

SECURE ONLINE TRADING BY STANDRDIZATION OF THE LOGO

¹Dr. B. P. Santosh Kumar,² Dr. S. Shafiulla Basha,³Dr. Syed Jahangir Badshah ⁴T. Pavithra, ⁵K. Geethanjali,

¹Assistant Professor, M.Tech., Ph.D., MISTE, MIE. ² M.Tech., Ph.D., MISTE., MIETE., MIE. ³ Assistant Professor. ^{4,5}B. Tech Students.

Department of ECE,
YSR Engineering College of Yogi Vamana University, Proddatur, Kadapa, AP, India.

Abstract: Now a days most of the people giving Priority to online shopping. In online trading there is a possibility that the customers are get cheated by the e-commerce websites, that are run by the fake logos. Logos have high importance in today's marketing world. Online product frauds in the booming e-commerce market have become a major concern for the market surveillants and commercial companies, the logo detection plays a crucial role in preventing the increasing online counterfeit trading attempts. There are many techniques for the detection of fake logos. The Least significant bit (LSB) approach is an efficient method to provide security from online counterfeit attempts. The LSB based approach is a popular type of steganographic algorithms. Steganography plays a major role in data communication security. So, the main aim of this project is to secure online trading.

Index Terms - Information hiding; Logo security; information hiding; steganography.

I. INTRODUCTION

Steganography is the method of hiding image in another media. In place of image can we can insert audio and video files also. A digital image can be represented in spacial domain and frequency domain. The most well used method of special domain is least significant bit (LSB) method. The LSB method only concentrates on the write most least significant bits. By changing this bit our human eye could not detect the changes that have been made, our eyes are insensitive to the changes. So, this method makes us to insert one secret data or image with cannot be predicted by the hackers. The previous works specially made on changing the right most two bits which becomes easy for the hackers to detect the Stego image. So, our aim is mainly based on providing security by using multiple bits of a number.

II. PREVIOUS WORKS

In previous work, the right most bits of each pixel are replaced with the secret image bits. The technique here is they directly change the least significant bits. By changing the two LSB bits of the original image with secret bits in sequential order. There is a possibility that an unauthorized person can notice the order in which the secret bits placed and access that data. To embed the data first convert the original image to binary image. To the change unnoticeable, change the one or two least significant bits instead of more than two bits the attacker can guess the changes in the picture. We can change the last three or four bits and so on to original image bits if a message is too large.

III. LSB TECNIQUE ON MULTIPLES OF A NUMBER

This proposed approach does not pick up least significant bits. Here we place the secret bit in the multiples of the any number. This provides the additional level of security. It is applicable to grey level and color images also.



Fig 1: Embedding bits at 2-multiples and 3-Multiples

IV. ENCODING STEPS

1. Read the cover image (logo image) and converted into gray scale.
2. Read the color image (secret image) and converted into gray scale
3. Convert the logo image values into binary format.
4. Similarly Convert the secret image values into binary format.
5. Resize the logo image in accordance with secretimage.
6. Consider the four gray scale values for logo and one grey scale value of secret image.
7. Conversion from decimal to binary provide convenient for embedding.
8. Replace the logo least significant two bits by secret image bits. The replacement is done on any multiples of the number.
9. Repeat this process on entire logo image.
10. After embedding bits into original image, the resulting image is called Stego image.

V. DECODING STEPS

1. Read the Stego image.
2. Now, start from each multiple number of Stego image extract the secret bits.
3. These extracting bits are combined at the end and converted into the decimal.
4. If the decimal number matches with the secret image value then we conclude that the original image is real. Otherwise, fake.

