J. Basic. Appl. Sci. Res., 3(2s)255-259, 2013

© 2013, TextRoad Publication

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

Using Contourlet Transform and Jpeg Compression for Digital Image Steganography

Younes Barkhordari[1], Seyed Hossein Moayed[2], Ali Ghareh Aghaji[3], Abdolhossein Sa'aedi[4*]

[1] Department of Electronics, Poldokhtar Branch, Islamic Azad University, Poldokhtar, Iran
[2] Department of Electronics, Thecnical and Vocational University, Larestan, Iran
[3] Department of Electronics, Shahid Beheshti University, Tehran, Iran
[4] Department of Electronics, Boushehr Branch, Islamic Azad University, Boushehr, Iran

Received: June 10 2013
Accepted: July 10 2013

ABSTRACT

In this paper a new approach foe digital image steganography is presented. Using JPEG compression is a significant tool for this approach. Image modify is done according to embedded data bit in contourlet domain and on contourlet coefficients. In this approach proposing data embedding algorithm such that contourlet coefficients are modified only in embedding bit 1 helps to improve PSNR in a high capacity. Embedding each data bit is done in a block of contourlet sub-band. The difference between maximum and minimum of contourlet coefficients is the index of embedding in each block. Result of algorithm implementation show that also some strong steganalysis approaches don’t have good performance in detecting stego images.

KEYWORDS: countourlet transform; steganalysis; steganography; JPEG compression.

INTRODUCTION

Steganography like cryptography is a tool for hidden communication. In steganography a content such as video, voice, image or text is use for information transform. The main difference of two communication approach is that the enemy has no access to information codes in cryptograph in steganography there is no data available for enemy (Mathkour & Al-Sadoun, 2008). Now because of internet as an easy and general way for communication, digital image are proper tools for hiding data. From data hiding viewpoint in images, steganography is similar to watermarking but there is a basic difference between them, including that in watermarking the image itself is important and hidden data in that witch is used for demonstrating position right while in steganography The content is data transfer and image is used as a cover for transporting secret message and can be substitute by any other image. Generally, there are similar levels in hiding information. First information is imbedded in a raw image used for imbedding data and it called cover image by a key witch is common between start point and destination. There resulting image witch transport data bits is called stego image. hiding information in image methods are performed in two domain: spatial and transformed. Spatial domain advantages in which data algorithm, embedding in e short time, and high capacity spatial domain has a weak point witch is being weak against attack including steganalysis methods. Steganography in transform domain is that firstly a transform such as CT, DWT and DCT is captured from cover. The data is embedded in coefficients and the transformed inverse is applied. Is clear that this approach takes a lot of time and despite algorithm complexity against enemy attack in none-negligible property of that (Yu et al., 2009).

In hiding information, three main elements are important: capacity, security and robustness, and among them capacity and security are more important in steganography because of there use in hidden communication (Shetty et al., 2009). On the other hand we should make a tradeoff between this two properties because increasing capacity (number of hidden bits in image) causes low security and vice versa.

Increasing data has an impact on both security and image eye quality and causes image destruction in high capacity.

Against steganography, steganalysis is the art and knowledge of another use of steganalysis is in comparing security of attention recently. Steganography approaches. A steganalysis method decides whether an image contains information or not. According to this, images are divided into two groups: cover and stego (Sajedi & Jamzad, 2010a). Statistical steganalysis approaches are among successful ones witch act by the use of training learning methods based on cover and stego image features. So from invisibility viewpoint a good steganography method is the 1 witch makes the least changes in images during embedding data and the disturbance resulted from embedding doesn’t change data features. Besides different steganography approaches, strong approaches are proposed having high resistance against statistical steganalysis. Among

***Corresponding Author:** Abdolhossein Sa'aedi, Department of Electronics, Boushehr Branch, Islamic Azad University, Boushehr, Iran. e-mail: a.h.saaedi@iaubushehr.ac.ir

them we can point to (Solanki et al., 2007). Witch is a transform domain approach and is based on DCT. Despite its high capacity, this approach is invisible against steganalysis methods.

Also, Sallee in (Sallee, 2003) has tried for keeping statistical features of cover image unchanged after embedding and that led to the fail of statistical steganalysis approaches. In PQ method (Fridrich et al., 2004), lack of distortion in embedded image for escaping from discovering from steganalysis attack has been important and has had success. In (Sajedi & Jamzad, 2010b) Jamzad and his assistants have presented a better approach for fighting witch enemy's statistical attacks by embedding data in contourlet coefficients and according them with cover image. There are images with different formats but JPEG format has many uses specially in content with internet. Therefore many steganography methods or images are done by this format.

