ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Discrete Wavelet Transform Based Steganography for Transmitting Images

R.Asha
M.Tech Student,
Department of CSE,
Aditya Engineering College,
Surampalem, Kakinada.

M.Raja babu
Associate Professor,
Department of CSE,
Aditya Engineering College,
Surampalem, Kakinada.

ABSTRACT:

In this paper we propose a new steganography technique which embeds the secret messagesinfrequency-domain.Accordingtodifferentusers'demandsontheem beddingcapacity and image quality, the proposed algorithm is divided into two modes and 5 cases. Unlike the space domain approaches, secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Coefficients in the low frequency sub-band are preserved unaltered to improve the image quality. Some basic mathematical operations are performed on the secret messages before embedding. These operations and a well-designed mapping Table keep the messages away from stealing, destroying from unintended users on the internet and hence provide satisfactory security.

Keywords:
Discrete Wavelet Transform; Security; Steganography.

INTRODUCTION:

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word Steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphic meaning "writing". The first recorded use of the term was in 1499. The advantage of Steganography, over cryptography alone, is that message do not attract attention to themselves. Plainly visible encrypted messages no matter how unbreakable will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, Steganography can be said to protect both messages and communicating parties. It includes the concealment of information within computer files .In digital Steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. The Least Significant Bit (LSB) substitution is an example of spatial domain techniques. The basic idea in LSB is the direct replacement of LSBs of noisy or unused bits of the cover image with the secret message bits. Till now LSB is the most preferred technique used for data hiding because it is simple to implement offers high hiding capacity, and provides a very easy way to control stego-image quality [1] but it has low robustness to modifications made to the stego-image such as low pass filtering and compression and also low imperceptibility.

Algorithms using LSB in greyscale images can be found in [2, 3, 4]. The other type of hiding method is the transform domain techniques which appeared to overcome the robustness and imperceptibility problems found in the LSB substitution techniques. There are many transforms that can be used in data hiding, the most widely used transforms are; the discrete cosine transform (DCT) which is used in the common image compression format JPEG and MPEG, the discrete wavelet transform (DWT) and the discrete Fourier transform (DFT). Most recent researches are directed to the use of DWT since it is used in the new image compression format JPEG2000 and MPEG4, examples of using DWT can be found in [9, 10].

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

In [7] the secret message is embedded into the high frequency coefficients of the wavelet transform while leaving the low frequency coefficients sub band unaltered. While in [8].The advantages of transform domain techniques over spatial domain techniques are their high ability to tolerate noises and some signal processing operations but on the other hand they are computationally complex and hence slower [9].

Some of these techniques try to achieve the high hiding capacity low distortion result by using adaptive techniques that calculate the hiding capacity of the cover according to its local characteristics as in [2, 5, 7, 8]. However, the steganographic transform-based techniques have the following disadvantages; low hiding capacity and complex computations [9, 10].

Thus, to get over these disadvantages, the present paper, the use of optimum pixel adjustment algorithm to hide data into the integer wavelet coefficients of the cover image in order to maximize the hiding capacity as much as possible. We also used a pseudorandom generator function to select the embedding locations of the integer wavelet coefficients to increase the system security.Through the use ofsteganography, information can be transmitted while being disguised within another piece of data.Significant amounts of data can be moved through common means of electronic communication, with little threat of detection.

This data can be transmitted with the hidden information included, and travel across networks looking like normal traffic. Any third party that intercepts the data will not expect it to contain such a secret. Implementation of steganography is not hard to achieve, and there are multiple variations of programs that will encode and decode information [8]. Hiding data through steganographic means has become easier due to the availability of free programs online.

In addition, the number of technologically adept individuals is increasing on a daily basis. The ability to deal with steganography will become a more crucial skill in future information flows. Effort has been made to establish ways of detecting whether or not a piece of data contains a steganographic element. Unfortunately, not many steganographic messages can be detected [7]. In addition to the difficulties related to detection, the message is still encoded, and extra time is needed to translate the message into an understandable format.

The message can even be encrypted while hidden in the data via steganographic means, allowing the data to be sent without there appearing to be an encrypted file, but still having the benefits of being encrypted. This process of detection and analysis can be time consuming, meaning that the attack against steganography is not a real-time attack.

In addition, not all data that has steganographic content will be detected and stopped. A need for a better form of security against the transmission of steganography must be implemented, one which can be achieved in real time. This end could be accomplished through alterations to the picture. These alterations can either be made within the cover image, or directly to the bits that store the hidden message. Both methods result in the destruction of the hidden data with little damage to the image it is embedded in, also known as the cover image.

