A Novel Image Steganography in Contourletdomain Using Genetic Algorithm

H. Ramezani, F. Keynia, and F. Ramezani

Abstract—**Steganography is the science that involves communicating secret data in an appropriate multimedia carrier. This paper presents the application of contourlet Transform and Genetic Algorithm (GA) in a novel steganography scheme. We employ a genetic algorithm based mapping function to embed data in Discrete contourlet Transform coefficients in 4x4blocks on the cover image. The optimal pixel adjustment process (OPAP) is applied after embedding the message. GA employed to obtain an optimal mapping function to lessen the error difference between the cover and the stego image and use the block mapping method to preserve the local image properties. Also we applied the OPAP to increase the hiding capacity of the algorithm in comparison with other systems.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 similar existing methods. Moreoverthe 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.**

Index Terms—**Steganography, discrete contourlet transform, genetic algorithm, optimal pixel adjustment process.**

I. Introduction

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep thecontents of a message secret, it mayalso be necessary to keep the existence of the message secret. The technique used

to implement this, is called steganography [1]. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing”[2].

Steganography methods hide the secret data in a cover carrier so that the existence of the embedded data is undetectable [3]. The cover carrier can be different kinds of digital media such as text, image, audio and video [4]. Many image steganography methods have been proposed. In these methods, the secret data is embedded into the cover-image by modifying the cover-image to form a stego-image.The most important requirement for a steganographic algorithm is to be imperceptible [5]. Imperceptibility involves [5]:

Invisibility-The invisibility of a steganographic algorithm is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye.

Capacity-Steganography aims at hidden communication and requires sufficient embedding capacity. Capacity is measured in bits per pixel (bpp) in images.

Robustness against statistical attacks and image manipulation-The amount of modification the stego amount medium can withstand before an adversary can destroy the hidden information.

Achieving all this requirements simultaneously is difficult to a great extend.Steganographic methods can be broadly classified in to 3 categories [20]. 1. Spatial transform, 2. Transform domain, 3. Adaptive steganography methods. Common approaches in spatial domain include Least Significant Bit (LSB) manipulation [6]. LSB insertion is the simplest method and very weak in resisting even simple attack such as transform, compression, etc [5]. The transform technique involves modulating the coefficients of the cover data in the frequency domain. There are a few methods in fourier transform owing to it is not used for JPEG image format.

In contrast DCT is used extensively with image compression such as JPEG lossy compression. Although modification of properly selected DCT coefficient during embedding process will not cause noticeable visualartifacts, nevertheless they cause detectable statistical degradations [3]. Various steganography methods like YASS [7], MB [8], Outguess [9], Perturbed Quantization (PQ) [10] have been proposed with the purpose of minimizing the statistical artifacts which are produced by modifications of DCT coefficients.

In the Wavelet transform there are some steganography methods such as StegJasper [11] have been proposed that in comparison with DCT is more adaptive with HVS.

Adaptive steganography is special case of the two former methods. These techniques analyse the image and hide information in significant areas so that the hidden message is more a part of the image than being added noise in the image. e.g. [12] is an adaptive steganography based on contourlet domain.

This paper proposes a method to embed data in contourlet coefficients using a mapping function based on GA in 4x4 blocks on the cover image and, it applies the OPAP after embedding the message to maximize the Pick signal to noise ratio (PSNR).Only a few works on data hiding are done in contourlet transform domain [5], [12], [13], [26], besides there are some image steganography methods that

Manuscript received September 5, 2012; revised October 11, 2012.

F. H. Ramezani is with the Department of Computer Engineeringat Science and Research branch Islamic Azad University, Kerman, Iran (e-mail: hadiseramezani@yahoo.com).

C. F.Keynia is with the Department of Electrical Engineering, Semnan University, Molavi, Semnan 35195-363, Iran (e-mail: keynia@yahoo.com).

T. F. Ramezani is with the Department of Electrical Engineering, Yazd university, Yazd, Iran (e-mail: fereshte.ramezani@gmail.com).

DOI: 10.7763/IJFCC.2013.V2.185

used GA [18], [19].

This paper is organized as follows: Sect. 2 introduces the contourlettransform; Sect.3 introduces the proposed algorithm in detail. Sect. 4 discusses the achieved results and compares the proposed scheme with the state of the art algorithms. Sect. 5 concludes the paper.

