



# Reversible Secured Data Hiding using Binary Encryption and Digital Bit Modification Scheme

**Sunita Waykole<sup>1</sup>, Archana Sharma<sup>2</sup>**

<sup>1</sup>PhD. Scholar, Mewar University, Gangrar in Chittorgarh (Rajasthan), India  
Email: swaykole2021@gmail.com

<sup>2</sup>Professor, Technocrat Institute of Technology, Bhopal, India

Received 9 December, 2021; Revised 12 March, 2022; Accepted 12 March, 2022

Available online 13 March, 2022 at [www.atlas-tjes.org](http://www.atlas-tjes.org), doi: 10.22545/2022/00181

The information is getting precious day by day because of the digital revolution and more reach exposure of citizens to technology. Information security is in demand and the topmost priority among researchers to develop data security systems. Image steganography is an invisible data hiding scheme, although it uses visual image media to hide information. Steganography is not only limited to images. There are other media like text, audio, or video that can hide information. In this research work, a novel data hiding is being developed using an image as cover media. During the development of the technique, researchers face maintaining the payload capacity and higher Peak Signal to Noise Ratio (PSNR) values while maintaining other parameters. This work uses color images as cover and digital bit modification methods to hide secure information. Only hiding is not enough to secure information. An additional layer of security is added by encrypting a secure message using an encryption method. The digital bit modification method is unconventionally spread the sequential bitstream over channels. This would make this approach unique and better as it keeps the PSNR level higher along with NCC and lowers MSE. All this is done by keeping the payload capacity as the maximum available. According to the proposed algorithm results, the average value of PSNR is 60.295dB, NCC is 1.00, and MSE is 0.1567.

**Keywords:** Image processing; secure data hiding; high payload capacity; image steganography; information security; encryption, reversible data hiding.

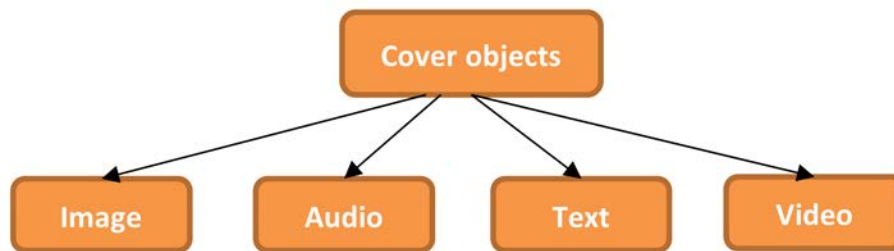
## 1 Introduction

The media of communication among all humans are being shifted to digital platforms. Such media are transfer information over wireless and wired networks. Such networks are mostly public networks, and the information is sharing through these methods are not secure enough and may present serious threats to reveal the private information. With such a problem's information security, the confidentiality of access control and its distribution arises among the researchers. Secret data hiding and protection should be higher at all levels of systems [1].

So, information hiding is under important consideration of digital data practices, which could either be sharing services or social media platforms or day to day chats applications. Cloud services are among the

most vulnerable system because it involves large of data transfer on public networks and access through insecure channels. This could lead to exposing personal data in serious trouble [2]. Various information security, including data hiding, has been proposed to deal with such situations. Steganography is a technique where the data transmission process is aimed to hide information in an ordinary manner without grabbing much attention for possible statistical detectability. Steganography has various forms of information hiding media which seem ordinary, like audio. The primary use of audio can be podcasts, voice recordings, music clips or audible stories. It is a maximal chance no one can feel suspicious about the audio having some information hidden with it. Similarly, photos, video are other ordinary mediums that are different primary interpretations than secure information-carrying mediums [3].

All digital documents steganography utilizes code fields for irrelevant pieces as spots to conceal encoded messages or images. While such control may somewhat change the nature of the first image, it by and large goes undetected by the unaided eye. During the interaction, attributes of these strategies are to change in the construction and highlights so as not to be recognizable by the natural eye. The three main aspects determining steganography and its usefulness are limit, secrecy, and robustness. The term limit refers to the maximum number of data bits that the cover media can cover. Secrecy refers to the discloser's ability to calculate the secret data without difficulty. Robustness is concerned with the opposite plausibility of modifying or erasing the hidden data.



**Figure 1:** *Different Cover objects for steganography (courtesy of ESO).*

Practically all advanced document configurations can be utilized for steganography, yet the configurations that are more appropriate are those with a severe level of repetition. Repetition can be characterized as the pieces of an article that give exactness far more noteworthy than needed for the item's utilization and show. The excess pieces of an article are those pieces that can be changed without the modification being recognized effectively. Image and audio records particularly follow this necessity, while research has likewise revealed other document designs that can be utilized for data hiding. Figure 1 shows the four principal classes of sight and sound document designs that can be utilized for steganography. There are three different approaches that can be used to hide information in a cover object [7]:

- Injection,
- Substitution and
- Generation

### ***Injection***

The data may be hidden in parts of documents that are ignored by the processing function using the injection approach. Therefore, customer-specific document parts are not changed and leave the documents completely functional. For example, it can add additional harmless bytes in an executable or binary document. Because those bytes don't affect the process, the end-user may not even realize that the documents contain additional

hidden information. However, using an insertion approach changes documents size according to the quantity of data hidden, and therefore, if the documents look extraordinarily huge, it may produce suspicion.

