Wireless Sensor Network, **2009, 3, 163-170**
doi:10.4236/wsn.2009.13022 Published Online October 2009 (http://www.SciRP.org/journal/wsn/).

ContSteg: Contourlet-Based Steganography Method

Hedieh SAJEDI, Mansour JAMZAD
Computer Engineering Department, Sharif University of Technology, Tehran, Iran
E-mail: *A_sajedi@ce.sharif.edu, Jamzad@sharif.edu*
Received April 26, 2009; *revised May* 20, 2009; *accepted May* 25, 2009

Abstract

A category of techniques for secret data communication called steganography hides data in multimedia mediums. It involves embedding secret data into a cover-medium by means of small perceptible and statistical degradation. In this paper, a new adaptive steganography method based on contourlet transform is presented that provides large embedding capacity. We called the proposed method ContSteg. In contourlet decomposition of an image, edges are represented by the coefficients with large magnitudes. In ContSteg, these coefficients are considered for data embedding because human eyes are less sensitive in edgy and non-smooth regions of images. For embedding the secret data, contourlet subbands are divided into 4×4 blocks. Each bit of secret data is hidden by exchanging the value of two coefficients in a block of contourlet coefficients. According to the experimental results, the proposed method is capable of providing a larger embedding capacity without causing noticeable distortions of stego-images in comparison with a similar wavelet-based steganography approach. The result of examining the proposed method with two of the most powerful steganalysis algorithms show that we could successfully embed data in cover-images with the average embedding capacity of 0.05 bits per pixel.

Keywords: Information Hiding, Steganography, Steganalysis, Contourlet Transform

1. Introduction

Steganography methods hide the secret data in a cover carrier so that the existence of the embedded data is undetectable. The cover carrier can be different kinds of digital media such as text, image, audio, and video [1]. In a successful steganography method the carrier medium does not attract attentions. The security of the steganography methods is mostly influenced by the kind of cover media, the method for selection of places within the cover that might be modified, the type of embedding operation, and the number of embedding changes that is a quantity related to the length of the embedded data.

The aim of the steganography methods is to communicate securely in a completely undetectable manner. As the steganography techniques progress, there is an increased interest in steganalysis algorithms which their main goal is detecting the presence of hidden data.

Many steganography methods have been proposed and several stego-products have been developed (e.g., EzStego [2]) in which an innocuous-looking image is used as the cover-image to conceal the secret data. In these methods, the secret data is embedded into the cover-image by modifying the cover-image to form a stego-image.

Some image hiding systems use uncompressed images (e.g., BMP) or lossless compressed images (e.g., GIF) as cover-images. These images potentially contain visual redundancy so that they can provide large capacity to hide secret data. For reducing transmission bandwidth and storing space, the JPEG is currently the most common format for images that are used on the Internet. Therefore, embedding techniques in Discrete Cosine Transform (DCT) domain are popular because of the large usage of JPEG images. Although modifications of properly selected DCT coefficients during embedding process will not cause noticeable visual artifacts, nevertheless they cause detectable statistical degradations. Various steganography methods like F5 [3], Outguess [4], Model-based (MB) [5], Perturbed Quantization (PQ) [6], and YASS [7] have been proposed with the purpose of minimizing the statistical artifacts which are produced by modifications of DCT coefficients.

On the other hand, some steganography methods based on wavelet transform have been presented. In [8], a steganography method based on wavelet and modulus function is proposed. In this method, the capacity of a

cover-image is determined considering the number of wavelet coefficients with larger magnitude.

Embedding data in adaptively selected parts of cover-images such as regions having edges and texture enhances the security of stego-images [9]. An adaptive steganography method attempts to provide secure embedding by ensuring that the changes introduced into the cover-images remain consistent with natural properties of them. Since human eyes are less sensitive in edgy and non-smooth regions of images, modifications in these parts of cover-images are less detectable.

