Volume: 07 Issue: 01 Pages: 2606-2610 (2015) ISSN: 0975-0290

Significant Data Hiding through Discrete Wavelet Transformation Approach

Premal B. Nirpal
Department of Computational Science, New Model Degree College, Hingoli-431513 (MS),
Email: premal.nirpal@gmail.com
Ganesh M. Magar
Department of Computer Science, SNDT Women's University, Mumbai-400049 (MS),
Email: drgmmagar@gmail.com

ABSTRACT

The methods of communication of invisible information have become need in the today's digital era. The network connectivity and high speed devices made easy passing massive data instantly. As boom of the huge data transmission has taken place due to easy use of the technology, the protection of the data has become prime issue. Steganography hides messages inside some other digital media. Cryptography, on the other hand obscures the content of the message. We proposed a novel integration of an incorporating text and image steganography to find a solution for improve security and protect data. The proposed methods shows a high level of efficiency and robustness by combining text and image which involves the scheme of discrete wavelet transformation combining text and image by secretly embeds encrypted secrete message text data (cipher text) or text image in the content of a digital image. A comparative study of the different techniques has been illustrated by computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR).

Keywords - **Discrete wavelet Tranformation, Extract message, Stegnography, Secrete message.**

Date of Submission: April 26, 2015 Date of Acceptance: June 25, 2015

I. INTRODUCTION

The rapidly increase of information technology and the growth of digital technologies in information hiding via multimedia have enhanced the access to digital data. It enables the reliability of the techniques to achieve the efficiency and accuracy of data processing, data storage, retrieval, control, transfer, protect and secure the information. The processing of communication via digital forms such as text, image, audio and video has reinvent itself by new technologies and applications that make it easy to the third party to access the contents of digital media and obtain the illegal protection. Data exchange over the networks (the Internet or LANs), however, has opened doors to a large number of security threats as it is easily accessible anywhere [1-3]. Thus, it was long thought to secure the confidentiality of the intended message and humans started to seek ways to secure the data. Securing the communication of intellectual property and providing protection for digital data in distributed system have drawn a lot of attention nowadays. Hence, it poses a novel challenge for researchers.

II. BACKGROUND OF STEGANOGRAPHY TECHNIQUES

The general idea in the steganography is of hiding some information in digital content. It is invisible communication over the channel. Visually seen information in the form of image content the information and usually concealed by the observer. A particular case of information hiding is digital watermarking. Digital watermarking is the process of embedding information into digital multimedia content such that the watermark can later be extracted or detected for a diversity of purposes including copy prevention and control. Digital watermarking has become an active and important area of research. In watermarking applications like copyright protection and authentication, there is an active opponent that would attempt to remove, invalidate or forge watermarks. In information hiding there is no such active adversary as there is no value associated with the act of removing the information hidden in the content. Nevertheless, information hiding techniques need to be robust against accidental distortions. Unlike information hiding and digital watermarking, the main goal of steganography is to communicate securely in an absolutely untraceable manner.

Steganography Enhancement Techniques share the important goal, to secure, maximizing the capacity, robust and imperceptibility of the stego channel.
The techniques of Steganography classified as follows:
2.1 Spatial Domain:
The processing is applied on the image pixel values directly or by modifying the pixel values. (Bit plane , LSB, Palette-based methods)
2.2 Frequency Domain:
The first step is to transform the image data into frequency domain coefficients by some mathematical tools. Then according to the different data characteristics generated by these transforms, embed the data into the coefficients in frequency domain.
The transform domains of steganography scheme's objective are to achieve a better balance between robustness, security and fidelity than the spatial domain schemes.

Volume: 07 Issue: 01 Pages: 2606-2610 (2015) ISSN: 0975-0290

III. INTRODUCTION TO DWT BASED ON STEGANOGRAPHY

Wavelets are mathematical functions that divide continuous time signal data into different frequency components. A wavelet is a localized change of a sound signal in 1-D or localized variations of detail in an image in 2-D. The DCT has a long history of showing its appropriateness for information hiding applications. The secret message can be embedded in the higher level frequencies, which are not as perceptible to the human eye, by reaching the wavelet coefficients in the HL and LH detail sub-bands.