### **Substitution**

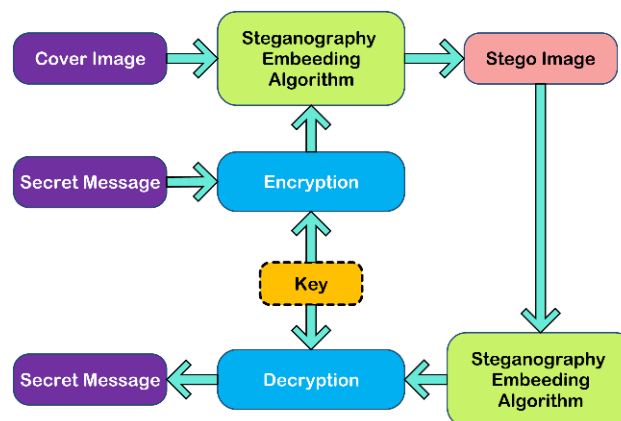
The two-dimensional replacement method is used to return the least important pieces of records. With the least amount of modification, this solves the meaningful content of the unique record. The core benefit of the approach is that the cover documents dimension does not modify after completing the algorithm. This approach has at least two drawbacks. First, the resulting steganography goal can be adversely tormented by exceptional degradation and which could arouse suspicion. Second, substitution limits the number of records that you may hide to the number of little bits within the document.

### **Generation**

Unlike injection and substitution, technology approaches don't need an existing wrap story. This technique generates a cowl document for the only cause of hiding the message. The primary flaw of the insertion and substitution approach is that humans can examine the stego item with any pre-present replica of the cover item (which is to be the same object) and discover differences between the two. Using a generic approach will not have that problem because the result is an original document and is therefore immune to comparison tests.

## **2 System Model**

This work takes images as a carrier medium for secret information, commonly known as image steganography. This image processing domain involves pixel intensities to accommodate the secret information with a cover image. The cover image is the image that is working as a medium. The modification of pixel intensities can be done in various ways. But most of them are based on the least significant bit or LSB in short. One LSB is the most appropriate way of hiding information because of its reversibility, or you can say that robustness against different attacks [4].



**Figure 2:** *Reversible image steganography system.*

This work mainly focuses on image steganography [5]. Therefore, the term cover object now becomes cover image. Figure 2 illustrates an essential information hiding scheme in which the embedding technique takes a cowl photo and a secret photograph as inputs and produces as output a stego image, which is the seemingly unchanged cover image with the embedded data. The stego picture may be sent over the communication links to the receiver, who can bring out the removal course of action to recover the secret message from the stego image [6].

### 3 Methodology

Here we are using text as secret information and colour image as the cover. The least significant bit (LSB) is generally used for secret hiding information behind the cover image because of the robust behaviour against losses. However, in this work LSB method is slightly amended. The colour image has three layers red, green and blue, also called channels. The difference among these is that the LSB method utilizes one channel after another, which clearly means that the first information hides into one of the three channels then the second channel and at the last third channel.

But as per the proposed algorithm, data were hiding using all three channels, but the order is slightly different. All the information is spread over all three channels. The information bits are spread over a channel is as follows  $R \rightarrow G \rightarrow B \rightarrow G \rightarrow R$  and keep Repeating.

Here the steganography algorithm is reversible. That depicts the secret information hidden behind the cover image that can be recovered successfully without any loss. The secret information was secured with logical encryption before being embedded. The whole system is divided into two modules. 1. Secret data embedding module behind a cover image to get stego image. 2. Retrieval or recovering module from stego image. Kindly refer the Figures 2 and 3. Figure 3 shows the module for embedding secret messages, and Figure 4 shows the extraction process.

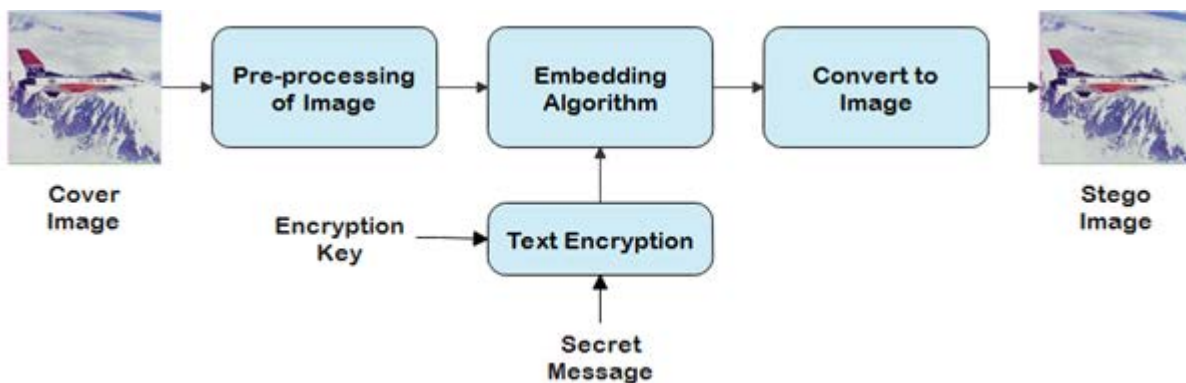


Figure 3: Block diagram of embedding module of secret message.

The proposed algorithm uses MATLAB as a simulation environment for the experiment.

