ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

Review of Least Significant Bit Technique for Color Image Steganography

Abhishek Deep[1], Prof. Arun Jhapate[2]

M. Tech. Scholar, Department of Computer Science and Engineering, Sagar Institute of Research Technology, Bhopal, India[1]

Assistant Professor, Department of Computer Science and Engineering, Sagar Institute of Research Technology, Bhopal, India [2]

ABSTRACT: In this paper a digital image watermarking based on 2-D discrete wavelet transform (DWT) is presented. In this technique a multi-bit watermark is embedded into the low frequency sub-band of a cover image by using alpha blending technique. During embedding, watermark image is dispersed within the original image depending upon the scaling factor of alpha blending technique. Extraction of the watermark image is done by using same scaling factor as for embedding. Performance of method for different value of scaling factor is analyses & compare with 2-D DWT method by using statistical parameters such as peak signal-to-noise-ratio (PSNR) and mean square error (MSE).

KEYWORDS: Discrete Wavelet Transform, Haar wavelet, JPEG Image Encoding, Peak Signal to Noise Ratio,

I. INTRODUCTION

Steganography is hiding private or secret data within a carrier in invisible manner. It derives from the Greek word steganos, meaning covered or secret, and graphy (writing or drawing) [1]. The medium where the secret data is hidden is called as cover medium, this can be image, video or an audio file. Any stego algorithm removes the redundant bits in the cover media and inserts the secret data into the space. Higher the quality of video or sound more redundant bits are available for hiding. Application of Steganography varies from military, industrial applications to copyright and Intellectual Property Rights (IPR). By using lossless steganography techniques messages can be sent and received securely [2]. Traditionally, steganography was based on hiding secret information in image files. But modern work suggests that there has been growing interest among research fraternity in applying steganographic techniques to video files as well [3], [4]. The advantage of using video files in hiding information is the added security against the attack of hacker due to the relative complexity of the structure of video compared to image files.

Video based steganogrpahic techniques are broadly classified into temporal domain and spatial domain. In frequency domain, images are transformed to frequency components by using FFT, DCT or DWT and then messages are embedded in some or all of the transformed coefficients. Embedding may be bit level or in block level. Moreover in spatial domain the bits of the message can be inserted in intensity pixels of the video in LSB positions. The advantage in the method is that the amount of data (payload) that can be embedded is more in LSB techniques. However most of the LSB techniques are prone to attack as described in [5] and [6]. This makes research fraternity interested in designing new methods. Techniques other than LSB substitution also exist in literature and have been discussed in the next section. In this paper a hash based LSB Techniques is proposed in spatial domain. An application of the algorithm is illustrated with AVI (Audio Video Interleave) file as a cover medium. The results obtained are significant and encouraging. Effort has also been taken to study the steganalysis of the proposed scheme.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

II. LITERATURE REVIEW

Wu, H.-T et al. [1] proposed an algorithm in the field of steganography for JPEG images altering the block DCT coefficients. In this method the DCT coefficients are divided into four frequency bands by matrix encoding. A new method for selecting the coefficient is also used to make the concealed message less perceivable.

Gupta, R. et al. [2] proposed a new method for image security integrating cryptography stenography and watermarking techniques. It not only hides the message but also gives better results for MSE, PSNR and embedding power even after the noise attacks. It also provides security for watermarked video.

Baek, J et al. [3] presented a steganographic method for secret sharing of information using gray scale images. The relationship between the binary and gray code representation of a pixel is taken into consideration here. And an EX-OR operation is used upon N cover images accessible to sender and receiver.

Bajwa, I.S. et al. [4] proposed two methods for color image steganography. They have proceeded with a hashing approach for secure data hiding. Here secured images are transmitted at higher speed using gray scale images with this approach. Also various file formats such as bmp, JPEG, gif are supported in this technique of secured transmission.

Bouslimi, D. et al. [5] put forward an algorithm for concealing message in encrypted images using a predetermined watermark embedding before the process of encryption. Here the encryption/decryption has a unique key and watermark processing has a different key thus decryption of message is independent of extracting the image.

