A Robust Steganography Method using Adjustable Parameters

Ahmad R. Eskandari
Digital Media Lab, AICTC Research Center, Department of Computer Engineering, Sharif University of Technology

Article Info

Article history:

Received Dec 28, 2012
Revised Feb 25, 2013
Accepted Mar 10, 2013

Keyword:

Information hiding
Steganography
Image data hiding
Countorlet transform
Robust method

ABSTRACT

In this paper, a new steganography method based on contourlet transform is presented. Compared with the previous works, the proposed method causes far fewer distortions in high frequency coefficients. This significantly increases the quality of stegano image and extracted secret image and its robustness against to steganalysis algorithm. Furthermore, we proposed two adjustable parameters that could be suited in direction of changing the quality of stegano image and extracted secret images or its robustness against to attacks and steganalysis algorithms. Using these parameters, much better performance of storing data is accessible. The proposed algorithm has higher robustness against to steganalysis algorithm in comparison with related state of the art methods. Likewise, the experimental results show robustness respect to Gaussian noise and other attacks such as JPEG compression.

Corresponding Author:

Ahmad R. Eskandari,
Digital Media Lab, AICTC Research Center, Department of Computer Engineering,
Sharif University of Technology, Tehran, Iran,
eskandari@dml.ir

1. INTRODUCTION

Steganography is a branch of secret communication science with aim of hiding the communication by locating the message in a covering media so that the least discoverable change is created in the media. In general, the available steganography methods can be divided in two groups of spatial and transformation domain. 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]-[2]. 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 [3], with using zero-padding features, the authors presented a steganography method based on image Fourier domain. In [4] 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 [5], 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 [6].

The proposed method is among the transform domain methods which are based on hiding the secret image in block to block form. Many methods have been proposed which are based on the block to block storing in transform domain. In [7], both the secret and cover images are divided into blocks. Then, for each secret block, the most similar block in cover image is found, and then the secret block is finally replaced by that block. In this method, using extracted features from Gabor domain, the most similar block is found. However, as the Gabor filter is a band pass filter, the extracted features don't contain the low frequency information; hence this issue has a negative effect on quality of the created stegano image. In [8], 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.

The presented steganography approach is an improvement of the method in [9]. The authors in [9] proposed a technique by which, the differences of two blocks of approximation coefficients stored in high frequency sub-bands of cover image's contourlet transform. One of the advantages of contourlet transform compared with other pyramidal transformations for steganography applications is the existence of linearly independent sub-bands. This issue decreases the possibility of detection of the stegano image by steganalysis algorithms. Nevertheless, this technique could not significantly improve the quality of stegano image and extracted secret image. Because, the statistics of embed blocks are often far different from the statistics of high frequency coefficients. This issue which is also happens in wavelet domain, reduces the quality of stegano image, extracted secret image and even more, by distorting the distributions of high frequency coefficients reduces the robustness against to steganalysis algorithms.

Here, we propose a method by which, only the authorized block is embedded in high frequency coefficients (An authorized block is the one that its statistics is similar to the statistics of high frequency coefficients and an unauthorized block is the one that its statistics is not similar to). We also proposed a method to convert an unauthorized block to an authorized block. By doing these, our technique significantly increases the quality of stegano image and extracted secret image and its robustness against to steganalysis algorithm. Furthermore, we presented two adjustable parameters to manage between the quality of stegano image and extracted secret images or robustness against to attack and steganalysis algorithms. Moreover, we demonstrate that by using $p{-}normdistance$ instead of Euclidian distance, better results in terms of robustness and quality can be achievable.

The rest of the paper is organized as follows: The proposed technique is described in section 2. Section 3 describes Statistical characterization of total error blocks coefficients. Section 4 shows experimental results and discussion. Finally, the conclusions of this paper are given in section 5.

2. THE PROPOSED STEGANOGRAPHY METHOD

The proposed technique is similar to the work in [9]. Here we present the storing method of approximation coefficients which are more valuable parts of secret image compared with four other subbands' coefficients.