#### A. Embedding Module

The embedding module has the following operations: Input Cover Image: The cover image is given as input to the system and the secret message, as shown in Figure 3. After loading an image into the simulation environment, preprocessing is needed before hiding information. Simultaneously the secret information is encrypted with a key to add one more security layer to secret information. The key is an integer number that can be picked between 0 and 255. After this embedding algorithm or steganography algorithm will start hiding encrypted information behind preprocessed cover image. After completing the embedding process, output data is converted into an image. This is the final output of the embedding module and called a stego image.

The detailed execution flow of the embedding module is shown with the help of the flow chart in Figure 5. For the algorithmic and statement form of representation, a reader can refer to algorithm 1.

**Algorithm 1: Embedding Algorithm**

**Input:** C cover image sized  $M \times N$  and secret message  $S_m$ , sized with L.

**Output:** S stego image with size  $M \times N$ .

1. Load cover image C and secret message  $S_m$ , and convert the cover image into double.
2. Add header information with the secret message.
3. Encrypt secret message by choosing encryption key  $K_e$ , between 0-255.
4. Convert encrypted messages into binary sequences.
5. Check for available payload capacity
6. Separate channels of cover image C and start modifying pixel values in the following order:
  - a. Red Channel  $\rightarrow$  Green Channel  $\rightarrow$  Blue Channel  $\rightarrow$  Green Channel
  - b. Repeat above
7. Combine modified channels and convert them into an image as stego image S.

**B. Extraction Module**

This module is to extract the secret information hidden behind the cover image. For this stego image is given as input to the system. After processing of stego image, it goes to recovering algorithm. Recovering algorithm read the hidden information, and the decryption process follows this information with the same key used for encryption. Finally, as an output of the extraction process, we will get the original secret information hidden with the cover image to refer to in Figure 4.

The detailed execution flow of the extraction module is shown with the help of the flow chart in Figure 6. For the algorithmic and statement form of representation, a reader can refer to algorithm 2.

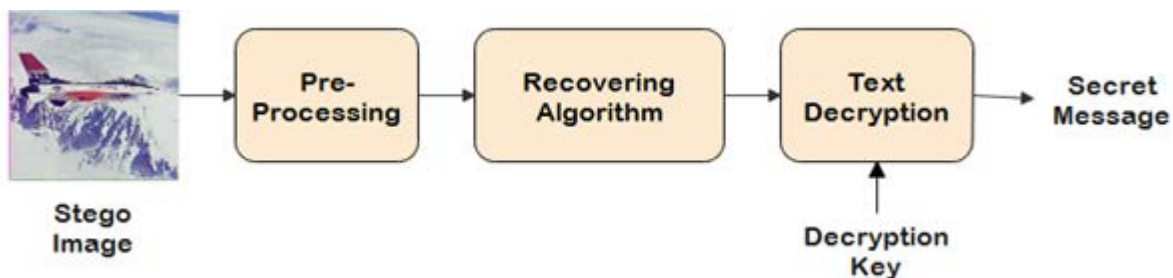


Figure 4: Block diagram of extraction module of secret message.

**Algorithm 2:** Extraction Algorithm**Input:** S stego image with size  $M \times N$ .**Output:** Secret message  $R_m$ , sized with L.

1. Load stego image S and convert into double.
2. Separate channels of cover image S and start reading pixel values in the following order:
  - a. Red Channel  $\rightarrow$  Green Channel  $\rightarrow$  Blue Channel  $\rightarrow$  Green Channel
  - b. append into a binary sequence  $S_b$
  - c. Repeat above
3. Convert binary sequence into characters
4. Decrypt recovered message by using an encryption key  $K_e$ .
5. Show recovered secret message  $R_m$ .

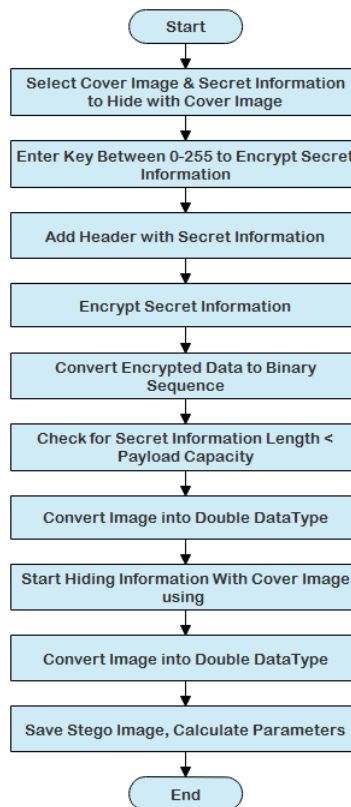


Figure 5: Flow chart of embedding process of secret message.

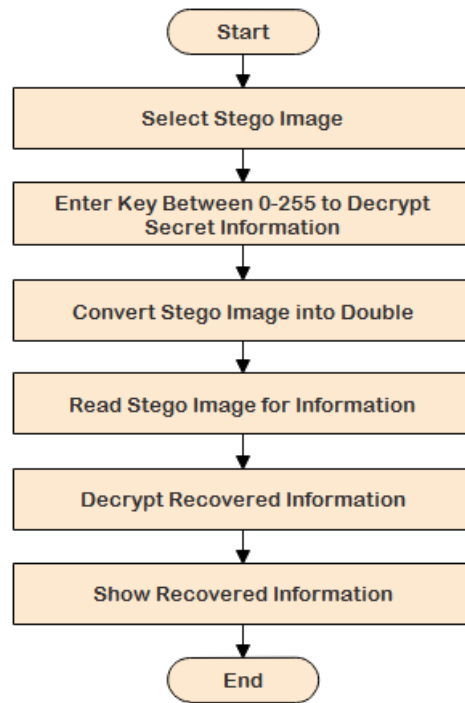


Figure 6: Flow chart of extraction process of secret message.

