International Journal of Computer Applications Technology and Research
Volume 5– Issue 9, 561 - 567, 2016, ISSN:- 2319–8656

Image Steganography using Fusion Based Advanced Encryption Algorithm and Embedding Techniques

Venkateshappa
Research Scholar
M.S Engineering College
Bengaluru-562110, Karnataka,
India

Sunitha.P.H
Research Scholar
M.S Engineering College
Bengaluru-62110, Karnataka,
India.

Gopala Krishna Murthy.CR
Electronics and
Communication
KSSEM, Bengaluru

Abstract: In real time application of transmitting data through internet or web encryption plays a vital role. Data that is being transmitted will be encrypted in order to be protected from the hackers. When data is sent through internet it can be viewed by number of people. The data transmitted first moves to the local network and then to internet service provider, who will be able to view your message. After this the data travels through number of routers to reach the internet service provider of the recipient. During this process data can be accessed by numerous people. Hence, we need to encrypt the data or message that is being transmitted. Encryption can be done by several techniques and different algorithms. This project will embed three different techniques to increase the level of security provided to the data. Haar DWT and Average alpha blending are the techniques used along with that LSB encryption algorithm is used. In all existing techniques lift DWT was widely used where, it produces a negative co-efficient. Handling negative co-efficient will degrade the PSNR value of the restored image at receiver side. Hence, it is replaced by Haar DWT. Haar wavelet will be implemented on the input image which provides one level security and using LSB algorithm where output of Haar wavelet pixel values are altered by pixel values of cover image used. This step provides two level security. Average blending is done at the last level so that levels of security are increased again and also speed is increased area is minimized. In this project using all techniques mentioned above, security is increased and use of Haar wavelet will also increase PSNR value.

Keywords: DWT, Haar wavelet, LSB technique, average embedding technique

1. INTRODUCTION:

In present era security is important issue in communication and storage of information, images, audio and videos. This must be protected from mischiefs, it is applied to any vulnerable and precious resources. rseparation is done between the resources and risk. Security is important in many fields such as home security, computer security, banking security, information security, etc. Home security: Home security is applicable to all of us. The home consists of many things which must be secured. Example: the widows must be closed, doors must be locked properly. Security is important to avoid a robbery.

Computer security: Computer security is also called as cyber security, IT security. Security is applied to processing devices such as computers and Smartphone and also computer networks. Computer security includes five components they are: hardware, software, data, people and procedures by which information is restricted to the unauthorized access. It also includes physical and information security, physical security is to prevent the theft of equipment. Information security is to protect the data on the equipment.

Banking security: In a core banking system, there is Chance of encountering forged signature for transaction and in the net banking system, the password of customer may be hacked and miss-used. Thus, security is still a challenge in these applications. The main aim is to secure he customer information and to prevent the possible forgery of password hacking.

Information security: In the present situation the use of internet is being increased rapidly. The innovation of the technology has lead to increase in the speed of transmission of data through communication channel which is easily exposed to the unauthorized person. Hence, there is a need for safeguarding individual's creation from the copyright. This can be done through a technique called Digital watermarking.

The Haar wavelet is a rescaled sequence "square–shaped" functions form a wavelet family or basis. The Haar sequence is now well-known as the first wavelet. Alfred Haar proposed Haar sequence in 1909, he used this function to give an example of an orthonormal system. Haar wavelet is also the simplest possible wavelet, it has orthonormal properties.

Alpha blending technique is used to blend or to insert the watermarked image. Cover image and watermarked image which is obtained after application of Haar DWT, they multiplied by a scaling factor and are added.

Data hiding in a grey scale image using LSB technique is simply replacing the LSB bits of the host image with the cover image. Each equivalent pixel of host image and each equivalent pixel of cover image are considered and then the LSB of the host is replaced by the LSB of the cover image it means that embedding the secret information in to the cover image. By making use of this technique the security enhances there by it is difficult for an unauthorized person to decrypt the secret information or image.

2. LITERATURE REVIEW

Steganography is masking of a file, message, image, or video. In this paper the Steganography is done on the boundary. This boundary based Steganography or steganalysis uses an auto-aggressive model [1].

Growing technology has made rapid increase in usage of internet. The advanced technology has lead to transmission of data through network which is easily exposed to the unauthorized person. Hence, there is a need for safeguarding individual's creation form copyright. This can be done through a technique called Digital Watermarking [2].

to enhance the security in a digital image captured by camera. As the image capturing has become passion for few people they wanted to publish their photography. But when there is mislead to tracking to theft the photograph would lead to great loss to that person. Hence the data must be secured carefully. Singular value decomposition (SVD) and DWT [3] is applied on the watermark of a RGB domain.

