IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

A Novel Digital Color Image Steganography using Discrete Wavelet Transform *(Digital Color Image Steganography using DWT)*

A. Goel[1*] , V. Deswal[2] , S. Chhabra[3]

[1]Department of BBA, Gateway School of Business, Sonipat, India.
[2] Department of BBA, Panipat Institute of Engineering & Technology, Samalkha, India.
[3] Department of Computer Science Engineering, Panipat Institute of Engineering & Technology, Samalkha, India.

[*]*Corresponding Author: ajay1989goel@gmail.com, Tel.: 9592617061*

DOI: https://doi.org/10.26438/ijcse/v7i3.266270 | Available online at: www.ijcseonline.org

Accepted: 18/Mar/2019, Published: 31/Mar/2019

Abstract— A novel color image steganography scheme based on discrete wavelet transforms (DWT) is proposed for better security. The proposed approach extracts R, G, and B planes from the color cover image. The DWT is applied on both secret image and RGB components of the cover image. The blocking process is applied to approximation coefficients of secret image and detail coefficients of RGB components of the cover image. The block of detail coefficients is replaced with approximation coefficient of secret image using root mean square error method. The key is used to store the position of best matching blocks. The proposed approach is compared with recently developed steganography technique. The experimental results reveal that the proposed approach improves the performance of steganography technique in terms of Peak Signal to Noise Ratio value. The stegano image has good visual quality also.

Keywords: Color image steganography, Discrete wavelet transforms, PSNR.

I. INTRODUCTION

In recent years, the development of internet and multimedia processing technologies have made digital data more easily distributed and than ever at low cost. The data can be well edited with almost trifling loss using multimedia processing techniques. Therefore, the need for copyright protection of data has issued. Steganography is a technique which becomes the main focus of research for copyright protection.

There are mainly two approaches related to steganography technique, i.e., Spatial-domain approach and Frequency-domain approach [9]. The spatial based steganography technique embed the secret data into least significant pixels (LSB) of cover data. This approach is very fast, but it is sensitive towards image processing attacks. The frequency based steganography technique transforms the cover data into frequency domain coefficients and then embed the secret message in it. The transformation can be done either Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) or both. These transformation methods are harder and slower than spatial domain approach. However, these methods provide more security and noise tolerant [3]. Among these methods, DWT have multi-resolution characteristics. Hence, It has been widely used in digital image steganography.

This fact motivated us to develop a novel image steganography technique based on DWT. The proposed approach uses the blocking concept to provide robustness against image processing attacks. The proposed approach provides better security due to DWT technique. The proposed approach applied on five color cover and two gray scale secret images.

The remaining structure of the paper is as follows. Section II presents the Literature Survey work which has been done in Steganography. Section III presents the proposed DWT based digital Steganography approach. Section IV shows the results and experimentation. Section V presents conclusions.

II. RELATED WORK

Kumar and Kumar proposed a steganography technique based on the combination of DCT and DWT [1]. They applied DCT on secret image for finding DCT coefficients. Thereafter, they applied DWT on the cover image and DCT coefficients image for finding the image features. The extracted image features of secret image are embedded into cover image. The main drawback of this technique is to hide the image features only in one portion of cover image. Tsuang-Yuan et al. [2] proposed a new technique for data hiding by a change tracking technique. Chan and Chang proposed a Least Significant Bit Substitution (LSB) steganography technique [4]. They replaced the LSB bit of

cover image with the secret image. The drawback of this technique has much smaller PSNR value and extracted secret image visual is not good. Sinha and Singh [5] proposed a technique based on encryption and decryption of an image. They encrypted an image using digital signature of image for secured transmission.

Fatiha et al. [6] proposed a method for digital audio steganography which emerged a prominent source of hiding across novel telecommunication technologies. Baisa and Suresh [7] proposed a technique which is based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). They applied DWT on cover image, then they applied SVD on decomposed image. This technique has high PSNR value. Ali et al. [8] proposed a blind image watermarking technique based on DWT and DCT. They used two DCT transformed sub-vectors to embed the bits of watermark sequence in a differential manner. McKeon [9] proposed a technique for steganography based on Fourier domain of an image with the help of zero-padding properties. These zeros can be changed a bit where change in image is not obtrusive. Kumar and Kumar [10] designed a new color image steganography technique using DWT. They divide the cover image based on RGB method. They hide the secret image into RGB of the cover image.

