HIGH CAPACITY AND SECURITY STEGANOGRAPHY USING DISCRETE WAVELET TRANSFORM

H S Manjunatha Reddy manjunathareddyhs @rediffmail.com

Dept. of Electronics and Communication
Global Academy of Technology, Bangalore, India-560098

K B Raja raja_kb@yahoo.com

Dept. of Computer Science and Engg
University Visvesvarya College of Engg,
Bangalore University, Bangalore-01

Abstract

The secure data transmission over internet is achieved using Steganography. In this paper High Capacity and Security Steganography using Discrete wavelet transform (HCSSD) is proposed. The wavelet coefficients of both the cover and payload are fused into single image using embedding strength parameters alpha and beta. The cover and payload are preprocessed to reduce the pixel range to ensure the payload is recovered accurately at the destination. It is observed that the capacity and security is increased with acceptable PSNR in the proposed algorithm compared to the existing algorithms

Keywords: Steganography, Wavelet Fusion, Security, Embedding strength parameters, Imperceptibility.

1. INTRODUCTION

The development in technology and networking has posed serious threats to obtain secured data communication. This has driven the interest among computer security researchers to overcome the serious threats for secured data transmission. One method of providing more security to data is information hiding. The approach to secured communication is cryptography, which deals with the data encryption at the sender side and data decryption at the receiver side. The main difference between steganography and cryptography is the suspicion factor. The steganography and cryptography implemented together, the amount of security increases. The steganography make the presence of secret data appear invisible to eaves droppers such as key loggers or harmful tracking cookies where the users keystroke is monitored while entering password and personal information. The Steganography is used for secret data transmission. Steganography is derived from the Greek word steganos which means “covered” and graphia which means “writing”, therefore Steganography means “covered writing”. In steganography the secret image is embedded in the cover image and transmitted in such a way that the existence of information is undetectable. The digital images, videos, sound files and other computer files can be used as carrier to embed the information. The object in which the secret information is hidden is called covert object. Stego image is referred as an image that is obtained by embedding secret image into covert image. The hidden message may be plain text, cipher text or images etc. The steganography method provides embedded data in an imperceptible manner with high payload capacity. Encrypting data provides data confidentiality, authentication, and data integrity.

Steganography, copyright protection for digital media and data embedding are the data hiding techniques. Steganography is a method of hiding secret information using cover images. Copyright marking classified into watermarking and fingerprinting. Watermarking is the process of possibly irreversibly embedding information into a digital signal. The signal may be audio, pictures or video etc. Fingerprinting attaches a serial number to the copy of digital media. Copyright protection prevents illegal transfer of data. In data embedding systems the receiver will know about the hidden message and the task is to decode the message efficiently. The main aspect of steganography is to achieve high capacity, security and robustness. Steganography is applicable to (i) Confidential communication and secret data storing, (ii) Protection of data alteration, (iii) Access control system for digital content distribution, (iv) Media Database systems etc.

The various steganographic techniques are: (i) Substitution technique: In this technique only the least significant bits of the cover object is replaced without modifying the complete cover object. It is a simplest method for data hiding but it is very weak in resisting even simple attacks such as compression, transforms, etc. (ii)Transform domain technique: The various transform domains techniques are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Fast Fourier Transform (FFT) are used to hide information in transform coefficients of the cover images that makes much more robust to attacks such as compression, filtering, etc. (iii) Spread spectrum technique: The message is spread over a wide frequency bandwidth than the minimum required bandwidth to send the information. The SNR in every frequency band is small. Hence without destroying the cover image it is very difficult to remove message completely. (iv)Statistical technique: The cover is divided into blocks and the message bits are hidden in each block. The information is encoded by changing various numerical properties of cover image. The cover blocks remain unchanged if message block is zero. (v) Distortion technique: Information is stored by signal distortion. The encoder adds sequence of changes to the cover and the decoder checks for the various differences between the original cover and the distorted cover to recover the secret message.

Steganalysis is the science of detecting hidden information. The main objective of Steganalysis is to break steganography and the detection of stego image is the goal of steganalysis. Almost all steganalysis algorithms rely on the Steganographic algorithms introducing statistical differences between cover and stego image. Steganalysis deals with three important categories: (a) Visual attacks: In these types of attacks with a assistance of a computer or through inspection with a naked eye it reveal the presence of hidden information, which helps to separate the image into bit planes for further more analysis. (b) Statistical attacks: These types of attacks are more powerful and successful, because they reveal the smallest alterations in an images statistical behavior. Statistical attacks can be further divided into (i) Passive attack and (ii) Active attack. Passive attacks involves with identifying presence or absence of a covert message or embedding algorithm used etc. Mean while active attacks is used to investigate embedded message length or hidden message location or secret key used in embedding. (c) Structural attacks: The format of the data files changes as the data to be hidden is embedded; identifying this characteristic structure changes can help us to find the presence of image.