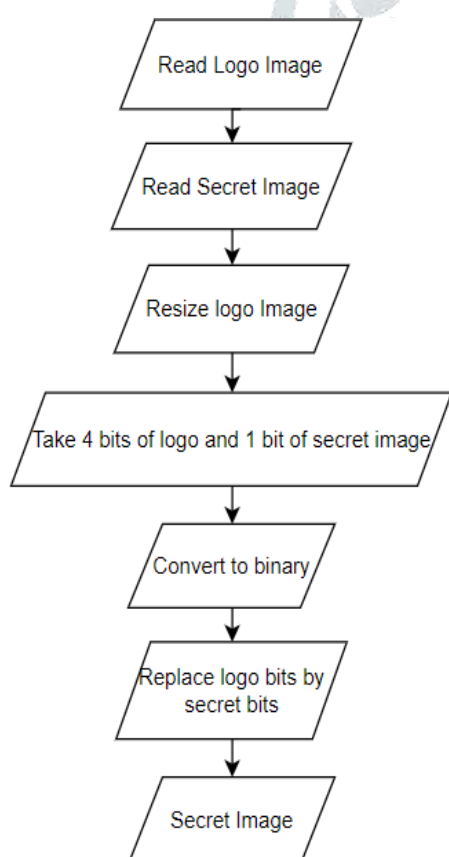


Fig 1: Encoding Flowchart

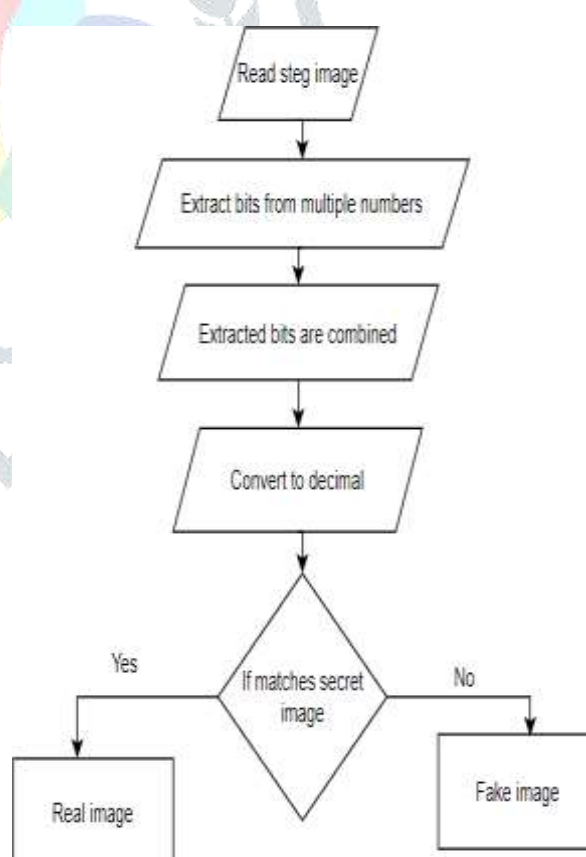


Fig 2: Decoding Flowchart

VI. FEATURES FOR INFORMATION HIDING TECHNIQUES

Any information hiding technique shall exhibit certain characteristics:

1. Capacity:

Capacity refers to the amount of information that can be hidden in the cover image. The amount of data that can be hidden is governed by the fact that information hidden should not completely alter the original image to avoid unintended user attention.

2. Security:

The information hiding method should provide security for data such that only the intended user can gain access to it. In other words, it refers to the inability of the unauthorized user to detect hidden information. This is very crucial to protect the confidentiality and sensitivity of the data being sent.

3. Robustness: It refers to the amount of information that can be hidden without showing any adverse effects and destroying confidential information.

4. Perceptibility: The data hiding method should hide data so that the original cover signal and the hidden data signal are perceptually indistinguishable.

