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. 9, September 2014, pg.656 – 662

RESEARCH ARTICLE

An Efficient Data hiding Method Based on Adaptive Pixel Pair Matching and Image Sharing

Anumol Raju, Dr. Sasidhar Babu

M-Tech Student, Sree Narayana Gurukulam College of Engineering and Technology, Kerala

Professor, Sree Narayana Gurukulam College of Engineering and Technology, Kerala

anumolraju1991@gmail.com, sasidharmails@gmail.com

Abstract- Steganography is one the main method of data hiding technique. So, it has wide varieties of applications in hiding secret information such as in the field of medical, military, law forensics and co-operate field etc. Here image steganography with Adaptive Pixel Pair Matching (APPM) and image sharing is used. The basic concept behind APPM is, consider the pixel pair value as a reference coordinate, and then find the neighborhood set of this pixel pair according to a given message digit. The secret data digit is embed by replacing of pixel pair and the searched coordinate. Security is a major issue in these systems because data embedding causes modification to the cover image pixels. By analysing these distortions, an attacker can easily detect the presence data hiding. In order to avoid these situations, this paper describes an efficient data hiding method based on APPM and image sharing. Here image sharing is done by using shamir's secret share algorithm. The experimental results show that the proposed method is much better than the existing methods.

Keywords— steganography, adaptive pixel pair matching, APPM, image sharing, shamir's secret share, pixel pair, data hiding

I. INTRODUCTION

The growth of information system is increased day by day. So security is the main aspect and has to ensure it for the safe data processing. In image steganography, the aim is to hide information in to a given image and the diagnosis of the hidden information will be probably difficult. Every steganographic methods consist of a cover medium and a stego medium. Here the cover medium will act as a carrier of the secret data and the stegno medium can be produced by replacing the redundant bits of cover medium with the secret data.

For every steganographic system must consider the three aspects, capacity, security and robustness. The capacity refers to the amount of secret information that can be hidden embeds in the image. Security aspects means the inability of detection of secret data. The amount of modification the embed image can survive prior to the detection of data is known as robustness. In order to improve these characteristics, there were so many steganographic methods proposed such as Least Significant Bit(LSB), Pixel Pair Matching(PPM), Exploiting

Modification Direction(EMD), Diamond Encoding(ED), Optical Pixel Adjustment Process(OPAP) etc. These all methods are different in different aspects. But the efficiency of steganography technique depends upon its related aspects. So here a new data hiding method based on APPM and image sharing is introduced, which will minimum distortions to the cover medium will acquire more attention. Here image sharing is done by using shamir's secret share algorithm.

II. SYSTEM OVERVIEW

This is the frame work for an efficient data hiding method. It is based on adaptive pixel pair matching and image sharing. So in this method, first we embed the secret message into image with user defined key. It is done using adaptive pixel pair matching technique. Thus we get the message embedded image. Then we share the encoded image as two image share using shamir's secret sharing algorithm. On the receiving side, the combining these two image share first. Then it extracts the secret message from the image. So main four steps involving in this method are; Data embedding, share creating image share, combine image shares, and extraction of data. So the data hiding method takes place the following order.
At sender site:
1) Data embedding using the steganographic method APPM
2) Create the image shares from the data embedded image.

At receiver site:
1) Combining of image shares using shamir's secret share algorithm.
2) Extract the secret data from the image using APPM.
The system architecture of the new data hiding method is given below.

