International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 4

An Efficient Algorithm for Hiding Text in Encrypted Domain of Image using Histogram Shifting Method

Dipali Bansal[1], **Sandeep Kumar Toshniwal**[2]
[1]P. G. Scholar, [2]Associate Professor
Department of Electronics & Comm.,
Kautilya Institute of Technology & Engineering, Jaipur, India

ABSTRACT

In this paper we have proposed an efficient algorithm for hiding text in various images using histogram shifting method. In this algorithm we have found locations of maximum and minimum repeated pixels. Then location of maximum repeated pixels is considered and location of minimum repeated pixels is avoided. We have analyzed this algorithm in MATLAB simulation tool. We have computed peak signal to noise ratio, mean square error, maximum embedded bits and maximum capacity.

Keywords: *Steganography, Maximum capacity, Histogram, Reversible Data Hiding*

1. INTRODUCTION

In the present era, transmission of text message from sender to intended recipient over the wireless communication network is utmost important. Therefore, it is very important to concentrate our mind to security of text message against the malicious users while transmission. In continuation to this, there are various methods to safe reception of text message at the receiver side among that one is during transmission of message, original form of message is totally converted into the unreadable form of message which comes in the category of encryption application. Other methods come in steganography application in which message which is to be sent to intended recipient is concealed inside the cover image and any big data so that it is very difficult to identify about the presence of the conceal message. In these applications main drawback is that during extraction of the original message or image from the image steganography some distortion occurs.

One of most popular technique which is used in defence areas, military areas and where security is main concerned is reversible data hiding (RDH) system. Important feature to use of RDH technique is data which is hidden in the cover image and transmitted and at receiver end both original data and cover image are decoded without distortion. This technique is preferred those area such a military and medical where little bit distortion is not acceptable. The RDH techniques categorized in many ways like LSB Modification, Histogram Shifting, interpolation technique, prediction error expansion, data embedding using difference expansion and others. These techniques have some merits and some demerits.

Cryptography techniques have been generally used to encrypt the plaintext information, exchange the cipher text over the Internet and unscramble the cipher text to separate the plain text at the receiver side. Be that as it may, with the cipher text not by any means making much sense when translated as it is, a programmer or an intruder can without much of a stretch see that the data being sent on the channel has been encrypted and is not the plaintext. This can normally raise the interest level of a malignant programmer or intruder to conduct cryptanalysis assaults on the cipher text (i.e., break down the cipher text opposite the encryption algorithms and decode the cipher text totally or incompletely). It would be fairly more reasonable if we can send the secret data,

either in plaintext or cipher text, by cleverly inserting it as feature of a cover media (for example, a picture, sound or video carrier file) such that the hidden data cannot be easily seen to exist for the unintended beneficiaries of the cover media.

Table 1 Difference between different data hiding methods

Parameter	Steganography	Watermarking	Encryption
Carrier	Any digital media	Image/Audio	Text
Secret Data	Payload	Watermark	Text
Key	Optional	Optional	Required
Input File	Two	Two	One
Detection	Blind	Informative	Blind
Visibility	Never	Sometimes	Always
Falls when	Detected	Removed	De – ciphered

2. STEGANOGRAPHY

Steganography is science to hide the message in cover medium in such a way that apart from the sender and intended recipient malicious users do not suspect the presence of message. The word steganography is of Greek origin which means "hide secret message". The meaning of Steganography is “conceal one piece of secret message into another medium”.

Now-a-day the media which are used in steganography to hide the message are video file, audios file and image files. However there is no significance difference between steganography and cryptography.

In cryptography, the secret message is scrambled inside the cover media so that the message becomes in unreadable form and at receiver end the normal users only can observe and identify the scrambled message but he cannot decode the correct secret message without knowing the correct secret keys used at the transmitter side.

