ISSN: 0975-766X
CODEN: IJPTFI
Research Article

Available Online through
www.ijptonline.com

A WELL SECURED AND EFFICIENT DATA EMBEDDING TECHNIQUE COMPARISON BASED ON LSB REPLACEMENT AND PIXEL PAIR MATCHING METHOD

Mary Reeba.A*, G.MaryValantina
Assistant Professor, Dept. of CSE, Sathyabama University, Chennai, India,
Email:maryreebaa@gmail.com

Received on 05-04-2015 *Accepted on 22-04-2015*

Abstract

This paper proposes the data hiding method comparison using pixel pair matching method and LSB replacement for secret data communication using steganography and cryptography techniques. LSB is the direct replacement of LSBs of noisy or unused bit of cover image with secret message bits which uses integer wavelet transform. In PPM a pixel pair created is replaced by the searched coordinate to conceal the message. Diamond encoding is used in PPM for region selection in the image. The MSE and PSNR parameters are measured and compared for PPM and LSB replacement methods. Then the best performance method is selected

Keywords*:* Least Significant Bit (LSB), Pixel Pair Matching (PPM), Diamond Encoding (DE).

I. Introduction

Steganography is one of the methods used for the hidden exchange of information and it can be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message [2]. Cryptography is the art of codifying messages. So that they become unreadable. Any digital file such as image, audio, video can be used to hide secret message. The file used to hide the data is referred to as cover object and the term stego-object is used for the file containing secret message.

LSB is the direct replacement of LSBs of noisy or unused bit of cover image with the secret message bits. The basic idea of PPM is to use the values of pixel pair as a reference coordinate and search a coordinate in the neighborhood set of this pixel pair according to a given message digit. The pixel pair is then replaced by the searched coordinate to conceal the digit. [1] Adaptive Pixel Pair Matching method, referred to as APPM in this paper, is a popular data hiding method.

This method not only allows concealing digits in any notational system. But also provides the same or even smaller embedding distortion than DE for various payloads.

An Optimal Pixel Pair Adjustment Process (OPAP) is proposed to enhance the image quality of stego-image obtained by the LSB substitution method. In this method the image quality of the stego image can be greatly improved with low extra computational complexity [3]. The diamond encoding method has been used to alleviate distortions after hiding

the secret digit in to two cover pixel. It not only keeps high stego-image quality but also conceals large amount of data into cover images for secret communication [4].

In 2010 proposed a novel section-wise exploring modification direction method to enhance the image quality of EMD. Their method segments the cover image into pixel sections, and each section is partitioned into the selective and descriptive groups. The EMD embedding procedure is then performed on each group by referencing a predefined selector and descriptor table. This method combines different pixel groups of the cover image to represent more embedding directions with less pixel changes than that of the EMD method. By selecting the appropriate combination of pixel groups, the embedding efficiency and the visual quality [5]. This method for improving embedding efficiency is presented in which the choice of whether to add or subtract one to/from a pixel depends both on the original gray value and a pair of two consecutive secret bits. In other words, the direction of modification to the cover pixels is exploited for data hiding. However, there exist two different modification-directions corresponding to a same pair of secret bits to be embedded, meaning that the exploitation is incomplete. The diamond encoding method produces a diamond characteristic value (DCV) of the pixel-pair block, and the DCV is revised as the embedded secret digit after data embedding procedure. For each block, the diamond encoding technique addresses the minimal changes of two pixel values under the embedding parameter k. The diamond encoding technique minimizes the distortion after the DCV alteration to perform better visual quality. The rest of this paper is organized as follows. The proposed method is given in Section II .Section III includes the conclusion.

II. Proposed Work

In this project, two algorithms and two techniques are used. Two algorithms are Least Significant Bit replacement (LSB) algorithm and Pixel pair Matching (PPM) algorithm. Two techniques are steganography and cryptography. For data security, data is concealing in the image using the two algorithms. After the hiding process, the image quality will degrade and error will occur. So we calculate the Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). Then we compare which algorithm provides better performance through the parameter evaluation.

