International Journal of Engineering & Technology, 7 (3.34) (2018) 688-691

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Data Hiding Using Yc_bc_r-DWT in Addition to Noise

[1]Maheswari.S, [2]Dr.Reeba Korah

[1]Research Scholar, Department of Electronics and communication,Satyabhama University, Chennai, India
[2]Professor, Alliance University, Bangalore, India

Abstract

An ability of hiding the important information's like image, audio, video files into the digital media is termed as steganography. Steganography helps to attain secret communication by using variety of conventional techniques like spatial domain method, spread spectrum method and so on. In various file formats, the data hiding has undergone by these techniques but the retrieval of the secret message from the cover is not efficient with these methods. The proposed approach mainly uses YC_bC_r color space for conversion. A color space conversion provides an efficient transmission of color information. Secondly, a frequency domain approach of Discrete Wavelet Transformation is applied after color conversion for four level of decomposition for secret data embedding. In this approach, the converted YC_bC_r color space image is used as a cover image which aims to segregate illumination and chrominance component of the original input color image. And in the high intensity red layer of the cover image, the secret information is embedded in this method. In addition, this methodology is used for analysing the proposed process by superimposing of noise and exclusive of different noises. In this work, the algorithm proposed is compared with existing LSB technique and provides better PSNR measure than the existing method.

Keywords: *Data hiding, YC_bC_r color space,DWT, Noise*

1. Introduction

In recent world, the internet plays a vital role in digital data transmission which needs secure communication, in spite of the confidential information being stolen, copied, modified, or destroyed by another observer. Therefore, the main issue is protected transmission by means of different attacks. Encryption is a prominent procedure for ensuring secured data transmission. In literature [1], steganography is referred to as concealed writing. Steganography is used to transfer information or data in a secured manner, in which the information cannot be detected and predicted. [1]- [5]Spatial Domain steganography is a process in which the secret data bits or information are hidden into the right most bit of the cover image. In a gray level image, each pixel value is represented by 8 bits only. In order to make sure that the original pixel values cannot be affected by adding secret data into the LSB plane. This method is simple and unconcealed method but has low ability to process the data hiding with noises. Hence secret data can be easily attacked and stolen by third party with extracting the entire LSB plane. [2][10]

Frequency domain steganography becomes more robust than the spatial domain whether the properties of the original cover image are mostly used. In general, it is preferable for hiding confidential data in noise affected regions rather than flat smooth regions as degradation in flat regions is more observed for human HVS(Human Visual System).Taking these aspects into account, operating in frequency domain technique provide more suitable and protectable way of information against attacks. In frequency domain, coefficients are extracted from the original cover image before embedding secret messages into it. Various sub-bands of frequency domain coefficients give significant information about where vital and non-vital pixels of image reside. Though these methods are complex than spatial domain methods, more need of secure transmission should attain by the technique. Discrete Cosine-DCT, Discrete Wavelet -DWT, Curve let transformation are the different frequency domain transformations techniques used by the researchers. [2][3][11]. the paper is organized as follows. Section 2 deals with relevant steganography techniques. In section 3, color space used is discussed in detail, the proposed methodology using DWT is elaborated in section 4 and section 5 shows the experimental results and discussion. Finally conclusion is discussed in section 6.

2. Steganography Methods

Literature deals with many of steganography methods. A comprehensive study of these techniques is provided below.

2.1. LSB based Steganography

LSB is the significant technique in the spatial domain. In [6], the author describes about the usage of one bit LSB steganography technique. A digital image is the most common type of media used for steganography. Often digital images have a huge amount of redundant information .This enables hiding information or data into an image file. With respect to recent processing, an image is a gathering of more numbers of different light intensities. This numeric representation forms a lattice and the separate values are named to as pixels. Image steganography is about to exploit the

limited power of the human visual system (HVS). A nearby perspective of the specific color is leading to
the observation that single digit value modifications to the contribution level are imperceptible to the human eye. But this LSB procedure is not strong enough against noise.
The ability to maintain stego image quality after data hiding is accomplished by means of sacrificing quite a few data hiding space in [6]. In LSB steganography, after embedding, the cover may contain random noises. Thus LSB is not feasible for basic decorrelation of the blocks at their boundaries. The least significant bits of the cover image are replaced with no variation of complete cover image. This technique is not resilient to compression, transformation etc. of the cover image.

2.2. Spread Spectrum Steganography

Here, the original message or information is spreading over an extensive frequency bandwidth compared to the minimum required bandwidth for sending the information. Since the small SNR is maintained in every frequency band in spread spectrum technique, it is very difficult to remove message completely without destroying the cover image [4].