2. RELATED WORK

Neil F. Johnson and sushil jajodia et al., [1] have provided several characteristics in information hiding methods to identify the existence of a hidden messages and also identify the hidden information. The images are reviewed manually for hidden messages and steganographic tool to automate the process. The developed tool is to test robustness of information hiding techniques in images such as warping, cropping rotating and blurring. Lisa M. Marvel and Charles T. Retter [2] have presented a method of embedding information within digital images, called Spread Spectrum Image Steganography (SSIS). SSIS conceals a message of substantial length with in digital images while maintaining the original image size and dynamic range. A hidden message can be recovered using the appropriate keys without any knowledge of the original image. Giuseppe Mastronardi et al., [3] have studied the effects of Steganography in different image formats (BMP, GIF, JPEG and DWT) and proposed two different approaches for lossless and lossy image. They are based on the creation of an “adhoc” palette for BMP and GIF images. LUI Tong and QIU Zheng-ding [4] have proposed a Quantization-based Steganography scheme. In this method the secret message is hidden in every chrominance component of a color image and the hiding capacity is higher than that of the popular Steganography software. Since the

Quantization-based hiding method is free from the interference and simulation results the hidden message can be extracted at low BER and our scheme is robust to common attacks.

Jessica Fridrich et al., [5] have proposed a new higher-order Steganalytic method called Pairs Analysis for detection of secret messages embedded in digital images. Although the approach is in principle applicable to many different Steganographic methods as well as image formats, it is ideally suited to 8-bit images, such as GIF images, where message bits are embedded in LSBs of indices to an ordered palette. The Ezstego algorithm with random message and optimized palette order is used as an embedding archetype on which we demonstrate Pairs Analysis and compare its performance with the chi-square attacks. Jessica Fridrich and David Soukal [6] have presented two approaches to matrix embedding for large payloads suitable for practical steganographic schemes – one based on family of codes constructed from simplex codes and the second one based on random linear codes for small dimension .The embedding efficiency of the proposed methods is evaluated with respect to theoretically achievable bounds. Yuan-Yu Tsai and Chung-Ming Wang [7] have proposed a novel data hiding scheme for color images using a BSP tree. This method shows high capacity with little visual distortion. Furthermore, there is an advantage of the tree data properties to improve the security of embedding process, making it difficult to extract the secret message without the secret key provided. Jun Zhang et al., [8] have proposed detection of steganographic algorithms based on replacement of the Least Significant Bit (LSB) plane. Since LSB embedding is modeled as an additive noise process, detection is especially poor for images that exhibit high-frequency noise.

M. Mahdavi et al., [9] presented a steganalysis method for the LSB replacement. The method is based on the changes that occur in histogram of an image after the embedding of data. It is less complex and more accurate than the RS steganalytic method for the images which are acquired directly from scanner without any compression. The RS method needs to count the number of regular and singular groups twice and also require LSB flipping for the whole image. This method has better average and variance of error comparing to RS steganalytic method. Shilpa p. Hivrale et al., [10] have presented various statistical measures and PMF based method of detection. It uses the frequency count of the pixel intensities in the image to test for the detection of stego image or not. Here LSB embedding technique is used. K. B. Raja et al., [11] have proposed a novel image adaptive stegnographic technique in the integer wavelet transform domain called as the Robust Image Adaptive Steganography using Integer Wavelet Transform. According to information theoretic prescriptions for parallel Gaussian models of images, data should be hidden in low and mid frequencies ranges of the host image, which have large energies. Jan Kodovsky and Jessica Fridrich [12] worked out the specific design principles and elements of steganographic schemes for the JPEG format and their security. The detect ability is evaluated experimentally using a state of art blind steganalyser. L.Y. Por et al., [13] have proposed a combination of three different LSB insertion algorithms on GIF image through stegcure system. The unique feature about the stegcure is being able to integrate three algorithms in one Steganography system. By implementing public key infrastructure, unauthorized user is forbidden from intercepting the transmission of the covert data during a communication because the stego-key is only known by the sender and the receiver. Gaetan Le Guelvoit [14] proposed a work which deals with public- key Steganography in presence of passive warden. The main aim is to hide the secret information within cover documents without giving the warden any clue and without any preliminary secret key sharing. This work explores the use of trellis coded quantization technique to design more efficient public key scheme.