In [10] we proposed a new steganography method that embeds secret data in contourlet coefficients of images. In this paper, we describe the method introduced in [10] with more details and complete our experiments with a larger image database. In this paper, we introduce ContSteg, which is a method based on contourlet transform for hiding data in images. In ContSteg, contourlet transform is applied to capture significant image coefficients across spatial and directional resolutions. Multiresolution flexibility, local and directional image expansion in the contourlet image representation, allow for easy subband processing [11]. To increase the embedding capacity and quality of stego-images compared to previous methods, we embed the secret data in proper contourlet coefficients of the cover-image. The embedding algorithm takes advantage of adaptive methods by embedding data in non-smooth regions of cover images. In this way, the visual degradation caused by the steganography method can be mitigated because the secret data is embedded in higher contourlet coefficients in edgy and non-smooth areas that can visually hide this information better [12]. The embedding process is carried on by changing the value of two contourlet coefficients to hide one bit of secret data.

The experimental results illustrated that the proposed method can hide much more data while maintaining a good visual quality of stego-images compared to the similar wavelet-based steganography methods. We verified that by employing two well-known and efficient steganalysis methods. They could not discriminate between clean and stego-images reliably.

The rest of this paper is organized as follows. In Section 2, we introduce the proposed steganography method, ContSteg, and discuss the main characteristics of contourlet transform. Performance of the presented method is analyzed in Section 3 and finally, we conclude this paper in Section 4.

2. ContSteg

Using suitable representation domain and proper coefficients to embed data, can result in stego-images with higher quality. Consequently, higher embedding capacity and enhanced security are provided. Accordingly, in this paper, a new method is proposed which is called ContSteg. It takes advantage of a multiscale framework and its directionality to extract the appropriate places of an image to hide data. ContSteg like other steganography methods consists of an embedding process and an extraction process. Figure 1 shows the block diagram of embedding and extraction processes of ContSteg. The details of these processes are described in the following subsections.

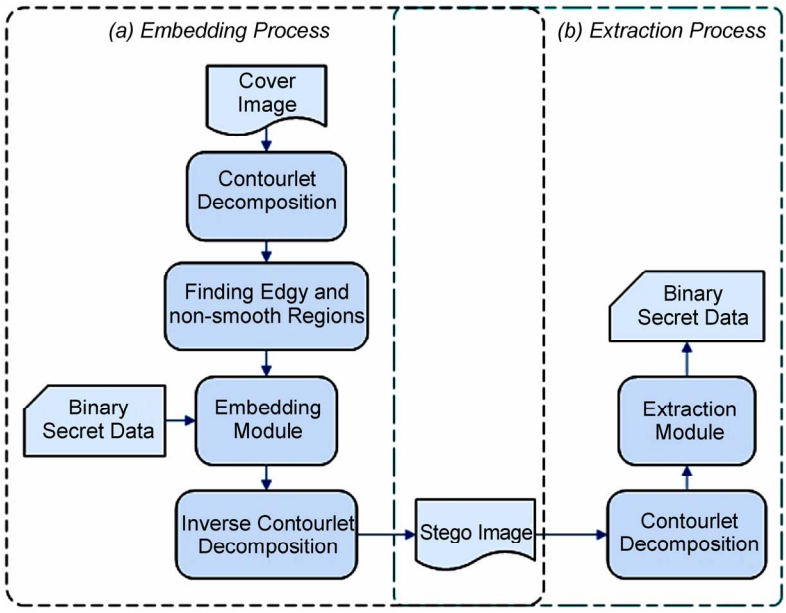

Figure 1. The block diagram of ContSteg steganography method, (a) Embedding process, (b) Extraction process.

