International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 5, September- October 2017 ISSN 2278-6856

A Comprehensive Study of Image Steganography Techniques

Dr. Israa T. Ali [1],Shaymaa Jawad[2]

[1] University of Technology, department of Computer Science,
Baghdad/ IRAQ, 110105@uotechnology.edu.iq
[2]University of Technology, department of Computer Science

Abstract:*Transmitting images confidentially from sender to an authorized receiver through an insecure (public) channel is a challenging task. Therefore, several methods are developed to protect important information for safe and secure communication. There are three main technologies used for securing digital data: watermarking, steganography and cryptography. Steganography and watermarking could be considered within the same field (information hiding). This paper presents a comprehensive study for various methodologies in the field of image steganography. Each methodology has its bad and good points, therefore, a part of advantages and drawbacks are also discussed as a comparative study to help future researchers by providing a review of the existing techniques.*

Keywords: image steganography, spatial domain, transform domain, cover image, and stego image

1. INTRODUCTION

Recently, the growth of the Internet gets the most important aspect in information technology. Thus Providing security has also become important issue by developing several methods to protect important transmitted information. These methods could be classified essentially into three categories: steganography, watermarking, and cryptography.

Cryptography is a method that areused to encrypt and decrypt the data so that it is protected from any third parties. Sometimes it is not enough to keep the data secret, it will be necessary to keep the existence of the data secret also. The problem with cryptography is that when intruder observes any such type of scrambled data, he tries to decrypt the data. Due to the availability of high computational device, the rate of successful decrypt of data has also been increased. Steganography can be considered as the solution to this problem. Steganography is a method that is used to hide an amount of secret data in a multimedia carrier (cover), thus hiding the existence of the data completely and nobody can guess it except the authorized receiver. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing" defining it as "covered writing". Both steganography and watermarking are data embedding methods. On the other hand, watermarking, that may be mainly used for proving copyright, aims to hiding small amount of secret data in multimedia carrier. It aims to make it impossible to removal or manipulation of secret message.

Steganography has three main factors: un-detectability, robustness, and capacity. These factors separate steganography from other related techniques e.g. cryptography and watermarking.Un-detectability is the ability of the algorithm to avoid the detection of hidden data through Human Visual System (HSV) or statistical analysis. Robustness is the ability of the algorithm to extract the hidden data after many image related operations such as rotating, filtering etc. Capacity is the number of bits of secret data that are hidden into each cover image.

The steganography carriers can be classified into five types: text, image, video, audio, and protocol as shown in figure 1.

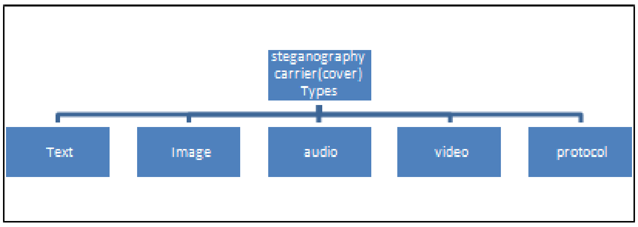


Figure 1: catigories of steganography carriers[15]

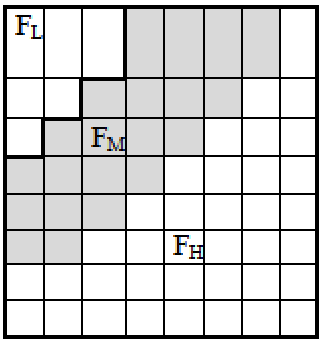


Figure 2 Discrete Cosine Transformation [3]

B. Discrete Wavelet Transformation

Wavelet transform is used in a wide range in signal processing applications and image compression. It separates the signal to set of basic functions which are called wavelets. Discrete Wavelet Transform (DWT) is described as an efficient and very flexible method for decomposing signals sub bands. In case of one-dimensional DWT, image is decomposed into 4 bands denoted by Low-Low (LL) level, High-Low (HL) level, Low-High (LH) level and High-High (HH) level [35], as shown in Figure 5 (a). Where, H symbolizes high-pass filter (High frequency) and L symbolizes low-pass filter (Low frequency). In case of Multi-Level Discrete Wavelet Transform, as shown in Figure 5 (b). This represents the image after applying three times of DWT. The image consists of frequency areas of LL1, LH1, HL1, HH1. The LL1 (low-to sub-level frequency area information of LL2, LH2, HL2,HH2. As the most essential part of image is concentrated at LLx (lower frequency sub-bands), the hiding of the data in this sub-bands will cause a problem because this may reduce the quality of the image significantly.

