An Effective Data Embedding Technique Based on APPM in Transform Domain

Phaneendra Reddy GS
E.C.E. Department, University College of Engineering, JNTUK,
Kakinada, Andhra Pradesh, India.
phaneendra.gsp@gmail.com

***Abstract*—** This paper proposes an efficient data embedding technique based on adaptive pixel pair matching in transform domain. The basic principle of a Pixel Pair Matching (PPM) based data embedding technique is to use the values of a pixel pair as a reference coordinate and search a coordinate in the neighborhood set of that pixel pair according to given message digit. In order to conceal secret data the pixel pair is then replaced by the searched coordinate. In transform domain data embedding techniques, the image pixels are converted into transform domain by using a particular transform and then the secret data is embedded by using an efficient data embedding algorithm. In this paper the Haar transform is used. The proposed method not only offers lower embedding distortion but also more robust against various noise attacks. The experimental results shows that this method performs better when compared to the spatial domain technique.

***Keywords*-** Adaptive Pixel Pair Matching (APPM), Stego object, Diamond Encoding (DE), Embedding distortion**.**

*****

I. INTRODUCTION

Steganography is the art of hiding messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of message. The main aim of Steganography is to hide the fact that communication is taking place. Most commonly used carrier objects are digital images, videos, audio files etc. Among these, image Steganography is more popular since the digital images are widely transmitted over the internet. Images used for carrying data are termed as cover images and the images with data embedded are termed as stego images. The distortion in the carrier image caused by the embedding process is called as embedding distortion. A good data hiding method should be able to minimize the embedding distortion.

There are two popular data embedding schemes used in image Steganography: spatial domain embedding and transform domain embedding. In spatial domain data embedding, the secret data is directly embedded into the pixel values. In transform domain data embedding methods, the image pixels are first transformed by using some well known transformation techniques and then the data is embedded. But before transmission it must be converted back into spatial domain to ensure obscurity of embedded data.

II. LITERATURE REVIEW

The Least Significant Bit substitution method is a well-known data hiding method. This method is simple and easy to implement. In this method, the pixel values with even values will be increased by one or kept unmodified. The pixels with odd values will be decreased or kept unmodified. In 2004, Chan et al. [2] proposed Optimal Pixel Adjustment Process (OPAP) method to reduce the distortion caused by LSB substitution method. In this method, if message bits are embedded into 'r' LSBs of an 'm' bit pixel value then the remaining 'm-r' bits are adjusted by a simple evaluation. If the adjusted result offers a smaller distortion, these m-r bits are either replaced by the adjusted result or otherwise kept unmodified. These two methods employ one pixel as an embedding unit per each message digit.

The data embedding methods which employ two pixels as an embedding unit to conceal a message digit D_B in B-ary notational system are known as Pixel Pair Matching (PPM) based methods. In 2006, Zhang et al. [3] proposed an Exploiting Modification Direction (EMD) method. This method improved the stego image quality under the same payload. In the same year, Mielikainen [4] proposed an LSB matching method based on PPM. The LSB matching method and EMD methods greatly improved the stego image quality but unable to increase the payload. In 2009, Chao et al. [5] proposed a Diamond Encoding (DE) method to enhance the Payload of EMD method. DE employs an embedding function to generate Diamond Characteristic Values (DCV) and embedding is done by modifying the pixel pairs in the cover image according to the DCVs and the given message digit. This method conceals a secret digit in a B-ary notational system into a pixel pair, where $B = 2k^2 + 2k + 1, k \geq 1$. If $k = 2,\ B = 13,\ i.e.$ digits in 13-ary notational system are concealed. DE greatly enhances the payload of EMD while preserving acceptable stego image quality. But there are several problems associated with DE. Firstly, the payload of DE is determined by the notational system, which depends on embedding parameter k; therefore the notational system cannot be arbitrarily selected. For example, when k=1, 2 and 3, then the digits in 5-ary, 13-ary and 25-ary notational system are used to embed data respectively. DE never supports embedding digits in 4-ary or 16-ary notational system. But the best PPM based method should satisfy the following requirements: 1).There should be exactly B coordinates in neighborhood set, 2).The DCVs of these coordinates should be mutually exclusive, 3). The design of neighborhood set and extraction function should be capable of embedding digits in any notational system so that the best B can be selected to achieve lower embedding distortion. The DE method failed to meet the third requirement and also the neighborhood set in DE is defined by a diamond shape, which may lead to some unnecessary distortion. In 2012, Wien Hong et al. [1] proposed an efficient data embedding method based on Adaptive Pixel Pair Matching (APPM) in spatial domain. This method reduces the embedding distortion by providing a simple extraction function and more compact neighborhood set.