## 4 Results and Discussion

In this section, we have carried out various input images to test the proposed data hiding algorithm. The payload capacity, visual quality, data security is measured with the help of different performance parameters. The payload capacity is very important in data hiding research because it shows the number of secret bits hiding with the cover image. The experimental setup has been designed and performed on MATLAB. The input cover images are of standard 8-bit of size  $512 \times 512$  pixels shown in Table 1. The secret message is encrypted using an integer key before hiding.

### 4.1 Analysis of Visual Quality of Stego Image

Different performance parameters have been evaluated to measure the visual quality of steganography images. The first one is mean square error (MSE), which finds out the difference between the cover image and stego image due to changes after hiding data. The second one is a root mean square error (RMSE). It is another difference measure evaluated with the help of MSE. The third one is peak signal to noise ratio (PSNR); it is a primary performance measure for quality analysis; if PSNR is higher, the visual quality is better; if it is lower, the visual quality will be degraded. The fourth one is the structural similarity index (SSIM), which shows the skeleton similarity of the cover and stego images. Another performance measure is normalized cross-correlation (NCC), which shows the similarity between two images or matrices, and Q-Value, which shows colour accuracy or quality of the image, is the last. All these measures evaluate the performance of the algorithm and image quality after embedding the information with a cover image.

Histogram comparison illustrates a minuscule change between the cover images and stego images. Hence the cover image and stego image attain decent imperceptibility. Added feature to be measured is Peak Signal to Noise Ratio (PSNR). PSNR is a measure of image quality. PSNR is measured in dB (decibels) and used as a statistical image quality estimation level to measure the distortion between the input and

output stego images. Stego image having PSNR value higher than 30dB than changes occurred due to information is hidden is not visible by human eyes for lower than 30dB PSNR visual difference can be noticed by bare eyes.

Table 3 and Table 9 shows the PSNR attained from the proposed data hiding system. A steganographic scheme needs a high PSNR value, which shows a low difference between the cover and steganography images. Before calculations of PSNR, one needs to calculate mean square error (MSE). Here, the error is the difference between two equal-sized matrices, followed by taking a square and its mean. The formula of PSNR using MSE is given below. The measurement of the quality between the cover image  $I_C$  and stego-image  $I_S$  of sizes  $i, j$  is defined by PSNR as:

$$\text{MSE} = \frac{1}{M.N} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} [I_S(i, j) - I_C(i, j)]^2 \quad (1)$$

$$\text{PSNR} = 10 \log_{10} \left( \frac{C_{\max}^2}{\text{MSE}} \right) \quad (2)$$

Where  $C$  is the maximum value of image colour intensity. The above two formulas are for grayscale or single-channel images. To calculate mean square error (MSE) for RGB (colour) image, we need to calculate MSE for individual channels first; after that, taking an average, it would be calculated for RGB image as given below:

$$\text{MSE}_{\text{RGB}} = \left[ \frac{\text{MSE}_R + \text{MSE}_G + \text{MSE}_B}{3} \right] \quad (3)$$

$$\text{PSNR}_{\text{RGB}} = 10 \log_{10} \left( \frac{C_{\max}^2}{\text{MSE}_{\text{RGB}}} \right) \quad (4)$$

The outcome of PSNR shows that the proposed data hiding scheme is robust and keeps image quality since high PSNR specifies significant image quality. A low value of MSE represents tiny distortion among original and stego images, thus representing high imperceptibility of the arrangement. Also, the proposed scheme offers security since the bits are embedded in unconventional order and have high data hiding capacity, keeping the visual perspective of steganography intact.

$$\text{NCC} = \frac{\sum_{i=0}^{N-1} \sum_{j=0}^{M-1} I_C(i, j) I_S(i, j)}{\sum_{i=0}^{N-1} \sum_{j=0}^{M-1} I_C^2(i, j)} \quad (5)$$

$$\text{NCC}_{\text{RGB}} = \left[ \frac{\text{NCC}_R + \text{NCC}_G + \text{NCC}_B}{3} \right] \quad (6)$$

$$\text{SSIM}(x, y) = I(x, y) \cdot c(x, y) \cdot s(x, y) \quad (7)$$

$$I(x, y) = \frac{2\mu_x \mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \quad (8)$$

$$C(x, y) = \frac{2\sigma_x \sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \quad (9)$$



$$S(x, y) = \frac{2\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \tag{10}$$

Where  $\mu_x, \mu_y, \sigma_x, \sigma_y,$  and  $\sigma_{xy}$  are the local means, standard deviations, and cross-covariance for images x, y.

Another more reliable visual quality metric known as the quality index Q [17] is also considered to measure the similarity between cover images and stego images. High values for Q mean that the cover images and stego images are highly correlated, and differences between them are very small. The universal quality index Q can be calculated using

$$Q = \frac{4\sigma_{xy}\bar{x}\bar{y}}{(\sigma_x^2 + \sigma_y^2)[(\bar{x})^2 + (\bar{y})^2]} \tag{11}$$

where x,y,  $\bar{x}$ , and  $\bar{y}$  are the value of the pixels in the cover image, the value of the pixels in the stego image, the mean value of x, the mean value of y, and the  $\sigma_x^2, \sigma_y^2$  and  $\sigma_{xy}^2$  are the variance and covariance of x,y and xy images, respectively.

