*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. IV (Jan. 2014), PP 76-80*
*www.iosrjournals.org*

# Edge Adaptive Image Steganography Based on Adaptive Pixel Pair Matching

Akhil P. V.[1], Akbersha K. E.[2], Mohammed Sidheeque[3]
[1](Computer Applications, MES-AIMAT, India)
[2](Computer Applications, MES-AIMAT, India)
[3](Computer Applications, MES-AIMAT, India)

***Abstract:*** *This paper proposes a new improved steganographic technique based on pixel pair matching which is driven by edge adaptive technique. The cover image is scanned first to explore the edges of the image and is used as the candidate region to perform data hiding using pixel pair matching. The basic idea of pixel pair matching (PPM) is to use the value of a 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. The method uses only sharper edge regions while keeping the other smoother regions as they are. In contrast to the existing methods based on PPM, the masking driven approach has lower distortion for various payloads. The proposed method is expected to provide better performance than the existing techniques based on LSB and also secure against well-known steganalysis techniques.*

***Keywords:*** *Image steganography, LSB encoding, payload, cover image, stego image*.

## I. INTRODUCTION

In recent years, the security and the confidentiality of the sensitive data has become of prime and supreme importance due to the explosive growth of internet and the fast communication techniques. Therefore how to protect secret messages during transmission becomes an important issue and hiding data provides a good layer of protection on the secret message. One of the widely accepted data hiding technique is image steganography. Image steganography uses a digital image as cover media and hence it is called cover image. The data is hidden in the cover image and the resulting image is called stego image. The data can be extracted out from the stego image and the existence of a hidden message in the cover image is invisible. The embedding of data in an image can cause distortion in the cover image and this distortion caused by data embedding is called embedding distortion. A good data-hiding method should be immune to statistical and visual detection while providing an adjustable payload [1], [2]. There are a number of techniques available which can perform image steganography in a digital image and this paper focuses on analyzing the different techniques and proposing a method which can offer better results over the methods that are studied.

### 1.1 Digital Steganography

A digital steganographic encoder is shown on Figure 1. The message is the data that the sender wishes to keep confidential and can be text, images, audio, video, or any other data that can be represented by a stream of bits. The cover or host is the medium in which the message is embedded and serves to hide the presence of the message. This is also referred to as the message wrapper. The message embedding technique is strongly dependent on the structure of the cover. It is not required that the cover and the message have homogeneous structure.

The image with the secretly embedded message produced by the encoder is the stego-image. The stego-image should resemble the cover image under casual inspection and analysis. In addition, the encoder usually employs a stego-key(optional) which ensures that only recipients who know the corresponding decoding key will be able to extract the message from a stego-image.[3]

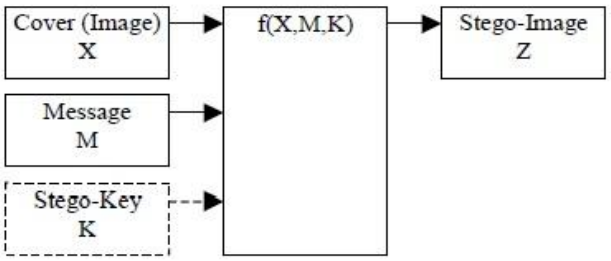


Fig. 1: Steganographic Encoding

**1.2 Human Visual System and Image Steganography**

The property of human eye on how an image is perceived is exploited by the human visual system (HVS). Certain characteristics of an image and not easily visible to human eye and those characteristics can be used and combined with image steganography to avoid visual and statistical detection of the embedded data. The key factors which influence them include:

- The eye is less sensitive to noise in the high resolution bands and in those bands having orientation of 45.
- The eye is less sensitive to noise in those areas of the image where brightness is high or low.
- The eye is less sensitive to noise in highly textured areas, but, among these, more sensitive near the edges.

These properties can prove handy when combined and exploited in image steganography. The regions located at the sharper edges present more complicated statistical features and are highly dependent on the image contents. Moreover, it is more difficult to observe changes at the sharper edges than those in smooth regions. Many of the data embedding techniques developed so far has concentrated only on the data hiding aspect of image steganography and not on studying the image characteristics and hiding the data.

The rest of this paper is organized as follows. Section 2 explains the various methods developed for image steganography, and also compares the various steganography techniques, a proposed system is presented in section 3 and section 4 includes conclusion and remarks.

