Secure Data Hiding In Digital Image Based On Skew Tent Map and LSB Technique

[1]Nasreen Mansuri and [2]Arun Jhapate

Department of Computer Science & Engineering
Sagar Institute of Research & Technology, Bhopal (M.P.), India

Abstract
We have proposed a novel method for embedding of secret data securely using Skew Tent Map. In this method first of all we convert the data into binary form and then shuffle the message bits using skew tent map and then finally hide the last two bit of message with the last two LSB of cover image. For recovery of the original image and message data we use Inverse function of skew tent map for inverse of shuffling and extraction of message. A comprehensive set of experiments is carried out to justify proposed method's applicability and evaluate its performance against Peak signal noise ratio (PSNR) and Time etc. The results showed that the proposed algorithm has a good hidden invisibility, good security and gives better result than the existing techniques.

Keywords:
Component, formatting, style, styling, insert.

1. Introduction

Image processing is defined as the process of converting an image into digital image and performing certain operations on it. There are various operations that are performed, so that enhanced image can be obtained from the original image or we can extract some useful and meaningful information from the original image. The output of the image processing can be an image or characteristics that are associated with the input image. Usually image processing considers images like two dimensional signals, where we apply certain operations on them. With the modern digital technology it is possible to manipulate images (also known as multidimensional signals) with certain systems. These systems range from certain digital circuits to parallel computers [1].

Image stegnography for hide a secret image in the cover image. This approach aims at improving the visual quality of the stego image along with the security of the secret image. This approach still provides high embedded capacity. As it is popular that, Steganography is a technique that allows the one to hide the data within an image while adding some notable changes. In this approach we have explored various steganography methods like image steganography, audio steganography, video steganography and text steganography. All these stenography techniques are used to embed the information in digital carriers. The two most important aspects that should be considered for the image based steganography system are as follows: the quality of stego image and the capacity of the cover image [2].

2. Different Type of Steganography

Different types of cover objects [3] like text, image, audio or video files can be used to hide secret data.

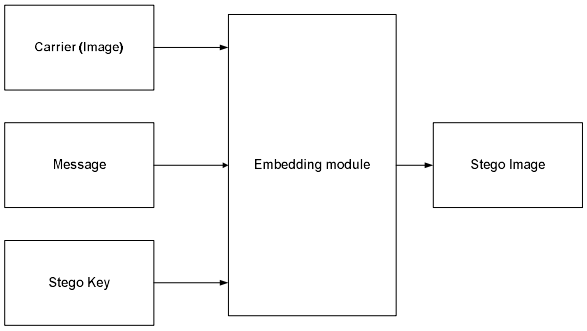


Figure 1. The Process of Data Hiding

(i) ***Text Steganography****:* It is one of the latest and most difficult types of steganography. It is a method of using written natural language to conceal a secret message. Text steganography is most challenging due to the presence of lesser redundancy in text documents as compared to the images and audio files [3].

(ii) ***Audio Steganography****:* Audio steganography embeds the message as noise into a cover audio file at a frequency out of human hearing range. Embedding secret messages in digital sound is generally more difficult than embedding

Manuscript received September 5, 2026
Manuscript revised September 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.9.10

messages in other media, compassion to additive random noise is also acute . Commonly used methods for audio Steganography are LSB coding, parity coding, phase coding, spread spectrum, and sound coming back hiding [3].

(iii) ***Image Steganography***: Images are used as the well-liked cover objects for steganography. A message is embed in a digital image through an embed algorithm, using the secret key. The resulting stego image is send to the receiver. On the other face, it is processed by the extraction algorithm using the similar key. During the transmission of stego image unauthenticated persons can only notice the transmission of an image but can't guess the existence of the hidden message [3].

3. Literature Review

In this section we will presents various papers related to steganography: "A Review of Methods and Approach for Secure Stenography" [5] has provided a complete review of all the methods and approaches that has been used in making the concept of stenography secure. In this approach, we had survey several different steganographic techniques for encrypting the data.