### 4.2 Tools Used

For the experimental simulation, MATLAB is used. It has significant advantages to performing various numerical calculations for processing the image in many ways. It also has coder and compiler support to convert an algorithm into executables to support all the machine configurations and different operating system environments.

### 4.3 Secret Message

This message is the secret information used in the below results as hiding information behind cover images given in Table 1. However, it will be encrypted with the secret key before hiding this information.

The greatest glory in living lies not in never falling, but in rising every time we fall. - Nelson Mandela

### 4.4 Encrypted Message









The output message is the encrypted version of the secret message given above. To get the original secret information secured. It has been encrypted with the key between 1-255. A key is a number between 1 and 255; beyond that range, the key will be invalid and may not achieve appropriate results. So keep the encryption key in this range will be the best practice to retrieve from the stego image.

```
~:~:~:;<^bo*mxok~oy~*mfexs*cd*fc|cdm*fcoy*de~*cd*do|ox*lkffcdm&*h&~*cd*x
cycdm*o|oxs*~cgo*}o*lkff$**Dofyed*Gkdnofk
```











Table 1 shows the input images and their stego counterparts after hiding the secret information shown above. The changes between input cover image and stego image are barely visible to the human eye. Analyzing the histogram changes will help us with numerical parametric comparison.

Visually cover, and stego images both are indistinguishable. Such visual results clearly show that the proposed algorithm is robust enough to hide information without affecting the cover image. As steganography changes pixel intensity value while embedding secret information, a graphical change is also introduced during this process. Therefore, histograms of cover and stego images also need to be compared. Table 2 shows the histograms of cover and stego images obtained, respectively. Lower the difference between the histograms of cover and stego image, better the performance of hiding algorithm.

**Table 1:** Input Image and Stego Image

Image	Input Image	Stego Image
Lena		
Baboon		
Pepper		
Airplane		

**Table 1:** Input Image and Stego Image (continued)

House		
Tiffany		
Barbara		
Couple		
Girl		

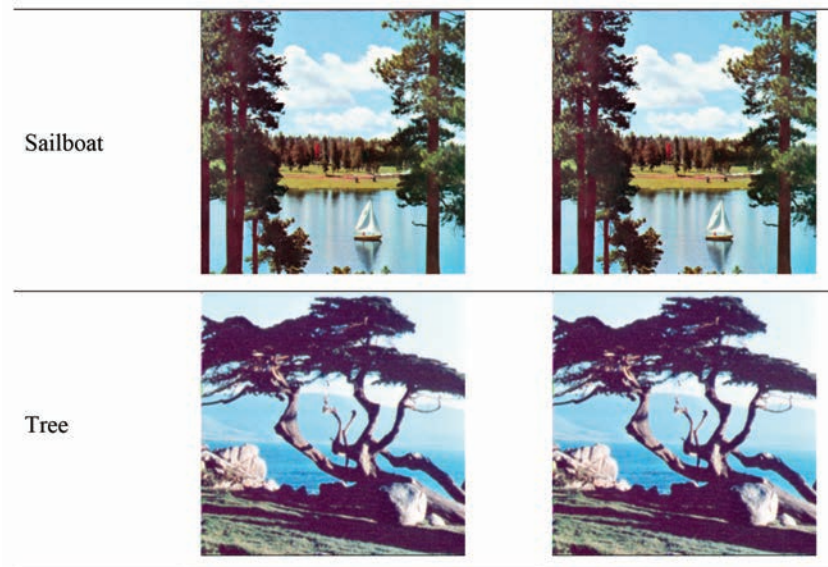
**Table 1:** Input Image and Stego Image (continued)

Table 2 depicts the histograms of the input cover images and their stego counterparts, along with the difference of histograms. This table shows the colour intensities of the red, green and blue channels before and after hiding information from the cover image. The hiding (embedding) process significantly changes the intensities of pixel values, which would reflect in the histogram of the cover image. Nevertheless, with bare eyes, it is hard to identify the changes. So, the histogram difference is also shown to get the exact idea of changes made by secret information to the cover image's red, green, and blue channels.

Table 4 shows the difference between cover image and steganography image and calculated as mean square error. The lowest value of the MSE is 0.15 for Baboon, Pepper and House and 0.17 for Tiffany image.

Table 5 shows the similarity between cover image and steganography image and calculated as normalized cross correlation. The the best value is 1 for all images compared to 0.99 in [1].