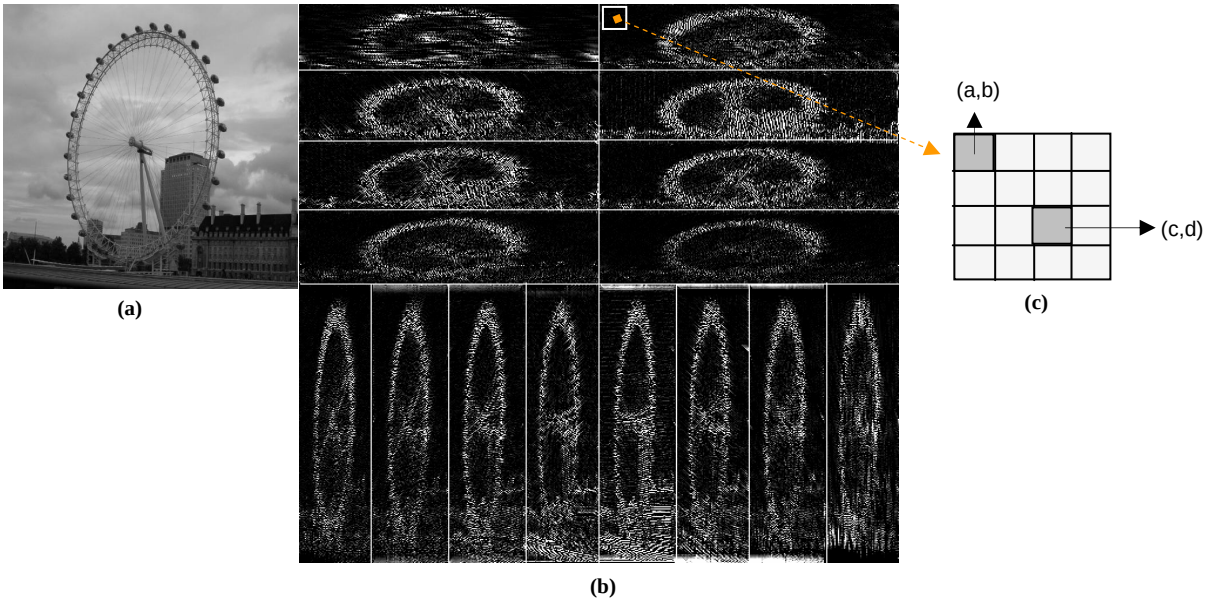

Figure 2. Embedding data in contourlet coefficients of an image, (a) Original input image, (b)Visualization of contourlet decomposition of an image into one pyramidal level and sixteen directional subbands, (c) A 4×4 block of contourlet coefficients and the place of two coefficients for embedding.

2.1. Hiding Data in Contourlet Coefficients

Contourlet transform is one of several transforms developed in recent years, aimed at improving the representation sparsity of images over the wavelet transform. The main feature of this transform is the potential to handle 2-D singularities efficiently, i.e. edges, unlike wavelet, which can deal with point (i.e.1-D) singularities exclusively [13]. Contourlet transform is a directional extension of wavelet transform that fixes the wavelet subband-mixing problem and improves its directionality. Two-dimensional wavelet transform produces one approximation subband, and three details subbands, corresponding to the horizontal, vertical, and diagonal directions. The diagonal subband mixes the directional information oriented at 45◦ and 135◦. The main idea of contourlet is to find some directional extensions to divide further each detail subband of the wavelet into a number of directions. This transform is based on a double filter bank structure by combining the Laplacian pyramid with a directional filter bank [14]. Figure 2 shows an image that is decomposed into one pyramidal level and sixteen directional subbands (higher coefficients are colored white).

Because of the subband-mixing problem in wavelet transform, manipulating one coefficient in diagonal subband affects the value of other relevant coefficients in other directions. We used the effectiveness of contourlet transform in image decomposition to separate directions. Hence, manipulating the value of a coefficient in the contourlet subbands has less effect in the quality of the image than changing a coefficient in wavelet subbands. Furthermore, most of the current existing steganalysis algorithms are limited to the domain of spatial, wavelet, and DCT transform. Therefore, distinguishing cover-images from stego-images (constructed by embedding data into their contourlet coefficients) is not easy by these steganalysis algorithms. Accordingly, considering the fact that higher embedding efficiency translates into better steganographic security, more secure stego-images are achieved using the proposed method.