This paper proposes an efficient data embedding method based on adaptive pixel pair matching in transform domain. After applying the Haar transform to cover image, the data will be embedded into LH and HL bands. This method offers a

 ISSN: 2321-8169
3901 – 3905

lower embedding distortion and better stego image quality when compared to the spatial domain APPM, DE and OPAP methods. Since the embedding in done after applying the transformation, the secret data is highly immune to noise.

III. PROPOSED METHOD

The basic idea of the PPM based method is to use pixel pair (x, y) as reference coordinate and searching a coordinate (x', y') within the predefined neighborhood set $\varphi(x, y)$ such that $f(x', y') = S_B$, where f is the extraction function and S_B is the message digit in B-ary notational system to be concealed. Data embedding is done by replacing (x, y) with (x', y'). In transform domain data embedding methods, the transform will be applied to cover image and then the data will be embedded. The block diagram of proposed method is as shown below.

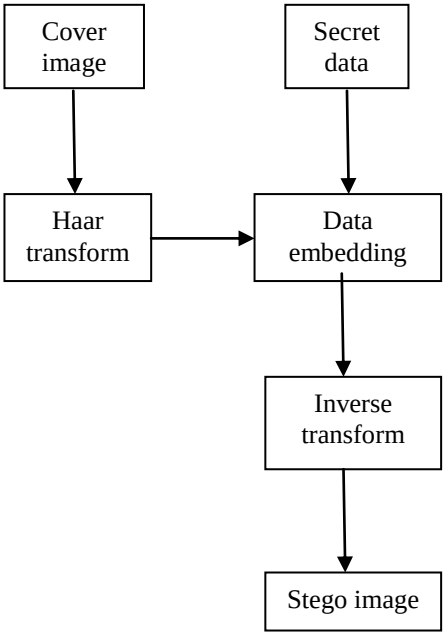

Fig. 1 Block diagram of the proposed method

A. *The Haar Transform*:

This is the simplest form of Discrete Wavelet Transform. A 2-D Haar transform generates four sub bands known as LL, LH, HL and HH. Haar wavelet operates on the input data by calculating the sums and differences of adjacent elements. This wavelet operates first on adjacent horizontal elements and then on adjacent vertical elements. The wavelet transform is considered to be more robust for multi-resolution analysis that has been widely used in most of the Steganography applications.

The low frequency sub-band LL preserves essential visual features for the original image and we can perform the second level DWT on it if multi-resolution representation is required. Since LL band is more sensitive to Human Visual System (HVS), it is not preferable to embed the data in that sub band. High frequency bands contain the information about the edges. So these are usually used for data embedding since the human eye is less sensitive to changes in the edges. The proposed method embeds the data into LH, HL and HH bands.

B. *Adaptive Pixel Pair Matching (APPM):*

In PPM based methods the definitions of neighborhood set and extraction function significantly affect the stego image quality. The designs of neighborhood set and extraction function have to fulfill the requirements: all values of $f(x, y)$ and $\varphi(x, y)$ have to be mutually exclusive and the summation of the squared distances between all coordinates in $\varphi(x, y)$ and (x, y) has to be the smallest.

The averaged Mean Square Error (MSE) can be obtained by averaging the summation of the squared distances between (x, y) and other coordinates of $\varphi(x, y)$, the expected MSE after embedding can be calculated by

$$MSE = \frac{1}{2B}\sum_{l=0}^{B-1}((x_l - x)^2 + (y_l - y)^2)$$

Let the extraction function be

$$f(x, y) = (x + C_B \times y) mod\ B$$

Where C_B is a constant value. The solution of $\varphi(x, y)$ and $f(x, y)$ is indeed a discrete optimization problem

$$Minimize: \sum_{l=0}^{B-1}((x_l - x)^2 + (y_l - y)^2)$$
$$Subject\ to: f(x_l, y_l) \in \{0,1,2,3, \dots, B-1\}$$
$$f(x_l, y_l) \neq f(x_j, y_j), if\ i \neq j$$
$$for\ 0 \leq i, j \leq B-1.$$

For an integer B and an integer pair (x, y), this can be solved to obtain a constant C_B and B pairs of (x_l, y_l). These B pairs forms the neighborhood set $\varphi_B(x, y)$. Table I lists the smallest values of C_B for different values of B.

