International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 10, October - 2013

High Quality Adaptive Pixel Pair Matching

Surya Chandra Rao Kunche
M-Tech - CNIS
CSE, MVGR COLLEGE OF ENGINEERING

Ravva Anil Kumar
Assistant Professor
CSE, MVGR COLLEGE OF ENGINEERING

Abstract

Steganography is the art of hidden messages in such a way that no one except the sender and intended recipient knows about the existence of the message. Image, audio and video can be taken used as a carrier in steganography. Digital images are serve as a carrier for the secret data transmission. A good data-hiding technique should be capable of eliminating visual and statistical detection with an adjustable payload. The APPM can allows users to choose digits in any notational system for data embedding, and thus achieves a better image quality and security but it is proposed only for the gray scale images. In this paper HQAPPM was proposed, which is extension to APPM for high quality color images. The proposed method provides low mean square error (MSE) without compromising the performance and security of APPM.

1.INTRODUCTION

Digital communication has become an important part of infrastructure now-a-days, a lot of applications are Internet based and in some cases it is required that, the communication should be made secret. To achieve this secrecy there are mainly two techniques are available: Cryptography and steganography. Cryptography is a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data for to keep the message secret[9]. Unfortunately in some cases it is not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message to be secret[12]. The technique used to implement this process, is called steganography.

Steganography is nothing but the invisible communication. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing"[7]. In the steganography the information is hidden completely in images. Steganography is differs from cryptography in the sense that where cryptography targets on keeping the contents of a message secret while the steganography focuses on keeping the existence of a message to be secret. Cryptography and steganography are both ways to protect information from unauthority parties but neither technology alone is perfect and can be compromised. Once the existence of secret message is revealed or even suspected, the use of steganography is partly defeated. The strength of steganography can be amplified by combining it with cryptography.

Many approaches of information hiding have been proposed for different applications, such as secret transmission, copyright protection, tampering detection, and image authentication. The familiar data hiding scheme is the least significant bits (LSBs) substitution method. In this LSB method we directly replace the LSB bits of cover image with the fixed-length of least significant bits secret message bits[11]. This LSB method is simple but the drawback is it effects a noticeable distortion when the number of embedded bits for each pixel exceeds three. Many methods are proposed to reduce the distortion caused in LSBs substitution. This draw back can be overcome with the OPAP with less distortion. The extension of exploiting modification direction (EMD) embedding scheme is the Diamond Encoding (DE) method.

The main idea of the exploiting modification is that the pixels in the image were grouped into n pixels per group. A pixel in each group is modified one gray scale value at most to hide a secret digit in a (2n+1)-ary notational system[1]. The Pixel pair matching-based data-hiding method provides high embedding efficiency. The main idea of PPM 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') = SB , where f is the extraction function and SB is the message digit in a (2n+1)-ary notational

system to be masked. The data embedding is done by replacing (x', y') in the place of(x, y) .

Related Work

The OPAP effectively reduces image distortion caused by the traditional LSB method. DE increases the payload of EMD by embedding the digits in a B-ary notational system. In this section LSB, OPAP,DE and APPM will be briefly reviewed.

LSB substitution Method

The most familiar steganographic technique is the least-significant-bits (LSBs) substitution method. This LSB method embeds the fixed-length of secret massage bits in to the same fixed length LSBs of pixels. This method is simple but in generally it causes a noticeable distortion when the embedded bits for each pixel exceed three. Several methods in steganography have been proposed to reduce the distortion caused by LSBs substitution. For example, adaptive methods vary the number of embedded bits in each pixel, and they possess a good image quality than other methods using only simple LSBs substitution. However this method can achieve at the low cost in the embedding capacity[3].