Otherwise, HHx (high frequency sub-bands) contain the textures and edges of the image and the changes on such sub-bands cannot be noticed by human naked eyes. So, The hiding process will be done on the coefficients of high frequency sub-bands. The DWT is featured by Imperceptibility and Robustness. However, the drawbacks of this method are that Long compression time, High computational cost, Noise/blur close to edges of images.

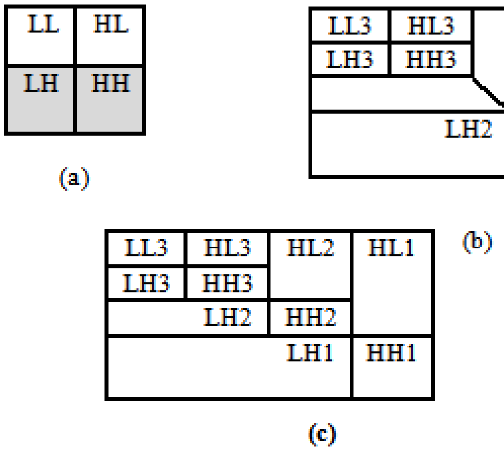


Figure 3 Discrete Wavelet Transformation[15]

2.3 Spatial or frequency Domain: some steganographic algorithms can either be categorized as being in the image domain or in the transform domain depending on the implementation.

A. Spread Spectrum

In spread spectrum techniques, hidden data is spread throughout the cover-image making it harder to detect [4]. A system proposed by Marvel et al. combines spread spectrum communication, error control coding and image processing to hide information in images [6]. Spread spectrum communication can be defined as the process of spreading the bandwidth of a narrowband signal across a wide band of frequencies [6]. This can be accomplished by adjusting the narrowband waveform with a wideband waveform, such as white noise. After spreading, the energy of the narrowband signal in any one frequency band is low and therefore difficult to detect [6]. In spread spectrum image steganography the message is embedded in noise and then combined with the cover image to produce the stego image. Since the power of the embedded signal is much lower than the power of the cover image, the embedded image is not perceptible to the human eye or by computer analysis without access to the original image [6]. The spread spectrum method is characterized by robustness versus statistical attacks.

B. Patchwork

Patchwork is a statistical technique that uses redundant pattern encoding to embed a message in an image [14]. The algorithm adds redundancy to the hidden information and then scatters it throughout the image . A random generator is used to select two areas of the image (or patches). The intensities of the pixels in the one patch are increased by a constant value, while the pixels of the other patch are decreased with the same constant value. The contrast changes in this patch subset encodes one bit and the changes are typically small and imperceptible, while not changing the average luminosity . A drawback of the patchwork approach is that only one bit is hidden. More bits could be hidden by first dividing the image into sub-images and applying the hiding to each of them. The advantage of using this technique is that the secret data is distributed over the entire image, so should one patch be destroyed, the others may still survive. Patchwork is most suitable for small amount ofdata.

1. Stego Image Quality Metrices

Thestego image quality mercies are basically *Peak Signal to Noise Ratio* (PSNR) and *Mean Square Error* (MES) value. The larger PSNR indicates to better quality, and the lower PSNR indicates poor quality of the stego image. The MES and PSNR could be calculated as in equation (1) and (2) respectively:

$$MES = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(x_{ij} - y_{ij}\right)^{2} \text{.....................}(1)$$

$$PSNR = 10\log_{10}\left(\frac{255^{2}}{MES}\right) dB \quad \text{........................} \ (2)$$

