Mansoura Engineering Journal

Volume 40 | Issue 5 Article 5

12-1-2021

Comparison of Steganographic Techniques to Embed Data in Medical Images.

Shaimaa Hussein
Electronics and Communications Department Faculty of Engineering, Mansoura University

Hossam El-Din Moustafa
Electronics and Communications Department Faculty of Engineering, Mansoura University,
hossam_moustafa@ieee.org

Ahmed Samra
Electronics and Communications Department Faculty of Engineering, Mansoura University

Recommended Citation

Hussein, Shaimaa; Moustafa, Hossam El-Din; and Samra, Ahmed (2021) "Comparison of Steganographic Techniques to Embed Data in Medical Images.," *Mansoura Engineering Journal*: Vol. 40 : Iss. 5 , Article 5.
Available at: https://doi.org/10.21608/bfemu.2020.96268

Comparison of Steganographic Techniques to Embed Data in Medical Images

مقارنة بين تقنيات أخفاء المعلومات لدمج البيانات فى الصور الطبية

Shaimaa Ateya Hussein, Hossam El-Din Moustafa and Ahmed Shaaban Samra

Electronics and Communications Department
Faculty of Engineering, Mansoura University

الملخص

(Steganography) هو فن وعلم أخفاء المعلومات بداخل وسط للتغطية بهذه الطريقة لا يكتشفها أى شخص ماعدا المتلقى المقصود يعلم بوجود المعلومات. الصور الرقمية هى الأكثر شيوعا لأستخدامها كوسط للتغطية فى ال steganography بسبب سهولتها وأنتشارها على الإنترنت. هذا العمل يقدم مقارنة للتقنيات المختلفة ل Steganography Steganography.يستخدم نوعين من المجالات لأخفاء المعلومات: مجال spatial (مجال زمنى) ومجال تحول (مجال التردد). بعض التقنيات من المجالين تم مناقشتها. الأداء و المقارنة بين التقنيات تم قياسها على أساس المعايير الثلاثة WPSNR , MSE و NCCC.

Abstract

Steganography is the art and science of hiding secret information in a cover media in such a way that it is not detectable to anyone, except the intended recipient knows the existence of the data. Digital images are most commonly used coverage medium in steganography because of their easy availability and popularity on internet. This work provides a comparison review to the various steganography techniques. Steganography uses two kinds of domain for hiding the data: spatial domain (time domain) and transform domain (frequency domain). Some techniques from these two domains are discussed. The performance and comparison of these techniques is measured on the basis of the three parameters WPSNR, MSE, and NCCC.

1- Introduction

In contrast to cryptography, steganography is not to keep others from knowing the hidden information but it is also to keep others from thinking even that the information exists. Figure 1 shows the basic model of steganography consists of the cover-object, which the message is embedded in and to hide the presence of the message, Message is the data that wanted to be secured. It can be text, image, audio, video or a serial number, or anything that can be embedded in a bit stream. Stego-key, which ensures that only the desired recipient will be able to extract the message [4].

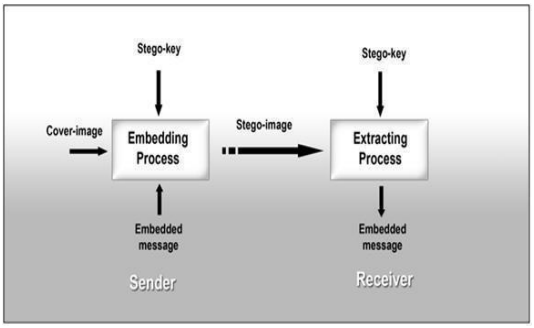

Figure 1: Basic Steganographic Process

Medical records of patients are extremely high sensitive information, needing uncompromising security during the storage and transmission. These records often have to be traceable to the patient medical data such as X-ray or scan (CAT, MRI, etc.) images. While numerous security tools have been used to encrypt

Accepted: 25 October, 2015

the information and prevent unauthorized access to the data exist, the possibility of hiding the very existence of these records, using image steganography, is discussed in this paper.

