International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Suitable Data Hiding Technique for Windows Phone

Zainalabideen Abdual Samad Rasheed

Assistant lecturer, Computer Science, Education College, Kufa University, Iraq

Abstract: ***People today are widely interest for exchanging their information through various communication tools which are development rapidly lately .for that reasons a secure communication is very important part to change vital data in safe way. Steganography can create a confident network to interchange the confidential information between sender and receiver. In this paper, some steganography techniques have been analyzed, implemented and test. The goal of the project is to presenta summary of some image steganography to pinpoint the requirements of a best steganography method. The selected approach is chosen to be as an application under mobile phone. This application should be able to hide a secret message and retrieve the secret message from stego-image too. Steganography techniques have been tested under personal computer using mat lab software for comparative purpose in terms of image quality, capacity, time and robustness which are considered the main requirements for smart phone application.***

Keywords: Time,Capacity,imagequality, key necessity andspatial domain

1. Introduction

Steganography is the skill or preparation of secreting a communication, image, or folder inside additional communication, image, or folder. Steganography contains the disguise of data in the interior supercomputer archives. In digital steganography, automatic transport network possibly will embrace steganography coding confidential of a transportation level, such as a folder file, copy file, database or procedure. Mass media archives are perfect for steganography communication since of their huge scope[1].In image steganography there is variety of steganography methods. This project will focus on some of important methods that relates to time, image quality, capacity as well as robustness to choose a method that justifies these factors and avoids doubt by assailant. The intimation of steganography is to outlaya safety objects as an inconclusive to handover confidential data forcefully in this knowledge of beating data. Moreover digital layout entities performance the imperative character for consuming as protection as well as conceals communication, similar image, video, audio and text file. [2]The word of Steganography is coming from a Greek, involves of two parts 'stega' and' nography' ,'stega' means covered and ' nography' means writing.[1]With increasing of mobile phone services, security of transmission message has one of the significant topics. Dissimilar procedures have been made for make safe the confidentiality of message and for protection the gratified of an information furtive [4].In recent times, hiding approach has opportunity to be roughly charity in the enhancement of info safe keeping. [1].

2. Spatial Domain Steganography

In spatial domain, the top-secretletter is embedded by straightaltering the pixel value of the cover image. Under are some of most important steganography approaches.

2.1 LSB Replacement

In LSB replacement technique, the bit of binary top-secretmemo is used to overmark the LSB of the protection image pixel. I.e. firstly, the secret message is transformed to binary bit watercourse. Secondly, the cover pixel value is converted to binary stream bit also. Finally, LSB of cover pixel is substituted by bit of secret message. As shown in Figure 1 the first three pixels value of cover image converted to binary bits and secret message convert to bits too. The first bit from secret message replace with LSB of first cover pixel ,second bit from secret message replace with LSB of second pixel and The third bit from secret message replace with LSB of third pixel.[2][3][12]

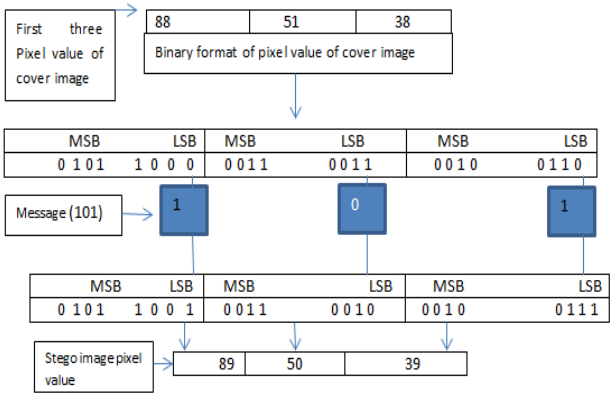

Figure 1: LSB replacement process [2]

2.2 Optimal Pixel Adjustment Procedure

OPAP method is used to minimize the distortion that happens to the cover image after the hiding process. This process will maintain the cover image quality without affecting the secret message. [3][5][6]

To start the hiding process the below steps must be completed

1) First the LSBs are substituted with the bits secret message
2) To give less error, the bits in the pixel are accommodated suitably before the hiding process
3) Let n be LSBs substituted in each pixel.
4) Let d= decimal value of the pixel after substitution.
5) d1 = decimal value of last n bits of the pixel.
6) d2 = decimal value of n bits hidden in that pixel.

If (d1-d2) <=(2^n)/2 then noaccommodate is made in this current pixel.
If (d1<d2) then d = d – 2^n
If (d1>d2) then d = d + 2^n.

This d is converted to binary and written back to pixel.
Below there are two examples of applying this method. Let n is three (3) for all three examples.

