International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 1 January 2013

TRANSFORM DOMAIN BASED STEGANOGRAPHY USING SEGMENTATION AND WATERMARKING

Inderjeet Kaur, Deptt. of IT, M.M. Engg. College, M.M. University, Mullana (Ambala)

Rohini Sharma, Deptt. of IT, M.M. Engg. College, M.M. University, Mullana (Ambala)

Deepak Sharma, Deptt. of ECE, M.M. Engg. College, M.M. University, Mullana (Ambala)

Abstract **-** Secret communication and copyright protection are the two important issues of modern communication system. The research done so far shows a variety of techniques to communicate secretly. The technique proposed in this paper is a combination of steganography and watermarking which provides copyright protection to the information being transmitted secretly. The proposed technique is a transform domain based technique with the aid of segmentation and watermarking (TDSSW). It is observed that the proposed technique comes up with good PSNR (Peak Signal to Noise Ratio) and enhanced Security.

Keywords **-** Steganography, Cover Image, Payload, DCT, Segmentation, Watermarking.

I. INTRODUCTION

The major growth took place in the field of information technology has given birth to many issues related to data security. Today the application areas which revolve around data security are: confidentiality of business transactions, payments in private communication and password protection. Cryptography is one essential aspect for secure communications. Encryption makes the communication suspicious by scrambling the data. The third party can see the two parties communicating in secret and can definitely make some way to unscramble the code. The technique used to keep the contents of a message secret is called steganography. The goal of steganography is to keep the existence of a message secret. Steganography is concealed writing and is the technique of hiding secret data within a cover media such that it does not draw the attention of an unauthorized person [18]. The hidden secret information can be extracted by retrieving algorithm. Most of the digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Image steganography is a covert communication method that uses an image as the cover to hide the truth from potential attackers. In transform domain based steganography the image is first transformed and then the message is embedded in the image. In transform domain, 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 [18]. Internet has lead to sharing of information worldly. People can simply copy information and claim it's their, however problem of ownership is introduced. Thus there raise the need for the technique which can provide protection against detection and removal. Protection against removal can be provided using watermarking. Steganography and watermarking bring a variety of techniques to hide important information in an undetectable and/or irremovable way in audio and video data. A watermark is an invisible mark placed on an image that can be detected when the image is compared with the original. This mark is designed to identify both the source of an image as well as its intended recipient. The kind of information hidden in objects using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection. Watermark is prominently used for tracing copyright infringements and for banknote authentication. The similarity between steganography and watermarking is that both employ steganographic techniques to embed data covertly in noisy signals but the goal of steganography is imperceptibility to human senses and watermarking tries to control the robustness at top priority. Typically, the visible watermark could be text or a logo, which identifies the owner of the media. The visible watermark is commonly used by television broadcasters.

II. RELATED WORK

O'Ruanaidh et al. [1] proposed Fourier-Mellin transform-based invariants technique that can be used for digital image watermarking and designed to be unaffected by any combination of rotation, scale and translation transformations. Yeung. et al. [2] proposed a new method for invisibly watermarking high-quality color and gray-scale images. Cox et al. [3] examined the similarities and differences between watermarking and traditional communications. Vidyasagar M. Potdar et al. Bassia et al. [4] proposed the audio watermarking method that offers copyright protection to an audio signal by time domain processing. Wang.Y et al. [5]