Wioletta and Marek [11] worked on steganography and watermarking technology include biometric recognition method. They used the combination of DFT, DCT, and DWT on the cover image and secret image then to get watermarked image. The performance is evaluated using Neural Network technique. Ghebleh and Kanso [12] proposed a technique chaotic algorithm based on a 3-dimensional chaotic cat map and DWT. They embedded the cat map of a secret image into cover image. Neha and Nidhi [13] designed a new technique in which they hide the secret data into an audio file using LSB and DWT. They applied DWT on audio file by taking higher frequency component as data. They hide the secret data into these components. Rashedul et al. [14] proposed a method based on LSB and AES cryptography technique for better security in steganography. They used filtering based technique which used MSB bits for filtering. AES cryptography changed the secret message into cipher text to ensure two layer security of the message. This method applied to hide the large data in a single image. Jero et al. [15] proposed a ECG steganography technique based on DWT and SVD. In this technique, they applied a 2D ECG image and embedded secret data in one sub-band. They replaced the singular values of the decomposed cover image by the singular values of secret data.

Kanan and Nazeri [16] designed a tunable visual image quality and data lossless method in spatial domain. This technique is based on a genetic algorithm. The steganography is modeled as a search problem in which the purpose is to find the best direction and best starting point in the cover image of hiding secret data. In order to search this space, a genetic algorithm is utilized. Suk-Hwan [17] proposed a DNA watermarking technique for copyright protection and ownership authentication of DNA sequences. In this method, a coding DNA sequence is divided into a number of subsequences and allocated all codons to subsequences to a numerical code using histogram rank of the amino acids. Thereafter, he found an optimal subsequence among them with DWT coefficients.

Duanhao and Wei proposed a method for image steganography based on the absolute moment block truncation coding (AMBTC) [18]. In this scheme, a threshold was predefined to classify the blocks of AMBTC compressed codes as smooth or complex blocks, in which data can be embedded. The two quantization level in smooth block is re-calculated to minimize the distortion in the image.

Jeng-Shyang et al. [19] proposed a technique which combined compressive sensing with subsampling. The cover image tends to be compressed in transform domain. The characteristics of compressive sensing, dimensional reduction, and random projection were utilized to insert secret message into the compressive sensing transform domain of the sparse image. Bit correction rate between original secret image and extracted message was used to compute accuracy. Asna et al. [20] presented a method for digital image watermarking based on DWT-SVD domain. They decomposed the cover image into sub-bands using 2-D DWT. Thereafter, they applied SVD on each band after modifying their singular values.

III. PROPOSED TECHNIQUE

In this paper, the novel steganography approach based on Discrete Wavelet Transform (DWT) is proposed. The proposed steganography technique consists of embedding and extraction procedure. The detail of these procedures is as follows.

A. Embedding Procedure

1) Read Cover image (C) and Secret image (S). Decompose the C into three planes R, G, and B.

$$C \rightarrow \{R_C, G_C, B_C\}$$

2) Apply DWT on RGB components of C and secret image S.

$$DWT(R_C) \rightarrow \{R_{CA}, R_{CH}, R_{CV}, R_{CD}\}$$

$$DWT(G_C) \rightarrow \{G_{CA}, G_{CH}, G_{CV}, G_{CD}\}$$

$$DWT(B_C) \rightarrow \{B_{CA}, B_{CH}, B_{CV}, B_{CD}\}$$

$$DWT(S) \rightarrow \{S_A, S_H, S_V, S_D\}$$

3) Apply blocking process on approximation coefficients of R, G and B planes of C and approximation coefficient of S. The approximation coefficients are decomposed into blocks of 4×4 *pixels.*

