An Asymptotically Uniformly Reversible Data Hiding in Encrypted Images by Pixel Pair Matching Techniques

K.SARANYA
II M.E
Computer science and Engineering
Vivekanandha College of Engineering for Women
Tamilnadu, India

Dr.C.SURESH GNANADHAS
Professor
Computer science and Engineering
Vivekanandha College of Engineering for Women
Tamilnadu, India

ABSTRACT: **The reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be losslessly recovered after embedded data is extracted while protecting the image content's confidentiality. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. A novel method called pixel pair matching which has the advantage of inserting the data without changing the image content, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility, ie. data extraction and image recovery are free of any error.**

The distortion caused by data embedding is called the embedding distortion. A good data-hiding method should be capable of evading visual and statistical detection while providing an adjustable payload. The LSB method employ one pixel as an embedding unit, and conceal data into the right-most LSBs.To achieve satisfactory hiding capacity Exploiting modification direction (EMD) and Diamond Encoding (DE) are two data-hiding methods proposed recently based on PPM. The maximum capacity of EMD is 1.161 bpp and DE extends the payload of EMD by embedding digits in a larger notational system. This method offers lower distortion than DE by providing more compact neighborhood sets and allowing embedded digits in any notational system.

Data-hiding method based on PPM.DE greatly enhances the payload of EMD while preserving acceptable stego image quality. The image preprocessing and binary operation of two pixels are scanned as an embedding unit and a specially designed neighborhood set is employed to embed message digits with a smallest notational system. PPM allows users to select digits in any notational system for data embedding, and thus achieves a better image quality.

Keywords: **Information hiding, Stego image, Attacks,Pixel Pair Matching(PPM).**

I. INTRODUCTION

Data hiding is a technique that conceals data into a carrier for conveying secret messages confidentially. The medium in which the message is embedded is referred as cover image and the resulting image and the message combined is referred as stego–image. Pixels of cover images will be modified after data embedding and also distortion occurs. The notion of distortion caused by data embedding is called the embedding distortion. In LSB embedding, the pixels with even values will be increased by one or more even it kept unmodified. The pixels with odd values will be decreased by one or more even it kept unmodified. LSB replacement is a well – known steganographic technique. In this embedded scheme, only LSB plane of the cover image is overwritten with the secret bit stream according to a pseudorandom number generator (PRNG). As a result, some structural asymmetry (never decreasing even pixels and increasing odd pixels when hiding the data) is introduced, and thus it is very easy to detect the existence of hidden message even at a low embedding rate using some reported steganalytic algorithms, such as the Chi-squared attack [1], regular/singular groups (RS) analysis[2], sample pair analysis [3], and the general framework for structural steganalysis [4]. Generally, the regions located at the sharper edges present more complicated statistical features and are highly dependent on the image contents. To reduce this problem, we propose an edge adaptive scheme and apply it to the LSBMR - based method, high-dimensional image models [5], amplitude of histogram local extrema [6], to improve efficiency LSB matching in image with high - frequency noise[7].Reversible Steganography scheme has the ability to embed the secret data into a host image and then recover the host image without losing any information when the secret data is extracted. This should be overcome by using some techniques. Reversible Steganography is also known as reversible data hiding. No modification is done in the digital representation of the cover image when reversible data hiding method is used. The

Reversible data hiding is used in the field of medical, military, legal applications etc.

II. PROPOSED SCHEME

The distortion caused by data embedding is called the embedding distortion. A good data-hiding method should be capable of evading visual and statistical detection while providing an adjustable payload. The LSB method employ one pixel as an embedding unit, and conceal data into the right-most LSBs.The least significant bit substitution method, referred to as LSB, is a well-known data-hiding method.To achieve satisfactory hiding capacity Exploiting modification direction (EMD) and diamond encoding (DE) are two data-hiding methods proposed recently based on PPM. The maximum capacity of EMD is 1.161 bpp and DE extends the payload of EMD by embedding digits in a larger notational system. This method offers lower distortion than DE by providing more compact neighborhood sets and allowing embedded digits in any notational system.

III. RELATED WORKS

OPAP effectively reduces the image distortion compared with the traditional LSB method. DE enhances the payload of EMD by embedding digits in a B-ary notational system. These two methods offer a high payload while preserving an acceptable stego image quality. In this section, OPAP and DE will be briefly reviewed.

A. Diamond Encoding (DE)

The EMD scheme embeds (2n + 1) B-ary digit into n cover pixels, but the diamond encoding scheme can conceal (2k2 + 2k + 1)B-ary digit into a cover pixel pair where k is the embedding parameter. The detail of this scheme is described as follows.

