Image Steganography Using Contourlet Transform And Diamond Encoding Method

Khushmanpreet Kaur[1], Er. Navroz Kahlon[2]
[1, 2] Dept of Computer Engineering
[1, 2] University College of Engineering, Punjabi University Patiala, Punjab

Abstract- *Steganography is information security tool which stores the secret information in any media file e.g. text, image, audio and video file in such way that no one else except the sender of the information and the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data satisfactory security is maintained. In this paper, Transform based techniques has been explored in which DWT and contourlet based decomposition method has been used to obtain the detailed coefficients for data embedding. Wavelets are not effective to represent the images with smooth contours in different directions. Directionality and anisotropy properties are handled by CNT by providing multi-scale and directional decomposition. IN CNT, Laplacian Pyramid (LP) structure has been introduced for multi-scale decomposition of images. Hence contourlet transform has been used instead of discrete wavelets. The proposed algorithm first converts the secret bits into a sequence of base-5 digits. Further Security of information has been achieved by random key generators which select scrambled pairs from different types of detailed coefficients needed by DE (diamond encoding) based embedding process. Experimental results that Contourlet based steganography gives low MSE and high PSNR and SSIM quality values as compared to discrete wavelet transform when similar rules for secret information selection and embedding methods are used.*

Keywords- Base5digit conversion, Diamond encoding, DWT Steganography , PSNR etc.

I. INTRODUCTION

Steganography and watermarking are two important sub disciplines of information hiding that deal with embedding information in digital media like images, audio and video. Steganography uses a media as a container for concealing secret messages without raising suspicion regarding the presence of a hidden communication. This method of hiding the existence of secret information has gained popularity due to the widespread deployment of the Internet around the world and frequent use of digital media for a large variety of applications [1]. Steganography has helped people maintain privacy of their communication even in the presence of monitoring agencies or governmental control. Watermarking technology is directed towards protection of digital media against misuse, illegal copying and false claims of ownership. Watermarking schemes are required to be attack resistant i.e., the information embedded in the media has to be recoverable at the receiving end even if an active attacker is able to modify the media significantly. The vital data is normally encoded in the most significant regions of the media. Digital steganography is used for secret transmission of text messages, numeric data, photographs, maps, drawings, human speech and other forms of sounds. An image as a container of these messages is quite popular. Techniques for data embedding in images include processing in the spatial-domain as well as transform-domain [2] like Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), which are quite popular. SVD for information hiding is not a well-exploited area but offers an attractive domain for this purpose. After selecting a particular domain, a stego-designer strikes a balance for catering to issues like perceptual transparency, capacity, survivability and secrecy of the hidden data. The additional requirement of robustness against different types of intentional attacks [3] in watermarking is addressed by embedding the external data in significant regions of the transformed domain. Spatial methods generally replace the direct least significant bit (LSB), substituting a redundant part of a cover image with the secret message. The disadvantage is that embedding in, say, the fourth LSB generates more visual distortion to the cover image than in the first LSB. The hidden information is seen as ‘non-natural’ and a tradeoff exists between payload and cover image distortion; thus, the payload, (embedding up to the first, second, third or fourth LSB) is analogous with the quality of the recovered embedded image [4].

Methods, such as Fourier transform, discrete cosine transform (DCT) and discrete wavelet transform (DWT), embed information in the frequency domain of a cover image. Messages are hidden in significant areas of the cover image, making them more robust against attacks such as compression, cropping and some image processing than the LSB approach [4].

Recent methods such as perceptual masking or adaptive steganography (AS) can be applied in the spatial or frequency domain [4].

AS measures statistical features of the image before attempting to interact with its LSB/DCT coefficients, to determine where best to make changes to avoid areas of uniform colour (smooth areas); AS is characterised by random adaptive selection of pixels, depending on the cover image, and selection of pixels in a block with large local standard deviation, and has proven robust with respect to compression, cropping and image processing.[4] For instance, since high-energy wavelet coefficients correspond to the signal features of sharp variation as edges and textures, and low-energy corresponds to the smooth regions, the current wavelet kernel is compared with a prescribed threshold level to identify the signal- or noise dominant regions in a scale. DWT coefficients based steganography is widely used in which secret information is inserted in detailed coefficients. For increase in security these coefficients are selected randomly based on some pre-defined key oriented random generators which assist in reversible way to extract the secret information from the steago image. DWT has less embedding capacity and low PSNR of the produced steago images. This drawback has been explored in current paper in which contourlet based transform has been used for multi-level decomposition. Contourlet tansform provides four directional coefficients instead of three as provided by DWT. By using Contourlet transform, embedding capacity as well as PSNR value has been increased. A brief of realted work in image steganography using different transform methods has been given below

II. LITERATURE SURVEY

In this section we have covered a brief survey of existed literature which used different steganographic techniques.