2.3. Statistical Technique

The cover image is segregated into blocks and each data bits are hidden in each block. The secret data is concealed by differing numerical qualities of the cover image whose blocks remain unchanged when the message block is zero which cannot provide invisible stego image [4].

2.4. Distortion Technique

Information is mainly stored by means of signal distortion. Here, adding up the sequence of changes to the cover has done by the encoder .The job of the decoder is to check the various differences between the original cover and the noise affected cover for recovering secret messages. The achievement of high capacity, security and robustness are the challenging aspect of steganography [4].

2.5. Transform Domain Technique

The various transformations used for hiding information in the transform coefficients are Discrete Cosine, discrete wavelet and Fast Fourier Transform. These methods may provide more robustness to attacks such as compression, filtering, etc.
The wavelets in steganography are used for isolating the high level frequency coefficients as well as low level frequency coefficients on a pixel by pixel basis. Haar Wavelet is a piecewise wavelet that is used to provide orthogonal decomposition given as Wavelet Transform. It may convert an image from time or spatial domain to frequency domain. DWT technique is favorably resistant to rotation, translation, cropping and noise impulses. Thus Discrete Wavelet Transform is highly preferred by the researcher to Discrete Cosine Transforms by reason of low frequency value in images at various levels can offer corresponding resolution.
The author [8] proposed an image steganography technique domain using wavelet transform for hiding audio signal in an image .The author says that the audio signal in any format will be encrypted and carried by the image without revealing by third party.

3. Materials and Methods

3.1. Color Space

It is important to segregate different color components in an image by the space transformation methods. The RGB color space is used for processing digital image data. The base components viz., Red, Green and Blue with its weighted combination is depicted in RGB model [14]. This space is simple and more popular in segmentation. HSV (Hue, Saturation, and Value) .Whenever a need for numerical specification of the property arises; hue-saturation based spaces were introduced. They describe the artist's idea of tint, saturation and tone with intuitive values. Hue defines the dominant color (such as red, green, purple and yellow) of an area; saturation measures the color purity of an area in proportion to its brightness. The luminance is termed to the brightness intensity value.
The intuitiveness of components of color space and its unequivocal separation amongst luminance and chrominance properties made the technique more popular in the research work of color image segmentation. YC_bC_r is an encoded nonlinear RGB color combination technique. This technique is used by European television studios which are applied for image compression. Two different blue based chrominance values C_b& red based chrominance values C_r are formed by subtracting luminance from blue & red components. YC_bC_r is used for separating luminance component from chrominance using a linear transform in RGB values consisting of a weighted sum of the three components [9] [12].

3.2. Proposed Method of Superimposing Noise.

The propose method is a kind of modification of transform domain technique where hiding the secret image in a particular high intensity area of the original cover image. Thus this methodology is more robust against attacks and rotation. Figure 1 shows the block diagram of the proposed YC_bC_r-DWTapproach. In this approach, input color image has been transformed to different level of component by YC_bC_r technique. The YC_bC_r color space converted image is now used as the cover image .Wavelet decomposition is carried on the cover image for concealing secret information and this resultant image from the proposed process is the stego image. The retrieving of cover image and secret information from the cover image is performed at the other end.

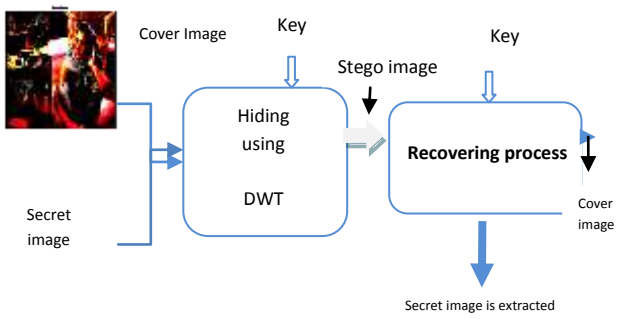

Figure 1: Block Diagram of YC_bC_r-DWT Steganography process

Discrete wavelet transform is simple and hence the most popular of all wavelet transforms. Here, the low frequency wavelet coefficient is generated by averaging the two pixel values as well as the high frequency coefficient is generated by considering half of the difference of the identical two pixels. Apart from that, these sub bands are termed as L_L – on a level plane and vertically low pass, H_L Evenly high pass and vertically low pass, L_H – on a level plane low

pass and vertically high pass and H_H - on a level plane and vertically high pass

The significant part of the spatial domain image is stored in the approximation band consists of low frequency wavelet coefficients. The other detail bands may consist of high frequency coefficients, which include the edge details of the spatial domain image. A technique for embedding secret data within a color space transformed image is introduced as it is not that much delicate to Human Visual System.

