- [5] Krenn, R. “Steganography and Steganalysis”, <http://www.krenn.nl/univ/cry/steg/article.pdf>
- [6] Dey, S., Abraham, A., Sanyal, S. (2007, August). An LSB data hiding technique using prime numbers. In Information Assurance and Security, 2007. IAS 2007. Third International Symposium on (pp. 101-108). IEEE.
- [7] Yu, L., Zhao, Y., Ni, R., Li, T. (2010). Improved adaptive LSB steganography based on chaos and genetic algorithm. EURASIP Journal on Advances in Signal Processing, 2010, 32.
- [8] Liao, X., Wen, Q. Y., Zhang, J. (2011). A steganographic method for digital images with four-pixel differencing and modified LSB substitution. Journal of Visual Communication and Image Representation, 22(1), 1-8.
- [9] Kumar, A., Kumari, S., Patro, S., Sh, T., Acharya, A. K. Image Steganography using Index based Chaotic Mapping., IJCA Proceedings on International Conference on Distributed Computing and Internet Technology, ICDCIT 2015(1):1-4, January 2015.
- [10] Zaghbani, S., Rhouma, R. (2013, April). Data hiding in spatial domain image using chaotic map. In Modeling, Simulation and Applied Optimization (ICMSAO), 2013 5th International Conference on (pp. 1-5). IEEE.
- [11] Anees, A., Siddiqui, A. M., Ahmed, J., Hussain, I. (2014). A technique for digital steganography using chaotic maps. Nonlinear Dynamics, 75(4), 807-816.
- [12] Ghebleh, M., Kanso, A. (2014). A robust chaotic algorithm for digital image steganography. Communications in Nonlinear Science and Numerical Simulation, 19(6), 1898-1907.
- [13] Kanso, A. (2012). Steganographic algorithm based on a chaotic map. Communications in Nonlinear Science and Numerical Simulation, 17(8), 3287-3302.
- [14] Juneja, M., Sandhu, P. S. (2013). An improved LSB based steganography technique for RGB color images. International Journal of Computer and Communication Engineering, 2(4), 513.
- [15] Bandyopadhyay, D., Dasgupta, K., Mandal, J. K., Dutta, P. (2014). A novel secure image steganography method based on Chaos theory in

	Results Obtained					
	Mean Squared Error (MSE)			Peak Signal to Noise Ratio (PSNR)		
	Red Component	Green Component	Blue Component	Red Component	Green Component	Blue Component
Proposed work	0.0269	0.0278	0.0082	65.3424	66.1546	72.6582
Adaptive LSB steganography [7]	-	-	-	38.521	39.72	39.93
Four pixel differencing LSB substitution algorithm[8]	-	-	-	44.58		
Index based chaotic mapping [9]	0.15	0.06	0.06	56.3392	60.3137	60.5805
Spatial domain imaging using chaotic maps [10]	-	-	-	52.8754		
Chaotic digital steganography [11]	0.0441	0.0108	0.0025	55.4126	55.4126	55.4126
Steganographic chaotic maps [13]	-	-	-	45.04	46.46	47.74
LSB steganography [14]	-	-	-	45.9238		

Table 6: Correlation of Proposed Calculation with a Portion of the Strategies Referenced in Literature Audit.

RESEARCH ARTICLE

spatial domain. *International Journal of Security, Privacy and Trust Management (IJSPTM)*, 3(1), 11-22.

[16] Dasgupta, K., Mandal, J. K., Dutta, P. (2012). Hash based least significant bit technique for video steganography (HLSB). *International Journal of Security, Privacy and Trust Management (IJSPTM)*, 1(2), 1-11.

[17] Cheddad, A., Condell, J., Curran, K., Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal processing*, 90(3), 727-752.

[18] Goel, S., Rana, A., Kaur, M. (2013). A review of comparison techniques of image steganography. *Global Journal of Computer Science and Technology*, 13(4).

[19] The USC-SIPI Image Database, University of Southern California, Signal and Image Processing Institute. Available at: <http://sipi.usc.edu/database/>, last accessed in February 2016.

[20] Zhou Wang and Alan C. Bovik (2009). Mean Squared Error: Love It or Leave It? A new look at signal fidelity measures. *IEEE signal processing Magazine*.

[21] www.merriam-webster.com/dictionary/cryptography.

[22] Suchi Agarwal, Dr. Jaipal Singh Bhist (2016). Data hiding in digital image processing using cryptography and steganography. *IRJET*, vol. 03, issue: 05.

[23] Mervat Mikhail, Yasmine Abouelseoud, Galal Elkobrosy. "Text Hiding in a Digital Cover Image using Two Dimensional Indexing based on Chaotic Maps" *International Journal of Computer Applications (0975 - 8887) Volume 138 - No.12, March 2016*.

[24] Vipul Sharma, Madhusudan (2015). "Two new approaches for image steganography using cryptography", 2015 Third international conference on image information processing (ICIIP), 2015.

[25] Vipul Sharma, Sunny Kumar (2013). "A new approach to hide text in images using steganography". *IJARCSSE* (2013).