Ratnakirti Roy et al [5] proposed an object based image steganography technique that utilizes image entropy to segment smooth and textured areas in a cover image and then embed data with a variable data rate high efficiency embedding scheme. The method is shown to yield promising results in terms of stegoimage fidelity and statistical imperceptibility.

Hyunho Kang et al [6] developed a method for block-based tamper detection steganography that can verify not only forgery but also a cutting attack on a stego image. For verifying the integrity of the secret information, both the previous block and the most significant bits (MSBs) of the current block were used. The number of insertion bits per pixel is determined according to the variance of adjacent pixels. Secret information embedding and extraction are performed by using a block unit in the spatial domain of an image.

Sabyasachi Kamila et al [7] proposed a new method for color image steganography in frequency domain where Discrete Wavelet Transform (DWT) of the cover image is used to differentiate high frequency and low frequency information of each pixel of the image. Proposed method hides secret bits in three higher frequency components making sure that the embedding impact on the cover image is minimum and not centralized in sensitivity domain.

Hamad A. Al-Korbi et al. [8] aimed at proposing a high capacity and efficient steganography technique, where binary images, color images, and large text files can be all concealed within a single cover image at the same time using Haar Wavelet transform.

Swarnjeet Kaur et al. [9] proposed a method, a hybrid approach of data hiding, in which a hybrid method of data hiding using optimal pixel adjustment process (OPAP) and identical matching has been used. Also, to make the algorithm more imperceptible data is divided into segments and image into blocks and a data segment is embedded into an image block where it affects the least image quality.

M. Tulasidasu et al. [10] presented a best approach for Least Significant Bit focused around picture Steganography that upgrades the current LSB substitution systems to enhance the security level of concealed data. In the proposed work shrouded data is stored into distinctive position of LSB of picture utilizing block division procedure relying upon the secret key. Therefore it is hard to concentrate the concealed data knowing the recovery systems..

Shuliang Sun et al. [11] proposed a novel algorithm which is based on Canny edge detector and 2k correction. The new method also utilizes Huffman encoding and coherent bit length. Firstly, Canny edge detector is applied to detect the edge of cover image and only edge pixels are selected for embedding payload. Sorting method is used to randomize the edge pixels in order to enhance security. Then Huffman table is constructed. Huffman encoding is practiced to code the secret data before embedded according to Huffman table..

Mohammad Reza Keyvanpour et al. [12] presented a new robust watermarking scheme. The proposed algorithm is based on a chaotic mapping and a dynamic blocking, operating in the DWT domain. The framework of the proposed embedding algorithm consists of a special encoding process that has used a chaotic map for producing the embedding key (first key) (in the LL (3) step of the DWT domain). Because of using Arnold's Cat Map, the key can be produced in the extraction phase without the need for the presence of the original or transmitted information. This phase utilized the special dynamic blocking method and wavelet coefficient quantization (HL (3) or LH (3)) too. The wavelet quantization process sends the sequence (second key) for completion of the extraction phase. Because of the fact that both watermark embedding and detection are accomplished without using the original image, the algorithm claims that it is blind.

Della Baby et al. [13] proposed a data securing technique that is used for hiding multiple color images into a single color image using the Discrete Wavelet Transform. The cover image is split up into R, G and B planes. Secret images are embedded into these planes. An N-level decomposition of the cover image and the secret images are done and some frequency components of the same are combined. Secret images are then extracted from the stego image. Here, the stego image obtained has a less perceptible changes compared to the original image with high overall security.

III. PRESENT WORK

A. System Design

The size of area to be hiding is based on user selection in which resizing of secret image can be done. The size of watermark depends upon the size of cover image and technique used. The steps in the process flow are given in figure below

B. Stepwise Description of Process

1. Secret and cover image selection

In this step, the image to be embedded is selected and resized to the desired size. Then cover image is selected which is converted to grayscale.