Contourlet transform

As mentioned above hiding data in transform domain is good method in steganography. In all transform domain approaches, first we capture a transform from cover, then the 0 or 1 of digital data is embedded in coefficient by the help of key by modifying resulting coefficients. Then a transform is captured from image remains to get to stego. This image is sent to destination and there also a transform is captured from stego first and then data is extracted by the use of a common data key.

One of the most important transforms for contourlet transform presented first in 2003 by Lu and Do. It consist of two structures: laplacian pyramid (LP) and directional filter bank. In LP structure like wavelet transform, the image is decomposed to several sub-bands in witch the low frequency sub-band can be decomposed again and it can be resumed if the user needs it. If a transform is captured from a N*N image, number of coefficients in level is N/2*N/2, and in third level N/4*N/4 and these coefficients decrease by this trend. Using directional filter bank of contourlet transform for level decomposition is in different directions. Applying directional filter bank after decomposition by pyramid bank is shown in *Fig. 1*. *Fig. 2* shows Lena decomposition in two scales and four and eight directions.

In this way, contourlet transform discovers image edges in frequency bands and different directions and shows them by numbers called contourlet coefficients. Advantage of this transform to wavelet transform in steganography is less effect of change in a frequency band on other bands coefficients. Though effect of changing a coefficient on neighbor ones is inevitable because of non-orthogonal contourlet transform and saving images in JPEG format. These changes are investigable after contourlet inverse transforms and their decomposition to coefficients.

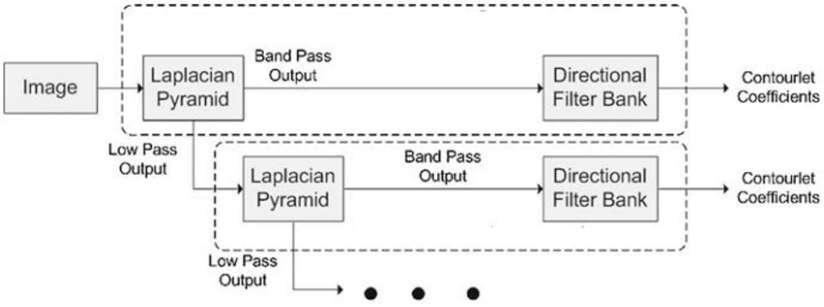

Figure 1. *Conourlet transform diagram*

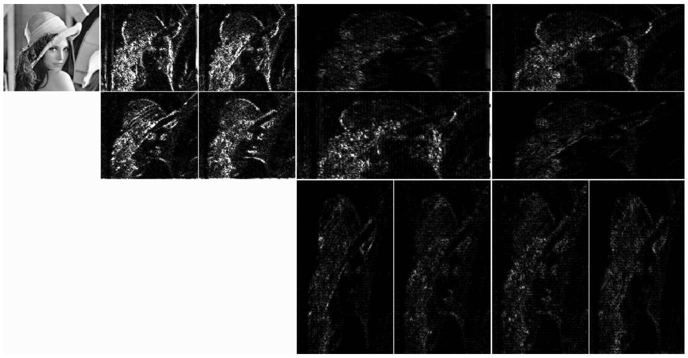

Figure 2*. Decompose Lena to Contourlet Coefficients*

Proposed method

In proposed approach which embeds data in image by modifying contourlet coefficients, despite high capacity of data, changes is image are little thus eye quality of image is high and its visibility against steganalysis attacks is low.

Data embedding

In this approach two important tools are used: contourlet transform and JPEG compression. First the image is compacted with an arbitrary quality coefficient (such as 50%). This coefficient then will be common as a key between transmitter and receiver. Then a two level contourlet transform each in four directions is captured from resulted image which is the same cover image. So first level contains four frequency sub-bands. To implement proposed algorithm, we use 3 high frequency sub-bands. m×n blocks of coefficients are selected in each sub-band in which any data bit is embedded in a block. Selected blocks aren't pasted to each other because of the effect of coefficient changes on other neighbor coefficients during coefficient modify for date embedding. Each block has a distance from 4 directions to other ones. It cause that modifying a coefficient doesn't have a significant change in important coefficients of other blocks. Its clear that the less distance of blocks, the more distance of embedding capacity and the more distortion caused by embedding data. Size and distance of blocks can be used as key. Important coefficients of each block are minimum and maximum coefficients which are changed. Embedding data steps are as follows:

step 1: A JPEG compression is captured from image with determined quality coefficient.