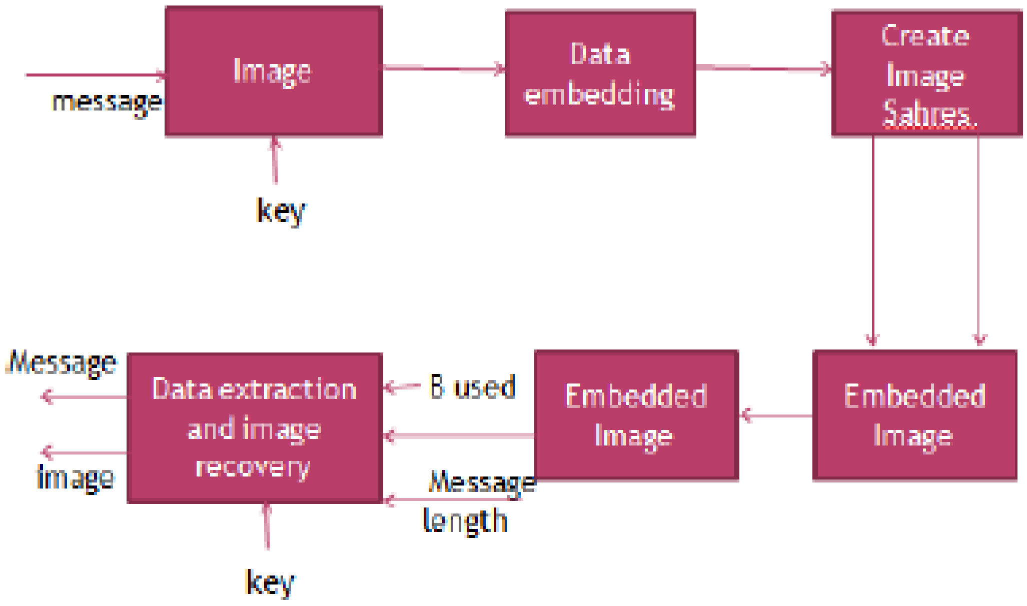


Fig1: System Architecture

A. ADAAPTIVE PIXEL PAIR MATCHING TECHNIQUE (APPM)

It is the data hiding method based on APPM. Also it is the extension of PPM (Pixel Pair Matching). The basic idea of the APPM-based data-hiding method is to use pixel pair (x,y) as the coordinate, and searching a coordinate(x',y') (reference co-ordinate) within a predefined neighborhood set ϕ(x,y) such that, where f(x,y)=sB where f is the extraction function and sB is the message digit in B ary notational system to be concealed. When selecting the reference co-ordinate, the following factors;
1) Selection based on the key

2) Co-ordinates should having two values (x and y axis)

3) First value should less than the number of columns in the image

4) Second value should less than the number of rows in the image.

Data embedding is done by replacing (x,y) with (x’,y’). These are the reference coordinate and pixel value from the neighbourhood set. The concept of a PPM-based steganographic method is that, let sB be the message bit is to be concealed and the range of sB is between 0 and B-1 . And their should be a coordinate (x’,y’) has to be found such that f(x’,y’)=sB. That is why the range of f(x,y) must be within integers between 0 and B-1. Also here each integer must occur at least once. In APPM, consider the compact neighbourhood set for reducing the distortion. The best PPM based data hiding method shall satisfy the following three conditions:
1) There are exactly B number of coordinates in the neighbourhood set ϕ(x,y).
2) These coordinates and the values of extraction function must be mutually exclusive.
3) The design aspects of neighbourhood set ϕ(x,y) and the extraction function f(x,y) should be capable of embedding the message bits in least notational system.

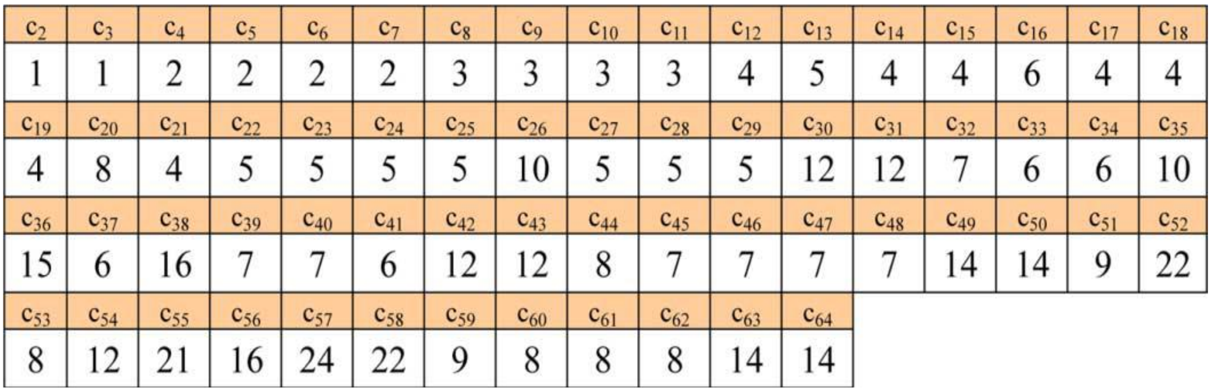
1. Finding Neighborhood Set And Extraction Function

