Efficient Image Data Hiding with Binary Encryption

Sunita Waykole[1], Deepa Indrawal[2], Dr. Archana Sharma[3]
[1,2]*PhD. Scholar, Mewar University*
[3]*Prof. TIT, Bhopal*

Abstract – The data is getting valuable step by step in view of advanced unrest and more arrive at openness of residents to innovation. The security of data is sought after and top most need among scientists to foster information security frameworks. The image steganography is one of the information hiding plan which is imperceptible in nature in spite of the fact that it's anything but an apparent media to shroud data. The steganography not just restricted to image there are other media like content, audio or video can be uses for hiding data. In this examination work a novel information hiding is being created utilizing image as cover media. Scientists are looking during advancement of method is keeping up the payload capacity just as higher PSNR esteems and different boundaries. This work uses color images as cover and digital bit modification method to hide secure information. Only hiding is not enough to secure information there is an addition layer of security was added by encrypting secure message using encryption method. The digital bit modification method is unconventionally spread the sequential bit stream over channels. This would make this approach unique and better as it is keeping the PSNR level higher along with NCC and lower MSE. The average value of PSNR is 53.78dB, NCC is 1.00 and MSE is 3.02.

Keywords – image processing, secure data hiding, high payload capacity, image steganography, information security, encryption, and reversible data hiding.

I. 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 presented serious threats to reveal the private information. With such problem's information security, 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. The cloud services are among most vulnerable system, because it involves large of data transfer on public networks, and access through insecure channels. This could lead to expose personal data in serious trouble [2]. To deal with such situations various information securities including data hiding have been proposed. Steganography is a technique where data transmission process is aimed to hide information in and ordinary manner without grabbing much attention for possible statistical detectability. Steganography has various forms of information hiding media which seems ordinary like audio, the primary use of audio can be podcasts, voice recordings, music clips or audible stories. It is a maximal chance no can feel suspicious about the audio having some information hidden with it. Similarly, photos, video, are other ordinary medium which are different primary interpretation than a secure information carrying medium [3].

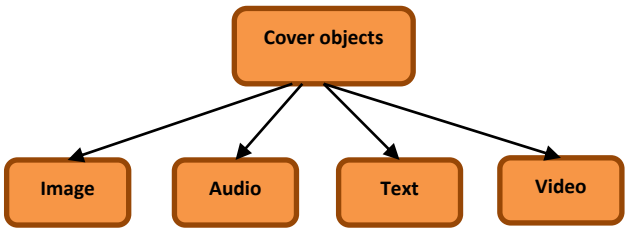

Figure 1 Different Cover Objects for Steganography

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 natural eye. Limit, classification and power, are the three principal perspectives influencing steganography and its value. Limit alludes to the measure of data bits that can be covered up in the cover medium. Secrecy identifies with the capacity of the discloser to calculate the secret data without any problem. Heartiness is worried about the oppose plausibility of adjusting or annihilating the concealed data.

Practically all advanced document configurations can be utilized for steganography, yet the organizations that are more appropriate are those with a serious 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 principle 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 injection approach. Therefore, documents bits that are applicable to a customer are not changed leave-taking the wrap 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

Replacement method is 2d-hand to put returned the least crucial bits of records that solve the meaningful content of the unique record with state-of-the-art statistics in a move that causes the least quantity of deformation. The core benefit of approach that the wrap documents dimension doesn't modify after the completing of the algorithm. On the other hand, this approach has at least two drawbacks. First, the resulting stego goal can be adversely tormented by exceptional degradation and which could arouse suspicion. 2nd, substitution limits the quantity of records that you may hide to the quantity of insignificant bits within the document.

Generation

Unlike inoculation and replacement, 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. It will not have that problem when using a generation approach, because the result is an original document, and is therefore immune to comparison tests.

II. SYSTEM MODEL

In this work images are taken as carrying media for secret information and commonly known as image steganography. This image processing domain involves changes in the pixel intensities to accommodate the secret information with cover image. The cover image is the image which is working as medium. The modification of pixel intensities can be done in various ways. But most of them are based on least significant bit or LSB in short. One or the other LSB is the most appropriate way of hiding information because of its reversibility or you can say that robust ness against different attacks [4].

Steganography approaches expected at furtively thrashing data in a multimedia carrier such as text, audio, image or video, devoid of raising any suspicion of alteration to its contents. The original carrier is referred to as the cover object. In this work, mainly focus on image steganography [5]. Therefore, the term cover object now becomes cover image. Figure 3.1 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].