Image quality metrics:

The image quality metrics are used to determine the quality of the Stego image and its similarity with the cover image. As a performance measure for image distortion due to hiding of message, the well-known peak-signal-to-noise ratio (PSNR), which is categorized under difference distortion metrics, can be applied to Stego images. It is defined as:

$$\text{PSNR} = 10 \log (\text{Cmax})^2 / \text{MSE}.$$

MSE = mean – square – error, which is

$$\text{given as: } \text{MSE} = 1/MN((S-C)^2).$$

$$\text{Cmax} = 255.$$

Where M and N are the dimensions of the image, S is the resultant Stego image, and C is the cover image. PSNR values below 30 dB indicate low quality (i.e., distortion caused by embedding is high). A high-quality Stego image should strive for a PSNR of 40 dB or higher. The greater the value of PSNR, the lower degree of distortion present for the Stego image. In comparison, the PSNR between two same and unchanged pictures is infinity (∞). To determine the PSNR in between two embodiments of the same size at first, we need to calculate MSE. MSE can be calculated by using the above formula. By using MSE, we can find PSNR. To expose the difference caused by message embedding inside the cover object, we have also shown the cover image's histogram and the Stego image. The results indicate that the proposed method has higher PSNR values in all test cases. It means that in all test cases, the proposed method gives lower MSE values since it decreases the number of altered pixels.

VII. SECURITY ANALYSIS

In this section, we will analyse the proposed method against three of famous statistical and visual attacks to ensure its immunity against these attacks, and have a more precise evaluation of our method in terms of security.

1. Histogram analysis

It is considered a statistical attack since an image's histogram shows a graph of the number of pixels at each different intensity value found in that image. This attack allows the human eye to distinguish between the cover and Stego images if there is a message embedded in channels. For colour, images of different intensities for each of the three channels (red, green, blue) are possible. Therefore, a histogram for each channel can be drawn separately, or an average histogram of all channels can be produced. The below two graphs shows the red-channel, green-channel, and blue-channel of Sequential-LSB and the proposed method. When we embedded sample pictures of different sizes from the graph, it can be noticed by the human eye that the red, green, and blue channels histograms of the Sequential-LSB method are different from the proposed LSB Technique that is LSB Technique on the multiples of a number. In contrast, the red, green, and blue channels histograms of the proposed method are almost identical to those of the original cover image due to data compression (which decreases the size of embedded data).

As per the histograms, the difference between two images is very little, thus, variance can't be spotted by naked eye. So, in plain view, humans cannot distinguish the difference between a Stego image and a cover image, after the proposed data hiding

approach is applied. This shows that the proposed algorithm works very well and this is an advancement of this algorithm as compared to others.

