An Efficient Approach for Hiding Image in Cover Image using Histogram Shifting Method

Irfanul Haque[1], Vipra Bohara[2], Laxmi Narayan Balai[3]
[1]*P. G. Scholar (Electronics & Comm.), Yagyavalkya Institute of Technology, Jaipur, Rajasthan, India*
[2]*Assistant Professor (Electronics & Comm.), Yagyavalkya Institute of Technology, Jaipur, Rajasthan, India*
[3]*H.O.D. (Electronics & Comm.), Yagyavalkya Institute of Technology, Jaipur, Rajasthan, India*

***Abstract*- In this paper we have proposed an efficient algorithm for hiding secret image also called payload in different types of cover image using histogram shifting method of reversible data hiding technique. Image utilized is jpeg, bmp and tiff images. We have analyzed this algorithm in MATLAB simulation tool. This analysis is performed to increase embedding capacity. We have calculated peak signal to noise ratio, mean square error and normalized signal to noise ratio.**

***Index Terms*- Steganography, Histogram, Fragile, Spatial, Reversible Data Hiding**

I. INTRODUCTION

The thought and practice of hiding secret data has a long history. Cryptography came into knowledge for securing the secrecy of communication and various methods were developed to encrypt and decrypt information with a specific goal to keep the information secret. Using Cryptography just encrypts the data so that it could be converted into a form not understandable by ordinary observation or it is relatively difficult to know the encrypted data without the key. Sadly it is sometimes not sufficient to keep the ingredients of a message secret, it may also be important to keep the presence of the message secret. The method used to execute this function, is known as Information Hiding or Steganography. Various methods of steganography are implemented and assessed in spatial, transform and compressed domain utilizing image and also Audio as the medium to hide confidential data. The strengths and weakness of the selected methods have been analyzed.

Steganography or Stego as it is often referred to in the IT community, literally means, "Covered writing" which is derived from the Greek language. Steganography is defined by Markus Kahn as follows, "Steganography is the art and science of communicating in a way which hides the existence of the communication. The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present".

In a digital world, Steganography and Cryptography are both intended to protect information from unwanted parties. Both Steganography and Cryptography are excellent means by which to accomplish this but neither technology alone is perfect and both can be broken. It is for this reason that most experts would suggest using both to add multiple layers of security. Steganography can be used in a large amount of data formats in the digital world of today. The most popular data formats used are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav, mainly because of their popularity on the Internet and the ease of use of the steganographic tools that use these data formats. These formats are also popular because of the relative ease by which redundant or noisy data can be removed from them and replaced with a hidden message.

II. DIGITAL IMAGING

In digital imaging, a picture element or pixel is the smallest item of information in an image that is represented by a series of Y rows and X columns. Pixels are normally showed in a 2−dimensional grid and are often represented using squares or rectangles for gray images. Each pixel is a sample of an original image, where more samples typically provide more accurate and better representations of the original. The intensity of each pixel is variable; for example in color systems, each pixel has typically three components and 3−dimensions, e.g., RGB (red, green and blue). The number of bits in order to represent each pixel determines how many colors can be displayed. For example, in an RGB color mode, the color monitor uses 24 bits each pixel (8 bits for each channel), allowing displaying 2^{24} (16,777,216) different colors. The number of colors can be achieved when bit depth is increased. This situation is important and useful for data hiding. Data hiding is the art and science of writing hidden messages in such a way that third parties apart from the sender and intended recipient can even realize that there is a hidden message. The result images are called as covered or stego image. Reversible data hiding is a technique, where not only the secret data can be extracted from the covered image, but also the cover image can be completely rebuilt after the extraction of secret data. Therefore, reversible data hiding is the choice in cases of secret data hiding, where the recovery of the cover image is a must.

Histogram modification is the most broadly used method for image embedding. This technique became very well known due to its easy execution. Basic thought behind this method is to perform the histogram shifting of the cover image either right or left depending upon the circumstances of overflow and underflow. Allocate the free space with information to be hidden by introducing the unity accretion or depreciation in the gray level, comparing to the histogram peak gray levels. Distortion generated by this technique will be very small and cannot be identified with eyes and tough to track with steganalyis devices.