Steganography is a technique that allows the one to hide the data within an image while adding some notable changes. In this approach we have explored various steganography methods like image steganography, audio steganography, and text steganography. All these stenography techniques are used to embed the information in digital carriers. The two most important aspects that should be considered for the image based steganography system are as follows: the quality of stego image and the capacity of the cover image. "Art of Hiding: An Introduction to Steganography" [6] has provided the new approach that attempts to identify the requirements that are required for a good stenographic technique. This approach also determines which stenography technique is best suited for which particular applications.

Though there are many different carriers file formats can be used for transferring information from one place to another. But of all these different file formats, digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. For example some techniques have high payload capacity, while on the other hand some techniques do not have high degree of robustness.

"A high quality image hiding scheme based upon Noise Visibility Function and an optimal chaotic based encryption method" [8] has provided a new novel approach for image stenographic for hiding a secret image in the cover image. This approach aims at improving the visual quality of the stego image along with the security of the secret image. This approach still provides high embedded capacity.

The main drawback of this approach is that, though this approach provides high quality of stego image while keeping the high security as well. This approach has capability to adjust the payload of each image pixel. The problem with this approach is that, the overhead computational time taken in this approach is much higher as compared to the previous methods. Because of this higher computational time, the complexity of the way is increased.

"An Efficient Image Encryption and Hiding Method Applied by Double Random Phase Encoding" [9] has provided the new optical ways those posses many advantages like high processing speed, high parallel and high dimension etc. This image encryption and hiding method is being applied by the use of new technique. This technique is known as double random phase encoding technique. The main drawback of this approach is that though this approach provides high processing speed, high parallel and high dimension etc. But still this approach is not widely used because of the fact that this approach does not demonstrate great experiment results. Moreover, this approach is not as effective as earlier approaches.

"An Appearance Based Approach for Gait Identification Using Infrared Imaging" [11] has proposed a new novel approach for gait identification by the using of new imaging system. This imaging system is also known as infrared imaging. This proposed approach is tested over a self created database of thirteen different people with different resolution conditions. The use of infrared cameras at night makes this approach advantageous over many traditional approaches. Though this approach has many approaches, but still this particular approach has some drawbacks in the fact that this particular approach is being applied on smaller datasets and how this approach will work on large datasets still remains questionable.

"A Secret Sharing Scheme for Secure Transmission of Colour Images" [12] has provided a new approach that is based on secret image sharing and key safeguarding technique. This technique is based on effective and generalized schemes for the hiding of the colour image. This deformation and reformation algorithm reduces the drawbacks of key safe and secret sharing scheme and having its advantages. The proposed scheme is more secure and efficient one because secret image sharing and key safeguarding both are merged so, the security is higher than the single scheme provides either secret sharing or key safeguarding. In this scheme the shares are pre selected and have meaningful information advert to secret sharing scheme shares are distorted one.

4. Performance Parameters

The performance of the steganography technique is measured by some of the basic parameters which are listed below: [10].

Visual Degradation (VD):

Visual degradation identifies the perceptual distortion of the image data with respect to the plain image.

Compression Friendliness (CF):

Compression Friendliness measures no or very little impact on data compression efficiency on the image . Some stegnography schemes impact data compressibility or introduce additional data that is necessary for decryption.

Format Compliance (FC):

Format Compliance parameter is used to measures compliance the encrypted bit stream with the compressor. Standard decoder should be able to decode the encrypted bit stream without decryption.

Speed (S):

This parameter measures how fast the encryption and decryption algorithms enough to meet real time requirements.

Cryptographic Security (CS):

Cryptographic security is used to identify whether steganography scheme is secure against different plaintext-cipher text attack.

5. Proposed Methodology

In this paper, we have taken two images, one is the 24 bit true color image (RGB) as a cover image and 8 bit gray scale image as a secreat image.

A 8-bit gray scale image uses 8 bits per pixel and each byte represent the intensity of image.
A 24-bit color scheme uses 24 bits per pixel and each byte represents the intensity of the three primary colors red, green, and blue (RGB), respectively. So, a cover image can be split into three matrices as shown fig 2.

