M.Lakshmi Prasanna, Mr. Sk.Mahaboob Basha / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 3, May-Jun 2013, pp.1484-1490

Extended Adaptive Pixel Pair Matching

M.Lakshmi Prasanna[1], Mr. Sk.Mahaboob Basha[2]
Department of Electronics and Communication Engineering, SreeVidyanikethan Engineering College, TIRUPATI

Abstract:

Steganography is a method of hiding secret messages into a cover-media such that an unintended observer will not be aware of the existence of the hidden messages. The carrier of steganography can be various kinds of digital media such as image, audio, and video, etc. Digital images are widely transmitted over the Internet; therefore, they often serve as a carrier for covert communication. A good data-hiding method should be capable of evading visual and statistical detection while providing an adjustable payload. In [1], authors proposed Adaptive Pixel Pair Matching (APPM). The basic idea of Pixel Pair Matching (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. APPM allows users to select digits in any notational system for data embedding, and thus achieves a better image quality. APPM not only resolves the low-payload problem 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 similar to those of the cover images, it offers a secure communication under adjustable embedding capacity. This paper proposes an extension to APPM, for high definition color images. EAPPM provides high data capacity without compromising on performance and security of APPM.

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

I. Introduction

The purpose of steganography is to send secret messages after embedding them into public digital multimedia. It is desired to embed as many messages as possible per change of the cover-object. In general, for given messages and covers, the steganography that introduces fewer embedding changes will be less detectable, i.e., more secure. Two fields of research have been proposed to enhance the communication security: cryptography and information hiding. Although they are both applied to the protection of secret message, the major difference is the appearance of the transmitted data. The cryptography methods, such as DES and RSA, referred almost exclusively to encryption which is the process of converting ordinary information (plaintext) into unintelligible gibberish (cipher-text). After data encryption, the secret data appears to be a total chaos of seemingly meaningless bits. However, the existence of the transmitted secret message can be detected. Because it does not conceal the fact that there is an important message, the encrypted message could motivate an unauthorized user to decrypt or destroy it.

Many approaches of information hiding have been proposed for different applications, such as copyright protection, secret transmission, tampering detection, and image authentication. The most well-known data hiding scheme is the least significant bits (LSBs) substitution method. This method embeds fixed-length secret bits into the least significant bits of pixels by directly replacing the LSBs of cover image with the secret message bits.

Although this method is simple, it generally effects noticeable distortion when the number of embedded bits for each pixel exceeds three. Several methods have been proposed to reduce the distortion induced by LSBs substitution. Another way of improving LSBs scheme is to reduce the amount of alterations necessary to be introduced into the cover image for data hiding when the number of secret bits is significantly less than that of available cover pixels. The method proposed by Tseng et al. [15] can conceal as many as $log_2(mn+1)$ bits of data in a binary image block sized m X n by changing, at most, two bits in the block. Matrix encoding, on the other hand, uses less than one change of the least significant bit in average to embed w bits into $2^w - 1$ cover pixels.

Diamond Encoding(DE)method is the extension of the exploiting modification direction (EMD) embedding scheme [2]. The main idea of the EMD embedding scheme is that each $(2n+1)$-ary notational secret digit is carried by n cover pixels, and only one pixel value increases or decreases by 1 at most. For each block of n cover pixels, there are $2n$ possible states of only one pixel value plus 1 or minus 1. The $2n$ states of alteration plus the case in which no pixel is modified form $(2n + 1)$ different cases. Therefore, the $(2n + 1)$-ary notational secret digit is embedded into the cover pixels by changing the state. Before the data embedding procedure, the pre-process can convert the secret data into sequences of digits with $(2n + 1)$-ary notational representation.

The basic idea of the PPM-based data-hiding method is to use pixel pair *(x, y)* as the coordinate, and searching a coordinate *(x', y')* within a predefined neighborhood set Ø(x, y) such that $f(x', y') = S_B$, where *f* is the extraction function and S_B is the message digit in a -ary notational system to be concealed. Data embedding is done by replacing *(x, y)* with *(x', y')*.

The rest of the paper is organized as follows: Section 2 gives the Literature review on the present work, Section 3 explains the proposed EAPPM with Section 4 presenting the Performance and Security analysis of proposed methods. Section 5 concludes the paper.

II. Literature Review

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. The OPAP method proposed by Chan *et al.* in 2004 greatly improved the image distortion problem resulting from LSB replacement.

