Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.23 – 36

RESEARCH ARTICLE

Adaptive Pixel Pair Matching Technique for Data Embedding

Nalimela Mounika[1], T. Madhavi Kumari[2]

[1]PG Scholar, Dept. Of Electronics & Communication, JNTU Kukatpally, Hyderabad, India
[2]Associate Professor and Coordinator, Academic & Planning, JNTUH, Hyderabad, India

[1] mounikanalimela5@gmail.com, [2] coordinator.dap.jntuh@gmail.com

Abstract — **This paper proposes a new data-hiding method based on pixel pair matching (PPM). The basic idea of PPM is to use the values of pixel pair as a reference coordinate. The PPM search a coordinate in the neighborhood set of this pixel pair according to a given message digit. The pixel pair is changed to the searched coordinate to conceal the digit. Exploiting modification direction (EMD) and diamond encoding (DE) are two data-hiding methods proposed recently based on PPM. The capacity of EMD is 1.161 bpp and DE prolongs the payload of EMD by embedding digits in a larger notational system. The designed method offers lower distortion than DE by providing more compact neighborhood sets and allowing embedded digits in any notational system. The proposed approach always has lower distortion for various payloads compare to optimal pixel adjustment process (OPAP) method. Experimental results reveal that the proposed method not only provides better performance than those of DE and OPAP, but also is secure under the detection of some well-known steganalysis techniques.**

Keywords—**Diamond encoding (DE); adaptive pixel pair matching (APPM); exploiting modification direction (EMD); least significant bit (LSB); optimal pixel adjustment process (OPAP); pixel pair matching (PPM).**

I. INTRODUCTION

Digital images are widely transmitted over the Internet and they often serve as a carrier for covert communication. Images are used for carrying data and termed as cover images and images with data embedded are termed as stego images. When embedding occurs, pixels of cover images will be modified and distortion occurs. The distortion occurred by data embedding is called the embedding distortion [3]. A good data-hiding method should be capable of evading visual and statistical detection [4] while providing an adjustable payload [5]. The least significant bit substitution method, indicated to as LSB, is a well- known data hiding method. This approach is easy to implement with low CPU cost, and had become one

© 2014, IJCSMC All Rights Reserved

of the popular embedding techniques. In LSB embedding, the pixels with even values will be increased by one or kept unmodified. The pixels with odd values will be reduced by one or kept unmodified. Since, the imbalanced embedding distortion emerges and is vulnerable to steganalysis [6], [7]. In 2004, Chan *et al.* [8] proposed a simple and efficient optimal pixel adjustment process (OPAP) method to reduce the distortion caused by LSB replacement. In their approach, if message bits are embedded into the right-most r LSBs of an m-bit pixel, other m-r bits are adjusted by a simple evaluation. Namely, if the regulated result offers a smaller distortion, these m-r bits are either replaced by the adjusted result or otherwise kept unmodified.

The LSB and OPAP methods employ one pixel as an embedding unit, and conceal information into the right most LSBs. Another group of data hiding methods employs two pixels as an embedding unit to conceal a message digit S_B in a B-ary notational system. We term these data hiding approach as pixel pair matching (PPM). In 2006, Mielikainen [9] proposed an LSB matching method based on PPM. It uses two pixels as an embedding unit. The LSB of the first pixel is represented for carrying one message bit, while a binary function is occupied to carry another bit. In Mielikainen's method, two bits are carried by two pixels. There is a 3/4 chance for pixel value has to be changed by one yet another 1/4 chance no pixel has to be modified. Accordingly, the MSE is $(3/4)\times(1_2/2)=0.375$ when payload is 1 bpp [9]. In contrast, the MSE obtained by LSB is 0.5. In the same year, Zhang and Wang [10] proposed an exploiting modification direction (EMD) approach. EMD improves Mielikainen's method in which only one pixel in a pixel pair is changed one gray-scale unit at most and a message digit in a 5-ary notational system can be embedded. Therefore, the payload is LSB matching and EMD methods greatly improve the traditional LSB method in which a better stego image quality can be achieved under the same pay-load. The maximum payloads of LSB matching and EMD are only 1 and 1.161 bpp, respectively. Hence, these two designs are not suitable for applications requiring high payload.
The embedding method of LSB matching and EMD offers no mechanism to increase the payload. The data-hiding method is based on Sudoku solutions to achieve a maximum payload of 121 to 9 bpp. The proposed a diamond encoding (DE) method to enhance the payload of EMD further. DE handles an extraction function to generate diamond characteristic values (DCV), and embedding is done by modifying the pixel pairs in the cover image according to their DCV's neighbourhood set and the given message digit. The EMD embedding procedure is then performed on each group by referencing a predefined selector and descriptor table. This approach 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 convenient combination of pixel groups the embedding efficiency is enhanced and also the visual quality of the stego image is enhanced.