Mohammad Ali Bani Younes and Aman Jantan [15] have proposed a steganographic approach for data hiding. This approach uses the least significant bits (LSB) insertion to hide data within encrypted image data. The binary representation of the data is used to overwrite the LSB of each byte within the encrypted image randomly. The hidden data will be used to enable the receiver to reconstruct the same secret transformation table after extracting it and hence the original image can be reproduced by the inverse of the transformation and encryption processes. Chang-Chu Chen and Chin-Chen Chang [16] have proposed that data hiding scheme is a modification of the LSB-based steganography using the rule of reflected gray code. The embedding ability and distortion level of our novel method are similar to those of the simple LSB substitution scheme. The difference is that the LSBs of stego-image are not always the same as the secret bits while the simple LSB substitution keeps them equally. Babita Ahuja and, Manpreet Kaur [17] have presented LSB based steganography algorithm with high data hiding capacity, as four LSB's are used to hide data, high confidentiality as distortions which can cause suspiscions for the intruders, are removed through filtering techniques and two level high security is applied. Debnath Bhattacharyya et al., [18] a security model is proposed which imposes the concept of secrecy over privacy for text messages. The proposed model combines cryptography, steganography and along with an extra layer of security has been imposed in between them. Chin-Chen Chang et al.,[19] proposed a scheme embeds a larger-sized secret image while maintaining acceptable image quality of the stego-image and also improved image hiding scheme for grayscale images based on wet paper coding.

3 MODEL

The definitions, Wavelet Transform and HCSSD model are described in this section.

Definitions:

- *Cover Image*: It is defined as the original image into which the required secret message is embedded. It is also termed as innocent image or host image. The secret message should be embedded in such a manner that there are no significant changes in the statistical properties of the cover image. Good cover images range from gray scale image to colored image in uncompressed format.
- *Payload:* It is the secret massage that has to be embedded within the cover image in a given Steganographic model. The payload can be in the form of text, audio, images, and video.
- *Stego image:* It is the final image obtained after embedded the payload into a given cover image. It should have similar statistical properties to that of the cover image.
- *Hiding Capacity*: The size of information that can be hidden relative to the size of the cover without deteriorating the quality of the cover image.
- *Robustness:* The ability of the embedded data to remain intact if the stego image undergoes transformation due to intelligent stego attacks.
- *Security*: This refers to eavesdropper's inability to detect the hidden information.
- *Mean Square Error (MSE)*: It is the measure used to quantify the difference between the initial and the distorted or noisy image. Let *Pi* represents the pixel of one image of size N and Q_i that of the other.

$$MSE = \sum_{i=1}^{allpixels} \sum_{i=1}^{allpixels} \frac{\left(Cover(i,j) - stego(i,j)\right)^2}{N \times N} \tag{1}$$

From MSE we can find Peak Signal to Noise Ratio (PSNR) to access the quality of the Stego image with respect to cover image given by

$$PSNR = 20\log_{10}\frac{255}{\sqrt{MSE}} \tag{2}$$

- Haar Wavelet: It is a piecewise wavelet that provides orthogonal decomposition given as

$$\psi(t) = \begin{cases} +1, & if\ 0 \le t \le 1/2 \\ -1, & if\ 1/2 \le t \le 1 \\ 0, & otherwise \end{cases} \tag{3}$$

- Wavelet Transform: It converts an image from time or spatial domain to frequency domain. It provides a time-frequency representation. The Wavelet Transform is obtained by repeated filtering of the coefficients of the image row-by-row and column-by-column.
- *Approximation Band*: It is the band having the lower frequency coefficients of the image in the wavelet domain. It contains all the significant features of the image.
- *Detail Band*: It has high frequency components of the image in the wavelet domain and consists of insignificant features of the image.
- *Payload Encryption*: Encryption of payload is done not only to protect data frame theft or alteration, but can also be used for authentication and increase security level. Secret key cryptography is used, wherein the same key is used for both encryption and decryption.

- *Inverse Wavelet Transform*: It is applied over the stego image to convert it from frequency domain to spatial domain. Hence it is frequency-time representation.
- *Fusion*: It is the process of adding the wavelet coefficients of both the Cover Image and Payload.
- *Cover-escrow*: The scheme in which the original Cover image is required at the extraction model to get the Payload.
- *Normalization*: It is the division of all the pixel values of an image in the spatial domain with the maximum pixel value of the image. For gray scale image the maximum value of any pixel is 255.
- *Preprocessing*: All the pixels of an image in spatial domain are multiplied by embedding strength factors alpha or beta.

