A Survey on Different Steganographic Techniques

Haritha H[1], Anish Kumar B[2]

[1]MEA Engineering College, State Highway 39, Nellikunnu-Vengoor, Perinthalmanna, Malappuram, Kerala

[2]Assistant Professor, MEA Engineering College, State Highway 39, Nellikunnu-Vengoor, Perinthalmanna, Malappuram, Kerala

Abstract: ***Steganography is basically the art of secretly hiding data or message in any cover medium such as an image, audio or video. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data. In this paper gives an overview of different steganographic techniques such as histogram Shifting based Reversible Data Hiding Scheme, Reversible Data Embedding Using a Difference Expansion, An LSB Data Hiding and compare these methods according to PSNR, MSE and SSIM.***

Keywords: Stegnography, LSB, DE, Histogram Shifting, PSNR, MSE, SSIM

1. Introduction

Internet Technology has led to the need of high level security of data transmission. Steganography plays a major role in society. In ancient Greece, people used to write on wax-covered tablets. Another form of steganography is in null ciphers, or unencrypted text messages. Recently, computerized steganography has become popular. Water marking and finger printing are the two technologies related to steganography. Text Steganography consists of hiding information inside the text files. Image Steganography is simple and secure technique for hiding the data. Hiding the data by taking the cover object as image is referred as image steganography. Audio Steganography involves hiding data in audio files such as WAV, AU and MP3 sound files. Video Steganography is a technique of hiding any kind of files or data into digital video format. Network or Protocol Steganography involves hiding the information by taking the network protocol such as TCP, UDP etc, as cover object[1].

In LSB method the embedding is done by replacing the least significant bits of image pixels with the bits of secret data. Change occurs at only one bit so intensity of image is not affected too much.

In histogram based data hiding technique the crucial information is embedded into the image histogram. The peak point and zero point are identified for pixel shifting.

In Difference Expansion (DE) calculate the differences of neighboring pixel values, and select some difference values. The original data will all be embedded into the difference values.

In section 2 the different categories of techniques are described. In section 3 the performance measurement parameters of image steganography methods have been illustrate. Finally in section 4 the paper is concluded.

2. Steganography Techniques

Spatial domain techniques are :

1] Least significant bit (LSB) Difference
2] Expansion (DE)
3] Histogram Shifting

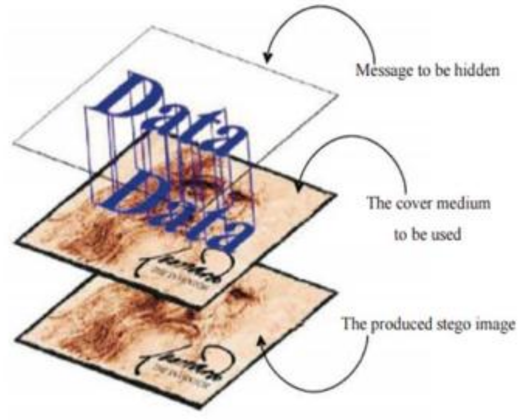

Figure 1: Data Hiding Scheme

2.1 Least Significant Method (LSB)

Least significant bit (LSB) insertion is a simple approach to embedding information in a cover image in least significant bit position. In pixel processing patch the encrypted data in to the image. Least significant bit is used to patch the data. Intensity of image is only change by ‘0’ or ‘1’ after hiding the information. Change occurs at only one bit so intensity of image is not effected too much and we can easily transfer the data.

To insert data in an image first we take an input image then find the pixels values and select the pixel on we want to insert the data. The pixel selection depends on user’s choice as either alternate or continuous manner and insert data values into pixels[5].

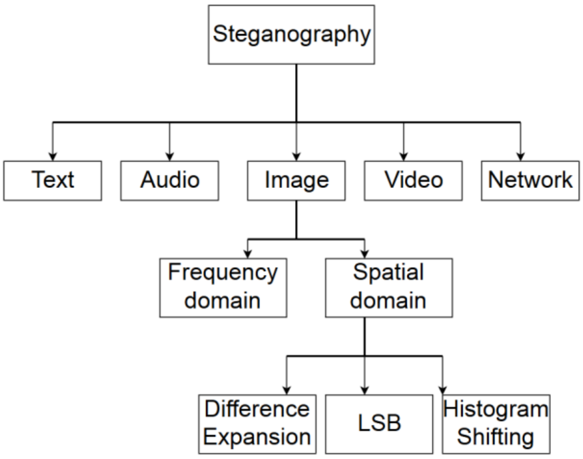

Figure 2: Steganographic Classification

Consider a grid for 3*3 pixels of a 24 bit image,

11001010	00110110	10101000
01111000	11100001	00001100
11000110	01010101	11111100

The number 84, which binary representation is 01010100, is embedded in to the least significant bit of the image then resulting grid is as follows:

11001010	00110111	10101000
01111001	11100000	00001101
11000110	01010100	11111100

Methods of Steganography:

One Bit stego: The message can be stored in the LSB of one colour of the RGB value or in the parity bit of the entire RGB value.