2.2. Embedding Process

The embedding process is done in the following steps:

Step 1: The cover-image is decomposed with one pyramidal level and sixteen directional contourlet transform.

Step 2: The regions of the subbands in which the data can be embedded are identified. Then the embedding process determines higher contourlet coefficients in these regions that can be used for embedding.

Step 3: According to Kerckhoffs' principle [15], the embedding algorithm is supposed to be known to the public. Therefore, the embedding process may use an embedding key so that only the legal user can successfully extract the embedded data by using the corresponding extraction key in the extraction process. Accordingly, a key that is a seed for generating a random sequence is considered to provide the embedding location addresses of 4×4 blocks.

Step 4: In this step, the embedding module is activated. The place of two coefficients in each block are chosen by the embedding module and agreed upon by both send and receive parties. These two coefficients are suitable for embedding if both of them belong to the higher coefficients set. The embedding module hides each bit of the secret data by comparing and if needed exchanging the values of two contourlet coefficients in non-smooth regions of the image. We use two coefficients that are shown in Figure 2(c). A 4×4 block encodes bit *1* if its *coefficient*(*a,b*) >= *coefficient*(*c,d*) and bit *0* otherwise. Two coefficients are swapped if their values do not match with the bit to be encoded. Since the JPEG compression, rounding in computation, and non-orthogonality of contourlet transform can affect the relative size of the coefficients, the embedding module ensures that $|coefficient(a,b) - coefficient(c,d)| > t$, where t is a value that represents the tradeoff between image quality and hidden data retrieval error rate. We set t =2 experimentally. Due to the cases we mentioned before, manipulating the value of coefficients may cause loss of the embedded data in inverse contourlet transform. In addition, it may affect the value of neighborhood coefficients and thus the embedded data in such neighborhood may be lost. To maintain a high level of similarity between the original clean and stego-images, and to have minimum loss in extracted data, each candidate coefficient for embedding should has a distance form other candidate coefficients. Considering these properties, we embed each bit in coefficient block of size 4×4. In this fashion, a candidate coefficient has the least closeness to other candidates. Figure 3 shows a part of a contourlet subband, which has some 4×4 blocks. As the figure shows, candidate coefficients for embedding are considered far from other candidates.

2.3. Extraction Process

The stego-key used in the embedding process should be shared by both the sender and receiver so that the embedded data can be extracted by a legal receiver. The extraction module consists of the following steps:

Step 1: Decompose stego-image with a one level contourlet transform.

Step 2: Recognize higher contourlet coefficients.

Step 3: Form the random sequence by using the same key as the sender has used.

Step 4: Retrieve the embedded data by comparing *coefficient* (*a,b*) and *coefficient*(*c,d*) in each 4×4 coefficient block. If *coefficient*(*a,b*) >= *coefficient*

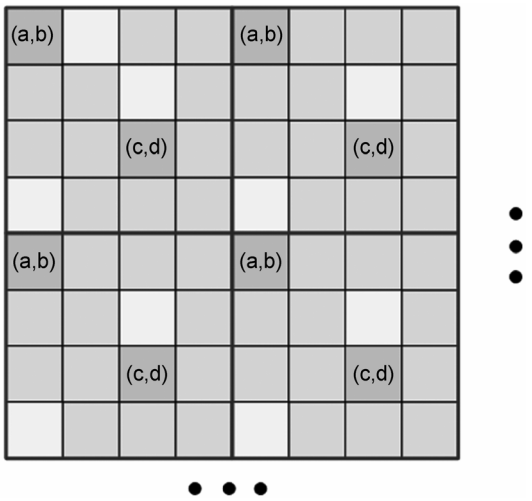

Figure 3. A part of a contourlet subband with some 4×4 blocks. Candidate coefficients (shown in dark gray) for embedding are at least one pixel apart from other candidates.