2.Base five digit conversions

The arrangement of base-5 digits (B5D) is created from the base 10 digit in which four single digit values ranging between 0-4 are generated. These values are embedded into the coefficient pairs of the sub-bands utilizing the DE plot.

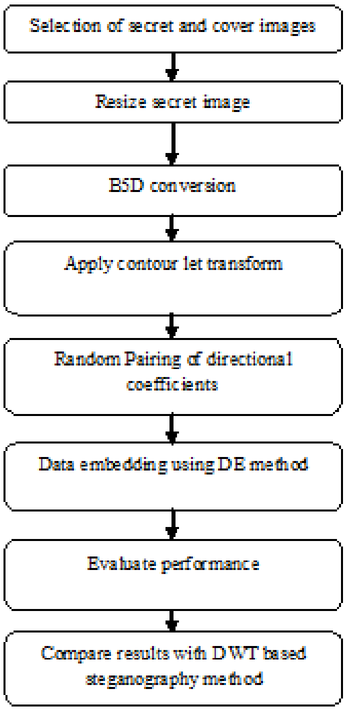
Selection of secret and cover images
Resize secret image
B5D conversion
Apply contour let transform
Random Pairing of directional coefficients
Data embedding using DE method
Evaluate performance
Compare results with DWT based steganography method

Figure 1: Proposed Model of Embedding process

3. Embedding

(a) Steps in the Embedding Procedure

Step1)

To begin with, according to the secret data size, a parameter k is selected, and we transform secret data into diamond encoding digits. Assume that the secret data size is s, and then the embedding parameter k is determined by finding the minimal positive integer that satisfies the following inequality [14]:

$$\left\lfloor \left(\frac{m\times n}{2}\right)\log_2(2k^2+2k+1)\right\rfloor \geq s. \qquad (1)$$

Set the embedding base l = 2k^2 + 2k + 1. Then, the secret message is regarded as a sequence of digits in l-ary notational system.

Step 2)

In the data embedding procedure, the original image is first decomposed using contourlet transform. Then its coefficients are segmented into a number of non-overlapping two-pixel blocks. Then, we can select each block from top-down and left-right in turn for data embedding process. The block vector (x, y) is defined as x = I(2t) and y = I(2t + 1) where I is the cover image sized m × n, and t is the block index. The embedded secret data bit stream is transformed into l-ary digit sequence. Moreover, the embedded secret digit s_t is obtained from the tth index of the sequence of l-ary digits.

Step 3)

Compute the DCV of two pixel values x and y

$$DCV\left(a,b\right)=\left(3a+b\right)\bmod 5$$

f(x, y) = ((2k + 1) × x + y) mod l. (2)

Step 4)

The new stego-image pixel pair can be calculated by replacing f (x, y) with st. The used equation is shown as follows:

$$d_t = \left(s_t - f\ \left(x, y\right)\right)\ mod\ l \quad . \qquad (3)$$

The symbol d_t shows the modulus distance between the st and f (x, y). By applying the distance dt, the stego-pixel values x' and y' can be found in D_k such that the DCV is replaced with s_t. However, in this step, the overflow or underflow problems might be occurred; that is, the stegopixel value x' or y' might go beyond 255 or below 0. If it happens, the next step, namely Step 5, has to be processed; otherwise, Step 5 has to be skipped, and the data embedding procedure is finished.

Step 5)

When one stego-pixel value has the overflow or underflow problem, the critical vector (x' , y') has to be adjusted to the appropriate value. The adjustment rules are defined as follows:

(1) if x' > 255, x' = x' − l;
(2) if x' < 0, x' = x' + l;
(3) if y' > 255, x' = x' − l;
(4) if y' < 0, y' = y' + l.

From the above rules, it can be observed that the overflow/underflow problem is solved and the DCV also has the same value. After all, we take the next pixel pair from the cover image and repeat Steps 2–5. Repeat until all the secret data have been concealed. Then we collect all stego-pixel values to form the stego-image I'. The embedding parameter k has to transmit to the receiver in order to extract data.

(b) Extraction

Here are the steps to extract the secret data from the stego-image I' and the detailed secret data extraction is described as follows [14].