Example1: Embedding secret message (101) using OPAP method
Let the binary format of a secret message is (101), and (65) is a decimal pixel value of cover image. Then the Binary format of pixel is (0 1 0 0 0 0 0 1). Then replace the last three LSBs of pixel binary format (0 1 0 0 0 0 0 1) with secret message (101). The new pixel binary format will be (0 1 0 0 0 1 0 1) and the decimal pixel value will be (69). The value of d1, d and d2 will be d1=1, d=69 and d2=5. Now we find | d1-d2|<=2^n, |1-5|<= (2^3/2) in this example because first condition is true the value of pixel is left and we don't do anything as we explained in the algorithm of OPAP above.

Example 2 embedding secret message (111) using (OPAP)
Let the binary format of a secret message (111), and (40) is a decimal pixel value of cover image. Then the Binary format of pixel is (0 0 1 0 1 0 0 0), Then replace the last three LSBs of pixel binary format (0 0 1 0 1 0 0 0),with secret message (111).The new pixel binary format will be (0 0 1 0 1 1 1 1) and the decimal pixel value will be (47).The value of d1, d and d2 will be d1=0, d2=7 and d=47. Now we find | d1-d2|<=2^n, |0-7|<= (2^3/2). In this example the first condition is not true but the second condition (d1<d2) is true. The new pixel value will be (39) which is calculated by this formula d=47-8=39 as we explained in OPAP algorithm. In summary, instead of sending 47 as pixel value of Stego image 39 will be sent, and it is clear that 39 is nearest to the original pixel value (40) of cover image.

For retrieving the secret message the pixel value of Stego imageis converted into binary format, and the three LSBs (1st, 2nd and 3rd) of pixel binary forma are extracted from each pixel.

2.3 Inverted Pattern Method

This method is based on the concept of handling secret data before the hiding process. Before the hiding process each segment of secret message is decided to be inverted or not inverted after dividing the secret message into segments with equal lengths.
.below the steps of IP method
1-**S** is the string of the secret message to be hidden.
2-**R** is the replacement string of the cover image; R and S are equal in length
3-**S'** is the inverted pattern of **S**.
4- Divide the secret message into P parts with equal lengths.
For i=1 till p, where p is the number of parts of secret message , then compare between(Si ,Ri) and (S'i,Ri) for each part i in the p parts of secret message :

- If Mean Square Error **[MSE]** (Si,Ri) ≤**[MSE]** (S'i,Ri) that is mean (Si is near to Ri) then:
- 1- Use Si to be embedded.
- 2-Mark key(i) =0
- If MSE(Si,Ri) ≥ MSE(S'i,Ri) that is mean (S'i is near to Ri) then:
- 1-use S'i to be embedded.
- 2-Mark key(i) =1

End of loop when i=p. [7][8].
Below is an example of hiding secret message (1 0 1 10 1 1 1) using inverted pattern method.

87	19

1) Let assume the pixel value of cover image is
2) Assume we divide secret message into two parts, S1 (1 0 1 1) , S2 (0 1 1 1)
3) The inverted pattern of S1 and S2 are S'1(0 1 0 0) , S'2(1 0 0 0)
4) To find R1 we must convert pixel value (87) into binary format [0 1 0 1 0 1 1 1], then R1 is (0 1 1 1)
5) find MSE (S1,R1) and MSE(S'1,R1):MSE(S1,R1)=0.750 and MSE(S'1,R1)=0.250,therefore
1) Use S'1(0 1 0 0) to be embedded
2) Mark key (1) = 1
The formula of one dimensional vector MSE is given: [7]

$$E_i = \frac{1}{n}\sum_{j=1}^{n}(P_{(ij)} - T_j)^2$$

P and T are the two vectors, and n is the length of vector.
Note, we will flow the same steps for second parts of secret message S2 (0 1 1 1).
A stego image, key and length of string are needed for retrieving the secret message. A pixel value of stego image is converted to binary format. Then,Depending on the value of the key, the retrieved bits will either flip or not flip. Next, the retrieved bits are kept If the key is =0 or inverted if the key is =1. Length is used to determine numbers of bits are extracted from each pixel.

2.4 Mod 10 method

This method uses Mod 10 function for hiding the secret message in the pixel of cover image. This method needs a key to decide the embedding of the multiple sub-divisions of the secret message as shown in the steps below:

1) The secret message is divided into segments with 3 bits length and each time 3 bits will be hidden into the pixel value. Each three bits is taken in its binary format from the secret message. This will be converted to decimal numbers and stored in let say variable x.
2) Let P be a pixel value in the cover image.
3) Calculate d1 from the formula d1= (P mod 10)-x, and find d2 from formula d2= (P mod 10)-(10-x).

