# Appm: A Narrative Data Embedding Method Using Adaptive Pixel Pair Matching

## P.Ramesh Babu[1] Y.Chitti Babu[2] Dr.P.Harini[3]

[1] *II Year M.Tech, St.Ann's College Of Engineering And Technology,*
*Chirala, Prakasam(Dt), Andhra Pradesh, India*
[2] *Associate Professor , Dept Of CSE , St.Anns's College Of Engineering & Technology,*
*Chirala, Prakasam(Dt), Andhra Pradesh, India*
[3] *Professor And HOD Dept Of CSE , St.Anns's College Of Engineering & Technology,*
*Chirala, Prakasam(Dt), Andhra Pradesh, India*

## ABSTRACT

*Here We Proposed A New Data-Hiding Method Based On Pixel Pair Matching (PPM). In This Paper The Basic Idea Of PPM Is To Use The Values Of Pixel Pair As A Reference Coordinate, And Coordinate Search In The Neighborhood Used To 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.(EMD)Exploitedmodificationdirection(EMD) And Diamond Encoding (DE) Are Two Data-Hiding Methods Proposed Recently Based On PPM. Then 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 Is The Proposed Method Offers Lower Distortion Than DE By Having High Compact Neighborhood Sets And It Will Also Accepting Embedded Digits In Any Representative System. Then It Will Be Compared With The (OPAP)Optimal Pixel Adjustment Process Method, Then This Method Always Has Lower Distortion For Various Payloads. Experimental Results Reveal That The Proposed Method Does Not Only Provides Performance Better Than Those Of OPAP And DE, But Also Is Secure Under The Detection Of Some Well-Known Steganalysis Techniques.*

*INDEX TERMS: (ADPPM)Adaptive Pixel Pair Matching,(DE) Diamond Encoding , Exploiting Modification Direction (EMD), Least Significant Bit (LSB), Optimal Pixel Adjustment Process (OPAP), Pixel Pair Matching (PPM).*

## I.  INTRODUCTION

In digital image processing, while processing images here we need to follow certain criteria. Combining data into a carrier for conveying secret messages that should be confidentially is the technique of data hiding [1], [2]. After embedding, pixels of cover images will be modified and deformation occurs. The distortion caused by data embedding is called the embedding distortion [3]. A good data-hiding method must be capable of evading visual and statistical detection [4] while providing an adjustable payload [5].Many approaches of information hiding have been proposed for diverse applications, such as patent protection, top secret transmission, tampering exposure, and figure authentication.  large amount well-known data hiding format is the least significant bits (LSBs) replacement process. This process embeds fixed-length covert bits into the least significant bits of pixels by directly replacing the LSBs of cover picture with the secret message bits. Although this process is simple, it generally effects noticeable deformation when the number of embedded bits for each pixel exceeds three. Several methods have been proposed to decrease the distortion induced by LSBs replacement. Another approach of improving LSBs scheme is to decrease the amount of alterations required to be introduced into the cover image for data hiding when the numeral of secret bits is significantly less than that of available cover pixels. The method proposed by Tseng et al. [6] can cover up as many as *log2(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*2w - 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 worth 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 method, the pre-process can convert the secret data into sequences of digits with $(2n + 1)$-ary notational representation

## II .RELATED WORK

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.

**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
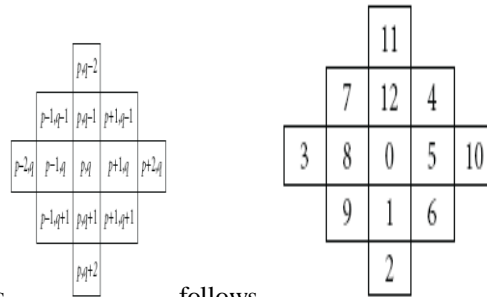
described as                     follows.

$$f(x, y) = ((2k + 1) \times x + y) \bmod (2k^2 + 2k + 1)$$
$$k = 2, (x, y) = (0, 0)$$

$$f(x, y) = (5 \times x + y) \bmod (13)$$
$$f(0, 0) = (5 \times 0 + 0) \bmod (13) = 0$$
$$f(1, 0) = (5 \times 1 + 0) \bmod (13) = 5$$
$$f(2, 0) = (5 \times 2 + 0) \bmod (13) = 10$$
$$f(0, 1) = (5 \times 0 + 1) \bmod (13) = 1$$
$$f(0, 2) = (5 \times 0 + 2) \bmod (13) = 2$$
$$\vdots$$
$$f(0, -1) = (5 \times 0 + (-1)) \bmod (13) = 12$$