Two Bit Stego: In this method two LSBs of one of the colours in the RGB value of the pixels will be used to store message bits in the image.

Three Bit Stego: In this method three LSBs of one of the colours in the RGB value of the pixels will be used to store message bits.

Four Bit Stego: In this method four LSBs of one of the colours in the RGB value of the pixels will be used to store message bits[3].

The Figure:2 and Figure:3 represents original image and output image respectively.

Figure 2: Original Image

Figure 3: Output Image

Advantages of LSB technique are:

- There is less chance for degradation of the original image.
- More information can be stored in an image.

Disadvantages of LSB technique are:

- Less robust, the hidden data can be lost with image manipulation.
- Hidden data can be easily destroyed by simple attacks [2].

2.2 Difference Expansion Method (DE)

Difference expansion (DE) is one of the most important techniques which are used for reversible data hiding. This technique have high efficiency and simplicity.

In DE calculate the differences of neighboring pixel values, and select some difference values. The original data will all be embedded into the difference values.

Example:
Assume we have two values x=206, y=201 and reversibly embed one bit b=1. ‘l’ is the integer average value and ‘h’ is the difference of x and y.

$$l = \frac{206+201}{2} = \frac{407}{2} = 203$$

$$h = 206 - 201 = 5$$

The binary representation of difference value,

$$h = 5 = 101.$$

Then append ‘b’ into the binary representation of ‘h’ after the least significant bit (LSB), the new difference value will be

h_1 = 101b = 1011 =11.

This is equivalent to

h_1 = 2 * h + b = 2 * 5 + 1 =11

Then compute the new values, based on the new difference value and the original integer average value,

$$x_1 = 203 + \frac{11+1}{2} = 209$$

$$x_2 = 203 - \frac{11}{2} = 198$$

From the embedded pair (x_1, x_2), we can restore the original pair (x, y) and extract the embedded bit b. Then compute the integer average value and difference again.

$$l_1 = \frac{209+198}{2} = 203$$

$$h_1 = 209 – 198 = 11$$

The binary representation of h_1 = 11 = 1011. Extract the least significant bit b=1, which leaves the original value of the difference as h = 101 = 5. This is equivalent to

$$b = \text{LSB}(h_1) = 1$$

$$h = \frac{h_1}{2} = 5$$

With the restored difference value h and integer average value l_1, we can restore exactly the original pair. In this example, we have embedded one bit b by increasing the valid bit length of the difference value h from 3 bits (101) to 4 bits (1011). This reversible data-embedding operation h_1 = 2 * h + b is called the Difference Expansion [6].

2.3 Histogram Shifting Based Method

Histogram based data hiding is another commonly used data hiding method. Histogram shifting technique prevents overflow and underflow problems. The pixel histogram is generated by counting the frequency of pixel values from 0 to 255 in the image. Then the peak point and zero point are identified for pixel shifting. If a pixel is between the peak point and zero point, the pixel is shifted by one from the peak point towards the zero point. Then, the secret data is embedded into the pixel belonging to the peak point.

The embedding rule is that: if the secret bit equals to ‘1’ and the pixel belongs to the peak point, then the pixel value is increased by one; else if the secret bit equals to ‘0’ and the pixel belongs to the peak point, then the pixel value remains unchanged. In the data extraction phase, the secret bit ‘1’ is extracted if the pixel belongs to the peak point plus one. The secret bit ‘0’ is extracted if the pixel belongs to the peak point.. After all secret bits have been extracted, the image can be fully restored by shifting the pixels back to between the peak point and zero point[7].

3. Performanace Measurement Parameters

3.1 Mean Squared Error(MSE)

Measure of the quality of an estimator is called as Mean Squared Error.

$$\text{MSE} = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \qquad (1)$$

In equation (1) m, n are the number of rows and columns in the cover image matrix, K(i,j) is the pixel value from stego image and I(i,j) is the pixel value from cover image. Higher value of MSE indicates dissimilarity of between compared images.

