International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 3, Number 1 (2013), pp. 13-24

http://www. irphouse.com

An Integer Wavelet Transform Based Steganography Technique for Color Images

Hemalatha S.[1], U Dinesh Acharya[2], Renuka A.[3] and Priya R. Kamath[4]

[1]Dept. of CSE, MIT, Manipal, Manipal, India.
E-mail: hema.shama@manipal.edu
[2]Dept. of CSE, MIT, Manipal, MIT, Manipal, Manipal, India.
E-mail: dinesh.acharya@manipal.edu
[3]Dept. of CSE, MIT, Manipal, Manipal, India.
E-mail: renuka.prabhu@manipal.edu
[4]Dept. of CSE, Dept. of CSE, MIT, Manipal, Manipal, India.
E-mail: priyarkamath@gmail.com

Abstract

This paper proposes a secure color image steganography technique to hide a secret image using the keys, when both the cover image and the secret image are color images. The secret image is hidden by considering the three color components separately. The secret image itself is not hidden, instead the keys are generated using the corresponding color components and the keys are hidden in the respective color components of the cover image. Using the keys the secret image can be extracted. Integer Wavelet Transform (IWT) is used to hide the keys. Experimental results show better Peak Signal to Noise Ratio (PSNR), which is a measure of security compared to other existing color image steganography techniques. In this technique the secret information is hidden in the middle bit-planes of the integer wavelet coefficients in high frequency sub-bands.

Keywords: Steganography, IWT, DWT, PSNR, lifting scheme, RGB.

Introduction

Advancement in digital communication and networking has posed serious threats to secure data transmission. This has driven significant rise in interest among the information security researchers in the field of information hiding. The early approach to secure communications was via data encryption termed as Cryptography.

Cryptography makes the information unintelligible. Steganography is another method used for secret communication. It is the science and art of covert communication. Steganography attempts to hide the existence of the information. Research in steganography has mainly been driven by a lack of strength in cryptographic systems. Steganography gives more freedom to communicate and send secret information without leaving any evidence that opponent will intercept and try decoding the information. The object used to conceal the secret information is called as cover object. The cover can be a text, an image, an audio or video [1]. In this paper an image steganography technique is proposed. The color image is taken as cover and secret information is also considered as color image.

Generally the secret information can be hidden directly by modifying the intensity value or pixel value of an image or its frequency components. The former is called spatial domain technique and the later is called frequency domain or transform domain technique. The advantage of spatial domain techniques is simplicity. The disadvantage is low ability to bear signal processing operations such as filtering, compression, noise insertion, cropping etc. Least Significant Bit Insertion methods and their variants, Pallet based methods come under this category.

In transform domain methods, the first step is to transform the cover image into different domain. Then the transformed coefficients are processed to hide the secret information. These changed coefficients are transformed back into spatial domain to get stego image. The advantage of transform domain methods is the high ability to face signal processing operations. However, methods of this type are computationally complex. Steganography methods using Discrete Cosine Transforms (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transforms (DFT) come under this category [2]. In this paper DWT and Integer Wavelet Transform (IWT) are used.

Discrete Wavelet Transform in Images

Discrete Wavelet Transform (DWT) transforms discrete signal from time domain into time frequency domain. The result of transformation is a set of coefficients organized in the way that enables not only spectrum analysis of the signal but also spectral behavior of the signal in time.

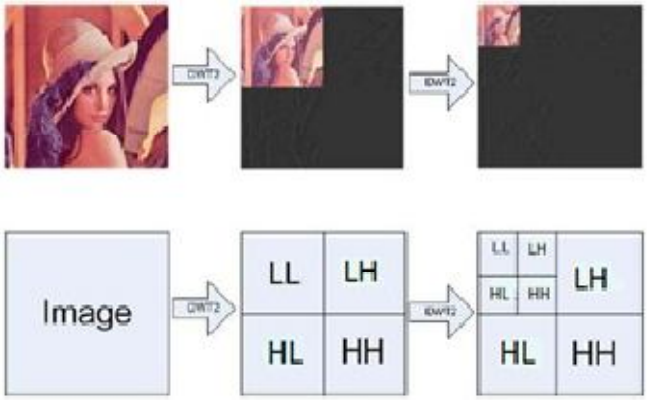

Figure 1: A 2D DWT for images.