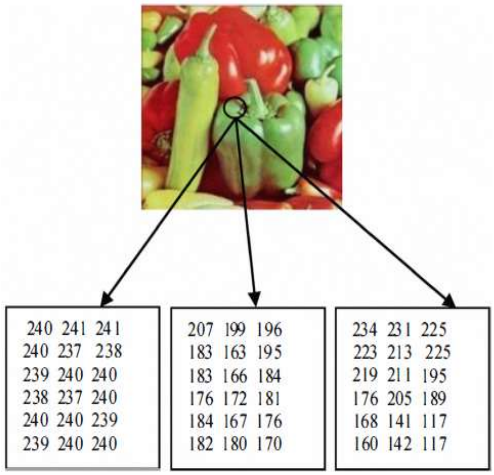


Fig. 2 RGB matrix representation of a cover image

6. Proposed Algorithm

1) Input 8 bit gray scale Message image P of size of M*N.

$$P = \{p_{ij} \mid 1 \le i \le m, 1 \le j \le n, p_{ij} \in \{0,1,...,255\}\}$$

2). Calculate the size of message image and Select the cover image at least 8 times of the size of message image. Let C is the original 8-bit gray-level cover-image of M*N pixels. It is denoted as:

$$C = \{c_{ij} \mid 1 \le i \le M, 1 \le j \le N, c_{ij} \in \{0,1,...,255\}\}$$

3). Pixilates both the image and convert to binary form.

4).Generate array T that defines the locations in cover image where the data is to be embedded by using Skew tent map. Procedure to generate array is given below.

The skew tent map is formulated as

$$F(x)=\begin{cases} x/p & x\in[0,p] \\ (1-x)/(1-p), & x\in(p,1] \end{cases}$$

5).Iterate Skew tent map to obtain a pseudo random sequence of size M*N, denoted by $X = \{x_0, x_1, ..., x_{MN-1}\}$

6).Sort X in ascending order to get $Y = \{y_0, y_1, ..., y_{MN-1}\}$

7).According to the relationship of X and Y, a scrambling vector $T = \{t_0, t_1, ..., t_{MN-1}\}$ is obtained such that $y = x_{t_i}$ i,i=0,1,2,…,MN-1.

8). Replace the LSB's of true color cover image red matrix pixels in the sequence generate in step 4 with secrat image bits.

Figure shows the block diagram of proposed method:

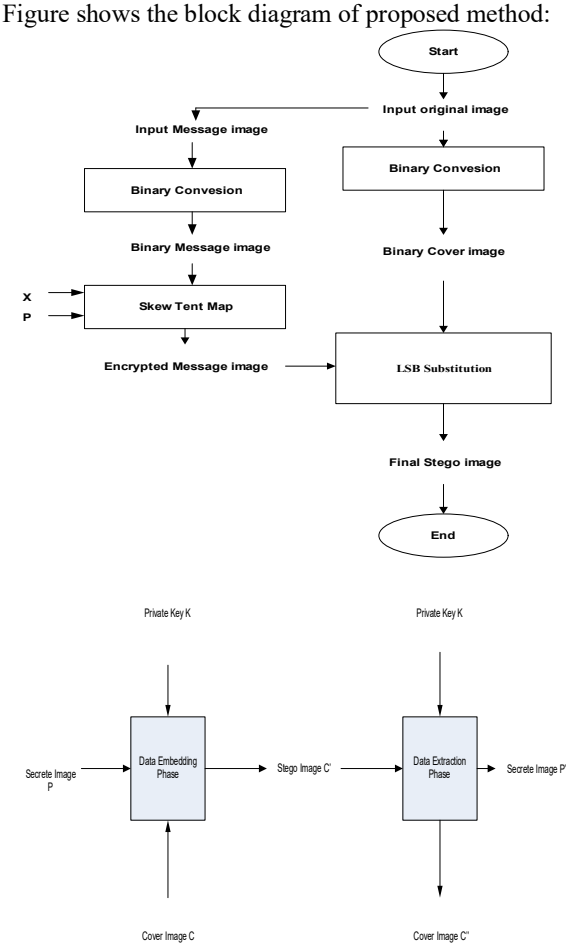


Figure 3: Block Diagram of Proposed Method

7. Evaluation Metrics

In this investigation, the set of criteria for comparing the selected algorithms are: the MSE, PSNR and Time.