2.1 LSB substitution

Let C be the original 8-bit grayscale cover-image of $M_c \times N_c$ pixels represented as

$$C = \{x_{ij} | 0 \le i < M_c, 0 \le j < N_c, \quad x_{ij} \in \{0,1,\dots,255\}$$

M be the n-bit secret message represented as

$$M = \{m_i | 0 \le i < n, m \in \{0,1\}\}$$

Suppose that the n-bit secret message M is to be embedded into the *k*-rightmost LSBs of the cover-image *C*. Firstly, the secret message *M* is rearranged to form a conceptually *k*-bit virtual image *M'* represented as

$$M' = \{m_i' | 0 \le i < n', \quad m_i' \in \{0,1,\dots,2^k - 1\}\}$$

where $n' < M_c \times N_c$. The mapping between the n-bit secret message $M = \{m_i\}$ and the embedded message $M' = \{m_i'\}$ can be defined as follows:

$$m_i' = \sum_{j=0}^{k-1} m_{i \times j \times k} \times 2^{k-1-j}$$

Secondly, a subset of *n'* pixels $\{x_{l1}, x_{l2},..,x_{ln'}\}$ is chosen from the cover-image *C* in a predefined sequence. The embedding process is completed by replacing the $_k$ LSBs of x_{li} by m_i'. Mathematically, the pixel value xli of the chosen pixel for storing the *k*-bit message m_i' is modified to form the stego-pixel x_{li}' as follows:

$$x_{li}' = x_{li}' - x_{li}' mod\ 2^k + m_i'$$

In the extraction process, given the stego-image *S*, the embedded messages can be readily extracted without referring to the original cover-image[3]. Using the same sequence as in the embedding process, the set of pixels $\{x_{l1}, x_{l2},..,x_{ln'}\}$ storing the secret message bits are selected from the stego-image. The *k* LSBs of the selected pixels are extracted and lined up to reconstruct the secret message bits. Mathematically, the embedded message bits m_i' can be recovered by

$$m_i' = x_i' mod\ 2^k$$

2.2 Diamond Encoding (DE)

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

Assume that a, b, p, and q are pixel values, and k is a positive integer. The neighborhood set S_k (p, q) represents the set that contains all the vectors (a, b) with the distance to vector (p, q) smaller than k, and S_k(p, q) is defined as the following form:

$$f(p,q) = \big((2k+1) \times p + q\big) mod\ l$$

Let the absolute value |Sk| denote the number of elements of the set Sk, and each member in Skis called neighboring vector of (p, q). We calculate the value of |Sk| to obtain the embedding base and embedded base with a parameter k. Diamond encoding method uses a diamond function f to compute the diamond characteristic value (DCV) in embedding and extraction procedures. The DCV of two pixel values p and q can be defined as follows:

$$S_k(p,q) = \{(a,b) || p-a| + |q-b| \le k$$

where *l* is the absolute value of Sk. The DCV have two important properties: the DCV of the vector (p, q) is the member of S_k belongs to {0, 1, 2, . . ,l-1}and any two DCVs of vectors in S_k(p, q) are distinct. Assume that E_k represents the embedded digit and E_k belongs to{0, 1, 2, . . . ,l − 1}. For secret data embedding, we replace the DCV of the vector (p, q) with the embedded secret digit. Therefore, the modulus distance between f (p, q) and S_k is d_k= f (p, q)−E_k mod *l*. For each k, we can design a distance pattern D_k to search which neighboring pixel owns the modulus distance d_k. Then, the vector (p, q) is replaced with the neighboring vector (p', q') by dk. The vector (p', q') is the member of S_k(p, q) and the DCV of (p', q') equals to the embedded secret digit E_k. The vector (p', q') can extract the correct secret digit by

$$f(p',q') = \big((2k+1) \times (p'+q')\big) mod\ l$$

The diamond encoding scheme promises that the distortion of vector (p, q) is no more than k after embedding a secret digit Ek. Therefore, this minimal distortion scheme can be employed to embed large amount of data.

2.3 Adaptive Pixel Pair Matching

The basic idea of the PPM-based data-hiding method is to use pixel pair (x, y) as the coordinate, and

searching a coordinate (x',y') within a predefined neighborhood set Ø(x, y) such that $f(x', y') = S_B$, where f is the extraction function and S_B is the message digit in a B-ary notational system to be concealed. Data embedding is done by replacing (x, y) with (x', y') [1].

