International Journal of Electrical and Computer Engineering (IJECE)
Vol.2, No.5, October 2012, pp. 699~708
ISSN: 2088-8708

A New Approach for Image Hiding Based on Contourlet Transform

Saeed Masaebi*, Amir M Eftekhary Moghaddam**
* Department of Electrical and Computer Engineering, Qazvin Branch, Islamic Azad University
** Department of Electrical Engineering, Qazvin Branch, Islamic Azad University

Article Info

Article history:

Received Aug 6, 2012
Revised Sep 13, 2012
Accepted Sep 22, 2012

Keyword:

Contourlet Transform
Image Data hiding
Image Hiding
Steganography

ABSTRACT

A new image hiding method based on the contourlet transform is proposed in this paper. This strategy is based on storing information in high frequency sub-bands of contourlet transform. The embedding approach is in direction that the contourlet sub-bands have the least statistical disorder. As a result, the proposed algorithm has a higher robustness against to common steganalysis approaches. In addition, the quality of stegano image has considerably improved in comparison with related state of the art methods, with the extracted secret image having an acceptable quality. Furthermore, the experimental results show robustness respect to Gaussian noise and other attacks such as JPEG compression.

Corresponding Author:

Saeed Masaebi,
Department of Electrical, Computer and IT engineering, Qazvin Branch,
Islamic Azad University, Qazvin, Iran
saeed.masaebi@qiau.ac.ir

Amir Masoud Eftekhary Moghaddam,
Department of Electrical, Computer and IT engineering, Qazvin Branch,
Islamic Azad University, Qazvin, Iran,
eftekhari@qiau.ac.ir

1. INTRODUCTION

Steganography is the art of hidden the communication with the aim of hiding the communication through locating the message in a covering media so that the least discoverable change is created in it, and as a consequence it is impossible to recognize the identity of hidden message. Steganography is derived from secret communication science. Secret communication contains different areas such as cryptography and watermarking. The main difference between steganography and cryptography is that the aim of cryptography is hiding the content of messages rather than message existence. However, the purpose of steganograohy is hiding any sign of message existence. In cases that the transferring of encoded data is difficult, then we should hide the existence of communication. The current approaches in steganography domain could be divided into two categories of spatial and transformation domains. In spatial domain, there are many strategies of image steganography based on manipulating the least significant bit using direct replacing of least significant bit levels with the bits of secret image. [1-6]. Because of the limitation of the total number of least significant bit levels in a cover image, these methods have appropriate outputs only when the size of secret image is small enough. To reach this goal, the secret image size is not bigger than 25 percent of the cover image size. Nevertheless, when the hidden message is big proportional to cover image, the quality of stegano image is low in these methods. Another group is related to methods that the embedding process is implemented through frequency domain and wavelet transform. For instance the work presented in [7], with

using zero-padding features, the authors presented a steganography method based on image Fourier domain. In [8] a frequency domain method was proposed so that embedding is realized in bit planes of sub-band wavelet coefficients obtained by using the Integer Wavelet Transform. In the work proposed in [9], a chaos based spread spectrum image steganography method is addressed. The majority of LSB steganography algorithm embed message in spatial domain such as pixel value differencing [10].

The presented work is among the frequency domain methods that are based on storing the secret image data in block to block form. Many methods have been proposed which are based on the block to block storing in frequency domain. In [13], the authors proposed a method to embed the approximation coefficients of discrete wavelet transform of secret image. In this case, low frequency coefficients of secret and cover image are divided into 4*4 blocks. Then for each block in approximation coefficients of secret image, the most similar block in approximation coefficients of cover image is found. However, instead of direct replacement, the difference between two blocks is calculated and this block is stored in the most similar block in high frequency coefficients of wavelet. Although this approach is efficient and robust against to many attacks, but in this approach, the stegano image doesn't have high quality, and as we will see in simulation results, this approach doesn't show the enough robustness against to steganalysis algorithms. In the presented work in [12], it was claimed that the output of stegano image of the represented algorithm has more quality compared to the method proposed in [13], and also it has more robustness against to attacks. However, this method only objectively improves the quality of stegano image and the simulation indicates some defects that are appeared as small squares in the stegano image. In other words, the quality of output image is not acceptable enough. Furthermore, the extracted secret image has a very low quality in this method.