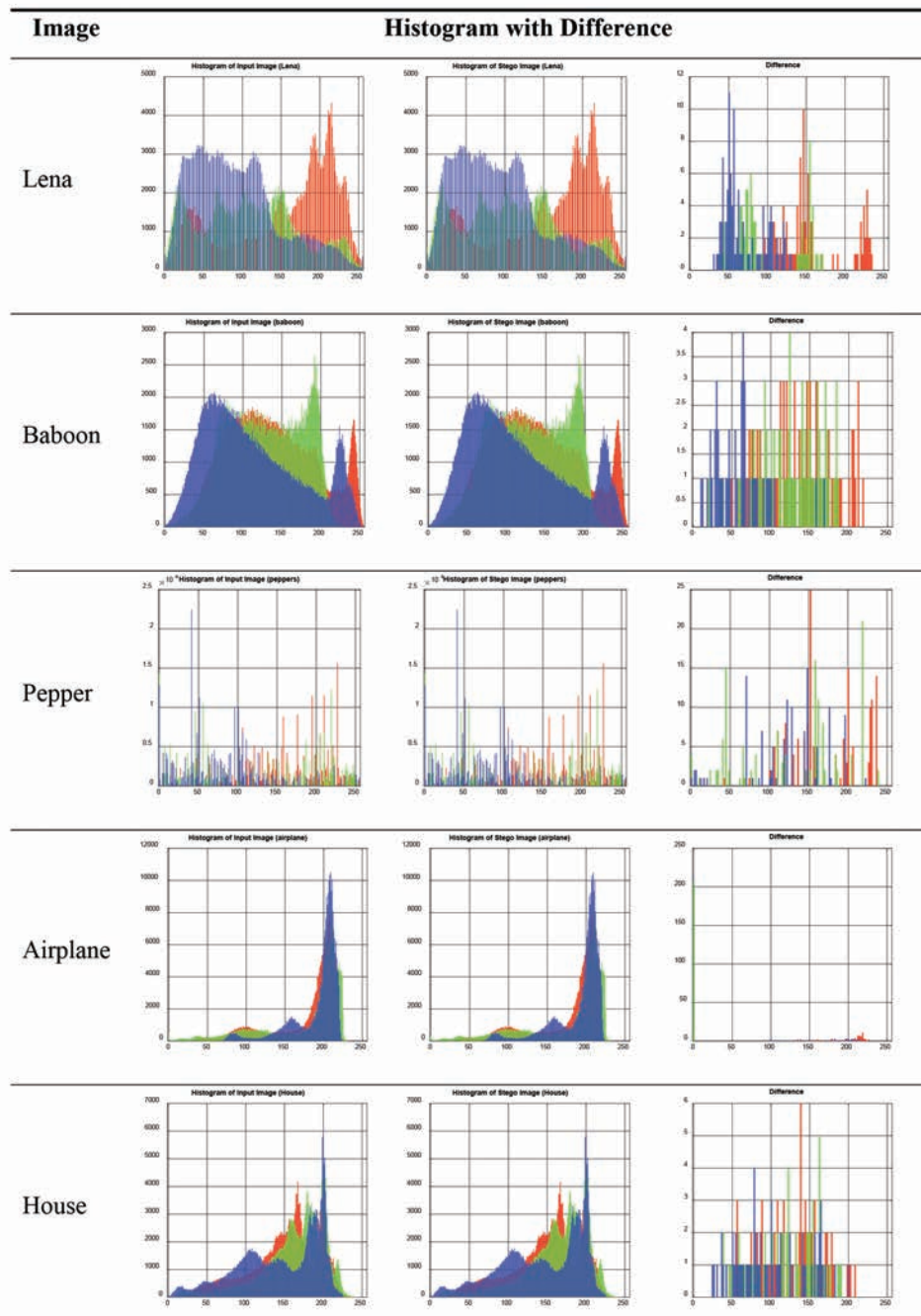
Table 5 shows the square root of MSE. The the lowest value is 12.21 and highest 12.94. The value of SSIM is 1.00 for all images. Table 6 shows the RMSE value of the input images. Table 7 and Table 8 shows the computation time of embedding of secret information with cover image to get steganography image and extraction time of secret message from stego image. The lowest embedding time is 0.034 seconds and highest embedding time is 0.056 seconds. Similarly retrieval time is 0.029 seconds lowest and 0.04 highest. These timings are compared with [2] and found 98% faster total (embedding + retrieval) time.

Table 10 shows the Q-value comparison with [2] and achieved 1.0 for all images using proposed algorithm.