Suppose the cover image is of size $M \times M$, $S$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. Then, message digits are sequentially concealed into pairs of pixels. First minimum B satisfying $|M \times M / 2| \geq |S_B|$, and convert S into a list of digits with a B-ary notational system S_B. The discrete optimization problem is solved to find c_B and $Ø_B(x,y)$. In the region defined by $Ø_B$(x, y), record the coordinate (x', y') such that f(x', y') = i, $0 \leq i \leq B-1$.

Construct a nonrepeating random embedding sequence Q using a key K_r. To embed a message digit s_B, two pixels (x, y) in the cover image are selected according to the embedding sequence Q, and calculate the modulus distance

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

between s_B and f(x, y), then replace (x, y) with (x + x', y+y').

III. Proposed Methodology

As APPM is proved to offer better security against detection and lower distortion, we take forward APPM for colored images. We propose to explore a better mechanism and provide better security and lower distortion for embedding data in colored images. Also, performance in terms of payload can be improved. In colored images, which consists three different colored layers, in each layer one can embed message bits so that the capacity of the Adaptive Pixel Pair Matching can be improved without any distortion in the original colored image.

The R, G, B layers are separated and the each is considered as a gray image, referred as Channel Image. For a PPM-based method, suppose a digit s_B is to be concealed. The range of s_B is between 0 and B-1, and a coordinate (x', y') in Ø(x, y) has to be found such that f(x',y') = s_B. Therefore, the range of (x ,y) 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 Ø(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 Ø(x, y).

2) The values of extraction function in these coordinates are mutually exclusive.

3) The design of Ø(x, y)and f(x, y) should be capable of embedding digits in any notational system so that the best can be selected to achieve lower embedding distortion.

The definitions of Ø(x, y) and f(x, y) significantly affect the stego image quality. The designs of Ø(x, y)and f(x, y) have to fulfill the requirements: all values of in have to be mutually exclusive and the summation of the squared distances between all coordinates in Ø(x, y) and f(x, y) has to be the smallest. This is because, during embedding, (x, y) is replaced by one of the coordinates in Ø(x, y). Suppose there are B coordinates in Ø(x, y), i.e., digits in a B-ary notational system are to be concealed, and the probability of replacing (x, y) by one of the coordinates in Ø(x, y) is equivalent. The averaged MSE can be obtained by averaging the summation of the squared distance between and other coordinates in Ø(x, y). Thus, given a Ø(x, y), the expected MSE after embedding can be calculated by

$$MSE_{\emptyset(x,y)} = \frac{1}{2}\sum_{i=0}^{B-1}((x_i - x)^2 + (y_i - y)^2)$$

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

$$minimize: \sum_{i=0}^{B-1}((x_i - x)^2 + (y_i - y)^2)$$

$$subject\ to: \ f(x_i, y_i) \in \{0,1,\dots,B-1\}$$

$$f(x_i, y_i) \neq f(x_j, y_j), \quad if\ i \neq j$$

for $0 \leq i, j \leq$ B-1.

Embedding Procedure:

Consider the cover image is of size $M \times M$, then each of R, G, B channels will be of size $M \times M$. S is the message bits to be concealed for each channel image and the size of S is $|S|$. First we calculate the minimum B such that all the message bits can be embedded. Then, message digits are sequentially concealed into pairs of pixels.

1. First minimum B satisfying $|M \times M / 2| \geq |S_B|$, and convert S into a list of digits with a B-ary notational system S_B.
2. The discrete optimization problem is solved to find c_B and $Ø_B(x, y)$.
3. In the region defined by ØB(x, y), record the coordinate (x', y') such that f(x', y') = i, $0 \leq i \leq B-1$.
4. Construct a nonrepeating random embedding sequence Q using a key K_r.
5. To embed a message digit s_B, two pixels (x, y) in the cover image are selected according to the embedding sequence Q, and calculate the modulus distance

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

between $_{sB}$ and f(x, y), then replace (x, y) with (x + x', y + y').

6. Repeat step 5, until all the message bits are embedded.

To avoid any distortion because of replacing pixels right under each other in different layers, the regions Ø(x, y) for each layer are taken as distinct subsets.

Say the regions for red channel image be $Ø_{Br}$, green channel image be $Ø_{Bg}$ and blue channel image be $Ø_{Bb}$ $Ø_{Br}$, $Ø_{Bg}$ and $Ø_{Bb}$ are selected such that

$$Ø_{Br} \not\subset Ø_{Bg} \not\subset Ø_{Bb}$$

As the three are taken as distinct sets, the clash of getting pixel pair at the same positions is avoided. The three layers are merged again to retain original image.