$$S_A \rightarrow \left\{ BS_{A_i}, 1 \le i \le BS_{A_N} \right\}$$

$$R_{CA} \rightarrow \left\{ BR_{CA_i}, 1 \le i \le BR_{CA_N} \right\}$$

$$G_{CA} \rightarrow \left\{ BG_{CA_i}, 1 \le j \le BG_{CA_N} \right\}$$

$$B_{CA} \rightarrow \left\{ BB_{CA_i}, 1 \le k \le BB_{CA_N} \right\}$$

4) Apply blocking process on detail coefficients of R plane of C. All of these coefficients are decomposed into blocks of 4×4 *pixels.*

$$R_{CH} \rightarrow \left\{ BR_{CH_i}, 1 \le i \le BR_{CH_N} \right\}$$

$$R_{CV} \rightarrow \left\{ BR_{CV_i}, 1 \le i \le BR_{CV_N} \right\}$$

$$R_{CD} \rightarrow \left\{ BR_{CD_i}, 1 \le i \le BR_{CD_N} \right\}$$

5) Apply blocking process on detail coefficients of G plane of C. All of these coefficients are decomposed into blocks of 4×4 *pixels.*

$$G_{CH} \rightarrow \left\{ BG_{CH_i}, 1 \le i \le BG_{CH_N} \right\}$$

$$G_{CV} \rightarrow \left\{ BG_{CV_i}, 1 \le i \le BG_{CV_N} \right\}$$

$$G_{CD} \rightarrow \left\{ BG_{CD_i}, 1 \le i \le BG_{CD_N} \right\}$$

6) Apply blocking process on detail coefficients of B plane of C. All of these coefficients are decomposed into blocks of 4×4 *pixels.*

$$B_{CH} \rightarrow \left\{ BB_{CH_i}, 1 \le i \le BB_{CH_N} \right\}$$

$$B_{CV} \rightarrow \left\{ BB_{CV_i}, 1 \le i \le BB_{CV_N} \right\}$$

$$B_{CD} \rightarrow \left\{ BB_{CD_i}, 1 \le i \le BB_{CD_N} \right\}$$

7) For each block of Secret image $\left(BS_{A_i} \right)$ *is matched with block detail coefficients of R, G and B planes of C. The matching is done with root mean square error. The position of minimum error blocks of R, G and B planes are stored. The position of best matched blocks are stored in Key K1.*

8) Replace the best matched detailed coefficients of R, G, and B planes of C with approximation coefficients of Secret image.

9) Apply IDWT on modified detailed coefficients of R, G, and B planes of C. The Stegano-image (ST) is produced.

B. Extraction Procedure

1) Decompose the Stegano image (ST) into three planes; R, G, and B.

2) Apply DWT on R, G, and B planes of ST.

3) The position of embedded blocks of secret image is found using the Key K1. These embedded blocks are the approxiation coefficients of S.

4) Apply IDWT on extracted approximation blocks and detailed coefficients of S. This will produce extracted secret image from stegano-image.

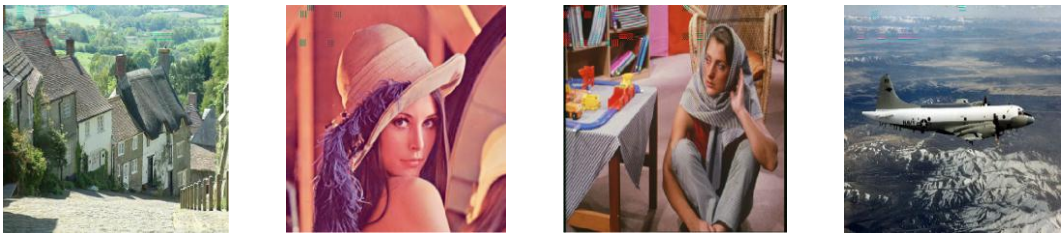
IV. RESULTS AND EXPERIMENTATION

The performance of proposed approach is evaluated using four color cover images and two grey scale secret images. The color images are *Goldhill*, *Lena*, *Barbara* and *Plane*. The secret images are *Cameraman* and *Baboon*. The size of these images is 256×256. All the cover and secret images are shown in Figure 1. Figure 2 shows the stegano image after embedding *Cameraman* image into above-mentioned cover images. Figure 3 shows the stegano image after embedding *Baboon* image into above-mentioned cover images.