2- Techniques

Steganographic techniques can be broadly classified as

- Spatial domain techniques
- Transform domain techniques
- Hybrid domain techniques

In spatial domain technique all manipulations applied to the cover object and payload in the time domain. LSB is the most commonly used method in spatial domain technique. Transform domain techniques mean frequency domain techniques. DCT is the most popular transform domain technique. In case of hybrid domain technique image is divided into cells and then applying spatial or transform domain technique [7]. Modulating the LSB does not result in a human-perceptible difference because the amplitude of the change is small. This allows high perceptual transparency of LSB. Therefore, to the human eye, the resulting stego-image will look identical to the cover-image. This allows high perceptual transparency of LSB.

3.1- Traditional lsb technique

The basic image steganography algorithm is Least Significant Bit technique. The image will be act as reference image to hide the text in it and result the stego image. Each character of a text can be represented by 8-bit. LSB also gives good capacity any huge amount of text material can be hidden in a small size image [6]. The text can't be deciphered intercepting the image or data file separately. So, it is more secured [5].

Figure 2: Least Significant Bit Representation

For example a grid for 3 pixels of a 24-bit image can be as follows:
(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the ascii character 'h', which binary representation is 1101000
, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:
(00101101 00011101 11011100)
(10100111 11000100 00001100)
(11010010 10101101 01100011)

Although the character was embedded into the first 7 bytes of the grid, only the 2 underlined bits needed to be changed according to the embedded message. These changes cannot be perceived by the human eye thus the message is successfully hidden.

The original image and its stego image after embedding in the lsb along with their histograms are presented in Figure 3.

The Embedded text='duplex kidney mean that two separate pelvicalcyeal systems draining a single renal parenchyma Duplex kidney usually does not require any treatment per se however complications may necessitate intervention: vesicoureteric reflux into lower pole moiety or marked hydronephrosis of the upper pole moiety may have mass effect or become infected';

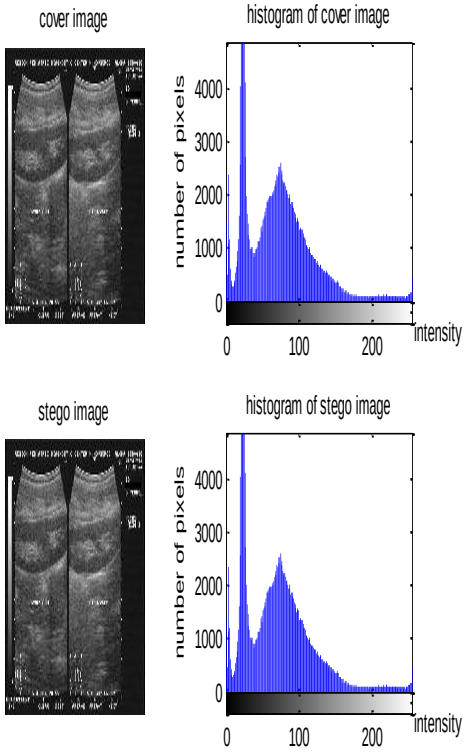

Figure 3: Original and Stego Image Embedded in LSB with Histograms

3.2- Embedding text message in each minimum value in each column of image

Let cover image be

51	3	106	213	128	40	12
50	190	215	5	180	112	45
153	113	133	173	109	5	146
69	237	51	96	77	56	81
50	118	171	212	48	94	215
60	111	58	25	96	16	159
78	25	63	18	75	93	64

The minimum gray level in each column is

50 3 51 5 48 5 12

Let the message be ‘shaimaa’ ie the value to be embedded is

115 104 97 105 109 97 97

Replacing the minimum values with the message bytes we get

51	(104)	106	213	128	40	(97)
(115)	190	215	(105)	180	112	45
153	113	133	173	109	(97)	146
69	237	(97)	96	77	56	81
50	118	171	212	(109)	94	215
60	111	58	25	96	16	159
78	25	63	18	75	93	64

Now extracting from above from each column from each minimum location

[115 104 97 105 109 97 97]

We get, ‘shaimaa’.

The original image and its stego image embedded in each column minimum value of memory locations along with their histograms are presented in Figure 4.

