International Journal of Computer Applications Technology and Research
Volume 3– Issue 6, 361 - 363, 2014, ISSN: 2319–8656

Effective Parameters of Image Steganography Techniques

Fariba Ghorbany Beram
Sama Technical and Vocational Training College
Islamic Azad University
Masjedsoleyman Branch
Masjedsoleyman, Iran

Abstract: Steganography is a branch of information hiding method to hide secret data in the media such as audio, images, videos, etc. The use of images is very common in the world of electronic communication. In this paper, the parameters that are important in steganography images, have been studied and analyzed. Steganography purposes of security, robustness and capacity of which three are located at three vertices of a triangle, each note entail ignoring others. The main parameters of the methods steganography they've Security, Capacity, Psnr, Mse, Ber, Ssim are the results of the implementation show, steganography methods that these parameters provide have mentioned goals than other methods have improved.

Keywords: Steganography;psnr;mse,ber; Capacity

1. INTRODUCTION

The term Steganography is forked from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing" [1]. Steganography is the art and science of secret communication, in which the secret message in a cover media such that the hidden message is not detectable [2]. Today, a large part of the communications in electronic form. As the use of digital media coverage can be a good choice to hide the secret information. The media can, text, images, audio and video, etc. (Figure 1).

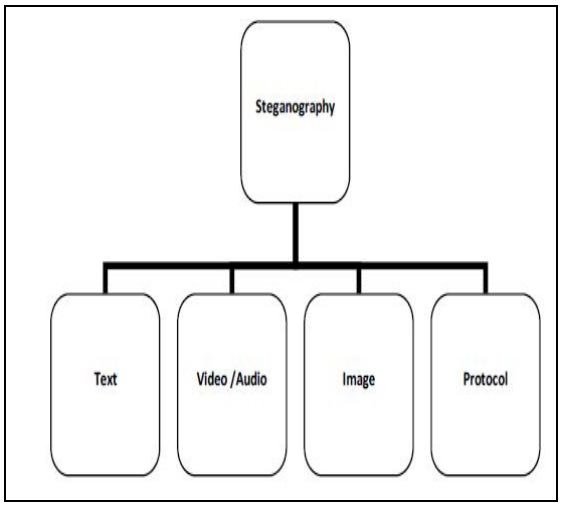

Figure 1: The media used in steganography (3)

It is very common nowadays for transferring images on the Internet. The eye is not very sensitive to the details of the pictures, so little change on steganography in an image is created, it is not tangible. Select an image masking confidential information is very important because it greatly affects the design of steganography systems. Bottom colors uniform texture images, or images are not suitable for steganography [4]. In recent years, steganography has been more noticeable secure data transfer [5]. Steganography in images is presented in many different techniques, which target all of them have access to high capacity, security, and robustness[6].

As seen in Figure 2, the three vertices of a triangle are three objectives. Should be given to the use of reconciliation established between them [7].

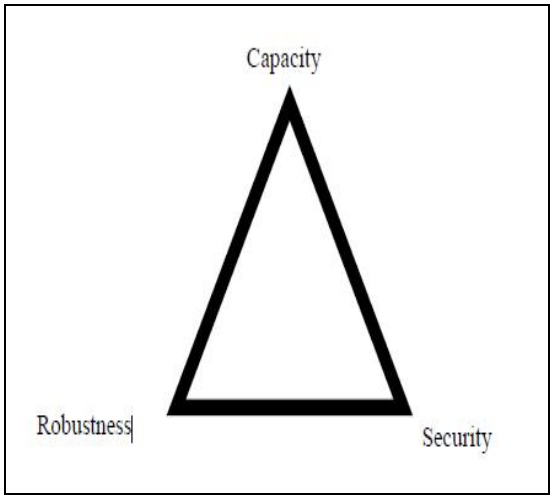

Figure 2: Characteristics of information hiding systems.

Ghasemi et al [8] have presented a method in which a combination of genetic algorithm and wavelet transform has been used. This capacity is taken into consideration. Ghorbany et al [9] have presented a method which establishes a compromise between the maximum rate and capacity are Signal to Noise.

2. Image Quality

Important factor in the field of steganography, image quality is carrying a secret message about the PSNR and MSE are considered [10]. If the original image and stego image H by H1 and HWIDTH, HLEN length and width of the image PSNR and MSE is calculated from the equation 2 is calculated from equation 1.

equation 1

$$MSE= \frac{\sum_{i=1}^{H.LEN}\sum_{j=1}^{H.WIDTH}[H(i,j)-H1(i,j)][H(i,j)-H1}{HLEN*HWIDTH}$$

equation 2

PSNR=10*log(255*255/mse)

The Mean squared error (MSE) is less indicative of the quality of the stego image, a low value, the maximum amount of signal to noise ratio (PSNR) indicate low quality of the image carrier [11]. The peak signal-to-noise level, noise level, which is the carrier of media placement information, the media has been created. The peak signal to noise level is measured in units of dB. If amount over thirty-dB signal-to-noise ratio, the human eye can hardly recognize the difference between the original image and data carriers [12]. Mean square error between the original image and the image shows an information carrier. As we see in Figure 3, there is an inverse relationship between PSNR and MSE. So which way is better PSNR value is high and low MSE value.