$f(x , y) = ((2k + 1) \times (x + y) mod\ (2k^2+2k+1)$
$K=2, (x , y)=(0,0)$
$f(x, y) = (5 \times x + y) mod(13)$
$f(0 , 0) = (5 \times 0 + 0) mod(13)=0$
$f(1 , 0) = (5 \times 1 + 0) mod(13)=5$
$f(2 , 0) = (5 \times 2 + 0) mod(13)=10$
$f(0 , 1) = (5 \times 0 + 1) mod(13)=1$
$f(0 , 2) = (5 \times 0 + 2) mod(13)=2$

.
.
.

$F(0 , -1) = (5 \times 0 + (-1)) mod(13)=12$

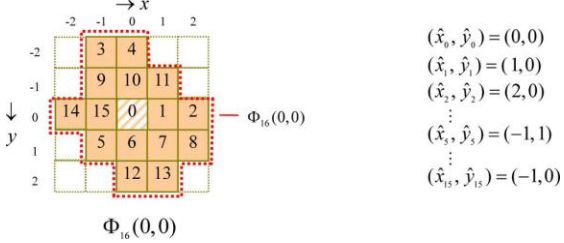

Fig. 1 Neighborhood set

B. Embedding System

Initially select the cover image in which secret information has to be enhanced. Once cover image is selected, it is processed.

The following steps are to be followed for embedding the secret information

- ✓ Select the cover image in which the secret information are to be embed
- ✓ Process the cover image
- ✓ Now select the Secret Information(i.e., Text File)
- ✓ Find the pixel co - efficient value and also find reference pixel to which the data is to be embedded.
- ✓ Embed the secret information using Least Significant Bit (LSB) embedding techniques.
- ✓ The error difference between the original coefficient value and the altered value by checking the right next bit to the modified LSBs can be minimized using the PPM algorithm.

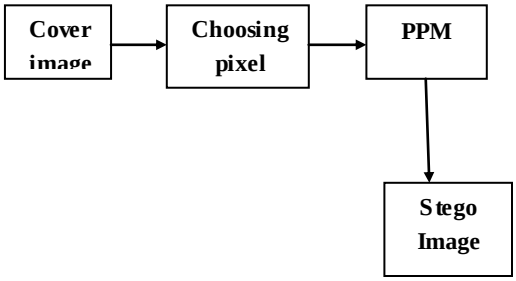

Fig2. Embedding Process

LSB and OPAP employ every pixel in the cover image as an embedding unit, and bits can be embedded into each pixel.Therefore, the payload is bpp. For the PPM-based embedding method, a payload with bpp is equivalent to embedding bits for every two pixels, which is equivalent to concealing digits ina B-ary notational system.

Fig. 3 Cover image and stego images under various payloads. (a) Cover image. (b) Stego image, 2 bpp at 46.86 dB. (c) Stego image, 3bpp at 40.97 dB. (d) Stegoimage, 4 bpp at 34.90 dB.

C Extraction System

The following steps are to be followed for extraction of the secret Information

- ✓ Take the stego image i.e., the image in which the secret data is embedded.
- ✓ Now using any of the extracting technique the secret information is extracted from the stego image.
- ✓ After extraction process, the secret information can be extracted from the cover image with the quality.

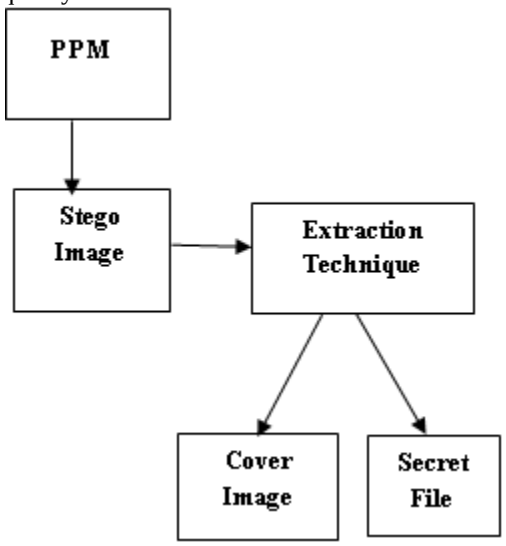

Fig4. Extraction Process

IV. PROCEDURE AND ALGORITHM

D. ADAPTIVE PIXEL PAIR MATCHING (APPM)

The basic idea of the PPM-based data-hiding method is to use pixel pair (x,y) as the coordinate and thorough a coordinate(x1,y1), surrounded by a predefined locality set φ(x,y) such that f(x,y)=Sb, where f is the drawing out function and Sb, is the message digit in a B-ary notational structure to be covered. Data embedding is done by replacing(x,y) with (x1,y1). For a PPM-based process, suppose a digit Sb is to be covered. The range of Sb is between 0 and B-1 , and a coordinate (x1,y1) € φ(x,y) has to be such that f(x1,y1)=Sb. Therefore, the range f(x , y) of must be integers between 0 and B-1, and each integer must occur at least once. In addition ,to reduce the distortion, the number of coordinates in φ(x,y) should be as small as possible.