2.1. Embedding

Consider S and C as secret image and cover image respectively.

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, SH3and SH4.

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

$$SL = \{BS_i; 1 \leq i$$
$$CL = \{BC_{k_1}; 1 \leq$$
$$CH1 = \{BH_{k_2}; 1$$
$$CH2 = \{BH_{k_2}; nc$$
$$CH3 = \{BH_{k_2}; 2n$$
$$CH4 = \{BH_{k_2}; 3n$$

BS_iandBC_{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. nsis 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 inBS_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}. In [9] the authors used the Euclidean distance for computing the similarity measure to find the matching block. But here we profit from the norm (P) distance for computing the similarity measure. In this work P is equal to 2.5.

$$p - norm\ distance = \left(\sum_{i=1}^{n} |x_i - y_i|^p\right)^{1/p} \quad (1)$$

The advantage of using the norm (P) distance respect to the Euclidean distance is represented in part 3-1.

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

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

Stage 5) finding the unauthorized error blocks and transforming them to the authorized blocks. The authorized block is the block that all of its members are smaller than the predetermined threshold (Thr). If an unauthorized block is found, then the block is changed to the authorized block by multiplying all of its members by the predetermined factorβ<1. The method of computing the value of threshold (Thr) and the factor β is represented in the section 6-2. We get the corrected EB in this stage.

Stage 6) 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 norm (p) distance. Then, using LSA method, the matched block for each error block in BH_{K2} blocksis 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. Then an extra bit is added to each address of k2 for identifying that the related error block is among the authorized blocks or not.

Stage 7) In this stage, by applying inverse contourlet transform to CL, CH1, CH2, CH3 and CH4 the stegano image is created.

2.2. 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 blockEB_i.

Stage 3) Using the bit that determines the type of block (Authorized or unauthorized block), the members of unauthorized block are multiplied by $\frac{1}{\beta}$, and the value of EB_i is returned to the initial state.the block BS_i is computed by the following equation:

$$BS_i = Bc_{k1} - EB_i \quad (3)$$

Stage 4) Repeat stages 2 and 3 until all of the secret blocks 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.

3. STUDY OF STATISTICAL CARACTRIZATION

In this section, we discuss the statistical properties of the total error coefficients and the high frequency sub-bands of contourlet transform. Then, regarding the findings, we justify the using of norm p distance and also we explain how to calculate the threshold value Thr and β coefficient.

In the Figure 5, the distributions of the coefficients of the total error blocks and high frequency sub-bands coefficients of contourlet transform of cover image are shown. It should be mentioned that distribution of the total error blocks coefficients is meant the distribution of the matrix coefficients that is created by putting all the error blocks together. As could be seen in the Figure 5, the distribution of the total error coefficients follows the Gaussian model. This issue is verified by testing more samples. In the Table. 1, the mean and standard deviation of each distribution can be seen. As shown in Table. 1, there are clear differences between the standard deviation of the distribution of error blocks coefficients and distributions of the high frequency sub-bands coefficients in contourlet transform. According to the statistical parameters of the error blocks, we can realize that replacing these values in high frequency sub-bands coefficients of the contourlet with lower variance can reduce the quality of steganoimage.Furthermore, it occasionally happens that the error block coefficients are so large, so that after embedding and applying the inverse contourlet, the intensity value of some pixels of the stegano image becomes lower than zero or higher than 255. In this situation, because the intensity value of image is limited between zero and 255, the embedded information will be destroyed. This issue, in turn, could create error in retrieving secret image. Therefore, direct embedding of the error blocks can cause decreasing the quality of stegano and extracted secret images. In this work, we benefited from two different methods to solve the problem which are explained as follow:

