Performance Evaluation of Data Hiding Algorithm according to PSNR Value in Various Images using Histogram Shifting Method

Dipali Bansal [1], Sandeep Kumar Toshniwal [2]

[1]P. G. Scholar (Electronics & Comm.), Kautilya Institute of Technology & Engineering, Jaipur
[2]Associate Professor (Electronics & Comm.), Kautilya Institute of Technology & Engineering, Jaipur

ABSTRACT

In this paper we have used an efficient algorithm for hiding secret text in different types of cover image using histogram shifting method of reversible data hiding technique. This algorithm considers only maximum repeated pixels in histogram. We have analyzed this algorithm in MATLAB simulation tool. In this analysis various types of cover images are used to hide secret text in encrypted domain. Some performance metrics are calculated to compare performance of all the images. Metrics are like maximum embedded bits, mean square error, maximum capacity and peak signal to noise ratio.

Keyword: - *Encryption, Mean square error, Embedding, Extraction, Data hiding*

1. INTRODUCTION

Hiding of data is a source of secret communication which uses different types of resources as a cover media and hides the secret media into cover media to produce marked media. Data hiding technique is used to prevent copyright issues, detection of tempering with data, data integrity etc. Imperceptibility and embedding capacity are the two main properties which should be possessed by data hiding technique which ensures that hidden data is undetectable and efficiency is high.

Embedding method and extracting method are the two main methods existed in data hiding process. In embedding method, secret information is hidden into cover image. Cover image is changed after embedding the secret information. This modified cover image which exhibits secret information is called marked data. Secret information is extracted from the marked data and generates the original cover image.

Steganography is the specialty of undetectable communication. The term invisible is not connected to the significance of the communication, as in cryptography in which the objective is to secure the communication from an meddler. In actuality it alludes to concealing the presence of data itself. The general thought of Hiding Information (messages) in like manner digital contents, interests a more extensive class of applications that go past Steganography. The techniques engaged with such applications are by and large alluded to as Information Hiding. For example, while it is conceivable to include metadata around a picture in extraordinary labels (exif in JPEG standard) or document headers, this data will be lost when the picture is printed, in light of the fact that metadata embedded in labels on headers are attached to the picture as long as the image exists in digital form and are lost when the record is printed.

In a digital world, Steganography and Cryptography are both expected to shield data from unwanted gatherings. Both Steganography and Cryptography are fantastic means by which to achieve this yet neither technology alone is impeccable and both can be broken. It is consequently that most experts would recommend using both to include various layers of security. Almost all digital file formats can be utilized for steganography, yet the formats that are more reasonable are those with a high level of redundancy.

2. LITERATURE REVIEW

Due to increase in demand of internet, risks of illegal access and unauthorized tempering of information also increases. Today, one and only main issue is protection of secret information from unauthorized subscribers in public network. Before, few years, data hiding techniques were more used in spatial domain of cover image. The secret data which is embedded into the least significant bits of some selected pixels of image is consequently exhibits less changes in their pixel value or high frequency components of image. Few researchers have diverted their mind into the direction of enhance the robustness in the reversible data hiding techniques.

In 2010, Chin-Feng Leea, Hsing-Ling Chenb and Hao-Kuan Tso have proposed an adaptive reversible data hiding technique related to prediction of difference expansion.

In 2013, Pramod R Sonawane and K.B.Chaudhari have proposed a technique based on adaptive embedding and pixel selection to increase embedding capacity and compared it with conventional technique.

In 2016, Fangjun Huang, Xiaochao Qu, Hyoung Joong Kim and Jiwu Huang have proposed a new reversible data hiding technique based on histogram shifting for JPEG images in which they have expanded coefficients with values 1 and -1 to carry message bits.

In 2017, Nour Kittawi and Ali Al-Haj have proposed an algorithm for reversibly hiding the data into encrypted grayscale medical images. They have hidden two watermarks in a particular encrypted image.

3. APPLICATIONS OF STEGANOGRAPHY

A wide vary of applications like digital watermarking are often used for:

Medical security: Current picture formats for example, DICOM isolate picture data from the text (for example, patients name, date and doctor), with the outcome that the link between picture and patient occasionally gets ruined by protocol converters. In this way embedding the patients name in the picture could be a useful security measure.

Terrorism: As indicated by government officials militants use to hide data, maps and images of targets for communicating or commanding other militants or their alliance groups.

Hacking: The programmer hides a monitoring tool, server behind any picture or sound or text document shares it with mail or talk which will get embedded and executed. This quite installer monitoring device will help the hacker to perform hacking inside the workstation.

Licensed property offenses: Licensed property, defined as the equations, models, copyrights and customer records maintained by a company, can be significantly more valuable than the real things they sell.

Corporate espionage: Utilization of spies to gather data about what another element is doing or arranging in a professional workplace.

Watermarking: Uncommon inks to compose hidden messages on bank notes and furthermore the entertainment industry utilizing digital watermarking and fingerprinting of sound and video for copyright protection.