On the other hand, in steganography, the message is hidden inside the cover medium with some secret keys called stego key so that it cannot be seen. In simplest way it can be understood with following formul

cover_medium + hidden_message + stego_key = stego_medium

At the receiver side, the hidden message is extracted from the stego medium with same stego keys used at the transmitter side. The keys other than correct secret keys provide the incorrect result at the receiver end.

3. HISTOGRAM SHIFTING

The histogram modification technique involves generating histogram and finding the peak point and the zero point and shifting histogram bins to embed message bits. For a given host image, we first generate its histogram and find a peak point and a zero point. A peak point corresponds to the grayscale value which the maximum number of pixels in the given image assumes. On the contrary, a zero point corresponds to the grayscale value which no pixel in the given image assumes. Fig 2 shows a histogram of an image.

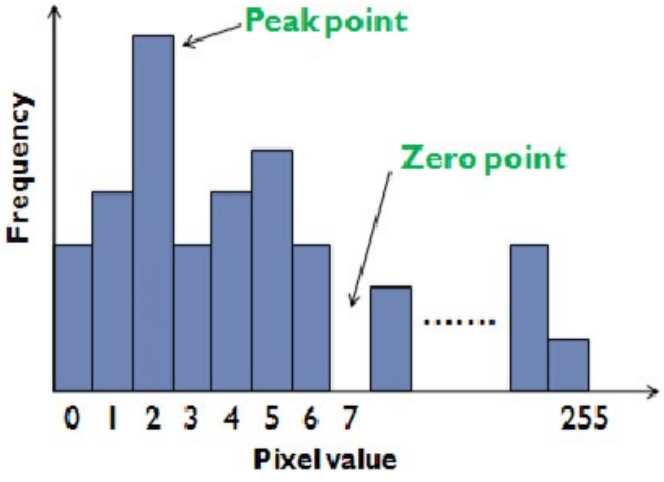

Fig-1: Histogram of image

In the above image peak point is at 2 and the zero point is at 7. Let P be the value of peak point and Z be the value of zero point. The range of the histogram, [P+1, Z-1], is shifted to the right-hand side by 1 to leave the zero point at P+1 as shown in Fig 3.

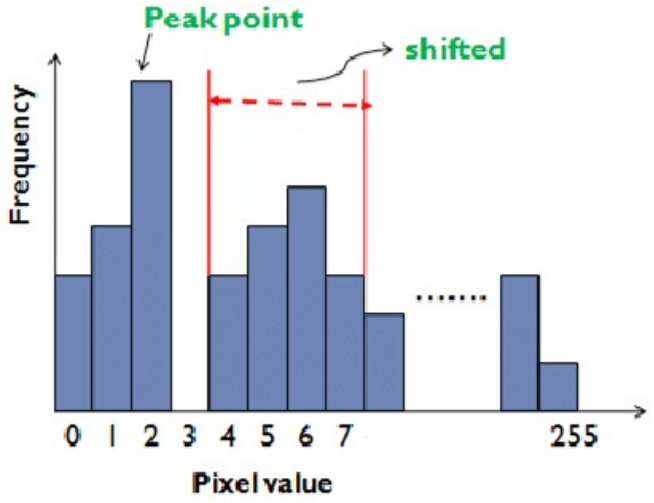

Fig-2: Shifting a range of histogram

Once a pixel with value P is encountered, if the message bit is "1," increase the pixel value by 1. Otherwise, no modification is needed. We note that the number of message bits that can be embedded into an image equals to the number of pixels which are associated with the peak point.

4. PROPOSED ALGORITHM

The steps involved during embedding of secret text message inside cover image with the help of proposed histogram shift method of reversible data hiding are shown in Fig. 3 and mentioned below the figure.