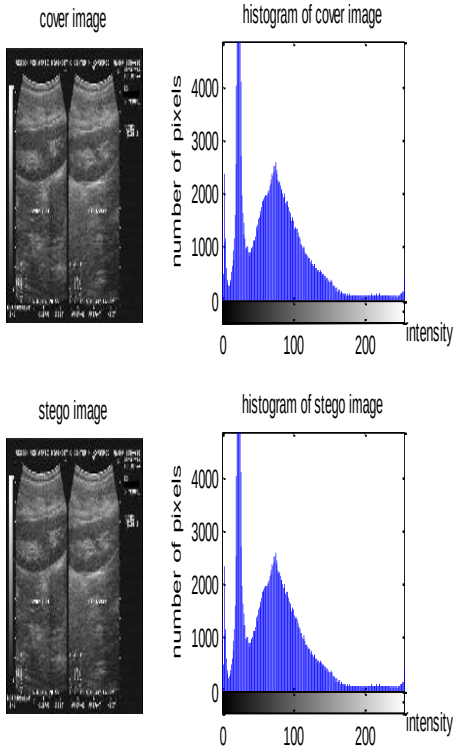

Figure 4: Original and Stego Image Embedded in Column Minimum Value with Histograms

3.3-Embedding text message in each maximum value in each column of image

Let cover image be

51	3	106	213	128	40	12
50	190	215	5	180	112	45
153	113	133	173	109	5	146
69	237	51	96	77	56	81
50	118	171	212	48	94	215
60	111	58	25	96	16	159
78	25	63	18	75	93	64

The maximum gray level in each column is

153 237 215 213 180 112 215

Let the message be ‘shaimaa’ ie the value to be embedded is

115 104 97 105 109 97 97

Replacing the maximum values with the message bytes we get

51	3	106	(105)	128	40	12
50	190	(97)	5	(109)	(97)	45
(115)	113	133	173	109	5	146
69	(104)	51	96	77	56	81
50	118	171	212	48	94	(97)
60	111	58	25	96	16	159
78	25	63	18	75	93	64

Now extracting from above from each column from each maximum location

[115 104 97 105 109 97 97]

We get, ‘shaimaa’.

The original image and its stego image embedded in each column maximum value of memory locations along with their histograms are presented in Figure 5.

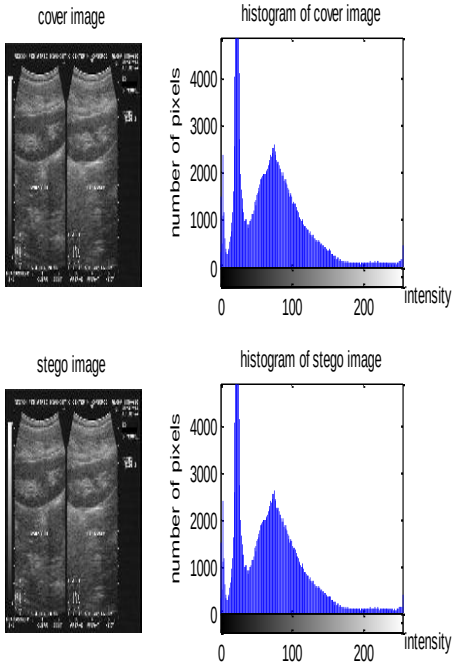

Figure 5: Original and Stego Image Embedded in Column Maximum Value with Histograms

3.4- Embedding text message in each even memory location of image

Let cover image be

51	3	106	213	128	40	12
50	190	215	5	180	112	45
153	113	133	173	109	5	146
69	237	51	96	77	56	81
50	118	171	212	48	94	215
60	111	58	25	96	16	159
78	25	63	18	75	93	64

Let the message be ‘shaimaa’ ie the value to be embedded is

115 104 97 105 109 97 97

Replacing the values with the message bytes at every even location, we get

51	(105)	106	213	128	40	12
(115)	190	215	5	180	112	45
153	(109)	133	173	109	5	146
(104)	237	51	96	77	56	81
50	(97)	171	212	48	94	215
(97)	111	58	25	96	16	159
78	(97)	63	18	75	93	64

Now extracting from above from each even locations

[115 104 97 105 109 97 97]

We get, 'shaimaa'.