The proposed methodology is briefly introduced as follows. To start with the input image which is segregated into luminance and chrominance layers using YC_bC_r technique. This image is used as a cover image in this proposed method. Secondly image embedding has been done with the use of standard internet image .This image will be considered as secret image which has minimum of 1000 pixels. Image embedding is done in the high intensity layer using the DWT technique. By applying Haar-DWT, the image is leading to four levels of subands. Finally, secret data embedding is performed in high frequency chrominance sub-bands without tracing low value pixels in that band. Embedding of data only in certain chrominance layers immediately and not in the entire image provides high security. DWT is applied on the entire image. DWT offers better energy compaction compared to DCT without any blocking artifact. As already known that DWT technique splits component into four frequency bands called sub bands known as L_L – Horizontally and Vertically low pass, H_L - Horizontally high pass and vertically low pass, LH – Horizontally low pass and vertically high pass and H_H - Horizontally and vertically high pass .Since human eyes are much more sensitive to the low frequency part, secret message can be covered only in parts without making any alteration in sub bands. Thus the superiority of stego image is maintained by embedding secret information in high frequency chrominance sub-bands in which human eyes are less sensitive to.

The proposed algorithm provides good quality image with the effect of more noises. Here two different noises are considered which is to be superimposed in the cover image to show the system is more robust to noises. In the proposed method, the noises like Gaussian random noise, Salt and Pepper are filtered efficiently after retrieving the secret information. Thus the output image is a noise free stego image. In addition to efficient noise removal, embedding of secret message into the image is achieved through YC_bC_r-DWT technique. Not only is the filtering technique introduced for removing the different noises and also to produce noise free outcome with secret data hiding. Therefore the proposed algorithm is better than the existing LSB technique against noise variations.

4. Results and Discussion

A sample of results acquired for standard images like Barbara and Lena are depicted in Figure.2. For performance evaluation of the proposed schemes standard color images of size 512 × 512 such as Lena, Barbara images have been used as cover images. Any image of 1000 pixels has been used as secret image. The following figure.2 depicts (a) shows a standard input image (b) YC_bCrcolor space image and figure 3 depicts (a) cover image (b) final stego image.

Figure 4 depicts the stego image has undergone filtering of Gaussian in addition to Salt & Pepper noise. In this proposed method, cover image is obtained by YC_bC_r color space transformation .The stego image obtained by hiding secret image using DWT technique is free of those noises. Even in presence of these two noises, the hiding of information has been done by DWT technique and corresponding PSNR value is tabulated in Table 1.

(a) **(b)**

Figure 2: (a) Input image (b) YC_bC_r color space image

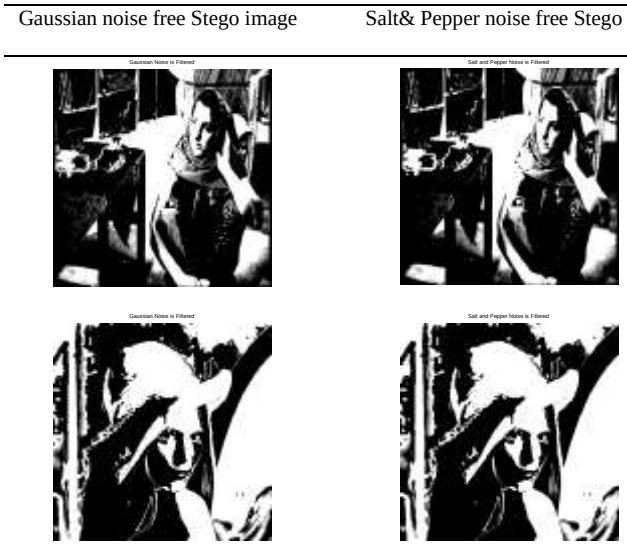

Figure 3: (a) Cover image (b) Stego image

Figure 4: (a) Gaussian noise filtered output image (b) Salt & Pepper noise filtered output image

The quantitative results are listed in Table 1 using Proposed DWT approach and existing LSB technique with and without noise. The two different noises are considered in this methodology. In addition, after filtering of noise, data hiding of secret information process is done in this approach. Peak Signal to Noise Ratio-PSNR measure of proposed approach using YC_bC_r space and existing HSV color space in presence of Gaussian and Salt & Pepper noise, are tabulated in table 1.Improved PSNR is an outcome of proposed methodology in presence and absence of noise compared to existing LSB technique.

