*Journal of Information Hiding and Multimedia Signal Processing* ©2015 ISSN 2073-4212
**Ubiquitous International** Volume **6**, Number **5**, September **2015**

# A Novel Image Steganography Based on Contourlet Transform and Hill Cipher

Shuliang Sun[1,2], Yongning Guo[1,2]

[1]School of Electronics and Information Engineering,
Fuqing Branch of Fujian Normal University
Fuqing, 350300, China
[2]Innovative Information Industry Research Center,
Fuqing Branch of Fujian Normal University
Fuqing, 350300, China
tjussl_07@126.com

Received July, 2014; revised March, 2015

Abstract. *In this paper, a novel image steganography is proposed, which is based on contourlet transform and hill cipher. Firstly, cover image is decomposed with contourlet transform. Contourlet transform provides a multi-scale and multi-directional representation of an image. One of the subbands is selected to embed secret data. Then hill cipher is applied to encrypt the secret message. In this approach, it's important to find a proper cipher matrix. The selected matrix should be inevitable and relatively primary to the number of alphabets. The skill of $2^k$ correction is applied to ease the difference between cover and stego image. The experiment results show that both stego image and retrieved image have better quality in the proposed approach than other methods.*

**Keywords:** Contourlet transform; Hill cipher; $2^k$ correction; Cipher matrix

1. **Introduction.** There are two methods available for information security in secret communication: cryptography and steganography. Cryptography is a skill in which the data is scrambled so that the unauthorized users will not be able to extract the secret message without secret key [1]. Steganography is derived from the Greek for covered writing and essentially means to hide in plain sight [2]. Anybody could find that both parties are secretly communicating in cryptography. However, in steganography, hackers will not suspect the cover medium containing secret data at all. Secret data could be embedded into cover medium such as a text file, an image file, an audio file or a movie file. Two skills are adopted in this paper. Capacity, security (imperceptibility) and robustness are three different aspects in modern steganography system. Generally speaking, there is a fundamental compromise between capacity and security in all steganography systems. Two kinds of methods are often applied in steganography. One is based on original (spatial) domain and the other is based on transform domain. Especially, least-significant-bits (LSB) substitution [3] is the most well-known steganographic technique in the spatial domain. This method is simple and easy, but it is weak in robustness and compression, such as JPEG compression [4]. Since human eyes are not sensitive to tiny alterations of noisy data, it will not be noticed when the data in noisy regions is replaced with secret message. That is another famous method in original domain - bit-plane complexity segmentation steganography (BPCS) [5]. The transform domain is also divided

as discrete Fourier transform (DFT) [6], discrete cosine transform (DCT) [7], discrete wavelet transform (DWT) [8] and contourlet transform [9].