Destruction of steganography on a mass scale will serve as a means to protect information, and prevent hidden communication. In this paper a novel steganographic technique using Discrete Wavelet Transform for transmitting pictures is proposed. Two different techniques are proposed one using three level wavelet decomposition and another using single level wavelet-decomposition. We illustrate our technique by considering Vladimir Banoci et al [1] for three level wavelet transform and Po-Yueh Chen et al [3] for single level wavelet decomposition. Experiments show that PSNR generated by the proposed method are better than those generated by the reported schemes.

Proposed System:

The Embedding Algorithm:

The blocks of the embedding algorithm is explained in the following steps:

Step 1: Read the cover image file into a two dimensional decimal array to handle the file data more easily.

Step 2: Histogram modification it is used to prevent overflow/underflow that occurs when the changed values in Integer wavelet coefficients produce stego-image pixel values to exceed 255 or to be smaller than 0. This problem was found to be caused by the values near 255 or 0.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Step 3: Divide the cover image into 8x8 non overlapping blocks. By this division each 8x8 block can be categorized as a smooth or complex block.

Step 4: Transform each block to the transform domain using 2D Haar integer wavelet transform resulting LLI, LHI, HLI and HHI.

Step 5: Calculate hiding capacity of each coefficient, we used a modified version of the hiding capacity function. From experiments we found that as we lower the bits used to hide the secret message in the LL sub band the resulted distortion.

in the stego-image becomes lower; so that we modified this hiding capacity function by using different ranges for k for the LH, HL and HH sub bands where its values are form 1 to 4. For the LL sub band the value of k is equal to 0 and in some cases the bits used is fixed to only bits to enhance the stego-image quality.

Step 6: Embed L bits of message into the corresponding randomly chosen coefficients. Random selection of coefficients provides more security where the sequence of the message is only known to both sender and receiver by using a previously agreed upon secret key.

Step 7: Apply optimal pixel adjustment algorithm, while taking into consideration that each modified coefficient stays in its hiding capacity range where each value of L is calculated according to the absolute value of the wavelet coefficients any significant change in this value will produce different value of L to be calculated at the receiver. The main idea of using the optimum pixel adjustment (OPA) algorithm is to minimize the error difference.

IMPLEMENT AnON OF THE PROPOSED METHOD 2

A. Procedure for embedding using single level wavelet decomposition

1. Take the original image and the secret image and take the Red (R) plane separately and perform single level 2D- Daubechies DWT decomposition on the original image as well as the secret image.

2. Assume a embedding co-efficient aof value ranging from 0 tol, coefficient of a, large increase in robustness, small increase in transparency

3. To find the approximation co-efficient, horizontal co-efficient, vertical co-efficient and diagonal coefficient of the embedded image use the formula:

• Approximation co-efficient of the embedded image = (1-a)* Approximation coefficient of the original image +a* Approximation coefficient of the secret image Similarly the same is used to fmd the horizontal co-efficient, vertical co-efficient and diagonal co-efficient of the embedded image 4. Perform single level level 2D- Daubechiesinverse DWT decomposition on the calculated approximation, horizontal, vertical and diagonal coefficients to get the approximation, horizontal, vertical and diagonal coefficients of the R plane of the embedded image.

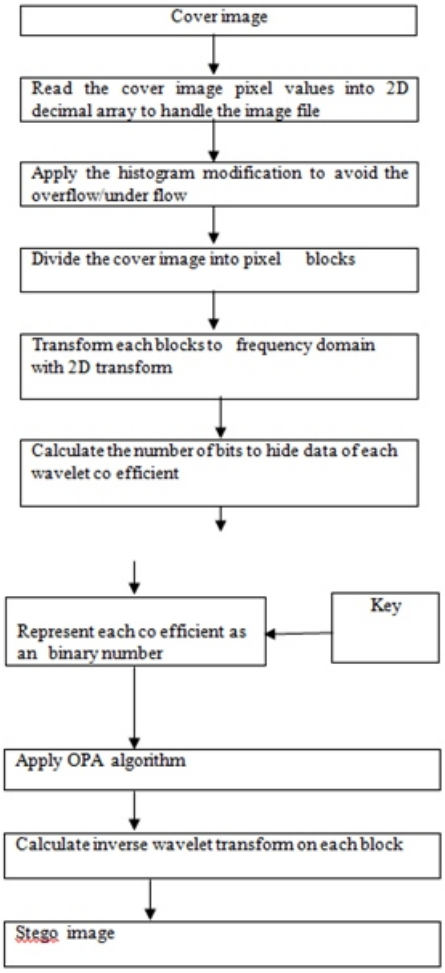
Integer Wavelet Transform:

Generally wavelet domain allows us to hide data in regions that the human visual system (HVS) is less sensitive to, such as the high resolution detail bands (HL, LH and HH), Hiding data in these regions allow us to increase the robustness while maintaining good visual quality. Integer wavelet transform maps an integer data set into another integer data set. In discrete wavelet transform, the used wavelet filters have floating point coefficients so that when we hide data in their coefficients any truncations of the floating point values of the pixels that should be integers may cause the loss of the hidden information which may lead to the failure of the data hiding system [9].

