International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 24 Issue 8 – MAY 2017.

ENCRYPTING SECRET KEY IN STEGANOGRAPHY TO EMBED SECRET IMAGE AND RETRIEVE IT USING CONTOURLET TRANSFORM

N.Lettishyal [#1]

[#] *Research Scholar, Department of CS, Jerusalem College of Engineering, Chennai, India*

***Abstract*— In this paper, we present a new adaptive contourlet-based steganography method that hides secret data in an explicit or automatically selected cover image. Our proposed steganography method primarily decomposes the cover image by contourlet transform. Then, every bit of secret data is embedded by increasing or decreasing the value of one coefficient in a block of a contourlet subband. Contourlet coefficients are manipulated relative to their magnitudes to hide the secret data adaptively. In addition to proposing contourlet-based steganography method, this work investigates the effect of cover selection on steganography embedding and steganalysis results. We demonstrate, through the experiments, that choosing suitable cover image by a proper selection measure could help the steganographer reduce detectability of stego images. The proposed technique is examined with some state-of-the-art steganalysis methods, and the results illustrate that an image can successfully hide secret data with average embedding capacity of 0.02 bits per pixel in a random selected cover image. Cover selection improves the embedding capacity up to 0.06 bits per pixel. Several experiments and comparative studies are performed to show the effectiveness of the proposed technique in enhancing the security of stego images, as well as to demonstrate its gain over the previous approaches in literature.**

***Index Terms*— Contourlet transform · Steganography · Steganalysis · Cover selection · Image Encryption**

I. INTRODUCTION

In Steganography methods hide the secret data in a cover carrier so that the existence of the embedded data is undetectable. The cover carrier can be different kinds of digital media such as text, image, audio, and video [1]. 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 methods is to communicate securely in a completely undetectable manner. As the steganography techniques progress, there is an increased interest in steganalysis algorithms which their main goal is detecting the presence of hidden data. Many steganography methods have been proposed and several stego-products have been developed (e.g., EzStego [2]) in which an innocuous-looking image is used as the cover-image to conceal the secret data. In these methods, the secret data is embedded into the cover-image by modifying the cover-image to form a stego-image.

Some image hiding systems use uncompressed images (e.g., BMP) or lossless compressed images (e.g., GIF) as cover-images [3]. 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 [4]. 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. Various steganography methods like F5, Outguess [4], Modelbased (MB) [5], Perturbed Quantization (PQ) [6], and YASS [7] have been proposed with the purpose of minimizing the statistical artifacts which are produced by modifications of DCT coefficients. 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. Embedding data in adaptively selected parts of coverimages such as regions having edges and texture enhances the security of stego-images [9].

An adaptive steganography method attempts to provide secure embedding by ensuring that the changes introduced into the cover-images remain consistent with natural properties of them. Since human eyes are less sensitive in edgy and non-smooth regions of images, modifications in these parts of cover-images are less detectable. In [10] we proposed a new steganography method that embeds secret data in contourlet coefficients of images. In this paper, we

describe the method introduced in [10] with more details and complete our experiments with a larger image database.

In this paper, we introduce a contourlet transform based setganography for hiding data in images. In ContSteg, contourlet transform 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 [11]. 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 [12].

The remainder of this paper is organized as in the following sections. We will describe the related works in Section 2. Section 3 will present the proposed contourlet transform based steganography method. In Section 4, we will analyze the proposed method and compare it with standard steganography methods. Finally, a brief conclusion will be given in Section 5.

II. RELATED WORK

Contourlet transform, proposed by Do and Vetterli, provides a flexible multiresolution and directional expansion method for an image representation. Based on these features, contourlet transform can act as a useful tool in steganography. However, only a few methods have used contourlet transform for data hiding in the past. Liu et al. proposed the first article on the data hiding with contourlet transform. They proposed the adaptive watermarking method based on nonsubsampled transform (NSCT) for color images. Using this method, the watermark is embedded in the singular values of the blocks of NSCT subbands. The transform is applied to the blue component of the color image because of the insensitivity of eyes to the color blue. Since the focus of their work was on watermarking, they have emphasized the robustness and fidelity, and have not discussed the security of the algorithm [13].