Step 1)

To begin with, in the data extraction procedure, the steago image is decomposed using contourlet transform. Then its coefficients are segmented into a number of non-overlapping two-pixel blocks. Then, we can select each block from top-down and left-right in turn for data extraction process. The block vector (x’, y’) is defined as x' = I (2t) and y' = I (2t + 1). The block construction of the proposed scheme is illustrated by Figure 2.

Step 2)

According to the parameter k, set the embedding base l = 2k^2 + 2k + 1. For each stego-pixel pair p' and q’, the DCV of (x, y) is obtained:

$$f\ \left(x'\ , y'\right)\ =\ \left(\left(2k\ +\ 1\right)\ \times\ x'\ +\ y'\right)\ mod\ l \qquad (4)$$

Therefore, the secret digit st is obtained by the DCV of (x’, y’).

Step 3)

Take the next pixel pair from the stego-image and repeat Steps 1 and 2. The same thing goes on and on until all secret digits have been extracted for each block with index t.

Step 4)

Finally, the secret data can be obtained by transforming the secret symbols to binary bits with base 2.

IV. RESULTS AND DISCUSSIONS

Table 1: Comparison of DWT based and Contourlet transform based steganography using MSE and PSNR parameters

Image	MSE with DWT based steganography	PSNR with DWT based steganography	MSE with Contourlet transform based steganography	PSNR with Contourlet transform based steganography
	217.066	24.764	42.865	31.809
	238.551	24.354	35.175	32.668
	132.558	26.906	29.464	33.437
	95.193	28.344	12.897	37.025
	39.742	32.138	8.905	38.633

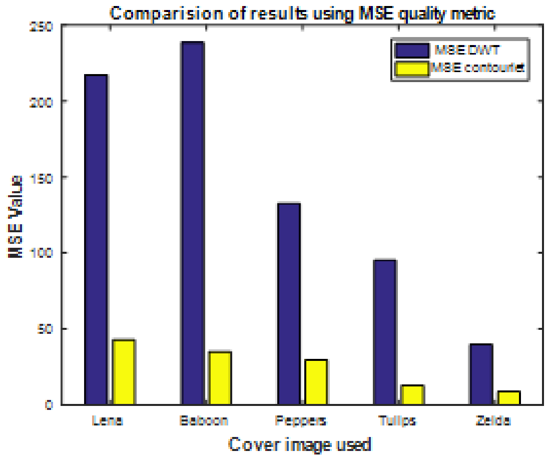

Figure 3: Bar graph using MSE metric for DWT and contourlet based steganography method

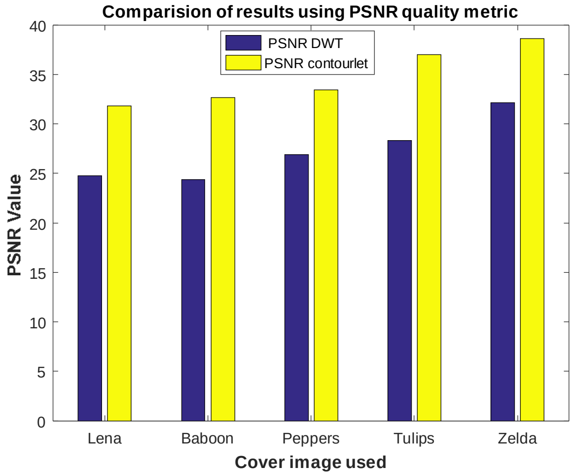

Figure 4: Bar graph using PSNR metric for DWT and contourlet based steganography method

In contour let transform, Laplacian pyramid scheme generates down-sampled low pass version of original image and the difference between the original and the low pass image, resulting a band pass image. Then the obtained band pass image is further processed through directional filter bank (DFB). DFB contains the high frequency information like smooth contour and edge information of images. It is implemented by k-level binary tree decomposition method followed by 2k directional subbands where k is a positive integer. Combination of LP and DFB provides the double filter bank structure, which is known as CNT. When Contourlet is used for decomposing and embedding purposes, it gives high PSNR values.