(*c,d*) , the hidden bit is *1* and it is *0* otherwise.

Figure 1(b) shows the block diagram of the extraction process of ContSteg.

3. Experiments

We did different experiments to assess the efficiency of the proposed method. We collected 1000 images from some typical images and some random ones from Washington University image database [16]. All images were converted to grayscale and cropped to size of 512×512. The JPEG quality factor of images is 75. To obtain a stego-dataset, for each cover-image a random binary data was embedded using ContSteg. Therefore, in our database we have 2000 images, 1000 cover-images, and 1000 stego-images.

3.1. Efficiency of ContSteg

In this experiment, we assess the efficiency of ContSteg in terms of quality of stego-images and embedding rate of ContSteg.

3.1.1. Calculation of Embedding Rate

In the proposed method, the desired frequency partitioning for a $N \times N$ size image by contourlet transform contains of sixteen directional subbands of size $N/8 \times N/2$ in first level of decomposition. By embedding one bit of secret data in each 4×4 block of all subbands, the embedding capacity of an image will be $(N \times N)/16$. If C percents of coefficients are used for embedding, then the embedding rate is $C/16$ bits per pixel. In most of the steganography methods based on wavelet transform, approximation subband is not used for embedding. Because

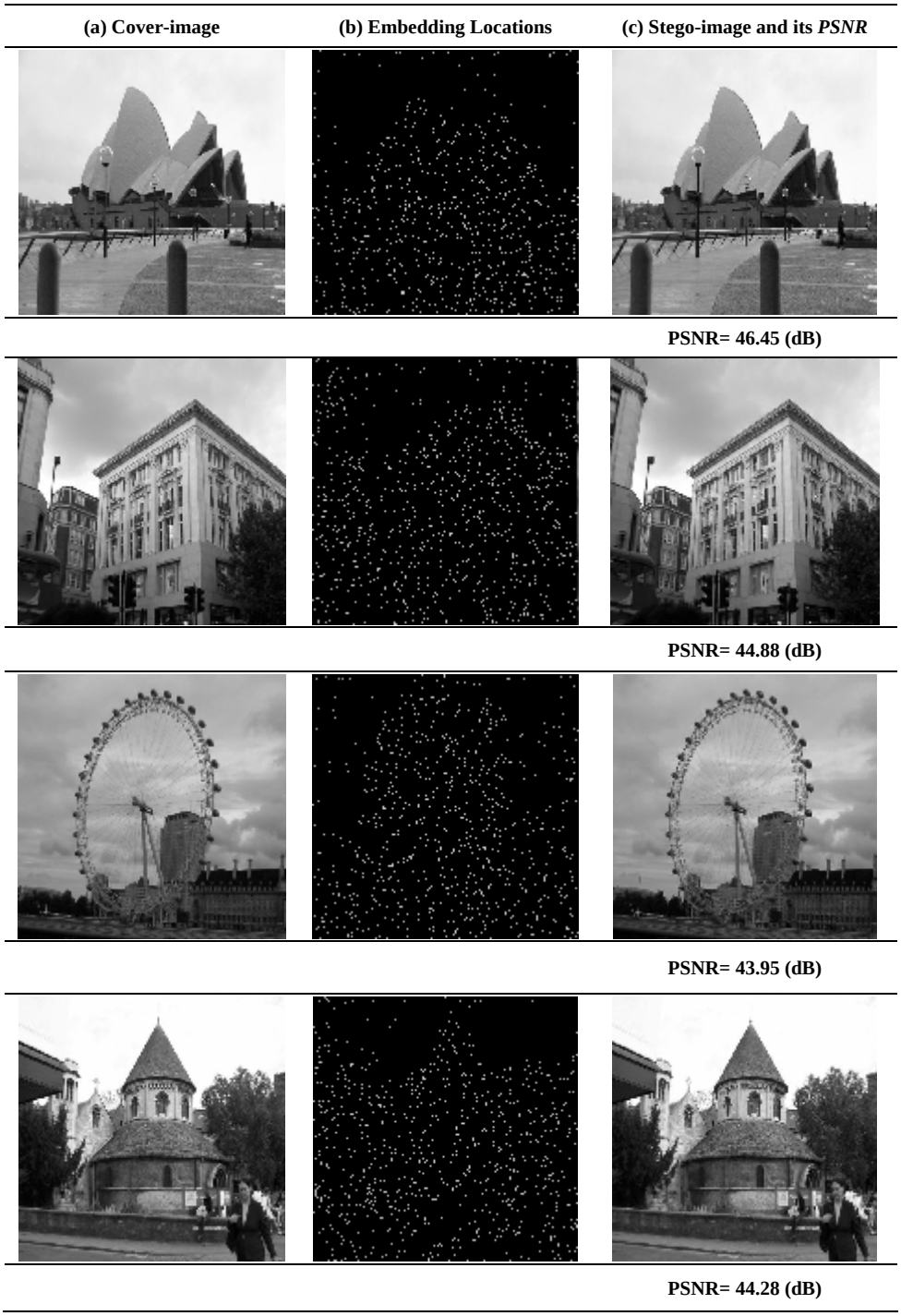

Figure 4. Computing the quality of stego-images, (a) Cover-image, (b) Proper locations for embedding are colored white, (c) Stego-image with its PSNR.

changing the coefficients in approximation subband imposes a large distortion in the stego images. Hence, in this case the embedding rate should be very low. Therefore, for a $N \times N$ image, in the first level of decomposition, the number of contourlet coefficients is $(N \times N)/4$ more than wavelet coefficients. Therefore, more embedding rate can be archived in this domain. For a 512×512 size image, the number of contourlet coefficients is 262144. This number is equal to the number of image pixels. If we keep 50 percent of higher coefficients, we have 131072 coefficients. If one bit is embedded in each 4×4 block, the maximum rate for embedding is about 0.03