Another group of rather practical data -hiding methods considers security as a guiding principle for developing a less detectable embedding scheme. These designs may either be implemented by avoiding embedding the message into the conspicuous part of the cover image, or by developing the embedding efficiency, that is, embed more messages per modification into the cover. The former can be achieved, for example, using "the selection channel" such as the wet paper code pro-posed. The latter can be done by en-coding the

© 2014, IJCSMC All Rights Reserved

message optimally with the smallest embedding impact using the near-optimal embedding schemes [4]. In these methods, the data bits were not conveyed by individual pixels but by groups of pixels and their positions.

This paper proposes a new data embedding method to reduce the embedding impact by providing a simple extraction function and a more compact neighborhood set. The proposed design embeds more messages per modification and thus in-creases the embedding efficiency. The image quality achieved by the proposed method not only performs better than those obtained by OPAP and DE, but also bears higher payload with less detectability. However, the best notational system for data concealing can be determined and employed in this new method according to the given payload so that a lower image distortion can be achieved.

II. 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 give a high payload while preserving an acceptable stego image quality. In this section, OPAP and DE will be shortly reviewed.

A. Optimal Pixel Adjustment Process (OPAP)

The OPAP method proposed by Chan *et al.* in 2004 greatly improved the image distortion problem resulting from LSB replacement. The OPAP method is detailed as follows [8], [18]. Suppose a pixel value is v, the value of the right-most r LSBs of v is $v_{(r)}$. Let v' be the pixel value after embedding r message bits using the LSB replacement method and s be the decimal value of these r message bits. OPAP employs the following equation to adjust v' so that the embedding distortion can be minimized

$$v'' = \begin{cases} v' + 2^r, & v^{(r)} - s > 2^{r-1} \text{ and } v' + 2^r \leq 255 \\ v' - 2^r, & v^{(r)} - s < -2^{r-1} \text{ and } v' - 2^r \geq 0 \\ v', & \text{otherwise} \end{cases}$$

B. Diamond Encoding

Diamond Encoding method is based on PPM. This approach conceals a secret digit in a B-ary notational system into two pixels, where $B = 2k^2 + 2k + 1$, $k \geq 1$. The payload of DE is $(1/2)\log(2k^2+2k+1)$ bpp. Note that when $k=1$, DE is equivalent to EMD in which both methods conceal digits in a 5-ary notational system. The DE method is briefly described as follows.

Let the size of m bits cover image be $M \times M$, message digits be s_B, where the subscript B represents s_B is in a B-ary notational system. First, the smallest integer k is determined to satisfy the following equation:

© 2014, IJCSMC All Rights Reserved

$$\left\lfloor \frac{M \times M}{2} \right\rfloor \geq |S_B|$$

where $|S_B|$ denotes the number of message digits in a B-ary notational system. To conceal a message digit s_B into pixel pair $(x\,y)$, the neighborhood set $\Phi(x\,y)$ is determined by

$$\Phi(x, y) = \{(a, b) \big| |a - x| + |b - y| \leq k\}$$

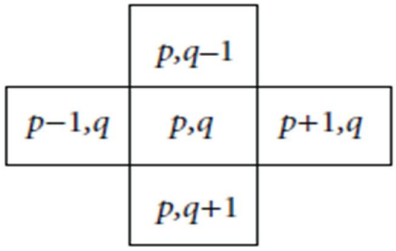
The DE method in detail can be explained as follows:

This method involves mainly two processes

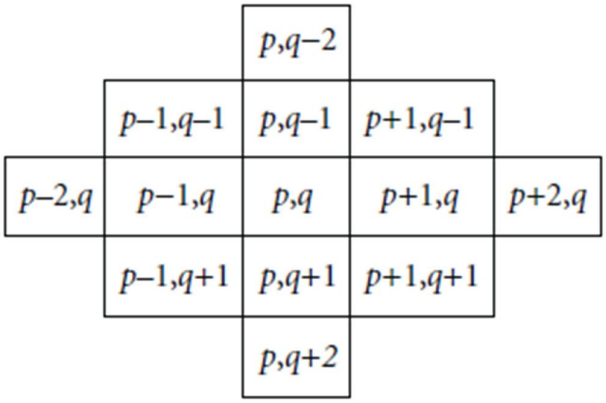
1. Data embedding method.
2. Data extraction method.