III. HISTOGRAM SHIFTING

The basic histogram shifting scheme for reversible data hiding was first introduced by Zhicheng in 2006. In this proposed scheme, the image histogram is generated at first by considering all the pixel values of an image. To insert secret data, some pixel values are changed. At the receiver, for extracting the concealed data, the changed pixels are returned back to their actual condition. Thus the reversible data hiding scheme is obtained. During data embedding, at first from the image histogram the pair of zero and peak points are searched. The zero point refers to the pixel with least repeated value and the peak point refers to the pixel with most repeated value in the image histogram. Here, data is carried only by the peak pixel values. The peak pixel value is modified by 1 closer to the zero point for the corresponding secret data O. Where the data is 1 the peak pixel values remain unchanged. The pixels in between the pair of peak and zero points are also modified by 1 to a value closer to zero point but they do not carry any secret data. After processing all the pixels sequentially, the stego-image is produced. At last, the processed-image and the pair of peak and zero points are ready to transmit. At the receiver, the concealed data is regained and the actual image is regenerated. Lena image and its histogram are shown in Fig. 1 & Fig. 2 respectively.

Fig-1: Lena image

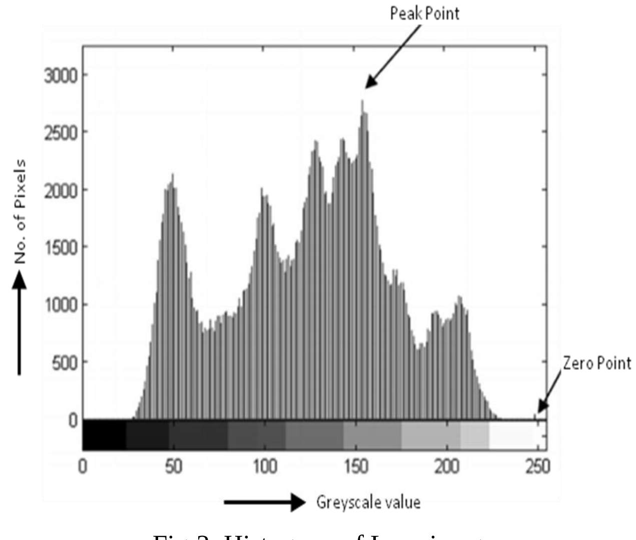

Fig-2: Histogram of Lena image

IV. PROPOSED WORK

In our work we have proposed an algorithm for hiding image in cover image using histogram shifting method of reversible data hiding procedure. All the simulations are carried out in MATLAB simulation tool. Proposed technique is used to enhance embedding capacity, mean square error and signal to noise ratio. Fig. 3 shows the method to hide image in cover image and to obtain the stego image.

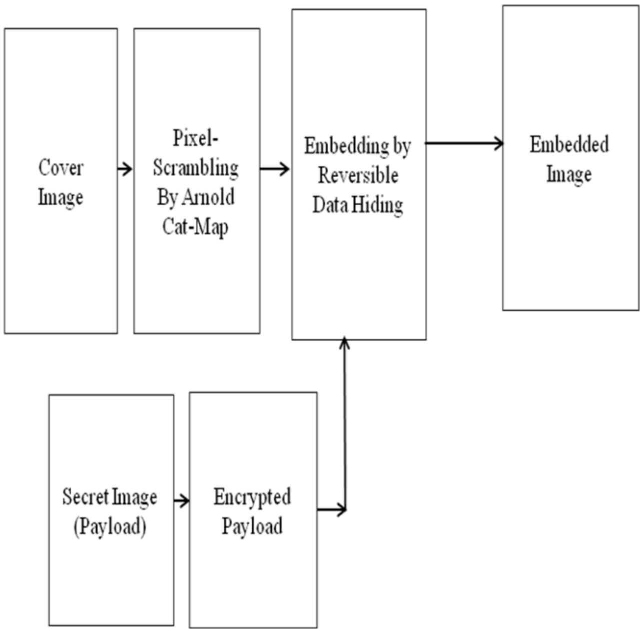
Cover Image
Pixel-Scrambling By Arnold Cat-Map
Embedding by Reversible Data Hiding
Embedded Image
Secret Image (Payload)
Encrypted Payload

Fig-3: Proposed method to generate stego image

In this technique initially, the cover image in which secret image (payload) is hidden is selected. Then encrypted domain of a secret image is obtained with the help of Arnold cat map by using number of iteration and this parameter is treated as one part of secret key which is required at the time of retrieve the same original secret image at receiver side. After this, partial encrypted secret image is obtained. Now the histogram of cover image is calculated and find out the maximum repeated pixels in that image so that the total maximum repeated pixels are found out with their pixel locations.

The maximum repeated pixels provide the information of embedding capacity of data which is converted and obtained by the secret image. Then enter the secret image which is to embed, converted it into its pixel values and then converted into binary stream with the help of ASCII code.