Discrete Wavelet Transformation Steganography:

i. Many different schemes proposed and have been effectively utilized as a powerful tool in many diverse fields.
ii. It is applied to entire image or to it's subparts of its coefficients by some mathematical tools.
iii. The operating in the transform domain Compared to the spatial domain is more secure and robust to visual or statistical attacks

IV. PROPOSED ALGORITHM

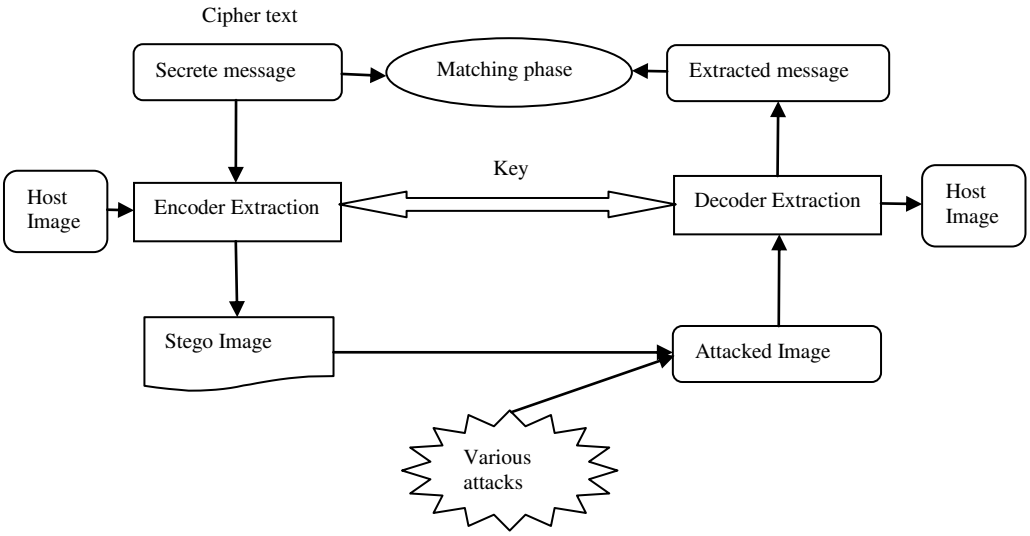

Fig.4.1: shows the overall view of the proposed system

i. Steganography enhancement of the proposed system that's based on the Discrete Wavelet Transform (DWT), which focuses on how to enhance the security communication and robustness of the secret data by combining text and image of the hiding technique approaches such as text, Ciphertext, biometric data and embedding and extracting process.
ii. Steganography methods
    a. Embedding (Hide)
    b. Extracting (retrieve)
iii. Steganography architectural design
    a. Cover object
    b. Secret message (text, Cipher text, text image, image, biometrics)
    c. Embedding process
    d. Extracting process

V. EXPERIMENTAL WORK

Experimental work is carried out and implemented in the JPEG, Bitmap in the color and gray scale images and was resized to 512×512 with various types of content images, performed by embedding and extracting an actual bit-stream. The unnoticeable visual difference after embedding is a good indicator of the proposed method. secret messages (like text, cipher text, text image, and biometrics) Several kinds of distortion including unintentional attacks such as JPEG compression, filtering, and noising as well as intentional attacks such as cropping, rotation was performed on the stego images. We tested the performance of the present algorithms such as LSB, DCT and DWT on these database images with various quality measurements like MSE, PSNR and NC.

The aim of our study is to ensure the security and robustness of the proposed algorithm. It is analyzed by measuring the differences of the cover image and stage image through MSE, PSNR and NC by using the techniques of LSB, DCT and DWT.

The improved results shown in the form of PSNR are given, where the result of LSB technique obtained the average between (30 – 45) db. The result of DCT technique obtained the average between (45 – 60) db and the result of DWT technique obtained the average between (45 – 85) db and above.