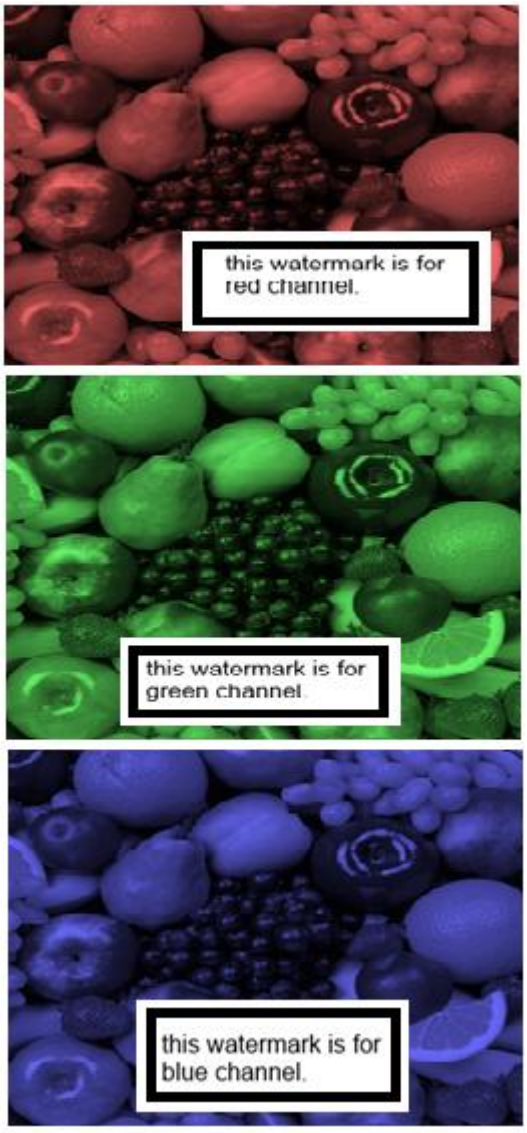

Figure 1. Embedding respective watermarks for different Channel Images

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.

1. The watermarked image is split into respective R, G, B layers and each is considered as a Channel Image.
2. Construct the embedding sequence Q using a 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 can be obtained by converting the extracted message digits into a binary bit stream.

Theoretical Analysis:

Image distortion occurs when data are embedded because pixel values are modified. MSE is used to measure the image quality.

$$MSE = \frac{1}{M \times M} \sum_{i=0}^{M} \sum_{j=0}^{M} (p_{i,j} - p'_{i,j})^2$$

where $M \times M$ denotes the image size, $p_{i,j}$ and $p'_{i,j}$ denote the pixel values of the original image and the stego image, respectively.MSE represents the mean square error between the cover image and stego image. A smaller MSE indicates that the stego image has better image quality.

When data are embedded using LSBs of each pixel, each bit valued 0 or 1 has equal probability. The squared error caused by embedding a bit in the *i*th LSB is $(1/2)(2^{i-1})^2$; therefore, the averaged MSE of embedding LSBs is given by

$$MSE_{LSB} = \frac{1}{2} \sum_{i=1}^{r} (2^{i-1})^2 = \frac{1}{6} (4^r - 1)$$

Let the original pixel value be *v* and the stego pixel value be *v'*. The probability of $|v - v'| = 0$ or $|v - v'| = 2^{r-1}$is $1/2^r$; the probability of $|v - v'|$ to be within the range $[1, 2^{r-1}-1]$is $1/2^r$. Therefore, the averaged MSE caused by embedding *r* bits is

$$MSE_{opap} = \frac{1}{2^r}(2^{r-1})^2 + \frac{1}{2^{r-1}} \sum_{i=1}^{2^{r-1}-1} (i)^2 = \frac{1}{12} (4^r + 2)$$

For the DE method, assume that the probability of selecting a coordinate (x_i, y_i) in the diamond shape $Ø(x, y)$ to replace a pixel pair (x, y) is the same. Therefore, the averaged MSE caused by embedding digits in a B-ary notational system is

$$MSE_{DE} = \frac{1}{2B} \sum_{i=1}^{B-1} ((x_i - x)^2 + (y_i - y)^2) = \frac{k(k+1)(k^2+k+1)}{3 + 6k(k+1)}$$

Where *k* is the embedding parameters of DE.