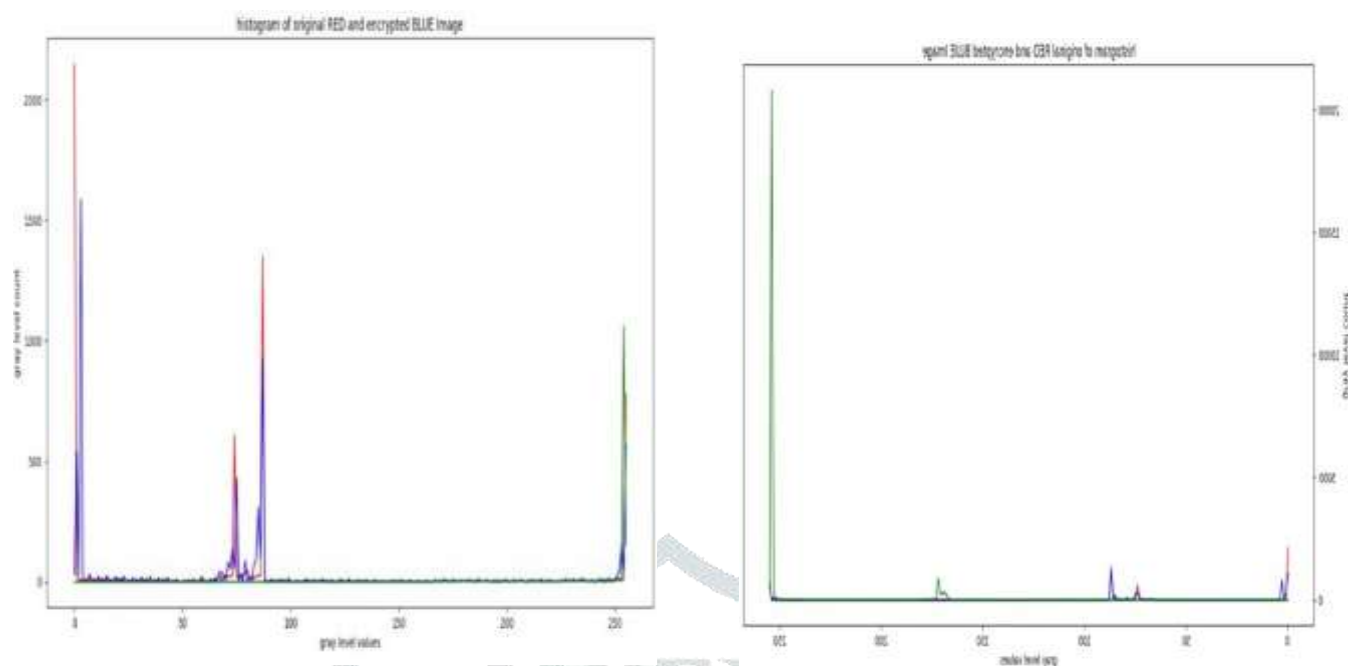


Fig 4: Histogram of Original logo(red) Steg Image(blue) and secret Image(green)

2. Analysis of LSB Enhanced Method:

The LSB method is based on the changes made in the least significant bits of the image, since the modifications are not precipitate by seeing an image i.e., the quality of image cannot be changed. The fundamental ideology of the enhanced LSB attack, which is visual examination of the Stego image, is to remove seven high level bits of each channel of the pel and focus on the last LSB. If we alter the MSB bits of the original image with the secret image bits, total image gets changed. By the human eye the changes can be easily detected. Hence, we place the secret bits in cover image (original image) of the two right most bits. Here we enhance the security by placing the secret image bits in multiples of a number in the cover image.

VII. EXPERIMENTAL RESULTS

The proposed technique has been implemented for cover image. With the help of this Stego image has been evaluated. PSNR Peak Signal to Noise Ratio is used to measure the quality between cover image and Stego image with in size.

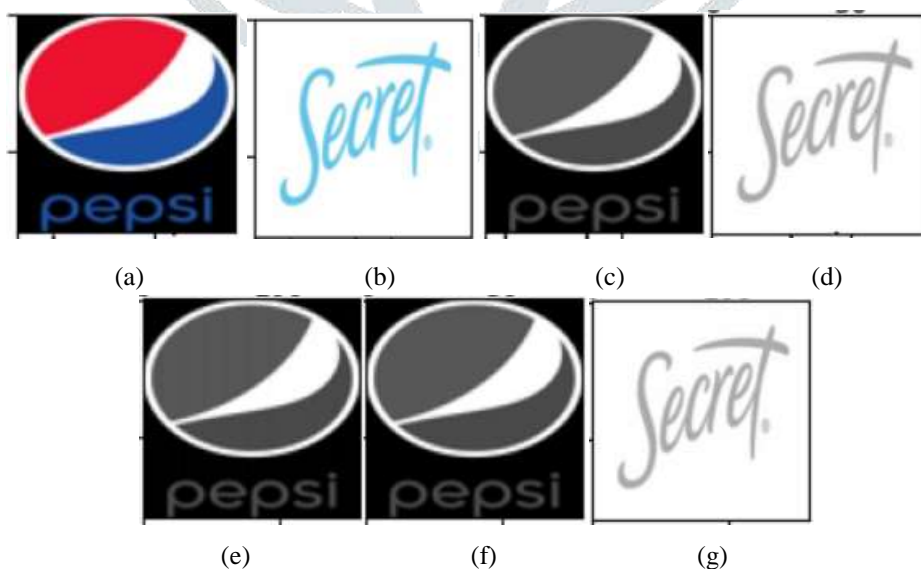


Fig 5. (a) Original Logo Image (b) Secret Image (c) Logo Grey Image (d) Secret Grey Image (e)Steg image (f)Extracted Logo Image (g) Extracted Secret Image





