ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

Transform Domain Techniques for Image Steganography

Vaishali P[1], Pradyumna Bhat[2]

Student of Department of E.C.E., M. Tech., NMAMIT, Nitte, India[1]

Assistant Professor, Department of ECE, NMAMIT, Nitte, India[2]

Abstract: Steganography is the powerful tool for hiding information inside useful cover medium in ways such that the hidden message is undetectable. In Greek language, stego means covered or secret and graphy means to write. Hence, steganography means covered writing. Transform domain steganography is one of the techniques used for hidden exchange of information in frequency domain and it can be defined as the study of invisible communication that deals with the ways of hiding the existence of the communicated message. In this way, if successfully achieved, the message does not get attention of attackers and eavesdroppers. In steganography, information can be hidden in different cover carriers. Cover media can be a text, image, audio or video files.

Keywords: DCT, DWT, SVD, PSNR, MSE, Stego-image.

I. INTRODUCTION

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows that a message has been sent. In steganography secret communication can be done in either of the following cover media i.e. text, image, audio or video. The goal of steganography is always to conceal the very existence of the secret message. Steganography is useful in many applications. Here the recipient receives a secret message in a hidden form in any of the cover media which is invisible to the human visual system. Steganography's ultimate objectives are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data that separates it from related techniques such as watermarking and cryptography. Depending on the media used for cover, steganography can be classified as text, image, audio and video steganography. Block diagram of image steganography is as shown in the Fig. 1

A. Block Diagram Of Image Steganography

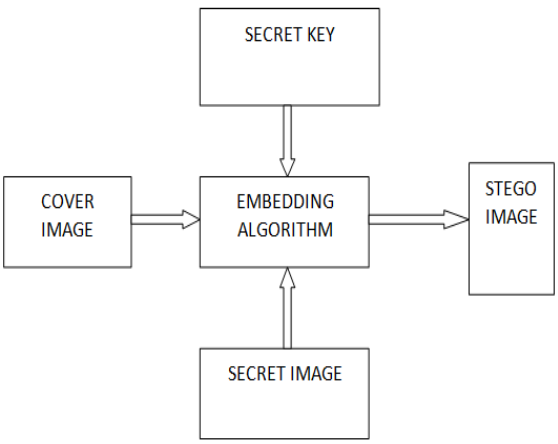

Fig. 1 Block Diagram of Image Steganography

B. Steganography v/s Cryptography

Basically, the purpose of cryptography and steganography is to provide secret communication. But, steganography is not the same as cryptography. Cryptography is the science in which data is encrypted in such a way that one cannot understand the encrypted message, whereas steganography conceals the mere existence of the data such that even its presence cannot be noticed.

Cryptography scrambles a message by applying some cryptographic algorithms for converting it into unintelligible form. On the other hand, Steganography hides the secret message so that it cannot be seen. Cryptography offers the ability of information transmission between persons in a way that prevents a third party from reading it.

Cryptography can also be used to authenticate and verify the identity of someone or something when it is needed. In contrast, steganography does not alter the structure of the secret data, but hides it inside a cover media so it cannot be seen.

C) Types of Steganography

Depending on the type of the cover object there are different types of steganographic techniques which are followed in order to obtain security.

1) *Text Steganography*

In Text Steganography text message is taken as the cover media. Tabs, white spaces, special characters are used to scramble the message.

2) *Image Steganography*

In this technique image is taken as the cover object. Either text or an image can be hidden in another image. Generally in this technique pixel intensities are varied in order to hide the information.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

3) *Audio Steganography*

Here audio is taken as a carrier for information hiding. It uses digital audio formats such as WAVE, MIDI, AVI, MPEG etc for steganography.

4) Video Steganography

Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. In this technique, first the video is converted into frames and in one of the frame the secret information is embedded. Generally discrete cosine transform (DCT) is used to hide the information in each of the images in the video, which is not noticeable by the human visual system. Video steganography uses some of the video formats like MPEG, AVI or other.

II. RELATED WORK

In order to make communication over the internet secure, it is essential to develop security schemes that can take care of the attacks from the eavesdroppers.