Now, embedding of secret image in encrypted domain of image is done by proposed histogram method of reversible data hiding technique by selecting only maximum repeated pixel values, converted these pixels into their binary equivalent value and embed the ASCII converted binary stream of secret image as per proposed technique of histogram shift method of reversible data hiding. Then the pixels which are most responsible are converted back into their decimal equivalent and restore into their original position in encrypted domain and finally encrypted image is obtained.

At the receiver side an algorithm is used to extract the payload and to reconstruct the cover image without any loss of features of cover image. Fig. 4 shows the proposed technique at the receiver side.

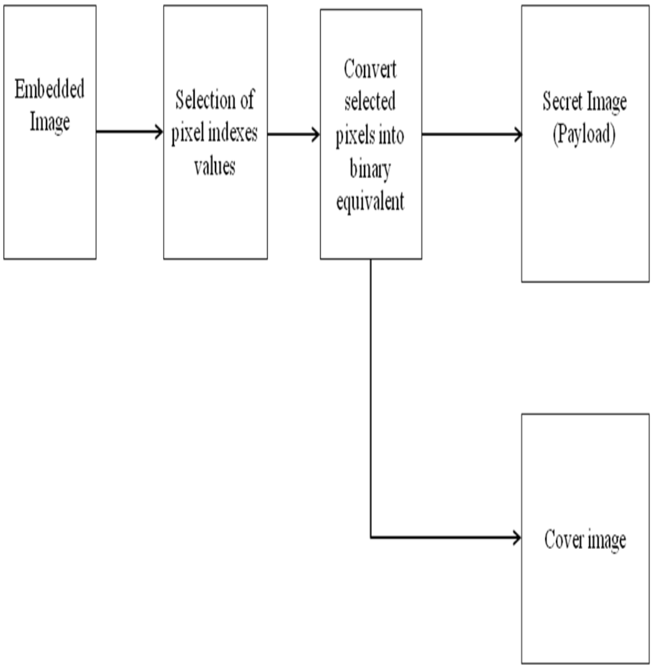
Embedded Image
Selection of pixel indexes values
Convert selected pixels into binary equivalent
Secret Image (Payload)
Cover image

Fig. 4 Proposed method at the receiver side

In this technique initially the transmitted embedded image is received at the receiver side and then the person whom the image and secret image are being sent. He must be known about the embedded key as well as encryption key in order to decode the secret image and cover image. On basis of embedded keys, the maximum repeated pixels are selected as per their pixels locations as these pixels are most responsible to decode the secret image which is hidden at transmitter side. Converted into binary equivalent values and then extract the binary values which are re-back converted into the secret image with help of ASCII table. After extracting the secret image from the selected pixels value, these pixels are again converted into decimal form and placed into their original positions.

After restoring all pixels which are responsible to embed the image, the partial encrypted secret image is obtained which is now required to recover the secret image from this. This is done only if the encrypted keys are correctly used at the receiver side. Then the original cover image is retrieved.

V. EXPERIMENTAL RESULTS

In the proposed technique we have considered cover image of size 256 x 256 named as ‘rice.png’ and secret image (payload) of size 32 x 32 named as ‘cameraman.tiff’. Histogram of cover image is calculated by MATLAB tool. Fig. 5 represents cover image and Fig. 6 represents histogram of that image. Fig. 7 & 8 represents payload image & encrypted payload image respectively. Fig. 9 represents stego image and Fig. 10 represents decoded payload image.

