# Information Hiding Scheme on Image Using Contourlet Wavelet Transform

**A. Saravanan[1], A. Sivabalan[2] & Ramkumar Prabhu[3]**

[1]Department of EEE, [3]Department of ECE,
[1&3]Dhaanish Ahmed College of Engineering, Chennai
[2]Department of ECE, SRM University, Chennai

*Abstract* - **Steganography studies the scheme to hide secrets into the communication between the sender and the receiver such that no other people can detect the existence of the secrets. A steganographic method consists of an embedding algorithm and an extraction algorithm. In this paper, a new adaptive steganography method based on contourlet wavelet transform is presented that provides large embedding capacity. contourlet wavelet transform provides better embedding efficiency and embedding speed. Higher embedding efficiency implies better undetectability for steganographic methods. It hides the data with more accuracy and extracts the data without any loss of any information. The simulation is done using MATLAB 7.**

***Keyword - Steganography, contourlet wavelet transform, image hiding***

## I. INTRODUCTION

Steganography methods hide the secret data in a cover carrier so that the existence of the embedded data is un-detectable. The cover carrier can be different kinds of digital media such as text, image, audio, and video [7]. In a successful steganography method the carrier medium does not attract attentions. The security of the steganography methods is mostly influenced by the kind of cover media, the method for selection of places within the cover that might be modified, the type of embedding operation, and the number of embedding changes that is a quantity related to the length of the embedded data. The aim of the steganography method is to communicate securely in a completely undetectable manner.

Some image hiding systems use uncompressed images (e.g., BMP) or lossless compressed images (e.g., GIF) as cover-images. These images potentially contain visual redundancy so that they can provide large capacity to hide secret data. For reducing transmission bandwidth and storing space, the JPEG is currently the most common format for images that are used on the Internet. Therefore, embedding techniques in Discrete Cosine Transform (DCT) domain are popular because of the large usage of JPEG images. Although modifications of properly selected DCT coefficients during embedding process will not cause noticeable visual artifacts, nevertheless they cause detectable statistical degradations.

On the other hand, some steganography methods based on wavelet transform have been presented. In [8], a steganography method based on wavelet and modulus function is proposed. In this method, the capacity of a cover-image is determined considering the number of wavelet coefficients with larger magnitude.

Crandall first introduced the idea of matrix embedding, which turned out to be very successful. Fridrich[2] et al. proposed a scheme, called the wet paper code, for the situation that some positions in the cover object are invariant. Fridrich and Soukal[3] discussed the scenario when the relative payload (the ratio of the hidden message length to the number of positions used for embedding in the cover object) is relatively large.

Matrix embedding uses linear codes, which is also called syndrome coding or coset encoding. It embeds and extracts a message by using the parity check matrix of a linear code. Zhang and Li[6] generalized the idea of matrix embedding and defined the codes with the matrix as steganographic codes (abbreviated stego-codes). For matrix embedding, finding the stego object with least distortion is difficult in general.

In some special cases, there exist constructive and fast methods. Fridrich et al. utilized LT codes to improve the computational complexity of wet paper codes. Westfeld derived a hash function to efficiently obtain the stego object. Li et al. proposed a scheme called tree-based parity check (TBPC) to reduce distortion on a tree structure.

Chung proposed a toggle criteria of a node in the TBPC method can be relaxed by the strategy of majority vote. This strategy inherits the efficiency of the TBPC method and produces a stego object with least distortion under the tree based parity check model. The time complexity of this embedding (extraction as well) algorithm is asymptotically optimal, that is, it is linearly bounded by the hidden message length. The embedding efficiency is defined to be the number of hidden message bits per embedding modification. Higher embedding efficiency implies better undetectability for steganographic methods.

The lower embedding efficiency is defined to be the ratio of the number of hidden message bits to the maximum embedding modifications. The lower embedding efficiency is related to undetectability in the worst case. It implies steganographic security in the worst case. Thus, the lower embedding efficiency is also an important security factor for a steganographic system.

The Wet Paper Code [1]with Improved Efficiency provides a new tool for Steganography. A coding method that empowers the steganographic with the ability to use arbitrary selection channels while substantially decreasing the number of embedding changes, assuming the embedded message length is shorter than 70% of maximal embedding capacity. The method can be flexibly incorporated as a module into majority of existing steganographic methods.

The Wet Paper channel is highly relevant to Steganography and arises in numerous different situations. One of them is adaptive Steganography, where the sender selects the location of pixels that will carry message bits based on pixels neighborhood in the cover image. A fundamental problem with adaptive schemes is that the requirement that the recipient be able to recover the same message-carrying pixels from the stego image undermines the security of the algorithm because it gives an attacker a starting point for mounting an attack.