II. Contourlet Transform

Contourlet transform [14] is a double filter bank structure and provides a multi-scale and multi-directional representation of an image. It is implemented by the pyramidal directional filter bank (PDFB) which decomposes images into directional subbands at multiple scales. PDFB consist of a double filter bank structure for obtaining sparse expansions for typical images having smooth contours. In this double filter bank, the laplacian pyramid (LP) [16] is first used to capture the point discontinuities, and then followed by a directional filter bank (DFB) [15] to link point discontinuities into linear structure. contourlet decomposition is shown in Fig. 1. In contourlet decomposition of an image, edges are represented by the coefficients with large magnitudes. Selecting more Co-efficient in more directions is achieved by means of combining Laplacian Pyramidwith Directional filter bank structure which captures directional information efficiently. The capacity depends on the number of levels in contourlet decomposition and how many subbands we have selected for embedding [5].

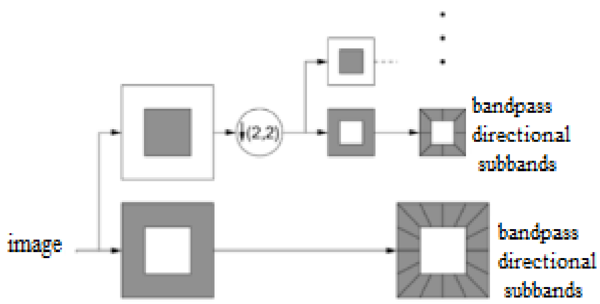


Fig. 1. Contourlet decomposition, laplacian pyramid followed by directional filter bank.

A. Contourlet Domain Properties

Contourlet possesses the important properties of directionality and anisotropy which wavelets do not possess and so it outperforms wavelets in many image processing applications. Moreover contourlet provides a much richer set of directions and shapes than wavelets and thus is more efficient in capturing smooth contours [17].as far as more data can be hidden in the high frequency regions without perceptually distorting the original image, contourlet coefficients are more suitable for data hiding applications.

III. Proposed Work

The proposed method embeds the message in Discrete Contourlet Transform coefficients based on GA. OPAP algorithm then applied on the obtained embedded image. This section describes this method, and embedding and extracting algorithms in detail.

A. Embedding Algorithm

The following steps explain the embedding process:

Step 1. The image selected is first decomposed using two levelcontourlet transform. The result contains a low pass imageand many high pass subbands. One of the high pass subbands is chosen for embedding the data.

Step 2.Divide the selected subband into 4×4 blocks.

Step 3. Generate 16 genes containing the pixels numbers of each 4×4 blocks as the mapping function.

Step 4.Embed the message bits in k-LSBs contourlet coefficients each pixel according to mapping function.

Step 5. Fitness evaluation is performed to select the best mapping function.

Step 6. Apply Optimal Pixel Adjustment Process on the image.

Step 7. Calculate inverse contourlet transform on each 4x4 block.

B. Extraction Algorithm

The extraction algorithm consists of four steps as follows:

Step 1. The image is decomposed usingtwo level contourlet transform. The subband in which data is embedded is taken.

Step 2. Divide the selected subband into 4x4 blocks.

Step 3. Employ the obtained function in the embedding phase and find the pixel sequences for extracting.

Step 4. Extract k-LSBs in each pixel.

C. Genetic Algorithm

GA is a technique which mimics the genetic evolution as its model to solve problems. Here we utilize the frequency domain to improve the quality of steganography by implementation of GA to obtain an optimal mapping function.We used message embedding positions as our search space and then applied the genetic algorithmic operators to find the best combination of message and image, So in this approach the given problem is considered as input and the solutions are coded according to a pattern.

1) Fitness function:

Pick Signal to Noise Ratio (PSNR) can be an appropriate evaluation test for the aim of suitable quality.so the definition of fitness function will be:

$$PSNR = 10log_{10}\frac{M\times N\times 255^2}{\sum_{ij}(y_{ij}-x_{ij})^2} \quad (1)$$

where M and N are the image size, x and y are the image intensity values before and after embedding respectively.

2) Chromosome design:

In our proposed GA, a chromosome is encoded as an array of 16 genes containing permutations 1 to 16 that point to pixel numbers in each block.

3) GA operations:

Tournament method is used to produce offsprings from parent chromosome.

For the crossover, one point in the selected chromosome would be selected along with a corresponding point in another chromosome and then point in another chromosome and then the tails would be exchanged.

Mutation processes causes some bits to invert and produces some new information. The only problem of mutation is that it may cause some useful information to be corrupted. Therefore we used elitism which means the best individual will go forward to the next generation without undergoing any change to keep the best information.

D. Optimal Pixel Adjustment Process

The basic concept of the OPAP is based on the technique proposed in [21]. After applying OPAP algorithm the embedding error is reduced to 1.