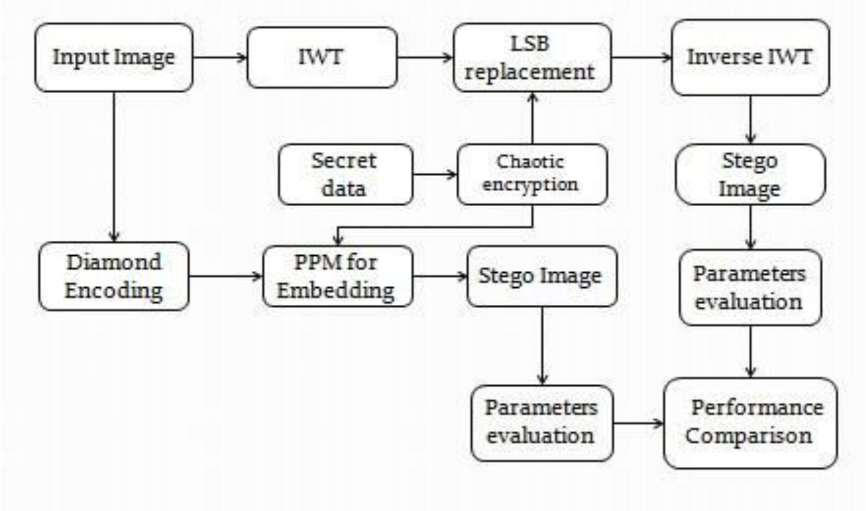


Fig-1: Block Diagram Explanation for data embedding.

1. Chaos Encryption

It is an advanced encryption standard to encrypt the privacy data for secure transmission. Then the encrypted text is obtained by xor- ing the input data with encrypted key Value. The Key values are obtained from Chaotic Sequence Generation with threshold function.

2. Input image

The image contains RGB (Red, Green, and Blue) plane. Here Red plane is over brightness, Green plane is visible and Blue plane is darkness. Here we select the blue plane for data security.

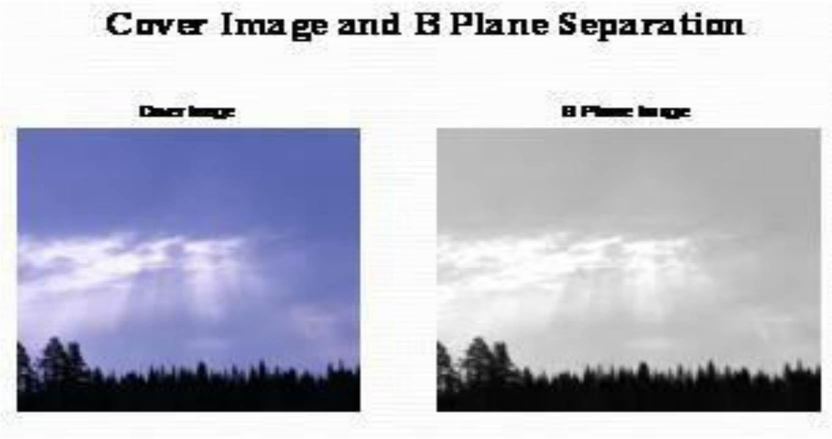


Fig 2: Cover Image and B plane Separation.

3. Integer Wavelet Transform

Integer Wavelet Transform (IWT) decomposes the image into different sub-band images namely LL, LH, HL, and HH for embedding the messages in the pixel coefficients of sub-bands.