Assume that a, b, p, and q are pixel values, and k is a positive integer. The neighborhood set Sk (p, q) represents the set that contains all the vectors (a, b) with the distance to vector (p, q) smaller than k, and Sk(p, q) is defined as the above.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 above: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 Sk belongs to {0, 1, 2, . . ,l-1}and any two DCVs of vectors in Sk(p, q) are distinct. Assume that Ek represents the embedded digit and Ek 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 Sk is dk= f (p, q)−Ek mod *l*. For each k, we can design a distance pattern Dk to search which neighboring pixel owns the modulus distance dk. Then, the vector (p, q) is replaced with the neighboring vector (p', q') by dk. The vector (p', q') is the member of Sk(p, q) and the DCV of (p', q') equals to the embedded secret digit Ek. The vector (p', q') can extract the correct secret digit by above formulas 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.
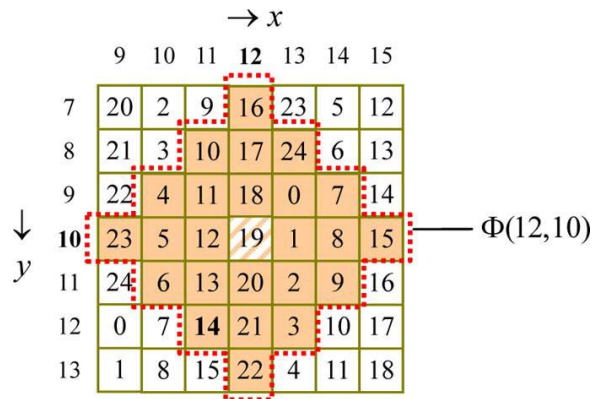
Fig. 1. Neighborhood set for .ω(12,10) for k=3.

## III.PROCEDURE AND ALGORITHM:

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 ω(x,y) such that f(x,y)=Sb, where f is the drawing out function and Sb, is the message digit in a -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)Є ω(x,y). has to be found 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 ω(x,y) should be as small as possible.
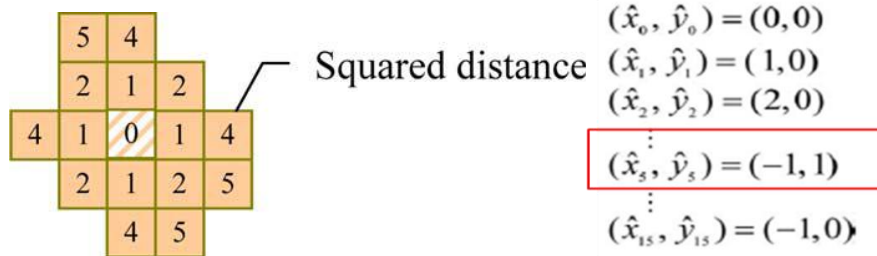


$$(\hat{x}_o, \hat{y}_o) = (0,0)$$
$$(\hat{x}_1, \hat{y}_1) = (1,0)$$
$$(\hat{x}_2, \hat{y}_2) = (2,0)$$
$$\vdots$$
$$(\hat{x}_s, \hat{y}_s) = (-1,1)$$
$$\vdots$$
$$(\hat{x}_{15}, \hat{y}_{15}) = (-1,0)$$

Fig: Neighborhood set $\omega_{16}$ (0, 0) and f(x,y) , where . 0<=i<B-1.

The best PPM metbhod shall satisfy the following three requirements:
1) There are exactly B coordinates in ω(x,y).

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

3) The design of ω(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.

DE is a data-hiding method based on PPM. DE greatly enhances the payload of EMD though preserving acceptable stego image quality. but, there are several problems. First, the payload of DE is determined by the selected notational structure, which is restricted by the bound ; therefore, the notational system cannot be arbitrarily selected. For example, when is 1, 2, and 3, then digits in a 5-ary, 13-ary, and 25-ary notational structure are used to surround data, respectively. However, embedding digits in a 4-ary or 16-ary (i.e., 2 bits per pixel) notational system are not supported in DE. Second, ω(x,y) in DE is defined by a diamond shape, which may lead to some unnecessary distortion when k>2 . In fact, there exists ω(x,y) a better other than diamond shape resulting in a smaller embedding deformation The wished-for method not only allows concealing digits in any notational structure, but also provides the same or even smaller embedding deformation than DE for various payloads.