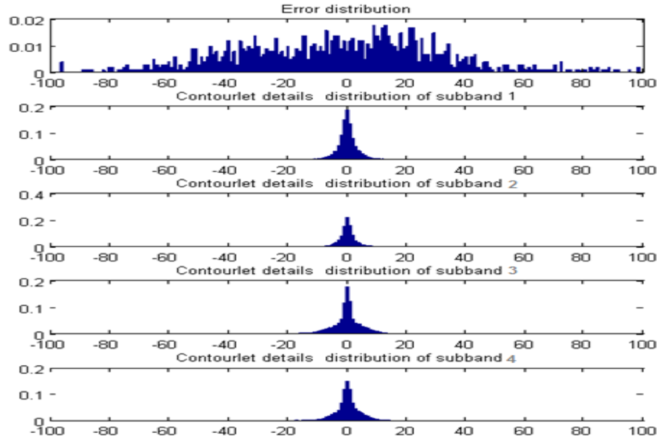

Figure 1. Distribution of error blocks coefficients and Distribution of high frequency sub-bands of contourlet's transform.

Table1. Mean and standard variance of cover image contourlet's high frequency coefficients and also the distribution of total differences blocks coefficients for a sample secret image and it's related cover.

	Total error	Sub-band 1	Sub-band 2	Sub-band 3	Sub-band 4
Mean	1.2341	0.2123	0.1320	0.0225	5330.0
Standard deviation	902.352	45.4755	37.8874	40.3422	54.9477

3.1. The way of computing the similarity

According to the reasons that mentioned in the section 4, the members of error block that are used in the distance calculation should not be higher than a certain threshold. Here, for measuring similarity, we applied norm distance (p) instead of Euclidean distance [1] in order to increase the effect of members which create greater error: Equation 1 (p is considered 2.5). This could cause that the members creating higher error play more important role in calculating distance and this, in turn, can significantly decrease the number of unauthorized blocks. It is essential to note that the large increase in p could also have a reverse effect. The reason is that, the more the high value members of error block are considered, the low value members of error block are less regarded. In other words, differences are more regarded than similarities and this issue will decrease the quality of stegano image.

3.2. Using the threshold Thr and the factor β for converting unauthorized error block to authorized error block

As mentioned before, the large values of error blocks can reduce the quality of stegano and extracted secret images. To solve this problem, if a member of a error block is more than a threshold value, the members of that block are multiplied by a factor smaller than 1, and so the destructive effect of that member is decreased. The threshold value Thr is considered equal to α time of the minimum of the standard deviations that computed from the distributions of high frequency sub-band's coefficients.

$$Thr = \alpha * \sigma_{min} \tag{4}$$

In the above equation, the Thr and$\sigma_{min}$are the threshold value and the minimum standard deviation respectively.

In our experiments, α is considered equal to 4. The 4σ is the value there are approximately 99% of absolute value of the high frequency coefficients less than this value. This threshold means that the members of error blocks should be placed in the range of 4σ otherwise it will be regarded as an unauthorized block. When the block was not authorized, all its members are multiplied by a factor, and then embedded. This coefficient is calculated as follows:

$$\beta = Thr\ /Erorr_{max} \qquad (5)$$

Here, $Erorr_{max}$ is the maximum amount that each member of error block can reach. In this work, this value was considered 500. $Erorr_{max}$ Occurs while calculating the error block, if one member of block from approximation coefficients of secret or host image is zero and another corresponding member has the maximum value of the approximation coefficients relevant to the contourlet transform. In practice, the probability of this issue is very low, and for this reason, the $Erorr_{max}$ can be considered less than its maximum value. The following should be considered in determining the Thr and$Erorr_{max}$values:

1. With increasing the threshold value, more blocks will be considered authorized, and for this reason, the quality of the stegano image is reduced. However, this can increase the quality of the extracted secret image. Because the quantization process which is done after the inverse contourlet transform in embedding stage, Cause the multiplying by β factor during replacement and dividing by β during retrieving will not exactly be reversed processes. As a result, error blocks must be less manipulated as far as possible to have better quality for extracted secret image. In addition, since with multiplying by factor β in one block, all the members value are diminished, it is possible to create members with very small value. In this situation, these members become so sensitive to attacks such as noise and Gaussian bluer, and this issue with the presence of such attacks leads to reduction of the quality of the extracted secret image. However, since increasing Thr increases the number of authorized blocks, this cause more disorder in the frequency model; therefore, the possibility of detection using steganalysis algorithms will be increased.
2. By increasing the $Erorr_{max}$ value, the quality of stegano image increases, but the quality of the extracted secret image is reduced. Because this will cause the coefficients of unauthorized error blocks would become smaller or in other words, it willbecome closer to the average value of high frequency sub-bands coefficients of contourlet transform. On the other hand, this operation causes the error blocks coefficients to be more manipulated, and as mentioned before, this will reduce the quality of the extracted secret imageand make it more sensitive to attacks such as noise and Gaussian blur. However, since increasing the $Erorr_{max}$cause less disorder in the frequency model; therefore, the possibility of detection using steganalysis algorithms will be decreased.

Table 2. This table shows the variations of quality measure of stegano and extracted secret images and robustness against to attacks and steganalysises algorithm respect to increasing and decreasing $\text{Error}_{max}$and α The up arrow (↑) means increase and the down arrow means decrease (↓)

	α (↑)	α (↓)	$Error_{max}$ (↑)	$Error_{max}$ (↓)
quality of stego image	(↓)	(↑)	(↑)	(↓)
quality of extracted image	(↑)	(↓)	(↓)	(↑)
robustness against to detection	(↑)	(↓)	(↑)	(↓)
robustness against to attack	(↑)	(↓)	(↓)	(↑)

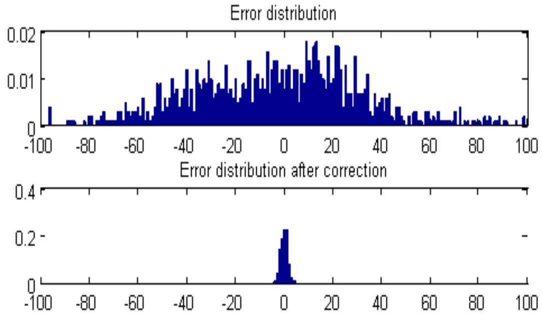

Figure 2. The distribution of error coefficients in initial state and after correction

In the Table 2, we have demonstrated the effects of changes in $Erorr_{max}$ and αvalues in the quality of stegano image, the extracted secret image and also sensitivity to attacks and also detection algorithms. The up arrow (↑) means increase and the down arrow means decrease (↓). The Figure 6 illustrates the distribution of error coefficients in initial state and after converting unauthorized blocks to authorized blocks. As could be seen, the error distribution coefficients are very similar to the distribution of high frequency sub-bands coefficients of contourlet transform.

4. RESULTS

In this section we examined the performance of the proposed method in image quality, robustness against stegananalysis algorithm and attacks through three different experiments. The database contains 300 different gray-level format images derived from standard SIPI database in the University of Southern California and standard databases of CSIQ and Zurich Buildings. In each test, cover images and secret image size has been changed based on the tests implemented in previous works. All of the 300 images of database were generated in three different sizes: 256 × 256, 128 × 128 and 64 × 64.

Firstly, we have investigated the robustness of the proposed method against to detection algorithms. As the proposed method applies changes in high frequency sub-bands, hence we used the algorithm presented in [10] to check the robustness of the proposed method.In the work [10], 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. The 300 images of 256*256 dimensions formed the cover database and the 300 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 5-fold approach for training and testing the data. The comparison of the proposed method and other methods presented in [8] and [9] is illustrated in Table 3. 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. We have performed the same experiment for comparing our proposed method with the work done in [7]. In this method, a suitable algorithm was applied for extracting cover image. We also used this algorithm [7] for selecting the cover image, however, with assuming that the applied feature is 4×4 blocks of approximation coefficients of contourlet transform in database of the cover images. The results of this experiment are shown in Table 4. As could be seen, the quality of the stegano image in the proposed method is much better and has more robustness against to the detection algorithms. In this experiment we set $Error_{max}$=500 and α =4.