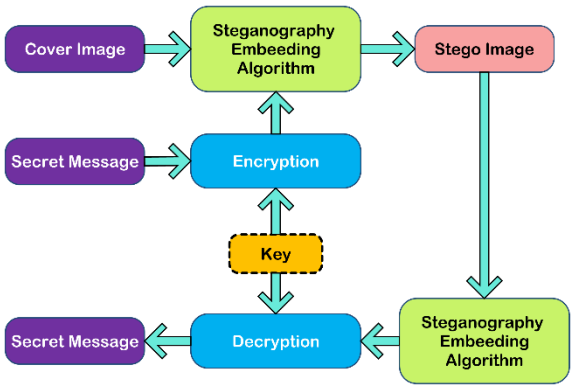

Figure: 1.1Reversible Image Steganography System

III. PROPOSED DATA HIDING METHODOLOGY

Image steganography is a method of hiding one type of information into other type of information. The information being hiding is called secret information, whereas the kind of information behind which secret information is being hidden is called cover. The cover information type can be image, audio or video whereas the secret information can be text, image or audio.

Here we are using text as secret information and color image as cover. For hiding secret information behind cover least significant bit or LSB is generally used. Because of the robust behavior against losses. But in this work LSB method is slightly amended. The difference among these is

that LSB method is utilizes the one channel after another, which clearly means that first information is hiding into one of the three channels than second channel and at last third channel.

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

Here the steganography algorithm is reversible in nature. That depicts the secret information hidden behind cover image 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 cover image to get stego image. 2. Retrieval or recovering module from stego image. Kindly refer the figures 3.1 and 3.2. Figure 3.1 shows the module of embedding secret message and Figure 3.2 shows the extraction process.

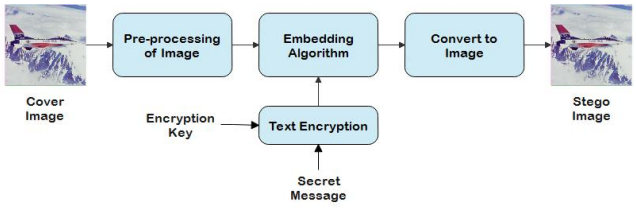

Figure 3.1 Block Diagram of Embedding Module of Secret Message

A. Embedding Module

The embedding module has following operations:

Input Cover Image: Image which is cover image is given as input to the system along with secret message as shown in the figure 3.1. After loading image into simulation environment, there is need of preprocessing before start hiding information. Simultaneously the secret information is encrypted with an encryption to add one more security layer to secret information. After this embedding algorithm or steganography algorithm will start hiding encrypted information behind preprocessed cover image. After completion of embedding algorithm output data converted in to image. This the final output of the embedding module and called as stego image.

The detailed execution flow of embedding module is shown with the help of flow chart in figure 3.3. For the algorithmic and statement form of representation reader can refer algorithm 1.

B. Extraction Module

This module is to extract the secret information hidden behind cover image. For this stego image is given as input to the system and after processing of stego image it goes to recovering algorithm. Recovering algorithm read the hidden information and this information is followed by the decryption process with the same key used for encryption. Finally, as an output of extraction process, we will get the original secret information hidden with cover image refer figure 3.2.