**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 $|M{\times}M / 2| \geq |SB|$, and convert $S$ into a list of digits with a $B$-ary notational system $SB$.
[2] The discrete optimization problem is solved to find $cB$ and $\varnothing B(x, y)$.
[3] In the region defined by $\varnothing B(x, y)$, 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 $Kr$.
[5] To embed a message digit $sB$, two pixels (x, y) in the cover image are selected according to the embedding sequence $Q$, and calculate the modulus distance between $sB$ and f(x, y), then repace (x, y) with (x + x', y + y') [7].
[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 $\varnothing(x, y)$ for each layer are taken distinct subsets.
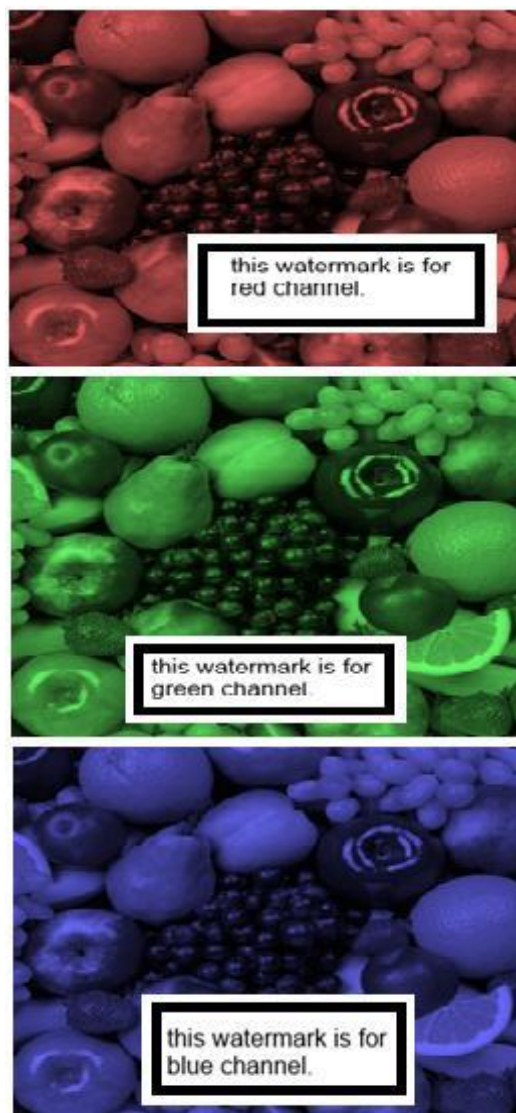


Figure 1. Embedding respective watermarks for different Channel Images

.

**. 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.

## IV.  EXPERIMENTS AND EVALUTION

**Performance**

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.

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

Table1. MSE Comparison

| 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 |

Table2. Max Payload support Comparison

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

[2]     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.

[3]     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.

[4]     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.

[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]     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.

[7]     W. Zhang, X. Zhang, and S. Wang, "A double layered plus-minus one data embedding scheme," *IEEE Signal Process. Lett.*, vol. 14, no. 11,pp. 848–851, Nov. 2007.

# AUTHORS:

**Dr. P. Harini** is presently working as a professor and HOD,Dept of Computer Science and Engineering,in St.Ann's College of Engineering and Technology, Chirala.She obtained Ph.D in distributed and Mobile Computing from JNTUA, Ananthapur. She Guided Many UG and PG Students. She has More than 15 Years of Excellence in Teaching and 2 Years of Industry Experience. She published more than 20 International Journals and 25 Research Oriented Papers in Various Areas. She was awarded **C**ertificate of Merit** by JNTUK, Kakinada on the University Formation Day on 21 - August - 2012. . from JNTUk, Kakinada.

**Y.Chitti babu** is presently working as an Asso*ciate professor ,Dept of Computer Science* and Engineering ,in St.Ann's College of Engineering and Technology,Chirala.He Guided Many UG and PG Students. He has More than 10 Years of Teaching Experience.He published more than 5 International Journals and 7 Research Oriented Papers in Various Areas.

**P.Ramesh babu** is presently Studying the M.Tech (CSE) in St.Ann's College Of Engineering                                                                                                          a
and  Technology, Chirala affiliated to Jawaharlal Nehru Technological University,Kakinada.