discussed the features that a practical digital watermarking system for ownership verification requires. K.B.Raja et al. [6] presented an image based steganography that combines LSB, DCT, and compression techniques on raw images to enhance the security of the payload. Nan et al. [9] developed steganographic techniques for gray scale images and introduced schemes like high hiding capacity schemes and high stego-image degradation imperceptibility schemes. Suresh Babu et al. [8] proposed an authentication model of steganography to detect any attack on the stego image by modifying two AC coefficients of the DWT in each row of cover image based on a verification code. Hassan et al. [9] proposed a synonym text steganographic technique in which the words in American English are substituted by the words having different terms in British English and vice-versa. Abbas Cheddad et al. [10] enhanced steganography in digital images by proposing a color image steganography which performs better than S-Tools and F5. R O EI Safy et al. [12] proposed an adaptive steganographic technique in which the bits of the payload are hidden in the integer wavelet coefficients of the cover image adaptively along with optimum pixel adjustment algorithm. Naji et al. [13] analysed different steganographic techniques and weaknesses in the respective techniques and given an overview on hidden data in a different carrier. Vladimir Banoci et al. [14] presented Code Division Multiple Access Technique, where the embedding process is carried out by hiding secret image in each block of quantized DCT coefficients. Daniela Stanescu et al. [15] proposed a technique in which steganographic algorithm is implemented on embedded devices and also suggests on using microcontrollers or microprocessors. Kumar V. et al. [16] evaluated the performance of Discrete Wavelet Transform based image steganography and concluded by observing the effect of embedding the secret message in different bands such as CH, CV and CD. K.B Raja et al. [18] proposed coherent steganography using segmentation and DCT.

The motivation behind the research proposed in this paper is to provide the copyright protection to the information being transported secretly. The proposed technique has been evaluated using the parameters MSE, PSNR and MHC. Mean Square Error (MSE) is the measure of distortion in the image. Peak Signal to Noise Ratio (PSNR) is used as a quality measurement between two images. If PSNR ratio is high then images are best of quality.

Maximum Hiding Capacity (MHC) shows the number of bits per pixel which are replaced with the payload bits.

III. PROPOSED WORK

The problem statement consists of embedding the payload in the DCT coefficients of the cover image. The stego image obtained was to be made secure with the aid of watermarking. Proposed work consists of embedding technique, retrieval technique and algorithms.

A. Proposed TDSSW Embedding Technique

The payload is embedded into the cover image using segmentation, DCT and bit length. Visible watermark is added to the stego image. The Figure 1 shows the complete flowchart of proposed embedding technique. The gray scale cover image of any size and format can be used but the image with any size is resized to 256x256. The next step consists of limiting the pixel intensity values of the cover image to lower 15 and upper 240 instead of 0 and 255. The cover image is segmented into 8x8 matrices. The DCT is applied on each 8x8 block to get DCT coefficients which are used to hide the payload Most Significant Bit (MSB) based on the DCT coefficient values of the cover image. 2D-DCT is used to transform each 8x8 matrix into frequency domain. Applying 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 [18]. The length *L*, which determines the number of LSBs of each DCT coefficients (C0) of cover image that can be used to hide the payload MSB bits, is calculated according to the conditions given below:

If $Co \geq 2^5$; L=5

If $2^5 \leq Co \geq 2^4$; L=4

If $2^4 \leq Co \geq 2^3$; L=3

Else L=2

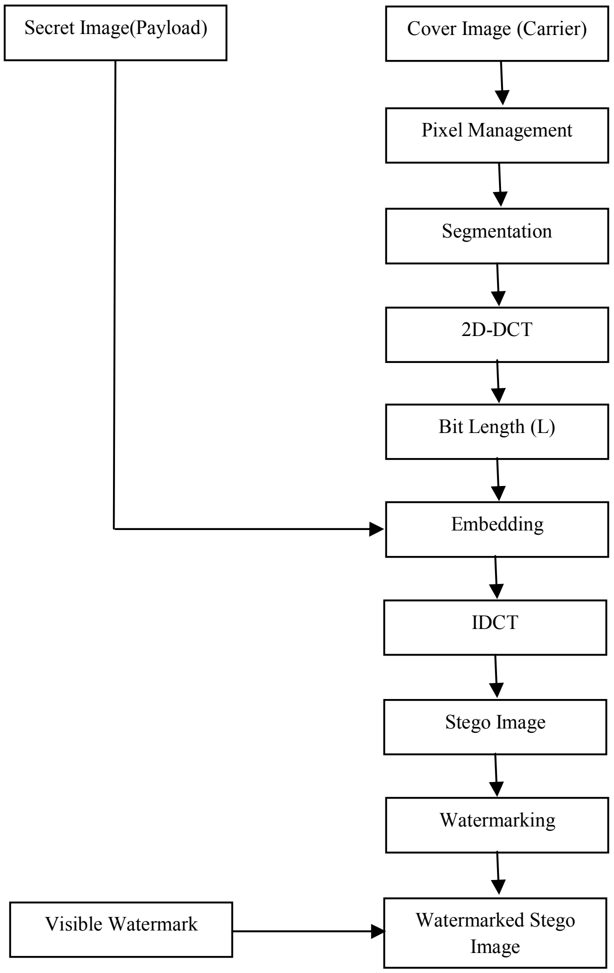


Figure- 1 Flowchart of Proposed Embedding Technique: TDSSW

Four MSBs of each payload pixel are embedded into the cover image DCT coefficients in a continuous manner depends on the value of *L* to derive the stego image in DCT domain. IDCT converts the stego image in the transform domain to the spatial domain. The stego image obtained in spatial domain is identical to the cover image and normal observations cannot detect the difference between the two. The visible watermark is added to the stego image. Watermark provides identity of the owner and protects the content from being manipulated and altered. This image is transmitted to the destination over the open channel.

B. Proposed TDSSW Retrieval Technique

Figure - 2 depicts the retrieval process. First of all visible watermark is extracted from watermarked stego image. The stego image is segmented into 8x8 blocks and two dimensional DCT is applied on each 8x8 sub blocks of stego image to transform it into frequency domain to generate DCT coefficients. At the receiver *L* is determined based on the DCT coefficient values similar to the conditions of embedding technique. Using this *L,* payloads bits are extracted from the stego image.

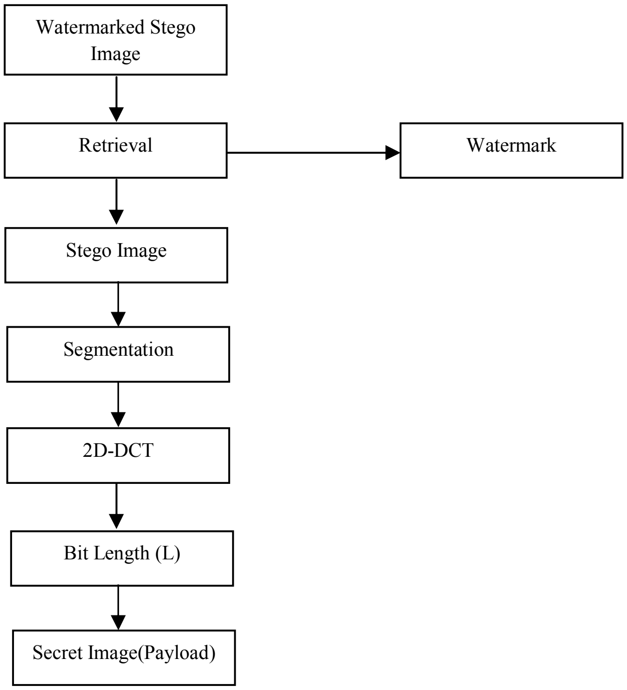


Figure- 2 Flowchart of Proposed Retrieval Technique: TDSSW

C. Algorithms

Proposed TDSSW Embedding Algorithm

Step 1. A gray scale cover image of any size and format is considered but the images with any size are resized to 256x256.

Step3. Applying pixel management to cover image to avoid underflow and overflow[18].

Step2. Segmentation of cover image into 8*8 blocks and are transformed into DCT domain[18].

Step3. Calculation of bit length(*L*)[18].

Step4. The number of bits *L* of each DCT coefficient of cover image to be replaced by the payload MSB bits using adaptive bit length[18].

Step5. The stego image obtained in the DCT domain is converted into the spatial domain using IDCT [18].

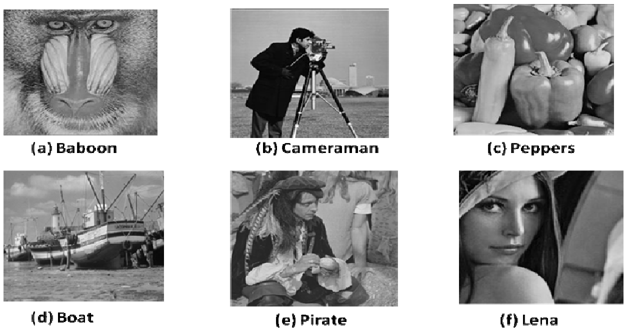
Step6. Visible Watermark is added to the stego image to get the watermarked stego image.