## II. SURVEY

There are various data hiding techniques developed in recent years.J. Mielikainen developed a method [4] which is based on pixel pair matching and it uses a pair of pixels as the embedding unit. The LSB of first pixel carries one bit of information and a binary function of the two pixel values carry another bit of information. This method offers same payload (number of bits embedded in the cover image) as LSB matching with fewer changes to cover image. The MSE of LSB for 1 bpp is 0.5, while for LSBMR it is 0.375.

OPAP [5] is an enhancement of LSB substitution method and it is based on embedding error. It uses only one pixel as embedding unit. In this method, for a m-bit pixel, if message bits are embedded to the right-most r LSB's then other m-r bits are adjusted by a simple evaluation. These m-r bits are either replaced by the adjusted result or otherwise kept unmodified based on if the adjusted result offers smaller distortion.

An improvement of LSB matching revisited method is EMD [6] in which each (2n+1)-ary notational system is carried by n cover pixels and at most only one pixel is increased or decreased by 1. The secret message is converted into a sequence of digits in the notational system with an odd base. Then pseudo-randomly permute all cover pixels according to a secret key, and divide them into a series of pixel-groups, each containing n pixels. The method is very well able to provide better stego image quality under the same payload than traditional LSB.

Diamond Encoding [7] an extension of EMD method and it first partitions the cover image into non-overlapping blocks of two consecutive pixels and transforms the message to a series of K-ary digits. For each block a Diamond Characteristic Value (DCV) is calculated and one secret K-ary digit is concealed into DCV. The DCV is modified to secret digit and it is done by adjusting pixel values in a block. This method is capable of hiding more secret data while keeping the stego-image quality degradation imperceptible.

Method used in [8] is an enhancement of the EMD method and this 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. The method combines different pixel groups of the cover image to represent more embedding directions with less pixel changes than the EMD method. By selecting the appropriate combination of pixel groups, the embedding efficiency and the visual quality of the stego image is enhanced. It offers higher embedding efficiency than EMD method.

The method [9] partitions the cover image into non-overlapping blocks of two consecutive pixels. The difference value is calculated from the values of the two pixels in each block and all possible difference values are classified into a number of ranges. The selection of the range of intervals is based on the characteristics of human vision's sensitivity to gray scale values from smoothness to contrast. The difference value is then replaced by a new value to embed the value of a sub-stream of the secret message. The resultant image offers better quality results.

Edge Adaptive Image steganography [10] extends the LSB matching revisited steganography. The method first divides the cover pixels into blocks and rotates each block by a random degree based on the secret key. The rotation causes new edges to appear and among the edges a threshold value is used to get the most suitable areas where data is hidden. Now the blocks are rotated back to normal and thus the data gets embedded. The reverse of the method is employed to extract the data. The method offers better image quality and immunity to steganalysis than the LSBMR method.

Reversible data embedding using interpolation and reference pixel distribution introduced in [11] is a reversible data hiding method based on image interpolation and detection of smooth and complex regions in the cover image. A binary image that represents the locations of reference pixels is constructed according to the local image activity. In complex regions, more reference pixels are chosen and fewer pixels are used for embedding and vice-versa for smooth regions. Pixels are interpolated according to the constructed binary image, and interpolation errors are then used to embed data through histogram shifting. It offers better prediction and a mechanism to add or remove reference pixels based on local image characteristics. The method achieves better PSNR for a range of embedding rates.

Pixel Pair Matching(PPM) [12] method uses 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 searched digit conceals the digit and it replaces the pixel pair. It makes use of a more compact neighborhood set than used in Diamond encoding. The extraction process finds the replaced pixel pair to extract the message data. Exploiting Modification Direction(EMD) method has a maximum capacity of 1.161 bpp and Diamond Encoding(DE) extends the payload of EMD by embedding digits in a larger notational system. The proposed method offers lower distortion than DE by providing more compact neighborhood sets and allowing embedded digits in any notational system. Compared with the optimal pixel adjustment process (OPAP) method, the proposed method always has lower distortion for various payloads.

The proposed method in [13] is a hiding scheme by replacing the LSB of a cover according to the difference values between a pixel and its four touching neighbors. Although this method can embed most secret data along sharper edges and can achieve more visually imperceptible stegos, the security performance is poor. Since the method just modifies the LSB of image pixels when hiding data, it can be easily detected by existing steganalytic algorithms, such as the RS analysis.

