International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

A Secure Color Image Using Integer Wavelet Transform with Linde-Buzo Gray Algorithm

S.Anusuyya [1], Mrs.N.Jothy [2]

[1]*M.Tech (Electronic and Communication Engineering), Sri Manakula Vinayagar Engineering College, Madagadipet,Pondicherry.*
[2]*Asst., Professor, Dept. of Electronic and Communication Engineerin , Sri Manakula Vinayagar Engineering College, Madagadipet,Pondicherry.*

Abstract - *Steganography is a technology that is used to conceal the information within some objects such as image, audio or video so that no one can sense the information. Steganographic method has several advantages including high hiding capacity and undetectablity. The secret content has been hidden into compressed cover image using IWT and Linde-buzo-gray (LBG) algorithm. It is difficult to detect the hidden information by Steganalysers since Stego Image and Cover image seems to be similar. High PSNR (Peak Signal to Noise Ratio) value for the extracted image is as same as the secret image. This has been substantiated by comparing techniques which are similar to IWT and the results throws light that the proposed IWT technique is simpler and also gives better PSNR values.*

Key Words: **Steganography, IWT, Stego Image, Cover Image, PSNR, LBG.**

1. INTRODUCTION

In recent days, Information hiding technique has attained major significance in the field of information security. It can be achieved either by digital watermarking or steganography. In earlier days, mainly used for copyright protection whereas nowadays mainly used to secure the information by hiding into some other medium such as image, audio or video. The medium used to embed the information is known as cover object. The cover object along with the concealed information is said to be Stego object [1]. In order to get a Stego Image, both secret image and stego key are embedded in the cover image.

The main goal of Steganography is to prevent some unauthorized observer from recovering or altering the confidential information. The design of steganographic system can be categorized into spatial domain methods and transform domain methods. Here, Integer wavelet transform method is used to design the stegnographic system.

1.1 Integer Wavelet Transform

Most information hiding techniques perform embedding information by altering the contents of a source media. As a result, while extraction it causes some distortion in cover image and thus the steganalyser can try to extract the secret information. This can be avoided by using Integer Wavelet Transform.

IWT is a more efficient method to hide secret information without distortion. IWT maps integers to integers. Whereas in DWT, if the input consists of integers, the resulting output doesn't consists of integers. Thus it causes difficulty in restoration of the original image. But in case of IWT, resulting output can be completely categorized with integers. In IWT, LL sub-band appears to be a close copy of the original image with smaller scale whereas in DWT the resulting LL is distorted slightly, as shown in Fig1

Fig -1: (a) Original image Lena. (b) One level DWT in sub band LL (c) One level IWT in Sub-band LL.

If the original image (O) is X pixels high and Y pixels wide, the level of each of the pixel at (i, j) is denoted by $O_{i,j}$.[3].

The IWT coefficients are given by

$$LL_{i,j} = | (O_{2i,2j} + O_{2i+1,2j}) /2 | \quad (1)$$

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

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

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

The inverse transform is given by

$$O_{2i,2j} = LL_{i,j} - | HL_{i,j}/2 | \quad (5)$$

$$O_{2i,2j+1} = LL_{i,j} + | HL_{i,j+1}) /2 | \quad (6)$$

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

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

Where, $1 \le i \le X/2$, $1 \le j \le Y/2$ and| | denotes floor value.

1.2 Linde-Buzo-Gray Algorithm

Linde-Buzo-gray (LBG) algorithm [2] is the conventional codebook generation algorithm. Firstly, image is divided into non overlapping blocks of fixed size to form initial cluster. Then, centroid of initial cluster is computed. After that add and subtract constant error from that centroid to get two error vectors e1 and e2 for cluster 1 and 2 respectively. Compare each vector of cluster with error vectors e1 and e2 and split the cluster into two. For next iteration calculate centroid of cluster and compute error vectors to further split that cluster into two. Repeat above procedure till given number of clusters not form. Each codebook vector is obtained by computing centroid of each cluster. Fig shows LBG clustering for two dimensional space.