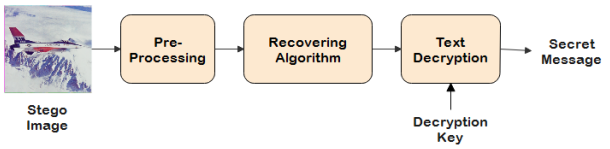

Figure 3.2 Block Diagram of Extraction Module of Secret Message

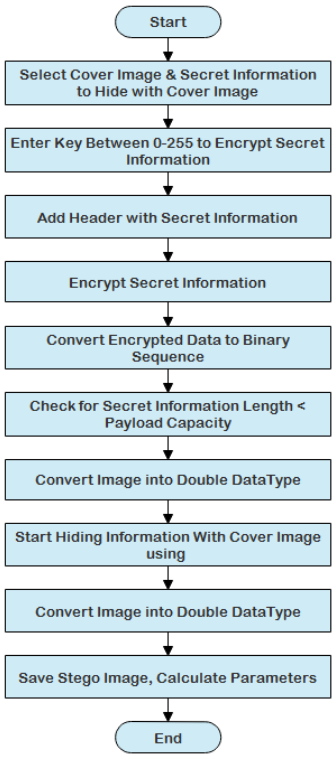

Figure 3.3 Flow Chart of Embedding Process of Secret Message

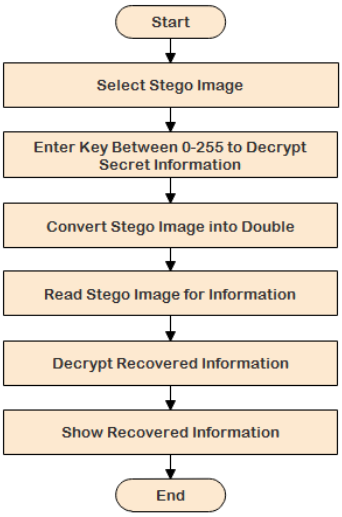

Figure 3.4 Flow Chart of Extraction Process of Secret Message

The detailed execution flow of extraction module is shown with the help of flow chart in figure 3.4. For the algorithmic and statement form of representation reader can refer algorithm 2.

IV. EXPERIMENTAL RESULTS

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 of it shows the number of secret bits hiding with the cover image. The experimental setup has been designed and performed on the MALAB. The input cover images are of standard 8-bit of size 512×512 pixels shown in table 4.1. The secret message is encrypted before hiding.

Analysis of Visual Quality of Stego Image:

For the measurement of visual quality of stego images different performance parameters have been evaluated. First one is mean square error (MSE), it finds out the difference between cover image and stego image due to changes occur after hiding data. Second one is peak signal to noise ratio (PSNR), and NCC it is normalized cross correlation it the main performance measure for quality analysis, if PSNR is higher the visual quality is better, if it is lower than visual quality is degraded. All these measures are for evaluating the performance of algorithm and image quality after embedding the information with cover image.

Added feature to be measured is Peak Signal to Noise Ratio (PSNR). PSNR is a measure to image quality. PSNR is measured in dB (decibels) is used as a statistical image quality estimation level to measure the distortion between the input image and output stego image. Stego image having PSNR value higher than 30dB than changes occurred due to information hidden is not visible by human eyes for lower than 30dB PSNR visual difference can be noticed by bare eyes.

Table 4.2 shows the PSNR attained from the proposed data hiding system. A steganography scheme needs high PSNR value which shows low difference between cover image and stego image. Before calculations of PSNR, one needs to calculate mean square error (MSE). Here error is nothing but the difference of two equal sized matrices, followed by taking square and taking mean of it. 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:

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

$$\mathrm{PSNR} = 10 \lg \left(\frac{C_{\max}^2}{\mathrm{MSE}} \right)$$

The above two formulas are for the grayscale or single channel images. To calculate mean square error (MSE) for RGB (color) image, we need to calculate MSE for individual channel first after that taking average it would be calculated for RGB image as given below:

$$\mathrm{MSE_{RGB}} = \left[\frac{\mathrm{MSE}_R + \mathrm{MSE}_G + \mathrm{MSE}_B}{3} \right]$$

$$\mathrm{PSNR}_{RGB} = 10 \lg \left(\frac{C_{\max}^2}{\mathrm{MSE_{RGB}}} \right)$$

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

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

$$\mathrm{NCC_{RGB}} = \left[\frac{\mathrm{NCC}_R + \mathrm{NCC}_G + \mathrm{NCC}_B}{3} \right]$$

Tools Used:

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

Secret Message:

This message is the secret information used in the below results as hiding information behind cover images given in table 4.1.But before hiding this information it will be encrypted with the secret key.

> *If we could change ourselves, the tendencies in the world would also change. As a man changes his own nature, so does the attitude of the world change towards him. We need not wait to see what others do. - Mahatma Gandhi*

Encrypted Message:

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

```
~::::88:Cl*}o*ie□fn*ibkdmo*e□xyof|oy&*~bo*~odnodic
oy*cd*~bo*}exfn*}e□fn*kfye*ibkdmo$*Ky*k*gkd*ibkdmo
y*bcy*e}d*dk~□xo&*ye*neoy*~bo*k~~c~□no*el*~bo*}exf
n*ibkdmo*~e}kxny*bcg$*]o*doon*de~*}kc~*~e*yoo*}bk~
*e~boxy*ne$*'*Gkbk~gk*Mkdnbc
```

Table 4.1 shows the input images and their stego counterparts after hiding secret information shown above. The changes between input cover images and stego image is barely visible to human eye. To analyze the changes in histogram will help us along with numerical parametric comparison.