Zhang et al. [6] presented an approach for data concealing by reversible image transformation. Here RTI based framework is used to convert the content of original image into another target image having same size. Traditional RDH scheme and unified embedding and scrambling scheme are used to insert watermark in the encrypted image.

Khodaei, M et al. [7] put forward a method for data hiding using pixel value differencing and LSB substitution. Here an image is split into blocks of two successive pixels. The difference of two pixels is calculated, and as per the difference, it will estimate the number of embedding bits into LSBs of two pixels.

Conci et al. [8] proposed AES cryptography in color image by genetic algorithms and path re-linking. It presents a hybrid approach that replaces the LSB substitution methods thus increasing the usage of color images to hide a text.

Panda, S.S. et al. [9] presented a secured approach to spatial image steganography by changes in the neighbourhood pixels of the cover image. By this technique, the embedded area looks more regular and uniform.

Nilizadeh, A. et al. [10] presented a modern steganography technique grounded on matrix pattern and LSB algorithms proposed for RGB images. These methods utilize the spatial domain of image for concealing the data. The Matrix pattern divides the RGB image into various B*B blocks into non overlapping layers.

Karthikeyan.B. et al. [11] proposed an approach of cryptography and steganography by deploying rotor cipher for assured conveyance of data in an interrupted communication channel using 2-bit LSB steganography which helps in hiding the information from the intruder. They have also put forward an advanced steganographic method by LSB substitution on a scanned image which increases the security level of the message. In addition to this they have presented a LSB dependent steganography with multi-layered encryption by using caeser cipher technique to conceal the text in the image and encrypting it based on the chaos theory. Also they have put forth [14] a composite method for hiding information through random theory and reversible integer depiction in which DCT is applied to the image and is hidden by LSB substitution.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

III. TYPES OF STEGANOGRAPHY

The sender writes an innocuous message and then conceals a secret message on the same piece of paper. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. The data can be visible in basic formats like: Audio, Video, Text and Images etc. These forms of data are detectable by human hiding, and the ultimate solution was Steganography. The various types of steganography include:

a. Image Steganography: The Image Steganography is technique in which we hide the data in an image so that ther will not be any change in the original image.

b. Audio Steganography: Audio Steganography can be used to hide the information in an audio file. The audio file should be undetectable.

c. Video Steganography: Video Steganography can be used to hide the information in video files. The video files should be undetectable by the attacker.

d. Text files Steganography: Text Steganography is used to hide the information in text files. The general process of steganography i.e., preparing a stego object that will contain no change with that of original object is prepared but using text as a source.

IV. DISCRETE WAVELET TRANSFORM

The model used in [5] to implement the tree structure of Direct Wavelet Transform (DWT) is based on the filtering process. Figure 1 depicted a complete 3-level Direct WT. In this figure G and H is the high pass and low pass filter respectively.

Computation period is the number of the input cycles for one time produces output samples. In general, the computation period is M= for a j-level DWT. The period of the 3-level computation is 8. Figure 1, The Sub band Coding Algorithm As an example, suppose that the original signal X[n] has N- sample points, spanning a frequency band of zero to π rad/s. At the first decomposition level, the signal passed through the high pass and low pass filters, followed by subsampling by 2. The output of the high pass filter has N/2- sample points (hence half the time resolution) but it only spans the frequencies π/2 to π rad/s (hence double the frequency resolution).

The output of the low-pass filer also has N/2- sample points, but it spans the other half of the frequency band, frequencies from 0 to π/2 rad/s. Again low and high-pass filter output passed through the same low pass and high pass filters for further decomposition. The output of the second low pass filter followed by sub sampling has N/4 samples spanning a frequency band of 0 to π/4 rad/s, and the output of the second high pass filter followed by sub sampling has N/4 samples spanning a frequency band of π/4 to π/2 rad/s. The second high pass filtered signal constitutes the second level of DWT coefficients. This signal has half the time resolution, but twice the frequency resolution of the first level signal. This process continues until two samples are left. For this specific example there would be 3 levels of decomposition, each having half the number of samples of the previous level.

