International Journal of Modern Trends in Engineering and Research
www.ijmter.com
e-ISSN No.:2349-9745, Date: 2-4 July, 2015

Data Hiding Techniques: Survey and current status

Salman Shaikh[1], S. R. Kinge[2]

[1]*E&TC, MITCOE, Pune, India (M.E. Student), sk.salman61@gmail.com*
[2]*E&TC, MITCOE, Pune, India (Professor),sanjaykinge100@gmail.com*

Abstract-For rapid development of network technology data is needed to be communicated over the network. Although network transmission is convenient and fast, the data is often attacked. Steganography is used to hide the data in the images. Images used for carrying data are called cover images and images with embedded data are called stego images. Data is embedded in the images in such a way that it should be detected by human eyes and it should be robust so that it offers resistance to various image processing methods and compression. In this survey paper our focus is on development and current status on data hiding techniques in spatial domain of images.
Keywords-Steganography, stego image,least significant bit(LSB), optimal pixel adjustment process (OPAP), diamond encoding(DE).

I. INTRODUCTION

Steganography/Data hiding is a secure communication method that conveys secret messages in the form of plaintexts so that the appearances of the secret messages will not draw eavesdroppers attention while they are being transmitted through an open channel. The word steganography is originally derived from Greek words which mean ‘‘Covered Writing’’. It has been used in various form for thousands of years. In the 5th century B.C Histaiacus shaved a slave’s head, tattooed a message on his skull and the slave was dispatched with the message after his hair grew back[1].

1.1Development

For decades peoples worked on development on methods of secret communication. Generally three methods are used for security systems steganography, cryptography & watermarking [1].

1.1.1Steganography

Carrier usd in communication for steganography can be any digital media. Main objective of steganography is for secret communication. There is no visibility in the o/p file. Any cover image can be used for communication.

1.1.2Cryptography

Carrier used in cryptography is text or image file. Main objective is data protection. There is visibility in o/p file.

1.1.3Watermarking

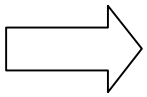
Carriers are mostly image /audio files. Main objective is copyright preservation. Cover image choice is restricted.

II. RELATED WORKS

Steganography is checked on two aspects imperceptibility and embedding capacity (payload). Imperceptibility is nothing but the differences between stego image and cover image which is not visible to human eyes. This measurement is done by MSE and PSNR. Payload is maximum number of bits that can be embedded in pixel with acceptable stego image quality.

78	90	99
109	100	84
102	98	111

0	3	7
4	6	1
3	5	2



72	91	103
108	102	81
99	101	106

COVER IMAGE ***SECRET MESSAGE*** ***STEGO IMAGE***

Steganography can be done in spatial domain as well as transform domain. Spatial domain has advantages over transform domain. It is simpler and faster to implement the techniques,stego image quality is under control with high embedding capacity. In this paper we shall introduce methods that embeds message in spatial domain.Above diagram shows simple example of data hiding in image.

2.1. LSB Method

Most traditional method used for data embedding is LSB method .as we know that every pixel value is eight bit which can be represented as

$$P_x = (a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0) = \sum_{x=0}^{7} a_x 2^x$$

$$P_x \quad any\ pixel\ value$$
$$a_7 \quad MSB \quad , \quad a_0 \quad LSB$$

Usually $a_2 a_1 a_0$ can be used to hide secret data because LSB bits carry less information than MSB Embedding procedure goes on every pixel one by one. Let the message bits be $s_2 s_1 s_0$

$$P'_x = (a_7 a_6 a_5 a_4 a_3 s_2 s_1 s_0)$$

We directly replace 3 LSB bits of pixels with the message bits. *P*'is the new pixel value with the embedded data[3].

2.2 Optimal Pixel Adjustment Process

It was proposed by Chan *et al.* In 2004 [5].The simple LSB method is modified so that stego image quality is improved. OPAP algorithm uses LSB method as its base. OPAP gives good results than LSB replacement method [5][4].

Let p be the pixel value. Decimal value of right most n LSB be p^n. p'be the pixel valuedirect embedding and m be message data to be embedded in the pixel. OPAP employs following equations to embed a data to get minimum distortion.

$$P'' \begin{cases} p' + 2^n, p^n - m > 2^{n-1} \ and \ p' + 2^n \leq 255 \\ p' - 2^n, p^n - m < -2^{n-1} \ and \ p' - 2^n \geq 0 \\ p', \quad otherwise \end{cases}$$

$P''$is the result obtained after algorithm implementation [7].