Firstly, the embedding parameter 'k' is determined and the diamond encoding with parameter 'k' can conceal secret data into the cover image.

In general DE patterns for different 'k' values can be seen as (a) k=1 and (b) k=2.



(a) $S_1(p, q)$



(b) $S_2(p, q)$

1. Data Embedding procedure

Step 1

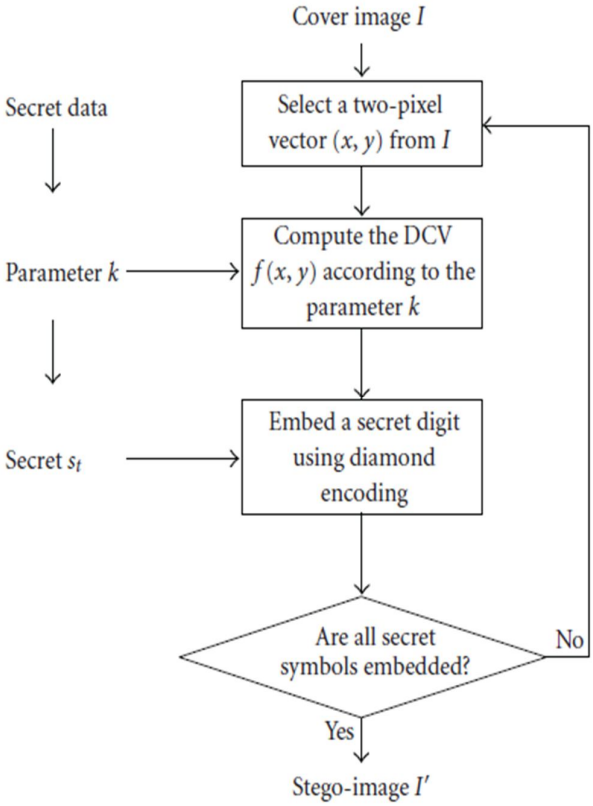
Firstly, according to the secret data size, embedding parameter 'k' value is selected.

Assuming that secret data size as 's' and then the embedding parameter k is determined by finding the minimal positive integer that satisfies the following inequality:

$$\left\lfloor \left(\frac{m \times n}{2} \right) \log_2 (2k^2 + 2k + 1) \right\rfloor \geq s.$$

© 2014, IJCSMC All Rights Reserved

Data embedding procedure:



Step 2

The original image is segmented into a number of non overlapping two pixel blocks. Then, select the each block from top-down and left-right in turn for data embedding process.

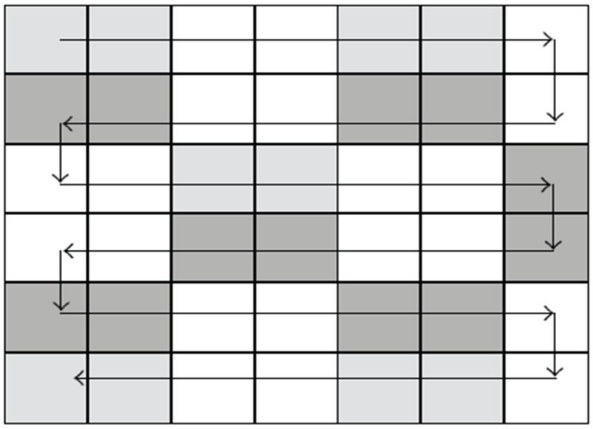
The block construction vector (x,y) is defined as

x = I(2t), y=I(2t+1)a nd cover image I sized m×n ,and t is block index

The embedded secret data bit stream is transformed into l-ary digit sequence. Moreover, the embedded secret digit is obtained from the index of the sequence of l-ary digits.