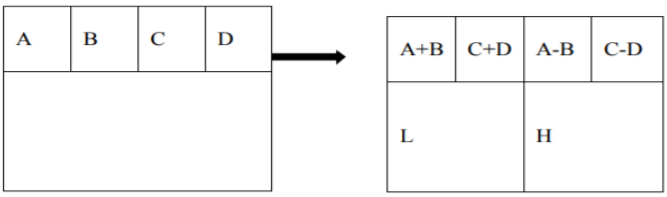

Figure1: The horizontal operation on first row

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

Step 2: Secondly, it will scan the pixels from top to bottom in vertical direction. It will also perform the addition and subtraction operations on neighboring pixels and then it stores the sum on the top and the difference on the bottom as illustrated in Figure 2. Repeat this operation until all the columns process is complete. Finally we will obtain 4 subbands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and it looks very similar to the original image. The whole procedure described is called the first-order 2-D Haar-DWT.

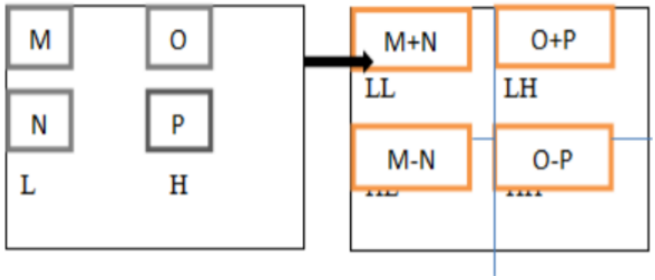

Figure 2: The vertical operation

Algorithm to retrieve the text message:-
Step 1: Read the cover image and text message that has to be hidden in the cover image.
Step 2: Convert the text message into binary. Apply 2D-Haar transform on the cover image.
Step 3: Obtain horizontal and vertical filtering coefficients of the cover image and the cover image is then added with data bits for DWT coefficients.
Step 4: Obtain stego image.
Step 5: Calculate the Mean square Error (MSE) and Peak signal to noise ratio (PSNR) of the stego image.

Algorithm to retrieve text message:-
Step 1: Read the stego image.
Step 2: Obtain horizontal and vertical filtering coefficients of the cover image and then extract the message bit by bit and recomposing the cover image.
Step 3: Convert the data into a message vector and then compare it with original message.[2] 2. Evaluation of Image Quality: [2] For comparing the stego image with cover results it requires a measure of image quality and the commonly used measures are Mean-Squared Error, Peak Signal-to-Noise Ratio and capacity.
The DWT of the original signal is then obtained by concatenating all coefficients starting from the last level of decomposition (remaining two samples, in this case). The DWT will then have the same number of coefficients as the original signal.

V. METHODOLOGY

The following algorithm approach hides the message or image in a cover image assuming that image is 24-bit. The same algorithm approach can be applied to any bit image. In 24-bit image, each pixel is represented as three layers with colors Red, Green and Blue (8-bits each).

a. Convert the message or image into its binary form. Similarly convert the cover image into binary format. Now, when the cover image is converted into binary format, it is assumed to be represented as three layers image as shown below.

b. Using the dimensions (width and height) of the cover image, find the centre of the image to be used to choose the pixels that would be used to hide the text message or image.

c. Calculate the length (as radius) on the basis of width or height of the cover image whichever less is. Take the radius as the integer number of half of (width-I) or (height-I) whichever is chosen for fmding the radius.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

d. As shown in Fig. 3, keep on fmding and storing the pixels in an array in clockwise fashion that lie on the circumference of the circle with the specified centre and radius of the circle using midpoint circle approach.

e. Fig. 4 show the three components red, green and blue in binary format, we are storing for a single pixel. If we have n pixels on the circle, then the array will have 3 * n bytes.