## 5 Conclusion

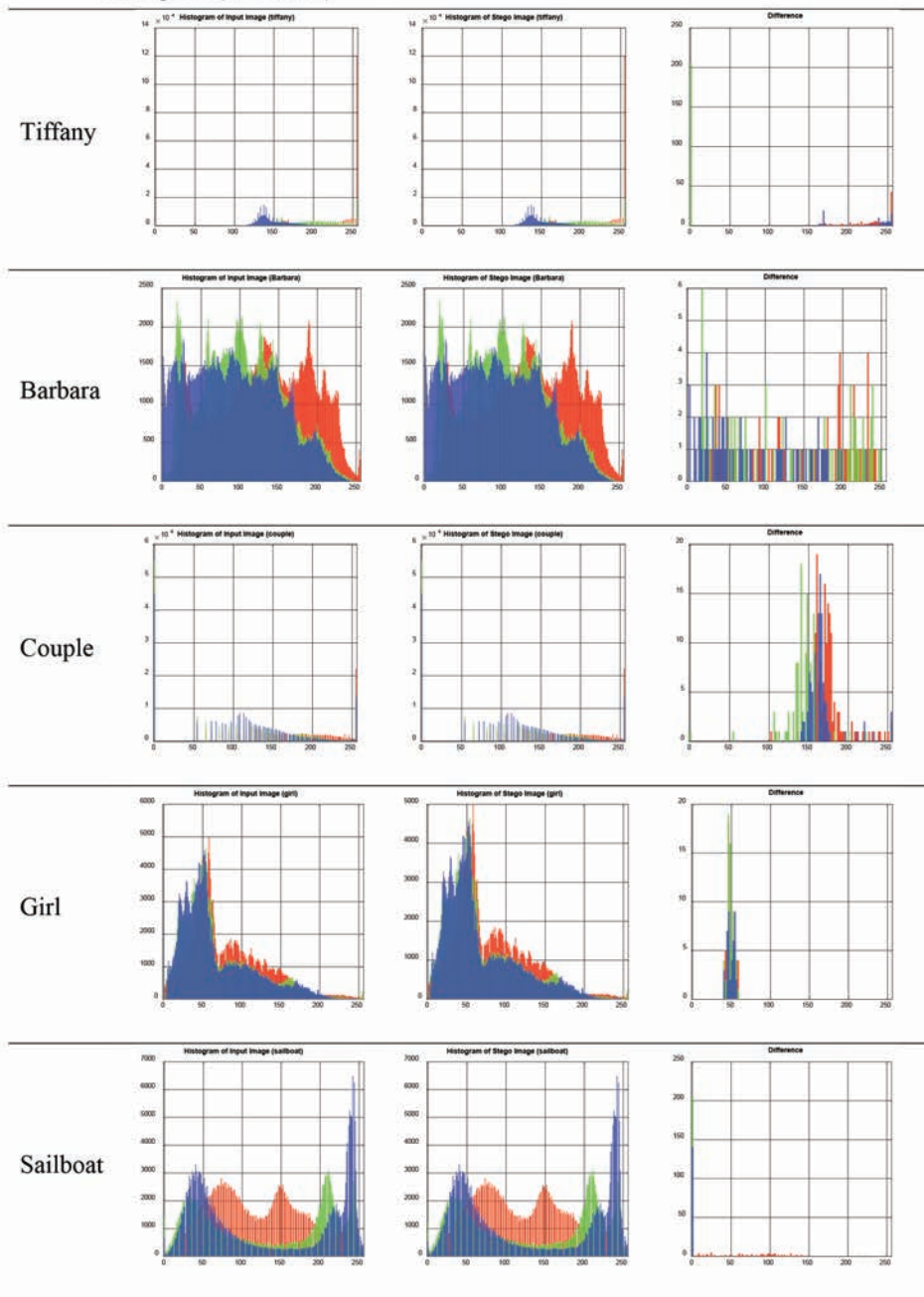
The image steganography system developed in this research work has targeted the problem of lower payload capacity and the peak signal to noise ratio problem due to changes in the pixel intensities during the hiding of secret information. This method utilizes the digital bit modification method and spreads the encrypted information unconventionally over channels. The security is enhanced with binary encryption to secure secret messages before being hidden in the cover image. This approach performed significantly better in PSNR, NCC, and MSE, keeping payload capacity at the maximum level. The unconventional

Table 2: RGB Histogram of Input Image and Stego Image respectively with difference histogram

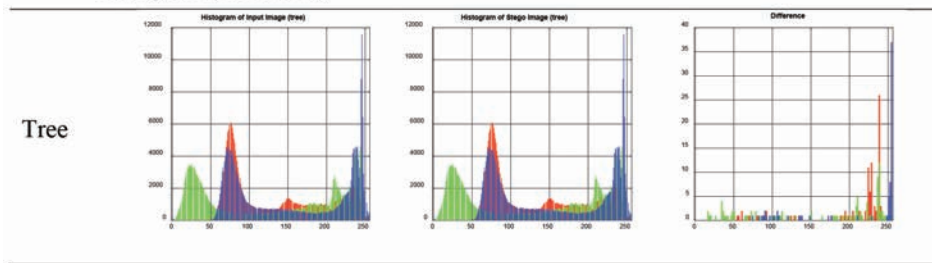


way to spread the information looks similar to LSB but has a different approach to modifying pixel values, making it unique and secure than the benchmark and standard methods.

**Table 2:** RGB Histogram of Input Image and Stego Image respectively with difference histogram (continued)



**Table 2:** RGB Histogram of Input Image and Stego Image respectively with difference histogram (continued)



**Table 3:** PSNR (dB) values comparison

Technique	Lena	Baboon	Pepper	Airplane	House	Tiffany
Proposed	59.93	60.72	60.79	60.03	60.67	59.63
IWT-LSB[1]	55.51	55.56	55.20	54.79	55.55	53.06

**Table 4:** MSE values comparison

Technique	Lena	Baboon	Pepper	Airplane	House	Tiffany
Proposed	0.16	0.15	0.15	0.16	0.15	0.17
IWT-LSB[1]	0.18	0.18	0.17	0.18	0.18	0.32

**Table 5:** NCC values comparison

Technique	Lena	Baboon	Pepper	Airplane	House	Tiffany
Proposed	1.00	1.00	1.00	1.00	1.00	1.00
IWT-LSB[1]	0.99	0.99	0.99	0.99	0.99	0.99

**Table 6:** RMSE and SSIM values for images

Parameter	Lena	Baboon	Pepper	Airplane	House	Tiffany
RMSE	12.74	12.25	12.21	12.68	12.28	12.94
SSIM	1.00	1.00	1.00	1.00	1.00	1.00