Parul et al., [8], introduced a modified secure and high capacity based steganography scheme of hiding a large-size secret image into a small-size cover image. Arnold transformation is performed to scrambles the secret image. Discrete Wavelet Transform (DWT) is performed in both images and followed by Alpha blending operation. Then the Inverse Discrete Wavelet Transformation (IDWT) is applied to get the stego image.

They have investigated the performance of their scheme by comparing various qualities of the stego image and cover image. The results show that the proposed algorithm for modified steganography is highly secured with certain strength in addition to good perceptual invisibility.

Rajib Biswas et al., [9], introduced a new arena in steganography in colour images in frequency domain or more precisely that in Discrete Cosine Transform (DCT) domain. In this paper the authors have proposed the exploration of a deft method for image-secret data-steg pass based sampling along with encryption and embedding in frequency domain with a variable bit retrieval function where the secret data becomes more secure by hiding with the steg password, so that without knowing the steg password one cannot get the secret data explored.

Monika Gunjal and Jasmine Jha [10], have developed a new technique that has combined LSB and DCT embedding algorithm with blowfish algorithm.

First the plain text is converted into cipher text using Blowfish algorithm. The cover image is converted into its DCT domain.

The cipher text is then embedded in LSBs of the DCT coefficients. Method achieved good quality stego-image.

III. PROPOSED METHODS OF STEGANOGRAPHY

A) DCT Image Steganography

DCT is one of the general orthogonal transform for digital image processing with advantages such as high compression ratio, small bit error rate and good information integration ability.

Discrete Cosine Transform is a technique applied to image pixels in spatial domain in order to transform them into a frequency domain in which redundancy can be identified. In JPEG compression, image is divided into 8 × 8 blocks, and then the two-dimensional Discrete Cosine Transform (DCT) is applied to each of these 8 × 8 blocks. Then in LSB of each DCT coefficient the Secret image is hidden. In JPEG decompression, the Inverse Discrete Cosine Transform (IDCT) is applied to the 8 × 8 DCT coefficient blocks.

For most images, much of the signal energy lies at low frequencies appear in the upper left corner of the DCT. Since the lower right values represent higher frequencies, and are small values, enough to be neglected with little visible distortion compression can be achieved.

B) DWT Image Steganography

A wavelet is a small wave which oscillates and decays in time domain. The Discrete Wavelet Transform is a relatively recent and computationally efficient technique. Wavelet analysis is advantageous as it performs local analysis and multi-resolution analysis. Analyzing the signal at different frequencies with different resolutions is called multi-resolution analysis (MRA). Wavelet analysis can be of two types: continuous and discrete.

The DWT divides an image into four parts namely a lower resolution approximation component (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The LL sub band is obtained after low-pass filtering both the rows and columns and contains a rough description of the image.

The HH sub-band is high-pass filtered in both directions and have the high-frequency components along the diagonals.

The HL and LH sub bands are the results of low-pass filtering on one direction and high-pass filtering in the other direction. After the image is processed by the wavelet transform, most of the information contained in the host image is concentrated into the LL image. LH sub band contains mostly the vertical detail information which corresponds to horizontal edges.

HL band represents the horizontal detail information from the vertical edges. The process can be repeated to obtain multiple 'scale' wavelet decomposition [8]. And the wavelet decomposition is shown in the Fig. 2.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

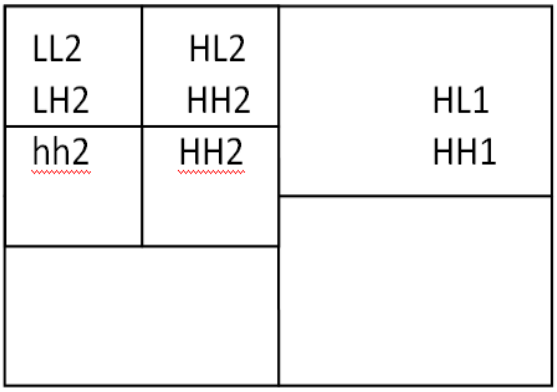

Fig.2 Wavelet Decomposition

Algorithm:

Step 1: First chose the cover image and the secret image.