If (d1<d2) the new value of pixel will be calculated using this formula:
P= (P- (P mod 10)) +x and mark key =0
Else the new value of pixel will be calculated using this formula
P= (P- (P mod 10)) + (10-x) and mark key =1

For retrieving the key and Stego image are needed. Based on key value either formula 1 or 2 is used to extract the secret

message from the pixel value. If key=0 we use formula 1 otherwise we use formula 2.
Formula 1: data= (P mod 10)
Formula 2: data=10-(P mod 10). [9]

2.5 Parity Method

The concept of parity checker is used by (Yadav, Rishi, & Batra)[10].Each pixel value either contains odd parity or even parity. Odd parity means the number of 1's in pixel value is odd, however even parity means the number of 1's in pixel value are even. This method hides 0 bits from secret message into the odd parity bit of the selected pixel. If the selected pixel value does not have an odd parity bit, it adds or subtracts one to make the pixel value an odd parity. However, 1's from secret message are hidden in the selection pixel of even parity, if the selection pixel value is not even one is added or subtracted to made pixel value even. For retrieving, the Stego image and key selection are needed. Using selection location we determine the location of the pixel. 0's are extracted if the parity of the pixel value is odd and 1's if parity of pixel is even. The process of extracting is going through all pixels that are used in hiding process.

2.6 Basic Fibonacci

"The classical Fibonacci numbers introduced in the 13th century by Leonardo of Pisa" .The sequence Fibonacci numbers is defined by the relation F (N) =F (N-1) +F (N-2).
Where F (0) =1 and F (-) =0. [11]

Fibonacci sequence is [1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377,… etc.]. It can be used to represent any numeric value like binary representation. If N is the number of bits allocated to represent any numeric value then it will be easy to distinguish between binary representation and Fibonacci representation because in binary N is 8 bits are used while in Fibonacci N is 12 bits.As a result, this sequence can be used in steganography. It uses Fibonacci sequence to represent the pixel value instead of binary representation. I.e. 12 bits are used to represent the values from (0,255) instead of using 8 bits in binary system. The bit of secret message is written over the bit plan of the cover pixel .i.e. the secret message is converted to binary bit stream. The pixel value of the cover image which is selected for hiding the secret message is converted to Fibonacci representation, and then the bit plan of the pixel value of the cover image is replaced with the secret message. Finally, decompose the Fibonacci representation into the pixel value of the cover image. To retrieve the Stego image, the key of selected pixels are needed. The value of the selected pixel is converted to Fibonacci representation and secret message is reconstructed from the cross pounding bit plan [1],[2].accordign to (Zainalabideen,2014)[1],[2]an improving and optimal using of fibonacci LSB method which are appliaed in image steganography,in this project we will implement a new proposal of fibonacci by uisng 11 bits representaion and set zeros to the both nighbour of bit planes which were seprately used in previouse works in [1][2].

