Optimal Image Steganography Content Destruction Techniques

Prof. Siddeeq Y. Ameen
College of Electronics Engineering
University of Mosul
Mosul, Iraq
prof.siddeeq@uomsoul.edu.iqs

Muthana R. Al-Badrany
College of Engineering
University of Mosul
Mosul, Iraq
muth85cnet@yahoo.com

***Abstract*— The paper presents two approaches for destroying steganogrphy content in an image. The first is the overwriting approach where a random data can be written again over steganographic images whereas the second approach is the denoising approach. With the second approach two kinds of destruction techniques have been adopted these are filtering and discrete wavelet techniques. These two approaches have been simulated and evaluated over two types of hiding techniques, Least Significant Bit LSB technique and Discrete Cosine Transform DCT technique. The results of the simulation show the capability of both approaches to destroy the hidden information without any alteration to the cover image except the denoising approach enhance the PSNR in any received image even without hidden information by an average of 4dB.**

Keywords—Steganography; stego-destruction; DCT; LSB; Denoiseing and Filtering; overwriting

I. INTRODUCTION

Steganography is the process of hiding a secure message in such a way that makes communication between sender and intended receiver to be invisible. From steganography a technique of authorization is evolved called watermarking, is the art of embedding information such as watermark, or logo within digital media. A watermark perhaps represents copyright, authorship or license etc. [1]. The applications of steganography have been attracted and being used by many international terrorist organizations, competitive companies, military and industrial bodies in their communication over the Internet [2]. This is because such services provide the secrecy involved and achieving their demands. Therefore, governmental security agencies and police forces try to restrict their use [1] [3].

The philosophy of stego destruction is different from other steganalysis branches, by destroying any embedded information within digital medium for any type of embedding algorithm was used in hiding process. A limited number of researches and ideas fight to destroy the hidden information content within the digital medium without any harm to the cover image. One of the initial investigation in such field is achieved by the Al-Naima1, Ameen and Al-Saad via the usage of discrete wavelet denoising DWT technique. The research has the ability of DWT to remove the hidden information with and leaving the cover image enhanced [3]. The latter research suggests the usage of such technique as a Stego-firewall. Extra research has been achieved by Moskowitz, Lafferty and Ahmed suggest an architecture that will remove steganography content and they called this method Stego Scrubbing. This philosophy lays the groundwork for the actual development of a stego scrubber, which can be inserted in a manner similar to a guard or firewall [4]. Further approach of hidden information destruction is achieved by who suggested two techniques for such purposes these are dissolving and overwriting. Dissolving has the ability to modify the pixels of the images so as to make the decoding process of the steganographic image being impossible. On the other hand, with overwriting idea, random data can be written again over steganographic images The results of such approach have shown that the hidden message is destroyed without giving any noticeable evidence [5]. Finally, extra research conducted by Terki have shown the ability of filtering to destroy hidden information and enhancing the cover image quality [6]. However, the research has shown the failure of several filtering techniques. Therefore, the scope of the research is to be conducted:

- Investigation some well-known information hiding techniques and studying the noise effect on cover image quality as a result to add stego content within that cover.
- Destruction and remove stego content for any used embedding mechanism, also possibility enhancing cover image quality using denoising techniques based wavelet and image enhancement filters in Matlab software, compared with destruction using overwriting technique.
- Design a firewall system that allows to pass digital image without stego hidden content after destroying it (and removing it) and tries to enhance it.

II. STEGO DESTRUCTION TECHNIQUES

A number of researches and concepts for detecting the existence of steganography were presented with what's called steganalysis. These sorts of steganalysis attempt to find or spot the hidden information and then destroying it accordingly. It involves scanning all the electronic communication medium

such as Internet traffic to a country or organization or even identified people. This of course time consuming and may not be able to spot or identify the hidden information. Thus the proposed destruction approaches will attempt to dam any stego content if gift in any space of the medium, without steganalysis detection method. These methods act as a filter or firewall that defend and destroy any stego content that attainable be embedded into the digital stream that goes through the firewall.

The idea was extracted from the capabilities of digital filtering or image processing that may be applied to digital media (audio and pictures information stream). This method takes into its account the stego content embedded within the quilt as an intrusive noise added to the initial cover. Then, just by employing any form of digital signal processing algorithm to get rid of the noise from the covered file, it removes and destroys the stego content embedded within the covered file.