3.1 ***Wavelet Transform***:

Wavelet transform is used to convert a spatial domain into frequency domain. The use of wavelet in image stenographic model lies in the fact that the wavelet transform clearly separates the high frequency and low frequency information on a pixel by pixel basis. Discrete Wavelet Transform (DWT) is preferred over Discrete Cosine Transforms (DCT) because image in low frequency at various levels can offer corresponding resolution needed. A one dimensional DWT is a repeated filter bank algorithm, and the input is convolved with high pass filter and a low pass filter. The result of latter convolution is smoothed version of the input, while the high frequency part is captured by the first convolution. The reconstruction involves a convolution with the synthesis filter and the results of this convolution are added. In two dimensional transform, first apply one step of the one dimensional transform to all rows and then repeat to all columns. This decomposition results into four classes or band coefficients.

The Haar Wavelet Transform is the simplest of all wavelet transform. In this the low frequency wavelet coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. The four bands obtained are approximate band (LL), Vertical Band (LH), Horizontal band (HL), and diagonal detail band (HH). The approximation band consists of low frequency wavelet coefficients, which contain significant part of the spatial domain image. The other bands also called as detail bands consists of high frequency coefficients, which contain the edge details of the spatial domain image.

Research into human perception indicates that the retina of the eye splits an image into several frequency channels, each spanning a bandwidth of approximately one octave. The single in these channels is processed independently. Similarly in a multilevel decomposition, the image is separated into bands of approximately equal bandwidth on a logarithmic scale. It is therefore expected that use of the DWT will allow independent processing of the resulting components without significant perceptible interaction between them, and hence makes the process imperceptibility marking more effective. For this reason the wavelet decompositions is commonly used for the fusion of images. Fusion technique include the simple method of pixel averaging to more complicated methods such as principal component analysis and wavelet transform fusion. Several approaches to image fusion can be distinguished; depending on whether the image is fused in the spatial domain or any other domains, and their transform fused. Image fusion is a process that produces a single image from a set of input images. The fused image contains more complete information, than any individual input. Since this is a sensor-compresses information problem, it follows that wavelets, classically useful for human visual processing, data compression and reconstruction are useful for such merging. Other important applications of the fusion of images include medical imaging, microscopic imaging, remote sensing, computer vision and robotics.

3.2 ***High Capacity and Security Steganography using Discrete wavelet transform model (HCSSD)***

(i) HC*SSD Encoder:* Figure 1 shows the block diagram of the embedding algorithm. The main idea behind the proposed algorithm is wavelet based fusion. It involves merging of the wavelet decomposition of the normalized version of both the cover image and the payload into a single fused result. Normalization is done so that the pixel range of the image lies between 0.0 to 1.0 instead of the integer range (0, 255). Hence we convert the integer range (0, 255) of pixels into floating point values between 0.0 and 1.0. This normalized pixel values is fed as input to the floating point filters which results in reconstruction of the transformed image with better accuracy compared to direct integer values of the pixels as input. Normalization is a process on both the cover image and the payload in order to guarantee pixel values do not exceed their maximum value of one due to modifying corresponding coefficients of the cover image and payload during fusion. Both cover image and payload is convert into DWT domain. Further, apply DWT on the payload in order to increase the security level. The single fused resultant matrix is obtained, by the addition of wavelet coefficients of the respective sub-bands of the cover image and payload is given by the Equation (4).

$$F(x,y) = \alpha C(x,y) + \beta P(x,y) \tag{4}$$

$$\alpha + \beta = 1 \tag{5}$$

Where F is modified DWT coefficients, C is the original DWT coefficients and P is the approximation band DWT coefficients of the payload. Also alpha and beta are the embedding strength factors. Since alpha and beta are chosen such that the payload is not predominantly seen in the Stego

image obtained in the spatial domain and also for full utilization of the bandwidth of both the Cover Image and the payload. Once fusion is done, we apply Inverse Discrete Wavelet Transform (IDWT) followed by renormalization to get the Stego image in the spatial domain.

ii) HCSSD Decoder: Figure 2 shows the block diagram for retrieval of payload from the Stego image. The Stego image is normalized, and then DWT is taken. The extraction process involves subtracting the DWT coefficients of the original cover image from the DWT coefficients of the Stego image. It is then followed by decryption of the subtracted coefficients. Then first step of IDWT on these coefficients is applied followed by second IDWT only with respect to the approximation band of the first IDWT coefficients of the payload. Finally, denormalization is done to get back the payload in spatial domain.