In the proposed method, like the method presented in [13], we store the differences of two blocks of approximation coefficients in high frequency sub-bands, but we use counterlet transform instead of wavelet transform. One of the advantages of counterlet transform compared to wavelet transform is the existence of linearly independent sub-bands. This issue decreases the possibility of detection of the stegano image by steganalysis algorithms. Furthermore, in the proposed method, we could get a better quality of stegano image. Moreover, the extracted secret image will also have better quality compared to the existing approaches.the In this work, we used the linear sum assignment(LSA)[14] for replacing the error blocks. The simulation results indicate that the linear assignment will improve the quality of images and resistance of algorithm.

The rest of the paper is organized as follows: In the next section, a brief introduction to contourlet transform is presented. The proposed technique is described in section 3. Section 4 shows experimental results and discussion. Finally, the conclusions of this paper are given in section 5.

2. CONTOURLET TRANSFORM

We can obtain a sparse expansion for natural images by first applying a multiscale transform, followed by a local directional transform to gather the nearby basis functions at the same scale into linear structures. In essence, we first use a wavelet-like transform for edge detection, and then a local directional transform for contour segment detection .Figure 1 shows a multiscale and directional decomposition using a combination of a Laplacian pyramid (LP) and a directional filter bank (DFB).

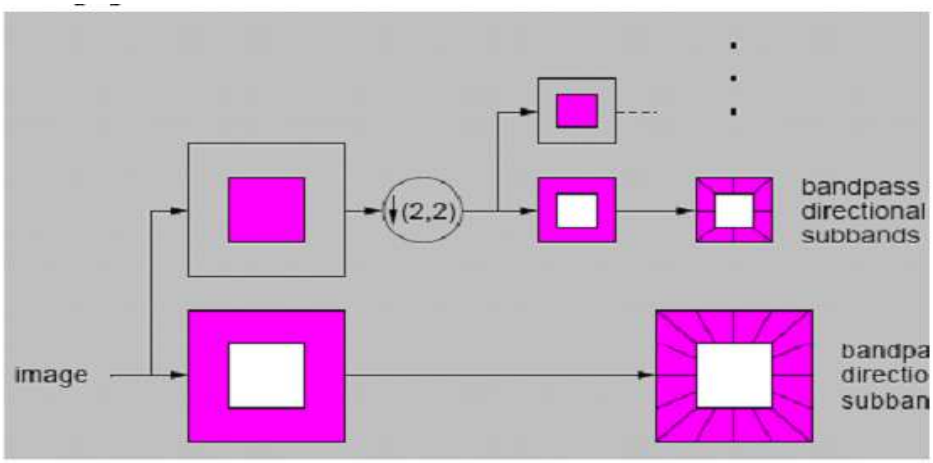

Figure 1. The diagram of the Contourlet transform [15]

The directional filter bank has a flexible number of directions and it only capture the high frequency of the input image because the low frequencies of the input image are removed before applying it. At first, we use the Laplacian Pyramid to compute a multiscale decomposition. The down sampled lowpass image and the difference image of the next level can be computed in the same way. Then we can obtain a series of bandpass images. The Laplacian Pyramid decomposition can avoid the frequency scrambling that happens in the wavelet filter bank because it downsample the lowpass channel only.The directional filter bank is firstly decompose the directional image and have good performance in image reconstruction. It has a simpler rule for expanding the decomposition tree while maintaining perfect reconstruction. One can decompose each scale into any arbitrary power of two's number of directions by applying the shearing operator combined with the two-channel quincunx filter bank at each node in a binary-structured bank.

2.1. The advantages of using the contourlet transform in comparison with wavelet transform:

It is true that the contourlet include all of the wavelet's advantages. The contourlet transform like wavelet transform is one of the pyramidal decomposition's methods. However, contourlet transform has other advantages compared to wavelet transform that can play the greater role for the applications of data hiding. Despite the wavelet transform which divides the high frequency only into three sub-bands at each level; it is possible to divide the high frequency into more sub-bands in the contourlet transform. This fact provides the variety of sub-bands for embeding the secret data. Moreover, in spite of the sub-bands in wavelet transform that are correlated, the sub-bands in the contourlet transform are linearly independent and hence uncorrelated . This could lead to more security in steganography. Because of the correlation between sub-bands in wavelet transform, each variation in a sub-band should cause changes in other sub-bands to be undetectable. Otherwise, there is the possibility of detecting by the steganalysis algorithms. However, as the sub-bands are linearly independent in contourlet, so there is lower possibility of detecting. In order to make optimal use of contourlet transform in image processing applications, we will have two important variables: The appropriate level of pyramid filters and the number of directional filters applied on the output. These two parameters are usually determined experimentally. In this work, the contourlet transform was carried out in level one, and as could be seen in Figure.2, the orthogonal directional filters are applied in four directions. Original image is decompose into 5 contourlet sub-bands, and each sub-band contains part of the original image frequency content. In fact, because of using orthogonal filters, these subbands will not overlap. The details of suggested method are explained in the next section.