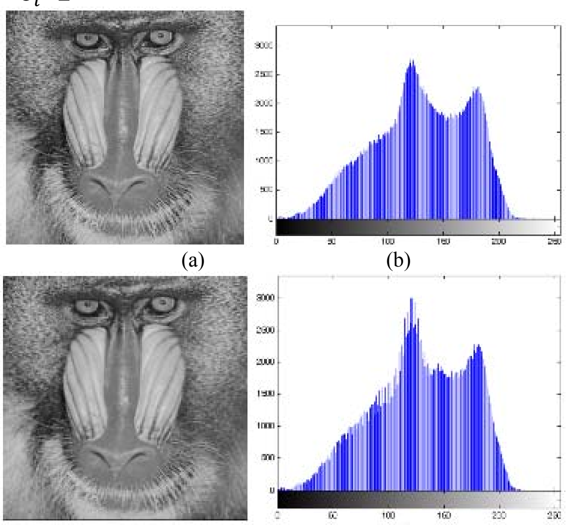
Let P_i, P_i' and P_i'' be the corresponding pixel values of the ith pixel in the cover-image C, the stego-image $\acute{C}$ obtained by the simple LSB substitution method and the refined stego-image obtained after the OPAP. If $\delta_i = P_i' - P_i$ be the embedding error between P_i and P_i' The OPAP algorithm can be described as follows:

Case1: ($2^{k-1} < \delta_i < 2^k$):
If $P_i' \geq 2^k$ then $P_i'' = P_i' - 2^k$ otherwise $P_i'' = P_i'$

Case2: ($-2^{k-1} < \delta_i < 2^{k-1}$): $P_i'' = P_i'$

Case3: ($-2^k < \delta_i < -2^{k-1}$):
If $P_i' < 256 - 2^k$ then $P_i'' = P_i' + 2^k$ otherwise $P_i'' = P_i'$

Therefore after embedding k-LSBs of P_i with k message bits, δ_i will be as follows:
$-2^k < \delta_i < 2^k$



(a) (b) (c) (d)

Fig. 2. Baboon Image and its histogram before (a, b) and after (c, d) embedding.

IV. Experimental Result

The proposed method is applied on 512×512 8-bit grayscale images such as Barbara and Baboon. The messages are generated randomly with the same length as the maximum hiding capacity. The PSNR is most commonly used as a measure of quality of reconstruction in image compression etc. it gives the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. In k-LSB substitution, k equal to 1 or 2, provide low hiding capacity with high visual quality of the stego-image and k equal to 7 or 8, provide low visual quality versus high hiding capacity. The experiment results show that for k=4 or k=5, we have the highest hiding capacity and reasonable visual quality [19]. This paper embedded the messages in the 4-LSBs and received a reasonable PSNR. Fig. 1.shows image for k=4 that there is no significant change in stego image histogram for 4-LSBs images, thus it is robust against some statistic attacks.

TABLEI: Comparison of Hiding Capacity Achieved and the Obtained PSNR Between our Proposed Method and Methods in [19], [22], [23].

Cover image	Method	PSNR(db)	Hiding Capacity (%)
Lena	Adaptive[22]	31.8	47%
	GA-DWT[19]	39.94	50%
	DWT [23]	44.90	27.34%
	Proposed method	45.20	56.36%
Baboon	Adaptive[22]	30.89	48%
	GA-DWT[19]	40.34	50%
	DWT [23]	44.96	27.34%
	Proposed method	43.69	51%
Boat	GA-DWT[19]	40.44	50%
	DWT [23]	44.92	27.33%
	Proposed method	42.63	58.30%
Jet	GA-DWT[19]	45.20	50%
	DWT [23]	44.76	27.33%
	Proposed method	45.55	46.02%

TABLE II: Accuracy of WBS, and CBS Steganal Ysismethods on Detection of Stego-Images Produced by this Proposed Method in Comparison with ContSteg Method [26].

Secret Data Size (bits)	**method**	**Average Detection Accuracy (%) of WBS Steganalysis Method**	**Average Detection Accuracy (%) of CBS Steganalysis Method**
5,000	Proposed method	49	59
	ContSteg	51	59
10,000	Proposed method	56	62
	ContSteg	53	63
15,000	Proposed method	54	65
	ContSteg	58	68

Moreover another image feature, skewness is analysed and compared with the implementation of proposed method in spatial domain.

Skewnesscharacterize the degree of asymmetry of distribution around its mean. Skewness characterizes only the shape of the distribution [5].it is given by:

$$Skewness = \frac{1}{N}\sum\left(\frac{x_i - \mu}{\sigma}\right)^3 \quad (2)$$

where σ is the standard deviation, that is a measure of gray level contrast, x_i represents the gray level of image, N is the number of distinct gray levels and μ is the mean.