The PSNR values of different file formats, (color BMP, Color JPG, Gray BMP, Gray JPG) in a various Images of the size, (512×512) pixel, for the techniques LSB, DCT and DWT have been tested

Volume: 07 Issue: 01 Pages: 2606-2610 (2015) ISSN: 0975-0290

Lena image has improved the value of PSNR above 60 db reveals that PSNR value of the proposed system is greater than other techniques mentioned in the tables. In the Lena image of different format as color JPG of LSB technique obtained 47.2564, DCT obtained 57.1256 and DWT 73.7188 indicating that the DWT value of PSNR has greater than LSB and DCT. In color of BMP of LSB technique obtained 45.1242, DCT obtained 46.3541 and DWT obtained 74.5857, it also reveals that the DWT value of PSNR has greater than LSB and DCT. In Gray Scale of JPG of LSB technique obtained 43.1842, DCT obtained 57.2541 and DWT obtained 99.0. In Gray Scale of BMP of LSB technique obtained 41.0564, DCT obtained 57.6106 and DWT obtained 66.8151, that reveals the improvement in DWT technique of PSNR value.

VI. CONCLUSION

In this research work, the result discussed and interpreted through experimental work has accomplished by DWT and shows the effectiveness and robustness of the proposed system that enhances security system by combining text and image. The proposed work uses metrics such as PSNR, MSE and NC to judge the existence of secret message between the original and stego image, where a high PSNR and low MSE indicates that the stego image is closer to the original image. The effectiveness and efficiency can be enhanced in the way of capacity, Security and robustness. However to develop the healthy and unique robust methods for various kinds of media content format using DWT need to explore more for different format and size of images.

REFERENCES

[1] William Stallings, "Cryptography and Network security: principles and Practice", Prentice Hall International Inc. 2002.

[2] Jae K. Shim, Anique A. Qureshi and Joel G. Siegel, "The International Hand book of Computer Security", Glenlake Publishing Company, Ltd. 2000.

[3] Saraju P. Mohanty, "Digital Watermarking: A Tutorial Review", Dept. of Comp Sci. and Eng. University of South Florida Tampa, FL 33620 smohanty@csee.usf.edu. 1999

[4] S. Katzenbeisser, A.P Fabien, Petitcolas, 2000. "Information hiding techniques for Steganography and digital watermarking" editors. p. cm. (Artech House Computing library).

[5] Chung-Li Hou, Chang Chun Lu, Shi-Chun Tsai, and Wen Guey Tzeng2011. "An Optimal Data Hiding Scheme With Tree-Based Parity Check," IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 20, NO. 3.

[6] Furht, B., Muharemagic, E., Socek, D., "Multimedia Encryption and Watermarking, Multimedia Systems and Application Series", vol. 28, Springer Science Business Media, Inc. 2005.

[7] Wenbo Mao, "Modern Cryptography: Theory and Practice", Prentice Hall PTR,, Prentice-HallInc. 2004.

[8] Poularikas, A.D., "The Transforms and Applications Handbook", CRC Press LLC (with IEEE Press). 1996.

[9] Grigoryan, A.M., Agaian S.S., "Multidimensional Discrete Unitary Transforms:Representation, Partitioning, and Algorithms", Marcel Dekker, Inc., New York. 2003.

[10] P. Y. Chen, E. C. Liao, "A New Algorithm for Haar Wavelet Transform." IEEE Int. Symposium on Intelligent Signal Processing and Communication System: 453-457, 2002.

[11] Po-Yueh Chen, Hung-Ju Lin, "A DWT Based Approach for Image Steganography," Int. J. Appl. Sci. Eng., 4, 3. 2006.

[12] S. Youssef, A. Abu Elfarag, R. Raouf, "A Robust Steganography Model Using Wavelet-Based BlockPartitionmodification," Int. J. Comp. Sci.& I. T, Vol. 3, No.4. 2011.

[13] Huang Daren, L. Jiufen, H.Jiwu and L.Hongmei "A DWT Based image watermarking algorithm," IEEE Int. Conf. on Multimedia and Expo.

[14] HONG CAI, M.S., "Wavelet Structure Based Transform: Information Extraction and Analysis," University Of Texas, Dissertation. 2007.