Proposed TDSSW Retrieval Algorithm

```
Step1.  Extraction of watermark from the watermarked stego image.
Step2.  Segmentation of stego image into 8*8 blocks and transform these blocks into frequency
        domain using DCT[18].
Step3. Calculation of payload length($L$)[18].
Step4. Extract $L$ bits from each DCT coefficients [18].
Step5. The payload is constructed using $L$ number of bits [18].
```

IV. PERFORMANCE ANALYSIS

For the performance analysis images of Baboon, Lena, Cameraman, Peppers, Pirate, Barbara and Boat are considered. The Mean Square Error (MSE), Maximum Hiding Capacity (MHC) and the Peak Signal to Noise Ratio(PSNR) of different stego images is shown in the table 1.



(a) Baboon (b) Cameraman (c) Peppers

(d) Boat (e) Pirate (f) Lena

Table 1 MHC, MSE and PSNR comparison

Cover Image(256x256)	Payload(256x256)	MHC in %	MSE	PSNR
Pepper	Cameraman	29.81	17.24	35.76
Lena	Pirate	30.44	15.55	36.21
Barbara	Boat	29.58	17.87	35.60

Pepper	Baboon	29.81	14.18	36.61
Barbara	Cameraman	29.58	20.94	34.91

The Peak Signal to Noise Ratio(PSNR) between different cover images & their stego images and PSNR between different cover images & watermarked stego images is shown in the table 2 and figure – 3 shows the graphic representation of the same.

Table 2 PSNR comparison between different Cover & Stego Images and Cover & Watermarked Stego Images

Cover Image (256x256)	**Payload (256x256)**	**PSNR between Cover & Stego Images**	**PSNR between Cover & Watermarked Stego Images**
Pepper	Cameraman	35.76	36.22
Lena	Pirate	36.21	36.25
Barbara	Boat	35.60	36.12
Pepper	Baboon	36.61	37.19
Barbara	Cameraman	34.91	35.35

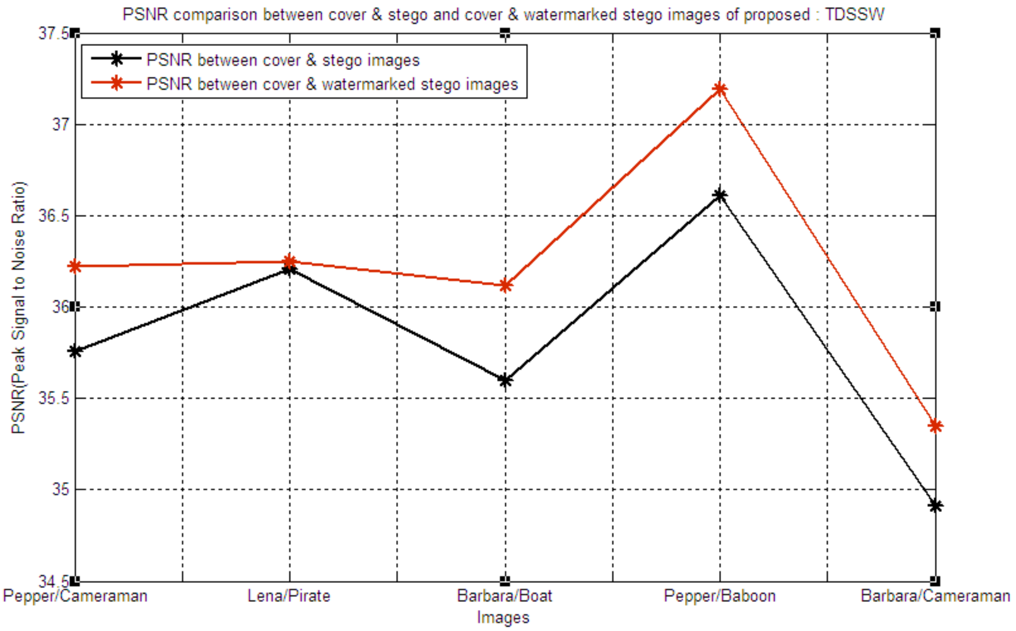


Figure – 3 The graphical comparison of PSNR between different cover & stego Images and cover & Watermarked stego Images

The PSNR between the cover image and stego image is tabulated for existing algorithm An Adaptive Steganographic Technique Based on Integer Wavelet Transform (ASIWT) [12] and the proposed algorithm TDSSW is given in the Table 3. It is observed that the PSNR is improved in the proposed algorithm compared to the existing algorithm.