It is very successful in preventing the secret message being restored. When modifications apply on LSB bits, steganographic image will suffer unobservable minor alterations. Overwriting data is same as or longer than hidden message and has the ability to totally disable it. Unfortunately, this approach can target specific steganographic technique that is LSB technique while it may not compatible with other techniques of steganography. With overwriting process, the new message is written over the old message to destroy steganographic content within the steganographic image. The new message may be different message or a constant message consists of zeros or ones written instead of the last bit of steganographic message. Therefore, the disabling of steganographic content may not be guaranteed against most robust techniques [5].

In image transmission and its acquisition, the image is mostly corrupted by various types of noise [7]. The scope of denoising approach is to select the corrupted pixels by noise and substitute predicted value instead of noisy value and this is the true definition of image enhancement. The mechanism in which the pixel is estimated as noisy or not noisy depends on how the estimate is calculated. This approach is very useful for destroying stego content and can be investigated by two techniques:

1. Filters technique.
2. Wavelet technique.

In filters based denoising approach, there are many filtering techniques, each one has its special way that's different from others when estimating accuracy for the noisy pixel from its surrounding pixels. This research presents a comparative analysis of various image filters with window size (3x3) such as standard mean filter (SMF), wiener filter and hybrid mean-wiener filter. These filters are used widely because of their effective noise suppression capability. Practically, one of the main disadvantages of these filters is that it modifies both noisy and non-noisy pixels thus removing some fine details of the image. However, steganographic image will completely scan by filter so as to remove noise including noisy steganographic content as well as minor blur adds to image especially its edges. Noise removal or rims blur will firstly target secret message length or steganographic key, if found, which is shared between intended parties in addition to targeting other parts of the image. For this reason, reverse steganographic algorithm can't retrieve these keys to be capable to read the hidden message.

In recent years, there have been a fair amount of research on wavelet thresholding and its application in image denoising. This is because wavelet has the capability of noise isolation from the noisy image. This is because the wavelet transform has the feature of separation in its output transform the small coefficient from the large coefficient. This will separate the noise that is related to the small coefficients from the important signal feature that are related to the large coefficients. Having achieved the isolated, thresholding can be used to remove the small coefficients (noise) leaving the significant features of the image [8]. This function is called wavelet denoising. The procedure that can be adopted to achieve wavelet denosing is as follows [9]:

1. The input noisy image is decomposed into several levels of approximations and detailed coefficients. This can be achieved via the using of selected wavelet basis.
2. The decomposed coefficients should be thresholded to isolate the coefficients containing the true signal from those of the noise. The former is extracted and the others are discarded.
3. The last step is the reconstruction of the signal using approximations and detailed coefficients. This can be achieved via the use of the inverse wavelet transform.

The above procedure relies on the proper selection of the mother wavelet. In this case it is preferred to select a mother wavelet that is as ‘‘similar’’ as possible to the measured signal [10]. Hard-threshold function and soft-threshold functions are the most important function to be used for thresholding. These threshold functions can be represented as [10]

$$Hard\ threshold: \begin{cases} y = x & if\ |x| \geq \lambda \\ y = 0 & if\ |x| < \lambda \end{cases} \quad \text{..... (1)}$$

$$Soft\ threshold: y = sign(x)(|x| - \lambda) \quad \text{..... (2)}$$

where x, y and λ are the input signal, signal after threshold and the threshold value, respectively. The threshold value is very important and critical because of its effect on the values of a wavelet coefficient estimate [10].

The noise can be removed or reduced after thresholding. Thus it is essential to know the estimation of the noise level. This estimate can be computed from the standard deviation of the detail coefficients that gives the value of the thresh value. The latter will help the process of soft thresholding to reduce the wavelet coefficient to a thresh value. On the other hand, with hard thresholding, the wavelet coefficients below a given value are stetted to zero. Fig. 1 shows the two types of thresholding [11].