Optimized Bit Plane splicing algorithm [14] is implemented by M. Naseem et.al. where in the pixels are grouped based on their intensity and then the number of bits are to represent the hidden data are chosen. As the bits are grouped based on the intensity of the pixels, more number of darker intensity pixels can be used to represent the hidden data than just the LSB.

In [15] the authors implemented a Combined Linked-list and LSB technique that uses the concept linked list of randomly embedding the data in the image and linking them together. The attacker is unable to guess the next message as the data is not hidden sequentially. Also, without the password it is not possible to access the hidden data.

## III. PROPOSED SYSTEM

The data embedding methods discussed so far does not take into consideration any of the image characteristics. A good data-hiding method should be capable of evading visual and statistical detection while providing an adjustable payload. This immunity can be achieved by exploiting one of the characteristics of human visual system (HVS). If the image characteristics are considered and candidate areas in an image for data embedding are found out, the data can be embedded on those areas, and the result can offer more immunity towards statistical and visual evaluation methods of steganography. The input to the method is the cover image, key and secret message. The proposed method first divides the cover image into non-overlapping blocks. Each small block is related to a random degree based on secret key. The rotation causes new edges to appear and among the edges a threshold value is used to get the most suitable areas where data can be hidden. Data hiding is done using adaptive pixel pair matching technique. Now the blocks are rotated back to normal with data embedded in it. The reverse of the method is employed to extract the data.

### 1.1 Embedding Procedure

Suppose the cover image is of size M × M, S is the message bits to be concealed and the size of S is |S|. First we calculate the minimum B such that all the message bits can be embedded. Message digits are sequentially concealed into pairs of pixels. The detailed procedure is listed as follows.

Input: Cover image I of size M × M, secret bit stream S, and key K.

Output: Stego image $I'$ ,cB , ΦB(x,y) and Kr.

1. Divide the cover image into non-overlapping blocks of Bz x Bz pixels. For each small block, we rotate it by a random degree in the range of {0, 90, 180, 270}, as determined by a secret key Kr.
2. Find the minimum B satisfying $\lfloor M \times M/2 \rfloor \geq |SB|$, and convert S into a list of digits with B -ary notational system SB.
3. The value of cB and ΦB(x,y) are computed.
4. In the region defined by ΦB(0,0), record the coordinate $(xi', yi')$ such that $f(xi', yi') = i$ , $0 \leq i \leq B - 1$ .
5. Construct a nonrepeat random embedding sequence Q using a key K.
6. To embed a message digit sB, two pixels (x,y) in the cover image are selected according to the embedding sequence , and calculate the modulus distance between sB and f(x,y), then replace (x,y) with (x + xd, y + yd) .

7. Repeat Step 5 until all the message digits are embedded.
8. After data hiding, the resulting image is divided into non-overlapping blocks Bz x Bz. The blocks are then rotated by a random number of degrees based on key K. The process is very similar to Step 1 except that the random degrees are opposite. Then we embed a parameter Bz into the image.

**1.2 Extraction Procedure**

To extract the embedded message digits, pixel pairs are scanned in the same order as in the embedding procedure. The embedded message digits are the values of extraction function of the scanned pixel pairs.

Input: Stego image I´ ,cB , ΦB(x,y) and Kr..
Output: Secret bit stream S.

1. To extract data, we first extract the needed information, i.e., the block size Bz. We then do exactly the same things as Step 1 in data embedding. The stego image is divided into Bz x Bz blocks and the blocks are then rotated by random degrees based on the secret key Kr.
2. Construct the embedding sequence Q using the key Kr.
3. Select two pixels (x´ ,y´ ) according to the embedding sequence Q.
4. Calculate f(x´ ,y´ ), the result is the embedded digit.
5. Repeat Steps 2 and 3 until all the message digits are extracted.
6. Finally, the message bits S can be obtained by converting the extracted message digits into a binary bit stream.