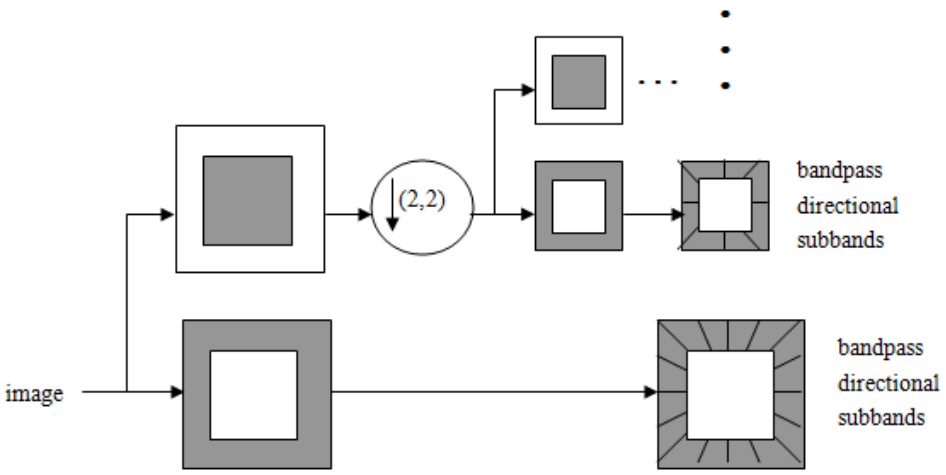


FIGURE 1. The diagram of the contourlet transform

2. **The Contourlet Transform.** The contourlet transform was proposed by Do and Vetterli [9]. It consists of a Laplacian pyramid (LP) [10] and a double filter bank (DFB) [11]. The contourlet transform provides a multi-scale and multi-directional representation of cover image. Especially, Laplacian Pyramid is used to compute a multiscale decomposition and capture the point discontinuities. The down sampled lowpass image and the different image of the next level can be achieved in the same way. Then a series of bandpass images are obtained. The high frequency of the input image is captured in the directional filter bank. That's because the low frequency of the input image is removed before applying it. Points of discontinuity are linked into contour segments by a directional filter bank. The number of directions can be changed according to different requirements. Since more directions could be provided in contourlet transform than wavelet transform, it is more suitable for data hiding applications and more messages can be hidden in the high frequency regions without perceptually distorting the original image [12]. Contourlet decomposition is shown in Figure 1.

Directionality and anisotropy are important properties of contourlet. Contourlet transform could offer a much richer set of directions and shapes than wavelet transform. So they are more effective in capturing smooth contours and geometric structures in images. Manipulating the values of coefficients in contourlet domain has less effect in the quality of image than in wavelet domain [13]. Firstly the cover image is decomposed by two level contourlet transform. A low pass image and many high pass subbands are obtained. Then one of the high pass subbands is chosen for embedding the secret data. In order to increase the security of the secret data, it is encrypted firstly before embedding. Finally the least significant digit of the contourlet coefficient is replaced with one digit of the encrypted data. The process is continued until the entire data is embedded.

3. **Hill Cipher.** The Hill cipher was invented by Lester. S. Hill in 1929 [14]. It is a polygraphic substitution cipher based on linear algebra. Each letter is represented using modulo 26 in this way. For example: A=0, B=1,...,Z=25. In order to encrypt a message, $n*n$ cipher matrix is chosen randomly as the cipher key firstly. The cipher matrix should be invertible and relatively primary to 26 [15]. Then each block of n letters is multiplied by $n*n$ cipher matrix, and the result is done modulo 26. On the contrary, each block is

multiplied with the inverse of the cipher matrix to decrypt the secret message. The result should also be done modulo 26. The method can be done modulo the number of letters instead of 26 if an alphabet with other number of letters.

If the message is 'MONKEY', the steps of encryption are done as follows: 1) Select a $3 * 3$ encryption matrix and the cipher matrix is shown as below (or **SLFWTYCOU** in letters):

$$\begin{bmatrix} 17 & 11 & 5 \\ 21 & 18 & 23 \\ 2 & 13 & 19 \end{bmatrix}$$

This matrix has the determinant -1967. Since -1967 is 0, this matrix is invertible. -1967 is also relatively prime to 26. The selected matrix satisfies the two requirements as key matrix. 2) Divide the message into blocks of size 3 and align these blocks as column vectors. If the length of the message is not evenly divisible by 3, repeat the last character to the end of the string until the message is evenly divisible by 3. Since 'M' is 12, 'O' is 14, 'N' is 13, 'K' is 10, 'E' is 4 and 'Y' is 24, the message is the vector :

$$\begin{bmatrix} 12 & 10 \\ 14 & 4 \\ 13 & 24 \end{bmatrix}$$

The enciphered vector is given by

$$\begin{bmatrix} 17 & 11 & 5 \\ 21 & 18 & 23 \\ 2 & 13 & 19 \end{bmatrix} \begin{bmatrix} 12 & 10 \\ 14 & 4 \\ 13 & 24 \end{bmatrix} = \begin{bmatrix} 423 & 334 \\ 803 & 834 \\ 453 & 528 \end{bmatrix} \equiv \begin{bmatrix} 7 & 22 \\ 23 & 2 \\ 11 & 8 \end{bmatrix} \big[mod 26\big]$$

After encryption, MONKEY is converted into HXLWCI. For the decryption process, inverse of the cipher matrix is calculated first.