3. Testing and Conclusion

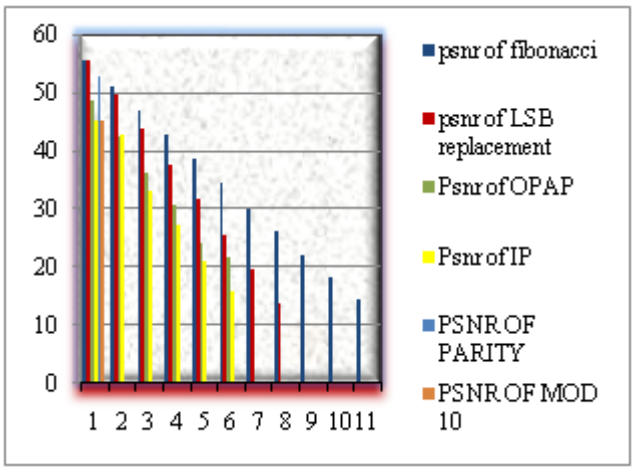

Figure 1: PSNR of all methods

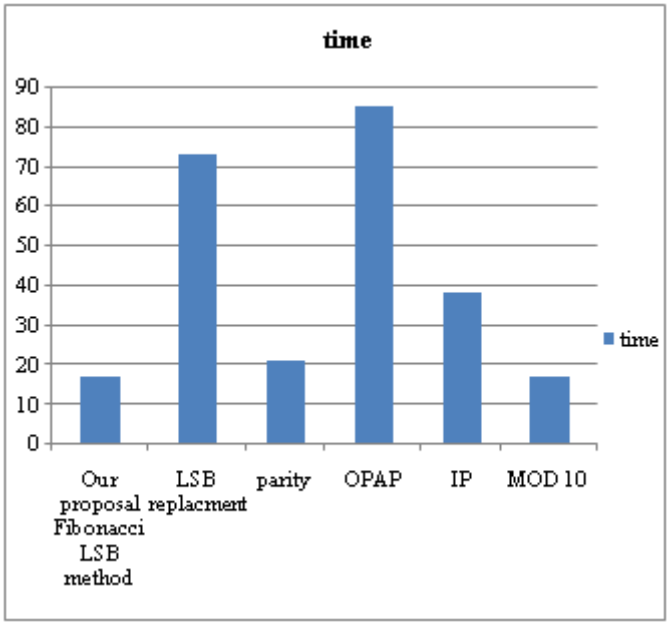

Figure 1: Time of all methods

1. In terms of stego imagequality (PSNR) it is clear from figure 1 our proposal Fibonacci method scored better PSNR for all levels of bit plan. However, OPAP and IP methods could also be acceptable.Other applications that check the quality of the stego_image could as well use these methods.
2. In terms of time, figure 2 shows that our proposal, mod 10 and parity methods were better compared with the other methods. This will make it very suitable to be implemented in smart phones.
3. In terms of bit plan, the Fibonacci method is the best because it allows flexible bit plans .i.e. 11 bits while binary representation is 8 bits. For that reason, Fibonacci representation do less change to the pixel value by using the same bit plane with binary representation and Fibonacci means less distortion to the cover image resulting in a high quality stego image.
4. OPAP, IP and mod 10 are the best methods in terms of capacity. However, the long-time and key required make these methods are not so suitable for windows phone.

5. In terms of key necessity, LSB replacement and my proposal Fibonacci LSB is the best since these procedures are practicaldeprived of a key unlike the other steganography methods where a key is needed for embedding and retrieving. This releasesenquiries for in what way a key can guided to the receiver side.

For all these reasons my proposal, Fibonacci LSB method maybe considered the best choice to develop a steganography application under windows mobile phones in terms of time and quality of stego image and key necessity. For future work the whole apps under windows mobile phone using Fibonacci LSB will be done.

References

[1] ZainalabideenAbdualSamad Rasheed ''Steganography Technique for Binary Text Image'' International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064,2015
[2] ZainalabideenAbdualSamad Rasheed,Improving Classical Fibonacci in Steganography, International Journal of Advanced Research in Computer Science and Software Engineering(ijarcsse) ISSN: 2277 128X, 2014
[3] ZainalabideenAbdualSamad Rasheed, ''comparative study For steganography techniques'' International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, 2015
[4] Morkel, T.,Eloff, J.,&Olivier, M. (2005) .An overwiew of image steganography
[5] Hong, W., & Chen, T. (2011). A Novel Data Embedding Method Using Adaptive Pixel Pair Matching. *Information Forensics and Security, IEEE Transactions on*(99), 1-1.
[6] Chan, C., & Cheng, L. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition*, *37*(3), 469-474.
[7] Yang, C. (2008). Inverted pattern approach to improve image quality of information hiding by LSB substitution. *Pattern Recognition*, *41*(8), 2674-2683.
[8] Kamal.deep. (2011). Relative Antropy Based Analysis of Image Steganography Techniques. *International Journal of P2P Network Trends and Technology*(99), 1-1.
[9] Amirtharajan, R., Akila, R., & Deepikachowdavarapu, P. (2010). A Comparative Analysis of Image Steganography. *International Journal of Computer Applications IJCA*, *2*(3), 41-47.
[10] Yadav, R., Rishi, R., & Batra, S. (n.d.). A new Steganography Method for Gray Level Images using Parity Checker. *International Journal of Computer Applications (0975-8887) Volume*.
[11] Picione, D., Battisti, F., Carli, M., Astola, J., & Egiazarian, K. (2006). A Fibonacci LSB data hiding tecnique.
[12] Ker, A. (2005). Steganalysis of LSB matching in grayscale images. *Signal Processing Letters, IEEE*, *12*(6), 441-444.

Author Profile

ZainalabideenAbdullasamd Rasheed University of kufa, Education of College, Najaf /Iraq. Has a BSc (Baghdad University, Iraq), and MSc (Buckingham university, UK).he has a long experience in teaching various computing practical courses at Baghdad university .at AL Kufa university, Mr. Rasheed teaches different courses like computer organization, operating system and computer architecture .he supervises undergraduate projects. He interest in data security (steganography and cryptography) and digital image processing (biomedical image and edge detection, de-noising images), Iraq.