The sequence of non overlapping consecutive two-pixel blocks is constructed in a cover image is as shown:

© 2014, IJCSMC All Rights Reserved



Step 3

Obtain the DCV of two pixel values x and y by

$$f(x, y) = ((2k + 1)x + y) \bmod B$$

Step 5

The overflow or underflow problem of an stego pixel (x',y')ncan be handled by;

(1) if x'>255,x'=x'-l;

(2) if x'<0,x'=x'+l;

(3) if y'>255,y'=y'-l;

(4) if y'<0,y'=y'+l;

Repeat until all the secret data have been concealed. Then collect the all stego pixel values to form the stego-image I. The embedding parameter k has to transmit to the receiver in order to extract data.

2. Data Extraction procedure

The steps involving extracting the secret data from the stego-image I' and the detailed extraction can be explained as follows:

Step 1

Firstly, the stego image is segmented into a number of non overlapping two-pixel blocks(same as in embedding procedure).

The block vector (x',y') is defined as x'=I'(2t) and y'=I'(2t+1).

Step 2

According to the parameter k, set the embedding base $l=2k^2+2k+1$

For each stego pixel pair p' and q',the DCV of (x',y') is obtained from

$$F(x,y)=((2k+1)x'+y')\bmod l$$

and then secret digit is obtained by DCV of (x',y').

© 2014, IJCSMC All Rights Reserved

Step 3
Repeating the steps 1 and 2 by taking next pixel pair from stego image. This can be done until secret digits have been extracted for each block with index.

Step 4
Finally, the secret data can be computed by transforming the secret symbols to binary bits with base 2.

In Diamond Encoding the length of hidden messages decides the embedding parameter *k*. The parameter k plays a dominant role in deciding the payload and the stego-image quality for each image.
The payload

$$P = \frac{\left[\log_2(2k^2 + 2k + 1)\right]}{2}.$$

The MSE is the mean square error between the cover image and stego-image:

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \left[I(i,j) - I'(i,j) \right]^2$$

III. ADAPTIVE PIXEL PAIR MATCHING (APPM)

The proposed approach not only allows concealing digits in any notational system, but also provides the same or even smaller embedding distortion than DE for various payloads.

A. Extraction function and neighborhood set

It will propose an adaptive pixel pair matching (APPM) data-hiding method to explore better f(x,y) and φ(x,y) so that MSE is minimized.
The equation gives B
$(M \times M \times log_2 B)/2 \geq S_B$, B obtained
Data is then embedded by using PPM by using the f(x,y) and φ(x,y). Let

$F(x,y)=(x+c_B \times y) \bmod B$

The solution of f(x,y) and φ(x,y) is indeed a discrete optimization problem

$$\begin{aligned} \text{Minimize:} \quad & \sum_{i=0}^{B-1} (x_i - x)^2 + (y_i - y)^2 \\ \text{Subject to:} \quad & f(x_i, y_i) \in \{0, 1, \ldots, B-1\} \\ & f(x_i, y_i) \neq f(x_j, y_j), \quad \text{if } i \neq j \\ & \text{for } 0 \leq i, j \leq B-1. \end{aligned} \tag{1}$$

© 2014, IJCSMC All Rights Reserved

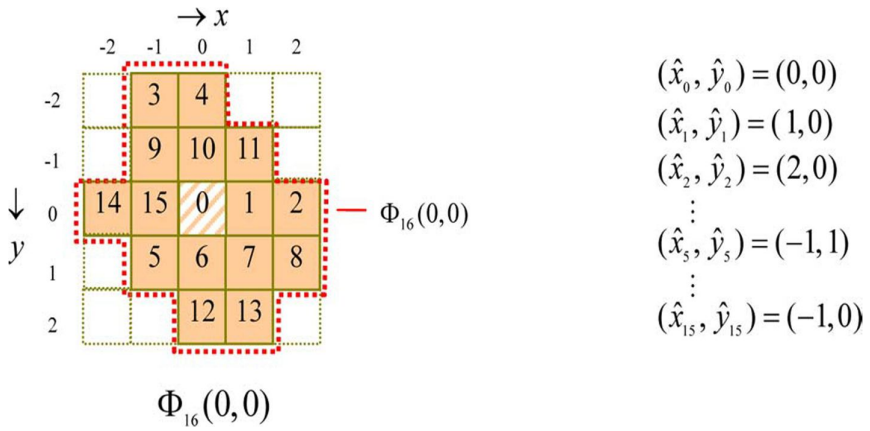


Fig. 1 Discrete Optimization

can be solved to obtain a constant c_B and B pairs of (x_i, y_i) are denoted by $\varphi_B(x,y)$ table1 gives c_B

Note that the four corners of the diamond shape may cause larger MSE but ours selects a more compact region for embedding ,and thus smaller distortion can be achieved.