Mohan and Anurenjan presented a data hiding technique for embedding text data into an image using contourlet transform. In this algorithm, by contourlet transforming the cover image, the encrypted data is embedded into the image by modifying the least significant digits of contourlet transform coefficients. Embedding is performed on the high frequency directional pass-band of contourlet transform. The proposed method is designed for the digits and it is not comparable to the standard steganography methods which use pseudorandom message bits. Also, it does not discuss the message retrieval error rate in message extraction [14].

Sajedi and Jamzad have utilized contourlet transform for adaptive steganography. They used contourlet transform coefficients for embedding the message bits. In their algorithm, each contourlet transform subband is divided into 4 × 4 blocks. In this model, large values of t are more appropriate because they yield lower message retrieval error rate, while, however, image quality is damaged. In the above methods, the contourlet transform coefficients are manipulated to embed the message bits. There are high dependencies between the neighboring contourlet transform coefficients. Therefore, changing the magnitude of coefficients may affect neighbor coefficients which may lead to the loss of the embedded data during inverse contourlet transform. In this method each message bit is embedded into a 4 × 4 block of contourlet transform coefficients to avoid effects of dependencies. Even with its low embedding capacity, this method cannot reach a perfect message retrieval rate [15].

III. PROPOSED WORK

The proposed method consists of four modules namely encryption, image embedding, image de-embedding and decryption. Blowfish algorithm is used to encrypt the secret image. Then the discrete contourlet transform algorithm is applied on the encrypted secret image and it is embedded into the cover image. Hence the stego-image is created and sent to the receiver. This is the process takes place at the sender side. Once the receiver gets the stego-image, then the contourlet transform is applied to extract the encrypted secret image from the cover image. Finally the image is decrypted to obtain the secret image. The following algorithm explains the process of the proposed method.

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 2k 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.

A. The Contourlet Transform

The contourlet transform was proposed by Do and Vetterli. It consists of a Laplacian pyramid (LP) and a double filter bank (DFB). 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. 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. 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.

The architecture of the proposed work is given in the figure 1.

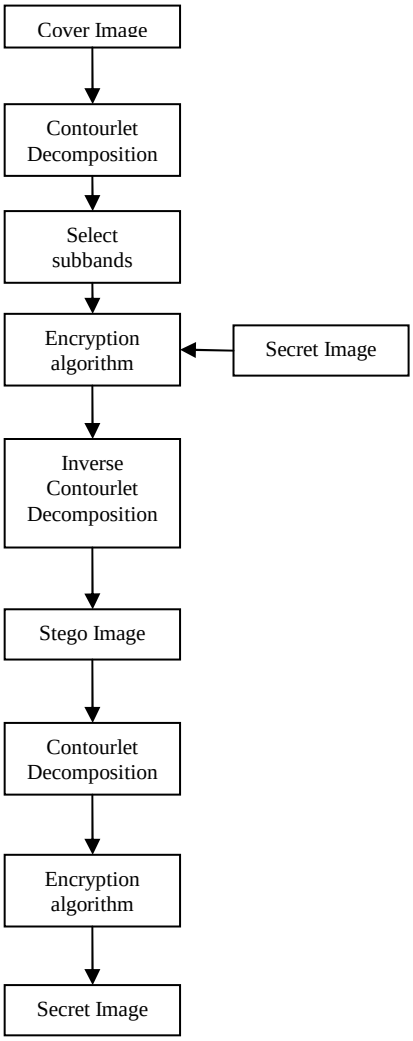

Figure 1. Proposed system architecture

B. Steganography in Contourlet Domain

Using appropriate embedding domain to hide data can provide higher embedding rate, less detectability, and enhanced security. Based on this idea, we propose a steganography approach that takes advantage of the multiscale framework and directionality of contourlet transform.

Adaptive steganography methods hide secret information considering the features of the cover object. This adaptation results in less detectability for stego images. To achieve an adaptive steganography algorithm, we employ an iterative embedding procedure. Our proposed method hides one bit of secret data in a block of contourlet coefficients. Unlike other adaptive steganography methods whose embedding rate depends on the cover image content, in our proposed method the embedding rate can be determined by the steganographer. Choosing different sizes for the block of coefficients gives various embedding rates.

The embedding process is summarized in the following steps.

Step 1: Decompose the cover image by one level CT.

Step 2: The size of a square block of contourlet coefficients to embed one bit of secret data is determined based on the secret data size.