The wavelet transform has emerged as a cutting edge technology, within the field of image compression. Wavelet-based coding provides substantial improvements in picture quality at higher compression ratios. Figure 1 shows the 2D DWT for image at various levels [3]:

DWT decomposes the image into four sub-bands LL, LH, HL and HH. The LL sub-band contains all significant features of the image. They are the low frequency components. It is possible to reconstruct the original image by considering only LL sub-band. LH, HL and HH contain high frequency components and contain only the edge details of the image. When DWT is applied again to the LL sub-band of the first level decomposition, it is called as second level decomposition. With multiple levels of decompositions some of the features of the original image may be lost.

Integer Wavelet Transform

Since the discrete wavelet transform allows independent processing of the resulting components without significant perceptible interaction between them, hence it is expected to make the process of imperceptible embedding more effective. However, the used wavelet filters have floating point coefficients. Thus, when the input data consist of sequences of integers (as in the case for images), the resulting filtered outputs no longer consist of integers, which doesn't allow perfect reconstruction of the original image. However, with the introduction of Wavelet transforms that map integers to integers the output can be completely characterized with integers. The LL subband in the case of IWT appears to be a close copy with smaller scale of the original image while in the case of DWT the resulting LL subband is distorted as shown in Figure 2 [4].

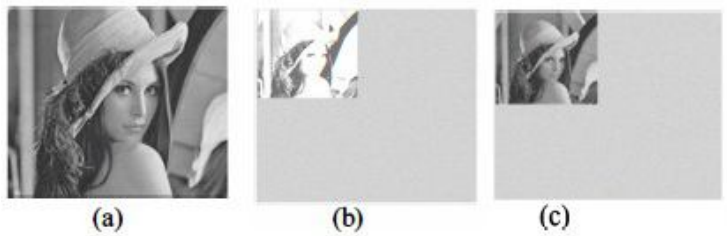

Figure 2: (a) Original image Lena. (b) One level 2D DWT in subband LL (c) One level 2D IWT in subband LL.

If the original image (I) is X pixels high and Y pixels wide, the level of each of the pixel at (i,j) is denoted by Ii,j. Lifting
Scheme is one of the techniques on IWT. The decomposing filter in IWT can be calculated as [5]

$$LL_{i,j} = \lfloor (I_{2i,\,2j} + I_{2i+1,\,2j}) / 2 \rfloor \quad (1)$$

$$HL_{i,j} = I_{2i+1,\,2j} - I_{2i,\,2j} \quad (2)$$

$$LH_{i,j} = I_{2i,\,2j+1} - I_{2i,\,2j} \quad (3)$$

$$HH_{i,j}=I_{2i+1,\,2j+1}-I_{2i,\,2j} \quad (4)$$

The inverse transform is given by

$$I_{2i,\,2j}=LL_{i,j}-\lfloor HL_{i,j}/2 \rfloor \quad (5)$$

$$I_{2i,\,2j+1}=LL_{i,j}+\lfloor (HL_{i,j+1})/2 \rfloor \quad (6)$$

$$I_{2i+1,\,2j}=I_{2i,\,2j+1}+LH_{i,j}-HL_{i,j} \quad (7)$$

$$I_{2i+1,\,2j+1}=I_{2i+1,2j}+HH_{i,j}-LH_{i,j} \quad (8)$$

where, $1 \le i \le X/2$, $1 \le j \le Y/2$ and $\lfloor\ \rfloor$ denotes floor value.