step 2: Using contourlet transform we decompose resulted image to contourlet coefficients.

step 3: We select m*n blocks with distance in 3 high frequency sub-bands and find minimum and maximum of coefficients. We then find their difference and call it dif (dif=max-min).

step 4: To embed data we do as follows: if data bit is 1 then we increase calculated difference as threshold. To do that we increase the maximum as half of threshold and decrease the minimum as half of threshold too. So the new difference is greater than old one as threshold, it means dif=dif +t. to assure this increase in difference, we capture an inverse transform and contourlet transform in a repeated loop and do it until reaching proper value. But if the data bit is 0, we don't change or modify coefficients.

step 5: We do steps 3 and 4 for all bits. In other words, we keep blocks containing 0 unchanged and apply modify on blocks containing 1.

We capture inverse contourlet transform from final modified coefficients and after sawing that in JPEG format, make stego image ready to send.

Data extraction

Extracting data steps in destination are as following:

step 1: We compact received image called S with the same quality coefficient. Result is S'. We capture a contourlet transform form S and S'.

step 2: in each coefficient caused by contourlet decomposition in three sub-bands, we determine blocks and calculate minimum, maximum and their difference.

step 3: In each block if dif is greater than dif' as t/2 then extracted bit is 1 else it is 0. In watermarking approaches, there is a blind watermarking comprehension. This comprehension means that we need main image besides stego image to extract data bits. Then 0 or 1 bit is easily extracting by comparing changes in stego and over image it causes low increase or decrease of coefficient during data embedding. As cover steganography is only a tool for data transport. We have no access to main image during data extracting. Thus blind watermarking has no place.

What is interesting in this method is that when we compact the cover image in destination, we reach an image quite similar to main image. Thus we can express opinions about extracted bit by comparing difference in cover blocks and the same parameter.

We can understand from what expressed about proposed approach the reason of that for embedding 0s we have no change in coefficient despite many approaches.

Implementation results

Proposed algorithm is first applied on unknown images such as Lena and Peppers and evaluate the eye quality of image in respect to capacity (which is the size of blocks and their distances). Then for investigating the robustness of algorithm against steganalysis attacks, we have used 1000 images. These images are chosen random and with no special feature. First we change size of image to 512×512 and make it gray scale. Then we embed data in 1000 images and reach to 1000 stego images which are totally 2000 images and steganalysis images are tested on them.

Investigating distortion

The comparison rate of this parameter in steganalysis approaches is the signal to noise ratio which is calculated as Eq. (1).

$$PSNR = 20\log_{10}\frac{255}{\sqrt{MSE}} \qquad (1)$$

In this relation mean square error is called MSE and is written as Eq. (2).

$$MSE = \sum_{x=1}^{m}\sum_{y=1}^{n}[p(x,y) - p'(x,y)]^2 \qquad (2)$$

In which m×n, P(x,y) and P'(x,y) are image size, cover image pixels and stego image pixels in x and y location respectively.

Signal to noise ratio is calculated in respect of dB and as it increases, distortion caused by data embedding in image decreases. *Table 1* shows PSNR for different data embedding capacities.

Table 1. *PSNR for different data embedding capacities for Lena*

Block Size	**2*3**	**2*2**	**4*3**	**5*3**	**4*3**	**5*3**
Block Distance	2	3	2	2	3	3
Capacity (bits)	9450	7500	6300	5400	4536	4032
PSNR	47/18	47/59	50/13	51/29	51/82	52/56

As expected, PSNR is decreased as hidden bits increase. In *Table 2*, PSNR is compared to the one presented in . It is seen that signal to noise in proposed approach is very different from (Sajedi & Jamzad, 2010b) in the same capacities.

Table 2. *PSNR comparison of method in (Sajedi & Jamzad, 2010b) and proposed method*

Propose Method		**(Sajedi & Jamzad, 2010b)**	
PSNR	Number of Bits	PSNR	Number of Bits
51.82	4536	40.37	4096
51.29	5400	39.43	5184
47.18	9450	37.25	9738

Steganalysis approach results

In steganalysis approaches, the main target is categorizing images in two groups: cover images and stego images in blind approach it is done by training and classifying by image features.