Step 3: Select a block of coefficients from a directional subband to embed one bit of secret data.

Step 4: Apply a rule that says: any modified coefficient value above or below zero represents a 1 or a 0 bit, respectively. Therefore, if the coefficient value does not match with the secret bit value, increase its negative value to become positive to represents a 1 bit or decrease its positive value to become negative to represents a 0 bit. The increment or decrement of coefficient values is repeated until in the data extraction process, the hidden bits can be extracted without any error. In this way, the value of a coefficient is changed repetitively depending on the context of the region in which the coefficient resides.

Step 5: Repeat Steps 3 to 5 until the entire secret data is embedded.

Step 6: Apply ICT to obtain the stego image.

In the homogenous regions of a cover image, a little change of a coefficient value can embed a bit. However, in non-smooth regions, a coefficient value may be affected by the value of its neighbor coefficients. This effect is caused by non-orthogonality of contourlet transform and JPEG compression. In this state, to embed a bit, a greater change is needed. We do not worry about this higher change because non-smooth regions generally can be considered noisy and the additional noise caused by embedding method is difficult to detect.

C.Embedding and Extraction of Secret Image

In the first stage of the proposed steganography method, an image is decomposed with a one level contourlet transform. Then the embedding method determines the regions of the subbands in which the data can be embedded. It also determines higher contourlet coefficients in these regions that can be used for embedding. After determining proper coefficients, a key that is a seed for generating a random sequence is considered to provide the embedding location

addresses of 4×4 blocks. The place of two coefficients in each block are chosen and agreed upon by both send and receive parties. These two coefficients are suitable for embedding if both of them be member of the higher coefficients set. Each bit of the secret data is hidden by comparing and if needed exchanging the values of two contourlet coefficients corresponding to non-smooth regions of the image.

A 4×4 block encodes a *1* if its *coefficient(a,b)* > *coefficient(c,d)* and *0* otherwise. Two coefficients are swapped if their values do not match with the bit to be encoded. Since the JPEG compression and non-orthog- of the coefficients, the algorithm ensures that $|coefficient(a,b) - coefficient(c,d)| > t$, where t is a value that represents the tradeoff between image quality and hidden data retrieval error rate. Due to the cases we mentioned before, manipulating the value of coefficients may cause loss of the embedded data in inverse contourlet transform. In addition, it may affect the value of neighborhood coefficients and thus the embedded data in such neighborhood may be lost. To maintain a high level of similarity between original clean and the stego images, and to have minimum loss in extracted data, each manipulated coefficient should be selected far enough from others. Considering these properties, we consider each coefficient block of size 4×4.

In extraction phase, the recipient first recognizes the higher contourlet coefficients and forms the random sequence by using the same key as the sender has used. Then he retrieves the embedded data by comparing the contourlet coefficients. Exact measures attempt to find the best cover image from the database considering a given secret data. Visual quality and amount of changes in a cover image are two exact measures that are described in following subsections. After the secret data is fed to the system, we need to evaluate each image in the database to select a suitable cover image.

In this approach, we obtain optimum amount of changes in contourlet coefficients that guarantees no lost bits in the extracted secret data while maintaining the least distortion in the stego image. Our proposed method changes one coefficient in a block of contourlet coefficients of size not necessary 8×8. Considering steganalysis algorithms that extract interand intra-block dependencies in 8 × 8 size DCT blocks, our method may not be easily detectable by such steganalyzers. The larger database has the higher the time complexity of this procedure. In spite of high time complexity, since the best cover image is selected regarding to the secret data, the performance of exact measures from visual quality and amount of distortion viewpoints is higher than the fast measures. Consequently, the detectability of stego images will be lower, and therefore to have a high capacity communication, it is worth to spend time on selecting an appropriate cover image.

IV. EXPERIMENTAL ANALYSIS

All tests have been performed using an Intel® core™i5 CPU M450 @2.4GHz with 6GB Memory, running Windows 7 64-bit operating system and using MATLAB 8. The image used is an RGB color JPEG images with size 512 × 512, resolution 96 × 96 dpi and bit depth 24. There are four main tests to determine the performance of any stegnanography approach; visual test to determine any degradation in quality or colors compared to original image, the Peak Signal-to-Noise Ratio (PSNR) of the stego image, the embedding algorithm CPU time, and the secret text message extraction complexity.