In this module, the extraction function is explained. That is how to find the neighborhood set. By using this method, we get a very simple extraction function and compact neighbourhood set. Thus the proposed method enhances the embedding efficiency. The image quality obtained by this method is much more better than the other existing data hiding method such as OPAP and DE. The another two advantages of this proposed method are higher payload capability and less detectability. Minimum notional system is used for data embedding gives increased performance .

The stegno image quality significantly affect by both definitions of ϕ(x,y) and f(x,y). All values of ϕ(x,y) in f(x,y) have to be mutually exclusive, also the summation of the squared distances between all the pixel values in ϕ(x,y) and x,y has to be the least one. This is because, during embedding procedure the pixel value (x,y) is replaced by one of the pixel in the neighbourhood set ϕ(x,y) . If there is B number of coordinates in ϕ(x,y), then message bits a B-ary notational system are to be concealed. The averaged MSE is calculated by averaging the summation of the squared distance between coordinates in ϕ(x,y) and the reference coordinate. Thus, given the expected MSE after embedding can be calculated the following equation by MSE=1/2B $\sum_{i=0}^{B-1}((xi-x)^2+(yi-y)^2$.

In this proposed adaptive pixel pair matching (APPM) data-hiding method to explore better ϕ(x,y) and f(x,y). So that MSE is minimum as compared with the other existing methods. In this method the extraction function, f(x,y)=(x+cB*y)mod B. So the calculation of both neighbourhood set ϕ(x,y) and the extraction function f(x,y) is done by a discrete optimization problem. For this consider the following conditions. Minimize$\sum_{i=0}^{B-1}(xi-x)^2+(yi-y)^2$ subject to f(xi,yi) ∊{0,1,…..B-1},f(xi,yi) ≠f(xj,yj)

Figures 2 and 3 show some representative ϕB(x,y) and their corresponding cB value which satisfying the above condition. In figure 3 the shaded with lines represents the the center of ϕB(x,y).



c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}	c_{13}	c_{14}	c_{15}	c_{16}	c_{17}	c_{18}
1	1	2	2	2	2	3	3	3	3	4	5	4	4	6	4	4
c_{19}	c_{20}	c_{21}	c_{22}	c_{23}	c_{24}	c_{25}	c_{26}	c_{27}	c_{28}	c_{29}	c_{30}	c_{31}	c_{32}	c_{33}	c_{34}	c_{35}
4	8	4	5	5	5	5	10	5	5	5	12	12	7	6	6	10
c_{36}	c_{37}	c_{38}	c_{39}	c_{40}	c_{41}	c_{42}	c_{43}	c_{44}	c_{45}	c_{46}	c_{47}	c_{48}	c_{49}	c_{50}	c_{51}	c_{52}
15	6	16	7	7	6	12	12	8	7	7	7	7	14	14	9	22
c_{53}	c_{54}	c_{55}	c_{56}	c_{57}	c_{58}	c_{59}	c_{60}	c_{61}	c_{62}	c_{63}	c_{64}					
8	12	21	16	24	22	9	8	8	8	14	14					