To validate the proposed approach, it is compared with well-known technique developed technique by Kumar et al. [10]. *PSNR* is used to measure the quality of an image. Tables I and II depict the *PSNR* values of stegano-images after embedding *Cameraman* and *Baboon* as a secret image respectively. The experimental results reveal that the *PSNR* value of proposed approach is better than Kumar's approach. It has also been found that the security of secret image is much better than Kumar's approach. The proposed approach provides better quality of stegano-image. Tables III and IV show the *PSNR* values of extracted *Cameraman* and *Baboon* secret images respectively. The results depict that the extract secret is better visual quality and *PSNR* value.

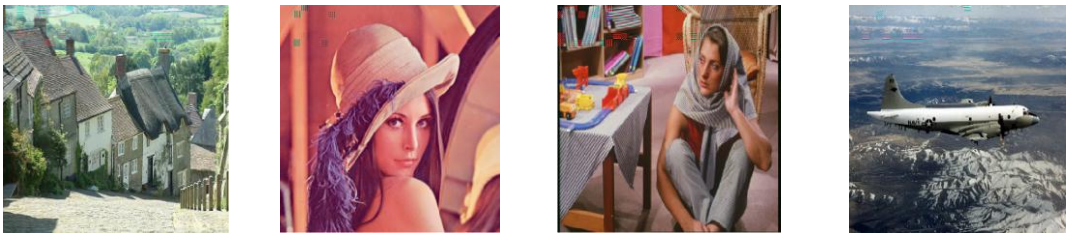
(a) (b) (c) (d) (e) (f)

Fig. 1. Original cover images (a) Goldhill (b) Lena (c) Barbara (d) Plane; Secret Images (e) Cameraman (f) Baboon



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

Fig. 2. Stegano images after embedding the *Cameraman* image: (a) Goldhill (b) Lena (c) Barbara (d) Plane



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

Fig. 3. Stegano images after embedding *Baboon* image: (a) Goldhill (b) Lena (c) Barbara (d) Plane

TABLE I. PSNR VALUES OF STEGANO IMAGE USING CAMERAMAN AS A SECRET IMAGE

Cover Images	Kumar Approach	Proposed Approach
Goldhill	26.8002	28.2911
Lena	32.9989	33.2558
Barbara	23.6012	25.9011
Plane	30.8876	32.6326

TABLE II. PSNR VALUES OF STEGANO IMAGE USING BABOON AS A SECRET IMAGE

Cover Images	Kumar Approach	Proposed Approach
Goldhill	27.0009	29.8260
Lena	34.6189	34.9175
Barbara	26.8685	27.7151
Plane	32.2478	33.8283

TABLE III. PSNR VALUES OF EXTRACTED CAMERAMAN

Cover Images	Kumar Approach	Proposed Approach
Goldhill	10.5545	12.0564
Lena	10.2479	10.7692
Barbara	10.9692	12.5284
Plane	10.4774	10.5619

TABLE IV. PSNR VALUES OF EXTRACTED BABOON

Cover Images	Kumar Approach	Proposed Approach
Goldhill	10.7568	13.7351
Lena	10.4920	12.4739
Barbara	10.7267	10.7329
Plane	11.3466	12.8437

V. CONCLUSIONS

A novel DWT-based color image steganography approach has been proposed. The proposed approach uses blocking and secret key computation concepts. The blocking concept uses the least variation concept. Secret key uses the concept of detail coefficient of DWT and least error matching criteria. The experimental results indicate that the proposed approach provides better stegano and secret images in terms of *PSNR*. The newly developed approach helps us to provide better visual quality. Moreover, this approach does not require the original cover image to extract secret image.