Step 2: Decompose the cover image using DWT to get approximated and detailed coefficients.

Step 3: Chose one coefficient as the cover image.Step 4: Hide the secret image in the least significant bits of the cover image using LSB embedding algorithm.

Step 5: Follow the steps in the reverse order to extract the secret image.

C) DWT & SVD Image Steganography

In this method in addition to DWT, singular value decomposition of both the cover image and secret image has been done to enhance the invisibility and robustness. The singular value decomposition (SVD) is a factorization of a real or complex matrix, with many useful applications in signal processing and statistics.

Formally, the singular value decomposition of an m × n real or complex matrix M is a factorization of the form M = UΣV*, where U is an m × m real or complex unitary matrix, Σ is an m × n rectangular diagonal matrix with non-negative real numbers on the diagonal, and V*(the conjugate transpose of V, or simply the transpose of V if V is real) is an n × n real or complex unitary matrix[12].

Algorithm:

Step 1: select the proper cover image and secret image.

Step 2: Apply Discrete Wavelet Transform on both the image by 2D Haar Discrete Wavelet Transform and get four subbands LL1, HL1, LH1, and HH1 matrices.

Step 3: Separate Red, Blue and Green component of both the images and apply Singular Value Decomposition.

Step 4: Then concatenate three components of the SVD matrix and embed the secret image into the cover image to get stego-image.

Step 5: Take the IDWT.

Step 6: Follow the same steps in the reverse order to extract the secret image.

IV. PERFORMANCE METRICS

A. MSE

MSE stands for Mean Square Error. Lower the value of MSE better the quality of the image. It is defined as shown in equation 1.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(Xij - Yij)^2 \quad (1)$$

Here M and N are the number of rows and columns of the cover image (Xij) and stego-image (Yij) respectively.

B. PSNR

PSNR stands for Peak Signal to Noise Ratio. Higher the value, higher is the quality of the image. It is given by the formula as shown in the equation 2.

$$PSNR = 10\log 255^2 / MSE \quad (2)$$

C. BER

BER stands for Bit Error Rate.It is Given by the equation 3.