A. Mean square error (MSE)

MSE is one of the most frequently used quality measurement technique followed by PSNR. The MSE [11] can be defined as the measure of average of the squares of the difference between the intensities of the Encrypted image and the original image. It is popularly used because of the mathematical tractability it offers. It is represented as:

$$MSE=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j)-C'(i,j))^2$$

Where C(i, j) is the original image and C' (i, j) is the encrypted image. A large value for MSE means that the image is of poor quality.

B. Peak signal to noise ratio (PSNR)

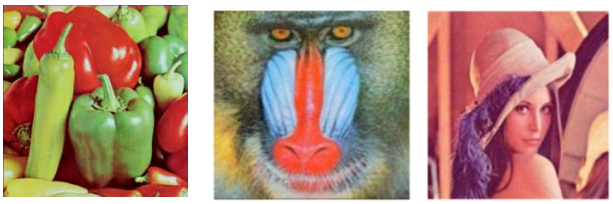
The PSNR depicts the measure of reconstruction of the encrypted image. This metric is used for discriminating between the cover and encrypted image. The easy computation is the advantage of this measure. It is formulated as:

$$PSNR=20\ \log\ 255^2/MSE$$

A low value of PSNR shows that the constructed image is of poor quality.

8. Experimental Results

Proposed technique, are implemented on Windows PC having Intel 2.4 GHz processor and 2GB RAM, and run using Matlab 9a. We have considered different color image files in this experiment to embed digital data. The secreat image are 8 bit gray scale images and the dimension of this image is 256×256 pixels shown in Fig 3. All the cover images are colored images and the dimension are these images 512*512 pixels shown in fig 4.in our method we only replace bits with red matrix of color cover



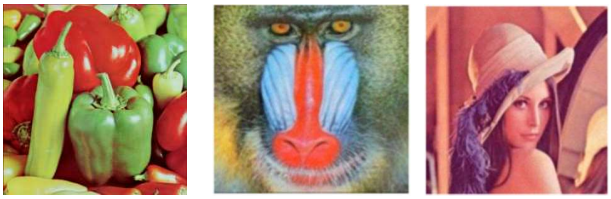
(a) Peppar (b) Baboon (c) Lena

Figure 4: Original color images

The hidden information used in our proposed method is shown below

Figure 5: Secreat message

The capacity of the proposed method is represented by 1/8 and ¼ of cover image and it remains the same. The payload is 0.125 bit/pixel in case of single bit LSB substitution and 0.25 two bits LSB Substitution .Proposed method has maximum capacity and it also varies depending on size of message image. The stego images resulted from our proposed method is shown in Fig. 6 there is small changes in stego images.



Pepper Baboon Lena

Figure 6: Resulted stego image

Fig.7 (a) is the histogram of original image Baboon. Figure 7(b) is the histogram of the stego image generated by the proposed method .fig 6 shows that there is small changes in histogram of the both image so we can say that quality of proposed method is good.

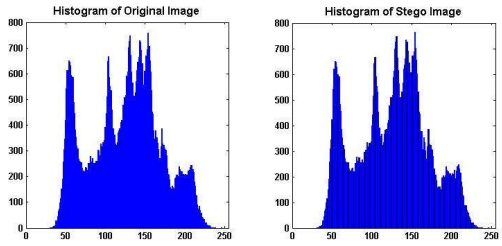


Figure 7 : Histograms of the Original Image and Stego Image

The Average quality parameters between the corresponding pixels values of the six encrypted images Lena, Baboon, Papper, Airplane, Butterfly, and Cat are tabulated in Table I.