$$\begin{bmatrix} 17 & 11 & 5 \\ 21 & 18 & 23 \\ 2 & 13 & 19 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 25 & 10 & 21 \\ 7 & 3 & 0 \\ 9 & 1 & 17 \end{bmatrix}$$

Then, the secret message is got by multiplying the inverse of the cipher matrix.

$$\begin{bmatrix} 25 & 10 & 21 \\ 7 & 3 & 0 \\ 9 & 1 & 17 \end{bmatrix} \begin{bmatrix} 7 & 22 \\ 23 & 2 \\ 11 & 8 \end{bmatrix} = \begin{bmatrix} 636 & 738 \\ 118 & 160 \\ 273 & 336 \end{bmatrix} \equiv \begin{bmatrix} 12 & 10 \\ 14 & 4 \\ 13 & 24 \end{bmatrix} \big[mod 26\big]$$

In a word, the principle can be concluded as [16]:

$$C_d = C_m * P_d \,[\mathrm{mod} N] \tag{1}$$

and

$$P_d = C_m^{-1} * C_d \,[\mathrm{mod}\ N] \tag{2}$$

Where, $C_d$ = Cipher Data, $C_m$ = Cipher Matrix, $Pd = PlainData$, and N is the number of alphabets.

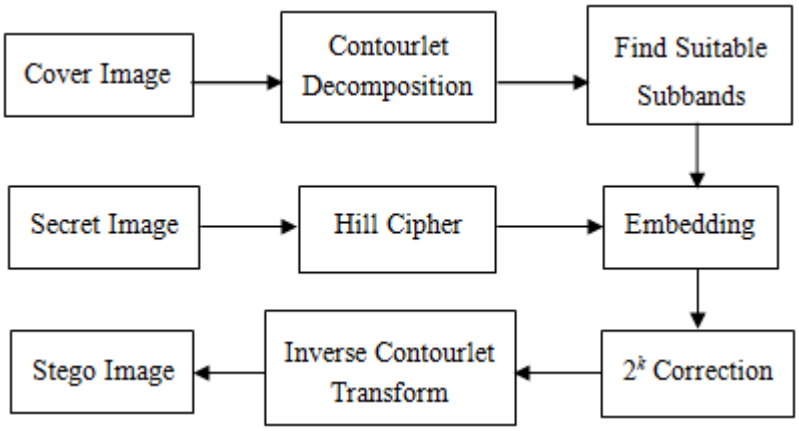


FIGURE 2. Block diagram of data embedding in contourlet domain

4. **The method of $2^k$ Correction.** A mathematic method is applied to achieve better visual effect in stego image. Usually there are some differences between cover pixel and stego pixel after embedding. To reduce these differences, $2^k$ correction method is adopted [17, 18]. The process of $2^k$ correction is defined as follows: *Error value (EV) = |actual pixel value (APV) - stego pixel value (SPV)|*, parameter $k$ is the number of bits which are embedded in actual pixel value.

If (SPV-APV> $2^{k-1}$) & (SPV-$2^k$ >=0)
New stego pixel value = SPV -$2^k$
Else if (SPV- APV< $-2^{k-1}$) & (SPV+$2^k$ <=255)
New stego pixel value = SPV +$2^k$
Else
New stego pixel value = SPV

For example: Actual pixel value (APV) 198 = 11000110, Secret binary data: 001001010, k =3;
Stego pixel value (SPV) 193 = 11000001
$SPV - APV = 193 - 198 = -5 < -2^{(3-1)}$
$SPV + 2^k = 193 + 2^3 = 201 < 255$
New stego pixel value = SPV + $2^k$ =201 = 11001001
New Error value = | 201-198 |= 3< | 198-193 |= 5
In this way, the new stego pixel value is much closer to the actual pixel value (APV) without affecting the secret data.

5. **The Proposed Algorithm.** The embedding procedure is shown as follows:

1) The cover image is decomposed using two level contourlet transform. A low pass image and many high pass subbands are obtained.
2) One of the suitable high pass subbands is selected which is used for embedding the data.
3) The selected high pass subband is divided into 4x4 blocks.
4) Secret image is encoded with Hill Cipher and the mod element will be modified to 256.
5) Embed the message bits in 2-LSBs contourlet coefficients.
6) Apply $2^k$ correction technique on the image to obtain better image visual effect.
7) Inverse contourlet transform is performed on each 4x4 block.
8) Connect all the 4x4 block images together and stego image is created finally.