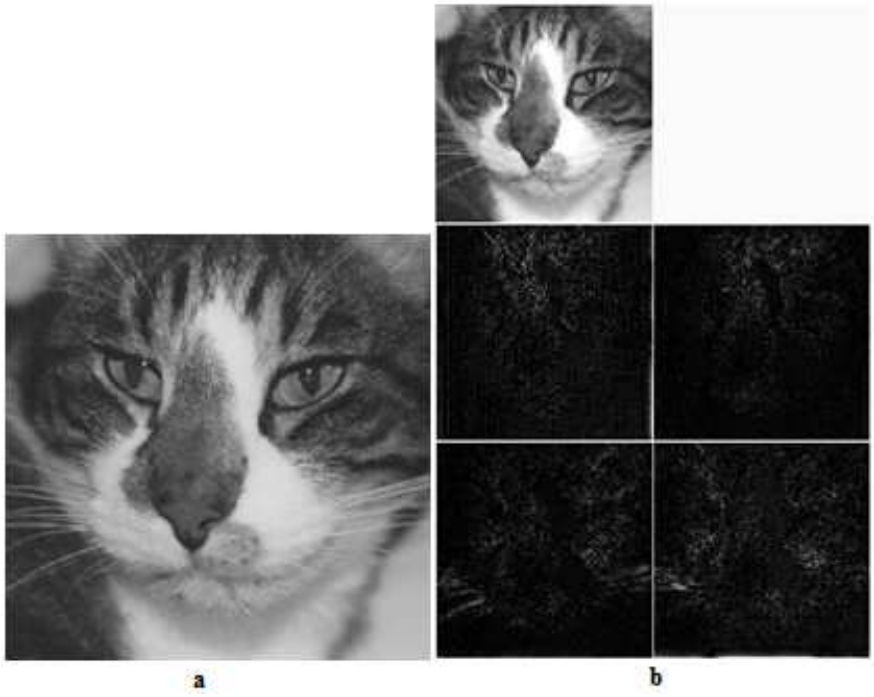

Figure 2. the contourlet transform in level one and four directions : a) orginal image b) decomposed image

3. THE PROPOSED METHOD

The proposed technique is based on the method presented in [13]. It means that the aim is the storing of approximation coefficients which are the most informative part of the secret image .

3.1. Embedding

Suppose that S and C are secret image and cover image respectively. We get the stegano image G by the following stages:

Stage 1) At first, by applying contourlet transform we decompose the host image (C) into a sub-image of low frequency coefficients CL and four sub-images of high frequency coefficients CH1, CH2, CH3 and CH4. In the same way, we decompose the secret image (S) into a sub-image of low frequency coefficients SL and four sub-images of high frequency coefficients SH1, SH2, SH3, SH4.

Stage 2) We divide each of the sub-bands SL, CL, CH1, CH2, CH3, CH4 into 4*4 blocks. By this method, we can describe the mentioned sub-bands as follows:

$$SL = \{BS_i; 1 \leq i < ns\}$$

$$CL = \{BC_{k_1}; 1 \leq k_1 < nc\}$$

$$CH1 = \{BH_{k_2}; 1 \leq k_2 < nc\}$$

$$CH2 = \{BH_{k_2}; nc + 1 \leq k_2 < 2nc\}$$

$$CH3 = \{BH_{k_2}; 2nc + 1 \leq k_2 < 3nc\}$$

$$CH4 = \{BH_{k_2}; 3nc + 1 \leq k_2 < 4nc\}$$

BS_i and BC_{k_1} are i^{th} block in SL and $k_1{}^{th}$ block in CL respectively. If the blocks of CH1, CH2, CH3 and CH4 are put together, BH_{k_2}, is the $k_2{}^{th}$ block in the Sequence blocks extracted from CH1, CH2, CH3 and CH4. ns is the entire number of 4*4 blocks in SL and nc is the number of 4*4 blocks in each of the sub-bands CL, CH1, CH2, CH3 and CH4.