The original image and its stego image embedded in even pixel memory locations along with their histograms are presented in Figure 6.

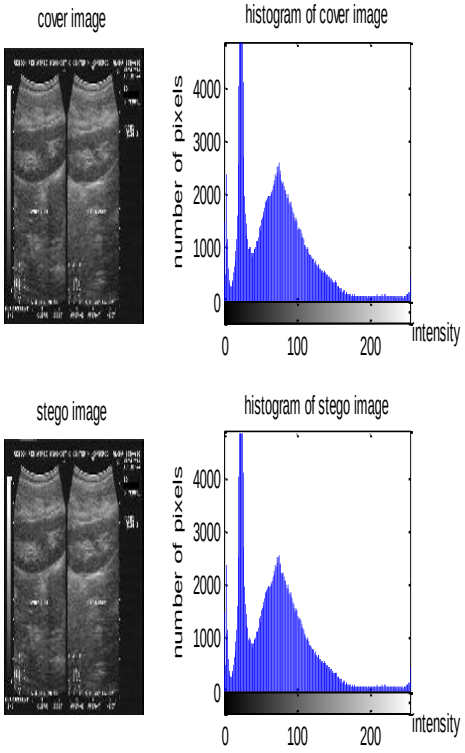

Figure 6: Original and Stego Image Embedded in Even Pixel Locations with Histograms

3.5- Embedding text message in each odd memory location of image

Let cover image be

51	3	106	213	128	40	12
50	190	215	5	180	112	45
153	113	133	173	109	5	146
69	237	51	96	77	56	81
50	118	171	212	48	94	215
60	111	58	25	96	16	159
78	25	63	18	75	93	64

Let the message be 'shaimaa' ie the value to be embedded is

115 104 97 105 109 97 97

Replacing the values with the message bytes at every odd location, we get

(115)	3	106	213	128	40	12
50	(109)	215	5	180	112	45
(104)	113	133	173	109	5	146
69	(97)	51	96	77	56	81
(97)	118	171	212	48	94	215
60	(97)	58	25	96	16	159
(105)	25	63	18	75	93	64

Now extracting from above from each even locations

[115 104 97 105 109 97 97]

We get, 'shaimaa'.

The original image and its stego image embedded in odd pixel memory locations along with their histograms are presented in Figure7.

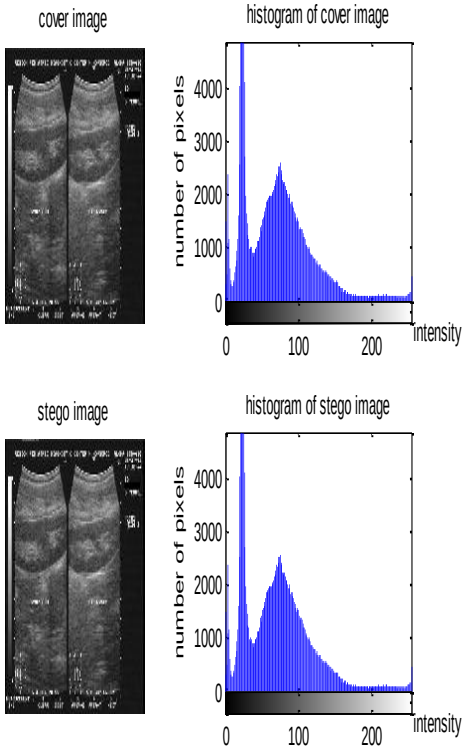

Figure 7: Original and Stego Image Embedded in Odd Pixel Locations with Histograms

3.6- Embedding text message in each prime number memory location of image

Let cover image be

51	3	106	213	128	40	12
50	190	215	5	180	112	45
153	113	133	173	109	5	146
69	237	51	96	77	56	81
50	118	171	212	48	94	215
60	111	58	25	96	16	159
78	25	63	18	75	93	64

Let the message be ‘shaimaa’ ie the value to be embedded is

115 104 97 105 109 97 97

Replacing the values with the message bytes at every prime number locations like 2, 3, 5, 7, 11, 13, 17, 19, …..
We get

51	3	106	213	128	40	12
(115)	190	215	5	180	112	45
(104)	113	(97)	173	109	5	146
69	(109)	51	96	77	56	81
(97)	118	171	212	48	94	215
60	(97)	58	25	96	16	159
(105)	25	63	18	75	93	64

Now extracting from above from each prime memory location

[115 104 97 105 109 97 97]

We get, ‘shaimaa’.