$$BER = \frac{1}{PSNR} \quad (3)$$

V. RESULTS

A. DCT Image Steganography

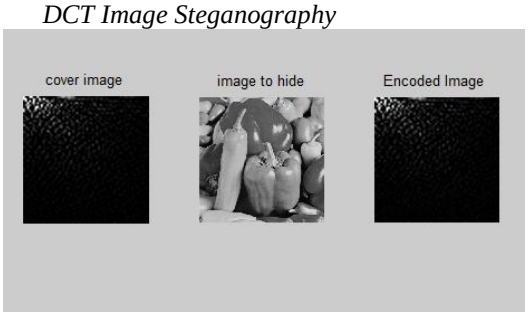

Fig. 3 Embedding in DCT domain

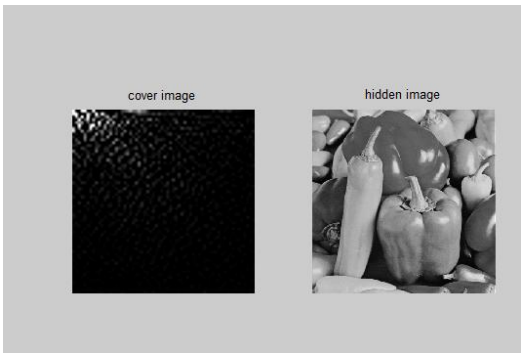

Fig. 4 Recovered Cover Image and Secret Image

B. DWT Image Steganography

Fig. 5 Wavelet Decomposition

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

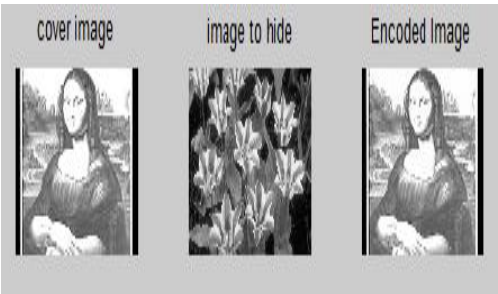

Fig. 6 DWT Image Steganography

Fig. 7 Recovered Cover Image and Hidden Image

C. *DWT & SVD Image Steganography*

Fig. 8 Embedding in DWT & SVD domain

Fig.9 Recovered Cover Image and Secret Image

The efficiency of above steganographic methods is compared based on the following parameters as shown in the table. 1. Which clearly indicates DWT & SVD method is the best in terms of good stego-image quality and least Bit Error Rate.

Table. 1 Comparison of Steganographic Methods Based on PSNR and MSE

CONSTRAINTS\ METHOD	DCT	DWT	DWT&SVD
COVER IMAGE	peppers.jpg	peppers.jpg	peppers.jpg
SECRET IMAGE	fruits.jpg	fruits.jpg	fruits.jpg
MSE	0.62	0.20	0.03
PSNR(Decibels)	50.27	55.23	63.88
Bit Error Rate(BER)	0.0198	0.0181	0.0156
Entropy	4.3989	5.6909	7.2508
Time Taken (secs)	3.1250	1.1406	1.9688

VI. CONCLUSIONS

DWT & SVD method is found to be best in terms of PSNR of the Stego-image and it gives lowest bit error rate. So the quality of the stego-image obtained in this method is high. Further these steganographic methods can be made more secure by encrypting them using strong encryption algorithms.

REFERENCES

[1] DeepeshRawat, VijayaBhandari , " A Steganography Technique for Hiding Text in an Image using LSB Method for 24 Bit Colour Image", International Journal of Computer Applications (0975 – 8887) Volume 67– No.1, February 2013, pp. 15-19.

[2] Rajkumar Yadav, Ravi Saini and Kamaldeep, "Cyclic Combination Method for Digital Image Steganography with Uniform Distribution of Message", Advanced Computing: An International Journal (ACIJ), Vol.2, No.6, November 2011, pp. 29-43.

[3] M.Sivaram, B.DurgaDevi and J.Anne Steffi, "Steganography of Two LSB Bits", International Journal of Communications and Engineering Volume 01– No.1, Issue: 01 March2012.

[4] Nitin Jain, Sachin Meshram, Shikha Dubey, "Image Steganography Using LSB and Edge – Detection Technique", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012, pp. 217-222.

[5] Sunny Dagar, Vinay Kumar and Yogendra Bagoriya, "Image Steganography using Secret Key & Gray Codes" , International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-5, April 2013, pp. 241-245.

[6] Ankita Sancheti, "Pixel Value Differencing Image Steganography Using Secret Key", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-1, December 2012, pp. 68-72.

[7] Saiful Islam, Mangat R Modi and Phalguni Gupta, "Edge-Based Image Steganography", EURASIP Journal on Information Security 2014, 2014:8.

[8] Parul, Manju, Dr. Harish Rohil, "Optimized Image Steganography using Discrete Wavelet Transform (DWT)", International Journal of Recent Development in Engineering and Technology, ISSN 2347 – 6435, Volume 2, Issue 2, February 2014). pp. 75-81.

[9] Rajib Biswas, Sayantan Mukherjee, and Samir Kumar Bandyopadhyay, "DCT Domain Encryption in LSB Steganography", 5th International Conference on Computational Intelligence and Communication Networks, Mathura, 2013, pp 405-408.

[10] Monika Gunjal, Jasmine Jha, "Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm", International Journal of Computer Trends and Technology (IJCTT) – volume 11, number 4 – May 2014, pp 144-150.

[11] William Stallings, "Cryptography and Network Security, Principles and practice" Fifth Edition.

[12] Seema and Sheethal Sharma, " DWT-SVD Based Efficient Image Watermarking Algorithm to Achieve High Robustness and Perceptual Quality" International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X , Volume 2, Issue 4, April 2012,pp. 75-78.

[13] "Electronic Sources", http: //www.cs. virginia.edu wm2a/Historial Overview.html