Fig. 3. Shows the variation of skewness for the proposed method in spatial and contourlet domain.

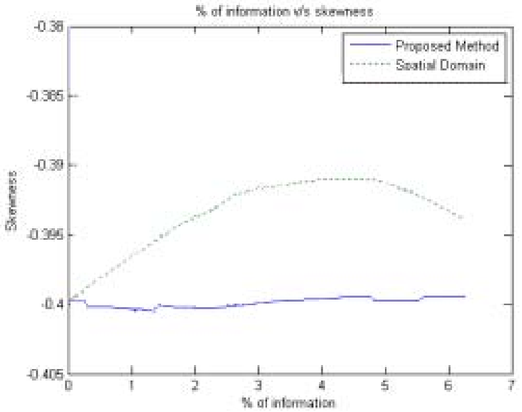


Fig. 3. The variation of skewness for the proposed method in spatial and contourlet domain.

A. Efficiency of this Proposed Method

In this experiment, we assess the efficiency of our method in terms of quality of stego-images and Hiding Capacity. Table1 shows, the comparison of hiding capacity achieved and the obtained PSNR between our proposed method and methods in [19], [22], [23].

B. Steganalysis Results

Wavelet-based steganalysis (WBS) [24], and Contourlet-based steganalysis (CBS) [25] methods are used to evaluate the security of our proposed method.

In WBS, a Fisher Linear Discriminator (FLD) and in CBS, a nonlinear Support Vector Machine (SVM) is trained to discriminate between clean and stego-images. 50 random images from Washington University image database [27] were chosen for testing and training. All images were converted to grayscale and cropped to size of 512×512.

The average of detection accuracy in comparison with ContSteg method [26] is shown in Table2. The accuracy is the average of true detection of both stego and clean-images. As can be seen, the detection accuracy is under 50% and the proposed method with payload of approximately 0.05 bits per pixel outperforms ContSteg and cannot be reliably detected by the applied steganalyzers.

V. Conclusions

Steganography that is a branch of information hiding technology aims to hide a secret data securely in a cover media for transmission. Hiding Capacity and stego-image quality are two important criteria in evaluating a steganography method. This paper presents a novel algorithm for embedding and extracting data in contourlet domain. We employ a genetic algorithm based mapping function to embed data in Contourlet Transform coefficients in 4x4 blocks on the cover image. The optimal pixel adjustment process is applied after embedding the message. We implement Genetic Algorithm and Optimal Pixel Adjustment Process to obtain an optimal mapping function to reduce the difference error between the cover and the stego-image, therefore improving the hiding capacity with low distortions. 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.

Refrences

[1] T. Morkel, J. H. P. Eloff, and MS. Olivier, “An Overview of Image Steganography,” in *Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005)*, Sandton, South Africa, 2005.

[2] T. Moerland. Steganography and Steganalysis. [Online]. Available: www.liacs.nl/home/ tmoerl/privtech.pdf.

[3] H. Sajedi and M. Jamzad, “ContSteg: Contourlet-Based Steganography Method,” *Wireless Sensor Network*, vol. 3, pp. 163-170, 2009.

[4] C. Liu and S. Liao, “High-performance JPEG steg-anography using complement ary embedding strategy,” *Pattern Recognition*, vol. 41, pp. 2945-2955, 2008.

[5] M. Mohan and P. R. Anurenjan, “A Novel Data Hiding Method in Image using Contourlet Transform,” *Recent Advances in Intelligent Computational Systems (RAICS)*, 2011.

[6] X. Luo, Z. Hu, C. Yang, and S. Gao, “A Secure LSB Steganography System defeating sample pair Analysis Based on Chaos System and Dynamic Compensation,” 2006.

[7] K. Solanki, A. Sarkar, and B. S. Manjunath, “YASS: Yet another steganographic scheme that resists blind stegana-lysis,” in *Proceeding of 9th International Workshop on In-formation Hiding*, June 2007.

[8] P. Sallee, “Model-based steganography,” in *Proceeding of International Workshop on Digital Watermarking*, Seoul, Korea, 2003.

[9] N. Provos, “Defending against statistical steganalysis,” in *Proceeding of 10th USENIX Security Symposium*, pp. 323–336, 2001.

[10] J. Fridrich, M. Goljan, and D. Soukal, “Perturbed quanti-zation steganography with wet paper codes,” in *Proc. of ACM Multimedia Workshop*, Germany, 2004.

[11] P. C. Su and C. C. J. Kuo, “Steganography in JPEG 2000 compressed images,” *IEEE Trans Consum. Electron*, pp. 824-832, 2003.