Automatic monitoring of radio advertisements: It is helpful to have an automated system to confirm that adverts are played as contracted.

The main goal of this research is to enhance the security and embed the text message inside the cover image by using histogram shift method and investigate the response of different types of cover image in order to increase the embedded capacity of text message.

4. RESEARCH METHODOLOGY

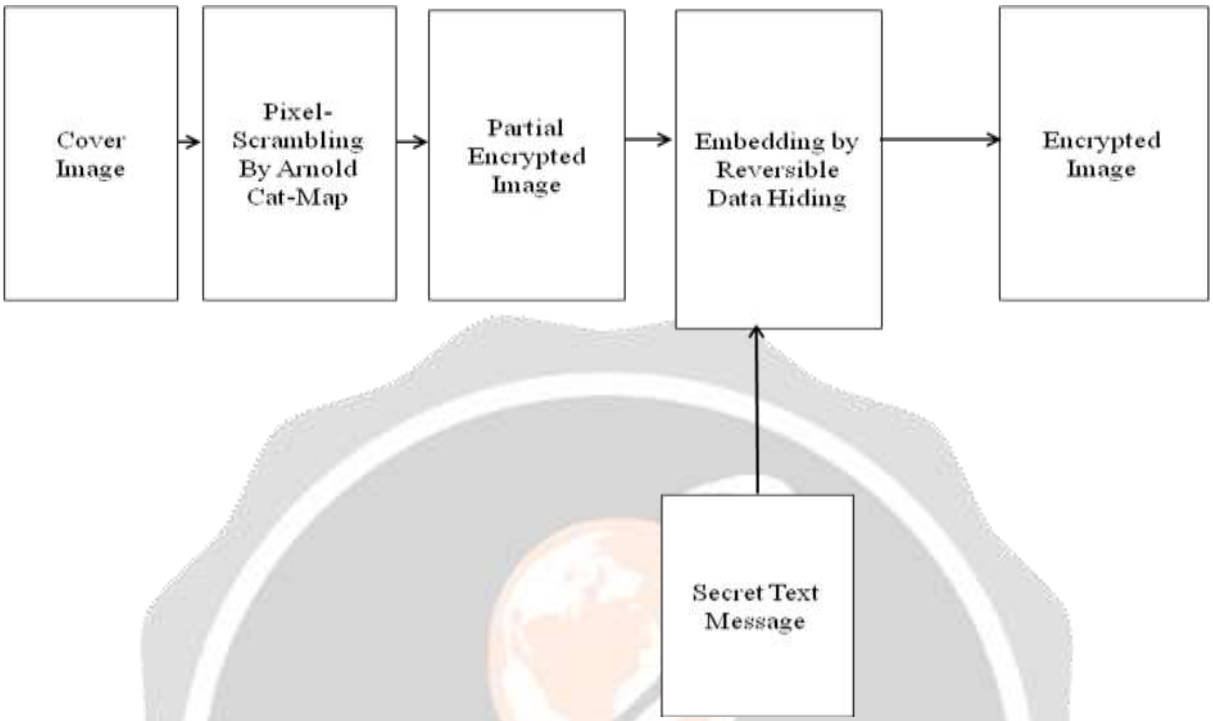


Fig 1 Embedding procedure

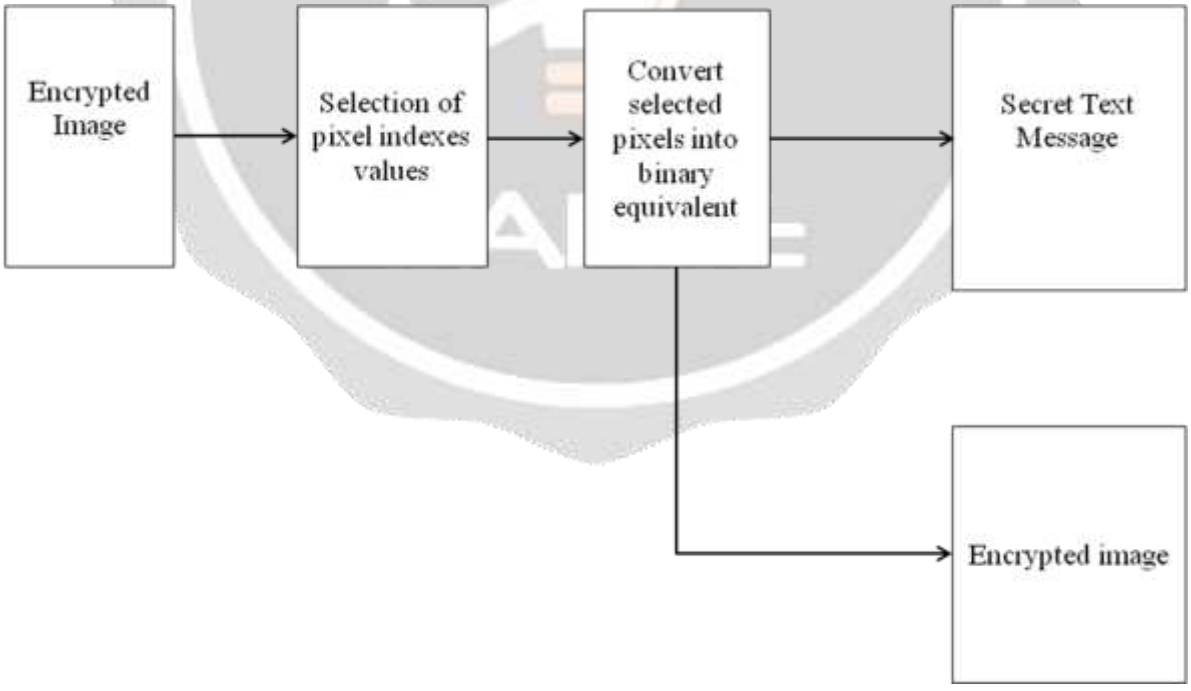


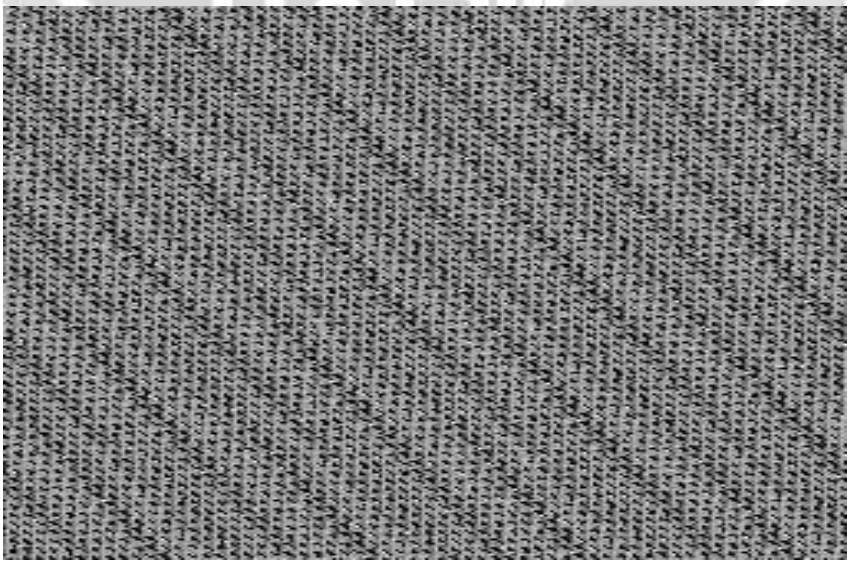
Fig 2 Extraction procedure

5. PROPOSED WORK

In this section, the results are presented which are obtained through experiments done on MATLAB platform. Various types of grey scale image of size having 256 x 256 is selected as cover image 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. 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.

Now, embedding of secret text message is done in the encrypted domain of the image by selecting locations of only maximum repeated pixels in the histogram of encrypted image and obtained the stego image which is ready to transmit over the wireless communication channel. In this process location of minimum repeated pixel is avoided.

Fig, 3 Cameraman image



Fig, 4 Encrypted Cameraman image

Fig, 5 Extracted Cameraman image

Similarly experiment is performed on other images also and simulation results are mentioned in the next section.

6. EXPERIMENTAL RESULTS