The Endeavour of this project is to detect the outcome of PSNR value by making use of implementing 5/3 2D lift DWT based watermarking technique [1], The expelled data during transmission and reception is preserved to its minimal by a technique called Alpha blending and resizing.

Compression of image and video now-a-days is unarguable. For different input patterns the multi level 2D DWT perform several computations for execution. The designs made used are 6 row-columns line-based and block-based [4].

The main criteria of the paper is to reduce the bandwidth of the image during transmission wavelet based technique such as JPEG2000 for image compression is the best method in compressing ratio[5].

The objective of this paper is to detect the power dissipation during data hiding using 2D-DWT using lifting technique. They have used a CoDel language which is a procedural language to order the statements implicitly represents the sequence of the activities[6][7].

In this paper they have made use of improved LSB based Steganography technique for image which gives better security. In the edges and sooth area of an image the secrete image or message is being hided in non-adjacent and random pixel locations. By making use of edge detection filter, the edges of the cover image is being detected and encrypted secrete image's edges will be replaced at the LSB of the cover image i.e., red, blue, green pixel components on randomly selected pixels on smooth area of the image [8][9][10][12].

The techniques used in this design are LSB, DCT and compression technique on row image. Steganography is nothing but hiding an image with in another image or video, text, etc. LSB technique [11] is to embed the payload bits in to the cover image which forms a stego image.

The paper explains that the image is hided in a frame of video they have made use of algorithm called frame decomposition technique. They have used three techniques that color map matrix of RGB image, LSB, CDT of RGB image and unique matrix of RGB image. The output of CDT will have some limitation that is the image has maximum of 255 pixel values after the application of CDT maximum pixel value will be 255 only for a single image. As the Steganography is done on the image and a video by CDT [13].

Amid the embedding process we will see that the size of the watermark is smaller than the cover image. Here the edge size of both the watermark image and host image are made equal. Since the watermark embedded in this paper is recognizable in nature or unmistakable, it is inserted in the low frequency approximation component of the host image. After alpha blending technique we will acquire the watermarked image which comprises of the original watermark along with the original image [15].

1.1. Summary on literature review

From the above review we came to conclusion that the image Steganography is carried out using digital watermarking, LSB technique, DWT, Alpha blending using multipliers and adders, lifting DWT. The security of the image is enhanced and proved that the encryption technique does not degrade the image quality by making a comparison with the PSNR values between the input secret image and the decrypted secret image. The PSNR value of the image can still be increased by making use of Haar DWT and by making use of Average Alpha blending using multipliers.

2.2. Speed is increased and the area utilization will be less when compared with normal alpha blending technique using adders. Hence an area and security efficient architecture of image Steganography is proposed. Limitations of Existing Systems

By making use of 5/3 lift DWT negative co-efficient results so there by Haar DWT will eliminate the negative co-efficient. Edge details are taken in to consideration and the security is enhanced but most of the information will be present in LL band so concentrating mainly on the major part of the information which is LL band and the security will be enhanced. Alpha blending technique uses more bit storage area. Therefore using average embedding algorithm which reduces the bit storage values and results in reduction of memory.

.

3.DESIGN AND IMPLEMENTATION

3.1. General Block Diagram

Steganography of an image includes a series of steps. The general block diagram for increasing the security of communication is shown below in figure 1, where each and every block will be elaborated.

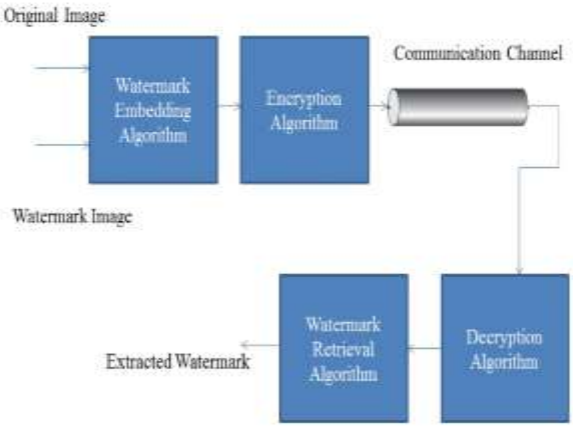

Figure 1 General block diagram

Initially the original image (secrete image) and watermarked image(cover image) is fed to the watermark embedding algorithm. Here, the embedding algorithm is LSB technique. The output of the embedding algorithm is then fed to encryption algorithm which is average embedding algorithm. The output of the encryption algorithm is passed through communication channel, it can internet or LAN, etc. At the other end decryption of all these algorithm is done by knowing which are techniques that is being used. Finally the image will be extracted.