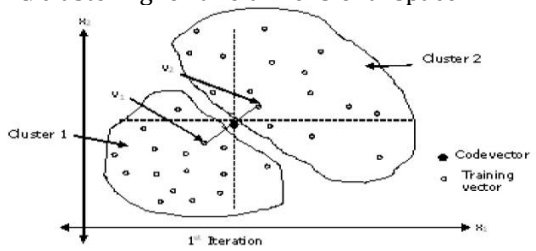

Fig -2: LBG clustering for 2 Dimensional space

2. RELATED WORK

Color images are represented in different color spaces such as RGB (Red Green Blue), HSV (Hue, Saturation, and Value), YUV, YIQ, YCbCr (Luminance/Chrominance) etc. YCbCr is one of the best representations for steganography because the human eye is sensitive to minute changes in luminance but not in chrominance, so the chrominance part can be altered, without visually diminishing the overall image quality. Y is luminance component and CbCr are the blue and red chrominance components respectively. The values in color space can be easily converted into another color space using conversion formula [4].

S.M. Masud Karim, et al., [5] 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 et al., [6] proposed a new approach in which the information is hidden in all RGB planes based on Human Visual System (HVS). Sunny Sachdeva et al., [7] introduced the Vector Quantization (VQ) table to hide the secret message which increases the capacity and the Stego size. Sankar Roy et al., [8] introduced a new improved steganography method for hiding text messages within lossless RGB images which will suffer from withstanding the signal processing operations. EI Safy et.al. [9], proposed an adaptive steganographic technique based on IWT, which improves the hiding capacity and PSNR. Nda Raftari and Amir Masoud E.M. [10] used IWT and Munkres' assignment algorithm which embeds secret image in frequency domain of cover image with high matching quality.

3. PROPOSED WORK

512x512 cartoon color image is used as the cover image and 128x128 Grayscale image is used as the secret information in the proposed method. In order to transfer the secret image more securely, instead of hiding the secret image a key is generated and then it is encrypted and Run Length Encoded. SWT method aids in hiding the resultant key in the cover image. Hence this improves the security and also the capacity can be upgraded to some extent since the key and secret information is compressed using LBG algorithm.

3.1 Key Generation

To generate the key following phases are implemented.

- In YCbCr color space, C_i denotes the cover image.
- Obtain single level 2D IWT of secret image S_i and Cr component of C_i
- The resulting transformed matrix consists of four sub-bands SLL, SHL, SLH and SHH and CLL, CHL, CLH and CHH obtained by transforming S_i and Cr components of C_i respectively.
- Non-overlapping blocks BC_{k1} and BS_i of size 2x2 are derived from the sub-images CLL and SLL.
- Every block BS_i is compared with B_{k1}. Then the pair of blocks which have Least Mean Square Error is determined. A key is used to determine the address of the best matched block BC_{k1} for the block BS_i. Then inverse 2D IWT is applied to obtain Cr component.
- The key is then encrypted and run length encoded.

3.2 Key Embedding

The key obtained in the previous sub section is hidden in the cover image using IWT. The steps are as follows:

- Find the IWT of Cr component of the cover image.
- Replace LSB planes by the bits of the key of the higher frequency components of the transformed image.
- Obtain the inverse IWT of the resulting image to get the Stego Cr component.
- Represent the resultant image in RGB color space to obtain Stego image G_i.

3.3 Key Extraction

The steps are as follows:

- Represent the Stego image G_i in YCbCr color space.
- Find the IWT of Cr component of the Stego image G_i.
- To convert back to RGB representation, key from LSB planes of the higher frequency components of the transformed image have to be obtained.
- Decompress the key and then decrypt it to get original key.

3.4 Linde-Buzo-Gray algorithm

- Convert RGB image into YCbCr color format.
- Take only Chrominance Red (Cr) component of YCbCr image, which will be the input image.
- Input image of size N X N is divided into subblocks of size n x n.
- Define the size of codebook and randomly select M vectors from the input vectors.

$$D(X,C) = \sqrt{\sum_{t=1}^{k}(Xt - Ct)^{\wedge}2} \quad (1)$$

Search the nearest codevector from C and then add the input vector into corresponding cluster of the closest codevector found.

- For each codevector in the current codebook C, find the centroid of its associated cluster and take the centroid as a new codevector for the next iteration. Repeat step 2 and 3 till codevector don't change or change is small.
- Measure the performance parameters PSNR and MSE of the reconstructed RGB image. The block diagram for compression process is shown in Fig 3. The cover image is converted into YCbCr color space and then LBG algorithm is applied and codebook and index is obtained. Thus the cover image is compressed.