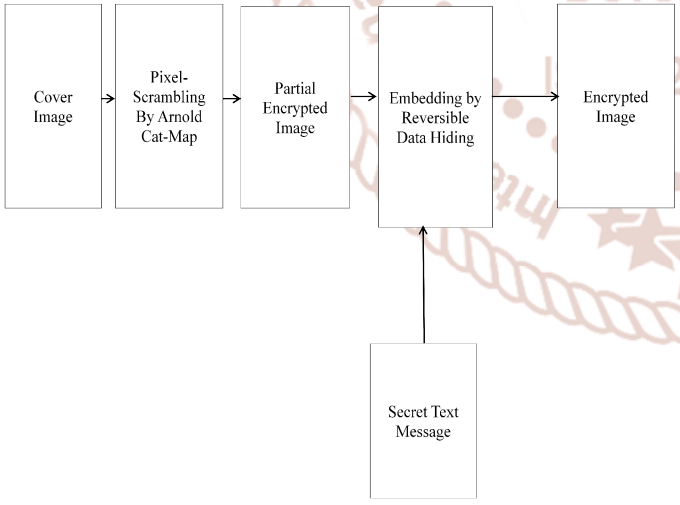

Fig-3: Proposed algorithm for embedding process

1. First, the cover image in which secret text message is hidden is selected.
2. The encrypted domain of an 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 image at receiver side. After this partial encrypted image is obtained.
3. After previous steps, the histogram of partial encrypted 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 text message.
4. According to the maximum embedding capacity of text message, enter the secret text message which is to embed. And converted into binary stream with the help of ASCII code.
5. Now, embedding of secret text message 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 text message as per proposed technique of histogram shift method of reversible data hiding.
6. After embedding the secret text message in encrypted domain of an image, 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.
7. These pixels indexing values are responsible to decode the secret message at the receiver side and these pixels indexing values are considered as secret keys of this system. Therefore, total secret keys which are involved in the system are embedding keys and secret keys.

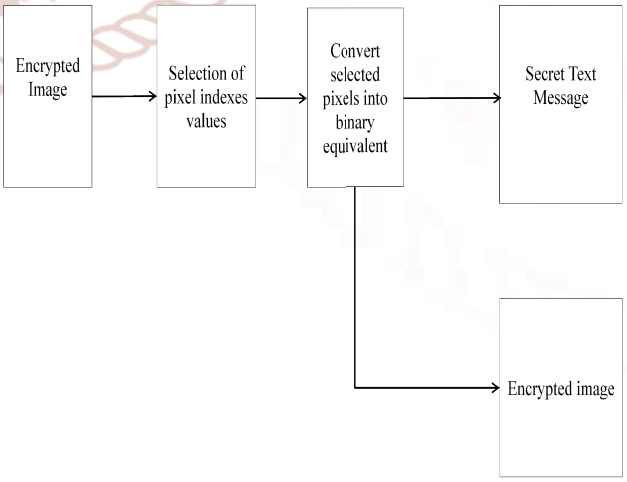

Fig 4 Proposed algorithm for extraction process

At the receiver side, the procedure which is utilized to decode the secret text message and cover image is just reverse the steps which are taken at the receiver side and shown in Fig. 4 and illustrated with the following given points:

1) First the transmitted encrypted image is received at the receiver side and then the person whom the image and secret text message are being sent he must be known about the embedded key as well as encryption key in order to decode the text message and cover image.
2) 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 message 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 text message with help of ASCII table. After extracting the secret text message from the selected pixels value, these pixels are again converted into decimal form and placed into their original positions.
3) After restoring all pixels which are responsible to embed the secret text message, the partial encrypted image is obtained which is now required to recover the original message from this. This is done only if the encrypted keys are correctly used at the receiver side. Then the original cover image is retrieved.

5. EXPERIMENTAL RESULTS

In this section, the results are presented which are obtained through experiments done on MATLAB platform. The grey scale image 'rice.png' of size having 256 x 256 is selected as cover image shown in Fig. 5 and secret text message is "Rajasthan Technical University, Kota" is selected to embed inside the cover image. Histogram of the cover image is calculated by MATLAB platform as shown in Fig.6. Partial encrypted image is obtained from the cover image by Arnold cat map with its iteration parameter (iteration = 50). Its parameter is considered as encrypted secret key which is used to recover the cover image from partial encrypted image at the receiver side.