To avoid problems of floating point precision of the wavelet filters when the input data is integer as in digital images, the output data will no longer be integer which doesn't allow perfect reconstruction of the input image [10] and in this case there will be no loss of information through forward and inverse transform [9]. Due to the mentioned difference between integer wavelet transform (IWT) and discrete wavelet transform (DWT) the LL sub band in the case of IWT appears to be a close copy with smaller scale of the original image while in the case of DWT the resulting LL sub band is distorted.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Lifting schemes is one of many techniques that can be used to perform integer wavelet transform it is also the scheme used in this paper. The following is an example showing how we can use lifting schemes to obtain integer wavelet transform by using simple truncation and without losing inevitability.



Blocks of embedding diagram

The Extraction Algorithm

MATLAB is a numerical computing environment and fourth-generation programming language. Developed by Math Works, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, Java, and Fortran. Although MATLAB is intended primarily for numerical computing, an optional toolbox uses the MuPAD symbolic engine, allowing access to symbolic computing capabilities. An additional package, Simulink, adds graphical multi-domain simulation and Model-Based Design for dynamic and embedded systems. At the receiver uses the extraction algorithm to obtain the secret message.

RELATED WORK:

Steganography is rapidly growing field of research. In the past years, so many papers have been published in the field of image steganography. Anjali et al. used DWT based approach for steganography using Biometrics. In that, skin region of images is used in DWT domain for embedding secret data and image cropping concept introduced to maintain security. Results are shown in the form of table of capacity and PSNR with highest PSNR (53.0 dB) and highest capacity 71% [1]. M.F. Tolba, et al. proposed a method for embedding message bit stream into the LSB's of Integer Wavelet Co-efficient of a true color image.

Cover image is adjusted before applying Integer Wavelet Transformation (IWT) followed by DWT (two levels). Results are shown in form of stego image with PSNR (73.91 dB). With data rate 1 bpp[4]. Po-Yueh Chen, et al. proposed a method, that hide data in high frequency domain resulted from Discrete Wavelet Transformation. Some basic pre-processing methods are applied before embedding. Author divides the algorithm in two modes and three cases. For fix mode 46.83 dB is the highest PSNR value and 39.00 dB is lowest. For varying mod highest PSNR is 50.85 dB and minimum is 44.76 dB [5].

Different styles of Steganography:

The four main classes of file formats that can be used for steganography are:

i. Text

ii. Images

iii. Audio

iv. Protocol

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Text steganography: Activity info in text is historically the foremost vital methodology of steganography. A straight forward methodology was to hide a secret message in each ordinal letter of every word of a text message. Due to the beginning of the web and due to the various kind of digital file formats it's remittent in importance. Text steganography mistreatment digital files aren't used fairly often because the text files have a very small amount of redundant knowledge.

Image steganography: Images area unit the foremost popular cover objects for steganography. A message is embedded in a digital image (cover image) through an embedding algorithm, by mistreatment the key. The resulting stego image is transmitted to the receiver. On the other hand, it is processed by the extraction algorithm mistreatment identical key. Throughout the transmission of stego image, it may be monitored by some unauthenticated persons WHO will only notice the transmission of a picture but can't guess the existence of the hidden message.

Audio Steganography: Audio Steganography is masking, which exploits the properties of the human ear to hide info observably. An audible, sound becomes voiceless within the presence of another louder sounding sound .This property allows to select the channel in which to hide info. Although it's almost like images in steganographic potential, the larger size of purposeful audio files makes them less popular to use than images [11].

Protocol Steganography: The term protocol steganography refers to embedding info at intervals network protocols like TCP/IP. Associate example of its activity info within the header of a TCP/IP packet in some fields that can be either optional or area unit never used.

Conclusions:

In this paper we proposed a data hiding scheme that hides data into the integer wavelet coefficients of an image. The system combines a data hiding technique and the optimum pixel adjustment algorithm to increase the hiding capacity of the system compared to other systems. The proposed system hide secret data in a random order using a secret key only known to both sender and receiver. In this method, embeds different number of bits in each wavelet co efficicient according to a hiding capacity function in order to increasing the hiding capacity without losses of the visual quality of resulting stego image. The proposed system also minimizes the error difference between original coefficients values and modified values by using the optimum pixel adjustment algorithm.The current proposed method is only applicable on colored image as well as on gray scaled image but not applicable on audio, video and other biometrics yet. Very large amount of message cannot feed in image. So the future work should focus on large message embedding, improve the data or message embedding capacity, security against attacks, hiding techniques apply to audio & video.