[12] H. Sajedi and M. Jamzad, “Adaptive steganography method based on contourlet transform,” in *Proceedings of 9th International Conference on Signal Processing (ICSP’08)*, October 26–29, 2008.

[13] N. M. Mathew and Navas K. A, “Data Hiding in Medical Image Using Contourlet Transform,” 2008.

[14] M. N. Do and M. Vetterli, “TheContourlet Transform: an efficient directional multiresolution image representation,” *IEEE trans. On image processing*, vol. 14, no.6, pp. 760-767, 2005.

[15] R. H. Bamberger and M. J. T. Smith, “A filter bank for the directional decomposition of images: theory and design,” *IEEE Trans. On Signal Processing*, vol. 40, pp. 882-893, April 1992.

[16] P. J. Burt and E. H. Adelson, “TheLaplacian pyramid as a compact image code,” *IEEE Trans. Commun*, vol. 31, no. 4, pp. 532540, April 1993.

[17] A. Arulmurugan, N. Arul, and P. Santhoshkumar, “Robaust Image Watermarking in Contourlet Domain Using Genetic Algorithm,” *Global Journal Of Computer Science And Tecgnology*, vol. 11, May 2011.

[18] T. R. G. Nair, V. Suma, and S. Manas, “Genetic Algorithm to Make Persistent Security and Quality of Image in Steganography from RS Analysis,” in *Proc. of Swarm Evolutionary and Memetric Computing Conference (SEMCCO)*, Vishakhapatnam.

[19] E. Ghasemi, J. Shanbehzadeh, and N. Fassihi, “High Capacity Image Steganography Based on Genetic Algorithm and Wavelet Transform,” *Intelligent Control and Innovative Computing, Lecture Notes in Electrical Engineering*, 2012.

[20] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, “Digital image Steganography: Survey and Analysis of Current Methods,” *Signal Processing*, vol. 90, no. 3, pp. 727-752, 2010.

[21] C. K. Chan and L. M. Cheng, “Improved hiding data in images by optimal moderately significant-bit replacement,” in *Proc. of IEEE lectron. Lett.*, vol. 37, no. 16, pp. 1017–1018, 2001.

[22] E. Safy, R. O. Zayed, and A. H. H, E. Dessouki, “An adaptive steganography technique based on integer wavelet transform,” *ICNM International Conference on Networking and Media Convergence*, pp. 111-117, 2009.

[23] P. Chen and H. Lin, “A DWT Based Approach for Image Steganography,” in *Proc. of International Journal of Applied Science and Engineering*, vol. 4, no. 3, pp. 275-290, 2006.

[24] S. Lyu and H. Farid, "Detecting hidden messages using higher-order statistics and support vector machines," in *Proceeding of 5th International Workshop on Information Hiding*, 2002.
[25] H. Sajedi and M. Jamzad, "A steganalysis method based on contourlet transform coefficients," in P*roceeding of 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2008.
[26] H. Sajedi and M. Jamzad, "Cont Steg: Contourlet-Based Steganography Method," *Wireless Sensor Network*, vol. 3, pp. 163-170, 2009.
[27] Computer Science and Engineering. [Online]. Available: http://www.cs.washington.edu/research/imagedatabase.

H. Ramezani was born in Shiraz, Iran in 1986. She received the B.Sc. degree in software computer engineering from Shiraz Islamic Azad University, Shiraz, Iran.Currently she is pursuing the M.Sc. degree in Computer Science the field of Artificial Intelligence from Department of Computer Engineering at Science and Research branch Islamic Azad University, Kerman, Iran.

Ms. Ramezani is a teacher at Dariyoon Islamic Azad University, Dariyoon, Shiraz, Iran and was teaching several computer science subjects.

F. Keynia was born in Kerman, Iran in 1974. He received the B.Sc. degree in electrical engineering from S. B. University, Kerman, Iran, in 1996 and the M. Sc. degree in electrical engineering from Semnan University, Semnan, Iran, in 2001. He received the Ph.D. degree in the Electrical Engineering Department of Semnan University. Prof. Keynia have written many issues that focuse on short-term and midterm price and load forecastingin deregulated electricity markets as well as feature selection and classification algorithms.

F. Ramezani was born in Shiraz, Iran in1991. Currently she is pursuing the B.Sc. degree in electrical engineering from department of electrical engineering, Yazd University, Yazd, Iran. Ms. Ramezani is a student member of IEEE and professional in Robotics(made Following & Maze solving robots) and Codvision- based on C language, Proteus, Protel and familiar with Bascom-based on Assembly.