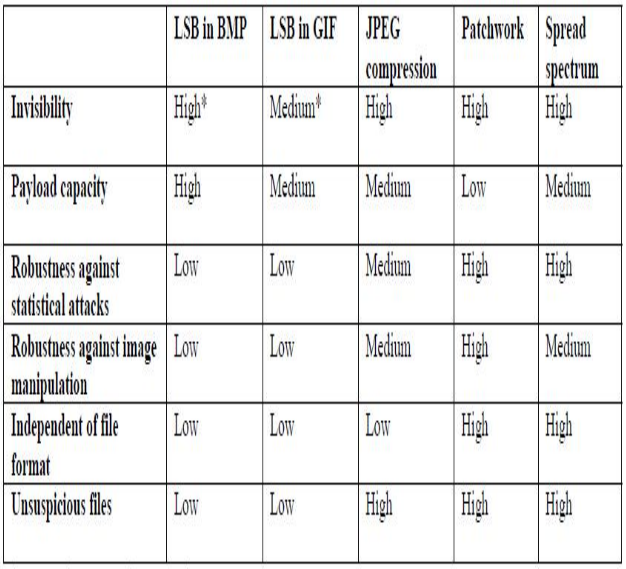
Where M and N are the number of cover image pixels in the horizontal and vertical dimension,x_{ij} and $y_{ij}$are the pixel values in the cover and stego image respectively.

2. Evaluation and Comparison of Different Steganography Techniques:

All the above mentioned techniques for image steganography have different strong and weak points and it isimportant to ensure that one uses the most suitable algorithm for an application as it is obvious in table 1. All steganographic algorithmshave to comply with a few basic requirements as shown in table 2. These requirements are as follows:

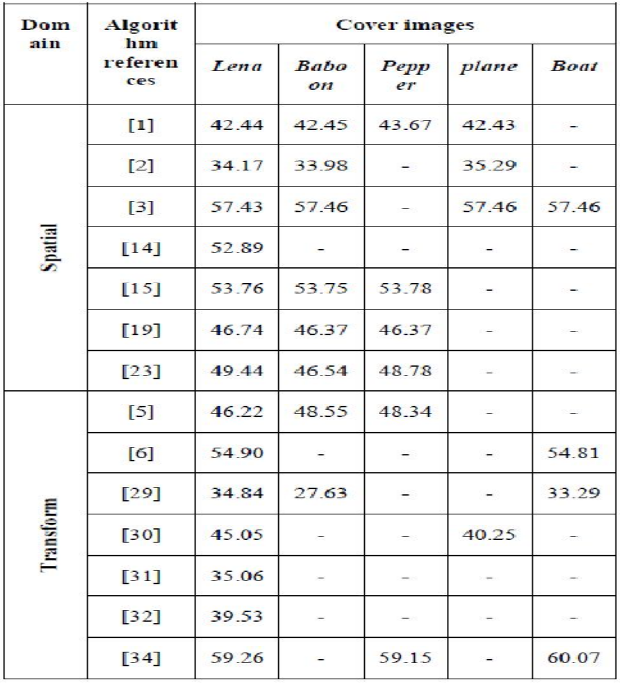
- **Invisibility** – The invisibility of a steganographic algorithm is the first and foremost requirement, sincethe strength of steganography lies in its ability to be unnoticed by the human eye. The moment thatone can see that an image has been tampered with, the algorithm is compromised.
- **Data Capacity**– Unlike watermarking, which needs to hide only a small amount of copyrightinformation, steganography aims tohidecomplete secret data and therefore requires sufficient hidingcapacity.
- **Robustness against image manipulation** –Image manipulation, such as cropping or rotating, can be done on the image before it reaches itsdestination. Depending on the technique in which the data is hidden, these manipulations maydestroy the hidden data. It is preferable for steganographic algorithms to be robust against eitherunintentional change to the image.
- **File Format Independency**–The most powerful steganographic algorithms that possess the ability to hidedata in anyformat of image. This also solves the problem of not always being able to find a suitable image at the rightmoment, in the right format to use as a cover image.
- **Unsuspicious files** – This requirement includes all characteristics of a steganographic algorithm thatmay result in images that are not used normally and may cause suspicion. Abnormal file size, forexample, is one property of an image that can result in further investigation of the image by a warden.

Table 1 illustrates the differences steganographic approaches between spatial domain and transformation domain according to their advantage and disadvantage:



	LSB in BMP	LSB in GIF	JPEG compression	Patchwork	Spread spectrum
Invisibility	High*	Medium*	High	High	High
Payload capacity	High	Medium	Medium	Low	Medium
Robustness against statistical attacks	Low	Low	Medium	High	High
Robustness against image manipulation	Low	Low	Medium	High	Medium
Independent of file format	Low	Low	Low	High	High
Unsuspicious files	Low	Low	High	High	High

Table2 compares image steganography techniques as discussed in section 3, with respect to the requirements that mentioned previously in section 5:



Domain	Algorithm references	Cover images				
		Lena	*Baboon*	*Pepper*	*plane*	*Boat*
Spatial	[1]	42.44	42.45	43.67	42.43	-
	[2]	34.17	33.98	-	35.29	-
	[3]	57.43	57.46	-	57.46	57.46
	[14]	52.89	-	-	-	-
	[15]	53.76	53.75	53.78	-	-
	[19]	46.74	46.37	46.37	-	-
	[23]	49.44	46.54	48.78	-	-
Transform	[5]	46.22	48.55	48.34	-	-
	[6]	54.90	-	-	-	54.81
	[29]	34.84	27.63	-	-	33.29
	[30]	45.05	-	-	40.25	-
	[31]	35.06	-	-	-	-
	[32]	39.53	-	-	-	-
	[34]	59.26	-	59.15	-	60.07

3. Conclusion

This paper presents a comprehensive study of the various digital image steganography techniques in spatial and frequency domain. First, a simple definitions and comparison among steganography, watermarking and cryptography is presented. Then a classification of steganography techniques based on hiding domain is shown. This paper will provide an insight to the researchers to come up with new ideas for developing a more reliable and efficient steganography algorithm, where determining the suitable method based on the wanted purpose.

From this study, it is observed that the hiding procedure is easy in spatial domain techniques compared to complex frequency domain technique has the ability to hold the secret data after s resizing, cropping, rotating etc. Again, it can be concluded that even before imposing hiding algorithms, usage of cryptography would provide a better level of security. In future, combination of cryptography and data compression in transform domain can help to achieve an improved steganography algorithm with high performance.

References

[1] F.Shih ,Digital Watermarking And Stegnography, Fundamental And Techniques.Usa:Crc
Press,2008.

[2] Mehboob ,Faruqui "A Stegnography Implementation" Biometrics And Security Technologies. Isbast Pp.,2008..

[3] RupeshGupta,Preet Singh "New Proposed Practice For Secure Image Combing Cryptography Stegnography And Watermarking Based On Various Parameters".

[4] Baek,Kim,Fisher,Chao "(N,1) Secret Sharing Approach Based On Stegnography With Gray Digital Images" Wireless Communications,Networking And Information

[5] Security(Wcnis),2010 Ieee International Conference.

[6] Parah,Sheikh And Bhat "Data Hiding In Intermediate Significant Bit Planes,A High Capacity Blind Stegnographic Technique" International Conference On Emerging Trends In Science,Engineering And Technology 2012.

[7] Imran Bajwa ,Riasat "A New Perfect Hashing Based Approach For Secure Stegnography" Ieee Sixth International Conference On Digital Information Management 102-107 Melbourne, Australia: Ieee Press.

[8] J.K Mandal,Debashis Das "Color Image Stegnography Based On Pixel Value Differencing In Spatial Domain" International Journal Of Information Sciences And Techniques (Ijist) Vol.2, No.4, July 2012..

[9] Anil Kumar,Rohini Sharma "A Secure Image Stegnography Based On Rsa Algorithm And Hash-Lsb Technique" International Journal Of Advanced Research In Computer Science And Software Engineering Volume 3, Issue 7, July 2013.

[10] Atallah "A New Method In Image Stegnography With Improved Image Quality" Applied Mathematical Sciences, Vol. 6, 2012, No. 79, 3907 - 3915.

[11] Mstafa "Information Hiding In Images Using Stegnography Techniques".

[12] Indradip Banerjee, Souvik Bhattacharyya, And GautamSanyal "Text Steganography Using Article Mapping Technique(Amt) And Ssce" Journal Of Global Research In Computer Science Volume 2, No. 4, April 2011.

[13] Youssef Bassil "A Text Steganography Method Using Pangram And Image Mediums" International Journal Of Scientific & Engineering Research (Ijser), Issn: 2229-5518, Vol. 3, No. 12, December 2012.

[14] MohitGarg "A Novel Text Steganography Technique Based On Html Documents" International Journal Of Advanced Science And Technology Vol. 35, October, 2011.

[15] Vanitha T , Anjalin D Souza , Rashmi B, SweetaDSouza, "A Review on Steganography – Least Significant Bit Algorithm and Discrete Wavelet

Transform Algorithm", International Journal of Innovative Research in Computer and Communication Engineering, 2014.

[16] Dr. D. Y. Patil," New robust LSB steganographic technique for increased security" International Journal of Engineering Research and General Science, 2015.