

Data Hiding using Cascading Feed Forward Network Prime Number Edge based Steganography

Dr. D. Ratna Kishore² and D. Suneetha²

¹Professor, CSE Dept, NRI Institute of Technology, Pothavarapadu, Andhra Pradesh, India
ratna.dasari@gmail.com

²Associate Professor, CSE Dept, NRI Institute of Technology, Pothavarapadu, A.P, India
sunithadavuluri8@gmail.com

Abstract—Steganography is one of the vital and popular techniques to protect the sensitive data from an unauthorized person or from third party. Now a day's providing security for data is one of the vital concepts. Due to this growing need for security of message, image steganography is become popular. The traditional steganography algorithms consists of Least Significant Bit embedding, but this technique known to everyone and easily detected by third party or hackers. In this Least Significant Bit embedding technique many of the algorithms are embed the secret data in sequential form. Instead of this if the data can be embedded in random pixels it leads to provide a better security. So in this a paper we present a novel approach to embed data in the prime number based edge pixels of the image by extending various least significant bit embedding algorithms. This prime numbers are also trained with Artificial Neural Networks in order to get actual pixels values for embedding secured data. This algorithm ensures better results against providing security for data when compared to other popular existing algorithms.

Index Terms— Steganography, Cascading Feed Forward Network, PSNR, MSE.

I. INTRODUCTION

The term Steganography comes from the Greek Words "STEGANOS, GRAPHIE". The Steganos means "covered" and Grpaphie means "writing". The main aim of steganography is to provide security for user data from unauthorized persons. In this technique the secret data is placed inside of the image which is not visible by the human eye directly. We have so many ways of steganogarpthy techniques, like image steganography, audio steganography and video steganography. Due to the need of security we choose either one the security technique in order to hide the data securely, among those in this we choose image steganography technique because in this data is not directly visible by the human eye typically.

The normal image steganography technique or algorithm uses Least Significant bit embedding. The main advantage of this algorithm is simple and it is easily to hide the secret data in LSB pixels of the image. But it can be easily detected by anyone who has the basic idea about the steganography technique because it is simple to extract an LSB pixels form an image. So it is less secure if we embed secret data in LSB pixels of an image. So instead of inserting an image in sequential pixels better to insert in the random pixels of an image it leads to performance improvement of the algorithm. But choosing random pixels of an image is also simple technique because every one generates random pixels with some basic predefined functions.

To overcome this problem in this paper we proposed a novel approach which will provide some better performance without changing the characteristics of an image. In this technique we choose the prime numbers based edge pixels of an image and input then to the artificial neural networks to train them and obtain the final pixel locations, then embed secure data in those obtained pixels.

The rest of the paper is organized as follows. The section 2 consists of some of the various existing algorithms. Section 3 consists of proposed approach i.e. data security algorithm based on prime number based edge pixels with the help of artificial neural networks. Section 4 consists of results and section 5 presents conclusion and future scope.

II. LITERATURE REVIEW

In real world data available in so many ways like text, images, audio and video etc. Every form the data is visible by the human eye directly. But hiding data in a image is not directly visible by human eye for this ultimate solution is the image steganography. There exists so many image steganography techniques are available to hide the data securely from unauthorized person or from third party.

In Sharma et. al's [1] has introduced a new algorithm to embed secret data in an image using cryptography and basic image steganography algorithm. In this two techniques are used one is image cryptography and second is image steganography. In this algorithm have two phases. In phase 1 the secret data is converted into cipher text with the help of DES algorithm and obtain the key. In phase 2 the obtained key from phase 1 is hidden in the Least Significant Bits of an image directly. Results are good with better PSNR and MSE values. In Yousef Bani et.al's[2] proposed a novel approach for hiding secret data from a third party. In this technique the data is hiding using genetic algorithm and blowfish algorithms. First, the secret message is converted into cipher text using blowfish algorithm and obtain the secure key from this phase. Next to hide the secret key from unauthorized person use genetic algorithm to identify the exact pixels from an image. And the algorithm is trained with basic general population as an input. Finally the secret is hidden in the selected pixels of an image. Results are good and compared with various existing algorithms and it provides less noise ratio and improvement in the quality of an image.