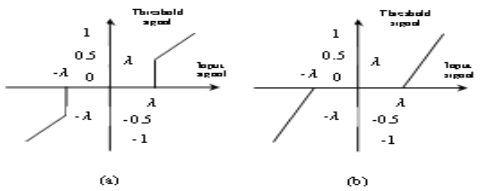

Fig. 1 Threshold Types (a) Hard (b) Soft

Three methods of thresholding the wavelet detail coefficients have been used in this research as follows [12]:

1. VisuShrink thresholding.
2. SureShrink thresholding.
3. BayesShrink thresholding.

III. Systems Simulation and Evaluation

Some famous steganography algorithms such as Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) have been investigated in RGB Lena image with size 256x256 pixel. The LSB and DCT have been adopted in this investigation as a candidate for information hiding comes from two reasons. The first reason because these two hiding techniques are well known and familiar and the second reason because the LSB operates in the time domain whereas the DCT operates in the frequency domain. Computer simulations using Matlab 2012a have been applied using overwriting approach and denoising approach based wavelet and image enhancement filter techniques to overcome stego images threats.

Initially, the hiding techniques have been investigated and the PSNR (Peak Signal to Noise Ratio) has been measured between the original image and the stego-and reconstructed images. This term is the most used term to compute image quality before and after any processing of images. Mathematically, the term PSNR is given by [13][14];

$$MSE = \frac{1}{N^2}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}[Io(x,y) - In\,(x,y)]^2 \quad \text{..... (3)}$$

$$PSNR = 10\,log_{10}\frac{(L-1)^2}{MSE} \quad \text{..... (4)}$$

where N is the height or the width of the image, L is the number of bits for pixel, Io is the initial image (cover image) and In is the noisy image (stego-image) or reconstructed image. However, the Mean Square Error MSE for RGB images is [15]:

$$MSE_{AVG} = \frac{MSE_R + MSE_G + MSE_B}{3} \quad \text{..... (5)}$$

where MSER, MSEG and MSEB are the MSE of red, green, and blue components respectively. “It has been shown that the best image quality can be found when the MSE value is very small or going to be zero since the difference between the original and reconstructed image is negligible. However, PSNR values between 20 and 40 can be considered as typical values. Moreover, as the PSNR value of a stego image is higher, the degree of hidden message imperceptibility is better” [15].

The results clearly showed that all the destruction techniques presented in section II destroy stego content in image file regardless of the kind of mechanism being used for embedding and sometimes enhance cover quality. The results shown in Table 1, show that the insertion of hidden text can cause minor alterations in the cover image. It will result image quality decreases but it may hard to distinguish visually. However, with the use of PSNR, the effect can be noticed. Therefore, tabulated results only presented because it can distinguish between the different systems under investigation as shown in Table 1. It is worth to mention that the PSNR achieved with hiding techniques are 17.35dB and 52.22dB, respectively for DCT and LSB hiding techniques. The results show that hiding a content in an image has the same effect as noise insertion. Thus denoising approaches can be used to destroy steganographic content because of their possibility to remove various noises from images. For this reason, reverse steganographic algorithm can't retrieve secret message from the steganographic image as well as the image quality will be increased.

The results shown in Table I show also the variation of PSNR for different cases of destruction techniques, overwriting and denoising. The investigation results show the effect of the type of filtering together with the thresholding used in the wavelet approach.

The results also shown in Tables II and III show the possibility of the proposed techniques to remove different image noise such as Gaussian, pepper and salt noise partially or totally, if exists. Table II shows the PSNR for denoising approach (filtering and wavelet) together with the overwriting approach when the cover image corrupted with Gaussian noise with variance (σ_n =20) , where σ_n is the noise variance. This effect is essential to show the effect of transmission or processing or any effect that might occur in the cover image. The results have shown the capability of all the present destruction techniques to remove the hidden data and recover the cover image but with different PSNR as shown in Table II. Extra form of noise has also been investigated Pepper and Salt with (d=0.02), where d is the noise density. The results also show the capability of the destruction achieved together with different PSNR as presented in Table III. Furthermore, it is well known that the forward steganographic algorithm adds a secret message to cover image noise. Therefore, the philosophy adopted in noise insertion in dealing with the secret content as a noise has been added to the pure image is verified. This is because most of the adopted techniques can remove noise (including noisy steganographic content, if any), and improve cover image quality. Thus, the noise effect and the investigation of PSNR after destruction are so essential to show how the cover image quality has been enhanced with the denoising techniques after hiding information destruction.