bits per pixel. By this configuration, in the best condition (since we embed only in coefficients with higher amplitude, a block is proper for embedding if it has coefficients with higher amplitude) we can embed 8192 bits of data in the mentioned image. Using greater percent ($C>50$) of coefficients with higher amplitude for embedding provides higher embedding rate (>8192).

3.1.2. Computing the Quality of Stego-Images

In this evaluation, we consider perceived quality of stego-images. Figure 4 shows some cover-images, the locations to embed data and the stego-images after embedding 5600 bits. The results show that the quality of stego-images is high, and unintended observers cannot be aware of the existence of hidden data in it. The imperceptibility is evaluated by the objective quality measurement *PSNR* (peak signal to noise ratio) [17]:

$$PSNR = 10 \times \log\left(\frac{255^2}{MSE}\right) \quad (1)$$

where *MSE* represents the mean square error between the cover-image x and the stego-image y both of size 512×512.

$$MSE = \left(\frac{1}{512 \times 512}\right) \sum_{i=1}^{512} \sum_{j=1}^{512} (x_{ij} - y_{ij})^2 \quad (2)$$

Figure 5 shows the average *PSNR* for images of size 512×512 after embedding the secret data of size 3000 to 12000 bits in wavelet and contourlet coefficients of images. In this figure, the points on the curve correspond to the average *PSNR* of stego-images in the database with certain payloads. For example, for payload of 3000 bits some stego images in our database has *PSNR* above 45 (dB) and some other have *PSNR* below 35 (dB) but averagely *PSNR* is about 38.8 (dB). The embedding and extraction processes in wavelet and contourlet domains are the same. The results show that embedding in contourlet transform domain increases the quality of stegoimages.