Optimal Pixel Adjustment Process (OPAP)

Chan et al. in 2004proposed the OPAP method that improves the image distortion problem which is the disadvantage of LSB replacement. This OPAP can be explained as follows: 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[6]. OPAP employs the following equation to adjust v' so that the embedding distortion can be minimized

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

Where v" is the result obtained by OPAP embedding. Observe that v" and v' have the same right-most r LSBs and thus from the from the right-most r LSBs we can directly extract the embedded data. Here is a simple example. Suppose a pixel value v=152 = $10011000_2$and the bits to be embedded are 101_2. In this case r =3, and s=5. Afters is embedded, we obtained v'=157. Because $v^{(3)} = 000_2=0$ and $v^{(3)} - s = 0-5 < -2^{3-1}$and, we obtained v" = v' - 2^3 = 157-8 = 149 = 10010101_2. Thus, after embedding101_2, the pixel value 152 is changed to 149. From right-most three LSBs of 149 we can extract the embedded data.

Diamond Encoding (DE)

In the diamond encoding the author considered the embedding parameter k such that the diamond encoding scheme can conceal (2k2 + 2k + 1)-ary digit into a cover pixel pair. The embedding and extraction procedures are shown in Figures 1 and 2, respectively. In this Embedding process a parameter k is selected based on secret data size, and he transform secret data into diamond encoding digits. Consider a secret data of size is s, and then the embedding parameter kcan be determined by finding the minimal positive integer which satisfies the inequality

$$[\left(\frac{m \times n}{2}\right) \log 2(2k^2 + 2k + 1 \ge s]$$

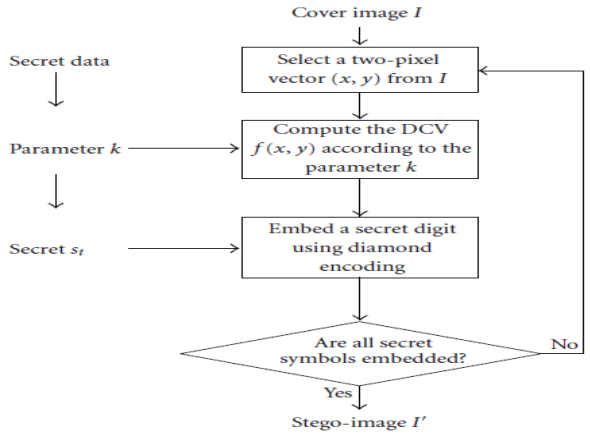
Set the embedding base B= $2k^2$+2k+1.then the secret message is considered as a sequence of digits in B-ary notational system. The original image is divided into a number of nonoverlapping two-pixel blocks. After that select each block from top-down and left-right in turn for the data embedding process. The embedded secret message is converted into B-ary digit sequence. And the embedded secret digitstis obtained from the t^{th} index of the sequence of B-arydigits. Then from $f(x,y)=((2k+1)x + y) \text{ mod} B$ we calculate the DCV of two pixel values x and y. Then by replacing f (x, y) with st we can calculate new stego-image pixel pair. The used equation is dt= (st–f(x, y))modB.

The symbol dt shows the modulus distance between the st and f (x, y). By applying the distance dt, the stego-pixel values x' and y' can be found in Dksuch that the DCV is replaced with st. However the underflow or overflow problems may occurred; that is, the stegopixel value x' or y' might go beyond 255 or below 0. If the stego-pixel value has the underflow or overflow problem, the critical vector (x', y') has to be adjusted to the appropriate value. The adjustment rules areas follows:

(1) if x'>255, x' = x'−B;
(2) if x_ <0, x' = x'+ B;
(3) if y'>255, x' = x' −B;
(4) if y'<0, y' = y'+ B.

From the above rules, it can be observed that the underflow or overflow problem is solved and also has the same DCV value. Next from the cover image we take the next pixel pair and repeat until all the secret data have been concealed. Then we can collect all the

Stego-pixel values to form corresponding stego-image.