The original image and its stego image embedded in odd pixel memory locations along with their histograms are presented in Figure 8.

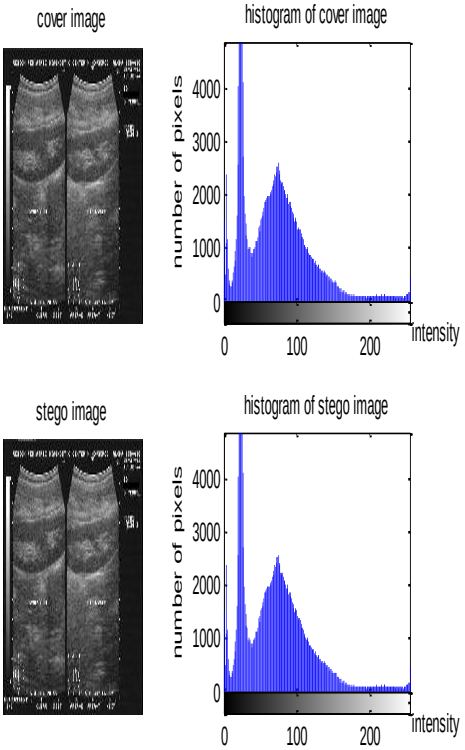

Figure 8: Original and Stego Image Embedded in Prime Number Memory Locations with Histograms

3.7- Hide message in image using wavelet transform

Applying DWT (Discrete Wavelet Transform) separates the image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH). With the DWT, the smooth parts of the spatial domain image exist in the approximation band that consists of low frequency wavelet coefficients and the edge and texture details exist in high frequency sub bands, such as HH, HL, and LH [8].

Haar Wavelet is a function which consists of a short positive pulse followed by a short negative pulse, which provides orthogonality decomposition of an image signal [9].

The secret message is embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Compared to all other methods mentioned earlier, this method provides the best quality of image, increases embedding capacity and is also robust against attack.