Related Work

Abdelwahab and Hassaan [6] proposed a data hiding technique in the DWT domain which decomposed both secret and cover images with 1-level DWT. The disadvantage of this method is that the extracted data is not completely as same as the embedded original version. This is improved by Neda Raftari and Amir Masoud Eftekhari Moghadam [7] who propose a new image steganography technique based on IWT and Munkres' assignment algorithm which embeds secret image in frequency domain of cover image with high matching quality. The improvement is obtained with higher computation. Here both cover and secret images are grey scale images.

El Safy, R.O, Zayed. H. H, EI Dessouki. A [8], used an adaptive steganographic technique based on IWT, which improves the hiding capacity and PSNR compared to DWT technique proposed by B. Lai and L. Chang [9]. The hiding capacity and PSNR are further improved by Elham Ghasemi, Jamshid Shanbehzadeh and Bahram ZahirAzami [4], who use a steganographic method based on IWT and Genetic Algorithm. Silvia Torres-Maya, Mariko Nakano-Miyatake and Hector Perez-Meana propose an image steganography system based on Bit Plane Complexity Segmentation (BPCS) and IWT [10], in which the data is hidden in bit planes of subband wavelet coefficients obtained by using the IWT. To increase data hiding capacity the replaceable IWT coefficient are defined by a complexity measure using BPCS.

Guorong Xuan et al [11], propose a watermarking technique using IWT in which the watermark is embedded in the middle bit planes of the IWT coefficients in the middle and high frequency subbands. In all these papers message bits are hidden in grey scale image. In the following paragraph some of the papers in color image steganography field are reviewed.

Masud, Karim S.M., Rahman, M.S., Hossain, M.I. [12], proposed a new approach based on LSB using secret key.

The secret key encrypts the hidden information and then it is stored into different position of LSB of image. This provides very good security. Xie, Qing., Xie, Jianquan., Xiao, Yunhua [13]., proposed a method in which the information is hidden

in all RGB planes based on HVS (Human Visual System). This degrades the quality of the stego image.

In the method proposed by Sachdeva S and Kumar A,[14], the Vector Quantization (VQ) table is used to hide the secret message which increases the capacity and also stego size. The method proposed by Chen, R. J., Peng, Y. C., Lin, J. J., Lai, J. L., Horng, S. J [15], presents the novel multi-bit bitwise adaptive embedding algorithm for data hiding by evaluating the most similar value to replace the original one. Roy, S., Parekh, R., [16] proposed an improved steganography approach for hiding text messages within lossless RGB images which will suffer from withstanding the signal processing operations. Minimum deviation of fidelity based data embedding technique has been proposed by Mandal, J.K., Sengupta, M., [17] where two bits per byte have been replaced by choosing the position randomly between LSB and up to fourth bit towards MSB.

A DWT based frequency domain steganographic technique, termed as WTSIC is also proposed by the same authors, [18] where secret message/image bits stream are embedded in horizontal, vertical and diagonal components. Shejul, A. A., Kulkarni, U.L [19], proposed an algorithm in which binary images are considered to be secret images which are embedded inside the cover image by taking the HSV (Hue, Saturation, Value) values of the cover image into consideration. The secret image is inserted into the cover image by cropping the cover image according to the skin tone detection and then applying the DWT. In this method the capacity is too low.
Sarreshtedari, S., Ghaemmaghami, S[20], proposed a method to achieve a higher quality of the stego image using BPCS (Bit Plane Complexity Segmentation) in the wavelet domain. The capacity of each DWT block is estimated using the BPCS. Rubab, S., Younus, M., [21], proposed a complex method using DWT and Blowfish encryption technique to hide text message in color image.

Proposed Method

In this proposed method, both cover and secret images are color images. The images are broken down into 3 constituent matrices consisting of Red, Green, and Blue components respectively. The cover image is of size 256X256 and the secret image is of size 128X128. To transfer the secret image confidentially, the secret image itself is not hidden, instead keys are generated for each color component and the IWT is used to hide the keys in the corresponding color component of the cover image. The following subsections describe the entire embedding and extracting process.

