International Journal of Engineering Research and General Science Volume 4, Issue 6,November-December, 2016
ISSN 2091-2730

Steganography By Use Binary Operations

Orooba Ismaeel Ibraheem Al-Farraji

AL-Nahrain Universty-College of Medicine

orooba1@gmail.com

Abstract- Steganography is the art and science of hiding messages or other secret information in a bunch of carrier information. This paper presents a new idea of robust steganography using Adding operation between image-pixel LSB (Least Significant Bit) value and secret message- character ASCII-binary value and use two keys in the extraction of secret text to enhance the power of concealment and the difficulty of breaking.

Keyword: Steganography , Binary operation, Hiding information , LSB , Image Steganography, 24 Bit Color Image

1.Introduction

The idea of information hiding is nothing new in the history. As early as in ancient Greece there were attempts to hide a message in trusted media to deliver it across the enemy territory. In the modern world of digital communication (2) , there are two ways to do that .

The first method is to encipher the message in such a way that no one else can read it. In this case, the encryption is obvious, and when intercepted, it is clear that the sender and the receiver are communicating secretly and people may be able to tell that a secret message is being transmitted; they just can't read it. This technique is called cryptography (1).

The second method is to hide the fact that a message is being transmitted. Steganography is an extremely useful method for covert information transmission (3). Steganography is the data hiding technique which allows hiding secret message or image within a larger image or message such that the hidden message or an image is undetectable (4). Cryptography provides the means for secure communications; steganography provides the means for secret communication. Steganography combined with cryptography would be the most secure way to go(1). Because the existence of an encrypted communication draws attention to it, hiding it in another le uppers up your .

2. Types of Steganography

The steganography is having following types as shown in fig.1

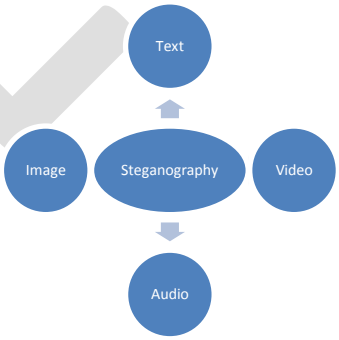

Fig. 1: Types of Steganography.

In the first type of Steganography, the cover media will be the “text cover”. The basic advantage of preferring text steganography is that, it requires less memory and Steganography simple communication. The message is embedded in cover text file by using some embedding algorithm, so that the “stego text”or “cipher text” is formed. This stego text is then sent to the receiver side through transmission channel. This stego text is processed by the extraction algorithm by using “secret key” or “stego key”. Among four types of steganography, image steganography is the most popular technique. We take the detail look on this in the next

section. The next technique is hiding the secret message by using Audio file as cover media. In the video steganography, we use the video file as cover media to embed the secret message (8).

3-Techniques of Image Steganography

There have been a large embedding techniques proposed number of steganography in the literature. These techniques modify the cover-image with different approaches as well as constrains. But all embedding techniques share the important goal of maximizing the capacity of the stego channel. In other words their aim is to embed at highest possible rate while remaining undetectable to steganalysis attack. All the popular data hiding methods can be divided into two major classes: spatial domain embedding and transform domain embedding(9). Next we will review them .

A. Spatial Domain Spatial domain techniques embed information in the intensity of the original image pixels directly. Basically least significant bit (LSB) method is used where it replaces the least significant bit of original pixel with the message bit (10).

B. Transform Domain Transform domain also known as frequency domain where images are first transformed then the message is embedded in the image. Discrete cosine transformation (DCT) technique is used in JPEG images to achieve compression. DCT is a lossy compression transform where the cosine values cannot be generated as original, because DCT alter values to hide the information(9).

3-1. Least Significant Bit

The LSB based technique is mainly uncomplicated and simple approach through which message bits are embedded within the least significant bits of cover image (7). In the LSB steganography method and for the purpose of covering the secret messages, the least significant bits of the cover-image are exploited. Thus, this method is considered one of the most common techniques that include the standard LSB replacement [6]. Consider the following cover-image and secret message in bits. The LSB replacement alternates the last bits of the cover image with each bit belong to the messages that are required to be hidden (5).

3-1.1. LSB Method For 24 Bit Color Image

In the case of 24 bit color image each pixel is composed of RGB values and each of these colors requires 8-bit for its representation. [R (8 bits), G (8 bits) , B (8 bits)].