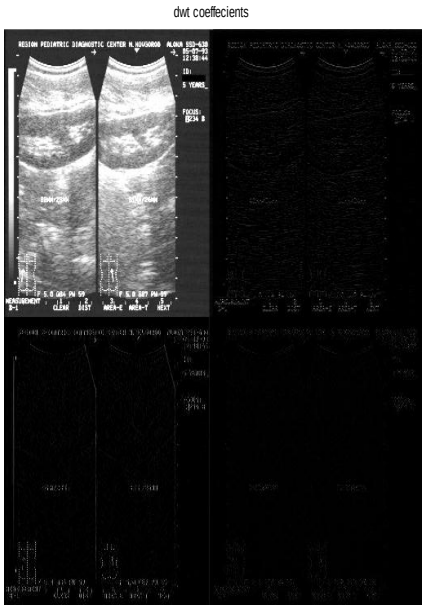

Figure 9: The DWT Coefficients of The Cover Image

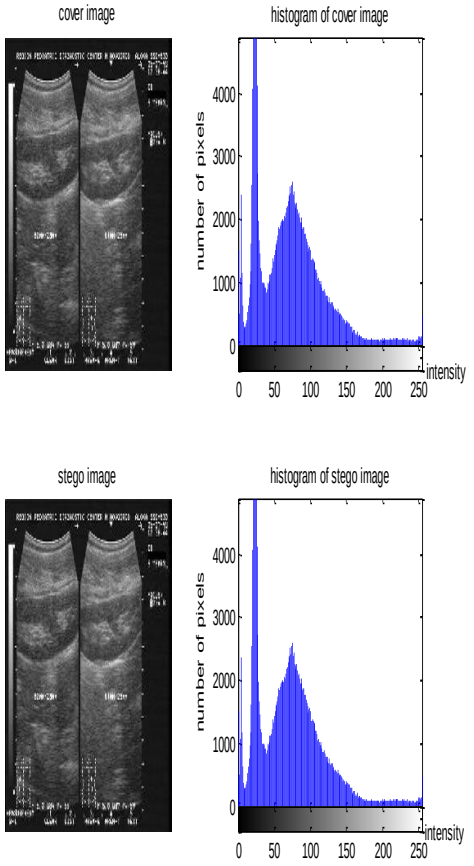

Figure 10: Original and Stego Image Embedded in High Frequency Coefficients with Histograms

3- Experimental results and analysis

All The algorithms have been implemented in Matlab and tested on medical colored and gray images and the NCCC has been measured. Normalized cross correlation has been commonly used as a metric to evaluate the degree of similarity (or dissimilarity) between two compared images the cross correlation is equitably simple to compute and independent of translations and scaling in the intensity domain. Thus it is fairly detached of lighting variations between the cover and the stego image [2].

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE

represents the cumulative squared error between the compressed/reconstructed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower is the error [1].

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(x_{ij} - y_{ij})^2 \quad \text{Eqn (1)}$$

The WPSNR is a different quality measurement suggested in [3]. The WPSNR uses an additional parameter called the Noise Visibility Function (NVF). NVF uses a Gaussian model to estimate how much texture exists in any area of an image. The WPSNR uses the value of NVF as a penalization factor.

$$WPSNR = 10log_{10}(\frac{i_{max}^2}{MSE \times NVF^2}) \quad \text{Eqn (2)}$$

The NVF is close to 1for flat region. And for edge or textured regions NVF is more close to 0. This indicates that WPSNR approximately equals to PSNR for smooth image. But for textured image, WPSNR is a little bit higher than PSNR. The form of NVF is given as

$$NVF(i,j) = \frac{1}{1 + \theta\sigma_x^2(i,j)} \quad \text{Eqn (3)}$$

	MSE	NCCC	WPSNR	PSNR
LSB	0.0033	1	87.9394	79.0157
Embedding in MIN	12.0169	0.9973	50.3018	43.3875
Embedding in MAX	23.7649	0.9946	47.2760	40.4516
Embedding in Even location	3.8755	0.9991	53.2006	48.3021
Embedding in Odd location	3.7655	0.9991	53.3697	48.4272
Embedding in prime location	4.0371	0.9990	52.9633	48.1247
DWT	0.0351	1	83.1843	62.6819

Table1: Comparison of The Techniques in The Same Cover Image

4- Conclusion

Recently, Security plays a controlling role in computer science and communications. The importance of security is further increased because of internet usage. In this paper, some commonly known steganography techniques were implemented. The implemented algorithms are applicable to all kinds of images and can be used in covert communication, hiding secret information like medical applications, banking information, copyrights and trade secrets. Comparing between all the methods the LSB and DWT provide the best quality of image. Although the DWT method more secured and also robust against attack it decomposes the entire image. It transforms the image rather than manipulating bits this method produces an irreversible image in terms of quality, image size, brightness and contrast ratio so LSB is recommended when using large amount of secret data because it increases the embedding capacity.

6- References

[1] A New Approach in Steganography using different Algorithms and Applying Randomization Concept.

[2] Application of Normalized Cross Correlation to Image Registration May2014. Available@ http://www.ijret.org

[3] Impact analysis of digital watermarking on perceptual quality using HVS models.

[4] International Journal of Research in Engineering and Technology May-2014 double layer security using visual cryptography and transform based steganography.

[5] International Journal Of Engineering And Computer Science August, 2013. A Survey on LSB Based Steganography Methods.

[6] International Journal of Engineering and Technology January, 2015 New Spatial Domain Steganography

Method Based On Similarity Technique

[7] International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com. January 2014 an Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques

[8] International Journal of Engineering and Technical Research March2014.Image Steganography Based On DWT Using Huffman LWZ Encoding

[9] International Journal of Application or Innovation in Engineering & Management. April 2014. A Novel Steganography Technique using Same Scale Wavelet