[15] Ali Al-Ataby and Fawzi Al-Naima, "A Modified High Capacity Image SteganographyTechnique Based on Wavelet Transform," The International Arab Journal of Information Technology, Vol. 7, No. 4. 2010.

[16] Xu Jianyun, A. H. Sung, P. Shi, Liu Qingzhong, "JPEG Compression Immune Steganography Using Wavelet Transform," IEEE International Conference on Information Technology, Vol.2, pp. 704 – 708. 2004.

AUTHORS PROFILE

Dr. Premal B. Nirpal
Assistant Professor,
Department of Computer Science,
SRTMUN's New Model Degree College, Hingoli.

Dr. Ganesh M. Magar
Associate Professor & Head,
P.G. Department of Computer Science,
SNDT Women's University, Mumbai

Volume: 07 Issue: 01 Pages: 2606-2610 (2015) ISSN: 0975-0290

PSNR OF HOME IMAGE			
Column1	LSB	DCT	DWT
color JPG	52.08	57.61	68.03
color BMP	51.08	57.61	75.34
Gray JPG	41.00	57.26	73.61
Gray BMP	49.18	53.04	66.87

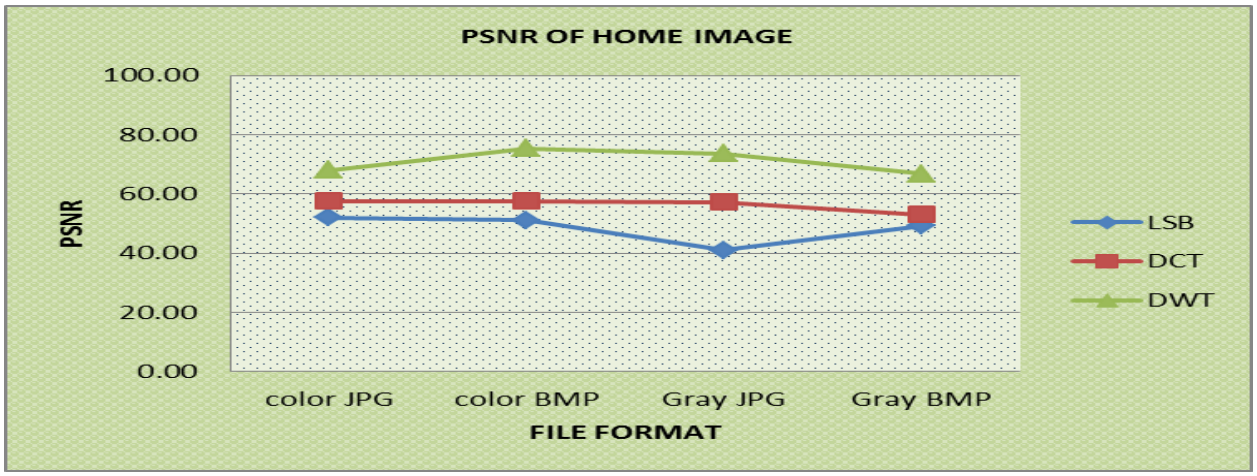

Table 5.1, Fig 5.1: The PSNR of different file formats (color BMP, Color JPG, Gray BMP, Gray JPG) of Home Image (512×512) pixel for LSB, DCT and DWT

MSE OF HOME IMAGE			
Column1	LSB	DCT	DWT
color JPG	0.00	0.11	0.01
color BMP	0.01	0.11	0.00
Gray JPG	0.00	0.12	0.00
Gray BMP	0.00	0.14	0.01