Example:

The letter ‘A’ has an ASCII code of 65(decimal), which is 1000001 in binary.
It will need three consecutive pixels for a 24-bit image to store an ‘A’:
Let’s say that the pixels before the insertion are:
10000000.10100100.10110101, 10110101.11110011.10110111, 1100111.10110011.00110011
Then their values after the insertion of an ‘A’ will be:
10000001.10100100.10110100, 10110100.11110010.10110110, 11100110.10110011.00110011

4- Binary Operation

Binary arithmetic is essential part of all the digital computers and many other digital system. The arithmetic of binary numbers means the operation of addition, subtraction, multiplication and division. Binary arithmetic operation starts from the least significant bit i.e. from the right most side.

4-1.Binary Addition

There are four steps in binary addition, they are written below

0 + 0 = 0
0 + 1 = 1
1 + 0 = 1
1 + 1 = 0 (carry 1 to the next significant bit)

In fourth case, a binary addition is creating a sum of (1 + 1 = 10) i.e. 0 is written in the given column and a carry of 1 over to the next column.

5. The Proposed Scheme

The new proposed system adding the secret text in image, use addition operation to insert secret text to LSB in pixels of image .

We use in our case an 24-bit image and use Math lab in execute the system and use two keys.

5.1- The Proposed Scheme Operation

The Add secret text of new system has many operations:

1- Input the secret text to be hidden that can be done by open new file and entered directly.
2- Convert secret text to Ascii system than to binary system , each letter consists 8 bit .

3- Input image (cover) to system

4- Save header of Image in a file and save the palette value of body in another file.
5- Save palette file in array and save binary secret text in another array.
6- Add the first bit in first letter from secret text which consists of 8 bit to first pixel in image by adding bit-text to first LSB in palette of image , if LSB equal 1 and bit-text equal 1 the result equal 0 With the neglect of the rest
And if LSB equal 0 and text equal 1 the result equal 1 and so on.

7- Save the locations of the bits which change values in array.
8- Every letter in secret text need two pixels and two colors from third pixel .
9- We use two keys in this system the key length of text and the length of array which content the location of bits which change values .

10- Save the two keys in end the palette of image by replaces LSB in palette with keys .

5.2- The Algorithm of The Proposed System

The following steps describe the algorithm:

Algorthim 1: Input the Secret text

Input : Secret text

Output : Binary Array

Step1- input text

Step2- convert text to ASCII system

Step3 – convert ASCII system to binary number

Step 4- save binary number in Array1

Step5 : End

Algorthim 2: Input the Image

Input : Image

Output : Array of binary code

Step1- Open Image (the bmp-file) Operation

This operation will open the bmp file and save header in a file and save the palette value of body in another file.

Step2- save the value of pixel palette in array2

Step3-End

Algorthim 3: Adding array1 of binary to array2 of pixels

Input : Array of binary code, Array of pixels

Output : Array of Adding two arrays , Array of locations bits that change

---

Step1- for i= 1 to length of the secret text

Step2-add the first bit from array1 to eight bit in array2

Step3 – If change the bit in palette then

Array3 = location of bit

endif

Step 3 – Shift seven bits

Step4- next i

Step5 : End

Algorthim 4: Hide the key1 , key2 and array3 in end palette

Input :key1, key2,array3

Output : array2 after hide

Step1 : Replace the LSB in last two pixels in palette with key1

Step 2: Replace the LSB in before last two pixels palette with key1

Step 3: for j= end of palette -4 to (end of palette -4)-length of array3

Tow LSB in array2[j] = array3

Next j

Step4 :end

Algorthim 5: extract the image again

Input : array2 after adding

Output :image

Step1 : Back array2 to Platte file

Step2 : Back header to Platte file

Step3 : This change is unnoticeable because the number of bits that change is small and in LSB.

Step4 : End

6-Extracting The Secret

The Extracting secret text of new system has many operations

1- Save header of Image in a file and save the palette value of body in another file.
2- Save the palette value in array4
3- Extract the keys from the end array4
4- Depending on the key extract the secret text by if the LSB change the text secret 1 else the secret text 0

6-1. The Algorithm of The Extracting

Algorithm1: Split the image

Input : image after hiding secret text

Output : Array4

Step1- Open Image (the bmp-file) Operation

This operation will open the bmp file and save header in a file and save the palette value of body in another file.

