International Journal of Electronics Communication and Computer Engineering
Volume 5, Issue (4) July, Technovision-2014, ISSN 2249–071X

Technovision-2014: 1st International Conference at SITS, Narhe, Pune on April 5-6, 2014

An Efficient Image Hiding Scheme using Optimal Pixel Adjustment Process

Rajashree Shitole
Department of Electronics &Telecommunication Engg.
Imperial College of Engineering and Research, Pune, India
Email: rajeeedev@gmail.com

Prof. Satish Todmal
Department of Information Technology
Imperial College of Engineering and Research, Pune, India
Email: srtodmal@gmail.com

***Abstract* – In the new era of developing information security techniques, it is necessary to maintain security of images which serve as a source for data analysis for different applications. Therefore there is rapid demand for reliable techniques, to ensure the security of images. This paper describes a novel method of data embedding, based on Pixel Pair Matching (PPM). In Optimal Pixel Adjustment Process (OPAP), pixel x is embedded in k-bits of message m, using Least Significant Bit (LSB) substitution method by adjusting stego pixel at optimal level.**

***Keywords* – Least Significant Bit (LSB), Optimal Pixel Adjustment Process (OPAP), Pixel Pair Matching (PPM).**

I. Introduction

Digital images are widely transmitted over the Internet; therefore, they often serve as a carrier for covert communication. Images used for carrying data are called cover images and images with data embedded as stego images. After embedding, pixels in the cover images will be modified and there will be distortion occurs. The distortion occurs during data embedding is called the embedding distortion. Data hiding is a technique which imperceptibly embeds important data into media such as images, voice, documents, etc. Data Hiding is defined by T. Morkel as follows, "Steganography is art and science of invisible communication."

Acceptable data hiding provides large amount of data to be embedded in the cover image maintaining quality of stego image. The most popular method of data hiding is Least Significant Bit method. There are basically two types of LSB methods LSB replacement and LSB matching. In both the cases data to be hidden is represented in binary form. Amount of data that can be embedded is called as embedding capacity and distortion present during embedding is called as embedding distortion. LSB method has average embedding capability. In this method each pixel of cover image is compared with data to be hidden depending upon even and odd values of pixels, they are increased or decreased respectively or kept unmodified. But because of this method, distortion during embedding increases, and results in degradable image quality. It becomes very easy to detect the change in values, because all these operations are performed on Least significant Bit [1][2] . In, 2001 Rang-Zan Wang *et al.* [3] proposed image data hiding scheme by optimal LSB substitution and genetic algorithm. But when this algorithm was implemented, Signal to Noise Ratio (SNR) obtained was much less than LSB substitution in some cases. Due to LSB replacement, embedding distortion increases, hence OPAP is conceptually defined as matching pixel to its optimal level was introduced. Basic concept of Pixel Pair Matching is to provide a new value of pixel pair with respect to value of reference pixel pair according to the secret message digit and new value of pixel pair is replaced by secret digit. In other words pixel pair is used for embedding, first pixel is used to carry one message bit and second pixel carries binary function related to it. In 2006, Mielikainen [4][5] proposed LSB matching method but here, two pixels were used to carry two bits. Therefore, error calculated is (3/4)*(12/2) = 0.315 of 1bpp[5].

II. Optimal Pixel Adjustment Process

This section describes the implemented technique based on PPM. Consider $P_{xi}, P_{xi}', P_{xi}''$ represent pixel values at ith pixel in the host image H, stego image is given as S. Stego image S is calculated by LSB substitution method. It is basically represented in [8]. LSB substitution works as follows [4][5]

$$\delta_i = P_{xi}' - P_{xi} \quad (1)$$

where, δ_i = embedding error

Cover or host image of M*N pixels is represented as

$$H = x_{ij} E\{0.1,....255\}$$

Secret message M in K secret bit is

$$m = \{mi \mid 0 \le i < n,\ mi \in \{0,1\}\} \quad (2)$$

Secret message is rearranged to form a virtual message of K-bit is denoted m'

$$m' = \{ m_i' \mid 0 \le i < n',\ m_i' \in \{0,1,\dots 2^k-1\}\} \quad (3)$$

where, n'=M*N

For embedding LSB substitution method is used

$$m' = \{ m_i' \}$$

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

Therefore Stego image comprises of chosen pixel value xli which stores K-bit of message m_i'. Stego pixel is denoted by

$$x_{li}' = x_{li} - x_{li} * mod * 2^k + m_i' \quad (4)$$

Therefore P_{xi} is nothing but x_{li}'. K is directly replaced by LSB of P_{xi} with secret message bit.

