Comparative Study for Steganography Techniques

Zainalabideen Abdul Samad Rasheed
Assistant lecturer, Computer Science, Education College, Kufa University, Iraq

Abstract: Various steganography techniques for hiding information have been created. Steganography is the art or science of hiding data in such a means that even the receiver cannot estimate the presence of the unseen data except he is responsive of the accomplishment of hiding letter. The whole awareness of steganography is to guarantee that the transferred message is fully covered; by this means make sure that the message is reachable only to the intentional receiver. Steganography generate a protected channel to exchange the top-secret information between two parties. In this project, several steganography techniques have been analyzed. The main idea of the project is to introduce an overview of image steganography to identify the requirements of a good steganography approach the terms of good approach is application depended. In general, this methodology should be able to hide a secret message in an image file (cover image) and should also be able to extract the hidden information from the cover image.

Keywords: Capacity, Jpeg compression, Stego -image quality, spatial domain and frequency domain

1. Introduction

Steganography is a technique for beating facts or information within a digital protection media without leaving indication. Leaving mark means the alteration to the cover media might be observed by an assailant and that income the scheme is cracked.” If there exists a steganalytic algorithm which can guess whether a given media is a cover or not with a higher probability than random guessing, the steganography system is considered broken.” [3]

In image steganography there is variety of steganography methods. This project will focus on most important methods that relates to image quality, capacity as well as number of bit planes to choose a method that justifies these factors and avoids suspicion by attacker. The clue of steganography is to expenditure a protection entity as a intermediate to transfer top-secret data tightly. In this science of hiding information digital format objects play the important role for using as a cover as well as secrete message, like image, video, audio and text file. The word of Steganography is coming from a Greek, consists of two parts ‘stega’ and ‘nography’, ‘stega’ means covered and ‘nography’ means writing. Security of information has one of the important issues of communication due to a huge use of internet. Different techniques have been created for securing the privacy of communication and for keeping the content of a data secret.[4]. In recent times, steganography has turn out to be broadly used in the improvement of information security. Digital media like image, video, audio and text can be used to hide top-secret.

2. Literature View

Steganography can be divided into two domains: Spatial domain and Frequency domain, figure3 shows the most important steganography methods which are grouped in terms of domain, type of cover image formats as well as number of embedding bits per pixel:

a) in terms of domain, Discreet Cosine Transform (DCT), Integer Wavelet Transform (IWT) and Discreet Wavelet Transform (DWT) steganography can be applied in frequency domain while the rest methods work in spatial domain.
b) in terms of cover image format, SLSB and 8 bits applications methods can be applied in an RGB format only, while all other methods could be applied on any type of cover format. These 2 methods cannot be compared to the other methods due to the specific type of cover format (RGB only).
c) in terms of how many number embedding bits per pixel and handling secret message before embedding. LSB replacement, LSB matching, Fibonacci LSB and parity methods are embedded one bit per pixel and do not handle secret message before embedding. However, Optimal Pixel Adjustment procedure (OPAP), Inverted Pattern (IP), Inverted Pattern using relative entropy (IPR), stream ones and zeros (stream 1’s and 0’s) and mod 10 methods are embedded 3 bits together per pixel and even handled secret message before embedding (handled secret message means change the pattern of secret message before embedding process)
3. Spatial Domain Steganography

In spatial domain, the secret message is embedded by directly changing the pixel value of the cover image. Below are some of most important steganography methods.

3.1 LSB Replacement

In LSB replacement method, the bit of binary secret message is used to overwrite the LSB of the cover image pixel. I.e. firstly, the secret message is converted to binary bit stream. Secondly, the cover pixel value is converted to binary stream bit too. Finally, LSB of cover pixel is replaced by bit of secret message. [1],[2]

3.2 LSB Matching

This technique is more robust than LSB replacement against warden, because does not work straight forward, the bit of the secret message is matched with the LSB of the cover pixel, if it does match, the pixel value remain the same, if it does not, the pixel value of the cover image will be either increment or decrement by one randomly. [5]

3.3 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. [6],[7]

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 no accommodate 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.