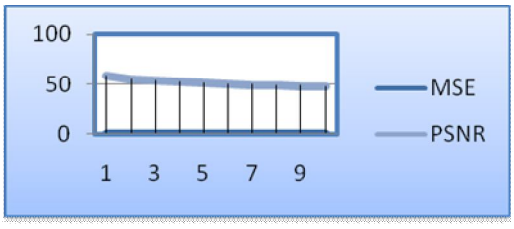

Figure 3: Relationship between PSNR and MSE

3. Similarity (SSIM)

The similarity between the original image and image information displays a carrier.

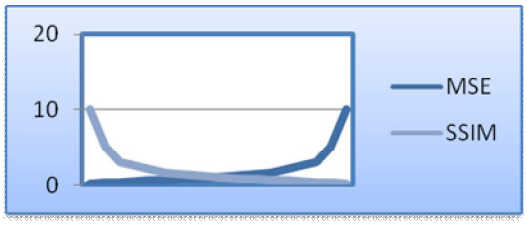

Figure 4: The relationship between MSE and SSIM

Figure 4 shows the relationship between MSE and SSIM. As you can see, there is an inverse relationship between these two cases.

4. Security Image

An attacker must be able to extract images without the secret key. Increase the security of steganography algorithms is the following:

- Use a combination of steganography and cryptography techniques.
- Use random key algorithm
- Failure to use a fixed number of bits
- Complexity of data discovery

5. Blind

At the time of extraction of secret information from the carrier object need not be the main object and the original object data can be properly extracted.

6. Bit error rate(Ber):

Information extracted from the raw data replaced the alternatives are compared, differences in the rates of high rises and shows the bit error parameter is incorrect algorithm. The bit error rate is lower, the higher the reliability of the algorithm used.

7. Capacity:

The maximum amount of information that can be carried in the media, steganography algorithm can be implanted without being carried in the media to apply tangible change. High capacity steganography algorithms is to evaluate the main parameters However, high-capacity, reduced image quality due to use of the algorithm can establish a compromise between quality and capacity of the application or the preference of one over the other.

8. conclusion

Steganography technique to hide the secret information in conventional media for safe transport through public channels such as the internet. In this study methods that are available in this area have been studied, the results show the effect of some key parameters to determine the right methods. These

parameters are provided in ways that other methods than others preferences and are more reliable. Security parameters, capacity and transparency are the key parameters steganography images.

Secure random key shared between transmitter and receiver can be used or can be used to blind steganography techniques. Capacity can be used for variable bit rate. Adaptive techniques can be used for clarity images can cover up to psnr, mse, ssim be acceptable. It is suggested to have a reliable method of the key parameters must be blind steganography techniques, adaptive steganography techniques, random Key steganography techniques, variable bit rate steganography techniques used.

9. REFERENCES

[1]Blossom K, Amandeep K, Jasdeep S.2011. STEGANOGRAPHIC APPROACH FOR HIDING IMAGE IN DCT DOMAIN. International Journal of Advances in Engineering & Technology,1:72-78

[2] Geetha C, Giriprakash H.2012. image steganography by variable embedding and multiple edge detection using canny operator . International Journal of Computer Applications (0975 – 888) 48:15-19

[3]Sivaiah S, Venkataiah C. 2011. An efficient lifting based 3-d discrete wavelet transform. IJCA Special Issue on “2nd National Conference- Computing, Communication and Sensor Network”CCSN, 2011:25-29

[4] Priya S, Amsaveni.2012. Edge Adaptive Image Steganography in DWT Domain. International Journal of Advances in Image Processing,2:91-94

[5] Hashemi Pour A, Payandeh A. 2012. A New steganography method based on the complex pixels. Journal of Information Security, 3: 202-208

[6] Pradhan A, Sharma D, Swain G. 2012. Variable rate steganography in digital images using two,three and four neighbor pixels. Indian Journal of Computer Science and Engineering (IJCSE),3:457-463

[7] Khare A, Saxena M, Jain H.2011. AMBTC-compressed image using genetic algorithm. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-2:68-71

[8] Ghasemi E, Shanbehzadeh J, Fassihi N. 2011. High capacity image steganography using wavelet transform and genetic algorithm . Proceeding of the International Multiconference of Engineers and Computer Scientists 2011 vol I,IMECS 2011. March 16-18,2011.Ho

[9] fariba ghorbany beram,Mashallah Abbasi Dezfouli,Mohammad Hossein Yektaie,"A New Steganography Method based on Optimal Coefficients Adjustment Process (OCAP)",International Journal of Computer Applications (0975 – 8887),Volume 87 – No.2, February 2014

[10] Kaushik P, Sharma Y.2012. Comparison Of Different Image Enhancement Techniques Based Upon Psnr & Mse.International Journal of Applied Engineering

[11] Verma A, Nolkha R, Singh A , Jaiswal G.2013. Implementation of Image Steganography Using 2-Level DWT Technique. International Journal of Computer Science and Business Informatics,1:1-14

[12] Maan V, Dhaliwal H.2013. Vector Quantization In Image Steganography. International Journal of Engineering Research & Technology (IJERT).2:10-15