Stage 3) For each block in BS_i, Best matching block in BC_{k_1} is searched. Secret key k1 includes the addresses of the best matching blocks in BC_{k_1}.Here, the Euclidean distance is used for computing the similarity measure to find the matching block.

Stage 4) Computation of error block EB_i between Bc_{k1} and BS_i as follows:

$$EB_i = Bc_{k1} - BS_i \quad (1)$$

Stage 5) in this stage, the corrected error blocks EB_i is replaced with some BH_{K2} blocks. LSA method is used to find out the best matched blocks . For this purpose, the cost of replacing each error block in all of BH_{K2} is computed by Euclidean distance. Then, using LSA method , the matched block for each error block in BH_{K2} blocks is computed. We can minimize the total cost of the entire replacing by using this method. In practice, this method improves the quality of stegano image. Moreover, regarding the fact that the total cost is minimum, we can conclude that the blocks are replaced with the least error that improves the quality of the extracted secret image.

After replacing the error blocks, the second secret key k2 that includes the addresses of the best matching blocks in BH is produced.

Stage 6) In this stage, by applying inverse countorlet transform to CL, CH1, CH2, CH3 and CH4 the stegano image is created.

Block Diagram of embedding process is shown in Figure 3.

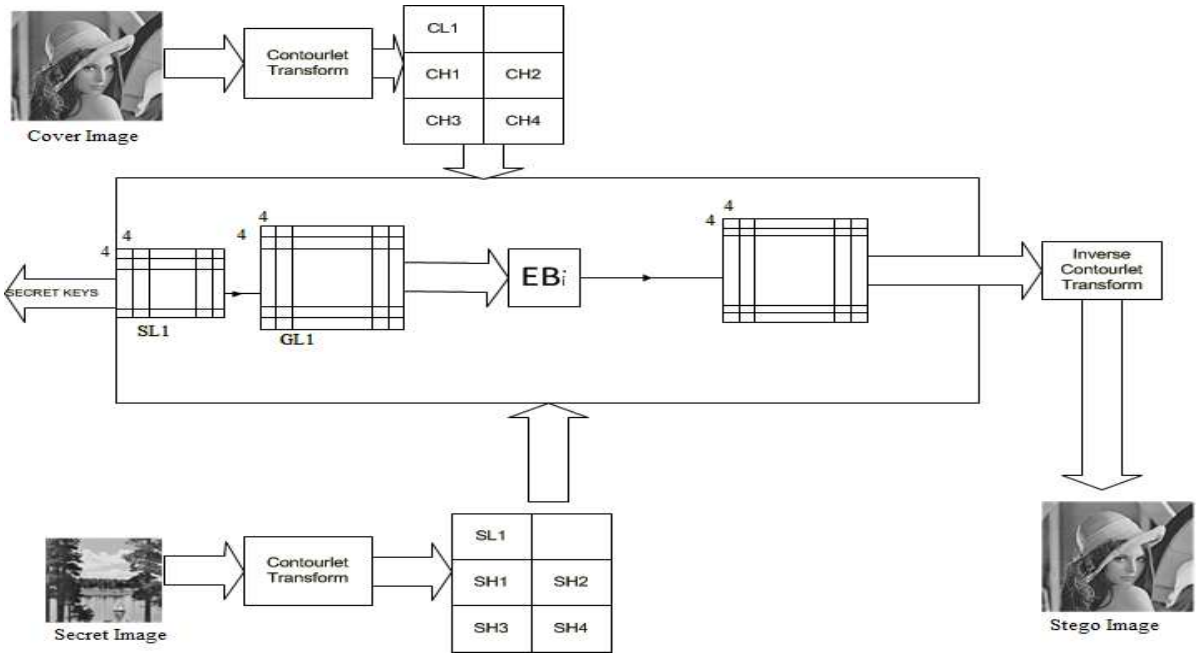

Figure 3. Block diagram of the embedding procedure

3.2. Extracting

Extracting process of secret image is as follows:

Stage 1: Decompose of the stegano image by applying contourlet transform for getting the sub-images GL, G H1, GH2, GH3, GH4.

Stage 2: The block BC_{K1} extracted by using of the first secret key from sub-image GL. The second secret key used for extracting the error block EB_i.

Stage 3: the block BS_i is computed by the following equation:

$$BS_i = Bc_{k1} - EB_i \quad (2)$$

Stage 4: Repeat stage 2 to 3 until all of the secret block are extracted and form sub-image SL.