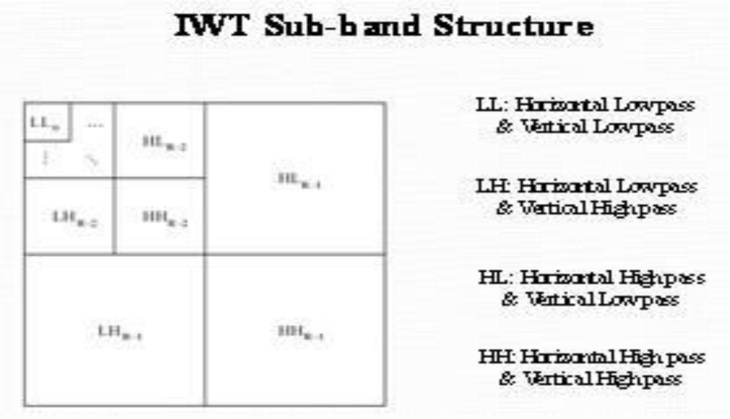

IWT Sub-band Structure
LL_N
...
HL_N-2
HL_N-1
LH_N-2
HH_N-2
LH_N-1
HH_N-1
LL: Horizontal Lowpass & Vertical Lowpass
LH: Horizontal Lowpass & Vertical Highpass
HL: Horizontal Highpass & Vertical Lowpass
HH: Horizontal High pass & Vertical Highpass

Fig 3

Here LL sub-bands contains the significant part of the spatial domain image and High-frequency sub-band contains the edge information of input image. Then the secret text data is embedded into the wavelet coefficients of high frequency sub- bands because it is non sensitive to human visual system.

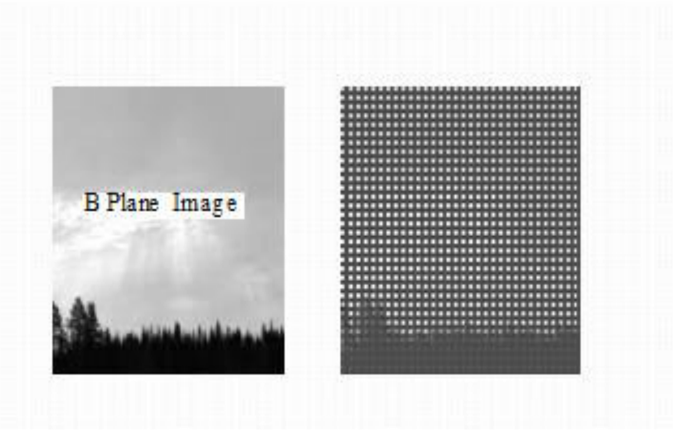


Fig 4.Block wise IWT Decomposition

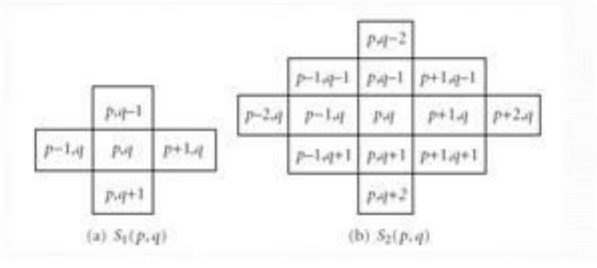
4. LSB Embedding

A 8-bit gray scale image matrix consisting m × n pixels and a secret message consisting of k bits. The first bit of message is embedded into the LSB of the first pixel and the second bit of message is embedded into the second pixel and so on. The resultant Stego- image which holds the secret message is also a 8-bit gray scale image and difference between the cover image and the Stego- image is not visually perceptible. The quality of the image, however degrades with the increase in number of LSBs.The hiding process will introduce the error between input and output image and it is determined by mean square error and Peak signal to noise ratio determines the image quality.

Fig 5

5. Diamond encoding

This technique used to increase the hiding capacity with minimum distortion and high visual quality. It hides the secret message digit in B - ary notational system into the pixel pair and B is $2k^2+2k+1$ where k is an embedding parameter. It uses a diamond function *f* to compute the Diamond characteristics value in embedding and extraction procedures. The function f(x , y) =((2K+1)x + y) mod B and coordinates(x ’, y’) belong to neighborhood set will find to replace the (x , y).



a) Diamond Encoding Pattern with k=1 b) Diamond Encoding Pattern with k=3
|s1=5| $|S_k|=2k^2+2k+1$ |s2 = 13|

Fig 6 Diamond encoding pattern

6. PPM Embedding

In PPM, two pixels are used for embedding process in that one pixel is equivalent to message digit and another pixel value in the neighborhood set is to be replaced by message digit. In order to minimize the Embedding error, the extraction function and neighborhood set are redefined by the constant factor based on Embedding Parameter. The modulus distance will be determined by, d = message digit – f(x, y) mod B for finding the coordinates (x', y') to replace the (x, y) coordinates.