REFERENCES:

[1] N. Wu and M. Hwang,"Data Hiding: Current Status and Key Issues," International Journal of Network Security, Vol.4, No.1, pp. 1-9, Jan.2007..

[2] C. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, pp. 469-474, Mar. 2004.

[3] Changa, C. Changa, P. S. Huangb, and T. Tua, "A Novel bnageSteganographic Method Using Tri-way Pixel-Value Differencing," Journal of Multimedia, Vol. 3, No.2, June 2008.

[4] H. H. Zayed, "A High-Hiding Capacity Technique for Hiding Data in images Based on K-Bit LSB Substitution," The 30th International Conference on Artificial Intelligence Applications (ICAIA - 2005) Cairo, Feb. 2005.

[5] A. Westfeld, "F5a steganographic algorithm: High capacity despite better steganalysis," 4th International Workshop on Information Hiding, pp.289-302, April 25-27, 2001.

[6] H. W. Tseng and C. C. Chnag, "High capacity data hiding in jpegcompressed images," Informatica, vol. 15, no. l, pp. 127-142,2004.

[7] P. Chen, and H. Lin, "A DWT Approach for bnageSte ganography,"International Journal of Applied Science and Engineering 2006.4, 3:275:290.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

[8] Lai and L. Chang, "Adaptive Data Hiding for bnages Based on Harr Discrete Wavelet transform," Lecture Notes in Computer Science,Volume 4319/2006.

[9] S. Lee, C.D. Yoo and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," IEEE Transactions on Information Forensics and Security, Vol. 2, No.3, Sep. 2007, pp. 321-330.

[10] M. Ramani, Dr. E. V. Prasad and Dr. S. Varadarajan,"Steganography Using BPCS the Integer Wavelet Transformed bnage", UCSNS International Journal of Computer Science and Network Security, VOL. 7 No.7, July 2007.

[11] T. Morkel, J.H.P. Eloff, M.S. Olivier, An Overview of Image Steganography, Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.

[12] T. R. Gopalakrishnan Nair, Suma, Manas, Genetic Algorithm to Make Persistent Security and Quality of Image in Steganography from RS Analysis, Swarm Evolutionary and Memetric Computing Conference (SEMCCO), Vishakhapatnam, 2012.

[13] A. Cheddad, J. Condell, K. Curran and P. McKevitt, Digital Image Steganography: Survey and Analysis of Current Methods, Signal Processing, Volume 90, Issue 3, March 2010, Pages 727-752.

[14] Samir Kumar Bandyopadhyay, TuhinUtsab Paul and AvishekRaychoudhury, Genetic Algorithm Based Substitution Technique of Image Steganography, Journal of Global Research in Computer Science, Volume 1, No. 5, December 2010.

[15] R.J. Anderson and F.A.P. Petitcolas, On the Limits of Steganography, J. Selected Areas in Comm., vol. 16, no. 4, 1998, pp. 474–481.

About Authors:

Miss.R.Asha

is a student of Aditya Engineering College, Surampalem. Presently she is pursuing her M.Tech [CSE] from this college and she received her B.Tech degree in Information Technology from Sriprakash College of Technology, affiliated to JNTU Kakinada in the year 2012.Her area of interest includes Digital Image processing and current trends in Computer Science.

M.Raja Babu

received the B.Tech degree from MVGR Engineering College, Vizianagaram in 2003. He completed M.Tech in Information Technology from NCET,Vijayawada in 2010. He is having nearly 9 years of teaching experience. He worked as an Assistant Professor in RGM Engg. College, Nandyal in C.S.E Dept. from September 2005 to May 2008 and worked as an Assistant Professor in Chaitanya Engg College, Rajahmundry in C.S.E Dept. from June 2009 to November 2010. He is Currently working as Associate Professor, Dept of IT, Aditya Engineering College, Kakinada, Andhrapradesh, India. He is a member of Srinivasa Ramanujan Research Forum (SRRF), Godavari Institute of Engineering and Technology (GIET), Rajahmundry. His research interest includes Image Processing, Information Retrieval and Pattern Recognition.. He is a life member of Computer Society of India(CSI)and Indian Science Congress Association(ISCA). He has published research papers in various National, Inter National conferences, proceedings and Journals.