Stage 5: by using the sub-bands SH1, SH2, SH3, SH4 that we receive from sender and by applying inverse contourlet transform We extract the hidden secret image. Figure 4 show the block-diagram of the extracting process.

4. EXPERIMENTAL RESULTS:

In this part, the efficiency and capability of the proposed method is investigated in comparison with other state of the art methods using three different experiments. The database is based on 380 standard images. Some parts of these images derived from SIPI database in the University of Southern California and other parts are derived from standard databases of CSIQ and Zurich Buildings. All images are applied with gray-level format. In each test, cover images and secret image size has been changed based on the tests implemented in previous works. All of the 380 images of database were generated in three different sizes: 256 × 256, 128 × 128 and 64 × 64.

4.1. Experiment 1:

In this experiment, we have investigated the robustness of the proposed method againts to detection algorithms. As the proposed method apply changes in high frequency sub-bands, hence we used the algorithm presented in [16] to check the robustness of the proposed method.

In the work[11], with extracting the appropriate features from the high frequency coefficients of wavelet transform and using the Fisher's Classification algorithm, a new method is designed for identifying the stegano image from other non containing messages (cover image). This algorithm can recognize stegano images with checking the imposed disorders in high frequency sub-bands of wavelet transform.

All of the 380 database images were transformed in two different sizes of 256 * 256 and 128 x 128. The 380 images of 256 * 256 dimensions formed the cover database and the 380 images of 128 * 128 dimensions formed the secret database. For each secret image, a host image was randomly selected from the relevant image database. We used the 4-fold approach for training and testing the data. The comparison of the proposed method and other methods presented in [12, 13] is illustrated in Table 1. As we see, in the proposed approach not only the stegano and extracted images have better quality, but also it has much more robustness compared to the detection algorithms. The low robustness of two mentioned methods is due to the replacement of the error block regardless of the statistical model of high frequency wavelet coefficients and this issue has caused their algorithm to be vulnerable of detection.