Table 3 PSNR of existing and proposed techniques

Image	Existing Method(ASIWT)	Proposed Method(TDSSW)
	PSNR	PSNR
CI: Lena Payload: Barbara	31.80	36.00
CI: Baboon Payload: Cameraman	30.89	35.13

V. RESULT

The proposed technique (TDSSW) dealt with steganography and watermarking. The data hidden in the frequency domain generates little distortion noticeable to the human eye. The computation time to hide information in the DCT coefficients of 8x8 matrices is less and the information hidden is more secure. The figure 4 shows the complete procedure used for embedding and retrieval of secret image. Here the cover image baboon is used to hide the secret image (payload) cameraman. The visible watermark is added to the stego image.

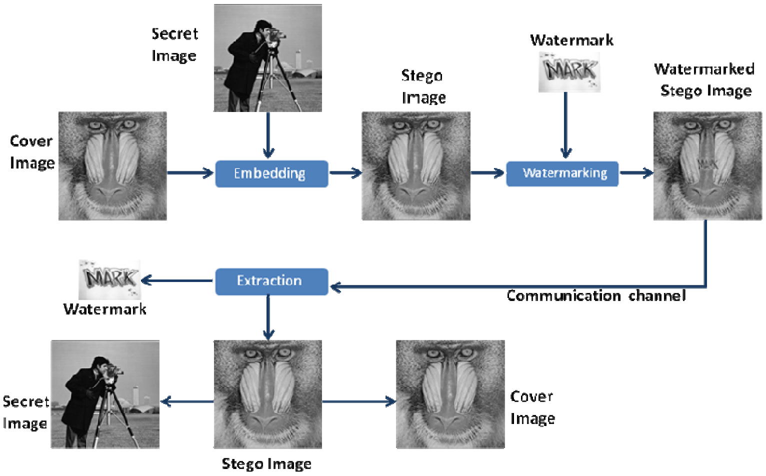


Figure – 4 Embedding and Retrieval of Secret image

Table 1 shows the different cover images with different payloads. The resultant stego images are having good PSNR (Peak Signal to Noise Ratio) and even shows satisfactory figures for MHC (Maximum Hiding Capacity). To hide the payload Cameraman, Pepper and Barbara are used as cover images. The PSNR for the two is different. Using Pepper as the cover image gives the better PSNR than Barbara. Same is true is the case of MSE (Mean Square Error). Pepper as the cover image gives lesser MSE than that of Barbara. So we can conclude that the quality of the stego image is not only determined by the algorithm but also by the cover image used. Table 2 shows that quality of stego images retain even after adding visible watermark i.e all the watermarked stego images stand with better PSNR than that of stego Images. The proposed technique TDSSW shows the better PSNR when it compared with existing technique ASIWT [12]. The visible watermark is used to identify the owner and protects the image from being copied and altered illegally.

VI. CONCLUSION AND FUTURE WORK

The objective of steganography is to communicate secretly using open channel. The technique proposed here is transform domain based with the aid of segmentation and watermarking. The carrier (cover image) is segmentated into 8*8 blocks and DCT is applied on each segment. The MSB of payload is embedded into DCT coefficients of the carrier (cover image) based on the values of DCT coefficients, to obtain the stego image. The following conclusions have been drawn from the work done:

1. The PSNR depends not only on the algorithm but also on the cover image used.
2. Integrity of the cover image retains even after adding the visible watermark.
3. Visible watermark identifies the intended owner and enhances the security.