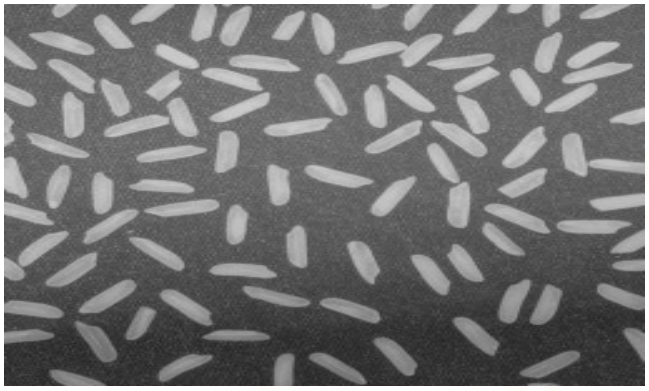

Fig 5 Cover image

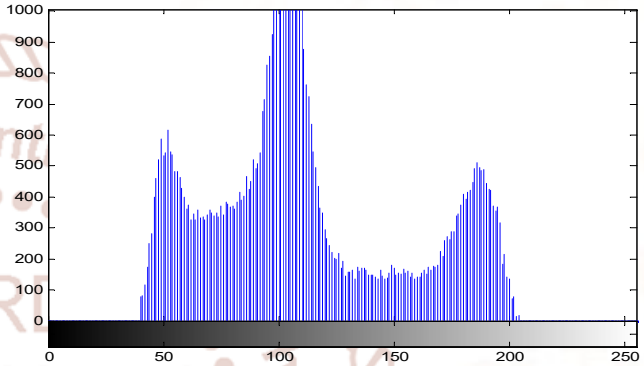

Fig 6 Histogram of cover image

Now, embedding of secret text message is done in the encrypted domain of the image as shown in Fig. 7 and obtained the stego image which is ready to transmit over the wireless communication channel.

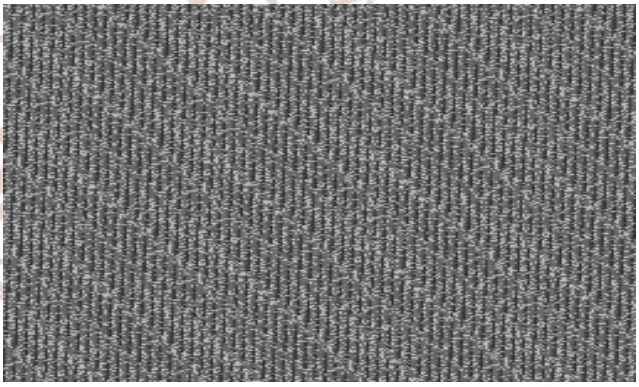

Fig 7 Encrypted image

At the receiver side, it is important to mention here that the correct cover image and correct secret text message will be decoded and retrieved at the receiver end if correct embedding key and correct encryption keys are utilized in the system.

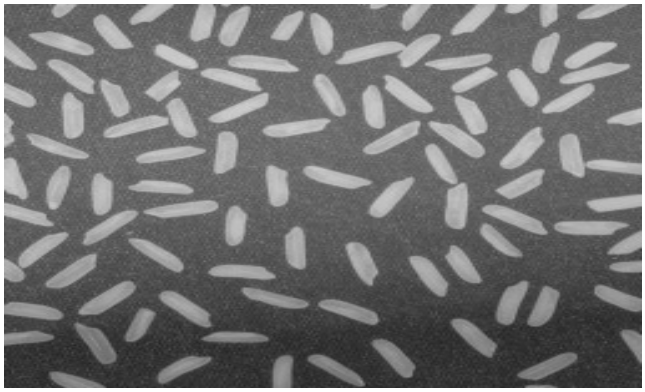

Fig 8: Recovered image

Decoded secret message- "Rajasthan Technical University, Kota".