Figures 1: Embedding Process

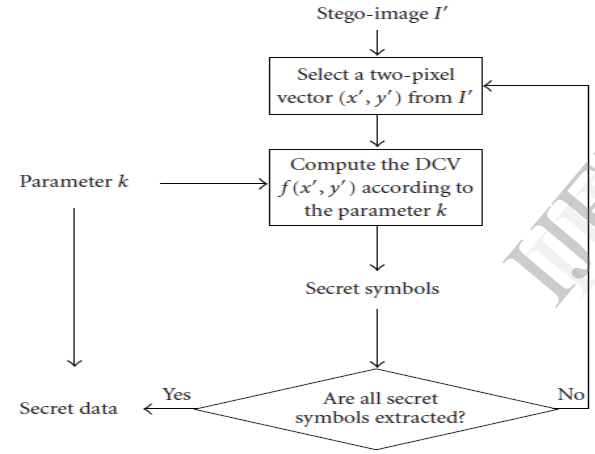


Figure 2: Extraction Process

Adaptive Pixel Pair Matching (APPM):

In this method the data can be embedded as fallows: consider a cover image is of size MxM, S is the message bits to be embedded and the size of S is |S| . In order do embed all the message bits firstly he calculated the minimum. Then, the message digits are sequentially embedded into pairs of pixels .Construct a nonrepeat random embedding sequence Q using a key K_r .Then 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))modB between s_B and f(x,y) , then replace (x,y) with $(x+\hat{x}d, y+\widehat{yd})$ repeat this until all the message digits are embedded.

To extract the embedded message digits, the pixel pairs are scanned in the same order as in the embedding procedure. Embedded message digits are the extraction function values of the scanned pixel pairs[1].

Proposed method:

As the APPM offers better security against detection and lower distortion, we will extend this APPM for colored images. The proposed method provides better security and lower distortion for embedding data in colored images. Also, performance in terms of payload can be improved. The colored images, consists three different colored layers (R,G,B), 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.

Firstly R, G, B layers are separated and the each layer is considered as a gray image, referred as Channel Image.

For a PPM-based method, suppose a digit s_B is to be embedded. The range of s_B is between 0 and B-1 , and a coordinate (x',y') $\epsilon\phi$(x,y) has to be found such that f(x'y')=s_B. Therefore, the range of f(x,y) must be integers between 0 and B-1, and each integer must occur at least once. The number of coordinates in ϕ(x,y) should be as small as possible in order, to reduce the distortion. The best PPM method should satisfy the following three requirements:

1) There should be exactly B coordinates in ϕ(x,y) .

2) The values of extraction function in those coordinates must be mutually exclusive.

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

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 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 less. 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. By averaging the summation of the squared distance between and other coordinates in Ø(x, y) we can obtained the average

MSE. 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≤I,j≤B-1

Embedding Procedure:

Consider the cover image is of size M×M, then each of R, G, B channels will be of size M×M. Size of S is |S| where S is the message bits to be concealed for each channel image. In order to embed all the message bits first we calculate the minimum B. Then the message digits are sequentially concealed into pairs of pixels.

1. First minimum B satisfying |M×M / 2| ≥|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 ØB(x, y).
3. In the region defined by ØB(x, y), record the coordinate (x', y') such that f(x', y') = i, 0 ≤ i ≤ B-1.
4. Construct a nonrepeating random embedding sequence Q using a key Kr.
5. Two pixels (x, y) in the cover image are selected to embed a message digit sB, 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 ØBr , green channel image be ØBg and blue channel image be ØBbØBr , ØBg and ØBb are selected such that

ØBr⊄ØBg⊄ØBb

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.

Extraction Procedure:

To extract the embedded message,the pixel pairs are scanned in the same order as done in the embedding procedure. Embedded message digits are the extraction function values of the scanned pixel pairs.

1. The high quality colored image is split into respective R, G, B layers and each is considered as a separate 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 thef(x', y'), the output is the embedded digit.
5. Repeat the Steps 2 and 3 until all the message bits are obtained.
6. By converting the obtained message digits into a binary bit form, Finally, the message bits can be obtained.

Theoretical and Performance Analysis:

MSE is the cumulative squared error between the compressed and the original image. Using MSE we can measure the image quality and it is given by

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

Where $p'_{i,j}$ and $p_{i,j}$ denote the pixel values of the stego image and the original image, respectively and M×M denotes the image size.MSE is the mean square error between the cover image and stego image. If the MSE is less it indicates that the stego image has better image quality.

To evaluate the performance of the proposed scheme, a high definition colored image is taken. The simulation is run using MATLAB. First, LSB, DE, APPM and HQPPM are evaluated for Mean Square Error (MSE) with different payloads. Table 1 presents the MSEs of all methods for the gray scale image and Table 2 presents the MSEs of all methods for the high quality colored image. It is observed that with the proposed method we got small MSE value compared to the older methods i..e for gray scale image. It is also observed that for the proposed method HQPPM we got very small MSE value.