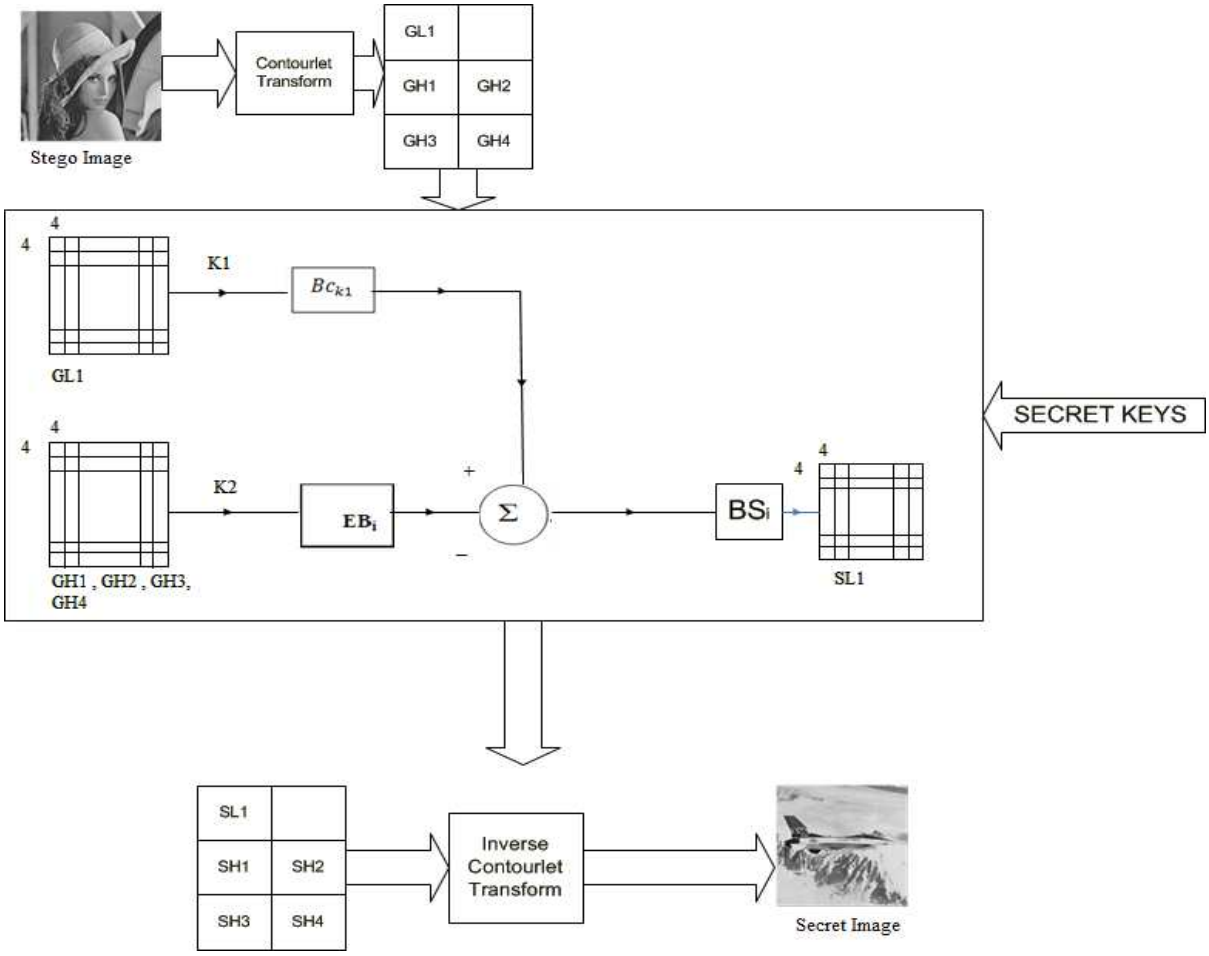

Figure 4. Block diagram of the extracting procedure.

Table 1. Detection accuracy of H Farid detection algorithm in Vijay Kumar approach and AAbdelwahab approach.

Average PSNR of extracted secret Image	Average PSNR of stego Image	False positive	Detection Accuracy (Steganalyzer H Farid[16])	Methods
33.5172	54.7821	46.4%	50.35%	The proposed method
24.3	42.07	34%	72%	Vijay Kumar method [12]
27.64	36	41%	64%	AAbdelwahab method[13]

4.2. Experiment 2:

In this experiment, a number of standard images with the size of 256 x 256 are selected as the the cover image and the redfort image is selected with the size of 128 ×128 as the secret image. In the Table. 2, the PSNR of the stegano image for the proposed algorithm and presented algorithms in [2, 5, 11] could be seen. As could clearly be seen in the Table 5, the quality of the stegano image in the proposed algorithm is much higher than others .The output of the proposed algorithm is illustrated in the Figure. 5 , Figure. 6 and Figure 7.

Table 2.Comparison between ahmed and vijay Kumar and the proposed method in terms of PSNR using redfort (128 * 128) as the secret image.

Image	PSNR value	PSNR value	PSNR value
Cover image size(256*256)	Ahmed method[5]	Vijay Kumar method[11]	Proposed method
Peppers	31.59	42.09	47.02
Lena	31.86	41.93	49.36
Goldhill	31.86	41.84	42.64
Boat	32.37	42.45	46.79

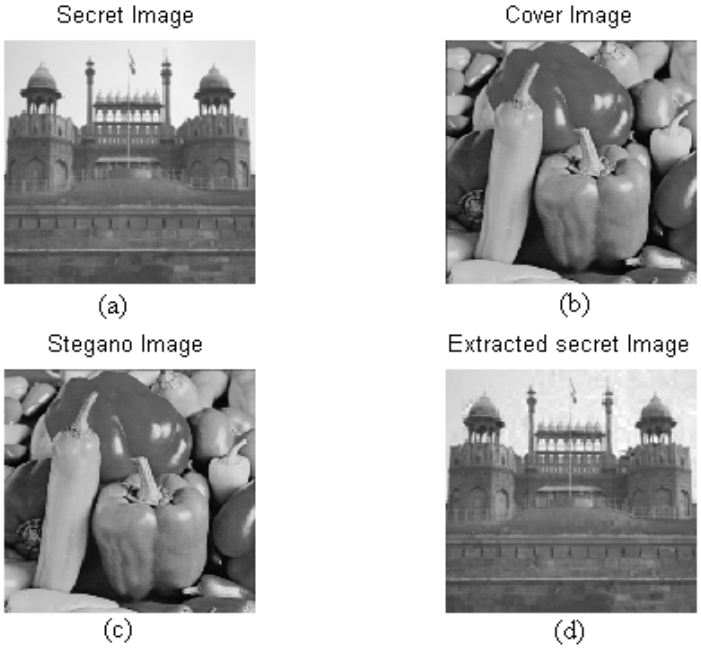

Figure 5. a) secret image. b) cover imge. c) stegano image with psnr=47.02db . d) extracted secret image with psnr=34.38 db.