4. ALGORITHM

4.1 Problem definition

Given a cover image *c* of size (n * m) and payload *p* of size (2n * 2m).

The objectives are:

(i) to embed the Payload into the Cover image in the wavelet domain.

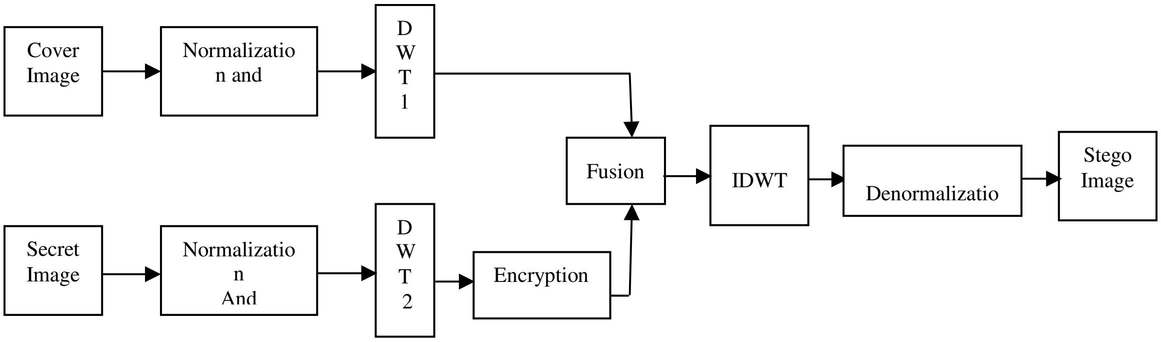


Fig: 1. HCSSD Encoder

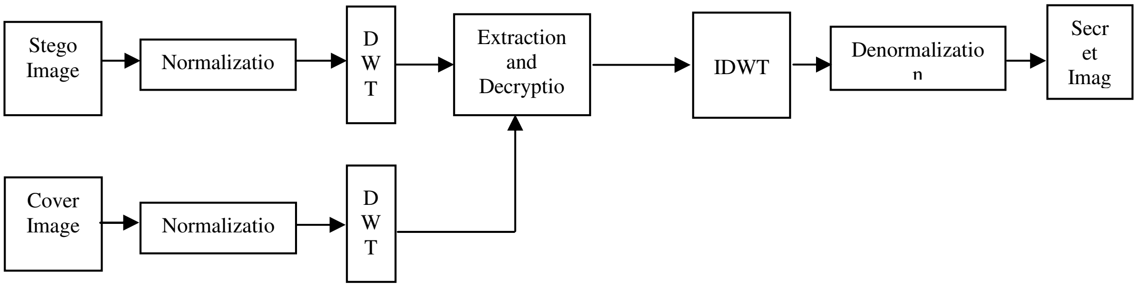


Fig: 2. HCSSD Decoder

(ii) to increase the embedding capacity into the Cover image.
(iii) to ensure reasonable PSNR of the Stego mage.

Assumptions:
Cover and payload images are grayscale uncompressed images, i.e., color images are converted into grayscale images.
(ii) Haar wavelet Transform is used to convert spatial domain image to wavelet domain.
Table 1 gives the HCSSD Encoder algorithm. The algorithm gives high security as encrypting the wavelet coefficients of Payload before embedding. The payload being double the size of the cover, the capacity is high due to the fact that we are embedding only the approximation band of the payload coefficients. For a cover image of size (n * m), when we apply two level DWT we get matrix dimension of size (n/2 * m/2), and we take a Payload of size (2n * 2m) and apply twice two level DWT, it gives matrix dimension of (n/2 *m/2). Since the matrix dimension of cover image and payload are same we are able to add their respective coefficients. Table II gives HCSSD Decoder to retrieve the Payload from the Stego image.

5. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

For performance analysis we considered the Cover Images (CI) such as Lady, Aero plane, Players, Cow boys and Flower. Payload images (PL) are Flower, Bank text, Astronauts, Dog and Elephant. The payload is embedded into the cover image to derive the Stego image at the sending end. The payload is recovered from the Stego image at the destination with minimum distortion. Fig. 3(a), 4(a), 5(a), 6(a) and 7(a) are the Cover Images (CI). Fig. 3(b), 4(b), 5(b), 6(b) and 7(b) are the Payload images (PL). Fig. 3(c), 4(c), 5(c), 6(c) and 7(c) are the Stego Images (SI). Fig. 3(d), 4(d), 5(d), 6(d) and 7(d) are the Retrieved Payload images (RPL). Table III shows the experimental results of the proposed HCSSD algorithm where the MSE, PSNR and Entropy between the cover image and Stego image are computed. The PSNR, MSE and Entropy are dependent on