3.4 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. [8],[9]

3.5 Inverted Patterns Using Relative Entropy (IPR)

This approach uses the same idea of IP method. However, a relative entropy formula is used instead of MSE. Relative entropy ’is a non-symmetric measure of the difference between two probability distributions P and Q. ’. [8].It is used by replacing the MSE in 3.4 by the formula below :[10]

\[ D(p \parallel q) = \sum_{x \in X} p(x) \log \frac{p(x)}{q(x)} = E_p \log \frac{p(X)}{q(X)} \]

3.6 Stream of 1’s and 0’s Method

This method is proposed by (Amirtharajan)[10] tries to count the consecutive 1’s and 0’s appearing in a binary format of the secret message. Firstly, the number of 1’s that appear before a 0 is counted. Then the number of 0’s that appear before a 1 is also counted. Afterwards, the number of 1’s will be hidden into pixels in the odd columns and 0’s into even columns by using (mod 10) to the pixel value. If the number of 1’s or number of 0’s is greater than 10, then (mod 100) is used instead of (mod 10) for the hiding process. Key are required to know if we need to use mod 10 or mod 100 in retrieving process.

3.7 Pixel Value Difference (PVD) method

PVD is based on using the difference between the pixel values of the cover image in hiding the secret message. This method provides a better quality for the Stego image and also provides high hiding capacity.
1. Let w be the value of the pixel in the cover image and y be the secret message to be hidden in binary format.
2. Nothing is done to the first row and column in the cover image.
3. The second row and column will be the current pixel. This pixel is used for hiding the secret message. Next, find the difference in binary between current pixel and the pixel to the left. This will be x1.
4. Calculate the difference in binary between the current pixel and the pixel on the top. Let this be x2. Let l1 be the length of x1 and l2 is the length of x2.
5. Extract the data from variable y with six different lengths (11-1, 11, 11+1 and 12-1, 12, 12+1).
6. Store these in the same order in an array of string and name it as xif[j], where j is from 1 to 6.
7. Then, find whether x1 or x2 is nearer to any of the elements in array xif[] and name it as min.
8. Finally, if min is nearer to x1, the difference between the current pixel value and the pixel to the left is used to hide the secret message, and mark key by 0. If min is nearer to x2, the difference between the current pixel and its top pixel is used to hide the secret message, and the key is marked as 1. The number of bits hidden is stored in the lower pixel of the current pixel. [11],[10],[12]

3.8 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. The secret message is divided into segments with 3 bits length and each time 3 bits will be hidden into the pixel value by using mod 10 function.[10]

3.9 SLSB steganography technique
This is a new way to improve the usability of LSB method for hiding information. This method is based on selecting one of the three color channels which are red, green, and blue. Then secret message will be hidden in each pixel of the chosen color. In most steganography, methods that uses LSB hides secret message using pixel values in all three color channels. However, in SLSB only one color channel will be used for hiding the secret message. The advantage of SLSB is that this method keeps two of the three colors channels unchanged. This will make the Stego image nearly similar to the original image. It actually reduces the doubt of finding hidden information in Stego image. Also it makes it very difficult to distinguish between original image and image stego. Table 2 and 3 shows resulting pixel values of the color channel, a 24 bits cover image, a RGB (Red, Green, and Blue) i.e. an 8 bits for each color. Pixel values in the resulting Stego image in using SLSB shows less change compared to the LSB method. Let a pixel value be (A8A8A8) then the binary format for Red, Green and Blue is 10101000-10101111-10101000. Let the secret message be (111) in binary format. The binary format of the pixel value after hiding secret message (111) using LSB is 10101001-10101001-10101001. However, the binary format of the pixel value after embedding secret message (111) using only the Green color is 10101000-10101111-10101000. From table (2) we can see the difference is 65793 for the pixel value after hiding ones to the LSB of each color of pixel value. While from table (3) we can see the difference is 1792 for the pixel value after hiding (111) to the Green color. (And the table show also the change to the green color is 7).[13]

3.10 Parity Method
The concept of parity checker is used by (Yadav)[14] and (Kamal)[9]. 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 make 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.