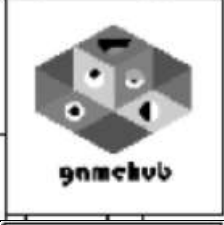

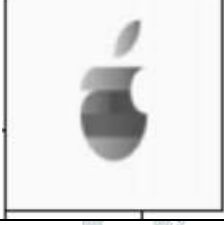
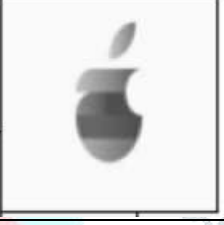
S.NO	Original Image (grey scale)	Stego Image	PSNR
1			45.76
2			46.38
3			48.37
4			48.95

Table 1. Comparison of different Images and their PSNR Values

IX. CONCLUSION:

In present world, the data transfers using internet is rapidly growing because it is so easier as well as faster to transfer the data to destination. So, many individuals and business people use to transfer business documents, important information using internet. Security is an important issue while transferring data using internet because any unauthorized individual can hack the data and make it unless or obtain information un-intended to him. LSB technique on the multiples of a number for hiding the secret image is proposed during this paper. Security analysis showed that the algorithm is secure enough to guarantee secure communication. Hiding a message with steganography method reduces the chance of a message being detected. Furthermore, the proposed algorithms extract the hidden data efficiently without using the original cover image. The efficiency of the proposed method is tested in terms of visual analysis, PSNR value and histogram of the both cover image and Stego image.

X. FUTURE SCOPE:

At some point using this least significant bit method, we can easily notice some distortions at higher numbers. So, to increase the peak signal to noise ratio we can update this algorithm to new technique that also been successfully steganalize along with peak signal to noise ratio (PSNR) value. So, for future scope it can be extended to be used with other algorithms like Discrete Hadamard Transform (DHT), Discrete Wavelet Transform (DWT), that it can be extended to the audio and video steganography.

XI. REFERANCES:

1. M. Juneja and P. S. Sandhu, "An analysis of LSB image steganography techniques in spatial domain," IJCSEE, vol. 1, no. 2, 2013
2. C. N. M. Pavani, S. Nag Anjaneyulu, "A survey on LSB based steganography methods," IJECS, vol. 2, no. 8, pp. 2464–2467, August 2013.
3. S. K. L. Gandharan Svvalin, "A novel approach to RGB channel-based image steganography technique," International Arab Journal of e-Technology, vol. 2, no. 4, June 2012.

4. M.-H. S. Jen-Chang Liu, "Generalizations of pixel value differencing steganography for data hiding in images," *Fundamental Informatic*, vol. 83, no. 3, pp. 319–335, 2008.
5. S. Gupta, G. Gujral and N. Aggarwal, "Enhanced least significant bit algorithm for image steganography", *Int. J. Comput. Eng. Manage.*, vol. 15, no. 4, pp. 40-42, 2012.
6. A. Singh and H. Singh, "An improved LSB based image steganography technique for RGB images", *Proc. IEEE Int. Conf. Electr. Comput. Common. Technol. (ICECCT)*, pp. 1-4, Mar. 2015.
7. A. Arya and S. Soni, "Performance evaluation of secrete image steganography techniques using least significant bit (LSB) method", *Int. J. Compute. Sci. Trends Technol.*, vol. 6, no. 2, pp. 160-165, 2018.
8. F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information hiding—A survey", *Proc. IEEE*, vol. 87, no. 7, pp. 1062-1078, Jul. 1999.
9. Y. Yigit and M. Karabatak, "A stenography application for hiding student information into an image", *Proc. 7th Int. Symp. Digit. Forensics Secure. (ISDFS)*, pp. 1-4, Jun. 2019.
10. R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques", *Proceedings of International Conference on Image Processing*, vol. 3, pp. 1019-1022, 2001.
11. W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for data hiding", *IBM Systems Journal*, vol. 35, no. 3. 4, pp. 313-336, 1996.
12. B. Li, J. He, J. Huang and Y. Q. Shi, "A survey on image steganography and Steganalysis", *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 2, pp. 142-172, 2011.