The following equation (1) is used to calculate the Peak Signal to Noise Ratio PSNR measure between cover and stego image. Similarly equation (2) is used to calculate the mean square error-mse measure between cover and stego image.

$$\text{PSNR} = 10 * \log_{10} \left(\frac{255^2}{mse}\right)\text{----------} \quad (1)$$

$$\text{mse} = \left(\frac{1}{M*N}\right) \sum_{i=1}^{M} \sum_{j=1}^{n} (X_{ij} - Y_{ij})^2\text{----} \quad (2)$$

Xand Yrepresent the image coordinates; *M* and *N* represent the dimensions of the image.

Table1: PSNR value of proposed and existing method in presence and absence of noise

Color space	Cover Image	With or Without Addition of Noise	PSNR of YC_bC_r DWT	PSNR of LSB [12]
YC_bC_r color space	Image 1	Exclusive of noise	44.5	29.69
	Image 2	Exclusive of noise	41.23	25.6
	Image 1	Presence of Gaussian Noise	31.24	24.83
	Image 2	Occurrence of Salt and Pepper Noise	28.39	24.01
HSV color space[6]	Image 1	Exclusive of noise	37.79	31.4
	Image 2	Exclusive of noise	36.05	33.21
	Image 1	Presence of Gaussian Noise	26.62	24.82
	Image 2	Occurrence of Salt and Pepper Noise	28.10	22.18

5. Conclusion

The performance of the YC_bC_r-DWT Steganography Process is analyzed quantitatively and qualitatively. The simulation results and performance measures show that the proposed methodology is better than that of LSB [6].The proposed approach will use YC_bC_r color space with DWT for secret data hiding. In this methodology, the converted color image using YC_bC_r color space is used as a cover image. This method is used for analyzing the steganography process with and without of different noises. When compared to existing LSB technique, the proposed YC_bC_r-DWT algorithm provides better PSNR measure than the existing method.

References

[1] Salomon D, Data hiding in text, Data privacy and security,//www.springer.com/978-0-387-00311-5

[2] Abbas Cheddad, J Condell, k Curran, Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods", signal processing, volume 90, issue 3, March 2010.

[3] Niranjan L. Bhale, "A Review of Digital Image Steganography Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6, June 2014

[4] Abdulaleem Z. Al-Othmani, "Survey on Steganography Techniques in Real Time Audio Signals and Evaluation",IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, January 2012

[5] Yih-Chuan Lin, Tzung-Shian Li, Yao-Tang Chang, Chuen-Ching Wang, Wen-Tzu Chen, "A Sub sampling and Interpolation Technique for Reversible Histogram Shift Data Hiding", Image and Signal Processing", Lecture Notes in Computer Science, Vol. 6134, 2010, Publisher: Springer Berlin/Heidelberg, pp. 384-393.

[6] Yu-Chee Tseng, Hsiang-Kuang Pan, "Data Hiding in 2-Color Images", IEEE TRANSACTIONS ON COMPUTERS, VOL. 51, NO. 7, JULY 2002

[7] Amritha.G Meethu Varkey, "Biometric Steganographic Technique Using DWT and Encryption",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013

[8] Hemalatha Sa, "Wavelet transform based steganography technique to hide audio signals in image", Procedia Computer Science 47 (2015) 272 – 281

[9] Youssef Bassil, "Image Steganography based on a Parameterized Canny Edge Detection Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 60– No.4, December 2012

[10] Srinath N K1, Usha B A2, Narayan K3, Tushara C K4, "Analysis of Data Embedding Technique in Image", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 6, June 2014

[11] M. Indra Sena Reddy, Dr. A.P. Siva Kumar, "Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm", International Conference on Computational Modeling and Security (CMS 2016), Procedia Computer Science (2016) 62 – 69

[12] V. Lokeswara Reddy, "Implementation of LSB Steganography and its Evaluation for Various File Formats", Int. J. Advanced Networking and Applications 868, Volume: 02, Issue: 05, Pages: 868-872 (2011)

[13] Ahmed Elgammal, "Skin Detection - a Short Tutorial" Crystal Muang and Dunxu Hu, Department of Computer Science, Rutgers University, Piscataway, NJ, 08902,

[14] N. Tiwari and M. Shandilya, (2010) "Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth", International Journal of Security and Its Applications Vol. 4(4)

[15] K. Vijayakumar and C. Arun, "Continuous Security Assessment of Applications in Cloud Environment", International Journal of Control Theory and Applications, ISSN: 0974-5645 volume No. 9(36), Sep 2016, Page No. 533-541.

[16] Vijayakumar, N. Divya Sri, M. Vijayashree, "An Effective User Revocation and Anti Collusion System for Dynamic Groups in Cloud", International Journal for Research in Applied Science & Engineering Technology, ISSN: 2321-9653, Volume 4 Issue V, May 2016