From fig.2, Note that the four corners of the diamond shape may cause larger MSE but ours selects a more compact region for embedding ,and thus smaller distortion can be achieved.

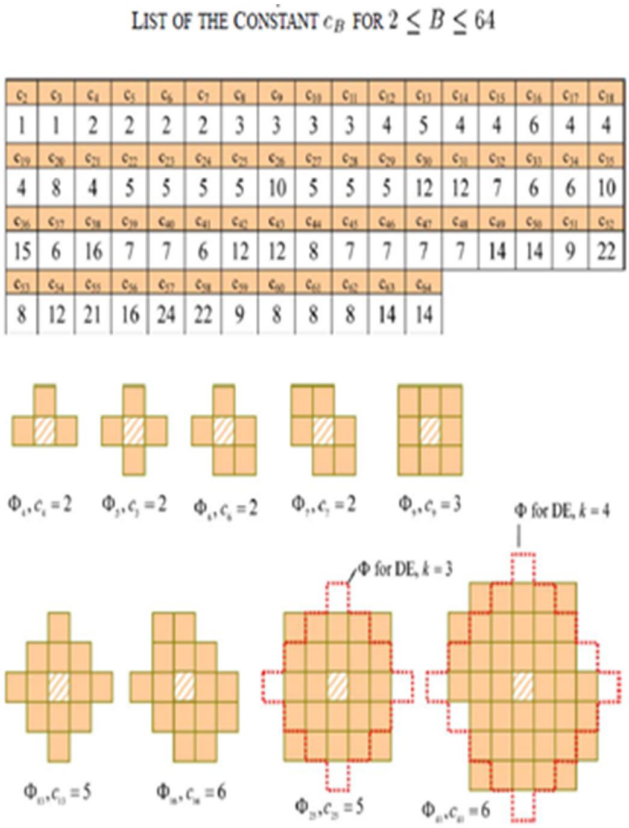


Fig. 2 Neighborhood set for (Shaded Region) for APPM

© 2014, IJCSMC All Rights Reserved

B. EMBEDDING PROCEDURE

The detailed procedure is

Input: Cover image of size M×M, secret bit stream S and key K
Output: Stego image I', C_B, $\varphi_B(x,y)$, and k.

1. Find the minimum B satisfying

$$\left\lfloor \frac{M \times M}{2} \right\rfloor \geq |S_B|$$

and convert the S into a list of digits with a B-ary notational system.

2. Solve the discrete optimization problem to find C_B and $\varphi_B(x,y)$.

3. Construct a non repeat random embedding sequence Q using key k.

C. **Extraction procedure**

The embedded information digits are the values of extraction function of the scanned pixel pairs.

Input: Stego image I', C_B, $\varphi_B(x,y)$, and k.
Output: Secret bit stream S.

1. Construct the embedding sequence Q using the key k .

2. Select two pixels (x', y') according to the embedding sequence Q.

3. Calculate f(x', y') the result is the embedded digit.

4. Repeat Steps 2 and 3 until all the message digits are extracted.

5. Finally, the message bits can be obtained by converting the extracted message digits into a binary bit stream.

We can say the MSE of APPM is smaller compared DE method by below equations

$$\mathrm{MSE}_{\mathrm{DE}} = \frac{1}{2B} \sum_{i=0}^{B-1} \left((x_i - x)^2 + (y_i - y)^2 \right)$$

$$\mathrm{MSE}_{\mathrm{DE}} = \frac{1}{2B} \sum_{i=0}^{B-1} \left((x_i - x)^2 + (y_i - y)^2 \right)$$

© 2014, IJCSMC All Rights Reserved

Smaller MSE indicates better image quality and from neighbourhood function of APPM we can say that it is a more compact and efficient data embedding method providing high payloads.