For embedding digits in a B-ary notational system using APPM, assume that the probability of replacing (x, y) with each (x', y') in Ø(x, y) is identical. With the knowledge of Ø(x, y) , the averaged MSE can be obtained by

$$MSE_{APPM} = \frac{1}{2B}\sum_{i=0}^{B-1}((x_i - x)^2 + (y_i - y)^2)$$

For EAPPM,

$$MSE_{EAPPM} = \frac{1}{3B}\sum_{i=0}^{B-1}((x_i - x)^2 + (y_i - y)^2)$$

Consider common MSE *M*, for all the above said techniques.

The maximum supported payload for LSB can be calculated from

$$r_{lsb} = log_4((M \times 6) + 1)$$

For DE, the maximum supported payload can be calculated as

$$r_{de} = log_4((M \times 12) - 2)$$

For the PPM-based embedding method, a payload with *r* bpp is equivalent to embedding*2r* bits for every two pixels, which is equivalent to concealing digits in a 2^{2r}-ary notational system. Hence for APPM,

$$r_{appm} = 2 \times r_{de}$$

Because of embedding data in three channels, the *r* bpp is equivalent to embedding *3 × 2r* bits for every three pairs of pixels. Hence for EAPPM,

$$r = 3 \times r_{appm}$$

IV. Performance and Security Analysis

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

Table2 presents the maximum payload supported by the four embedding methods at an MSE of 0.092. EAPPM is able to support 300% more than APPM. As the data is embedded in all the three layers, for EAPPM, the payload support will be more than 3 times that of APPM.

Payload (bpp)	LSB	DE	APPM	EAPPM
0.025431	0.168676	0.143649	0.094927	
0.076294	0.168676	0.143649	0.094927	0.091497
0.114441	0.164326	0.143727	0.091771	0.095604
0.15767	0.168766	0.143901	0.094807	0.091497
0.203451	0.168973	0.143826	0.094971	0.091497
0.257492	0.16924	0.144003	0.095374	0.091497
0.4673				0.091874
0.610352				0.091812
0.772476				0.091648

Table1. MSE Comparison

	Max Payload supported with MSE at 0.092
LSB	0.025431
DE	0.025431
APPM	0.114441
EAPPM	0.772476