Table 3. Detection accuracy of H Farid detection algorithm in the proposed method andMasaebe et al.[9] approach and AAbdelwahab et al. [8] approach

	Average PSNR of stego Image	False positive	Detection Accuracy	Average PSNR of extracted secret Image
The proposed method	48.76	47.5%	50.24%	34.35
Masaebe et al. [9] method	38.87	43.7%	59.45%	29.54
AAbdelwahab et al. [8] method	36.42	41.2%	63.67%	27.18

Table 4. Detection accuracy of H Farid detection algorithm in Sajedi et al. [7]approaches and the proposed approach

	Detection Accuracy	False positive	Average PSNR of stego Image	Average PSNR of extracted secret Image
The proposed method	50.11%	48.4%	51.781	34.51
Sajedi et al. [7] method	58.33%	37.11%	39.55	31.22

In the second 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

5, the PSNR of the stegano image for the proposed algorithm and presented algorithms in [7]-[9] could be seen. As could clearly be seen in the Table 5, the quality of the stegano images in the proposed algorithm are significantly higher than the others. The output of the proposed algorithm is illustrated in the Figure 7. In this experiment bydecreasing $\text{Error}_{\text{max}}$respect to experiment 1, we improvedthe qualityof extracted secret image and decreased the quality of the stegano image. However, as can be seen the quality of the estegano image is remained predominant incomaprision with other methods. In this experiment we set $\text{Error}_{\text{max}}$=400 and α =4.

Table 5. Comparison between AAbdelwahab et al. [8],Masaebe et al. [9], Sajedi et al.[7]and the proposed method in terms of PSNR using redfort (128 * 128) as the secret image. Cover image size is 256*256

	Peppers	Lena	Goldhill	Boat
Proposed method	48.32	50.14	43.87	48.08
AAbdelwahab et al. [8] method	31.95	31.74	31.15	32.56
[Masaebe et al. method[9	36.62	36.44	35.84	37.54
[Sajedi et al. method[7	38.79	39.43	32.19	37.14

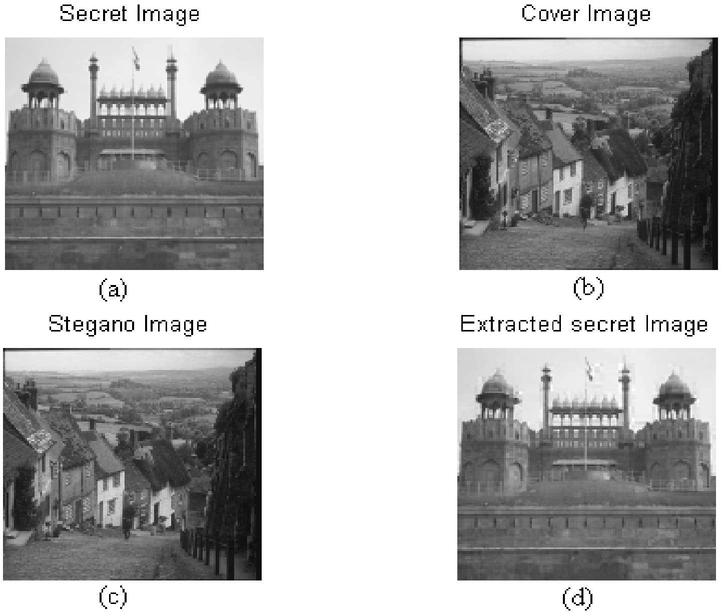

Figure 3. a) secret image . b) coverimge. c) stegano image . d) extracted secret image

In the next experiment, we examined the robustness of the proposed technique respect to the attacks such as JPEG compression, etc. As mentioned before, by increasing the factor α and also reducing the$Erorr_{max}$, the robustness of the proposed algorithm could be increased. In this case, the stegano image quality is reduced. Here, by considering optimal values for these two parameters, 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. In this experiment we set $\text{Error}_{\text{max}}$=200 and α =4. By decreasing $\text{Error}_{\text{max}}$respect to experiments 1 and 2, we increased robustness against to attacks. 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 6, 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.