V. CONCLUSION

This paper proposed an efficient information embedding algorithm based on the DE scheme in Contourlet domain. The proposed algorithm first converts the secret bits into a sequence of base-5 digits. After that, the cover image is transformed into the contourlet trasfrom domain and segmented into set of coefficient pairs. The dimanond encoding scheme is used thereafter to change at most one coefficient of each coefficient pair to embed one base-5 digit of the secret bits. Finally, the inverse contoulet is applied to obtain the stego-image. In contour let transform, Laplacian pyramid scheme generates down-sampled low pass version of original image and the difference between the original and the low pass image, resulting a band pass image. Then the obtained band pass image is further processed through directional filter bank (DFB). DFB contains the high frequency information like smooth contour and edge information of images. It is implemented by k-level binary tree decomposition method followed by 2k directional subbands where k is a positive integer. Combination of LP and

DFB provides the double filter bank structure, which is known as CNT. When Contour let is used for decomposing and embedding purposes, it gives high PSNR values and low mse values In future work, steganalysis can be carried out which is used for detecting messages hidden using steganography; this is analogous to cryptanalysis applied to cryptography. Different attacks can be applied to check the robustness of the proposed technique which can be evaluated from the extracted secret information when attacks are applied on the steago images.

REFERENCES

[1] S. K. Pal, P. K. Saxena and S. K. Muttoo, Smart steganographic applications, in Proceedings of the Pacific Rim Workshop on Digital Steganography, STEG'02, Japan, pp. 11–19, July 2002.

[2] S. K. Pal, Steganographic design issues, in Proceedings of the International Conference on Number Theory for Secure Communications, SASTRA, Thanjavur, India, December 2003.

[3] F. Petitcolas, R. J. Anderson and M. G. Kuhn, Attacks on copyright marking systems, in Proceedings of 2nd Workshop on Information Hiding, pp. 218-238, 1998.

[4] Cheddad, A., Condell, J., Curran, K. and McKevitt, P. Digital image steganography: survey and analysis of current methods. Signal Process., 2010, 90, 727–752.

[5] Ratnakirti Roy, Suvamoy Changder, "Image Steganography with Block Entropy based Segmentation and Variable Rate Embedding", published in: Business and Information Management (ICBIM), 2014 2nd International Conference on date of Conference: 9-11 Jan. 2014

[6] Hyunho Kang, Keiichi Iwamura, "Image Protection System with Steganography and Authentication", published in: Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014 Tenth International Conference on Date of Conference: 27-29 Aug. 2014

[7] Sabyasachi Kamila, Ratnakirti Roy, Suvamoy Changder, "A DWT based Steganography Scheme with Image Block Partitioning", published in: Signal Processing and Integrated Networks (SPIN), 2015 2nd International Conference on date of Conference: 19-20 Feb. 2015

[8] Hamad A. Al-Korbi, Ali Al-Ataby, Majid A. Al-Taee, Waleed Al-Nuaimy, "High-Capacity Image Steganography Based on Haar DWT for Hiding Miscellaneous Data", published in: Applied Electrical Engineering and Computing Technologies (AEECT), 2015 IEEE Jordan Conference on date of Conference: 3-5 Nov. 2015

[9] Swarnjeet Kaur, Navdeep Goel, "Segmentation and Block Based Image Steganography using Optimal Pixel Adjustment Process and Identical Approach", published in: Recent Advances in Engineering & Computational Sciences (RAECS), 2015 2nd International Conference on date of Conference: 21-22 Dec. 2015

[10] M. Tulasidasu, B.lakshmi sirisha, K. Rasool Reddy, "Steganography Based Secret Image Sharing Using Block Division Technique", published in: Computational Intelligence and Communication Networks (CICN), 2015 International Conference on date of Conference: 12-14 Dec. 2015

[11] ShuliangSun, "A novel edge based image steganography with 2kcorrection and Huffman encoding", published in Information Processing Letters 116(2016)93–99.

[12] MohammadReza Keyvanpoura, Farnoosh Merrikh Bayat, "Blind image watermarking method based on chaotic key and dynamic coefficient quantization in the DWT domain", published in Mathematical and Computer Modelling 58 (2013) 56–67.

[13] Della Babya, Jitha Thomasa, Gisny Augustinea, Elsa Georgea, Neenu Rosia Michaela, "A Novel DWT based Image Securing Method using Steganography", published in Procedia Computer Science 46 (2015) 612 – 618.

[14] Samer Atawneh; Ammar Almomani ; Hussein Al Bazar;Putra Sumari ; Brij Gupta "Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain." published in Multimed Tools Application,September 2017, Volume 76, Issue 18, pp 18451–18472