In Kiran .R et.al's[3] proposed an approach for embedding a secret data in an image. In this algorithm the secret data is inserted in to the multiple combinations of LSB and MSB pixels of an image. First the image is converted into binary form and the secret message is also converted into the binary form. If the combination of the pixels is 00 or 11 and 10 or 01 depend on the embed the secret data into image. This algorithm also provides a better results and improvement in the quality of an image.

In Sadeq et.al's[4] introduced a new technique for hiding secret data in an image using an algorithm back propagation neural networks. In this technique instead of taking one image, use two images one image as a cover image and the other one as a secret image. And the images are in 256 color images. The selected pixels is calculated using linear feedback shift register algorithms after obtain the selected pixels the data is hidden into the selected pixel location of an cover image and after that the cover image is also embed in the secret image. The results are analyzed with various existing algorithms and it provides better quality ratio.

In Singh et.al's [5] has introduced a new technique for hiding data using DCT coefficients. In this approach two things are used for secure data one is sequence generator and the other one is android transform. This algorithm is well suitable for JPEG images and it provides better PSNR and MSE values compared to various existing algorithms.

III. PROPOSED METHOD

In this proposed algorithm we consider prime number based edge pixels with the help of cascading feed forward network. First the original input color image is converted into black and white ie gray scale image. Then obtain the edge pixels of an image using canny edge detection algorithm. After getting edge image convert the image into binary and the values are given to the cascading feed forward network for training. After that select the prime number pixels from the output of cascading feed forward network. Secondly convert the original secret data into cipher text using AES encryption algorithm and obtain the secret key, then the secret key is converted into binary. Finally hide secret key into selected pixels of the original cover image.

At the decryption side take the stego image as a original image and apply the reverse process finally we decode the secret from the stego image. Then with the help of secret key decrypt the cipher text obtain the original data.

A. Embedding algorithm

Input: Original color image, Secret message

Output: Stego Image

Step1: Start.

Step2: Import the original image using imread() function

Step3: Convert the image into grayscale image using rgb2gray() function.

Step4: Calculate the edge pixels of an cover image using canny edge detection algorithm

Step5: Train the edge pixels using cascading feed forward networks

Step6: Select the prime number based pixels from the output of cascading network

Step 7: Read the original message and convert into cipher text using AEX encryption algorithm and obtain the key