3.2 . Proposed Model

The proposed model is as shown below in figure 2. DWT is nothing but the size of the image is compressed to increase the security Haar wavelet co-efficient are made used. To get the better performance additional technique is included that is LSB technique. The output of this LSB technique will be passed to average embedding algorithm which is also known as average embedding algorithm.

The next step is to verify the quality of images; the PSNR value is calculated between the watermarked images also known as encrypted image and the cover image. This forms a transmitter section encryption. To pass this encrypted image the size of the image should be as same as the original image, so applying inverse DWT and then passing it through the communication channel.

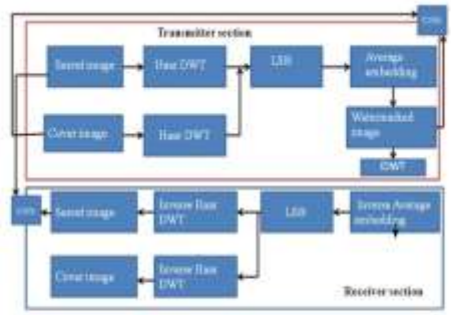

Figure 2 Proposed Model

The decryption must be done at the receiver section by applying inverse of all the techniques used, by doing this, the encrypted image will be retrieved. Finally, to know the percentage of security enhancement PSNR value will be calculated between the secrete image and retrieved secrete image and also between the cover image and retrieved cover image.

3.3 Haar DWT

DWT is nothing but Discrete Wavelet Transform, application of DWT to the image is to compress the size of it. The signals that are generated are translated into shifted and scale versions of the mother wavelet to generate DWT bands. Depending upon the wavelets chosen the security also increases. In this project Haar DWT is used to enhance the performance in terms of PSNR value and scaling the area.

Taking finger print as an example, decomposition of 2D Haar DWT is shown in figure 3.8.

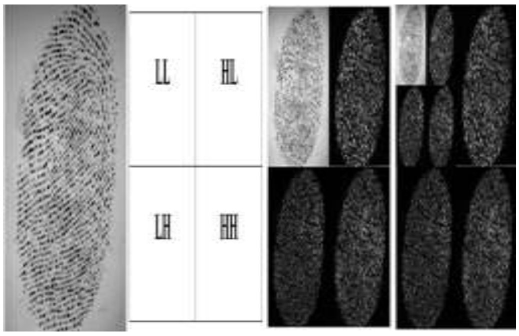

Figure 3 2D-DWT decomposition

The decomposition of fingerprint using DWT at two levels is shown in Figure 3.

The Haar wavelet has orthonormal properties i.e., orthogonal with unit vectors which is used as the mother wavelet and has simplest useful energy compression process. The Haar transformation of one dimensional input leads to two vector elements that is given by the equation 3.1.

$$\left(y(1), y(2)\right) = T\left(X(1), X(2)\right) \ldots\ldots\ldots\ldots\ldots\ldots 3.1$$

Where $T = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$is the Haar operator

y(1) and y(2) are sum and difference of x(1) and x(2) which produce low pass and high pass filtering respectively, it is scaled by 1/$\sqrt{2}$ to preserve the energy.

The Haar operator T is an orthonormal matrix since its rows are orthogonal to each other that is their dot products are zero and have unit lengths, therefore $T^{-1}=T^{T}$. Hence we may recover x from y using equation 3.2.

$$\left(x(1), x(2)\right) = T^{T}\left(Y(1), Y(2)\right) \ldots\ldots\ldots\ldots\ldots\ldots\ldots .3.2$$

For 2D image, Let *x* be 2×2 matrix of an image, the transformation *y* is obtained by multiplying columns of x by T, and then the rows of the result by multiplying by T^{T} using equation 3.3.

$$y = T * x * T^{T} \ldots\ldots\ldots\ldots\ldots\ldots\ldots 3.3$$

The original values are recovered using equation 3.4

$$x = T^{T} * y * T \ldots\ldots\ldots\ldots\ldots\ldots\ldots 3.4$$

An Example of DWT,

If $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is the original matrix, then DWT is given in equation 3.5.