TABLE I
VALUES OF CONSTANT C_B FOR $2 \leq B \leq 16$

C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9
1	1	2	2	2	2	3	3
C_{10}	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}	C_{16}	
3	3	4	5	4	4	6	

In APPM method, first we have to find out the minimum B satisfying $(M \times M \times log_2^B)/2 \geq |S_B|$. Now calculate constant C_B value by solving discrete optimization problem. Then define the neighborhood set φ_B such that the average of the summation of the squared distances between (x, y) and other coordinates of $\varphi(x, y)$ is minimum.

C. *Embedding Algorithm:*

Let $M \times M$ be the size of the cover image and S represents the message bits to be concealed and the size of S is represented as $|S|$. First we calculate minimum B such that all the message bits can be embedded. Then the message bits are concealed into pixel pairs by following the below algorithm.

1. Read the cover image and find out the size of the image $(M \times M)$.
2. Find the minimum B satisfying $(M \times M \times log_2^B)/2 \geq |S_B|$, where S_B is the secret data in B-ary notational system.
3. Solve the discrete optimization problem to find out the value of C_B and $\varphi_B(x, y)$.
4. Apply Haar transform to the cover image. It divides the image into four sub-bands LL, LH, HL and HH. In order to minimize the distortion LH, HL and HH bands are used for embedding data.
5. Find the characteristic values of all the coordinates in the neighborhood set by using extraction function

 ISSN: 2321-8169
3901 – 3905

6. To conceal a message digit S_B , Select a pixel pair from the selected band i.e. LH or HL or HH of transformed cover image and calculate modulus distance between S_B and $f(x,y)$

$$d = \big(S_B - f(x,y)\big) mod B$$

Then replace (x, y) with $(x + x_d, y + y_d)$.

7. Repeat step6 until all the message digits are embedded.

8. Find out the inverse Haar transform to obtain the stego image.

This embedding procedure can be illustrated with simple example. Let us suppose a cover image of size 512×512 with an embedding requirement of 500000 bits. The minimum B satisfying $(512 \times 512 \times log_2^B)/2 \geq 500000$ is 16. After applying the Haar transform the cover image will be divided into four sub images each of size 256×256. Hence both LH and HL sub images are used for embedding message bits. As the value of B is 16, C_{16} value is 6 and the neighborhood set $\varphi_{16}(0,0)$ can be obtained by solving discrete optimization problem. The neighborhood set $\varphi_{16}(0,0)$ and their characteristic values are shown in Fig. 2.

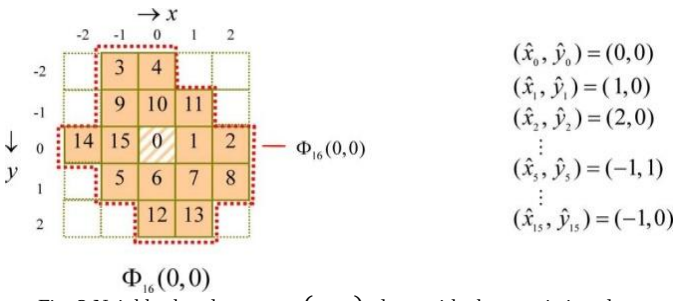

Fig. 2 Neighborhood set $\varphi_{16}(x,y)$ along with characteristic values

Suppose a secret digit 1_{16} in a 16-ary notational system is to be concealed into a coefficient pair (10,11) .Firstly, the modulus distance between 1_{16} and $f(10,11)$ is $d = (1 - 12)\ mod\ 16 = 5$ and $(x_5, y_5) = (-1,1)$; therefore, we replace (10,11) by (9,12) to conceal the digit 1_{16}.