The Pixel Pair Matching (PPM) method has only very little detection methods available and is considered to be a method which offers very good results. The edge detection actually considers the image characteristics and extracts out the suitable regions for data embedding. The resultant area applies the Pixel Pair Matching(PPM) method where 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 searched digit conceals the digit and it replaces the pixel pair. Thus the data is embedded in the cover image and during extraction, the corresponding pixel pair is found to extract the data. The resultant image produces no artifacts in stego images and the steganalysis results are similar to those of the cover images, it offers a secure communication under adjustable embedding capacity. The proposed method is shown below:

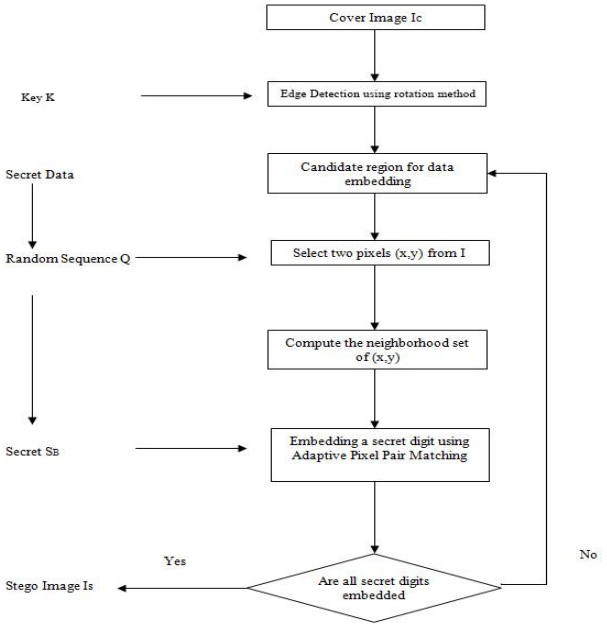


Fig. 2: Proposed System

## IV. CONCLUSION

This article discussed various steganography techniques available for data embedding in a digital image. The methods were closely observed for their limitations and based on this a new method was proposed which combines the idea of considering the image characteristics along with the pixel pair matching technique. The proposed method hides data on the edges identified in the host image and is expected to offer better results

over any of the available techniques. This adaptive way of data hiding can pave way for a new line of research in image steganography.

## REFERENCES


[1] T. Filler, J. Judas, and J. Fridrich, "Minimizing embedding impact in steganography using trellis-coded quantization," in Proc. SPIE, Media Forensics and Security, 2010, vol. 7541, DOI: 10.1117/12.838002.

[2] S. Lyu and H. Farid, "Steganalysis using higher-order image statistics,"IEEE Trans. Inf. Forensics Security, vol. 1, no. 1, pp. 111–119, Mar.2006.

[3] E Lin and E Delp, "A Review of Data Hiding in Digital Images" CERIAS Tech Report 2001-139

[4] J. Mielikainen, "LSB matching revisited," IEEE Signal Process. Lett., vol. 13, no. 5, pp. 285–287, May 2006.

[5] 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.

[6] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," IEEE Commun.Lett., vol. 10, no. 11, pp. 781–783, Nov. 2006

[7] R.M. Chao, H. C. Wu, C. C. Lee, and Y. P. Chu, "A novel image data hiding scheme with diamond encoding," EURASIP J. Inf. Security, vol. 2009, 2009, DOI: 10.1155/2009/658047, Article ID 658047.

[8] 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.

[9] Da-Chun Wu, Wen-Hsiang Tsai, "A steganographic method for images by pixel-value differencing", ELSEVIER Pattern Recognition Letters 24 (2003) 1613–1626

[10] WeiqiLuo, Fangjun Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited" , IEEE ransactions on infoemation forensics and security, Vol. 5, No. 2, June 2010

[11] W. Hong and T. S. Chen, "Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism," J. Vis. Commun. Image Represent., vol. 22, no. 2, pp. 131–140, 2011.

[12] Wien Hong ,Tung-Shou Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching", IEEE transactions on information forensics and security, Vol. 7, No. 1, February 2012.

[13] K. Hempstalk, "Hiding behind corners: Using edges in images for better steganography," in Proc. Computing Women's Congress, Hamilton, New Zealand, 2006.

[14] V.M. Potdar, S. Han, E. Chang, Fingerprinted secret sharing steganography for robustness against image cropping attacks, Proceedings of IEEE Third International Conference on Industrial Informatics (TNDIN), Perth, Australia, 10-12 August 2005,pp. 717- 724.

[15] M. Nosrati, R. Karimi, H. Nosrati, and A. Nosrati, "Embedding stego-text in cover images using linked list concepts and LSB technique", Journal of American Science, Vol. 7, No. 6, 2011, pp. 97-100.