Step2- save the value of pixel palette in array4

Step3-End

Algorthim 2: Extracting the keys and array3

Input: Array4

Output: keys ,array3

Step1: Read arrray4

Step2: key1= LSB in last two pixels in palette

Step3: key2= LSB before two pixels in palette

Step4: for j= end of palette -4 to (end of palette -4)-length of array3

array3 =Tow LSB in array2[j]

Step5: End

Algorthim 3: Extracting The secret text

Input : array3, keys ,array4

Output : secret text

Step1: for I=1 to key1

Read LSB in array4

If location of LSB in array3 then

Secret text = 1

Else

Secret text = 0

End if

Next I

Step2 : convert secret text from binary to ascii

Step 3: convert asci to text

Step 4 : print secret text

Step 5: end

7. Experimental Results

The proposed system has been built using Math Lab and can run on Pentium 3 computer and above, the setting of screen must be 800 X 600.

The results of the proposed system has been illustrated in the following

Example:

Fig2:image1

We add text1 " this is nice picture" in Image1

Fig.3: Image1 adding secret text1

8-Experimental Results And Performance Analysis

Use PSNR Function to Test the results

Signal to Noise Ratio (PSNR) is generally used to analyze quality of image, sound and video files in dB (decibels). PSNR calculation of two images, one original and an altered image, describes how far two images are equal.

MSE: Mean-Square error.
x: width of image.
y: height.
x*y: number of pixels (or quantities).

This function displays the PSNR (peak signal-to-noise ratio) between two images. The answer is in decibels (dB).

PSNR is very common in image processing. A sample use is in the comparison between an original image and a coded/decoded image. Typical quoted PSNR figures are in the range +25 to +35dB.

The syntax for this file is PSNR(A,B), where A and B are MATLAB Intensity Images, with matrix-elements in the interval [0,1]

$$PSNR(dB) = 10 * \log(\frac{255^2}{MSE})$$

$$MSE = \sum_{i=1}^{x}\sum_{j=1}^{y} \frac{\left(\left|A_{ij} - B_{ij}\right|\right)^2}{x * y}$$

.**PSNR formula**.

the PSNR (Peak Signal to Noise Ratio) value of the image is calculated using the equation and if the PSNR value is greater than 35dB, the cover image is within acceptable degradation levels.

$PSNR = 10 \times \lg((2n-1)2 / MSE)$ (3)

Where *n* means the number of bits per sample value, the *MSE* represents mean square error between the host image and the cover image.

By using Matlab we input fig.(2) and fig.(3) to function PSNR the results equal 30.100 db and this value acceptable.

9. Conclusion

The proposed system proved to be a good system used to hide a text in image by Adding Binary value of text to value of LSB in palette with this operation will change small number from LSB.

- In the proposed system change small number from LSB that's unnoticeable

- The proposed system proved to be easy to use and efficient in terms security and help to save text in image.

- We can develop the system encodes the secret hide text before and this is what it will do in the future.

REFERENCES:

[1] Houda JOUHARI ,"New Steganographic Schemes Using Binary and Quaternary Codes", Le 1er juillet, 2013.

[2] Vijaya Bhanda ," A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image ",International Journal of Computer Applications (0975 – 8887), Volume 64– No.20, February 2013 .

[3] Mekha Jose , Kottayam Dst , "Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality", International Journal of Science and Research , Volume 3 Issue 9, September 2014 .

[4] Padmini.K, Radhika .D. K ," Least Significant Bit algorithm for image steganography ", International Journal of Advanced Computer Technology (IJACT) ,Volume 3, Number 4, 2014 .

[5] Ankit Gupta, Rahul Garg , "Detecting LSB Steganography in Images", , rahuldotgarg.appspot.com/data/steg.pdf, 2016

[6] Chan, C.-K. and L.-M. Cheng, "Hiding data in images by simple LSB substitution. Pattern recognition", 37(3): p. 469-474, 2004.

[7] Mohammed Abdul Majeed, Rossil Awati Suliaman, "An Improved LSB Image steganography Technique Using Bit-Inverse In 24 Bit Color Image", Journal of Theoretical and Applied Information Technology 20th October , Vol.80. No.2, 2015.

[8] Sneha Bansod , Gunjan Bhure, "Data Encryption by Image Steganography", International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 4, Number 5 , pp. 453-458,2014 .

[9] A.P. Gurudev Jangra , M.Tech. Scholar ," Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014

[10] V. K.Shandilya Student, A.P, Sipna, "Spatial and Transformation Domain Techniques for Image Enhancement", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 1, Issue 2, November 2012

,