Table2. Max Payload support Comparison

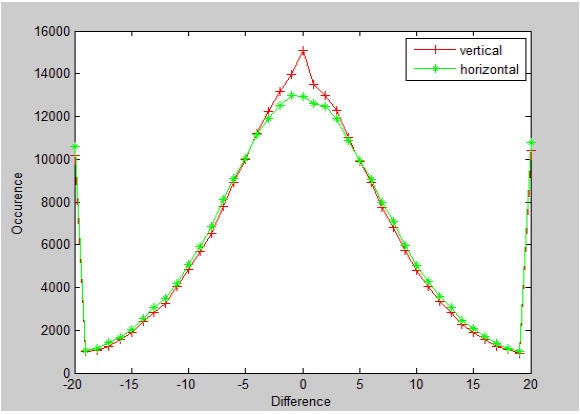

Figure2. Average vertical and horizontal difference histograms of LSB

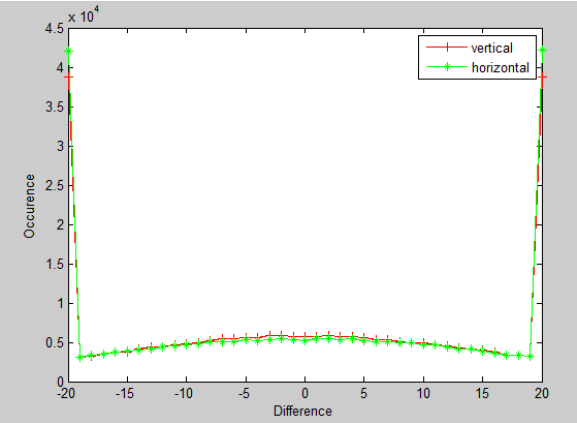

Figure3. Average vertical and horizontal difference histograms of DE

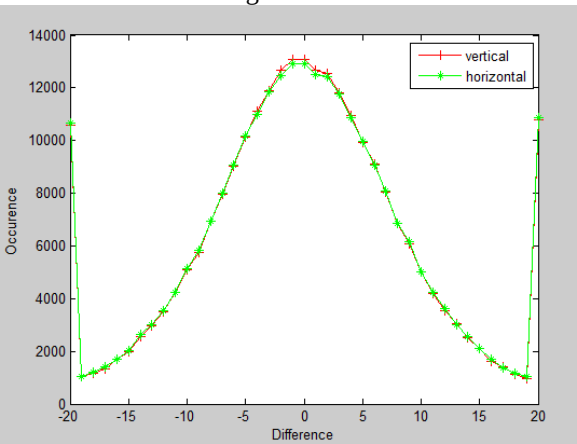

Figure4. Average vertical and horizontal difference histograms of APPM

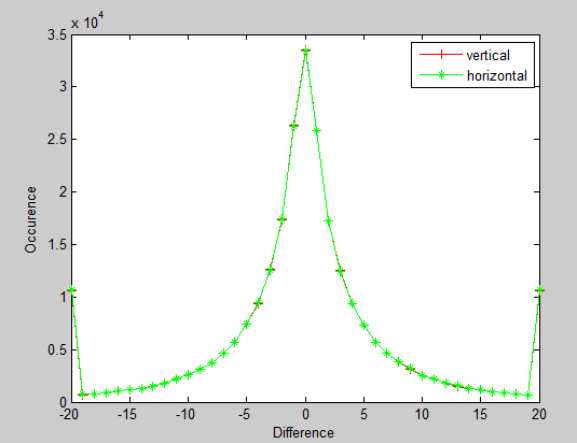

Figure5. Average vertical and horizontal difference histograms of EAPPM

Figures 1, 2, 3 and 4 show the average vertical and horizontal difference histograms of LSB, DE, APPM and EAPPM. It is observed that the difference is absolutely less to be noticed. This ensures high security of the data against different steganalysis.

V. Conclusion

This paper proposed an efficient data embedding algorithm EAPPM, based on APPM, which can successfully embed data into three layers of an RGB image. EAPPM is able to embed three times data more than APPM, without any compromise on MSE and security. The advantages of APPM, like the freedom for user to use any notational system and better image quality are carried to EAPPM. EAPPM not only achieves higher payloads, but also offers smaller MSE compared to DE and APPM. EAPPM offers high security along with the adjustable data embedding capacity.

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, FEBRUARY 2012.

[2] Ruey-Ming Chao,Hsien-ChuWu,Chih-Chiang Lee, and Yen-Ping Chu, "A Novel Image Data Hiding Scheme with Diamond Encoding", EURASIP Journal on Information Security Volume 2009, Article ID 658047.

[3] Chi-Kwong Chan, L.M. Cheng, "Hiding data in images by simple LSB substitution", Pattern Recognition Society. Published by Elsevier Ltd.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] J. Fridrich and D. Soukal, "Matrix embedding for large payloads,"IEEE Trans. Inf. Forensics Security, vol. 1, no. 3, pp. 390–394, Sep.2006.

[10] Chi-Kwong Chan, L.M. Cheng, Improved hiding data in images by optimal moderately signi7cant-bit replacement, IEEElectron. Lett. 37 (16) (2001) 1017–1018

[11] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognition 34 (3) (2001) 671–683.
[12] G. Cancelli, G. Doërr, I. Cox, and M. Barni. "Detection of steganography based on the amplitude of histogram local extrema". IEEE International Conference on Image Processing,ICIP,San Diego, California, October 12–15, 2008.
[13] F. Hartung and M. Kutter, "Multimedia watermarking techniques,"Proceedings of the IEEE, vol. 87, no. 7, pp. 1079–1107,1999.
[14] X. Zhang and S.Wang, "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security," Pattern Recognition Letters, vol. 25, no. 3,pp. 331–339, 2004.
[15] Y.-C. Tseng, Y.-Y.Chen, and H.-K. Pan, "A secure data hiding scheme for binary images," IEEE Transactions on Communications, vol. 50, no. 8, pp. 1227–1231, 2002.

AUTHORS PROFILE

M.LakshmiPrasanna was born in Andhra Pradesh, India, in 1988. She received the Bachelor degree, B.Tech (ECE) from the University of JNTU, Ananthapoor, in 2009. She is currently pursuing Master degree, M.Tech (DECS) in Sree Vidyanikethan Engineering College, Tirupathi.

Mr. Sk.Mahaboob Basha received his M.Tech degree. He is currently working as Assistant Professor, Department of ECE in SreeVidyanikethan Engineering College.