Fig 2: List of cB for 2≤B≤16

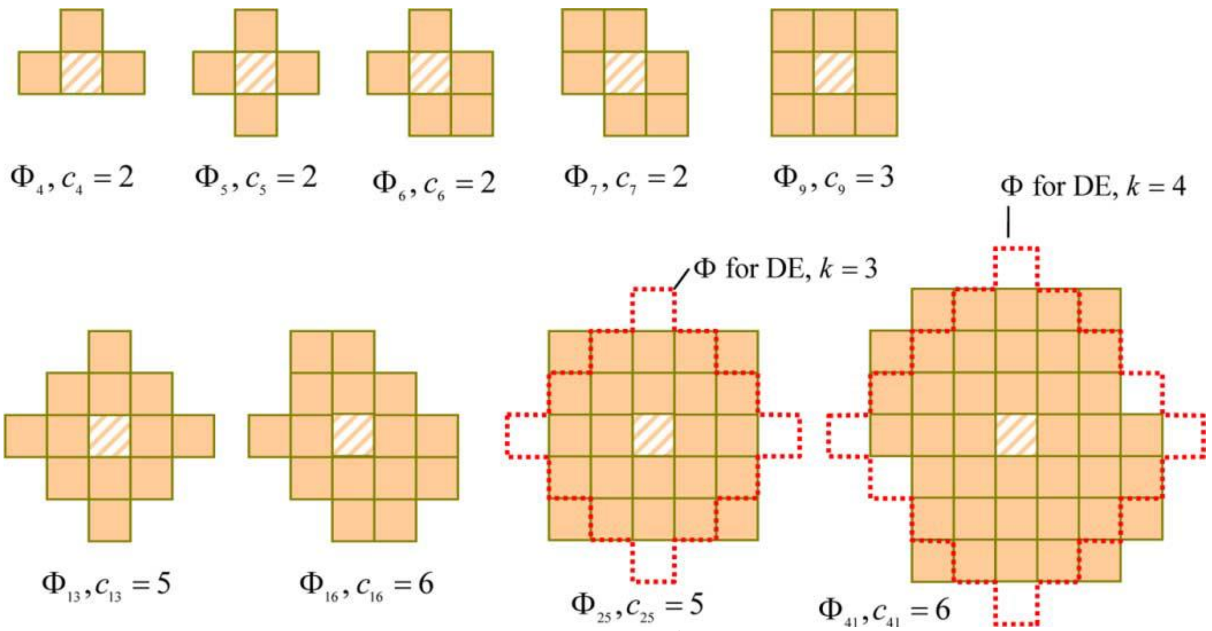


Fig 3: Neighbourhood set for APPM

2. Data Embedding Procedure

Here the secret data is embed into the given cover image. For this first we calculate the image size and message size. If the message size exceeds the image size, then the embedding procedure cannot be done. Consider the image size as M*M, For S message bits the size of secret message S is |S|. By using these, calculate the minimum B value for concealing all the message bits. Then, message digits are sequentially concealed into pairs of pixels. The detailed procedure is listed as follows.

Input: M*M size image , secret message sB, and key Kr
Output: Stego image I', minimum cB and key Kr .

1. Calculate the minimum B satisfying ∟M*M/2⅃>=|sB|.
2. Convert the secret message S into the sequence of digits with a B -ary notational system.
3. Find cB and ϕB(x,y) using the dicrete optimization equations.
4. From the neighbourhood region ϕB(0,0) find the coordinate positions (xi,yi) by satisfying the condition f(xi,yi)=i, 0≤ i≤ B-1
5. Create a nonrepeat random key Kr for embedding the secret message bits Q
6. To embed a secret message bits B, find the two pixels (x,y) in the cover image according to the secret message sequence Q,
7. Replace (x,y) with (x+xd,y+yd) for the modulus distance d=(sB-f(x,y))mod B between sB and f(x,y)
8. Repeat Step 6 and 7 until all the secret message bits are concealed.

3. Data 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.

Input: Stego image I', minimum cB, and key Kr.
Output: Secret bit stream S.