FIGURE 3. Cover images and their stego images with different methods (a) cover image (b) the result of Shahryaris (c) the result of Masaebis (d) the result of our method

The extracting procedure is shown as follows:

1) The stego image is decomposed by applying two level contourlet transform.
2) The subband in which secret data is embedded is selected.
3) Divide the selected subband into 4x4 blocks.
4) Extract 2-LSBs for each contourlet coefficient.
5) Decrypt the data using Hill cipher and secret image is got.

6. **Experiments and Results.** In this paper, the experiment is done with MATLAB 7 and Windows 7. The computer has Intel CPU 3.3 GHz and 8GB RAM. The peak signal-to-noise ratio (PSNR) and payload are used to evaluate the quality of the stego image after embedding.

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \|I(i,j) - S(i,j)\|^2 \tag{3}$$

Where MSE is the mean squared error between cover image (I) and stego image (S). M and N are the size of row and column of cover image. Thereafter PSNR value is calculated using formula 4 in decibels.

TABLE 1. Comparison between Shahryari and Masaebi and the proposed method in terms of PSNR using clock (128x128) as the secret image

| | | Method | | |
|---|---|---|---|---|
| | **Image** | **Shahryari method [19]** | **Masaebi method [20]** | **Proposed method** |
| **PSNR(db)** | **Baboon** | 43.12 | 51.09 | 52.66 |
| | **Lena** | 43.69 | 51.67 | 53.28 |
| | **Peppers** | 43.25 | 51.28 | 52.96 |
| | **Boat** | 42.93 | 50.87 | 52.49 |
| | **Barbara** | 43.47 | 51.48 | 53.14 |
| | **Airplane** | 40.84 | 48.53 | 51.35 |

$$PSNR = 20\log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \tag{4}$$

The ways of [19] and [20] are compared with the proposed method in this paper. The size of cover image is 512x512 and secret image is 128x128. They are both 8-bit grayscale images.

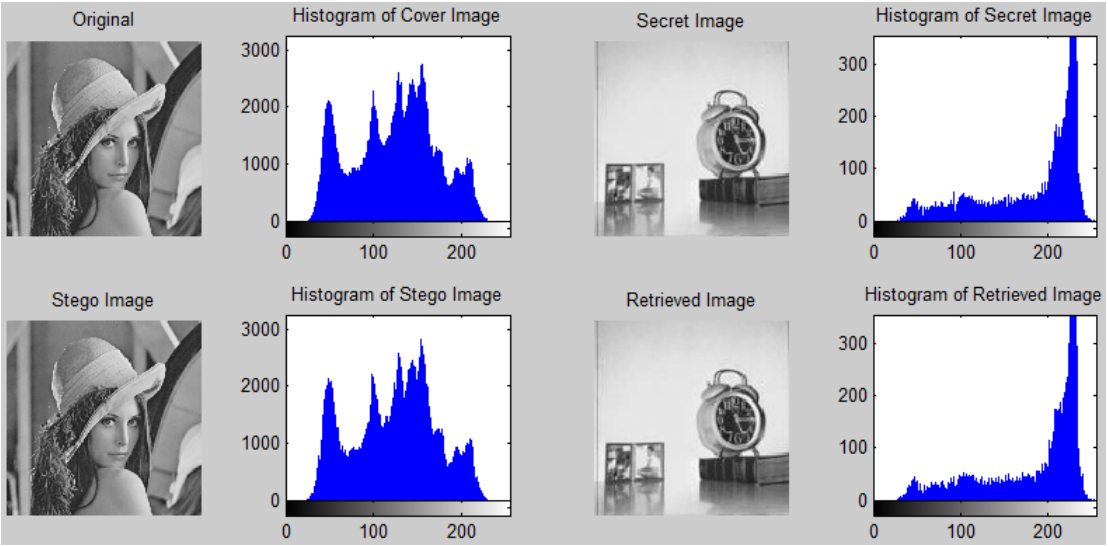


FIGURE 4. Lena and clock payload

From the table 1, it can be concluded that the quality of the stego image with the proposed algorithm is much better than others. The maximum embedding capacity for 2-LSB substitution in proposed method is 25%. Though hiding capacity is low, visual quality of the stego image is high. The embedding capacity can be increased by increasing the number of bits embedded in contourlet coefficients.