3.2 Peak Signal to Noise Ratio(PSNR)

PSNR is the error metric used to compare image compression quality and it is the ratio between the maximum possible power of a signal and the power of corrupting noise. This ratio is used as a quality measurement between the original and a compressed image. PSNR measures in decibels[6].

$$\text{PSNR} = 20\log_{10}(MAX_I) - 10\log_{10}(MSE) \qquad (2)$$

3.3 Structural Similarity(SSIM)

SSIM measuring the similarity between two images. The SSIM index is calculated as,

$$\text{SSIM(x,y)} = \frac{(2\mu_x\mu_y + c_1)\,(2\sigma_{xy} + c_2)}{(\mu_x{}^2 + \mu_y{}^2 + c_1)\,(\sigma_x{}^2 + \sigma_y{}^2 + c_2)} \qquad (3)$$

μ_x is the average of x

μ_y is the average of y

$\sigma_x{}^2$ is the variance of x

$\sigma_y{}^2$ is the variance of y

σ_{xy} is the variance of x and y c_1 and c_2 are stabilize the division with weak denominator L the dynamic range of pixel values.

3.4 Comaparitive Analysis

Table 1: Performance Comparison

METHODS	*PSNR*	*MSE*	*SSIM*
Least Significant Bit	Low	High	Low
Difference Expansion	High	Low	High
Histogram Shifting Based	Low	High	Low

Table 1 shows the performance comparison of the different data embedding techniques. From the table it can be find that histogram shifting based is more better than that of other techniques. Least significant based method have low peak signal to noise ratio, high mean squared error value and low structural similarity. Histogram based method have high peak signal to noise ratio, low mean squared error value and high structural similarity. Difference expansion method have low peak signal to noise ratio, high mean squared error value and low structural similarity.

Table 2 shows the advantages and disadvantages of the different data embedding techniques. From the table it can be find that histogram shifting based is more better than that of other techniques. Least significant method exhibits high perceptual transparency and low degradation in the image quality. The main disadvantage of least significant bit method is low robustness to malicious attacks. Difference expansion exhibits high visual quality and high computational complexity. The main disadvantage of difference expansion is vulnerable to accident. Histogram shifting method have high payload performance and visual quality greater than 33dB.

3.5 Applications of Steganeography

- Secret Data Storing and Confidential Communication
- Protection of Data Alteration
- Media
- Database Systems
- E-Commerce
- Digital watermarking[2].

Table 2: Advantages and Disadvantages of steganographic methods

Methods	*Advantages*	*Disadvantages*
LSB	Easy to understand and comprehend	Low robustness to malicious attacks
	High perceptual transparency	
	Low degradation in the image quality	
Difference Expansion	High visual quality	Vulnerable to environmental noise
	Low computational complexity	
Histogram shifted	High payload performance	Nill
	Visual quality greater than 33db	

4. Conclusion

By comparing different data embedding techniques it can be concluded that histogram shifting based reversible data hiding is better than that of other techniques. Histogram shifting based reversible data hiding has an high SSIM and low PSNR, MSE value. Due to this reason Histogram shifting based reversible data hiding is efficient than other techniques.

References

[1] J. Kour and D. Verma, "Steganography techniques–a review paper," International Journal of Emerging Research in Management &Technology ISSN, pp. 2278–9359, 2014.

[2] R. Kaur and B. Kaur, "A study and review of techniques of spatial steganography".

[3] M. Juneja and P. S. Sandhu, "An improved lsb based steganography technique for rgb color images," International Journal of Computer and Communication Engineering, vol. 2, no. 4, p. 513, 2013.

[4] N. Tiwari and D. M. Shandilya, "Evaluation of various lsb based methods of image steganography on gif file format," International Journal of Computer Applications (0975–8887) Volume, 2010.

[5] V. Tyagi, "Image steganography using least significant bit with cryptography," Journal of global research in computer science, vol. 3, no. 3, pp. 53–55, 2012.

[6] J. Tian, "Reversible data embedding using a difference expansion," IEEE transactions on circuits and systems for video technology, vol. 13, no. 8, pp. 890–896, 2003.

[7] C.-C. Tseng, Y.-H. Chiu, and Y.-C. Chou, "A histogram shifting-based reversible data hiding scheme using multi-pattern strategy," in Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2015 International Conference on. IEEE, 2015, pp. 125–128.

Author Profile

Haritha H received her B.Tech. degree in computer science and engineering from the MEA Engineering College, Kerala, in 2015. Right now she is pursuing her M. Tech degree in computer science at MEA Engineering College, Kerala from 2015 to 2017. Her research interests lie in Image Processing.

Anish Kumar B received his B.Tech. degree in computer science and engineering from the college of Engineering, Karunagappally, Kerala, in 2006. He had completed his M. Tech degree in computer science at college of Engineering, Chengannur, Kerala from 2014. His research interests lie in Image Processing.