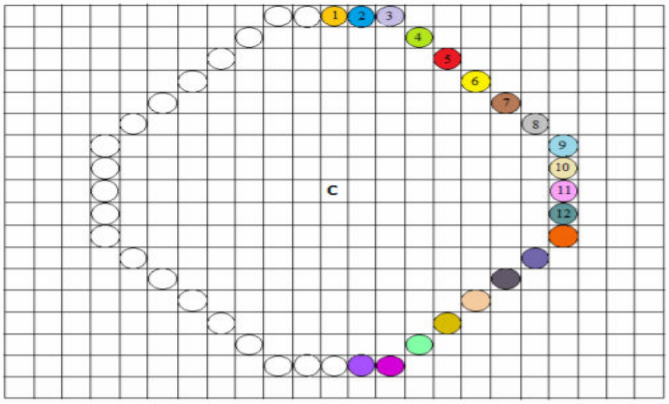

Figure 3: Selection of pixels using mid-point circle approach.

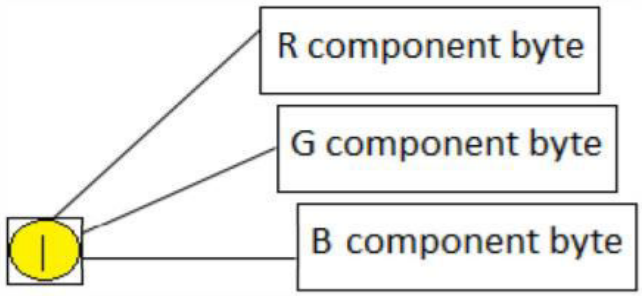

Figure 4: Pixel with three components.

VI. CONCLUSION

We have surveyed the two algorithms that are commonly used in the previous paper. From one of previous paper the evaluation done for image quality result states that the PSNR of LSB is high compared to DWT. That proves DWT is highly robust method compared to LSB because the image is not destroyed on extracting the message hidden in it and provides the maximum security. In future we are trying to implement and perform comparative analysis on LSB and DWT algorithm. Considering the parameters like PSNR, MSE, Robustness & Capacity on the different images and the results are evaluated to check best quality of Images having high PSNR ratio.

REFRENCES

[1] N. Senthil Kumaran, and S. Abinaya, "Comparison Analysis of Digital Image Watermarking using DWT and LSB Technique", International Conference on Communication and Signal Processing, April 6-8, 2016, India.
[2] Aase, S.O., Husoy, J.H. and Waldemar, P., A Critique of SVD-Based Image Coding Systems, IEEE International Symposium on Circuits and Systems VLSI, Orlando, FL, Vol. 4, Pp. 13-16.
[3] Ahmed, F. and Moskowitz, I.S. (2014) Composite Signature Based Watermarking for Fingerprint Authentication, ACM Multimedia and Security Workshop, New York, Pp.1-8.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

[4] Akhaee, M.A., Sahraeian, S.M.E. and Jin, C. (2013) Blind Image Watermarking Using a Sample Projection Approach, IEEE Transactions on Information Forensics and Security, Vol. 6, Issue 3, Pp.883-893.
[5] Ali, J.M.H. and Hassanien, A.E. (2012) An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory, Advanced Modeling and Optimization, Vol. 5, No. 2, Pp. 93-104.
[6] Al-Otum, H.M. and Samara, N.A. (2009) A robust blind color image watermarking based on wavelet-tree bit host difference selection, Signal Processing, Vol. 90, Issue 8, Pp. 2498-2512.
[7] Ateniese, G., Blundo, C., De Santis, A. and Stinson, D.R. (1996) Visual cryptography for general access structures, Information Computation, Vol. 129, Pp. 86-106.
[8] Baaziz, N., Zheng, D. and Wang, D. (2011) Image quality assessment based on multiple watermarking approach, IEEE 13th International Workshop on Multimedia Signal Processing (MMSP), Hangzhou, Pp.1-5.
[9] Bao, F., Deng, R., Deing, X. and Yang, Y. (2008) Private Query on Encrypted Data in Multi-User Settings, Proceedings of 4th International Conference on Information Security Practice and Experience (ISPEC 2008), Pp. 71-85, 2008.
[10] Barni, M. and Bartolini, F. (2004) Watermarking systems engineering: Enabling digital assets security and other application, Signal processing and communications series, Marcel Dekker Inc., New York.
[11] Barni, M., Bartolini, F. and Piva, A. (2001) Improved Wavelet based Watermarking Through Pixel-Wise Masking, IEEE Transactions on Image Processing, Vol. 10, Pp. 783-791.