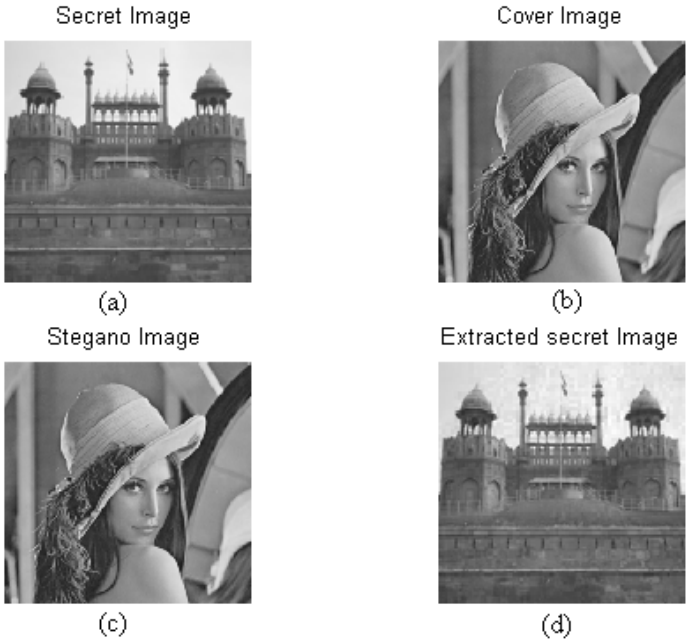

Figure 6.a) secret image. b) cover imge. c) stegano image with psnr=49.36 db. d) extracted secret image with psnr=33.72 db.

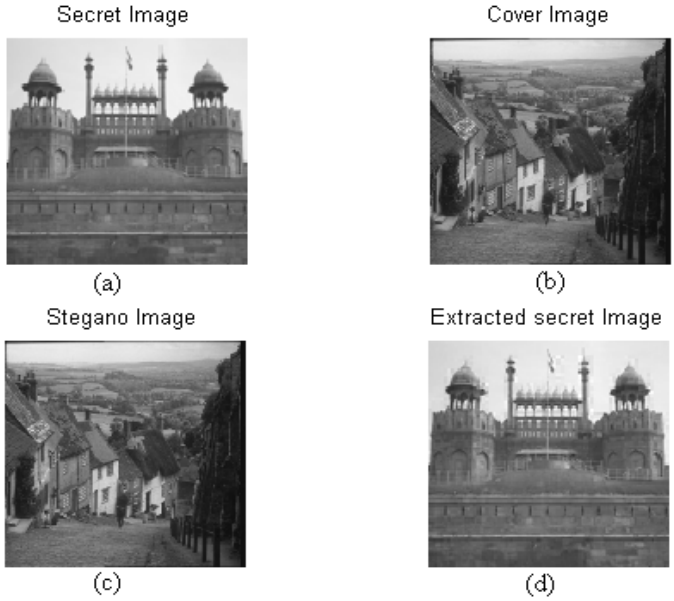

Figure 7. a) secret image. b) cover imge. c) stegano image with psnr=47.34 db . d) extracted secret image with psnr=34.54 db.

4.1. Experiment 3 examining the robustness of the proposed method to the attacks of noise and JPEG compression:

In this section, we examined the robustness of the proposed technique respect to the attacks such as JPEG compression, etc. In this section we show that the proposed algorithm has an appropriate robustness respect to Gaussian noise, histogram equalization, Gaussian Blur, gamma correction, a median filter and JPEG compression attacks. However, the JPEG compression has the most important because the probability of happening this attack is higher than other attacks. So in considering all the attacks, JPEG compression is also included. As could be seen in the Table 6, regarding to various attacks, acceptable PSNR values are obtained using proposed algorithm which is an indicator of the acceptable quality of extracted secret image after relevant attacks. As we find from Table 3, the acceptable amounts of PSNR is obtained by the core of the different attacks for the proposed algorithm that these amounts are indicators of the acceptable quality of the extracted secret image after the exertion of the related attacks.