If any of these keys are incorrect or not used in proper order then secret text message may be decoded. If encryption keys are not properly used and embedding keys are correct used then the secret keys is decoded correctly and incorrect retrieve image is obtained at the receiver end.

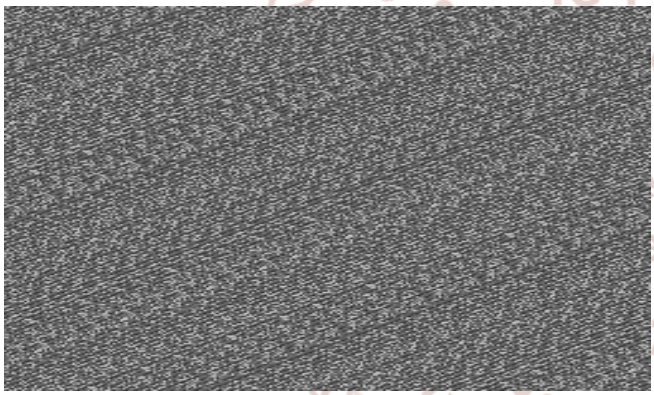

Fig-9: Received Image at receiver end with incorrect encryption keys

Decoded secret text message is "Rajasthan Technical University, Kota".

On the other hand, for malicious users or illegal users, embedding keys and encryption keys are being used incorrect, then cover image and text message are not correctly decoded and retrieved.

Moreover, if the embedding keys are incorrect while correct encryption keys then correct cover image is retrieved at the receiver end but wrong text message is decoded.

Similarly this procedure is implemented on one more image also whose results are shown below.

This is the process of hiding secret text in cover image at transmitter side and extracting secret text 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

Image name	Maximum embedded bits	Mean square error	Maximum capacity (bpp)	PSNR (dB)
Rice.png	1419	0.0020	0.022	75.12
Cameraman.tiff	1545	0.0023	0.024	74.51

6. CONCLUSIONS

In this paper, we have illustrated the proposed technique of embedding secret text message inside the cover image with proposed histogram shift method of reversible data hiding technique and also simulated and verified on MATLAB platform.

According to simulation results section, 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 left the minimum repeated pixels value and considered only maximum repeated pixel values and embed the secret text message. More number of maximum repeated pixels in cover image provides the more degree of freedom to embed the secret text message. PSNR value computed through our proposed work is better than previous work done in this field. Mean square error value is less. Therefore we can say that our approach provides better and efficient results in data hiding field.

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

REFERENCES

1) Nick Nabavian, Data Structures:Image Steganography, CPSC 350 , Nov. 28, 2007.

2) Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon, "Image Steganography: Concepts and Practice".

3) C.W. Honsinger, P. Jones, M. Rabbani and J.C. stoffel, "Lossless Recovery of an Original Image

Containing Embedded Data", U.S. Patent application, No. 6278791 B1, 2001.

4) Y.Q. Shi, Z. Ni, D. Zou, C. Liang, and G Xuan, "Lossless data hiding: fundamentals, algorithms and applications", IEEE International Symposium on Circuits and Systems (ISCAS), Vol. II, 2004, pp. 33-36.

5) G. Simmons, The prisoners problem and the subliminal channel," CRYPTO, pp. 51-67, 1983.

6) J. Tian, "Reversible data embedding using a difference expansion", IEEE Transactions on Circuits and System for Video Technology, Vol. 13, Issue. 8, pp.890-896, 2003.

7) E. P. Simoncelli, "Modeling the joint statistics of images in the wavelet domain", Proceedings of the 44th Annual Meeting, 1999.

8) Che-Wei Lee and Wen-Hsiang Tsai, "A lossless data hiding method by histogram shifting based on an adaptive block division scheme", Pattern Recognition and Machine Vision, 2010.

9) C. F. Lee, H. L. Chen, H. K. Tso, "Embedding capacity raising in reversible data hiding based on prediction of difference expansion", The Journal of Systems and Software, Vol 83, pp.1864-1872, 2010.