Key Generation

The following steps are used to generate a key for the Red component of the secret image. Similar steps are used to generate the keys for Green and Blue components of the secret image.

- Obtain single level 2D DWT of the Red components of the cover image C and secret image S.

- The resulting transformed matrix consists of four sub-bands CLL, CHL, CLH and CHH and SLL, SHL, SLH and SHH obtained by transforming images C and S respectively.
- The sub-images CLL and SLL are subdivided into non-overlapping blocks BCk1($1 < k1 < nc$) and BSi($1 < i < ns$) of size 4x4 where nc, ns are the total number of non-overlapping blocks obtained from sub-images CLL and SLL respectively.
- Every block BSi, is compared with block BCk1. The pair of blocks which have the least Root Mean Square Error (RMSE) is determined. A key is used to determine the address of the best matched block BCk1 for the block BSi. Then IDWT is applied to get red component of cover C.

Key Embedding using IWT

The generated key is hidden in the red component of the cover using the watermarking technique proposed in [10], using IWT. Since in steganography, the cover image is not required at the receiver once the secret information is extracted, some of the bit planes of the transformed coefficients of the cover can be entirely modified to hide the secret information. This increases the hiding capacity. In order to increase the robustness and security, the middle bit planes of the higher frequency components of the transformed cover image are used. The steps to hide the key are as follows:(similar steps are used to hide the keys corresponding to green and blue components of the secret image in green and blue components of the cover image respectively).

- Find the integer wavelet transform of red component of the cover image.
- Construct the binary image using the middle bit planes of the higher frequency components of the transformed image.
- Compress the Key.
- Replace the middle bit planes of the higher frequency components of the transformed image by the bits of the compressed key. (fourth and higher bit planes are used in the experimentation).
- Obtain the inverse IWT of the resulting image to get the red component of the stego image.

Similarly obtain the Green and Blue components of the stego image. Combine Red Green and Blue components to get the stego image G.

Key Extraction

The steps are as follows:

- Decompose the stego image into Red, Green and Blue components.
- Find the integer wavelet transform of each components of the stego image separately.
- Construct the binary image using the middle bit planes of the higher frequency components of the transformed image separately.

- The middle bit planes of the higher frequency components contain the compressed key.
- Decompress it to obtain the original key.

Secret Image Generation

- Decompose the stego image G into Red, Green and Blue components.
- Transform each component of the stego-image separately into single level 2D DWT.
- This transformation results in four sub-bands LL, HL, LH and HH in each component.
- Divide the sub-band image LL of each component into 4x4 non-overlapping blocks. The keys of the corresponding components are used to obtain the blocks that have the nearest approximation to the original blocks in secret image.
- The obtained blocks are then rearranged to obtain the sub-band image LLnew of each component. Assuming HLnew, LHnew, HHnew are zero matrices of dimension similar to LLnew, 2D IDWT is obtained for each component.
- The three components are combined together to get the secret image S.

Figure 3: Cover-images: (a) Lena (b) Nature.

Figure 4: Secret-images: (a) Penguin (b) Black Dragon.

Experimental Results

The proposed steganography technique is implemented in MATLAB 7.6. The cover images considered are Lena and Nature with dimensions 256x256 and the secret images are Penguin and Black Dragon with dimensions 128x128. All the images under consideration are color images. Figure 3 shows the cover images and Figure 4 shows the secret images. The stego images are shown in Figure 5. Penguin is hidden in Lena and black dragon is hidden in Nature. The extracted secret images are shown in Figure 6.

Figure 5: Stego images: (a)Lena as cover image and penguin as the secret image (b) Nature as cover and Black Dragon as the secret image.