Step 8: Embed the secret key into those selected pixels

Step 9: Finally obtain the Stego image

Step 9: stop

B. Receiver Side Decoding algorithm

Input: Stego object

Output: Secret Message

Step1: Start

Step2: Read the stego image using predefined matlab function

Step3: Convert the stego image into gray scale image

Step4: Identify the edge pixels of an image using canny edge based algorithm

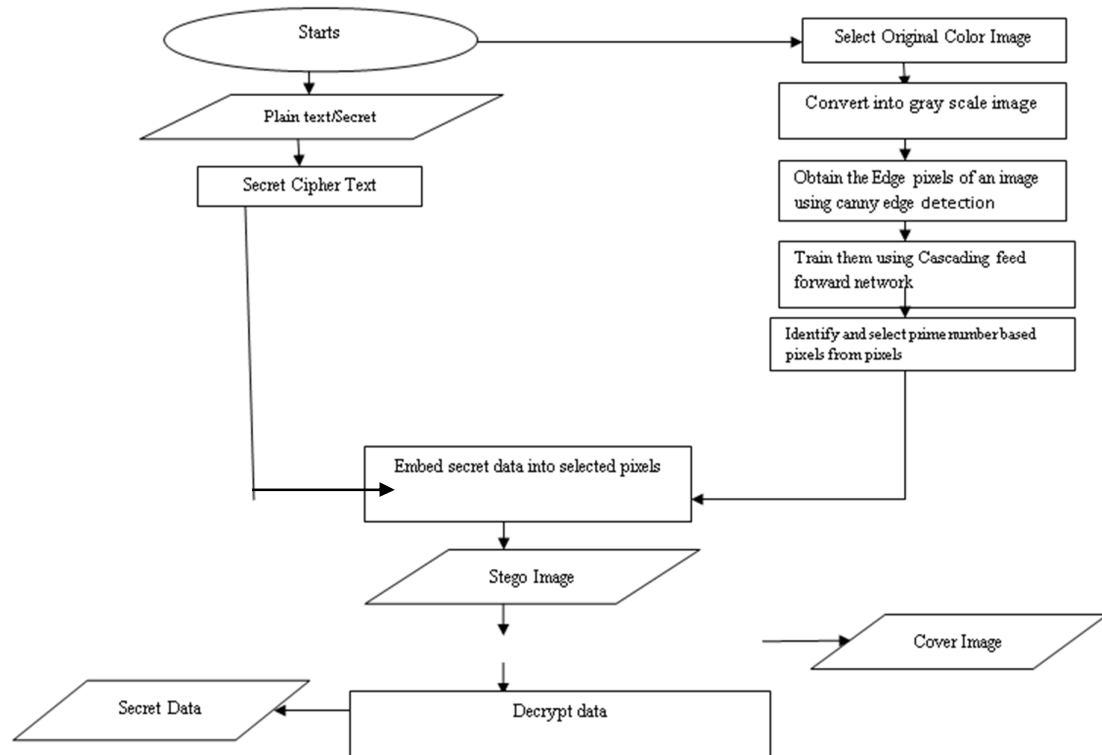
Step5: Select the prime number from the output of cascading feed forward network

Step5: Read the original key from the image

Step6: Decode the original data using original secret key and decrypt from cipher text to plain text

Step 7: stop

Flowchart for Proposed Approach:



IV. RESULTS AND ANALYSIS

The Proposed method is used to hide the secret data in the selected pixels of an image, which will meets all requirements without changing the original characteristics of an original image. The proposed approach has been tested and analyzed with various types of images and all the images are taken from the dataset <http://sipi.usc.edu/database/>. It provides comparatively good results with respect PSNR and MSE values as shown in Fig1 to Fig 4.

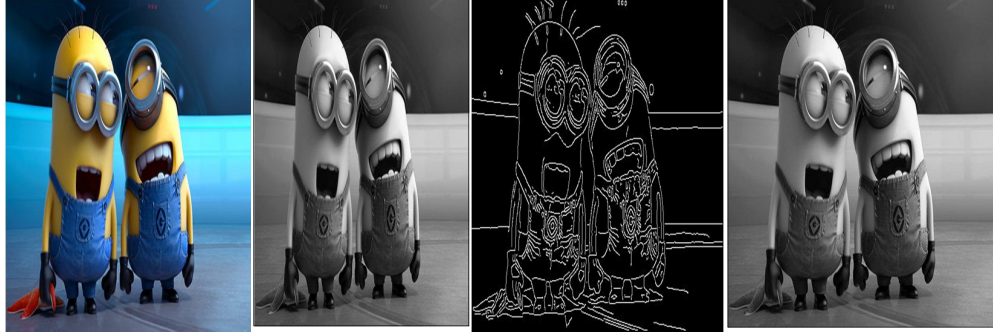


Fig 1: Original Cover Image

Fig2: Gray Scale Image

Fig 3: Edge Image

Fig4: Stego Image

A. Comparison Table and Chart

This section presents comparison of proposed approach with various existing algorithms. It shown the proposed algorithm calculated values are shown some significant difference with respect to PSNR and MSE Values. The PSNR (Peak Signal to Noise Ratio) means it shows the quality between the two images and MSE (Mean Square Error) means the error ration between two images. MATLAB tools are used for computing results. Table 1 shows comparison of MSE values and Table 2 Comparison of PSNR values of proposed and previous algorithms. Fig 5 and Fig 6 Shows Comparison charts for PSNR and MSE values.