It also can be shown in Figure 3 that the stego image in proposed approach is the closest to the original cover image in three methods.

Stego image with PSNR is 53.28db, and extracted image with PSNR is 46.47db.

Stego image with PSNR is 51.72db, and extracted image with PSNR is 45.83db.

Stego image with PSNR is 52.66db, and extracted image with PSNR is 46.28db.

Stego image with PSNR is 52.96db, and extracted image with PSNR is 46.47db. From Figure 4 to Figure 7, each image displays cover image, secret image, stego image, retrieved image and their histograms with proposed method. It also shows that retrieved image is

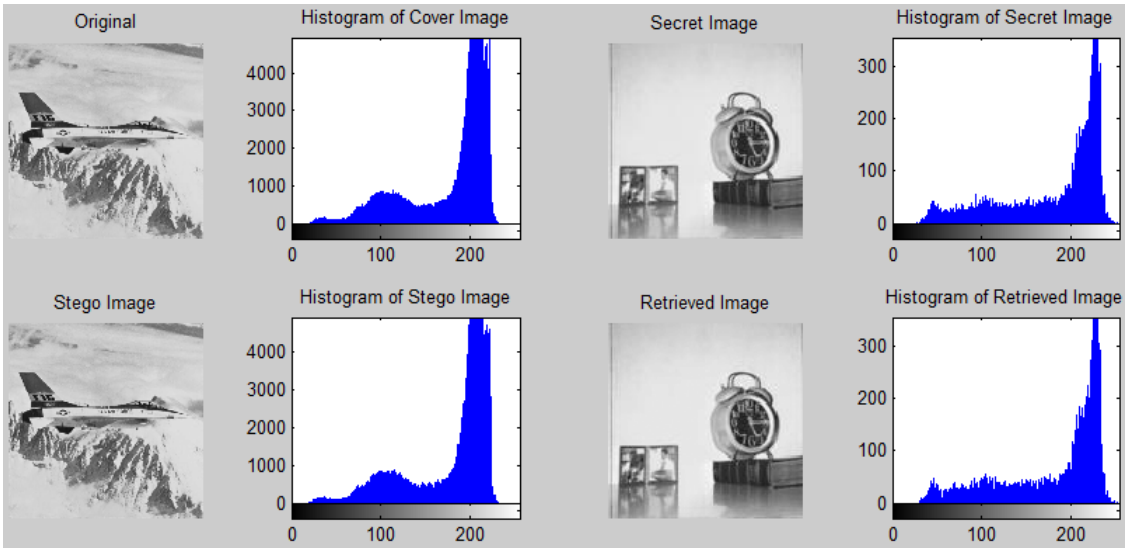


FIGURE 5. Airplane and clock payload

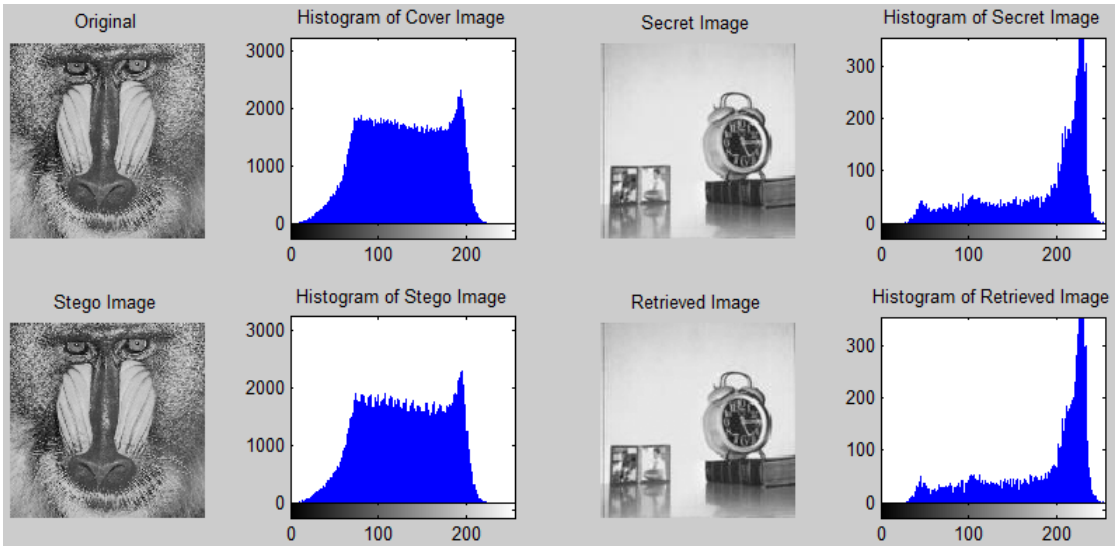


FIGURE 6. Baboon and clock payload

almost the same with original secret image. The conclusion also could be achieved from their histograms.