International Journal of Electronics Communication and Computer Engineering
Volume 5, Issue (4) July, Technovision-2014, ISSN 2249–071X

$-2^k < \delta_i < 2^k$

Therefore to convert P_{xi}' to P_{xi}'' i.e. original pixel to stego pixel three cases are defined.

Case 1: $(2^{k-1} < \delta_i < 2^k)$

$$P_{xi}'' = \begin{cases} P_{xi}' - 2^k & ; P_{xi}' \geq 2^k \\ P_{xi}' & ; \text{otherwise} \end{cases}$$

Case 2: $(-2^{k-1} \leq \delta_i \leq 2^{k-1})$

$$P_{xi}'' = P_{xi}' \quad ; \text{for all}$$

Case 3: $(-2^k < \delta_i < -2^{k-1})$

$$P_{xi}'' = \begin{cases} P_{xi}' + 2^k & ; P_{xi}' < 256 - 2^k \\ P_{xi}' & ; \text{otherwise} \end{cases}$$

So for optimal pixel pair matching, P = pixel value, rLSB = rightmost bit of v, P'= pixel value after embedding rLSB using LSB substitutions described above (8). Aim of OPAP is to adjust P; to its optimal level by decreasing embedding distortion.

$$P'' = \begin{cases} P' + 2^{rLSB} & ; P^{rLSB} - S > 2^{r-1} \ \& \ P' + 2^{rLSB} \leq 255 \\ P' - 2^{rLSB} & ; P^{rLSB} - S > -2^{r-1} \ \& \ P' - 2^{rLSB} \geq 0 \\ P' & ; \text{otherwise} \end{cases}$$

After embedding if value of P =160 is changed to P'' = 157 according to the above stated conditions. It is proved that pixel pair is matched at optimum level. If last three bits of P'' are extracted, embedded data can be extracted very easily

III. Embedding and Extraction Procedure of OPAP

A. Embedding procedure

Step 1. To begin, we have two images one cover and second secret image,so the first step is to read the images. After that check for the size mismatch of secret and cover image. All cover images should be greater or equal to secret images. If not so then Cover and secret image sizes mismatched message will be displayed.

Step 2. Find the maximum pixel value in the secret image after converting it to double and pixel value will be in terms of rows and columns. now find the number of LSB to be replaced in OPAP.

Step 3. Change the cover image pixels one by one using OPAP and get the original value of pixels. Save the value of LSB to be replaced, convert binary to decimal. get the bits to be embedded. Now to get the values with LSB substitution.

Step 4. Replace the pixels according to OPAP rules:

$$P'' = \begin{cases} P' + 2^{rLSB} & ; P^{rLSB} - S > 2^{r-1} \ \& \ P' + 2^{rLSB} \leq 255 \\ P' - 2^{rLSB} & ; P^{rLSB} - S > -2^{r-1} \ \& \ P' - 2^{rLSB} \geq 0 \\ P' & ; \text{otherwise} \end{cases}$$

Step 5. Check for the conditions:

If condition1 and condition 2 is true then use first formula, If condition 3 and condition 4 is true then use second formula, and if none of the conditions are satisfied then use the last formula.

B. Extraction Procedure

Step 1. To begin with, in the data extraction procedure, read the stego image.

Step 2. Find the maximum pixel value of the stego image in terms of rows and columns. Find the number of LSB which are replaced for OPAP.

Step 3. Extract data from each pixel and convert binary value into decimal value.

Step 4. Check all secret bits are extracted. If yes, then we will get finally the secret image or it starts execution from Step 1.