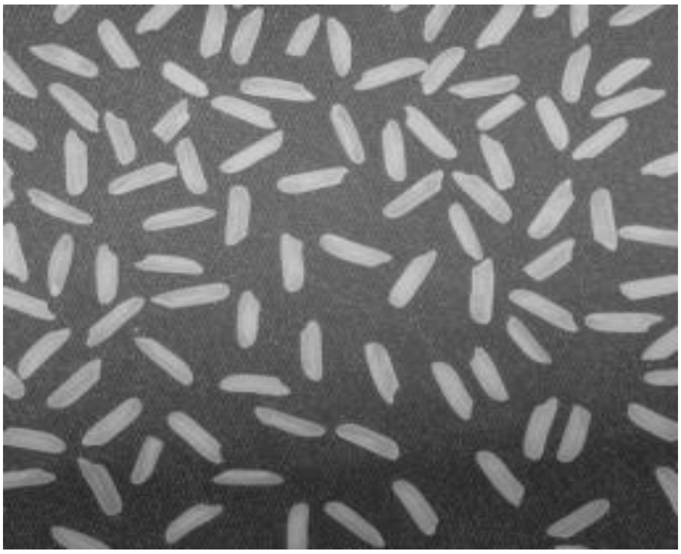

Fig5: Cover image

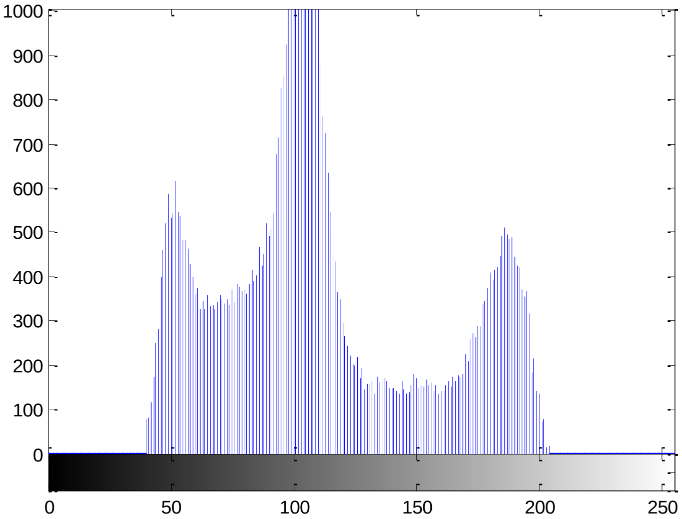

Fig-6: Histogram of cover image

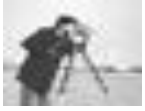

Fig-7: Payload image

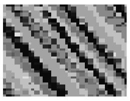

Fig-8: Encrypted payload image

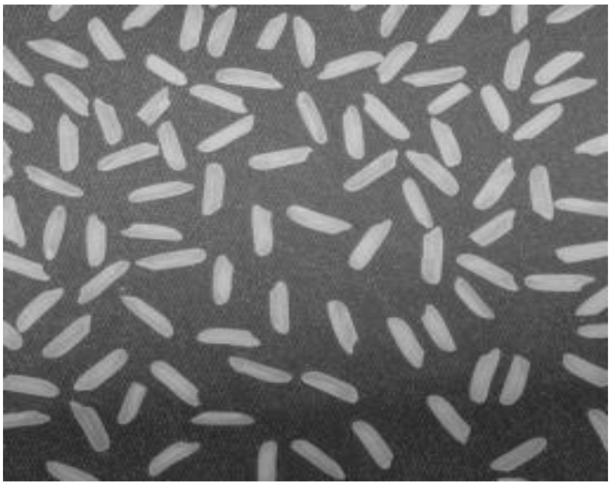

Fig. 9 Stego image

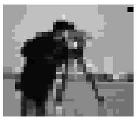

Fig. 10 Decoded payload image

This is the process of hiding secret image in cover image at transmitter side and extracting secret image from cover image at receiver side. In this case we have taken all the parameters correct. We have calculated some parameters also which are shown in table below.

Table 1: Resultant parameters

Parameter	Value
Mean Square Error	96.0492
Normalized Signal to Noise Ratio	0.9075
Peak Signal to Noise Ratio (dB)	56.6117

VI. CONCLUSIONS

In conclusion, it has been observed that from histogram calculation of cover image we have found out the maximum repeated pixels values and minimum repeated pixel values. We have avoided the minimum repeated pixels value and considered only maximum repeated pixel values and embedded the secret image. More number of maximum repeated pixels in cover image provides the more degree of freedom to embed the secret image.

In future we will implement this technique on different types of cover image and different types of secret image (payload) to examine the different features such as embedding capacity, signal to noise ratio etc.

REFERENCES

[1] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, “Reversible data hiding”, IEEE, 2002.

[2] C. C. Chang, J. Y. Hsiao, and C. S. Chan, “Finding optimal LSB substitution in image hiding by dynamic programming strategy”, Pattern Recognition, 2003.

[3] C. I. Podilchuk and E. J Delp, “Digital watermarking: Algorithms and applications,” IEEE, 2001.

[4] S. Katzenbeissar and F. Petitcolas, “Information hiding techniques for steganography and digital watermarking,” Artech House, 1999.

[5] Wayner, P., “Disappearing cryptography”, Morgan Kaufmann Publications, 2002.

[6] S. Jajodia, N. F. Johnson, and Z. Duric, “Information hiding: Steganography and Watermarking-attacks and Countermeasures,” Springer, 2001.

[7] Petitcolas, F., Anderson, R., Kuhn, M., “Information Hiding A Survey”, IEEE, 1999.

[8] Wei-Liang Tai, Chia-Ming Yeh, and Chin-Chen Chang, “Reversible data hiding based on histogram modification of pixel differences”, IEEE, 2009.