image formats and sizes of the cover and Stego image. The Entropy values approximately equal to zero which indicates that the security of the payload is high. Since all the bits in the pixel of the cover image are used for fusion purpose, the embedding capacity reaches its maximum that is 8 bit for pixel for a gray scale cover image The size of the payload is twice to that of the cover image. Table IV shows the experimental results of existing Wavelet Based Fusion (WBF) algorithm, wherein the MSE, PSNR and Entropy between the cover image and Stego image are computed. From Table III and IV, we observed that the PSNR values of proposed algorithm are within the acceptable range along with higher capacity and highly secure as the Entropy value is approximately zero.

Table: 1 **ALGORITHM OF DATA EMBEDDING**

- Input: Cover Image *c* and Payload image *p*.
- Output: Stego image *s*.

1. Normalize *c* and *p*, so that the wavelet coefficient varies between 0.0 and 1.0.
2. Preprocessing on *c* and *p*
3. Transform *c* and *p* into 2 levels of decomposition using Haar Wavelet.
4. Apply 2 levels DWT on the approximate band of the payload obtained.
5. Encrypt the DWT coefficients obtained.
6. Wavelet fusion of DWT coefficients of *c* and *p*.
7. Inverse transform of all the subbands of the fused image.
8. Denormalize the Fused image.
9. Stego image *s* is generated.

Table: II **ALGORITHM OF DATA EXTRACTION**

- Input: Stego Image s.
- Output: Payload *p*.

1. Normalize Stego Image *s*.
2. Transform *s* in to 2 levels of wavelet decomposition.
3. Subtract DWT coefficients of *c* from DWT coefficients of *s* to get DWT coefficients of only *p*.
4. Decrypt the DWT coefficients of *p* obtained.
5. Apply IWT of all the sub bands of *p*.
6. Apply IWT of payload obtained with respect to approximate band.
7. Denormalize the resultant of step 6.
8. Payload Image is obtained *p*.

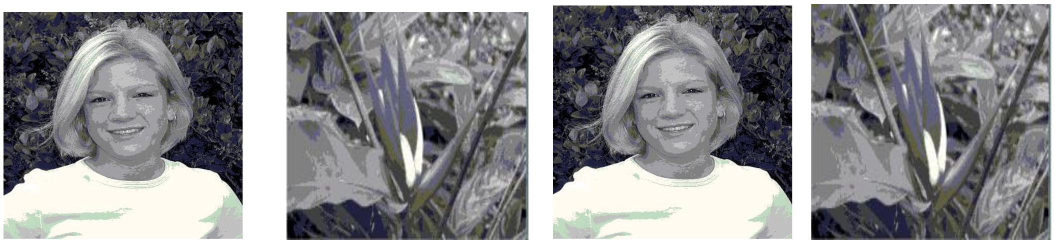
Table: III **MSE, PSNR and Entropy of Cover and Stego image of HCSSD**

Images	Type	Size	MSE	PSNR	Entropy
Lady Flower	JPEG JPEG	346×396 240×240	0.17	55.6	0.00019
Aero plane Bank Text	TIFF PNG	400×300 810×400	2.76	43.7\	0.0000
Player Astronauts	JPEG PNG	400×300 200×200	0.9	48.1	0.0004
Cow Boys Dog	JPEG TIFF	186×100 436×600	0.17	55.58	0.0000
Flower	JPEG	200×150	0.98	48.20	0.0000

Elephant	JPEG	335×219			

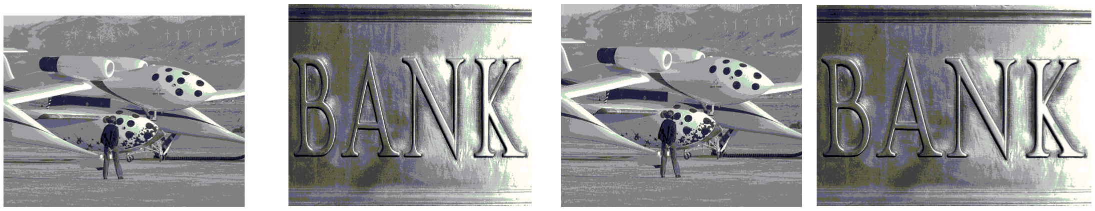
Table: IV **MSE, PSNR and Entropy of Cover and Stego image WBF**

Images	Type	Size	MSE	PSNR	Entropy
Lady Flower	JPEG JPEG	346×396 240×240	2.10	44.9	0.004
Aero plane BankText	TIFF PNG	400×300 810×400	0.41	51.9	0.0010
Player Astronauts	JPEG PNG	400×300 200×200	0.49	51.1	0.0060