The visible watermark is added to the stego image obtained to make it secured. The integrity of the data embedded in the stego image retains. It is observed that the proposed technique comes up with a good PSNR (Peak Signal to Noise Ratio) and enhanced security. Any intruder trying to interfere in between the transmission will only be able to see the image but would not be able to copy it or extract anything. In future the same technique can be extended by applying different transforms to both cover image as well as payload and thus the robustness of algorithm can be verified.

VII. REFERENCES

[1] O'Ruanaigh, J.J.K. Group de Vision par Ordinateur, Univ. de Geneve Pun, T. "Rotation, scale and translation invariant digital image watermarking" pp.536-539,vol-1,1997.

[2] Yeung, M.M., Mintzer, F. "An invisible watermarking technique for image verification" pp.680-683, vol.-2,1997.

[3] Cox, I.J, Miller, M.L., McKellips, A.L. "Watermarking as communication with side information" pp.1127-1141, vol-87, july 1999.

[4] Bassia, P. Pitas, I., Nikolaidis, N. "Robust audio watermarking in the time domain" pp.232-241, vol.-3, june 2001.

[5] Wang, Y., Doherty, J.F., Van Dyck, R.E. "A wavelet based watermarking algorithm for ownership verification of digital images" pp.66-78, Vol.-11, Feb 2002.

[6] Raja K B, C R Chowdary, Venugopal K R, L M Patnaik, “A Secure Steganography using LSB,DCT and Compression Techniques of Row Images” IEEE International Conference on Intelligence Sensing and Information Processing, Dec 2005.

[7] Nan-I Wu and Min-Shiang Hwang, “Data Hiding:Current Status and Key Issues”, International Journal of Network Security, January 2007.

[8] Suresh Babu K, Raja K B, Kiran K, Manjula Devi T H, Venugopal K R and Patnaik L M, “Authentication of Secret Information in Image Steganography” IEEE Conference on TENCON, November 2008.

[9] M Hassan Shirali-Shahreza and Mohammad Shirali-Shahreza, “A New Synonym Text Steganography”, International Conference on intelligent Information Hiding and Multimedia Signal Processing, August 2008.

[10] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, “Enhancing Steganography in Digital Images”, Canadian Conference on Computer and Robot Vision, May 2008.

[11] Mci-Chang Chen, Sos S Agaian and C L Philip Chen, “Generalized Collage Steganography on Images”, International Conference on Systems, Man and Cybernetics, October 2008.

[12] R O EI Safy, H H Zayed and A EI Dessouki, “An Adaptive Steganographic Technique Based on Integer Wavelet Transform”, International Conference on Networking and Media Convergence, March 2009.

[13] A W Naji, Teddy S Gunawan, Shihab A Hameed, B B Zaidan and A A Zaidan, “Stego-Analysis Chain, Session One”, International Spring Conference on Computer Science and Information Technology, April 2009.

[14] Vladimir Banoci, Gabriel Bugar and Dusan Levicky, “Steganography Systems by using CMA Techniques”, International Conference on Radioelectronika, April 2009.

[15] Daniela Stanescu, Valentin Stangaciu, Loana Ghergulescu and Mircea Stratulat , “Straganography on Embedded Devices”, International Symposium on Applied Computational Intelligence and Infromatics, April 2009.

[16] Kumar V and Kumar D, “Performance Evaluation of DWT Based Image Steganography”, IEEE International Conference on Advance Computing, February 2010.

[17] Weiqi Luo, Fangjun Huang and Jiwu Huang, “Edge Adaptive Image Steganography Based on LSB Matching Revisited”, IEEE Transactions on Information Forensics and Security, June 2010.

[18] K B Raja, R.K.Chhotary, K.B.Shiva Kumar,”Coherent Steganography using Segmentation and DCT”, IEEE 2010.

[19] Rosanne English “Comparison of High Capacity Steganography Techniques”, International Conference IEEE, 2010.

[20] Moreland, T., “Steganography and Steganalysis”, Leiden Institute of Advanced Computing Science, www.liacs.nl/home/tmoerl/privtech.pdf.

[21] “Reference guide: Graphics Technical Options and Decisions”, http://www.devx.com/projectcool/Article/19997.