**Table 7:** Computational Time (in seconds)

Module	Lena	Baboon	Pepper	Airplane	House	Tiffany	Average
Embedding	0.037	0.038	0.036	0.034	0.042	0.039	0.056
Retrieval	0.033	0.030	0.040	0.038	0.039	0.029	0.033
Total	0.07	0.068	0.076	0.072	0.081	0.068	0.089

**Table 8:** Comparison of Computational Time (in seconds)

Technique	Embedding Time	Extraction Time	Total Time	%
Proposed	0.056	0.033	0.089	98% Faster
HOG and PVD-LSB [2]	2.5	2.0	4.5	-

**Table 9:** Comparison of PSNR (dB) with [2]

Module	Lena	Baboon	Pepper	Airplane	Boat	Couple	Lake	Tiffany
Proposed Method	59.93	60.72	60.79	60.03	60.24	60.48	59.59	59.63
HOG and PVD-LSB [2]	44.61	42.86	44.64	44.88	43.51	43.76	44.91	44.71

**Table 10:** Comparison of Q-Value with [2]

Module	Lena	Baboon	Pepper	Airplane	Boat	Couple	Lake	Tiffany
Proposed Method	1.0000	1.0000	1.0000	1.0000	0.9999	1.0000	1.0000	1.0000
HOG and PVD-LSB [2]	0.9996	0.9925	0.9986	0.9993	0.9987	0.9988	0.9992	0.9991

**Funding:** This research article received no external funding.

**Conflicts of Interest:** The author declares no conflict of interest.



Copyright ©2022 by the authors. This is an open access article distributed under the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.



## References

- [1] Emad, E., Safey, A., Refaat, A., Osama,Z., Sayed, E., and Mohamed, E., (2018). A secure image steganography algorithm based on least significant bit and integer wavelet transform. in *Journal of Systems Engineering and Electronics*, vol. 29, no. 3, pp. 639-649.
- [2] Almohammad, A., Ghinea, G. and Hierons, R.M. (2009). JPEG Steganography: A Performance Evaluation of Quantization Tables, in *2009 International Conference on Advanced Information Networking and Applications*. Bradford, United Kingdom: IEEE, pp. 471–478.
- [3] Brandao, A.S. and Jorge, D.C. (2016). Artificial Neural Networks Applied to Image Steganography. *IEEE Latin America Transactions*, 14(3), pp. 1361–1366.
- [4] Cheddad, A. et al. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing*, 90(3), pp. 727–752.
- [5] Duan, X. et al. (2020). High-Capacity Image Steganography Based on Improved FC-DenseNet. *IEEE Access*, 8, pp. 170174–170182.
- [6] Hameed, M.A. et al. (2019). An Adaptive Image Steganography Method Based on Histogram of Oriented Gradient and PVD-LSB Techniques. *IEEE Access*, 7, pp. 185189–185204.
- [7] Hemalatha, S. et al. (2012). A secure image steganography technique using Integer Wavelet Transform, in *2012 World Congress on Information and Communication Technologies. 2012 World Congress on Information and Communication Technologies (WICT)*, Trivandrum, India: IEEE, pp. 755–758.
- [8] Khan, S. et al. (2020). Reversible-Enhanced Stego Block Chaining Image Steganography: A Highly Efficient Data Hiding Technique. *Canadian Journal of Electrical and Computer Engineering*, 43(2), pp. 66–72.
- [9] Ntalianis, K. and Tsapatsoulis, N. (2016). Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks. *IEEE Transactions on Emerging Topics in Computing*, 4(1), pp. 156–174.
- [10] Sachdeva, S. and Kumar, A. (2012). Colour Image Steganography Based on Modified Quantization Table. in *2012 Second International Conference on Advanced Computing & Communication Technologies. Communication Technologies (ACCT)*, Rohtak,Haryana, India: IEEE, pp. 309–313.
- [11] Soni, A., Jain, J. and Roshan, R. (2013). Image Steganography using Discrete Fractional Fourier Transform, p. 4.
- [12] Thangadurai, K. and Sudha Devi, G. (2014). An analysis of LSB based image steganography techniques. in *2014 International Conference on Computer Communication and Informatics. 2014 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India: IEEE, pp. 1–4.
- [13] Weiqi Luo, Fangjun Huang, and Jiwu Huang (2010). Edge Adaptive Image Steganography Based on LSB Matching Revisited. *IEEE Transactions on Information Forensics and Security*, 5(2), pp. 201–214.
- [14] Yang, J. and Zhong, S.-P. (2012). A JPEG image blind steganography detection method using KCCA feature fusion. in *2012 International Conference on Wavelet Analysis and Pattern Recognition. 2012 International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR)*, Xian, China: IEEE, pp. 222–226.

## About the Authors



**Sunita Waykole** is a Ph.D. research scholar at Mewar University, Chittorgarh Rajasthan (India). She received a Master of Technology degree in Digital Communication from Rajiv Gandhi Proudhyogiki Vishvavidyalaya, Bhopal

(India). She is a lifetime member of the Indian Society for Technical Education (ISTE). Her research interests include image processing, deep learning, and image steganography, including information security in communication.



**Dr. Archana Sharma** has received Ph.D. from Maulana Azad National Institute of Technology, Bhopal (India). She is currently a professor at Technocrats Institute of Technology, Bhopal (India). She is a lifetime member of Professional Institution (IETE). Her research interests include wireless communication, Data communication and security, microwave Antennas, and dielectric resonator antenna. She also reviewed various research papers, including the wireless personal communication in indexed journal.