3.11 Application of LSB Based Steganography Technique for 8-bit Color Images
According to (Juneja)[15] his proposal particularly applies to LSB on 8-bit image color. It starts to convert image from 24-bit image color to 8-bit image color by creating a color map. This is created such that the maximum number of colors in this color map is 256 colors, while the maximum number of colors in original image is 16777216. The process of creating a color map is by dividing the original image into (15 x16) quadrants as in Figure (6). Then randomly select one color from each quadrant. Once a color has been selected within a quadrant, it is compared with every color in the color map. If the color is already in the color map it will be discarded otherwise it will be added to the color map. This operation can be applied 5 times to choose colors that differ enough from all colors in the color map. The new 8-bit image color is created by scaling down each pixel from the original image 24-bit image color with the closest color from the color map. The secret message is hidden in the image by sequentially changing the LSB bit of the image. It will be difficult to recognize these different happenings by hiding or by converting operation and especially when the original 8-bit image is not there to compare with the Stego image.
3.12 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 \( F(-) = 0 \). [16]

Fibonacci sequence is \([1,1,2,3,5,8,13,21,34,55,89,144,233,377,\ldots\text{ etc.}]\). 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]

4. Frequency Domain

4.1 Discrete Cosine Transform (DCT) method

DCT is one of the transformation tools used in steganography in the frequency domain. DCT transformation transforms an image from spatial domain to frequency domain. It divides an image into different parts with different frequency components. DCT is widely used in image and video compression.

The following steps are explained using DCT:

First, the cover image is divided into 8X8 blocks of pixels, each block is 64 pixels. Secondly, a two dimensional DCT is applied into each block separately. Then the quantization process is applied into each block to scale the DCT coefficients of each block using quantization table. Next, LSB of the DC coefficient is calculated and replaced with the bit of the secret message. Finally, inverse DCT is applied to each block and Stego image is constructed. For retrieving the secret message, the same steps are applied to Stego image and secret message are reconstructed from the extracting the LSB of the DC coefficient. [17]

4.2 Discrete Wavelet Transform (DWT)

(Sarkar, Nag)[18] They developed steganography method based on DWT (Discrete Wavelet Transform). This method support high secure hiding process. Below are the steps for hiding secret message

1. The secret message will be encoded using Huffman table into stream of encoding bits
2. A cover image will be decomposed by using Haar Wavelet Transform into four sub-band(LL, LH, HL, HH)
3. Each time three bits from secret message will be selected and will be convert to decimal value let say \( Bi \) (i.e. the decimal value will be at the range of \([0..7])\)
4. Select one of the three high sub-bands (LH, HL, and HH) for hiding process. Name it F.
5. Hide the decimal value of the secret message in the coefficients of F using the formula below \( F=F-(F \mod 8) + Bi \), where \((F \text{ is the selected sub-band})\).
6. A stego image will be generated after applying the Haar inverse DWT.

4.3 Integer Wavelet Transform (IWT)

(Bhattacharyya)[19] Presented specific based image steganography for sending and receiving information more securely between two partners by applying the concept of secret key for verification process. First, the message is encoded using integer wavelet transformation for a more secure process. Second, the secret key is generated from the encrypted message. Then using normalization cut, the cover image is segmented in different cuts. The encrypted message is segmented into the parts with the same number of cuts too. Then each parts of the message are embedded on different cut of the cover image using LSB replacement. As a result, different stego objects will be produced. These stego objects will be combined into one stego image which will be sent to the receiver side. The inverse process is being applied for retrieving process.

5. Factors of Evaluation

The most important evaluation criteria which are used to compare steganography methods:

a) Invisibility(quality of stego-image): It is an important factor that reflects the strength of steganography method for producing a stego image unnoticed by human eyes

b) Capacity means allowable size of the cover image which can be used for embedding process

c) Bit plan means how many bits are available for use in the embedding process. E.g. for binary representation each value will be represented by 8 bits. Based on steganography methods some of them allow using all 8 bit plans from LSB to MSB while some methods do not allow a full 8 bit plan to use for embedding process. For
Fibonacci representation 11 or 12 bits could be used for represent pixel value.

d) Time means the time of hiding and retrieving processes.

e) Modification through channel means the modification could happen. Like loss compression i.e. how is the technique immunity against channel modification like jpeg compression.

f) Complexity of steganography algorithm

Table 1: a comparative of spatial domain methods which can be apply on all type of images