3.2. Protection against JPEG Compression

Due to the rounding in computation, and non-orthogonality of wavelet and contourlet, embedding methods in both of these domains have less than 1% loss of the secret data in the worst case. For lossless data recovery, we have to use a redundancy factor in an error correction framework. Table 1 shows the evaluation of proposed steganography technique against JPEG compression. As we see, the proposed method has not a good robustness against compression but with the cost of lower quality stego-images (e.g. using hamming code algorithm that makes the secret data secure with added redundancy), higher robustness against compression can be achieved.

3.3. Steganalysis Results

Wavelet-based steganalysis (WBS) [18], and Feature-based steganalysis (FBS) [19], and Contourlet-based (CBS) [20] methods are used to evaluate the security of ContSteg. In WBS, a Fisher Linear Discriminator (FLD) and in FBS and CBS, a nonlinear Support Vector Machine (SVM) is trained to discriminate between clean and stego-images. 1200 images (600 cover and 600 stego images) from database were chosen randomly for testing, while the remaining 800 images were used for training. This partitioning was repeated ten times, with different random subsets used for training and testing each time. The average of detection accuracy is shown in Table 2. The accuracy is the average of true detection of both stego and clean-images. As can be seen, the detection accuracy is about 50% and the proposed method with payload of approximately 0.05 bits per pixel cannot be reliably detected by the applied steganalyzers.

It is shown in [21] that the average embedding capacity of existing steganography methods for grayscale JPEG

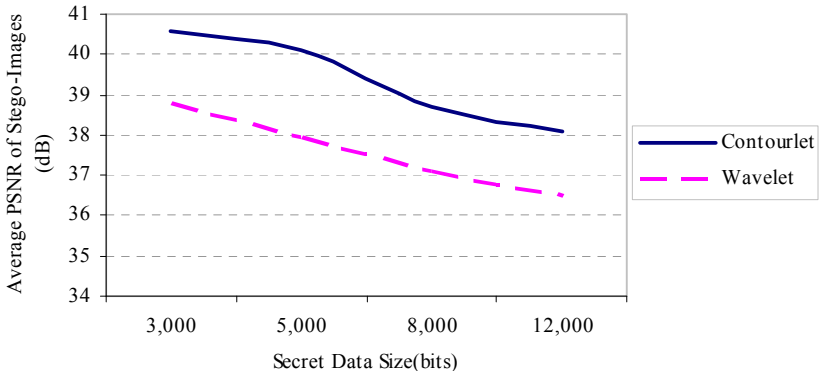

Figure 5. Comparing the quality of stego-images produced by wavelet-based and contourlet-based steganography methods.

Table 1. Retrieval error rate of hidden data after JPEG compression.

Secret Data Size (bits)	Quality Factor	Retrieval Error Rate (%)
5,000	90 , 70 , 50	10 , 14 , 20
10,000	90 , 70 , 50	13 , 18 , 26

Table 2. Accuracy of WBS, FBS, and CBS steganalysis methods on detection of stego-images produced by ContSteg.

Secret Data Size (bits)	Steganalysis Method	Average Detection Accuracy (%)
5,000	WBS	51
	FBS	53
	CBS	59
10,000	WBS	53
	FBS	54
	CBS	63
15,000	WBS	58
	FBS	61
	CBS	68

images with quality factor of 70 is approximately 0.05 bits per non-zero AC DCT coefficient. For a 512×512 image, 4096 blocks of size 8×8 is existed. Usually 20 AC DCT coefficients are considered non-zero. Therefore, we have 4096×20=81920 non-zero coefficients. Hence, the capacity is 81920×0.05=4096 which is 4096/ (512×512) =0.015 bits per pixel. We see that our proposed method has higher embedding capacity.