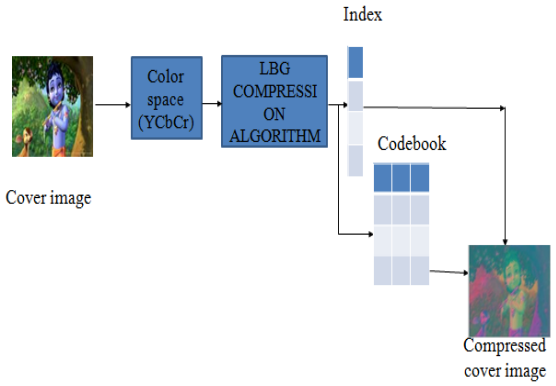

Fig -3: Compression Process

3.5 Embedding Phase

In embedding phase, cover image is compressed and then the secret information is concealed in it to achieve secure transmission of huge amount of secret information.

Steps for embedding secret information are listed as follows.

Read secret image and cover image.

- Resize both images to 256 x 256 size.
- Separate chrominance Red component from the cover image and then apply IWT and embed the secret image inside the Cr components along with key.
- Inverse IWT is applied to get stego image.

3.6 Extraction Phase

In extraction phase, secret image is extracted from the compressed cover image.

Steps for extraction of secret information are listed as follows.

- Read stego-image and then decompress the cover image using codebook and index vector
- Apply IWT to extract secret image from the cover image.

Table-1 shows the comparison between the existing and proposed technique:

Table-1: Comparison between Different Techniques

Techniques	Cover image size	PSNR value for hiding image (in dB)	PSNR value for hiding text (In dB)	SSIM
Existing methods: MPSteg color	512 X 512 JPEG	48.067	50.543	0.64
2 LSB Embedding	512 X 512 JPEG	51.642	53.864	0.75
Proposed method: Integer Wavelet Transform	512 X 512 JPEG	54.860	55.901	0.84

Peak Signal to Noise Ratio is the image quality measure. A good image should possess low MSE and high PSNR.

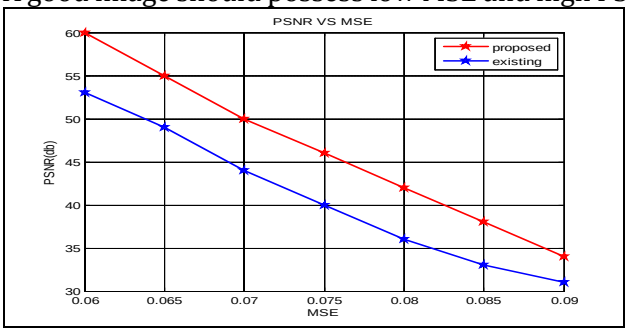

Chart-1: PSNR VS MSE

4. CONCLUSIONS

In this paper, the secret images can be extracted without any distortion to the original image. This technique provides the high quality of the Stego-image having high PSNR values compared to other methods. However, this method can enable us to transmit the secret information to the receiver independently, it is nearly impossible for any unintended parties to extract the secret information, and recover the original host image, when the Stego image is accessed by them.

REFERENCES

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

[2] Y. Linde, A. Buzo, R.M. Gray, " An algorithm for Vector quantiser design", IEEE Transaction on Communications, Vol.28, pp.84-95, 1980.

[3] Guorong Xuan et.al,"Distortionless Data Hiding Based On IWT", Electronics Letters, vol.38,No.25,pp.1646-1648,.2002.

[4] Shejul ,A. A.,Kulkarni, U.L., "A Secure Skin Tone based Steganography (SSTS) using Wavelet Transform",International Journal of Computer Theory and Engineering, Vol.3,No.1,pp.16-22,2011.

[5] 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, IEEE Conference Publications, pp 286-291,2011.

[6] Xie,Qing.,Xie,Jianquan.,"A High Capacity Information Hiding Algorithm in Color Image",2nd International Conference on E-Business and Information System Security,IEEE Conference Publicatications,pp.1-4,2010.

[7] Sachdeva, S and Kumar , A., "Color Image Steganography Based on Modified Quantization Table,"2nd International Conference on Advanced Computing and Communication Technologies, IEEE Conference Publications,pp 309-313,2012.

[8] Roy, S., Parekh, R., " A Secure Keyless Image Steganography Approach for Lossless RGB Images",International Conference on Communication Computing and Security ,ACM Publications,573-576,2011.

[9] EI Safy, R.O, Zayed. H. H, EI Dessouki,A., " An Adaptive Steganography based on IWT",IEEE Conference Publications.pp.111-117,2009.

[10] Neda Raftari and Amir Masoud Eftekharu Moghadam, "Digital Image Steganography based on IWT",6th Asia Modelling Symposium, pp.87-92,2012.