Then we compare the output of LSB Embedding and PPM Embedding algorithm to find which algorithm provides the better performance through the parameter evaluation.

Data Extraction

At this stage, An image and secret hidden text messages are extracted from stego encrypted image.[6] The secret data can be extracted from the embedded image with help of the coordinates used at PPM embedding process. This extraction process is opposite to data embedding, pixel coefficient and embedding rate are used here to extraction of data in LSB. The lifting wavelet transformation will be performed to stego image to find reserved space to select coefficients which are used at embedding side.[7],[8]. Finally, Extracted secret text data is in the form of cipher text and then convert into plain text using chaos decryption process.

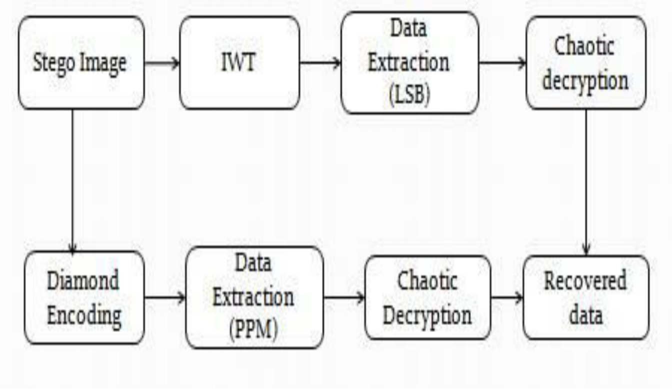


Fig 7 Flow diagram of Data extraction.

Parameter Measurement

The hiding process will introduce the error between input and output image and it is determined by mean square error and the peak signal to noise ratio determines the image quality.