REFERENCES

[1] V. Kumar, and D. Kumar, "Digital image steganography based on combination of DCT and DWT" (Ed. V. V. Das and R. Vijaykumar), Information and Communication Technologies, Kochi, Kerala, 2010

[2] T.Y. Liu and W. H. Tsai, "A New Steganography method for data hiding in Microsoft Word documents by a Change Tracking Technique", IEEE Transaction on information Forensics and Security 2(1), 2007 , 24–30 .

[3] A. A. Abdelwahab and L. Hasna, "A Discrete Wavelet Transform based Technique for Image Data Hiding", In: National Radio Conference, Egypt, 2008, pp.1–9.

[4] C.K. Chan and L.M. Cheng, "Hiding data in image by simple LSB substitution", Pattern Recognition 37, 2003, 469– 471.

[5] A. Sinha and K. Singh, "A technique for image encryption using digital signature", Optics Communications 218(4), 2003, 229–234.

[6] D. Fatiha, A. Beghdad, M. K. Abed and H. Habib, "Comparative Study of Digital audio Steganography Technique", EURASIP on Audio, Speech and Music Processing 2012, 2012:25.

[7] L.G. Baisa and N.M. Suresh, "MEO based secured, robust, high capacity and perceptual quality image watermarking in DWT-SVD domain", SpringerPlus 4:126, 2015, DOI 10.1186/s40064-015-0904-z.

[8] B. Ali, B. Khier and B. Noureddine, "Blind Image Watermarking Technique Based on Differential Enbedding in DWT and DCT domains", Benoraira et. al. EURASIP on Advances in Signal Processing 2015:55, 2015, DOI 10.1186/s13634-015- 0239-5.

[9] R.T. McKeon, "Steganography Using the Fourier Transform and Zero-Padding Aliasing properties", IEEE International Conference on Electro/

Information Technology, 2006, pp. 492–497.

[10] Dinesh Kumar and Vijay Kumar, "Improving the Performance of Color Image Watermarking Using Contourlet Transform", *Advances in Computer Science and Information Technology*, LNCS-CCIS, vol 131. Springer-Verlag, Berlin, 2011, pp.256-264.

[11] W. Wioletta andE.O. Marek, "Biometric watermarks based on face recognition methods for authentication of digital images", Wiley online library, 2014, DOI : 10. 1002/sec. 1114.

[12] M. Ghebleh and A. Kanso, "A robust chaotic algorithm for digital image steganography", Commun Nonlinear Sci Numer Simult 19, 2014, 1898-1907.

[13] G. Neha and S. Nidhi, "DWT and LSB based Audio Steganography", International Conference on Reliability, Optimization and Information Technology – ICROIT, 2014.

[14] I. Rashedul, S. Ayasha, U. Palash, K.M. Ashis and H. Delowar, "An Efficient Filtering based approach improving LSB image steganography using status bit along with AES cryptography", International Conference on Informatics, Electronics and Vision 2014.

[15] S.E. Jero, R. Palaniappan and S. Ramakrishnan, "Discrete Wavelet Transform and Singular Value Decomposition based ECG steganography for secured patient information transmission", J Med Syst, vol. 38, pp. 2014

[16] H.R. Kanan and B. Nazeri, "A novel image steganography scheme with high embedding capacity and tunable visual Image quality based on a genetic algorithm," Expert Systems with Applications, 2014

[17] L.S. Hwan, "DWT based coding DNA watermarking for DNA copyright protection", Information Sciences, 273, 2014, 263-286.

[18] O. Duanhao and S.Wei, "High payload image steganography with minimum distortion based on absolute moment block truncation coding", Multimed Tools Appl,

[19] P. J. Shyang, L. Wei, Y. C. Sheng and Y.L. Jun, "Image steganography based on subsampling and compressive sensing", Multimed Tools Appl.

[20] F. Asna and K. Munish, "Study and Analysis of Robust DWT-SVD Domain Based Digital Image Watermarking Technique using MATLAB", IEEE International Conference on Computational Intelligence and Communication Technology, 2015