TABLE I. PSNR FOR DIFFERENT STEGO CONTENT DESTRUCTION TECHNIQUES AND DIFFERENT STEGANOGRAPHICTECHNIQUES

Destraction Techniques		*Hiding Techniques*	
		LSB	***DCT***
Filters Technique	MeanFilter	30.23	28.99
	WienerFilter	35.30	21.94
	HybridFilter	29.12	28.23
Wavelet Technique	Visu-Shrink	31.73	29.16
	Sure-Shrink	31.74	29.20
	Bayes-Shrink	31.96	30.02
Overwriting Technique		42.69	17.35

TABLE II. PSNR FOR DIFFERENT STEGO CONTENT DESTRUCTION TECHNIQUES AND DIFFERENT STEGANOGRAPHICTECHNIQUES WITH GAUSSIAN NOISY COVER

Destruction Techniques		*Hiding Techniques*	
		LSB	***DCT***
Filters Technique	MeanFilter	27.78	26.92
	WienerFilter	28.34	21.51
	HybridFilter	27.87	27.02
Wavelet Technique	Visu-Shrink	26.88	26.11
	Sure-Shrink	26.92	26.12
	Bayes-Shrink	26.71	26.39
Overwriting Technique		22.10	16.04

TABLE III. PSNR FOR DIFFERENT STEGO CONTENT DESTRUCTION TECHNIQUES AND DIFFERENT STEGANOGRAPHICTECHNIQUES WITH PEPPER & SALT (D=0.02)NOISY COVER.

Destruction Techniques		*Hiding Techniques*	
		LSB	***DCT***
Filters Technique	MeanFilter	27.72	26.72
	WienerFilter	23.31	20.99
	HybridFilter	27.74	26.78
Wavelet Technique	Visu-Shrink	26.91	25.96
	Sure-Shrink	26.89	25.97
	Bayes-Shrink	26.59	26.13
Overwriting Technique		22.40	16.01

The results show that the best denoising technique among others in terms of PSNR value is a Mean filter in the case of filtering, whereas Bayes-Shrink is the best in the case of discrete wavelet denoising. The latter assessment come from the calculation of the total average PSNR before and after destruction as shown in Tables IV and V, respectivelt.

TABLE IV. PSNR FOR DIFFERENT STEGANOGRAPHICTECHNIQUES WITH DIFFERENT NOISY COVER.

Cover Types	*Hiding Techniques*		*Total Average*
	LSB	***DCT***	
Pure Cover	52.22	17.35	34.78
Gaussian Noisy Cover with (σ_n =20)	22.11	16.02	19.06
Pepper & Solt Noisy Cover with (D=0.02)	22.10	15.99	19.04
Total Average	32.14	16.45	**24.29**

TABLE V. TOTAL AVERAGE OF PSNR FOR DIFFERENT STEGO CONTENT DESTRUCTION TECHNIQUES AND DIFFERENT STEGANOGRAPHICTECHNIQUES WITH DIFFERENT NOISY COVER.

Destruction Techniques		*Hiding Techniques*		*Total Average*
		LSB	***DCT***	
Filters Technique	**MeanFilter**	28.57	27.54	**28.05**
	WienerFilter	28.98	21.48	25.23
	HybridFilter	28.24	27.34	27.79
Wavelet Technique	Visu-Shrink	28.50	27.07	27.78
	Sure-Shrink	28.51	27.09	27.80
	Bayes-Shrink	28.42	27.51	**27.96**
Overwriting Technique		29.06	16.46	22.76

It is clear from Tables IV and V, that an enhancement of about 4dB has been achieved in the total average PSNR with use of destruction over all the cases studied.

Further investigation showed that Coiflets (5) wavelet was found to perform better in preserving fine signal details. Using wavelet based denoising approach, steganographic content isn't removed entirely, but it will crash entirely or molecularly depending on the amount of information embedded as well as used steganographic technique. Experimental results for two level decomposition approved that the Bayes Shrink thresholding way is the best one when the wavelet type is soft and mother wavelet is coif5. The results also show that the wavelet approach enhancement in the cover quality is less after two levels decomposition. Therefore, higher levels than two have been neglected in the decomposition stage. Furthermore, coif 5 mother wavelet and soft thresholding have been chosen because of the good performance achievement.

Finally, the PSNR for various denoising techniques, various steganographic techniques (LSB and DCT) and covers corrupted with various noises (Gaussian and Pepper and Salt) are compared. Furthermore, the results show that overwriting achieves better results only with LSB and non noisy images because it has been designed only for the case of overwriting over the used LSB. However, it gives no enhancement to the PSNR compared with denoising approaches.