<table>
<thead>
<tr>
<th>Method</th>
<th>Capacity</th>
<th>Time</th>
<th>Number of bit planes</th>
<th>Key requirements</th>
<th>Key based on</th>
<th>Jpeg affect in retaining secret message</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSB replacement</td>
<td>Bit per pixel</td>
<td>short</td>
<td>8</td>
<td>Not necessary</td>
<td>Based on LSB</td>
<td>Negative</td>
</tr>
<tr>
<td>LSB matching</td>
<td>Bit per pixel</td>
<td>short</td>
<td>3</td>
<td>Not necessary</td>
<td>Based on LSB</td>
<td>Negative</td>
</tr>
<tr>
<td>Fibonacci LSB</td>
<td>Bit per pixel</td>
<td>short</td>
<td>12</td>
<td>Not necessary</td>
<td>Based on LSB</td>
<td>Negative</td>
</tr>
<tr>
<td>OPAP</td>
<td>3 bits per pixel</td>
<td>long</td>
<td>8</td>
<td>necessary</td>
<td>Based on LSB</td>
<td>Negative</td>
</tr>
<tr>
<td>IP</td>
<td>3 bits per pixel</td>
<td>long</td>
<td>8</td>
<td>necessary</td>
<td>Based on LSB</td>
<td>Negative</td>
</tr>
<tr>
<td>IP relative entropy</td>
<td>3 bits per pixel</td>
<td>long</td>
<td>8</td>
<td>necessary</td>
<td>Based on LSB</td>
<td>Negative</td>
</tr>
<tr>
<td>PVD</td>
<td>3 bits for two pixels</td>
<td>long</td>
<td>3</td>
<td>necessary</td>
<td>Negative</td>
<td></td>
</tr>
<tr>
<td>Mod 10</td>
<td>3 bit per pixel</td>
<td>Very short</td>
<td>3</td>
<td>necessary</td>
<td>Negative</td>
<td></td>
</tr>
<tr>
<td>Stream f's and 0's</td>
<td>3 bit per pixel</td>
<td>long</td>
<td>3</td>
<td>necessary</td>
<td>Negative</td>
<td></td>
</tr>
<tr>
<td>Parity</td>
<td>1 bit per pixel</td>
<td>Very short</td>
<td>3</td>
<td>necessary</td>
<td>Negative</td>
<td></td>
</tr>
</tbody>
</table>

6. Conclusion

In terms of most important factors which were used in this project, it is difficult to make a concrete decision comparing between steganography methods because there is conflict between these factors. Firstly, increase the capacity will case decrease the quality of stego –image. Secondly, keep the quality of stego- image by using the low level of bit plane case loss the information if the cover image goes through lossy compression like jpeg compression. Moreover, Increase the complexity of algorithm will increase the time of steganography process. Therefore choosing the good algorithm is application depended.

1. In terms of quality of stego image, LSB, parity, LSB matching and Fibonacci methods consider the best due to less change to the cover image one bits per pixel.
2. In terms of time: Table shows that mod 10 and parity are better compared with the other methods. This will make it very suitable to be implemented in real time application.
3. In terms of bit plan, table 1 shows Fibonacci method is the best because it allows flexible bit plan, the representation of Fibonacci bits gives flexible change to pixel value more than the normal binary bitwise. In binary bit representation each byte can be represented by 8 bits for the value from 0 to 255 (1,2,4,8,16,32,64,128) while in Fibonacci each byte can be represented by 12 bits using Fibonacci series 1,2,3,5,8,13,21,34,55,89,144,233.as result,Fibonacci do less change to the pixel value means less distortion to the cover image resulting in a high quality stego image[1],[2]

4. OPAP, IP and mod 10 are the best methods in terms of capacity. Therefore, applications that need bigger capacities can use these methods. Like hiding huge data need bigger cover file.

5. In terms of key necessity, table 1 shows LSB replacement Fibonacci LSB is the best because these algorithms are applied without a key unlike the other steganography methods where a key is needed for embedding and retrieving. This opens questions for how a key can sent to the recipient side.

6. Jpeg compression: table 1 shows LSB replacement, Fibonacci, OPAP, IP and PVD are based on level of bit plane i.e. as long as use the high bit plane the effect of compression will decrease.

7. Complexity: in frequency domain DCT, DWT and IWT more complex than all methods which works in spatial domain and make these methods suitable for application mention to the complexity of steganography algorithms.

References


Author Profile

Zainalabideen Abdulasamad 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).