Example: let the pixel value p=160=10100000(2), Data to be embedded be m= 7=111(2) .Let n(replacing bits) = 3.By direct LSB replacement p'=10100111=167. Check for the three conditions

of OPAP algorithm. It satisfies $p^n - m < -2^{n-1}$ *and* $p' - 2^n \geq 0$ = 0-7< -2^{3-1} .P''= p' - 2^n= 167 - 8 = 159. Hence 7 is embedded in the pixel 160 with distortion of only one unit.
Extraction: The n LSB bits of the stego image pixels is nothing but the data embedded ,hence extraction is very simple.

III. PPM (PIXEL PAIR MATCHING METHOD)

In PPM method data is embedded to reduce the embedding impact by providing a simple extraction and a more compact neighbourhood set. Diamond encoding (DE) is PPM method. The image quality obtained by these methods has less imperceptibility. The scanning method has to unique for transmitter and receiver side in communication[6].

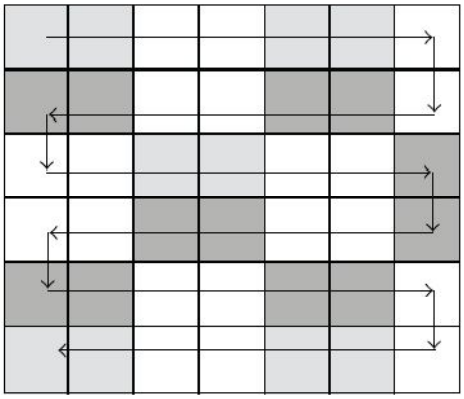


Fig 1. Sequence of non overlapping consecutive two-pixel blocks is constructed in a cover image.

3.1 Diamond Encoding

In 2009 Chao *et al.* [12] proposed a PPM based method Diamond Encoding. DE preserves acceptable stego image quality. Message is embedded in B-ary notational system, where

$$B = 2x^2 + 2x + 1 , \quad x > 1$$

B = payload & x is variable

Let cover image be M×M. Let message to be embedded be m .the variable integer x is determined to satisfy the equation

$$\lfloor M \times M/2 \rfloor \geq |m_B|$$

Where,

$|m_B|$is number of message bits in B-ary notational system.

The neighbourhood set of diamond encoding algorithm is determined as,

$$\Psi(p,q) = \{(a,b)||a-p| + |b-q| \leq x\}$$

$\Psi(p,q)$ represents the set of coordinates (a,b) whose absolute distance to the coordinates (x,y) is smaller or equal to x. first we use diamond encoding function

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

Then modulus distance between m and DE function is calculated as

$$d = mod(m - f(p,q), B)$$

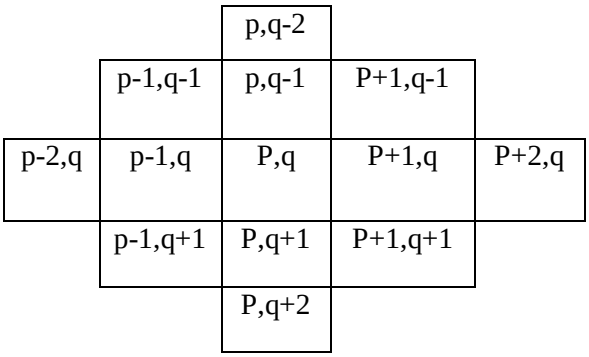


Fig 2. co-ordinates of neighbourhood set

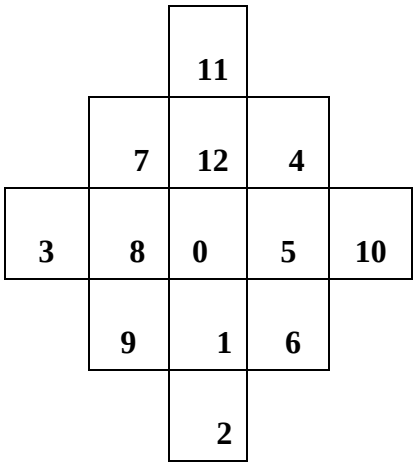


Fig 3. Neighbourhood set for k=3

After calculating the distance it is searched in the neighbourhood set of $\Psi(p,q)$ and coordinates are found out. (p,q) are modified according to the coordinates. The new pixels in the stego image are p'& q'. At the receiver side the embedded value is extracted from stego image by using equation

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

Hence the correct embedded value is extracted.