Table 4.1 Input Images and Stego Image

Input Image	Stego Image
	

Visually cover and stego images both are indifferentiable. Such visual results clearly show the proposed algorithm is robust to hide information without affecting cover image. As steganography make changes in 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 4.2 PSNR (dB) values comparison

Technique	***Proposed***	***2L-DWTS [1]***
Baboon	53.78	41.48
Lena	53.57	49.82
Barbara	53.93	46.26
Cameraman	53.55	39.82
Pepper	54.08	52.64
Average	*53.78*	*46.01*

Table 4.3 MSE values comparison

Technique	***Proposed***	***2L-DWTS [1]***
Baboon	3.0	4.62
Lena	3.1	0.67
Barbara	3.0	1.53
Cameraman	3.1	6.77
Pepper	2.9	0.35
Average	*3.02*	*2.79*

Table 4.4 NCC values comparison

Technique	***Proposed***	***2L-DWTS [1]***
Baboon	1	0.99
Lena	1	1.00
Barbara	1	0.99
Cameraman	1	0.99
Pepper	1	1.00
Average	*1*	*0.99*

V. CONCLUSION

The image steganography system developed in this research work has targeted the problem of payload capacity and the peak signal to ratio problem due to change in the pixel intensities during hiding of secret information. The method utilizing the digital bit modification method followed by the spreading the encrypted information unconventionally over channels. The security is enhanced with binary encryption so that secret message is secured before being hidden in cover image. This approach performed significantly better in terms of PSNR, NCC and MSE with keeping payload capacity at maximum level. The unconventional way to spread the information looks similar like LSB but has different approach to modify pixel values and this is making it unique and secured than benchmark and standard methods.

REFERENCES

[1] P. Bedi, V. Bhasin, and T. Yadav, "2L-DWTS — Steganography technique based on second level DWT," in *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Jaipur, India, Sep. 2016, pp. 1533–1538. doi: 10.1109/ICACCI.2016.7732266.

[2] S. Nemani, J. Talari, and S. Vangala, "Estimation of performance metrics for Reversible Data Hiding before encryption," in *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, Jun. 2017, pp. 1176–1181. doi: 10.1109/ICCONS.2017.8250653.

[3] A. Setyono, D. R. I. M. Setiadi, and Muljono, "StegoCrypt method using wavelet transform and one-time pad for secret image delivery," in *2017 4th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, Semarang, Oct. 2017, pp. 203–207. doi: 10.1109/ICITACEE.2017.8257703.

[4] N. Akhtar, P. Johri, and S. Khan, "Enhancing the Security and Quality of LSB Based Image Steganography," in *2013 5th International Conference on Computational Intelligence and Communication Networks*, Mathura, India, Sep. 2013, pp. 385–390. doi: 10.1109/CICN.2013.85.

[5] A. Soni, J. Jain, and R. Roshan, “Image Steganography using Discrete Fractional Fourier Transform,” p. 4, 2013.

[6] J. Yang and S.-P. Zhong, “A JPEG image blind steganography detection method using KCCA feature fusion,” in *2012 International Conference on Wavelet Analysis and Pattern Recognition*, Xian, China, Jul. 2012, pp. 222–226. doi: 10.1109/ICWAPR.2012.6294782.

[7] S. Sachdeva and A. Kumar, “Colour Image Steganography Based on Modified Quantization Table,” in *2012 Second International Conference on Advanced Computing & Communication Technologies*, Rohtak,Haryana, India, Jan. 2012, pp. 309–313. doi: 10.1109/ACCT.2012.37.

[8] S. Hemalatha, A. Renuka, U. Dinesh Acharya, and P. R. Kamath, “A secure image steganography technique using Integer Wavelet Transform,” in *2012 World Congress on Information and Communication Technologies*, Trivandrum, India, Oct. 2012, pp. 755–758. doi: 10.1109/WICT.2012.6409175.

[9] Weiqi Luo, Fangjun Huang, and Jiwu Huang, “Edge Adaptive Image Steganography Based on LSB Matching Revisited,” *IEEE Trans.Inform.Forensic Secur.*, vol. 5, no. 2, pp. 201–214, Jun. 2010, doi: 10.1109/TIFS.2010.2041812.

[10] A. Almohammad, G. Ghinea, and R. M. Hierons, “JPEG Steganography: A Performance Evaluation of Quantization Tables,” in *2009 International Conference on Advanced Information Networking and Applications*, Bradford, United Kingdom, 2009, pp. 471–478. doi: 10.1109/AINA.2009.67.