The best PPM method shall satisfy the following three requirements:

1) There are exactly B coordinates in φ(x,y).
2) The values of extraction function in these coordinates are mutually exclusive.
3) The design of φ(x,y) and f(x,y) should be capable of embedding digits in any notational structure so that the best B can be selected to achieve junior embedding deformation.

V. EXPERIMENTS AND EVALUTION

E. Performance

*T*o evaluate the performance of the proposed scheme, a high definition image is taken. The simulation is run using MATLAB. First, LSB, DE, APPM are evaluated for Mean Square Error (MSE) with different payloads. Table 1 presents the obtained MSEs. It is observed that APPM out performs APPM, DE and LSB.

Table1. MSE Comparison

LSB	0.025431
DE	0.025431
APPM	0.114441
EAPPM	0.772456

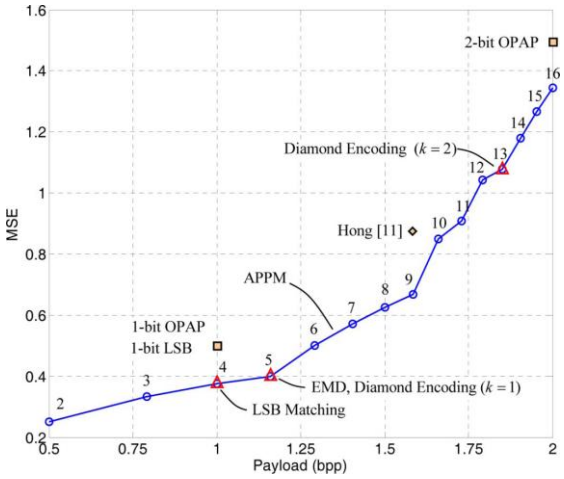

Fig.5 MSE comparison of various PPM-based methods.The payload-MSE relationship of APPM is denoted by circles. The B-ary digits used for a given payload are marked beside the circle.

VI. CONCLUSION

Proposed a simple and efficient data embedding process based on PPM. Two pixels are scanned as an embedding element and a specially designed neighbourhood set is employed to insert message digits with a smallest notational structure. APPM allows users to select digits in any notational structure for data embedding, and thus achieves a enhanced image quality. The proposed process not only resolves the low-payload trouble in EMD, but also offers smaller MSE compared with OPAP and DE. Moreover, because APPM produces no artifacts in stego images and the steganalysis results are comparable to those of the cover images, it offers a secure communication below variable embedding Capacity.

REFERENCES

[1] A.Westfeld and A. Pfitzmann, "Attacks on steganographic systems, "in *Proc. 3rd Int. Workshop on Information Hiding*, 1999, vol. 1768, pp. 61–76.

[2] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB Steganography in color, and gray-scale images," *IEEE Multimedia*, vol. 8, no. 4, pp. 22–28, Oct. 2001.

[3] S. Dumitrescu, X.Wu, and Z.Wang, "Detection of LSB Steganography via sample pair analysis," *IEEE Trans. Signal Process.*, vol. 51, no. 7, pp. 1995–2007, Jul. 2003.

[4] A. D. Ker, "A general framework for structural steganalysis of LSB replacement," in *Proc. 7th Int. Workshop on Information Hiding*, 2005, vol. 3427, pp. 296–311.

[5] A. D. Ker, "A fusion of maximum likelihood and structural steganalysis," in *Proc. 9th Int. Workshop on Information Hiding*, 2007, vol.4567, pp. 204–219.

[6] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*, 1st ed. Cambridge, U.K.: Cambridge Univ. Press,2009.

[7] G. Cancelli, G. Doerr, M. Barni, and I. Cox, "A comparative study of steganalyzers," in *Proc. IEEE Workshop Multimedia Signal Process.*, 2008, pp. 791–796.

[8] J. Zhang, I. Cox, and G. Doerr, "Steganalysis for LSB matching in images with high-frequency noise," in *Proc. IEEE Workshop Multimedia Signal Process.*, 2007, pp. 385–388.

[9] J. Fridrich, M. Goljan, and D. Soukal, "Wet paper codes with improved embedding efficiency," *IEEE Trans. Inf. Forensics Security*, vol. 1, no.1, pp. 102–110, Mar. 2006.

[10] C.-H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems,"*IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 488–497, Sep. 2008.

[11] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable Steganography," in *Information Hiding*. New York, NY, USA: Springer, 2010, vol. 6387, LNCS, pp. 161–177.

[12] G. Cancelli, G. Doerr, I. Cox, and M. Barni, "Detection of LSB Steganography based on the amplitude of histogram local extrema," in *Proc. IEEE Int. Conf. Image Process.*, 2008, pp. 1288–1291.

[13] 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.

[14] A. D. Ker, "Steganalysis of LSB matching in grayscale images," *IEEE Signal Process. Lett.*, vol. 12, no. 6, pp. 441–444, Jun. 2005.