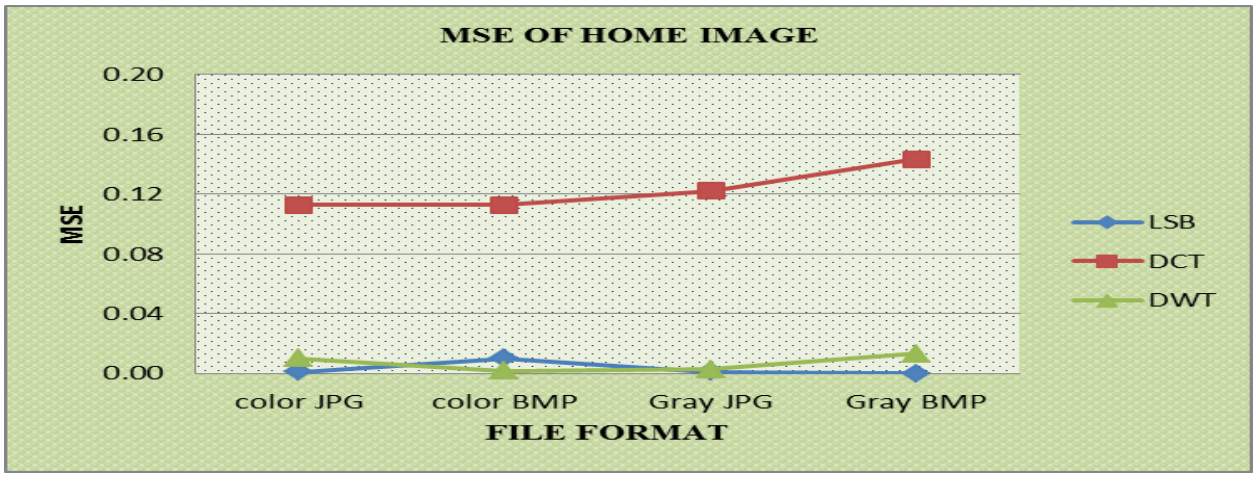

Table 5.2, Fig 5.2: The MSE of different file formats (color BMP, Color JPG, Gray BMP, Gray JPG) of Home Image (512×512) pixel for LSB, DCT and DWT

Volume: 07 Issue: 01 Pages: 2606-2610 (2015) ISSN: 0975-0290

NC OF Home IMAGE			
Column1	LSB	DCT	DWT
color JPG	0.98	0.89	0.99
color BMP	1.00	1.01	1.00
Gray JPG	1.00	0.98	1.00
Gray BMP	1.00	1.00	1.00

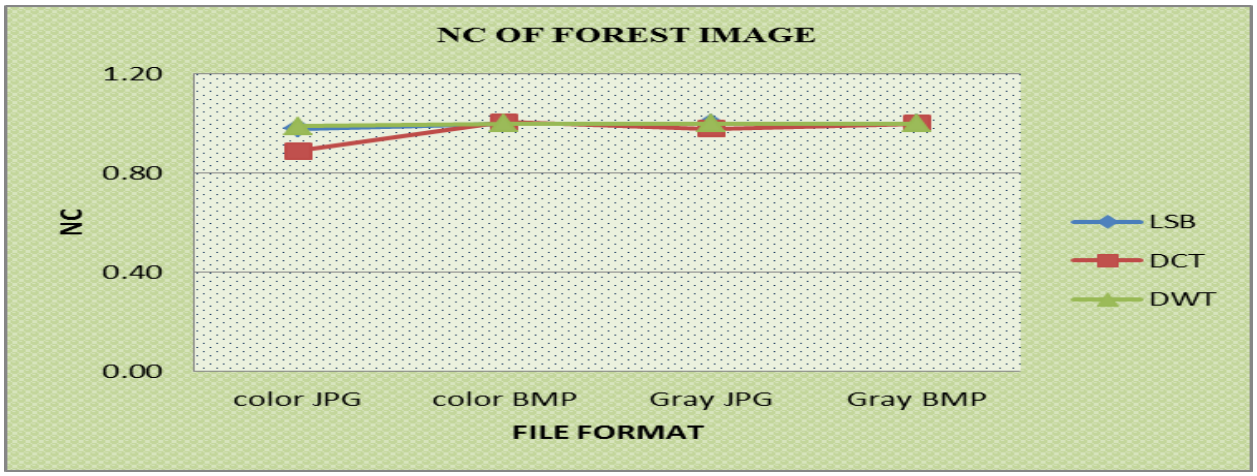

Table5.3, Fig 5.3: The NC of different file formats (color BMP, Color JPG, Gray BMP, Gray JPG) of Lena Image (512×512) pixel for LSB, DCT and DWT