Another potential problem is that the recipient may not be able to recover the same set of message carrying pixels from the stego image, which is modified by the embedding act itself. This problem is usually solved either by increasing the message redundancy using error correction to recover from random bit losses and inserts or by employing some artificial measures, such as special embedding operations matched to the selection rules.

## II. CONTOURLET WAVELET TRANSFORM:

Contourlets form a multiresolution directional tight frame designed to efficiently approximate images made of smooth regions separated by smooth boundaries. The Contourlet transform has a fast implementation based on a Laplacian Pyramid decomposition followed by directional filterbanks applied on each bandpass subband.

A filter bank structure that can deal effectively with piecewise smooth images with smooth contours, was proposed by Minh N Do and Martin Vetterli. The resulting image expansion is a directional multi resolution analysis framework composed of contour segments, and thus is named contourlet. This will overcome the challenges of wavelet and curvelet transform.

Contourlet transform is a double filter bank structure. It is implemented by the pyramidal directional filter bank (PDFB) which decomposes images into directional subbands at multiple scales. In terms of structure the contourlet transform is a cascade of a Laplacian Pyramid and a directional filter bank. In essence, it first uses a wavelet-like transform for edge detection, and then a local directional transform for contour segment detection. The contourlet transform provides a sparse representation for two-dimensional piecewise smooth signals that resemble images.The contourlet transform provides a multiscale and multi-directional representation of an image. It consists 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) is first used to capture the point discontinuities, and then followed by a directional filter bank (DFB) to link point iscontinuities into linear structures. The required number of directions can be specified by the user. Since Contourlets gives more edges, it is more suitable for data hiding applications as more data can be hidden in the high frequency regions without perceptually distorting the original image. The overall results in an image expansion using basic elements like contour segments, and, thus, are named Contourlets.Contourlet decomposition is shown in Fig.1.

Contourlet possesses the important properties of directionality and anisotropy which wavelets do not possess and so contourlet outperforms wavelets in many image processing applications. When compared with wavelets Contourlets offer a much richer set of directions and shapes, and thus, it ts 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.

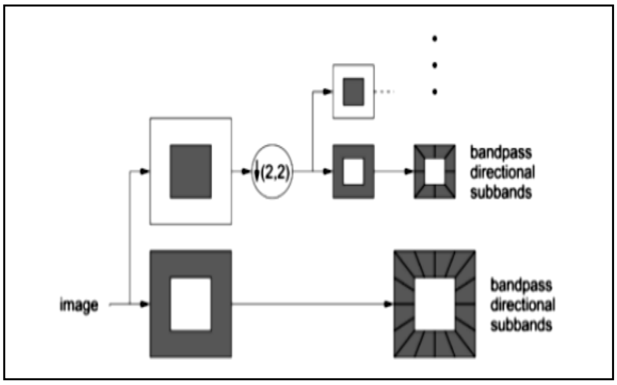

Fig.1 : Contourlet Decomposition Laplacian pyramid followed by directional filter bank.

The Cont-Steg, is a method based on contourlet transform for hiding data in images. In ContSteg, contourlet trans-form is applied to capture significant image coefficients across spatial and directional resolutions. Multiresolution flexibility, local and directional image expansion in the contourlet image representation, allow for easy subband processing. To increase the embedding capacity and quality of stego-images compared to previous methods, we embed the secret data in proper contourlet coefficients of the cover-image. The embedding algorithm takes advantage of adaptive methods by embedding data in non-smooth regions of cover images. In this way, the visual degradation caused by the steganography method can be mitigated because the secret data is embedded in higher contourlet coefficients in edgy and non-smooth areas that can visually hide this information better. The embedding process is carried on by changing the value of two contourlet coefficients to hide one bit of secret data.

Using suitable representation domain and proper coeffi-cients to embed data, can result in stego- images with higher quality. Consequently, higher embedding capacity and enhanced security are provided.It takes advantage of a multiscale framework and its directionality to extract the appropriate places of an image to hide data.

## III. BLOCK DIAGRAM:

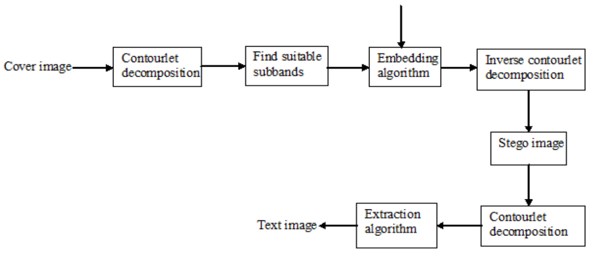

Fig.2 : Block Diagram For Contourlet Wavelet

*Transform*

The block diagram of embedding and extraction of data in contourlet domain is shown in Fig.2.The secret data is first encrypted using proper algorithm and then embedding algorithm is applied.