IV. RESULTS

RESULTS FOR APPM:

The corresponding cover images with stego images under various payloads

Fig. 3 Input Image

Fig. 4 Cover Image

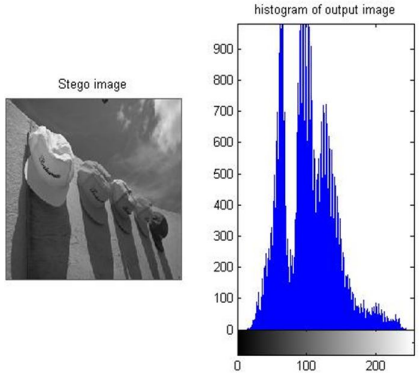


Fig. 5 APPM stego image for B=4 & embedding capacity 1bpp

© 2014, IJCSMC All Rights Reserved

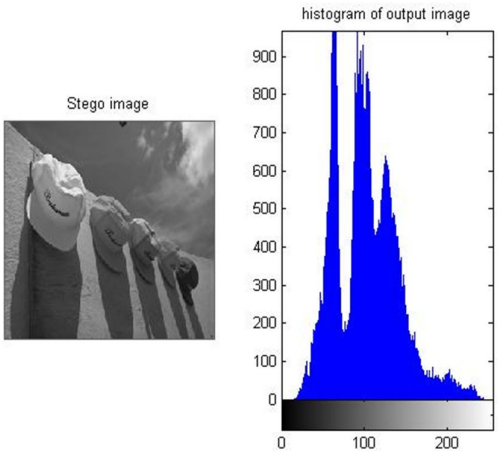


Fig. 6 APPM stego image for B=5 &embedding capacity 1.1610 bpp

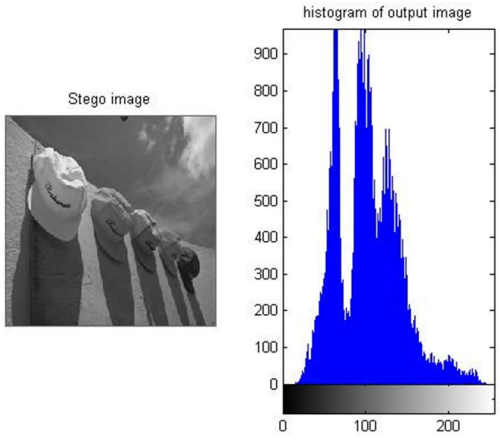


Fig. 7 APPM Stego image for B=6 &embedding capacity 1.2925 bpp

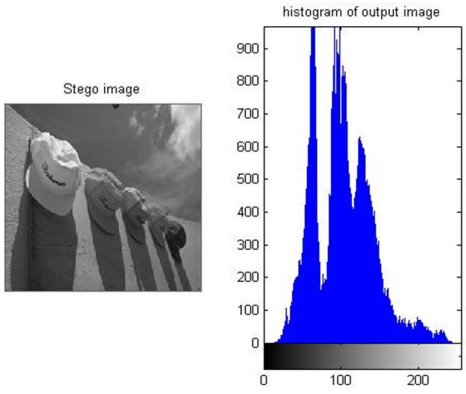


Fig. 8 APPM stego image for B=7 &embedding capacity 1.4039 bpp

© 2014, IJCSMC All Rights Reserved

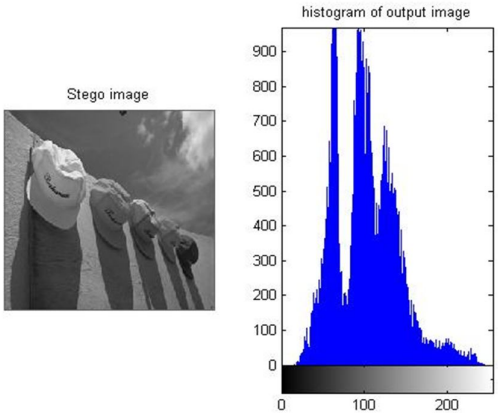


Fig. 9 APPM stego image for B=9 &embedding capacity 1.5850 bpp

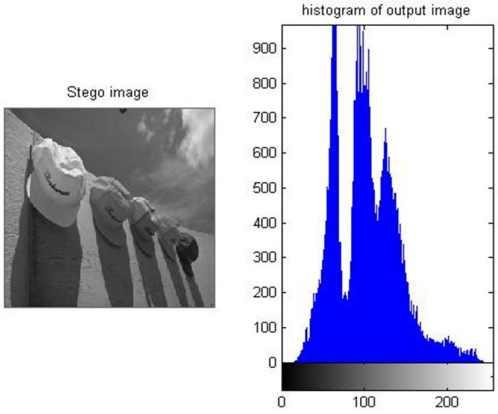


Fig. 10 APPM stego image for B=13 &embedding capacity 1.8502 bpp

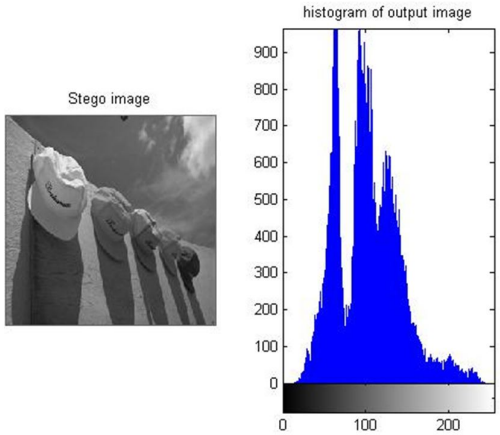


Fig. 11 APPM stego image for B=16 &embedding capacity 2 bpp

© 2014, IJCSMC All Rights Reserved

Graph between DE & APPM:

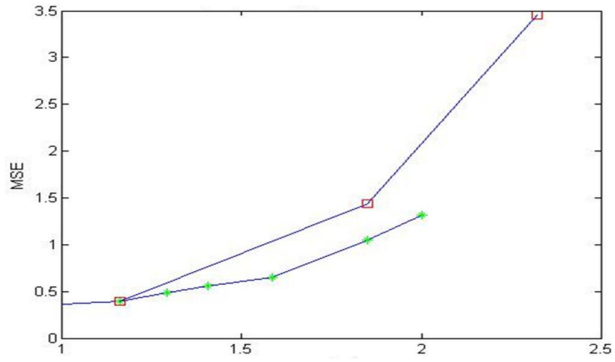


Fig. 12 Comparison between DE and AAPM

The above figures shows from Fig. 5 to Fig. 11 stego images for different B values with varying Embedding capacity

V. Security Analysis

The goal of steganography is to evade statistical detection. It shows that the MSE is not a good measure of security against the detection of steganalysis. For example, low-MSE embedding such as LSB replacement is known to be highly detectable [1], [6]. In this section, we analyze the security of APPM under two statistical steganalysis schemes, including Subtractive Pixel Adjacency Matrix (SPAM) steganalyzer proposed and the HVDH scheme proposed. SPAM steganalyzer is a novel Steganographic method for detecting stego images with low-amplitude independent stego signal, while the HVDH proposal is used to detect the presence of hiding message according to the distance between vertical and horizontal histograms. All the test images used in this section are obtained from the UCID and RSP image database, where some literature also adopts this database for their experiments.

VI. Conclusions

This dissertation proposed a simple and efficient data embedding method based on PPM. The 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. APPM allows users to pick digits in any notational system for data embedding, and thus attains a better image quality. The proposed approach not only resolves the low-payload problem in EMD, but also gives smaller MSE compared with OPAP and DE. Because of APPM produces no artifacts in stego images and the steganalysis results are similar to those of the cover images, it offers a secure communication under the adjustable embedding capacity.

- APPM is simple and efficient data embedding method compared to DE.
- APPM allows users to pick a digits in any notation system embedding.
- Offer small MSE compared with DE(&all previous methods).

© 2014, IJCSMC All Rights Reserved

REFERENCES

[1] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Process.*, vol. 90, pp. 727–752, 2010.

[2] 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.

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

[4] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *IEEE Security Privacy*, vol. 3, no. 3, pp. 32–44, May/Jun. 2003.

[5] 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.

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

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

[8] J. Fridrich, M.Goljan, and R.Du, "Reliable detection of LSB steganography in color and grayscale images," in *Proc. Int. Workshop on Multimedia and Security*, 2001, pp. 27–30.

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

[10] 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.

© 2014, IJCSMC All Rights Reserved