International Journal of Information Technology and Knowledge Management
December 2012, Volume 6, No. 1, pp. 23-25

COHERENT STEGNOGRAPHY USING SEGMENTATION AND DCT

Ramanjot Kaur[1] and Ramandeep Kaur Toor[2]

Abstract: Steganography is a means of establishing secret communication through public channel in an artistic manner. In this paper, we propose Bit Length Replacement Steganography Based on DCT Coefficients (BLSDCT). The cover image is segmented into 8*8 blocks and DCT is applied on each block. The numbers of payload MSB bits are embedded into DCT coefficients of the cover image based on the values of DCT coefficients. It is observed that the proposed algorithm has better PSNR, Security and capacity compared to the existing algorithm.

Keywords: Steganography, DCT Coefficients, Embedding algorithm.

1. INTRODUCTION

Steganography is used for covert communication. The secret image which is communicated to the destination is embedded into the cover image to derive the stego image. Steganography is the art of devising astute and undetectable methods of concealing the message themselves. It is therefore broader than cryptography. The origin of steganography is biological and physiological. Image Steganography includes several techniques of hiding the payload within the cover image. The most popular hiding techniques are Spatial Domain based Steganographic Techniques and Transform Domain based Steganographic Techniques. Spatial domain based steganography includes the Least Significant Bit (LSB) technique, and Bit Plane Complexity Steganographic (BPCS) technique. BPCS steganography hides secret data by means of block replacing. Each image plane is segmented into the same size pixel-blocks (a typical size of 8x8) which are classified into informative and noise like blocks. The noise like blocks is replaced by the secret blocks. In transform domain the cover image or the payload is transformed into frequency domain viz., Fast Fourier Transform, DCT, Discrete Wavelet Transform (DWT) and Integer Wavelet Transform. The DCT is used in common image compression format MPEG or JPEG, wherein, the LSBs of the DCT coefficients of the cover image are replaced by the MSBs of the payload. The Discrete Wavelet Transform [2] is used for hiding the secret message into the higher frequency coefficient of the wavelet transform while leaving the lower frequency coefficient sub band unaltered. The various ways of using transform domain techniques in steganography are (*i*) The cover image is transformed into frequency domain and LSBs of transformed domain are replaced by the spatial domain payload bit stream. (*ii*) The payload is converted into frequency domain and the coefficients are embedded into the spatial domain LSBs of cover image. (*iii*) Both the cover and payload are transformed into frequency domain for embedding process

[1,2] Department of CSE, Adesh Institute of Engg. and Tech. Faridkot, India
[1] *E-mail: kirandeep2226@gmail.com*

2. LIST OF COHERENT STEGNOGRAPHY METHODS

2.1 Clustering Methods

The K-means algorithm is an iterative technique that is used to partition an image into *K* clusters. The basic algorithm is:

1. Pick *K* cluster centers, either randomly or based on some heuristic
2. Assign each pixel in the image to the cluster that minimizes the distance between the pixel and the cluster center
3. Re-compute the cluster centers by averaging all of the pixels in the cluster
4. Repeat steps 2 and 3 until convergence is attained (*e.g.* no pixels change clusters)

2.2 Compression-based Methods

Compression based methods postulate that the optimal segmentation is the one that minimizes, over all possible segmentations, the coding length of the data. Each of these components is modeled by a probability distribution function and its coding length is computed as follows:

1. The boundary encoding leverages the fact that regions in natural images tend to have a smooth contour.
2. Texture is encoded by lossy compression in a way similar to minimum description length (MDL) principle, but here the length of the data given the model is approximated by the number of samples times the entropy of the model.

2.3 Histogram-based Methods

The histogram can also be applied on a per pixel basis where the information result are used to determine the most frequent color for the pixel location. Histogram-based methods are very efficient when compared to other image segmentation methods because they typically require only one pass through the pixels.

2.4 Edge Detection

Edge detection is a well-developed field on its own within image processing. Region boundaries and edges are closely related, since there is often a sharp adjustment in intensity at the region boundaries. Edge detection techniques have therefore been used as the base of another segmentation technique.

3. Present Work

The are steps used in the DCT dimensional are discussed below.

3.1 1D-Hierarchical Signal Segmentation

Witkin's seminal work in scale space included the notion that a one-dimensional signal could be unambiguously segmented into regions, with one scale parameter controlling the scale of segmentation. A key observation is that the zero-crossings of the second derivatives (minima and maxima of the first derivative or slope) of multi-scale-smoothed versions of a signal form a nesting tree, which defines hierarchical relations between segments at different scales.

3.2 2D-DCT Transform Each 8×8 Matrix into Frequency Domain Using 2D-DCT

Using DCT on 8*8 sub blocks has an advantage of less computation time for embedding as well as security to payload increases compared to applying DCT to whole cover image. A discrete cosine transform (DCT) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies

3.3 Embedding Algorithm

The embedding BSLDCT algorithm is given in Table 1, the payload is embedded into the cover image using segmentation, DCT and coherent length. The cover image is segmented into smaller blocks of size 8×8 matrices to increase the embedding capacity. The payload is embedded into the DCT coefficients of cover image based on coherent length L determined by the coefficient values to enhance the security to the secrete message

Table 1
Embedding Algorithm of BSLDCT

Inputs: Cover image

Output: Stego image

1. A cover image of any size and format is considered and is converted to gray scale.
2. Apply pixel management to the cover image, to avoid overflow and underflow
3. Segmentation of cover image into 8*8 blocks and are transformed into DCT domain.
4. The number of bits L of each DCT coefficient of cover image to be replaced by the payload MSB bits using coherent bit length
5. The stego image obtained in the DCT domain is converted into the spatial domain using IDCT.