In this paper four blind steganalysis approaches are used in which extracting some of statistical and their classification is done by support vector machine.

Steganalysis approaches are:

1. Steganalysis in discrete cosinusoidal transform domain and spatial domain in **(**Fridrich, 2004**)** which extracts 23 features of image.
2. Steganalysis in wavelet transform domain which extracts 36 steganalysis features **(**Lyu & Farid, 2002**)**.
3. Steganalysis approach presented in **(**Pevny & Fridrich, 2007**)** which uses 81 Markov features with 193 feature in DCT domain.
4. Approach presented in (Chen et al., 2006) which calculates 390 feature of image. In each of above approaches, after extracting features of 2000 images (1000 images without data and 1000 images containing data) in which the agent of each image is a vector with the length of number of proposed features in our algorithm, we give the vectors to a SVM.

SVM uses 60% of images (1200 images) for training and the 40% remaining for classifying. In each SVM run, training vectors are selected random.

Accuracy is steganalysis approach ability to diagnose stego from cover images correctly and it is expressed as percentage. In *Table 3*, accuracy of 4 steganalysis approach for stego images in comparison to 4 steganography approach are shown. Data capacity is 5000 and accuracy is in percentage ability of proposed algorithm than other ones is clear in both experiments.

Table 3. *PSNR for different data embedding capacities for Lena*

Steganalysis	**(Mathkour & Al-Sadoun, 2008)**	**(Pevny & Fridrich, 2007)**	**(Lyu & Farid, 2002)**	**(Fridrich, 2004)**
Steganography				
(Fridrich et al., 2004)	89	70	71	93
(Sallee, 2003)	98	76	61	87
(Solanki et al., 2007)	51	69	60	57
(Sajedi & Jamzad, 2010b)	55	65	62	54
Proposed Method	54	60	49	54

Conclusion

In this paper, a steganography approach based on JPEG compression feature and embedding data in contourlet coefficients is presented. In this approach, as we access to an image whose features are similar to main image by compression stego image, much change on contourlet coefficient are not essential during embedding and therefore image has high PSNR. Another capability of this approach is high capacity of hidden data.

Also, low changes on image caused by data embedding has caused steganalysis approach to diagnose stego from cover images with an accuracy close to random estimate.

REFERENCES

[1] Chen. C, Shi. Y.Q, Chen. W and Xuan. G, (2006), Statistical moments based universal steganalysis using JPEG-2D array and 2-D characteristic function, Proceedings of ICIP, 105–108.

[2] Fridrich. J, (2004), Feature-based steganalysis for jpeg images and its implications for future design of steganographic schemes, Int. Conf. on 6th Information Hiding Workshop. Toronto.

[3] Fridrich. J, Goljan. M and D. Soukal, (2004), Perturbed quantization steganography with wet paper codes", Proc. Int. Conf. on ACM Multimedia Workshop, Germany.

[4] Lyu. S and Farid. H, (2002), Detecting hidden messages using higher-order statistics and support vector machines, Proc. Int. Conf. on 5th International Workshop on Information Hiding.

[5] Mathkour and Al-Sadoun. B, (2008), A New Image Steganography Technique, IEEE Trans.2108-4244-1-978.

[6] Pevny. T and Fridrich. J, (2007), Merging markov and DCT features for multiclass JPEG steganalysis, Proceedings of SPIE, San Jose, CA.

[7] Sajedi. H and Jamzad. M, (2010a), CBS: Contourlet-Based Steganalysis Method, Sign Process Syst, 373-367.

[8] Sajedi. H and Jamzad. M, (2010b), Using contourlet transform and cover selection for secure steganography", Int. J. Inf. Secur. Vol.9 No.1, 337–352.

[9] Sallee. P, (2003), Model-based steganography, Proc. Int. Conf. on International Workshop on Digital Watermarking. Korea.

[10] Shetty. B, Rohith. J, Mukund. V and Rohan. H, (2009), Steganography using Sudoku Puzzle", Proc. Int. Conf. on International Conference on Advances in Recent Technologies in Communication and Computing.

[11] Solanki. K and Sarkar. A and Manjunath. B.S, (2007), YASS: yet another steganographic scheme that resists blind steganalysis", Proc. Int. Conf. on 9th International Workshop on Information Hiding.

[12] Yu. L, Zhao. Y, Ni. R and Z. Zhu. Z, (2009), PM1 steganography in JPEG images using genetic algorithm", Soft Comput , vol13, No. 1, 393–400.