We have considered different types of cover image to hide a secret text and computed different performance metrics which are then used to compare the performance of different images. In the below table all the metrics are mentioned.

Table 1: Performance parameters

Image name	Maximum embedded bits	Mean square error	Maximum capacity (bpp)	PSNR (dB)
Cameraman.tiff	1545	0.0023	0.024	74.51
Livingroom.tiff	842	0.0015	0.013	76.37
Pirate.tiff	1311	0.0018	0.020	75.58
Mandril_gray.tiff	811	0.0013	0.012	76.99
Woman_darkhair.tiff	2486	0.0028	0.038	73.66

6. CONCLUSIONS

We have successfully performed analysis of hiding secret text in different types of cover image. 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.

7. REFERENCES

[1] Pramod R Sonawane, K.B .Chaudhari ,"Reversible image watermarking using adaptive prediction error expansion and pixel selection", International Journal Of Engineering Science And Innovative Technology (Ijesit) , Volume 2, Issue 2, March 2013.

[2] Fangjun Huang,, Xiaochao Qu, Hyoung Joong Kim and Jiwu Huang, "Reversible Data Hiding in JPEG Images", IEEE, 2016.

[3] Nour Kittawi and Ali Al-Haj, "Reversible Data Hiding in Encrypted Images", IEEE, 2017

[4] C.-L. Liu, D.-C. Lou, and C.-C. Lee, "Reversible Data Embedding Using Reduced Difference Expansion", in Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2007.

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

[6] Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon, "Image Steganography: Concepts and Practice".

[7] 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.

[8] M. Awrangjeb, "An overview of reversible data hiding," International Coriference on Computer and Iriformation Technology (ICCIT), 2003, pp. 75-79.