[26] Hassan Elkamchouchi, Wessam M. Salama, Yasmine Abouelseoud. "Data hiding in a digital cover image using chaotic maps & LSB technique", 2017 12th International Conference on Computer Engineering and Systems (ICCES), 2017

[27] Goel, Stuti, Arun Rana, and Manpreet Kaur. "ADCT-based Robust Methodology for Image Steganography", *International Journal of Image Graphics and Signal Processing*, 2013.

[28] Sharif, Ami, Majid Mollaeafar, and Mahboubeh Nazari. "A novel method for digital image steganography based on a new three-dimensional chaotic map", *Multimedia Tools & Applications*, 2016.

[29] J.K. Mandal, A. Khamrui. "A Genetic Algorithm based steganography in frequency domain (GASFD)", 2011 International Conference on Communication and Industrial Application, 2011.

[30] [preview-springerplus.springeropen.com](http://preview.springerplus.springeropen.com)

[31] Abid Yahya. "Steganography Techniques for Digital Images", *Springer Nature*, 2019.

[32] Nadeem Akhtar, Pragati Johri, Shahbaaz Khan. "Enhancing the Security and Quality of LSB Based Image Steganography", 2013 5th International Conference on Computational Intelligence and Communication Networks, 2013.

[33] Reddy, Velagalapalli Lokeswara, Arige Subramanyam, and Pakanati Chenna Reddy. "A novel technique for JPEG image steganography and its performance evaluation", *International Journal of Advanced Media and Communication*, 2014.

[34] Jiang, Nan, Na Zhao, and Luo Wang. "LSB Based Quantum Image Steganography Algorithm", *International Journal of Theoretical Physics*, 2015.

[35] H. Nabaee, K.Faez. "An efficient steganography method based on reducing changes", 2010 25th International Conference of Image and Vision Computing New Zealand, 2010.

[36] Shabir A. Parah, Javaid A. Sheikh, Abdul M. Hafiz, G.M. Bhat. "Data hiding in scrambled images: A new double layer security data hiding technique", *Computers & Electrical Engineering*, 2014.

[37] Dadgostar, H., and F. Afshari. "Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB", *Journal of Information Security and Applications*, 2016.

[38] Prabira Kumar Sethy, Kamal Pradhan, Santi Kumar Behera. "A security enhanced approach for video Steganography using K-Means clustering and direct mapping", 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), 2016.

[39] Tamer Rabie, Mohammed Baziyad, Ibrahim Kamel. "Enhanced high capacity image steganography using discrete wavelet transform and the laplacian pyramid", *Multimedia Tools & Applications*, 2018.

[40] Maheshwari, S.Uma, and D.Jude Hemanth. "Different methodology for image steganography-based data hiding: review paper", *International Journal of Information and Communication technology*, 2015.

[41] Sajasi, Sara, and Amir-Masoud Eftekhari Moghadam. "An adaptive image steganographic scheme based on Noise Visibility Function and an optimal chaotic based encryption method", *Applied Soft Computing*, 2015.

[42] Vinsa Varghese. "A secure method for hiding data on cubism image using hybrid feature detection method", *International Journal of Research in Engineering and Technology*, 2014.

[43] Omar Banimelhem, Lo'ai Tawalbeh, Moad Mowafi, Mohammed Al-Batati. "A more secure image hiding scheme using pixel adjustment and genetic algorithm", *International Journal of Information Security and Privacy*, 2013.

[44] M.Ghebleh, A. Kalso. "A robust chaotic algorithm for digital image steganography", *Communications in Nonlinear Science and Numerical Simulation*, 2014

[45] "Intelligent Systems Design and Applications", *Springer Nature*, 2018

[46] Dogan, Sengul. "A new data hiding method based on chaos embedded genetic algorithm for color image", *Artificial Intelligence Review*, 2016.

[47] *Advances in Intelligent Systems and Computing*, 2016.

[48] Sarosh K. Dastoor. "Comparative Analysis of Steganographic algorithms intacting the information in the speech signal for enhancing the message security in next generation mobile devices", 2011 World Congress on Information and Communication Technologies, 2011.

Authors



Vipul Sharma is a research scholar in the Department of Computer Science & Engineering at NIT Srinagar, INDIA. He received his B.Tech (Hons) degree in Computer Science & Engineering from Lovely Professional University, Punjab in 2011 and his M.Tech degree in Computer Science & Engineering from JUIT Solan in the year 2013. His research interests include Steganography, Digital Image Processing, Pattern recognition & Machine Learning.



Dr. Roohie N Mir is a professor in the Department of Computer Science & Engineering at NIT Srinagar, INDIA. She received B.E. (Hons) in Electrical Engineering from University of Kashmir (India) in 1985, M.E. in Computer Science & Engineering from IISc Bangalore (India) in 1990 and Ph D from University of Kashmir, (India) in 2005. She is a Fellow of IET and IETE India, senior member of IEEE and a member of IACSIT and IAENG. She is the author

of many scientific publications in international journals and conferences. Her current research interests include reconfigurable computing and architecture, mobile and pervasive computing, security and routing in wireless ad hoc and sensor networks.