D. Extraction Algorithm

To extract the embedded message digits, coefficient 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 coefficient pairs.

1. Read the stego image.
2. Apply DWT to stego image and record the coefficients
3. Select a coefficient pair (x', y') according to embedding sequence. The embedding sequence should be same as the one which is used during the embedding process
4. Calculate $f(x', y')$, the result obtained is the embedded digit.
5. Repeat steps 2 and 3 until all the message bits are extracted
6. Finally the message bits can be obtained by converting the extracted message digits into binary bit stream.

Let us consider that the scanned coefficient pair is $(x', y') = (9,12)$. The embedded digit in 16-ary notational system can be extracted by calculating the extraction function value for $x' = 9\ and\ y' = 12$ .Therefore $f(x', y') = (9 + 6 \times 12) mod\ 16 = 1$.Hence the embedded digit is 1_{16}.

IV. Prepare Your Paper Before Styling

A. Peak Signal to Noise Ratio (PSNR):

The peak signal-to-noise ratio is an expression for the ratio between maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. As many signals have wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

It is defined as follows:

$$PSNR = 10 \times \log_{10}\left(\frac{255^2}{MSE}\right)$$

Where MSE is the Mean Square Error between the cover image and stego image and it is computed by averaging the squared intensity differences of distorted and reference image pixels.

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

Where $I(i,j)$ and $I'(i,j)$ represents the pixel values of the original cover image and stego image in the position (i,j) respectively, *m* and *n* represents number of rows and columns respectively.

B. Payload:

Payload refers to the amount of information that can be hidden in the cover image. It always depends on the size of the cover image. If the payload is high then the embedding distortion will be high and hence the stego image quality is poor. The main objective of a good data hiding technique is to reduce the distortion in the cover image caused by the embedding process while accommodating the given payload.

C. SSIM:

The Structural Similarity Index is a method for measuring the similarity between two images. The SSIM index is a full reference metric; in other words, the measuring of image quality is based on an initial uncompressed or distortion-free image as reference. The SSIM is designed to improve on traditional methods like peak signal to noise ratio (PSNR) and mean squared error (MSE), which have proven to be inconsistent with human eye perception.

The SSIM metric is calculated on various windows of an image. The measure between two windows x and y of common size $N \times N$ is:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

Where μ_x = the average of x,

μ_y = the average of y,

σ_x^2 = the variance of x,

σ_y^2 = the variance of y,

σ_{xy} = the covariance of x and y,

C_1 and C_2 are two variables to stabilize the division with weak denominator, where $C_1 = (k_1 L)^2$ and $C_2 = (k_2 L)^2$,

L = the dynamic range of pixel values,

$k_1 = 0.01$ and $k_2 = 0.03$ by default.

The resultant SSIM index is a decimal value between -1 and 1, and value 1 is only reachable in the case of two identical sets of data.

ISSN: 2321-8169
3901 – 3905

V. EXPERIMENTAL RESULTS

The LSB Substitution method, OPAP method, DE method and APPM methods are implemented in MATLAB. Four images Lena, Boat, Elaine and House, each sized 512×512, are taken as test images to compare the PSNR ,SSIM obtained by these methods.The payloads were set to 400000, 650000 and 1000000 bits per consecutive experiments respectively.

Table 2 PSNR comparison under the payload of 400000 bits

Image	LSB Substitution (2 bit)	OPAP (2 bit)	Diamond Encoding (k=2)	APPM (C_9=3)
lena	45.325	47.531	48.637	49.890
elaine	45.321	47.554	48.642	49.896
boat	45.199	47.542	48.632	49.916
house	45.313	47.546	48.647	49.922

Table 3 PSNR comparison under the payload of 650000 bits

Image	LSB Substitution	OPAP (3 bit)	Diamond Encoding (k=3)	APPM (C_{32}=7)
lena	38.742	41.554	43.122	43.986
elaine	38.702	41.543	43.118	43.988
boat	38.739	41.283	43.127	43.961
house	38.741	41.573	43.127	43.999

Table 4 PSNR comparison under the payload of 1000000 bits

Image	LSB Substitution (4 bit)	OPAP (4 bit)	Diamond Encoding (k=10)	APPM (C_{199}=37)
lena	31.992	35.001	35.607	36.043
elaine	32.079	35.012	35.527	36.051
boat	32.042	35.054	35.273	36.047
house	32.092	35.016	35.548	36.055