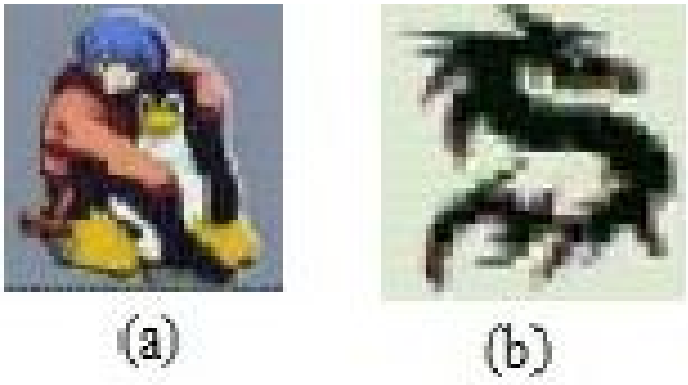

Figure 6: Extracted secret images: (a) Penguin from Lena as the cover image
(b) Black Dragon from nature as the cover image.

Table 1 shows the PSNR values in dB of the stego image with respect to cover image. Table 2 shows the PSNR values in dB of the extracted secret image with respect to original secret image In Table 3 the PSNR values of stego image in our method is compared with PSNR values of other methods which use color images for both cover and secret images.

Table 1: The PSNR Values in dB of the stego image with respect to cover image.

Cover image	**Secret image**	
	Penguin	**Black Dragon**
Lena	44.28	44.63
Nature	43.86	44.91

Table 2: The PSNR Values in dB of the extracted secret image with respect to original secret image.

Cover Image	**Secret Image**	
	Penguin	**Black Dragon**
Lena	27.00	25.94
Nature	28.45	25.94

Table 3: Comparison of PSNR in dB of the stego image in different methods.

Technique	**PSNR**
Ghoshal N *et. al.,* [22]	33.2
Ghoshal N *et. al.,* [23]	41.5
Mandal J.K *et. al.,* [17]	39.6

Conclusion

In this paper a secure color image steganography technique using IWT is proposed. The secret image is also a color image. In this technique the secret image is hidden using keys. The image itself is not hidden. Only keys are hidden. Same technique can be used to hide messages also. The experimental results show that the technique produces good quality stego images with better PSNR values compared to similar other techniques.

References

[1] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, "A Tutorial Review on Steganography", (IC3-2008 UFL and JIITU, p. no. 105-114).

[2] Katzenbeisser, S. and Petitcolas, F.A.P. "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, Inc., Boston, London. 2000.

[3] V. Srinivasa rao, Dr P.Rajesh Kumar, G.V.H.Prasad, M. Prema Kumar, S.Ravichand, "Discrete Cosine Transform Vs Discrete Wavelet Transform: An Objective Comparison of Image Compression Techniques for JPEG Encoder", International Journal of Advanced Engineering and Applications, Jan. 2010.

[4] Elham Ghasemi, Jamshid Shanbehzadeh and Bahram ZahirAzami, "A Steganographic method based on Integer Wavelet Transform and Genetic Algorithm", IEEE conference 2011, pp 42-45.

[5] M. F. Tolba, M. A. Ghonemy, I. A. Taha A. S. Khalifa "Using Integer Wavelet Transforms in Colored Image-Stegnography", International Journal on Intelligent Cooperative Information Systems, Volume 4, July 2004, pp 75-85.

[6] Ahmed A. Abdelwahab and Lobna A. Hassaan, "A Discrete Wavelet Transform Based Technique For Image Data Hiding", 25th National Radio Science Conference, 2008.

[7] Neda Raftari and Amir Masoud Eftekhari Moghadam, "Digital Image Steganography Based on Integer Wavelet Transform and Assignment Algorithm", Sixth Asia Modelling Symposium, 2012, pp 87-92.

[8] El Safy, R.O, Zayed. H. H, El Dessouki. A, "An Adaptive Steganographic Technique Based on Integer Wavelet Transform", IEEE conference, 2009, pp 111-117.

[9] Lai and L. Chang, "Adaptive Data Hiding for images Based on Harr Discrete Wavelet transform," Lecture Notes in Computer Science, Volume 4319, 2006.