Table1: MSE Comparison for Gray Scale Image

Method	Gray Scale Image	MSE
LSB	Cameraman	9.4481
OPAP	Cameraman	3.1541
DE	Cameraman	2.2377
APPM	Cameraman	1.5893

Table 2: MSE Comparison for Colored Image

Method	Color Image	MSE
COPAP	Peppers	0.9692
CDE	Peppers	0.716
CAPPM	Peppers	0.4075

Fig 3: Cover image

Fig 4: stego image of OPAP

Fig 5: stego image of DE

Fig 6: Stego image of HQAPPM

CONCLUSION

This paper proposed an efficient data Embedding method HQAPPM based on APPM. In this method the data is successfully embedded into the High quality colored image. With this HQAPPM we can able to embed three times data more than APPM, without compromising the security and MSE. The main advantage of APPM is to use any notational system and better image quality. This HQAPPM not only achieves higher payloads, but also offers smaller MSE compared to DE and APPM. HQAPPM offers high security along with the adjustable data embedding capacity.

REFERENCES

[1] Wien Hong and Tung-Shou Chen,2012,. "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching", IEEE transactions on information forensics and security, VOL. 7, NO. 1, FEBRUARY 2012.

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

[3]Mr. Rohit Garg," Comparison Of Lsb & Msb Based Steganography In" International Journal of Engineering Research & Technology (IJERT)
Vol. 1 Issue 8, October – 2012"

[4]R.Amirtharajan, Sandeep Kumar Behera, Motamarri Abhilash Swarup, Mohamed Ashfaaq K and John Bosco Balaguru Rayappan," Colour Guided Colour Image Steganography", Universal Journal of Computer Science and Engineering Technology 1 (1), 16-23, Oct. 2010.

[5] Pooja Kaushik and Yuvraj Sharma," Comparison of Different Image Enhancement Techniques Based Upon Psnr & Mse" International Journal of Applied Engineering Research, ISSN 0973-4562 Vol.7 No.11 (2012).

[6] Chi-Kwong Chan, L.M. Cheng," Hiding data in images by simple LSB substitution", www.elsevier.com/locate/patcog, Pattern .

[7] Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett,"Stegenography:the art of hiding",
School of Computer Science, The University of Birmingham, http://www.gnu.org/copyleft/fdl.html.
[8] T. Morkel, J.H.P. Eloff, M.S. Olivier," an overview of image steganography", Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa
[9] Ali m-Ahmad, Ghazali Bin Sulong, Mohd. Shafry, B. Mohd. Rahim, Saparudin," A 2-tier Data Hiding Technique Using Exploiting
Modification Direction Method and Huffman Coding", ACEEE Int. J. on Information Technology, Vol. 02, No. 02, April 2012.
[10] Miss. Vaishali V. Jadhav , Mrs. P.P.Belagali, Ms.Sapana Kishor Soudagar , Ms.Pooja Adgonda Patil," Edge Adaptive Image Steganography using LSB Matching Revisited", IOSR Journal of Electronics & Communication Engineering (IOSR-JECE) ISSN : 2278-2834, ISBN : 2278-8735, PP : 40-44.
[11] Himanshu Gupta, Prof. Ritesh Kumar, Dr. Soni Changlani," Enhanced Data Hiding Capacity Using LSB-Based Image Steganography Method", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 6, June 2013).
[12] vijay kumar sharma, vishal shrivastava," a steganography algorithm for hiding image in
image by improved lsb substitution by minimize detection", Journal of Theoretical and Applied Information Technology, 15th February 2012. Vol. 36 No.1
[13] cheng-hsing yang and shiuh-jeng wang," Transforming LSB Substitution for Image-based Steganography in Matching Algorithms", journal of information science and engineering 26, 1199-1212 (2010).
[14] M.Sangeetha,"
Analysing Image Quality via Color Spaces", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 1, January - February 2013, pp.1532-1536