TABLE I. COMPARISON OF MSE VALUES

Orginal Image	Previous Mean Square Error	Proposed Method Mean Square Error
Minion	0.0038	0.0036
One	0.0041	0.0032
Cammeeraman	0.0042	0.0034
Babo	0.014	0.0011

TABLE II. COMPARISON OF PSNR VALUES

Original Color Image	Existing Methods PSNR	Proposed Method PSNR
Minion	68.45	75.67
One	64.53	76.89
Cammerraman	78.67	83.99
Baboo	75.46	84.02

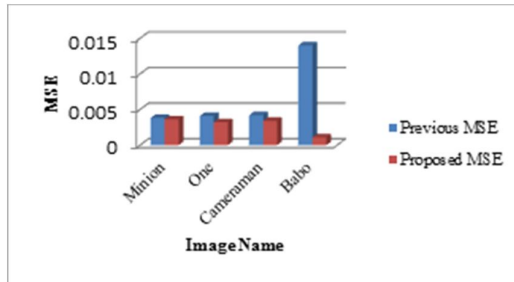


Fig 5: Comparison Chart for MSE Values

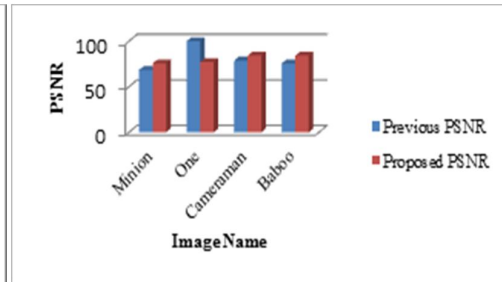


Fig 6: Comparison Chart for PSNR Values

Embedding Time: $ER=ES/SC$

Where ES indicates total number of embedded secret bit and SC represents size of the carrier image

TABLE III. PSNR VALUES OF VARIOUS IMAGES WITH VARIOUS EMBEDDING RATES

Embedding Rate	Original Image	Text Message Length(bits)	PSNR
10%	Baboo.bmp	34567	64.85
	Lena.png	34567	63.76
	Elanie.tiff	34567	66.56
	Mini.jpg	34567	64.09
Average PSNR=64.815			
30%	Baboo.bmp	83456	53.89
	Lena.png	83456	54.78
	Elanie.tiff	83456	51.57
	Mini.jpg	83456	58.96
Average PSNR=54.8			

V. CONCLUSION

In this approach the data is hidden into the prime number based edge pixels using cascading feed forward network. This algorithm produces better significant results with respect to PSNR and MSE values without changing the characteristics of an original image and also this approach has been analyzed with various types of images of various key length messages and it provides comparatively good results.

REFERENCES

- [1] Sharma. "A Two new methods for image Steganography using cryptography "Proceedings. Thrid International Conference on. Image Processing Vol. 3. IEEE, 2015.
- [2] Awwad, Yousef Bani,. "Genetic Algorithm using Blowfish algothrhim steganography." IJCSNS 17.3 (2017): 65
- [3] Kiran Kumar,." A Novel Algorithm for Enhancing the Data Storage Security in Cloud through Steganography", Advances in Computational Sciences and Technology (ACST) (ISSN: 0973-6107).
- [4] Singh "A Novel Approach For Data Security In Cloud Environment Using Image Segmentation And Image Steganography" IJCSI Issues, Vol. 9, Issue 3, No 1, PP 131-139, May 2017 .
- [5] Sadeq AlHamouz" Image Steganography System based on DiscreteWavelet Transformation and Resilient Back-Propagation" IJCSNS, VOL.15 No.1, January 2015