4. Conclusions

Steganography that is a branch of information hiding technology aims to hide a secret data securely in a cover media for transmission. Embedding rate and stego-image quality are two important criteria in evaluating a steganography method. In this paper, a new secure and adaptive steganography is presented which is called ContSteg. It embeds a secret data in contourlet transform coefficients of an image. Since embedding data in non-smooth and edgy regions of the image causes less delectability, these regions of the image are identified in contourlet domain and the secret data is embedded in the corresponding coefficients. According to the experimental results, in comparison with wavelet domain approach, the proposed steganography method increases embedding rate and image quality of the stego-images by hiding the secret data in contourlet coefficients corresponding to high frequencies. The results of our experiments show that employing two of powerful steganalyzers on stego-images produced by our method, they could not discriminate between stego and clean-images reliably. In general, ContSteg is a secure steganography method that provides high embedding capacity and high image quality.

5. References

[1] C. Liu and S. Liao, "High-performance JPEG steganography using complementary embedding strategy," Pattern Recognition, Vol. 41, pp. 2945–2955, 2008.

[2] EzStego, http://www.securityfocus.com/tools/586.

[3] A. Westfeld, "F5-a steganographic algorithm: High capacity despite better steganalysis," Proceeding of 4th International Workshop on Information Hiding, 2001.

[4] N. Provos, "Defending against statistical steganalysis," Proceeding of 10th USENIX Security Symposium, pp. 323–336, 2001.

[5] P. Sallee, "Model-based steganography," Proceeding of International Workshop on Digital Watermarking, Seoul, Korea, 2003.

[6] J. Fridrich, M. Goljan, and D. Soukal, "Perturbed quantization steganography with wet paper codes," Proceeding of ACM Multimedia Workshop, Germany, 2004.

[7] K. Solanki, A. Sarkar, and B. S. Manjunath, "YASS: Yet another steganographic scheme that resists blind steganalysis," Proceeding of 9th International Workshop on Information Hiding, June 2007.

[8] K. Zhiwei, L. Jing, and H. Yigang, "Steganography based on wavelet transform and modulus function," Journal of

Systems Engineering and Electronics, Vol. 18, No. 3, pp. 628–632, 2007.

[9] J. Fridrich and R. Du, "Secure steganographic methods for palette images," Proceeding of 2nd International Information Hiding Workshop. LNCS, Vol. 1768, pp. 47–60, 2000.

[10] H. Sajedi and M. Jamzad, "Adaptive steganography method based on contourlet transform," Proceedings of 9th International Conference on Signal Processing (ICSP'08), October 26–29, 2008.

[11] M. Do and M. Vetterli, "Contourlets: A directional multiresolution image representation," Proceedings of ICIP, 2002.

[12] N. Kaewkamnerd and K. R. Rao, "Wavelet based image adaptive watermarking scheme," Electronic Letters, Vol. 36, pp. 312–313, 2000.

[13] B. Matalon, M. Elad, and M. Zibulevsky, "Image denoising with the contourlet transform," Proceeding of SPIE Conference Wavelets, 2005.

[14] Y. Lu and M. N. Do, "A directional extension for multidimensional wavelet transforms," IP EDICS: 2-WAVP (Wavelets and Multiresolution Processing), 2005.

[15] J. Seberry and J. Pieprzyk, "CRYPTOGRAPHY: An introduction to computer security," Prentice-Hall, New York, 1989.

[16] http://www.cs.washington.edu/research/imagedatabase.

[17] A. K. Jain, "Fundamentals of digital image processing," Prentice-Hall, New Jersey, 1989.

[18] S. Lyu and H. Farid, "Detecting hidden messages using higher-order statistics and support vector machines," Proceeding of 5th International Workshop on Information Hiding, 2002.

[19] J. Fridrich, "Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes," Proceeding of 6th Information Hiding Workshop, Toronto, 2004.

[20] H. Sajedi and M. Jamzad, "A steganalysis method based on contourlet transform coefficients," Proceeding of 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008.

[21] J. Fridrich, T. Pevný, and J. Kodovský, "Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities," MM&Sec, ACM, Dallas, USA, 2007.