Then

$$y = \frac{1}{2}\begin{pmatrix} a+b+c+d & a-b+c-d \\ a+b-c-d & a-b-c+d \end{pmatrix} \ldots\ldots\ldots\ldots\ldots\ldots\ldots 3.5$$

The DWT bands correspond to the following filtering processes:

LL: a+b+c+d : Low pass filtering in horizontal as well as vertical direction.

HL: a−b+c−d : High pass filtering in horizontal direction and Low pass filtering in vertical direction.

LH: a+b−c−d : Low pass filtering in horizontal and High pass filtering in vertical.

HH: a−b−c+d : High pass filtering in both horizontal and vertical direction.

To use this transform to a complete image, the pixels are grouped into 2x2 blocks and transformations are obtained using equation 3.5 for each block. The 2 level DWT is applied on fingerprint image of size 256x256 to obtain 128x128 coefficients after first level and 64x64 coefficients after second level stage. The 64x64 LL sub-band coefficients are considered as DWT features. Haar DWT is as shown in figure 4.

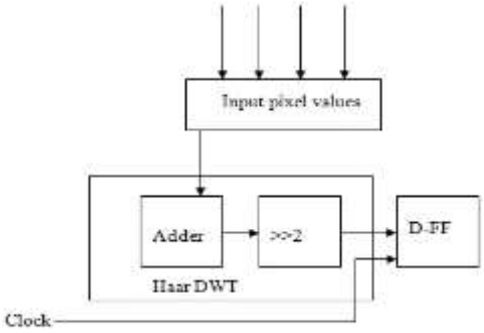

Figure 4 Block diagram of Haar DWT

3.4. LSB Technique

Least Significant Bit is encryption algorithm used to improve the security of communication through a communication channel. Taking two images that is one image is cover image and the other is a secrete image the operation will be performed. The idea behind this technique is to embed or hide the secrete image in a cover image. Embedding the image in an image is nothing but replacing the LSB of cover image with the MSB of secret image where LSB of secret image acts as a key. These bit values will be obtained from the previously obtained output that is from the Haar DWT output. The input to the LSB is the output of Haar DWT where the image size that is 256x256 of both cover and secret will be compressed to 128x128. At every clock cycle the input will be given to LSB technique from Haar DWT. At each and every clock cycle the pixel value gets encrypted. This operation continues till the complete image pixel value is covered that is 128x128.

For example: let the pixel value of cover image be 128 and 115 of secret image.

The binary equivalent of the pixel values are:

128:-10000000 and 115:-01110011

LSB algorithm:-10000000=cover image pixel

01110011=secret image pixel

10000111=embedded pixel

The decimal equivalent of embedded pixel value is 67 and 3 is the key for that pixel. Same process will be held to compute the entire pixels value to embed.

4. RESULTS AND DISCUSSION

A. Simulation Output for Haar DWT

The output of Haar DWT is shown in figure 5.

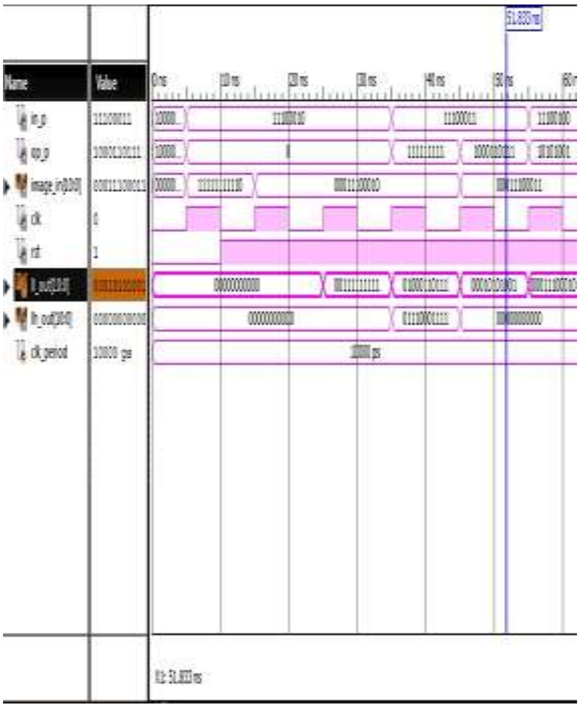

Figure 5 waveform of Haar DWT

4.1. Simulation Output of LSB Technique

The simulation output of LSB technique is show in figure 6.