1. By using the key Kr create the embedding sequence Q.
2. Find the two pixels positions (x',y') according to the embedding sequence Q of the secret message .
3. Calculate f(x',y') using the descrete optimization equation.
4. Save the secret message as the embedded digit.
5. Repeat Steps 2, 3and 4 until all the secret message bits are extracted.
6. Converting the extracted message digits into a binary bit stream, we get the secret message

B. IMAGE SHARING

After data embedding, the image shared into two shares. For this here, shamir’s secret share algorithm is used. In this image sharing concept[11], the image are shared based on the pixel intensity. Thus after sharing we get the shares of the same image. We can’t retrieve anything from a single share. After combining the shares, we get the original image. And all these shares are look in a same manner. Thus if an attacker may get an image share, he can’t retrieve the information. It may ensure the added security.

Here using shamir’s secret share, pixel intensity of image is divided into parts, giving each participant its own unique part. From this some of the parts or all of them are needed in order to reconstruct the secret message. Counting on all participants to combine together the secret might be impractical, and therefore sometimes the threshold scheme is used where any ***k*** of the parts are sufficient to reconstruct the original secret. Another advantage of using this algorithm is these two copies of image shares are visibly identical. So an attacker may misunderstand it, and considered as the normal embedded image.

1. Image Share Construction

For sharing a secret d, which is in teh form of integer. In this method it will be pixel intensity value. The threshold secret sharing method is *(k,n)* which means k is the total number of shares and n is the number participants. For secret recovery, n shares are collected from the k shares, where *k≤n* .The detail of the method is reviewed in the following;

Input: secret to be shared in the form of an integer as d, the number of participants as n, and a threshold value is k ≤ n.
Output: n secret shares in the form of integers

1. Select a prime number p randomly select which is larger than d.
2. Choose k-1 integer values as c1, c2, …, ck-1 within 0 through p-1.
3. Determine the n distinct real values x1, x2, …, xn.
4. Compute n function values F(xi) or partial shares by using the following (k -1) degree polynomial, where i=1,2,…..n

$$F(x_i) = (d + c_1x_i + c_2x_i^2 + \ldots + c_{k-1}x_i^{k-1})_{\mathrm{mod}\,p},$$

5. Deliver partial shares f(xi) as a share to the ith participant

2. Combining Image Shares

Input: k number of shares from the n participants, prime number p
Output: the secret d that hide in the shares using the coefficients ci used as in the share construction algorithm, where i = 1, 2, …, k -1.

1. Compute the following functions using the *k* shares (*x*1, *F*(*x*1)), (*x*2, *F*(*x*2)), …, (*xk*, *F*(*xk*))

$$F(x_j) = (d + c_1x_j + c_2x_j^2 + \ldots + c_{k-1}x_j^{k-1})_{\mathrm{mod}\,p},$$

Where j=1,2,…….,k
2. Using the Lagrange’s interpolation obtain the value of d, and solve all the *k* equations.

$$d = (-1)^{k-1}[F(x_1)\frac{x_2x_3\ldots x_k}{(x_1-x_2)(x_1-x_3)\ldots(x_1-x_k)} + F(x_2)\frac{x_1x_3\ldots x_k}{(x_2-x_1)(x_2-x_3)\ldots(x_2-x_k)} + \ldots + F(x_k)\frac{x_1x_2\ldots x_{k-1}}{(x_k-x_1)(x_k-x_2)\ldots(x_k-x_{k-1})}]_{\mathrm{mod}\,p}.$$