Example : Let consecutive pixels be (20,30). for k=3 B=25. Diamond encoding function be $f(20,30)$=mod((2×3+1)×20+30,25)=20.let data to be embedded be 15. So modulus distance be d=mod(15-20,25)=20. Coordinates of 20 are (p-1,q+2). Hence new pixel values are(19,32). We can observe that by embedding 15 in the pixels(20,30), pixels are modified by just 1 & 2 units respectively.

When any stego-pixel value has the overflow or underflow problem the critical vector has to be adjusted to the appropriate value, the adjustment rules are defined as follows

$$(1)\ if\ \ p' > 255\ , p' = p' - B$$
$$(2)\ if\ \ p' < 0\ \ \ \ , p' = p' + B$$
$$(3)\ if\ \ q' > 255\ , q' = q' - B$$
$$(4)\ if\ \ q' < 0\ \ \ \ , q' = q' + B$$

IV. COMPARISON AND ANALYSIS

In this section we will compare the performance of single pixel embedding method i.e LSB replacement method and optimal pixel adjustment process method. The stego image quality improves when we use OPAP method instead of LSB replacement method. Experimental results shows that PSNR value of the OPAP method is greater than LSB method. Stego image quality for 4 bits LSB replacement is acceptable for naked eyes but when embedding bits are increased beyond 4 bits it causes clear distortion. However in smooth areas even 4 bits LSB replacement method causes a noticeable distortion.
In case of PPM method they offer a high payload and acceptable stego image quality is preserved. It embeds more messages per modification and increases the efficiency. The stego image quality after embedding has last MSE and is less detectable in DE as compared to LSB, OPAP.

V. FUTURE WORKS

Future research efforts will be concentrated in attaining high embedding capacity and maintaining stego image quality. There should be variation in embedding depending upon the neighbourhood of the pixel i.e more data to be embedded in edge regions as compared to smooth region. Image should be divided into smooth and edge areas and then data hiding should be done.
During communication images are likely to get attacked. These attacks may cause problems while extraction of data. So research should be done so that at the receiver side initially attacks should be removed without causing any danger to message data. In future how to increase the payload for same PSNR level and how to increasePSNR value under same payload.Steganographic scheme itself should be able to avoid attacks.

CONCLUSION

Steganography is the art of secret communication under the cover of digital images. In this paper we have reviewed some good data embedding schemes which have either high stego image quality or high embedding capacity. If we want to embed large amount of data and if stego image quality is not so important than use OPAP method, But when image quality is of greater importance than embedding capacity, than DE is the best choice.
Though the embedding capacity is low they give a greater image quality where distortion is invisible to human eyes. DE is the best for secure communication under adjustable embedding capacity.

REFERENCES

[1] Cheddad, J. Condell, K. Curran, and P. Mc Kevitt," Digital image Steganography: Survey and analysis of current methods," Signal Process., vol. 90, pp. 727–752, 2010.
[2] Nan-I Wu, Min-shiang Hwang," Data Hiding: Current status and Key Issues", International Journal of Network security,vol.4. No.1, PP.1-9, 2007.
[3] J. Fridrich, M.Goljan, and R. Du, "Reliable detection of LSB steganography in color andgrayscale images",in Proc. Int. Workshop on Multimediaand Security, 2001, pp. 27–30.
[4] C. H. Yang, "Inverted pattern approach to improve image quality of information hiding by LSB substitution," Pattern Recognition., vol. 41,no. 8, pp. 2674–2683, 2008.
[5] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," PatternRecognition, pp. 469–474, Mar. 2004.
[6] R.M Chao, H.C.Wu , C.C.Lee and Y.P.Chu, "A novel image data hiding scheme with diamondencoding" EURASIP J Infsecurity, vol. 2009,2009.
[7] C.C.Thien and J.C.Lin," A Simple and high hiding capacity method for hiding digit by digit data in images based on modulus function", pattern Recognition, vol.36. no. 12. Pp 2875-2881, 2003.