IV. Quality Analysis

Whenever any Stego image is created, some new data is embedded in the original/ cover or so called Host image. Because of this embedding, pixel values are modified. To measure the quality of stego image SNR, MSE, etc. are used. So, here, we are dealing SNR of OPAP. SNR is defined as the ratio of signal to noise between cover and stego image. Larger value of SNR denotes better stego image quality. Mathematically, SNR is defined as follows

$$SNR = \frac{\sum_{x=0}^{m-1} \sum_{y=0}^{n-1} f1(x,y)]2}{\sum_{x=0}^{m-1} \sum_{y=0}^{n-1} [f1(x,y) - f(x,y)]2} \tag{5}$$

Where

$$f(x, y) = \frac{\text{Original Image}}{\text{Cover Image or Host Image}}$$

$$f_1(x, y) = \frac{\text{Stego Image}}{\text{Secret or Embedded Image}}$$

SNR value in dB given by,

SNRdB = 10 log10SNR (6)

The probability of | P - P'' | lies in the range of [1, 2^{rLSB} - 1] is $1/2^{rLSB}$

$$SNR_{OPAP} = \frac{12}{(4rLSB+2)} \tag{7}$$

V. Error Calculations

For error calculations we observe four calculations

1) Color map indicating maximum difference between cover image and stego image. Plot the change in the value of each pixel of cover image(*refer Fig1 and Fig3*)

2) Create histogram to check no. of pixels whose values are changed over the range of 0 to 8 for OPAP(*refer Fig2 and Fig4*)

3) Color bar indicating maximum difference between secret image and extracted image in this technique of OPAP (*refer Fig2 and Fig4*)

4) The maximum difference between stego image and secret image is measured by the parameter called SNR (Signal to noise ratio).And the formula is mentioned above in eq.5 and 6.

VI. Experimental Results

There are four combinations of cover and secret image used with OPAP but, in this case secret image is kept as lena and only cover images as baboon. But still there are two cases shown here once the size of secret and cover image is same and in other case size of secret image is less than that of cover image. The size of cover image is kept constant in both the cases that is 500*500,but in Case 1 the size of secret image is 500*500 whereas in Case 2 it is 400*400 consequently.

Case1:

Cover image = Secret image

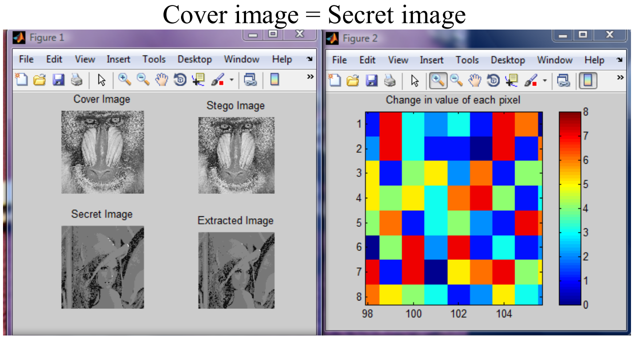

Fig.1. Cover and secret image of same size

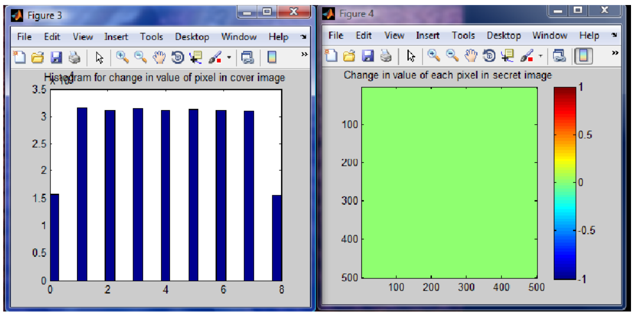

Fig.2. Histogram and change in the pixel value of extracted images of same sizes

Case 2:

Cover image >Secret image

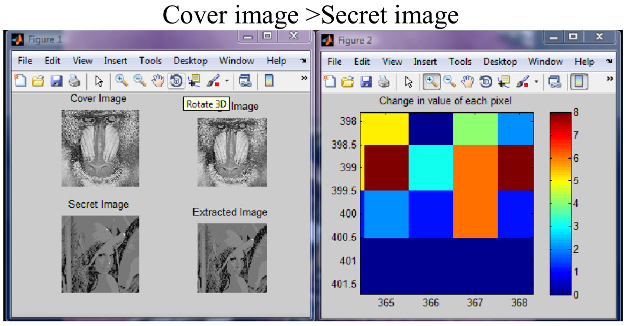

Fig.3. Cover greater than secret image

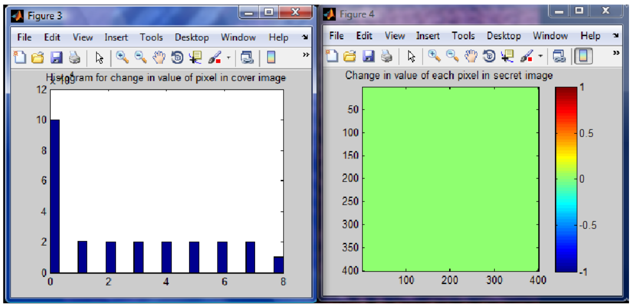

Fig.4. Histogram and change in the pixel value of extracted images when cover image is greater than secret image

Here Fig.1 and Fig.2 shows that the SNR decreases when cover image and secret image is of same size, whereas when cover image is greater than secret image then SNR increases. The tabular comparison of results in Table1 illustrates that large amount of data is embedded in cover image without losing imperceptibility of the image.

Table1: Result of OPAP

Sr. no.	Cover image	Size of cover image	Secret image	Size of secret image	SNR of OPAP (dB)
1	Baboon	500*500	Lena	500*500	29.341
2	Baboon	500*500	Lena	400*400	31.279
3	Kelly	500*500	Lena	500*500	27.932
4	Kelly	500*500	Lena	400*400	29.696

It is clear from Table 1 that OPAP outperforms LSB substitution in terms of embedding efficiency, quality of stego image, etc.

VII. Conclusion

This paper implements one efficient data embedding techniques. Optimal Pixel Adjustment Process gives acceptable image quality as compared to Least Significant Bit with optimal pixel matching and scores well with an improved SNR. OPAP gives no artifacts in stego image if cover image is much greater than secret image to be embedded, and large amount of data can be embedded in cover image. OPAP gives comparatively a better performance with respect to LSB. An alternate approach can be considered to give better image quality and embedding efficiency than OPAP.

Acknowledgment

This paper would not have been possible without the support of many people. The author wishes to express her gratitude to her guide, Prof. Satish Todmal HOD (IT department) Imperial College of Engineering and Research, Pune who was abundantly helpful and offered invaluable assistance, support and guidance. His technical knowledge was very insightful which acted as the backbone to structure this paper and even to implement the algorithm successfully. Lastly a greater thanks to the Prof.P.R.Badadapure HOD (E&TC department) and few staff members of Electronics and Telecommunication Department from Imperial College of Engineering and Research, Pune for their valuable support and guidance.

REFERENCES

[1] J. Fridrich, M. Golijan, 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

[2] A. D. Ker, "Steganalysis of LSB matching in grayscale images" *IEEE Signal Process. Lett*., vol. 12, no. 6, pp. 441-444, Jun. 2005

[3] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, "Image hiding by optimal LSB substitution and genetic algorithm," *Pattern Recognition*, vol.34, no. 3, 671683, 2001

[4] 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

[5] J. Mielikainen, "LSB Matching revisited," IEEE *Signal Process. Lett.,* vol.13, no. 5, pp. 285-287, May 2006.

[6] 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.

[7] Xinpeng Zhang and Shuozhong Wang, "Efficient Steganographic embedding by exploiting modification direction," *IEEE Communication Lett*. Vol. 10, no.11, Nov. 2006

[8] Chi-Kwong Chan, L.M. Cheng, "Improved hiding data in images in optimal moderately significant bit replacement," *IEE electron. Lett.* 37, vol. 16, pp. 1017-1018, 2001.