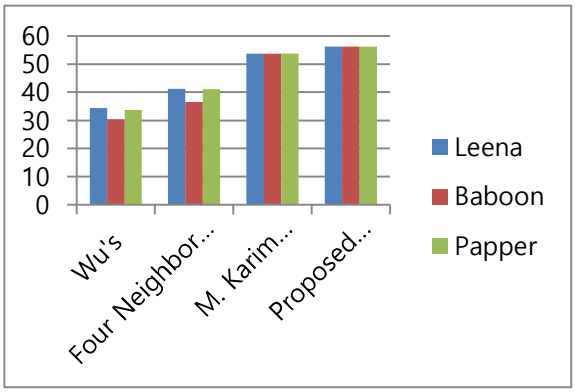
TABLE I RESULT OF QUALITY PARAMETERS ON DIFFERENT IMAGE

Images	PSNR (132.3591)	Time (0.1246)
Lena	56.1730	0.3234
Baboon	56.1862	0.3134
Pepper	56.1891	0.2969

Fig 6 and Fig 7 shows the comparison graph of proposed method on different images with respect to PSNR and Time respectively.

TABLE II COMPARISON RESULTS WITH NA-J WU'S METHOD AND FOUR NEIGHBOR METHODS

Images	Wu's method	Four Neighbor method	Masud Karim et.al method	Proposed Method
Lena	34.3962	41.1468	53. 7 61 8	56.1730
Baboon	30.413	36.5154	53. 7558	56.1862
Pepper	33.7496	41.031 5	53.7869	56.1891



. **Figure 1.** Shows Average PSNR comparison on different images .

9. Conclusion

In this paper we proposed a image steganography technique based on LSB and skew tent map .We have designed our image data hiding and extraction System using Matlab 7.8.0 to accomplish this research work. We have evaluated our proposed Data Hiding and Extraction System on gray Scale image of 256*256 . The experimental result proved that the PSNR obtained by our technique shows that the proposed technique gives better result than the existing techniques. We will future investigate in our proposed algorithm also can be applying to color image.

References

[1] K.Wawryn, R.Wirski, R.Suszynski, "2D image processing for auto-guiding system", IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 1 – 4, 2011.

[2] A.A.J Altaay, S.Sahib, M Zamani, "An Introduction to Image Steganography Techniques", International Conference

on Techniques Adavance Computer Science Applications and Technologies (ACSAT), pp. 122 – 126, 2012.

[3] Beenish Mehboob, Rashid Aziz Faruqui "A Stegnography Implementation" International Symposium on Biometrics and Security Technologie ISBAST, pp. 1 – 5, 2008.

[4] Vladimir Banoci, Gabriel Bugar, Dusan Levicky, "A novel method of image steganography in DWT domain", IEEE International conference on Radioelektronika, pp. 1– 4, 2011.

[5] Shaveta Mahajan, Arpinder Singh, "A Review of Methods and Approach for Secure Stegnography", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, No.10, pp. 67-70, 2012.

[6] Maninder Singh Rana, Bhupender Singh Sangwan, Jitendra Singh Jangir, "Art of Hiding: An Introduction to Steganography", International Journal Of Engineering And Computer Science, Vol. 1, No 1, pp. 11-22, 2012.

[7] F.I. Alam, M.M. Islam, "An Investigation into Image Hiding Steganography with Digital Signature Framework", IEEE International Conference on Informatics, Electronics & Vision (ICIEV), pp.1 – 6, 2013.

[8] S. Sajasi, A.M. Eftekhari - Moghadam, "A high quality image hiding scheme based upon Noise Visibility Function and an optimal chaotic based encryption method", IEEE Conference of AI & Robotics and 5th RoboCup Iran Open International Symposium (RIOS), pp. 1 – 7, 2013.

[9] Xu Hongsheng, Jun lie Xu ,"An Efficient Image Encryption and Hiding Method Applied by Double Random Phase Encoding", IEEE Fifth International Conference on Computational and Information science (ICCIS), pp. 302-305, 2013.

[10] Xu.Xikai Jing Dong , Wei Wang Tieniu Tan, "Video Stegaanalysis Based on the constraints of motion vectors", IEEE 20th International Conference on Image Processing (ICIP), pp. 4422 – 4426, 2013.

[11] A.Kanwar, P.Upadhyay, "An Appearance Based Approach for Gait Identification Using Infrared Imaging", IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), pp. 719-724, 2014.

[12] H.Kumar, A.Srivastava, "A Secret Sharing Scheme for Secure Transmission of Colour Images", IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), pp. 857 – 860,2014.