7. **Conclusion.** In this paper, a novel steganography method is proposed. It is applied in contourlet domain. The algorithm embeds two bits of digit in 2-LSBs contourlet coefficient in 4x4 blocks. Hill cipher and $2^k$ correction are also adopted in this approach. Hill cipher is used to increase the security of secret image. The way of $2^k$ correction is adopted to release the difference between cover and stego image and to get better image quality. It can be demonstrated by experiment that the proposed method provides better PSNR value compared with the existing methods.

**Acknowledgement.** This work was supported by a grant from the National Natural Science Foundation of China (No. 61473329), the Special Research Foundation of the Fujian Province (Grant No. JK2013062), and the Department of Education of Fujian Province (Grant No. JA15571).

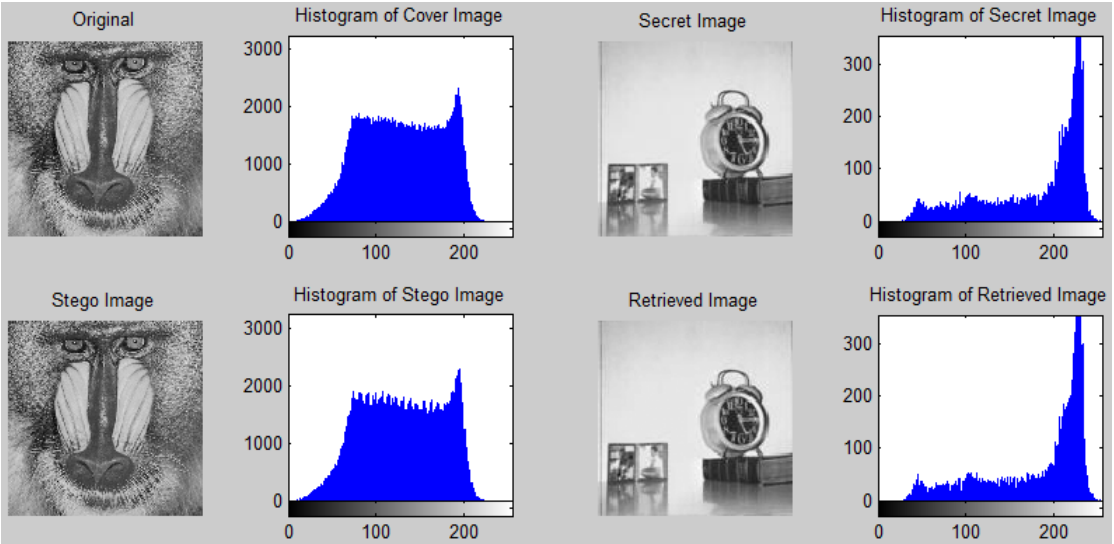


FIGURE 7. Peppers and clock payload

## REFERENCES

[1] S. Channalli, and A. Jadhav, Steganography an art of hiding data, *International Journal on Computer Science and Engineering*, vol. 1, no. 3, pp.137-141, 2009.