The formula for MSE is,

$$MSE= (1/ (M\times N)) \sum^{M}_{i=1} \sum^{N}_{j=1}(a_{ij} - b_{ij})^2$$

The formula for PSNR is,

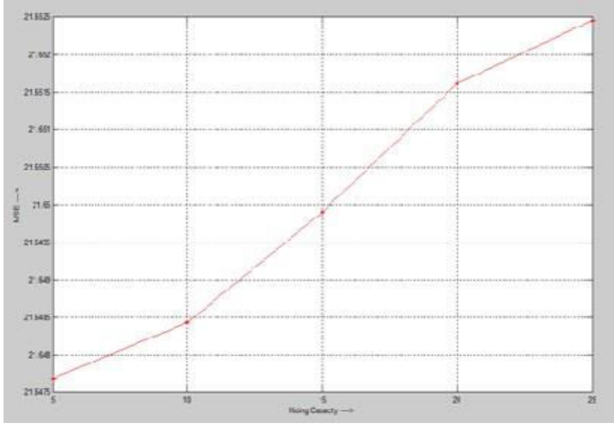
$$PSNR= 10 \log_{10} (255^2/MSE)$$

Where,

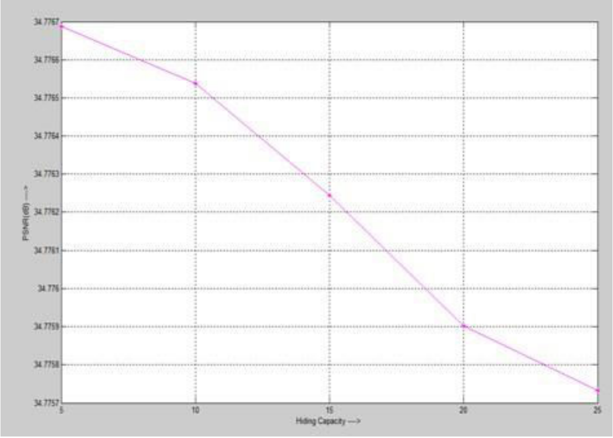
M, N are Number of Rows and Columns

a_{ij} – Image before embedding and b_{ij} – Image after embedding

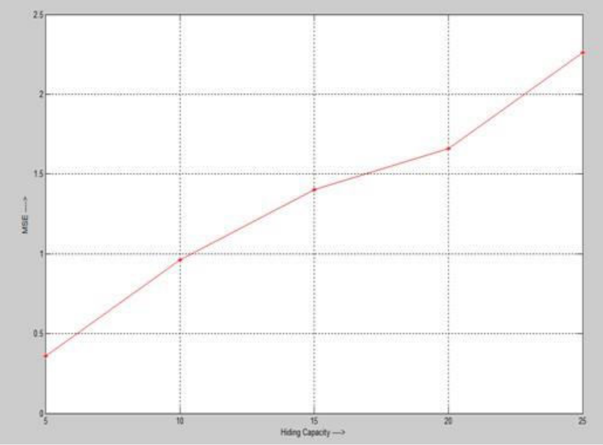
PERFORMANCE OF LSB INTERMS OF MSE AND PSNR



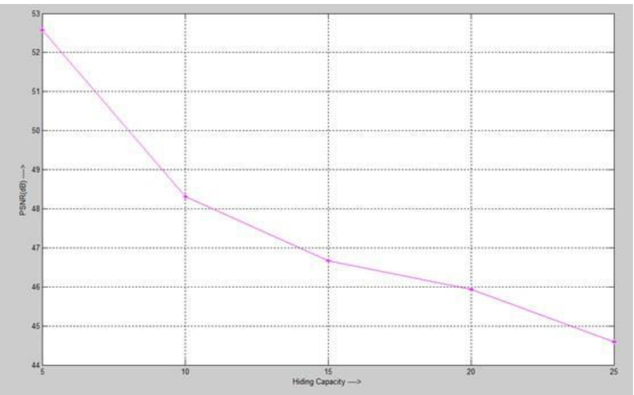
Hiding capacity vs MSE



Hiding capacity vs MSE



Hiding capacity vs PSNR



III. Conclusion

This paper proposed the data hiding method comparison using pixel pair matching method and LSB replacement for secret data communication using steganography and cryptography techniques. In PPM, the data security is high and it can preserve the image quality at high payload when compared to other methods. By Simulation we hiding capacity vs PSNR Proposed method show better performance than the existing methods.

References

1. Wien Hong and Tung-Shou Chen, –A novel data Embedding method using adaptive Pixel Pair Matching*,” IEEE transactions on information forensics and security*, vol. 7, no. 1, 2012.
2. J. Fridrich*, Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2009
3. C. K. Chan and L. M. Cheng, –Hiding data in images by simple LSB substitution,‖ *Pattern Recognit.*, vol. 37, no. 3, pp. 469–474, 2004.
4. R.M. Chao, H. C. Wu, C. C. Lee, and Y. P. Chu, –A novel image datahiding scheme with diamond encoding,‖ *EURASIP J. Inf. Security*, vol. 2009, 2009, DOI: 10.1155/2009/658047, Article ID 658047.
5. S J. Wang, Y. Sun, H. Xu, K. Chen, H. J. Kim, and S. H. Joo, –An improved section-wise exploiting modification direction method,‖ *Signal Process.*, vol. 90, no. 11, pp. 2954–2964, 2010.
6. A. D. Ker, –Steganalysis of LSB matching in grayscale images,‖ *IEEE Signal Process. Lett.*, vol. 12, no. 6, pp. 441–444, Jun. 2005.

7. J. Mielikainen, ―LSB matching revisited,‖ *IEEE Signal Process. Lett.*, vol. 13, no. 5, pp. 285–287, May 2006.

8. I. S. Jacobs and C. P. Bean, ―Fine particles, thin films and exchange anisotropy,‖ in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

Corresponding Author:

G.MaryValantina*,

Email: *Valantina78@gmail.com*