Figure 6 waveform of LSB technique

4.2. Software implementation

The software implementation using system generator for Haar DWT is as shown in figure 7.

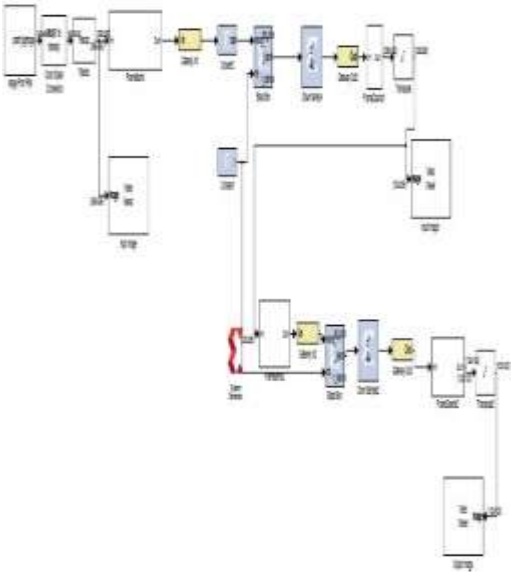

Figure 7 software implementation of Haar DWT

The software implementation using system generator for LSB is as shown in figure 8.

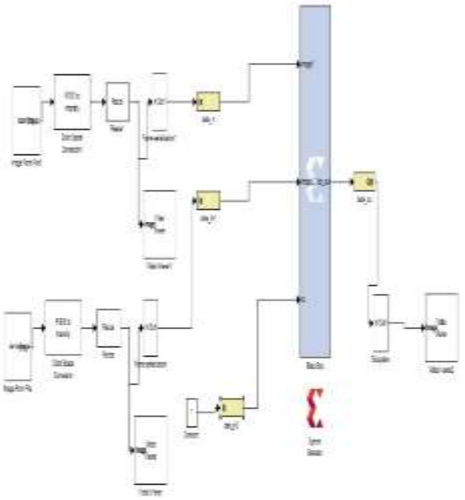

Figure 8 software implementation of LSB technique

4.3.Output of Haar DWT using system generator

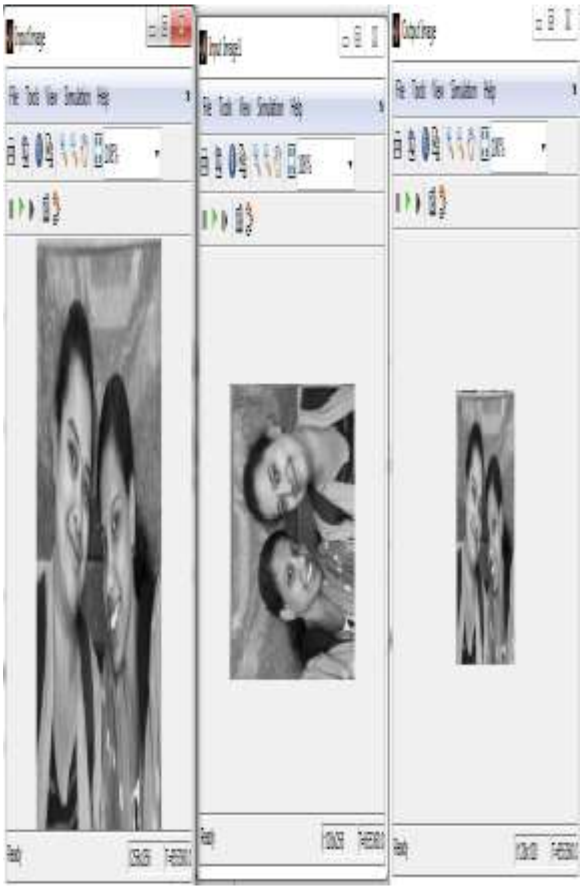

Figure 9 output image of Haar DWT

4.4. Output of LSB using system generator

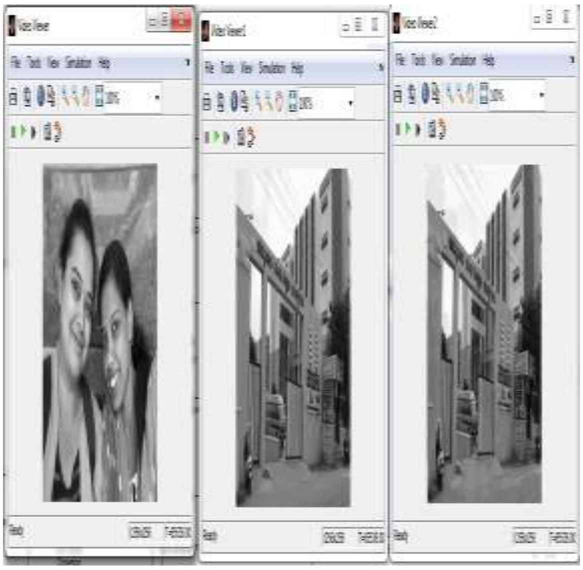

Figure 10 output image of LSB technique

5. CONCLUSION AND FUTURE SCOPE

The proposed paper embedded different techniques for encryption of a image. Since application of only DWT and average blending was producing a single level security. Now, in this it gives a 2-level security.

In future, the same techniques will be applied for decrypting the secrete image by applying the inverse of the algorithms and techniques used for encryption. Further this can also be used for video file steganography.

6. REFERENCE

[1] B.Pushpalatha, Mrs. Shalini Shravan, "An Efficient 2D 5/3 Lift DWT Based Invisible Watermarking Technique", National Conference at KSSEM 2015.

[2] M. Jiang, X Wu, E. K. Wong, and N. Meinon, "Steganalysis of Boundary-based Steganography using Autoregressive Model of Digital Boundaries", IEEE International Conference on Multimedia and Expo (ICME) 2004.

[3] Shaifali Bhatnagar, Shishir Kumar, Ashish Gupta, "An Approach of Efficient and Resistive Digital Watermarking using SVD", 978-1-4799-3080-7/14/c IEEE 2014.

[4] Maria E. Angelopoulou And Peter Y. K. Cheung, "Implementation and Comparison of the 5/3 Lifting 2D Discrete Wavelet Transform Computation Schedules on FPGAs", Journal of VLSI Signal Processing 2007) 2007 Springer Science + Business Media, LLC. Manufactured in The United State. DOI: 10.1007/s11265-007-0139-5.