To evaluate the performance of the proposed embedding algorithm experiment was conducted using gray scale images with different size.. The image is composed to level two using NSCT. The result contains a lowpass band and many highpass subbands. One of the subbands is chosen for data embedding related to its features. Proposed algorithm tested using different block sizes to embed data with different threshold values [$0.2 \leq$ Threshold ≤ 0.9] for extract data, figure(2) show that embedding process with block size (4×4) give high capacity for embedding data without any error more than other sizes (5×5 -11×11). Extraction process depends on threshold value, figure (3) show threshold value and Error rate percent in extracted data according to that threshold. It is clear that Error free appear on threshold value (0.5 and 0.55) for all block sizes.

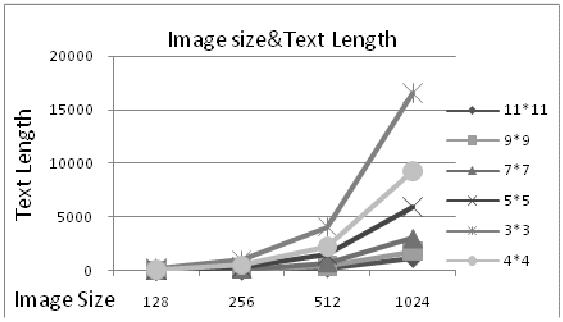

Figure 2. Embedding capacity according to block size

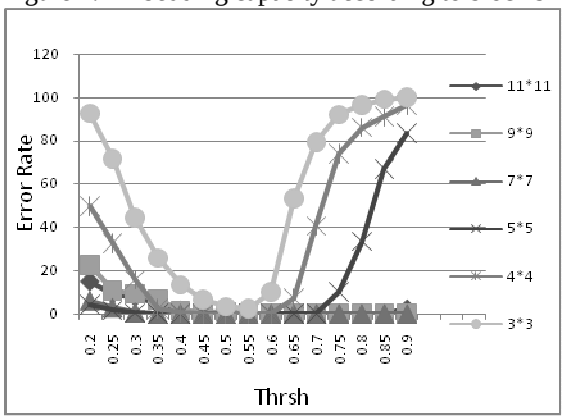

Figure 3. Error rate in extracted data from stego image 512×512

Image features like PSNR, MSE and Correlation are also analyzed between original image and retrieval one. PSNR stands for peak signal to noise ratio, which is a measure for image quality perpose. 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. 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.

Figure (4) shows the variation of PSNR and MSE and Correlation for different volume of embedded data.

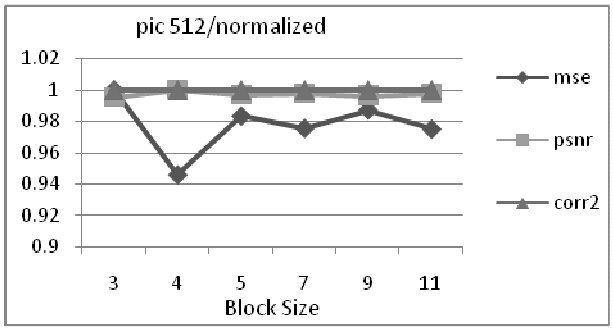

Figure 4. MSE & PSNR & Correlation

As shown from the visualization test, the stego images for the proposed approach and the other compared approaches in this paper do not have any degradation in quality. The evaluation results illustrate that the PSNR of the stego image for the proposed approach is in the range of the other state of the art approaches. The CPU time for the proposed approach is in the range of the other state-of-the-art approaches, the difference is a fraction of a second. Extracting the secret text message in the proposed approach is more complex, secure, and it could not be monitored by unauthorized users. It must be clarified that the proposed approach here is based on multi-crops. So it is possible to choose any number of crops and it can be used to hide images or texts by converting them into bit stream and then embedding this stream into the cover image using the proposed approach in this paper.

V. 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 coefficients 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 corresponding 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.

The future work will focus on studying the same idea on dynamic encryption technique in addition to look for other security features on the coefficients of the contourlet to select in which one the embedding process will applied.

REFERENCES

[1] S. Channalli, and A. Jadhav, Steganography an art of hiding data, International Journal on Com- puter 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 con_dentiality steganography using private key, International Jour- nal 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, Interna- tional 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 coe_cients, 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 e_cient 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 _lter 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.