EMBEDDING PROCESS:

The embedding process is done in the following steps:

Step 1: The cover-image is decomposed with one pyramidal level and sixteen directional contourlet transform.

Step 2: The regions of the subbands in which the data can be embedded are identified. Then the embedding process determines higher contourlet coefficients in these regions that can be used for embedding.

Step 3: According to Kerckhoffs' principle, the embedding algorithm is supposed to be known to the public. Therefore, the embedding process may use an embedding key so that only the legal user can successfully extract the embedded data by using the corresponding extraction key in the extraction process. Accordingly, a key that is a seed for gener-ating a random sequence is considered to provide the embedding location addresses of 4×4 blocks

Step 4: In this step, the embedding module is activated. The place of two coefficients in each block are chosen by the embedding module and agreed upon by both send and receive parties. These two coefficients are suitable for embedding if both of them belong to the higher coefficients set. The embedding module hides each bit of the secret data by comparing and if needed exchanging the values of two contourlet coefficients in non- smooth regions of the image.We use two coeffi-cients (a,b)and(c,d) A 4×4 block encodes bit *1* if its *coefficient*(*a*,*b*) >= *coeffi-cient*(*c*,*d*) and bit *0* otherwise. Two coefficients are swapped if their values do not match with the bit to be encoded.

EXTRACTION PROCESS:

The stego-key used in the embedding process should be shared by both the sender and receiver so that the em-bedded data can be extracted by a legal receiver. The extraction module consists of the following steps:

Step 1: Decompose stego-image with a one level contourlet transform.

Step 2: Recognize higher contourlet coefficients.

Step 3: Form the random sequence by using the same key as the sender has used.

Step 4: Retrieve the embedded data by comparing coefficient (a,b) and coefficient(c,d) in each 4×4 coefficient block. If coefficient(a,b) >= coefficient(c,d) , the hidden bit is 1 and it is 0 otherwise.

## IV. CONCLUSION

By introducing the contourlet wavelet transform, the stego image have effectively embedded and extracted without distortion. The main idea is to the image quality while increasing the data hiding ratio. This method will not degrade the image quality based on the amount it can hide. It embeds a secret data in contourlet transform coeffi-cients of an image. Since embedding data in non-smooth and edgy regions of the image causes less delectability, these regions of the image are identified in contourlet domain and the secret data is embedded in the corre- sponding coefficients.The stego image should not be distinguishable from cover image, so that attacker cannot discover any embedding message. In comparison with the TBPC and majority vote parity check method, this method significantly achieves higher embedding efficiency and embedding speed.

## V. REFERENCES

[1] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, "Writing on wet paper,"IEEE Trans. Signal Process., vol. 53, no. 10, pp. 3923–3935, Oct. 2005.

[2] J. Fridrich, M. Goljan, and D. Soukal, "Efficient wet paper codes," in Proc. 7th Int. Workshop Inf. Hiding (IHW 05), Lecture Notes in Com-puter Science, 2005, vol. 3727, pp. 204–218.

[3] J. Fridrich and D. Soukal, "Matrix embedding for large payloads," IEEE Trans. Inf. Forensics Security, vol. 1, no. 3, pp. 390–395, Sep.2006.

[4] M. Khatirinejad and P. Lisonek, "Linear codes for high payload steganography,"Discrete Applied Math., vol. 157, no. 5, pp. 971–981, 2009.

[5] R. Y. M. Li, O. C. Au, K. K. Lai, C. K. Yuk, and S.-Y. Lam, "Data hiding with tree based parity check," inProc. IEEE Int. Conf. Multi-media and Expo (ICME 07), 2007, pp. 635–638.

[6] W. Zhang and S. Li, "A coding problem in steganography,"Designs, Codes Cryptogr., vol. 46, no. 1, pp. 68–81, 2008.

[7] W. Zhang, X. Zhang, and S. Wang, "Maximizing steganographic em-bedding efficiency by combining hamming codes and wet paper codes," inProc. Int. Wo

[7] C. Liu and S. Liao, "High-performance JPEG steg- anography using complementary embedding strategy," Pattern Recognition, Vol. 41, pp. 2945–2955, 2008.

[8] K. Zhiwei, L. Jing, and H. Yigang, "Steganography based on wavelet transform and modulus function," Journal of Systems Engineering and Electronics, Vol. 18, No. 3, pp. 628–632, 2007.

◈◈◈