Table3. PSNR of stegano and extracted secret images under different image processing attacks (secret image size is 128 x 128 and cover image size is 256 * 256)

Cover image size is 256*256 and secret image size is 128*128	PSNR Without any attack	PSNR for JPEG compression + Gaussian noise	PSNR for JPEG compression + Histogram Equalization	PSNR for JPEG compression + Gaussian Blur	PSNR for JPEG compression + Gamma correction	PSNR for JPEG compression + Median filter
Stegano-Peppers	47.02	30.04	20.55	40.09	30.73	34.19
Extract-Redfort	34.38	21.62	19.28	27.59	26.04	26.28
Stegano-Lena	49.61	30.00	18.98	39.44	31.43	32.51
Extracted Airplane	33.18	20.03	16.24	26.06	24.10	24.93
Stegano- Truck and APCs	49.18	30.03	24.51	36.45	30.71	28.27
Extract- Einstein	31	23.13	22.75	28.00	26.46	26.18
Stegano-goldhill	46.99	29.98	17	40.01	32.65	32.01
Extract- clock	35.47	22.53	16.57	27.79	25.16	25.75

5. CONCLUSION

A new approach of steganography based on the contourlet algorithm is proposed in this paper. The generated stegano image in this method has better quality compared to the state of the art methods. In

addition, this method is much more robust against to stegano analysis algorithms that try to find disorders in higher frequency content. The created secret image has also better quality in this method in comparison with other algorithms.

REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto, Techniques for data hiding, IBM Systems J. 35 (1996) 313–336.
[2] T.S. Chen, C.C. Chang, M.S. Hwang, A virtual image cryptosystem based upon vector quantization, IEEE Trans. Image Process. 7 (1998)1485–1488.
[3] L.M. Marvel, C.G. Boncenet, C.T. Retter, Spread spectrum image steganography, IEEE Trans. Image Process. 8 (1999) 1075–1083.
[4] S.S. Maniccam, N. Bourbakis, Lossless compression and information hiding in images, Pattern Recognition 37 (2004) 475–486.
[5] R.Z. Wang, C.F. Lin, J.C. Lin, Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognition 34 (2001) 671–683.
[6] R. Wang, Y. Tsai, "An image-hiding method with high hiding capacity based on best-block matching and k-means clustering", Pattern Recognition, 2007.
[7] McKeon, R.T.: Steganography Using the Fourier Transform and Zero-Padding Aliasing Properties. In: IEEE International Conference on Electro/Information Technology , pp.492–497 (2006)
[8] Tarres, S., Nakano, M., Perez, H.: An Image Steganography Systems based on BPCS and IWT. In: 16th International Conference on Electronics, Communications and Computers, pp. 51–56 (2006)
[9] Satish, K., Jayakar, T., Tobin, C., Madhavi, K., Murali, K.: Chaos based spread spectrum image steganography. IEEE transactions on consumer Electronics 50(2), 587–590 (2004)
[10] Zhang, X., Wang, S.Z.: Vulnerability of pixel-value differencing steganography tohistogram analysis and modification for enhanced security. Pattern Recognition, 331–339(2004)
[11] Hedieh Sajedi, Mansour Jamzad," Cover Selection Steganography Method Based on Similarity of Image Blocks",IEEE 8th International Conference on Computer and Information Technology Workshops ,2008
[12] Vijay Kumar1 and Dinesh Kumar"Digital Image Steganography Based on Combination of DCT and DWT"ICT 2010, CCIS 101, pp. 596–601, 2010. © Springer-Verlag Berlin Heidelberg 2010
[13] Ahmed A. Abdelwahab and Lobna A. Hassaan "A DISCRETE WAVELET TRANSFORM BASED TECHNIQUE FOR IMAGE DATA HIDING" 25th NATIONAL RADIO SCIENCE CONFERENCE (NRSC 2008)
[14] J.Munkres," Algorithms for assignment and transposition problems" Jornal of the Society of Industrial and Applied Mathematics ,vil.5,pp.32-38,mar .1975
[15] Do M.N. and Vetterli M. (2005), The Contourlet transform: An efficient directional multiresolution image representation , IEEE Trans. On Image Processing, 14(12), 2091-2106.
[16] Hany Farid : Detecting Steganographic Messages in Digital Images . TR2001-412, Dartmouth College, Computer

BIOGRAPHIES OF AUTHORS

Saeed Masaebi received the B.A., M.A.,degrees from the University of qazvin islamic azad univercity. His main research interests are in steganalysis, steganography, and watermarking.

Amir Masoud Eftekhary Moghaddam received the B.A., M.A. and Ph.D. degrees from the University of Tehran. He currently teaches and directs research in computer security and software engineering atthe University of qazvin islamic azad univercity