3.Calculate *c*1 through *ck*-1 by expanding the following equality and comparing the result with the equation from step 1 while regarding the variable *x* in the equality below to be *xj* in the step 1

$$F(x) = [F(x_1)\frac{(x-x_2)(x-x_3)\ldots(x-x_k)}{(x_1-x_2)(x_1-x_3)\ldots(x_1-x_k)} + F(x_2)\frac{(x-x_1)(x-x_3)\ldots(x-x_k)}{(x_2-x_1)(x_2-x_3)\ldots(x_2-x_k)} + \ldots + F(x_k)\frac{(x-x_1)(x-x_2)\ldots(x-x_{k-1})}{(x_k-x_1)(x_k-x_2)\ldots(x_k-x_{k-1})}]_{\mathrm{mod}\,p}.$$

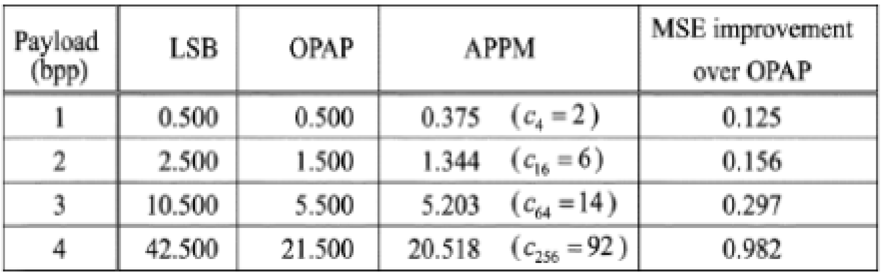
III.PERFORMANCE EVALUVATION

The analysis is mainly done for checking the results are correct or not. Analyzing is the only way to check the results of the work and to determine whether the further modification is needed or not. The analysis mainly done on the methodologies which are being used for implementing the whole system. The comparison of results are given below. Here the comparison analysis of APPM with the other existing data hiding method.

When data embed in an image, the pixel values in that image may modified and this process is known as image distortion or embedding distortion. MSE (Mean Square Error) is used to measure this distortion. MSE is calculated by the following equation.

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

Where M*M is the image size, Pij is the pixel value of original image and Pij' denote the pixel values of the stego image. Here the mean square error between the cover image and stego image is represented by MSE. The smaller MSE is for APPM which indicate the better image quality.



Payload (bpp)	LSB	OPAP	APPM	MSE improvement over OPAP
1	0.500	0.500	0.375 $(c_4 = 2)$	0.125
2	2.500	1.500	1.344 $(c_{16} = 6)$	0.156
3	10.500	5.500	5.203 $(c_{64} = 14)$	0.297
4	42.500	21.500	20.518 $(c_{256} = 92)$	0.982

Table 1: MSE Comparison

The following images are processed during the proposed method. Less detectability to the data hiding image is one of the desired aspect. In this case all of them visually similar. That is an attacker can't determine whether the given image is encoded or shared. The decryption of image share will gives the wrong message.

(a) (b) (c)

(d) (e)

Fig : 4 (a)- input image(cover image) , (b)-encoded image(stegno image), (c)- image share1, (d)-image share 2, (e)-image of combined image shares

IV. CONCLUSION

This work is a simple and efficient data embedding method based on APPM and image sharing. Here the two pixels positions are scanned and it considered as an embedding unit. Especially the compact neighborhood set is used for embed the secret message bits with a smallest notational system. APPM find out the least notational system for data embedding, and thus it can be achieves a better image quality. The image sharing also enhances the security from attackers.

REFERENCES

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

[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]C.K Chan and L.M Cheng, "Hiding data inimages by simple LSB substitution" vol.37,no.3,pp 469-474,2004 Signal Process., vol. 53, no. 10, pt. 2, pp. 3923–3935, Oct. 2005.

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

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

[6]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,*2009

[7]Wien Hong and Tung-Shou Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching", IEEE *Trans .Inf. Forensics Security,*vol 7,no. 1,feb 2012

[8] Che-Wei Lee, *Student Member, IEEE*, and Wen-Hsiang Tsai, *Senior Member,* A Secret-Sharing-Based Method for Authentication of Grayscale Document Images via the Use of the PNG Image With a Data Repair Capability, IEEE Transactions On Image Processing, Vol. 21, No. 1, January 2012