[10] Silvia Torres-Maya, Mariko Nakano-Miyatake and Hector Perez-Meana, "An Image Steganography Systems Based on BPCS and IWT", 16th IEEE International Conference on Electronics, Communications and Computers, 2006.

[11] Guorong Xuan, Jiang Zhu, Jidong Chen, Yun Q. Shi, Zhicheng Ni and Wei Su, "Distortionless data hiding based on integer wavelet transform", IEEE Electronic letters, December 2002 Vol. 38 No. 25, pp. 1646-1648.

[12] Masud, Karim S.M., Rahman, M.S., Hossain, M.I., "A New Approach for LSB Based Image Steganography using Secret Key", 14th International Conference on Computer and Information Technology (ICCIT 2011), (Dhaka, Bangladesh 22-24 December, 2011), IEEE Conference Publications, 286-291.

[13] Xie, Qing., Xie, Jianquan., Xiao, Yunhua, "A High Capacity Information Hiding Algorithm in Color Image", 2nd International Conference on E-Business and Information System Security (EBIISS2010), (Wuhan, China, 22-23 May, 2010), IEEE Conference Publications, 1-4.

[14] Sachdeva, S and Kumar, A., "Colour Image Steganography Based on Modified Quantization Table", Second International Conference on Advanced Computing and Communication Technologies (ACCT), (Rohtak, Haryana, India, 7-8 January 2012), IEEE Conference Publications, 309-313.

[15] Chen, R. J., Peng, Y. C., Lin, J. J., Lai, J. L., Horng, S. J., "Novel Multi-bit Bitwise Adaptive Embedding Algorithms with Minimum Error for Data Hiding"

Fourth International Conference on Network and System Security (NSS 2010), (Melbourne, Australia, 1-3 September 2010), IEEE Conference Publications, 306-311.

[16] Roy, S., Parekh, R., "A Secure Keyless Image Steganography Approach for Lossless RGB Images", International Conference on Communication, Computing and Security (ICCCS '11), ACM Publications, 573-576.

[17] Mandal, J.K., Sengupta, M., "Steganographic Technique Based on Minimum Deviation of Fidelity (STMDF)", Second International Conference on Emerging Applications of Information Technology (EAIT 2011), (February 19-20 2011), IEEE Conference Publications, 298-301.

[18] Mandal, J.K., Sengupta, M. "Authentication/Secret Message Transformation Through Wavelet Transform based Subband Image Coding (WTSIC)", International Symposium on Electronic System Design (ISED), (Bhubaneswar, India, 20-22 December, 2010) IEEE Conference Publications, 225-229.

[19] Shejul, A. A., Kulkarni, U.L, "A DWT based Approach for Steganography Using Biometrics", International Conference on Data Storage and Data Engineering, (Bangalore, India, 9-10 February 2010), IEEE Conference Publications, 39-43.

[20] Sarreshtedari, S., Ghaemmaghami, S. High Capacity Image Steganography in Wavelet Domain. In Proceedings of 2010 7th IEEE Consumer Communications and Networking Conference (CCNC) (Las Vegas, Nevada, USA, 9-12 January 2010), IEEE Conference Publications, 1-5.

[21] Rubab, S., Younus, M.,"Improved Image Steganography Technique for Colored Images using Wavelet Transform", International Journal of Computer Applications, Volume 39- No.14, February 2012, 29-32.

[22] Ghoshal, N., Mandal, J.K., "A Steganographic Scheme for Colour Image Authentication (SSCIA)", International Conference on Recent Trends in Information Technology (ICRTIT 2011), (Madras Institute of Technology, Chennai, India June 03-05, 2011), IEEE Conference Publications, 826-831.

[23] Ghoshal, N., Mandal, J.K., "Controlled Data Hiding Technique for Color Image Authentication in Frequency Domain (CDHTCIAFD)", Second International Conference on Emerging Applications of Information Technology,IEEE Conference Publications, 284-287.