[5] Jinal Patel, Ketki Pathak," Implementation of the 5/3 Lifting 2D Discrete Wavelet Transform", © 2014 IJEDR | Volume 2, Issue 3 | ISSN: 2321-9939.

[6] Nainesh Agarwal, Nikitas Dimopoulos, "Power Efficient Rapid System Prototyping Usig Codel; The 2D DWT Using Lifting", 0-7803-9195-0/05/© IEEE 2005.

[7] Nainesh Agarwa, Nikitas Dimopoulos, "Rapidly Prototyping DSP Extensions Using CoDeL: The DWT Using Lifting", 0-7803-8886-0/05/ ©2005 IEEE CCECE/CCGEI, Saskatoon, May 2005.

[8] Mamta Juneja and Parvinder S. Sandhu, "An Improved LSB Based Steganography Technique for RGB Color Images", International Journal of Computer and Communication Engineering, Vol. 2, No. 4, July 2013.

[9] Shamim Ahmed Laskar and Kattamanchi Hemachandran, "High Capacity data hiding using LSB Steganography and Encryption", International Journal of Database Management Systems (IJDMS) Vol.4, No.6, December 2012.

[10] Basant K. Mohanty and Promod K.Meher, "Pipelined Architecture for High-Speed Implementation ofMultilevel Lifting 2-D DWT using 9/7 Filters", 1-4244-0969-1/07/©C IEEE 2007.

[11] K.B.Raja, C.R.Chowdary, Venugopal K R, L.M.Patnaik, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images", 0-7803-9588-3/05/ © IEEE 2005.

[12] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A New Approach for LSB Based Image Steganography using Secret Key", 987-161284-908-9/11/ IEEE 2011.

[13] Saket Kumar, Ajay Kumar Yadav, Ashutosh Gupta, Pradeep Kumar, "RGB Image Steganography on Multiple Frame Video using LSB Technique", 978-1-4799-1819-5/15/© IEEE 2015.

[14] G. Raj Kumar, M. Maruthi Prasada Reddy, T. Lalith Kumar , "An Implementation of LSB Steganography Using DWT Technique", International Journal of Engineering Research and General Science Volume2,Issue6,October-November,2014 ISSN 2091-2730.

[15]Manpreet Kaur and Sheenam Malhotra,, " Review Paper on Digital Image Watermarking Technique for Robustness", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4,Issue 5, pp 948-952, May 2014.