IV. CONCLUSION

Several techniques have been investigated for destruction which is the main goal of the investigation. The paper has shown that it is possible to destroy any hidden information in images. The paper investigates the noisy effect of hiding and destruction. The results show Steganographic insertion causes minor alterations in cover image, so image quality decreases. Therefore, the approaches adopted of steganographic content behaviors as a noise in the image. The paper also shows that;

1. Denoising approaches can be used to destroy steganographic content because of their possibility to remove various noises from images. For this reason, reverse steganographic algorithm can't retrieve secret message from the steganographic image as well as the image quality will be increased.

2. Noise removal or rims blur will firstly target secret message length or steganographic key, if found, which is shared between intended parties in addition to targeting other parts of the image.
3. Mean filter and Bayes-Shrink thresholding techniques are the best methods in stego destruction and cover quality enhancement when compared to other methods that investigated in this research.
4. Overwriting approach is very successful in preventing the secret message being restored. However, the approach can target specific steganographic technique that is LSB or DCT technique while it may not compatible with other techniques of steganography. For this reason, denoising approach is much better than overwriting approach.

REFERENCES

[1] M. K. Sharma, and P. C. Gupta, " A Comparative Study of Steganography and Watermarking", International Journal of Research in IT & Management (IJRIM), Volume 2, Issue 2, pp. 2231-4334, February, 2012.

[2] S. Voloshynovskiy et-al, "StegoWall: Blind Statistical Detection of Hidden Data", *Proc. SPIE* 4675, Security and Watermarking of Multimedia Contents IV, 57 (April 29, 2002.

[3] F. Al-Naima, S. Y. Ameen, and A. F. Al-Saad, "Destroying Steganography Content in Image Files", The 5th International Symposium on Communication Systems, Networks and DSP (CSNDSP'06), Greece, 2006..

[4] I. S. Moskowitz, P. A. Lafferty, and F. Ahmed, "Stego Scrubbing A New Direction for Image Steganography", IEEE SMC Information Assurance and Security Workshop, IAW '07, 2007.

[5] W. Jamieson, "Destruction of Steganography: Targeting the Least Significant Bit in 24 bit Images", http://www.emich.edu/ia/pdf/research/pdf

[6] M.E. A. H. Al-Terki, "Implementationand Evaluationof Stego Image Destruction Method", MSc Thesis,Gulf University, Kingdom of Bahrain, January, 2012.

[7] S. Singh and T. J. Siddiqui, "A Security Enhanced Robust Steganography Algorithm for DataHiding",International Journal of Computer Science Issues (IJCSI), vol. 9, No. 1, pp. 1694-0814, May, 2012.

[8] A. Bijalwan, A. Goyal, and N. Sethi, "Wavelet Transform Based Image Denoise Using Threshold Approaches", International Journal of Engineering and Advanced Technology (IJEAT), Volume1, Issue-5, pp. 2249 – 8958, June, 2012.

[9] T. Y, H. Li and X. Zhao, "Noise Smoothing for Structural Vibration Test Signals Using anImproved Wavelet Thresholding Technique", MDPI, Sensors Journal , vol. 12, pp. 11205-11220, 2012.

[10] M. I. Mahmoud et-al, "Signal Denoising by Wavelet Packet Transformon FPGA Technology", UbiCC Journal, vol. 3, pp. 55-58, Jan. 2008.

[11] B. Ergen, " Signal and Image Denoising Using Wavelet Transform", Advances in Wavelet Theory and Their Applications in Engineering, Physics and Technology, Fırat University, Turkey, 2010.

[12] S. A. Hussain, and S. M. Gorashi, " An Efficient Implementation of Neighborhood based Wavelet Thresholding For Image Denoising" International Journal of Computer Applications, vol. 41, No. 9, March, pp. 0975 – 8887, 2012.

[13] S. A .H.Al-Ani, "Steganography Image in Image Using Modified Method in Least Significant Bit (LSB) Substitution", Um-Salama Science Journal, vol. 4, No.1, January, 2007.

[14] KM Harshitha and P. A. Vijaya, "Secure Data Hiding Algorithm Using Encrypted Secret Message", International Journal of Scientific and Research Publications, vol. 2, Issue 6, pp. 2250-3153,June, 2012.

[15] A. Almohammad, "Steganography-Based Secret and Reliable Communications: Improving Steganographic Capacity and Imperceptibility" MSc Thesis, Brunel University, August, 2010.