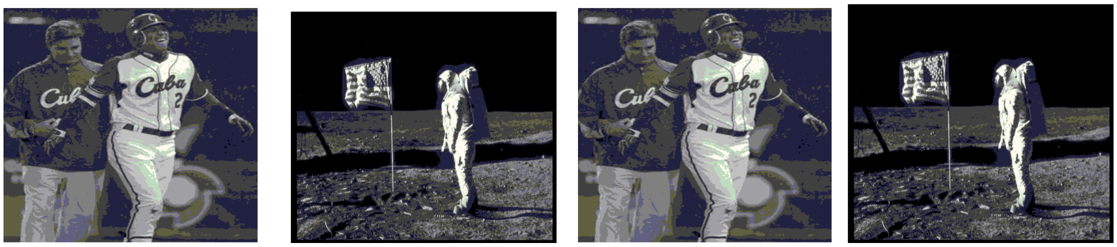
(a) Cover image (b) Payload Image (c) Stego Image (d) Retrieved Payload image

Fig. (3). Lady and Flower images



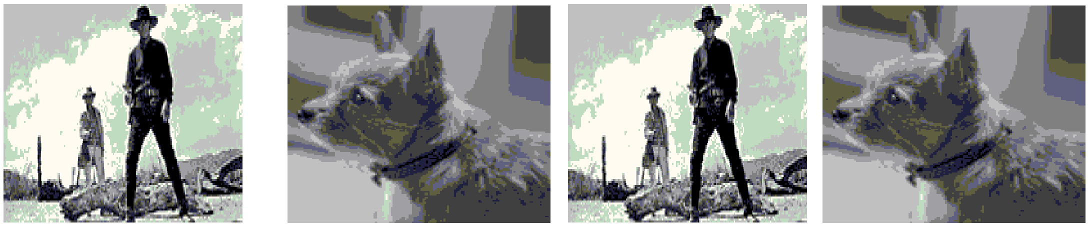
(a) Cover Image (b) Payload image (c) Stego Image (d) Retrieved Payload

Fig.4. Aero plane and Bank Text Images



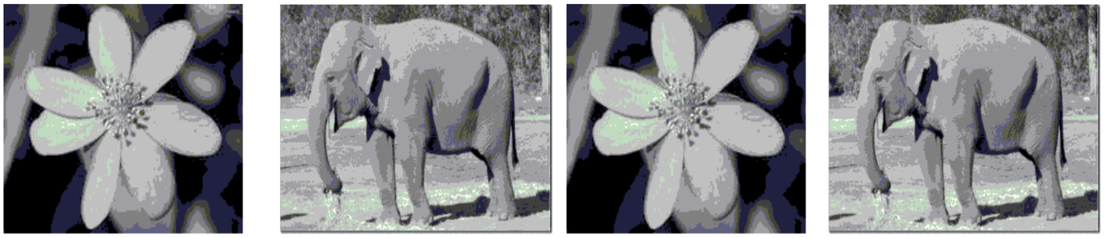
(a) Cover image (b) Payload Image (c) Stego Image (d) Retrieved payload

Fig.5. Player and Astronauts Images



(a) Cover image (b) Payload Image (c) Stego Image (d) Retrieved Payload image

Fig.6 Cow Boys and Dog Images



(a) Cover image (b) Payload Image (c) Stego Image (d) Retrieved Payload image

Fig.7 Flower and Elephant Images

6. CONCLUSIONS

The Steganography is used for secrete communication. In this paper High Capacity and Security Steganography using Discrete wavelet transform algorithm is proposed. The cover and payload are normalized and the wavelet coefficient is obtained by applying discrete wavelet transform. The approximation band coefficient of payload and wavelet coefficient of cover image are fused based on strength parameters alpha and beta. The capacity of the proposed algorithm is increased as the only approximation band of payload is considered. The Entropy, MSE and Capacity are improved with acceptable PSNR compared to the existing algorithm. In future the algorithm can be tested with curvelet transform and other transform techniques.

Contributions: In this paper the two level wavelet transform is applied as cover and payload. The payload wavelet coefficients are encrypted and fused with wavelet coefficients of cover image to generate stego coefficients based on the embedding strength parameters alpha and beta.

Acknowledgements : The first author thank full to the management and Principal Dr..Narendra Viswanath to support the entire research work.