Table 6. 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)

Image	PSNR					
	JPEG compression	Gaussian noise	Histogram Equalization	Gaussian Blur	Gamma correction	Median filter
Stegano-Peppers	39.33	35.54	25.57	36.54	31.38	34.74
Extract-Redfort	33.12	29.34	24.02	31.94	27.63	27.55
Stegano-Lena	41.76	33.82	24.91	35.23	33.92	33.28
Extracted Airplane	34.56	28.36	20.37	30.96	26.45	26.56
Stegano- Truck	39.92	34.26	29.75	35.43	31.73	28.84
Extract- Einstein	34.58	28.85	26.36	28.29	27.36	29.37
Stegano- goldhill	40.21	32.26	24.92	37.01	32.48	33.64
Extract- clock	33.72	28.73	21.63	29.44	28.16	29.24

5. CONCLUSION

A new approach of steganography based on contourlet transform is proposed in this work. The process is such that the high frequency coefficient of stegano image is far fewer distorted after embedding. This leads to better quality of stegano image and extracted secret image. Meanwhile, the robustness against to detection is increased significantly. Furthermore, we proposed to use two adjustable parameters by witch the efficiency of the embedding can be increased in terms of robustness and quality. We also proposed to use $p{-}normdistance$ instead of Eucledian distance. The simulation results indicate the effectiveness of the proposed method. Finally, Although our proposed technique is based on countorlet transform, one can use it on other transform domains like wavelet transform.

REFERENCES

[1] RZ Wang, CF Lin, JC Lin. Image hiding by optimal LSB substitution and genetic algorithm. *Pattern Recognition*. 2001; 34: 671–683.

[2] R Wang, Y Tsai. An image-hiding method with high hiding capacity based on best-block matching and k-means clustering. *Pattern Recognition*. 2007.

[3] McKeon RT. *Steganography Using the Fourier Transform and Zero-Padding Aliasing Properties*. IEEE International Conference on Electro/Information Technology. 2006; 492–497.

[4] Tarres S, Nakano M, Perez H. *An Image Steganography Systems based on BPCS and IWT*. International Conference on Electronics, Communications and Computers. 200: 51–56.

[5] Satish K, Jayakar T, Tobin C, Madhavi K, Murali K. Chaos based spread spectrum image steganography. *IEEE transactions on consumer Electronics*. 2004; 50(2); 587-590.

[6] Zhang X, Wang SZ. Vulnerability of pixel-value differencing steganography tohistogram analysis and modification for enhanced security. *Pattern Recognition*. 2004; 331–339.

[7] 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.

[8] Ahmed A Abdelwahab, Lobna A Hassaan. *A Discrete Wavelet Transform Based Technique For Image Data Hiding*. 25th National Radio Science Conference. 2008.

[9] Saeed Masaebe, Amir M Eftekhary Moghaddam. A New Approach for Image Hiding Based on Contourlet Transform. *International Journal of Electrical and Computer Engineering (IJECE)*. 201; 2(5): 699-708.

[10] Hany Farid. Detecting Steganographic Messages in Digital Images. TR2001-412, Dartmouth College, Computer.

[11] J Munkres. Algorithms for assignment and transposition problems. *Journal of the Society of Industrial and Applied Mathematics*. 1975; 5: 32-38.

[12] Do M, Vetterli M. The Contourlet transform: An efficient directional multiresolution image representation. *IEEE Trans. On Image Processing*. 2005; 14(12): 2091-2106.

BIOGRAPHY OF AUTHOR

Received the B.S., degrees from the Shahedunivercity. His main research interests are in machine vision, biometrics, annotation and steganography.