[2] D. Singla, and R. Syal, Data security using LSB & DCT steganography in images, *International Journal of Computational Engineering Research*, vol. 2, no. 2, pp. 359-364, 2012.

[3] S. Gupta, A high capacitive and confidentiality steganography using private key, *International Journal of Electronics Communication and Computer Technology*, vol. 1, no. 1, pp. 9-14, 2011.

[4] M. Juneja, and P. S. Sandhu, An improved LSB based steganography technique for RGB color images, *International Journal of Computer and Communication Engineering*, vol. 2, no. 4, pp. 513-517, 2013.

[5] P. R. Rudramath, and M. R. Madki, Improved BPCS steganography based novel approach for data embedding, *International Journal of Engineering and Innovative Technology*, vol. 1, no. 3, pp. 156-159, 2012.

[6] I. Singh, S. Khullar, and S.C. Laroiya, DFT based image enhancement and steganography, *International Journal of Computer Science and Communication Engineering*, vol. 2, no. 1, pp. 5-7, 2013.

[7] H. Patel, and P. Dave, Steganography technique based on DCT coefficients, *International Journal of Engineering Research and Applications*, vol. 2, no. 1, pp. 713-717, 2012.

[8] P. Y. Chen, and H. J. Lin. A DWT based approach for image steganography, *International Journal of Applied Science and Engineering*, vol. 4, no. 3, pp. 275-290, 2006.

[9] M. N. Do, and M. Vetterli, The contourlet transform: an efficient directional multiresolution image representation, *IEEE Transactions on Image Processing*, vol. 14, no. 12, pp. 2091 -2106, 2005.

[10] P. J. Burt, and E. H. Adelson, The Laplacian pyramid as a compact image code, *IEEE Transactions on Communications*, vol. 31, no. 4, pp. 532-540, 1983.

[11] R. H. Bamberger, and M. J. T. Smith. A filter bank for the directional decomposition of images: theory and design, *IEEE Transactions on Signal Processing*, vol. 40, pp. 882-893, 1992.

[12] H. Ramezani, F. Keynia, and F. Ramezani. A novel image steganography in contourlet domain using genetic algorithm, *International Journal of Future Computer and Communication*, vol. 2, no. 4, pp.359-363, 2013.

[13] A. Saravanan, A. Sivabalan, and R. Prabhu, Information hiding scheme on image using contourlet wavelet transform, *International Journal on Advanced Computer Theory and Engineering*, vol. 2, no. 2, pp. 67-70, 2013.

[14] L. S. Hill, Cryptography in an algebraic alphabet, The American Mathematical Monthly, vol.36, pp. 306-312, 1929.

[15] S. K. Mahata, A. Mondal, D. Kumar, and P. Majumdar, A novel approach of steganography using hill cipher, Special Issue of International Journal of Computer Applications, pp. 29-31, 2012.

[16] B. Karthikeyan, J. Chakravarthy, and S. Ramasubramanian, Amalgamation of scanning paths and modified hill cipher for secure steganography, *Australian Journal of Basic and Applied Sciences*, vol. 6, no. 7, pp. 55-61, 2012.

[17] A. Kaur, and S. Kaur, Image steganography based on hybrid edge detection and $2^k$ correction method, *International Journal of Engineering and Innovative Technology*, vol. 1, no. 2, pp. 167-170, 2012.

[18] M. Mahajan, and A. Sharma. Steganography in colored images using information reflector with $2^k$ correction, *International Journal of Computer Applications*, vol. 1, no. 1, pp. 53-59, 2010.

[19] K. Shahryari and M. Gholami. High Capacity Secure Image Steganography Based on Contourlet Transform, *Advances in Computer Science: an International Journal*, vol. 2, no.5, pp. 62-65, 2013.

[20] S. Masaebi and A.M.E. Moghaddam. A New Approach for Image Hiding Based on Contourlet Transform, *International Journal of Electrical and Computer Engineering*, vol.2, no.5, pp. 699-708, 2012.