7. REFERENCES

[1] Neil F. Johnson and Sushil Jajodia, "Steganalysis: The Investigation of Hidden Information," *IEEE conference on Information Technology*, pp. 113-116, 1998.

[2] Lisa M.Marvel and Charles T. Retter, "A Methodlogy for Data Hiding using Images," IEEE *conference on Military communication*, vol. 3, Issue. 18-21, pp. 1044-1047, 1998.

[3] Giuseppe Mastronardi, Marcello Castellano, Francescomaria Marino, "Steganography Effects in Various Formats of Images. A Preliminary Study," International Workshop on Intelligent data Acquisition and Advanced Computing Systems: Technology and Applications, pp. 116-119, 2001.

[4] LIU Tong, QIU Zheng-ding "A DWT-based color Images Steganography Scheme" IEEE International Conference on Signal Processing, vol. 2, pp.1568-1571, 2002.

[5] Jessica Fridrich, Miroslav Goijan and David Soukal, "Higher-order statistical steganalysis of palette images" *Proceeding of SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia ContentsV*, vol. 5020, pp. 178-190, 2003.

[6] Jessica Fridrich and David Soukal, "Matrix Embedding for Large Payloads" *SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents* , vol. 6072, pp. 727-738. 2006.

[7] Yuan-Yu Tsai, Chung-Ming Wang "A novel data hiding scheme for color images using a BSP tree" *Journal of systems and software*, vol.80, pp. 429-437, 2007.

[8] Jun Zhang, Ingemar J. Cox and Gwenael Doerr.G "Steganalysis for LSB Matching in Images With High-frequency Noise" *IEEE Workshop on Multimedia Signal Processing*, issue 1-3, pp.385- 388, 2007.

[9] M. Mahdavi, Sh. Samavi, N. Zaker and M. Modarres-Hashemi, "Steganalysis Method for LSB Replacement Based on Local Gradient of Image Histogram," *Journal of Electrical and Electronic Engineering*, vol. 4, no. 3, pp. 59-70, 2008.

[10]Shilpa P. Hivrale, S. D. Sawarkar, Vijay Bhosale, and Seema Koregaonkar "Statistical Method for Hiding Detection in LSB of Digital Images: An Overview *World Academy of Science, Engineering and Technology*, vol. 32, pp. 658-661, 2008.

[11]K. B. Raja, S. Sindhu, T. D. Mahalakshmi, S. Akshatha, B. K. Nithin, M. Sarvajith, K. R. Venugopal, L. M. Patnaik, "Robust Image Adaptive Steganography using Integer Wavelets" *International conference on Communication Systems Software*, pp. 614-621, 2008.

[12]Jan Kodovsky, Jessica Fridrich "Influence of Embedding Strategies on Security of Steganographic Methods in the JPEG Domain" *Proceedings of SPIE, the International Society for Optical Engineering*, vol. 6819, pp. 681902.1-681902.13, 2008.

[13] L. Y. Por, W. K. Lai, Z. Alireza, T. F. Ang, M. T. Su, B. Delina, "StegCure: A Comprehensive Steganographic Tool using Enhanced LSB Scheme," *Journal of WSEAS Transctions on Computers*, vol. 8, pp. 1309-1318, 2008.

[14]Gaetan Le Guelvouit, "Trellis-Coded Quantization for Public-Key Steganography," *IEEE International conference on Acostics, Speech and Signal Processing*, pp.108-116, 2008.

[15]Mohammed Ali Bani Younes and Aman Jantan, "A New Steganography Approach for Images Encryption Exchange by Using the Least Significant Bit Insertion," *International Journal of Computer Science and Network Security*, vol. 8, no. 6, pp.247-257, 2008.

[16]Chang-Chu Chen, and Chin-Chen Chang, "LSB-Based Steganography Using Reflected Grey Code," *The Institute of Electronics, Information and communication Engineers Transaction on Information and System,",* vol. E91-D (4), pp. 1110-1116, 2008.

[17]Babita Ahuja and, Manpreet Kaur, "High Capacity Filter Based Steganography," *International Journal of Recent Trends in Engineering*, vol. 1, no. 1, pp.672-674, May 2009.

[18]Debnath Bhattacharyya, Poulami Das, Samir kumar Bandyopadhyay and Tai-hoon Kim, "Text Steganography: A Novel Approach," *International Journal of Advanced Science and Technology,* vol.3, pp.79-85, February2009.

[19]Chin- Chen Chang, Yung- Chen Chou and Chia- Chen Lin, "A steganography scheme based on wet paper codes suitable for uniformly distributed wet pixels," *IEEE International Symposium on circuits and Systems,* pp. 501-504, 2009.