Table 5 PSNR comparison under payload of 400000 bits

Image	Spatial domain APPM	Transform domain APPM
Lena	49.890	57.176
Elaine	49.896	57.242
Boat	49.916	56.931
House	49.922	57.124

Table 6 PSNR comparison under the payload of 650000 bits

Image	Spatial domain APPM	Transform domain APPM
Lena	43.986	50.287
Elaine	43.988	50.258
Boat	43.961	50.194
House	43.999	50.110

Table 7 PSNR comparison under the payload of 1000000 bits

Image	APPM(spatial)	APPM(transform)
Lena	36.043	44.072
Elaine	36.051	44.295
Boat	36.047	44.949
House	36.055	44.225

Table 8 SSIM comparison under the payload of 400000 bits

Image	LSB Substitution	OPAP	DE	APPM (spatial)	APPM (transform)
Lena	0.642	0.727	0.791	0.801	0.916
Elaine	0.641	0.729	0.793	0.803	0.918
Boat	0.631	0.728	0.791	0.805	0.913
House	0.637	0.726	0.794	0.806	0.916

Table 9 SSIM comparison under the payload of 650000 bits

Image	LSB Substitution	OPAP	DE	APPM spatial	APPM (transform)
Lena	0.398	0.489	0.507	0.547	0.851
Elaine	0.401	0.478	0.499	0.543	0.846
Boat	0.397	0.484	0.506	0.537	0.841
House	0.391	0.491	0.510	0.551	0.842

Table 10 SSIM comparison under the payload of 1000000 bits

Image	LSB Substitution	OPAP	DE	APPM (spatial)	APPM (transform)
Lena	0.157	0.221	0.279	0.317	0.598
Elaine	0.163	0.232	0.283	0.309	0.603
Boat	0.159	0.241	0.271	0.320	0.591
House	0.152	0.218	0.278	0.315	0.602

Figure 1. Example of a ONE-COLUMN figure caption.

VI. CONCLUSION

Experimental results reveal that the proposed method performs better than the existing methods. In this method, a pair of transform coefficients is scanned as an embedding unit and a specially designed neighborhood set is employed to embed message digits with a smallest possible notational system. This method allows the users to select digits any notational system for data embedding and thus achieves better stego image quality when compared to existing methods. This method offers a better payload when compared to LSB substitution method, OPAP method since the secret digits are embedded in larger notational systems. The proposed method offers smaller embedding distortion than the OPAP and DE methods because of more compact neighborhood sets and also because of allowing embedding digits in any notational system.

REFERENCES

[1] 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.

[2] 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.

[3] X. Zhang , S. Wang, "Efficient steganographic embedding by exploiting modification direction," IEEE Communication Letters, vol. 10, no. 11,pp. 781–783, Nov. 2006.

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

[5] 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.

[6] 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, February 2012.

[7] 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.

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

[9] 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.

[10] A. D. Ker, "Steganalysis of LSB matching in gray scale images," IEEE Signal Process. Letters, vol. 12, no. 6, pp. 441–444, Jun. 2005.

[11] J. Fridrich and T. Filler, "Practical methods for minimizing embedding impact in Steganography," in Proc. SPIE, Security, Steganography, Watermarking of Multimedia, 2007, vol. 6050, pp. 2–3

[12] C. H. Yang, "Inverted pattern approach to improve image quality of information hiding by LSB substitution," Pattern Recognit., vol.41, no. 8, pp. 2674–2683, 2008.

[13] J. Fridrich and D. Soukal, "*Matrix embedding for large payloads*", IEEE Transactions on Information Forensics Security, vol. 1, no. 3, pp. 390–394, Sep.2006.

[14] L. M. Marvel, C. G. Boncelet Jr., and C. T. Retter, "*Spread spectrum image Steganography*," IEEE Transactions on Image Processing, vol. 8, no. 8, pp. 1075–1083, 1999.

[15] X. Zhang and S. Wang, "*Steganography using multiple-base notational system and human vision sensitivity*," IEEE Signal Processing Letters, vol. 12, no. 1, pp. 67–70, 2005.