Retrieving Al Algorithm:

The payload is retrieved from the stego image by the adaptive reverse procedure of embedding and is given in the table 2

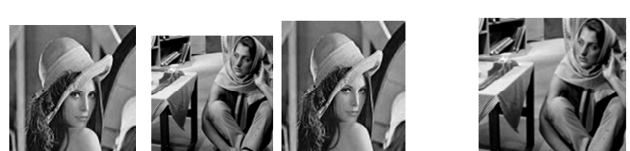
Input: Stego image

Output: Retrived Payload

1. The stego image is segmented into 8*8 blocks.
2. The 8*8 blocks are transformed into frequency domain using DCT.
3. The payload length *L* for each DCT coefficient is calculated similar to the procedure adapted in the embedding technique
4. Extract *L* bits from each DCT coefficients.
5. The payload is constructed using *L* number of bits.

4. PERFORMANCE ANALYSIS

For performance analysis, Cover Image (CI) and Payload (PL) of any size and formats are considered. The payload Barbara image is embedded into the cover Lena image to derive the stego image and the payload is retrieved from stego image using reverse embedding process at the destination is as shown in the Figure 1. The cover Baboon image is considered into which the payload Cameraman (CM) image is hidden to generate stego image. At the recipient end, the payload is extracted from the stego image is shown in the Figure.



(*a*) (*b*) (*c*) (*d*)

Figure 1: (*a*) CI: Lena (*b*) PL: Barbara (*c*) Stego Image (*d*) Retrieved PL

(*a*) (*b*) (*c*) (*d*)

Figure 2: (*a*) CI: Lena (*b*) PL: Barbara (*c*) Stego Image (*d*) Retrieved PL

The Maximum Hiding Capacity (MHC) in terms of bits and percentage as well as the PSNR between the cover image and stegoimage is tabulated for existing algorithm [4] Adaptive Steganography Based on Integer Wavelet Transform (ASIWT) and the proposed algorithm CSSDCT is given in the Table 3. It is observed that the PSNR is improved around 25% in the proposed algorithm compared to the existing algorithm for the same MHC.The corresponding PSNR for different embedding capacity values for two sets of images. In the first set Lena is used as cover image and Barbara as the payload and in the second set, Baboon is taken as the cover image and Cameraman as payload. The graph depicts that the quality of the stego image which is determined by PSNR not only depends on the algorithm but also on the images used. The Lena as cover image gives higher PSNR compared to the cover image Babbon.

Table 3
Capacity and PSNR of ASIWT and BSLDCT

Image	*Technique*	*MC(bits)*	*MC (%)*	*PSR(db)*
Lena	CSSDCT	986456	47	39.47
Barbara	ASIWT	986367	47	31.83
Baboon	CSSDCT	1007598	48	38.59
M	ASIWT	1005693	48	30.57

4. CONCLUSION

The steganography is used in the covert communication to transport secrete information. In this paper Bit Length Replacement Steganography using Segmentation and DCT is proposed. The cover image is segmented into smaller matrix of size 8x8 and converted to DCT domain. The MSB bits of payload in spatial domain are embedded into each DCT coefficients of cover image based on the coherent length L which is determined by the DCT coefficient values. The performance results in terms of PSNR for different kinds of images and dimensions are better in the proposed algorithm compared to the existing algorithm. In future the technique can be verified for robustness.

REFERENCES

[1] Raja K.B., C.R. Chowdary, Venugopal K.R., L.M. Patnaik. (2005). "A Secure Steganography using LSB, DCT and Compression Techniques on Raw Images", *IEEE International Conference on Intelligence Sensing and Information Processing*, pp. 171-176.

[2] Kumar V. and Kumar D. (2010). "Performance Evaluation of DWT Based Image Steganography", *IEEE International Conference on Advance Computing*, pp. 223-228.

[3] Weiqi Luo, Fangjun Huang, and Jiwu Huang (2010). "Edge Adaptive Image Steganography Based on LSB Matching Revisited", *IEEE Transactions on Information Forensics and Security*, **5(2)**, pp. 201-214.

[4] R.O. El Safy, H.H. Zayed and A. El Dessouki (2009). "An Adaptive Steganographic Technique Based on Integer Wavelet Transform", *International Conference on Networking and Media Convergence*, pp. 111-117.

[5] Mathkour H., Al-Sadoon B. and Touir A. (2008). "A New Image Steganography Technique", *International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1-4.

[6] V. Vijaylakshmi, G. Zayaraz and V. Nagaraj. (2009). "A Modulo Based LSB Steganography Method", *International Conference on Control, Automation, Communication and Energy Conservation*, pp. 1-4.

[7] Wien Hong, Tung-Shou Chen and Chih-Wei. (2008). "Lossless Steganography for AMBTC-Compressed Images", *Congress on Image and Signal Processing*, pp. 13-17.

[8] A.W. Naji, Teddy S. Gunawan, Shihab A. Hameed, B.B. Zaidan and A.A. Zaidan (2009). "Stego-Analysis Chain, Session One", *International Spring Conference on Computer Science and Information Technology*, pp. 405-409.

[9] M. Hassan Shirali-Shahreza and Mohammad Shirali-Shahreza (2008). "A New Synonym Text Steganography", *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 1524-1526.

[10] Vladimir Banoci, Gabriel Bugar and Dusan Levicky (2009). "Steganography Systems by using CDMA Techniques", *International Conference on Radioelectronika*, pp.183-186.