Int. J. Advanced Networking and Applications
Volume: 6 Issue: 5 Pages: 2464-2467 (2015) ISSN: 0975-0290

An Adaptive Data Hiding Scheme for Domain Based Secret Data in Random Order to Increase Steganography Using IWT

R. Indra Gandhi
Department of Computer Science and Engineering, Bharath University, Chennai, Tamil Nadu, India
Email: shambhavi.rajesh@gmail.com
Dr. K. P. Kaliyamurthie
Department of Computer Science and Engineering, Bharath University, Chennai, Tamil Nadu, India
Email: kpkaliyamurthie@gmail.com

ABSTRACT

In the recent trend steganography plays an important role in providing secrecy in internet. Steganography works by replacing bits of useless or unused data in regular computer files with bits of different, invisible information. Cryptography is used to scramble the information sent and make it as a scrambled text which is not understandable. Steganography is used to hide the information so that secrecy can be established. If Steganography and Cryptography are used together it has more advantage for providing security for the information. In this paper hiding of data in digital images formation carried out using adaptive hiding with the optimum pixel adjustment (OPA) algorithm. Resultant system evidences remarkable hiding rates with other Steganographic systems.

Keywords – **Data hiding, IWT, OPA, PSNR, Secret Key, Steganography.**

Date of Submission: March 01, 2015 Date of Acceptance: March 14, 2015

1 INTRODUCTION

Steganography works by replacing bits of useless or unused data in regular computer files with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images. Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen.

There are a large number of steganography methods that most of us are familiar with ranging from invisible ink and microdots to secreting a hidden message [1]. With computers and networks, there are many other ways of hiding information [2], such as:

- Covert channels
- Hidden text within Web pages
- Hiding files in "plain sight"
- Null ciphers

Steganography permits a user to hide large amounts of information within image and audio files. These forms of steganography often are used in conjunction with cryptography so that the information is doubly protected; first it is encrypted and then hidden so that an adversary has to first find the information and then decrypt it.

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 [3]. There are a number of uses for steganography one of the most widely used applications is for so-called digital watermarking[8] A watermark, historically, is the replication of an image, logo, or text on paper stock so that the source of the document can be at least partially authenticated. A digital watermark can accomplish the same function with an embedded signature so that others attempt to portray it can be avoided.

Digital watermarking and steganography techniques are used to address digital rights management, protect information, and conceal secrets [8]. Information hiding techniques provide an interesting challenge for digital forensic investigations. Information can easily traverse through firewalls undetected. Research into steganalysis techniques aids in the discovery of such hidden information as well as leads research toward improved methods for hiding information[5][6]. Nowadays all the messages are digitalized so that quality of message can be maintained properly after several operation on it .Among all digital file formats available nowadays image files are the most popular cover objects because they are easy to find and have higher degree of distortion tolerance over other types of files with high hiding capacity due to the redundancy of digital information representation of an image data [10]. We have

Volume: 6 Issue: 5 Pages: 2464-2467 (2015) ISSN: 0975-0290

two popular types of hiding methods; spatial domain embedding and transform domain embedding.

- *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.

2 INTEGER WAVELET TRANSFORM

A wavelet is a mathematical function used to divide a given function or continuous-time signal into different scale components [7]. Usually one can assign a frequency range to each scale component. Each scale component can then be studied with a resolution that matches its scale. A wavelet transform is the representation of a function by wavelets. The wavelets are scaled and translated copies (known as "daughter wavelets") of a finite-length or fast-decaying oscillating waveform (known as the "mother wavelet"). Wavelet transforms have advantages over traditional Fourier transforms for representing functions that have discontinuities and sharp peaks, and for accurately deconstructing and reconstructing finite, non-periodic and/or non-stationary signals.

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 [4][7], 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.

To manipulate 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 doesn't allow perfect reconstruction of the input image and in this case there will be no loss of information through forward and inverse transforms. Due to the mentioned difference between integer wavelet transform (IWT) and discrete wavelet transform (DWT) the LL sub band in the case of IWT [9] 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 as shown in Fig 1.

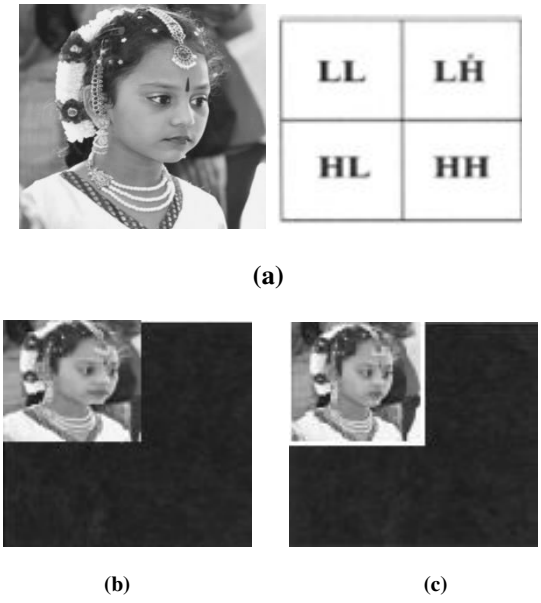

Figure 1. (a) Decomposition of image using wavelet filters
(b) 2DDW Technique Decomposition
(c) 2DIW Technique Decomposition

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. Fig 1 is an example showing how we can use lifting schemes to obtain integer wavelet transform by using simple truncation and without losing invariability.

3 PROPOSED SYSTEM

This proposed system is an adaptive data hiding scheme, in which randomly selected integer wavelet coefficients of the cover image are modified with secret message bits. Each of these selected coefficients hides different number of message bits according to the hiding capacity function. After data insertion, apply optimum pixel adjustment algorithm to reduce the error induced due to data insertion [11]. The block diagram is shown in Fig. 2. We can say that the proposed system is classified into three cases of operation based on different applications; Low hiding capacity with good visual quality (high value of peak signal to noise ratio "PSNR"), average hiding

Volume: 6 Issue: 5 Pages: 2464-2467 (2015) ISSN: 0975-0290

capacity with reasonable visual quality and high hiding capacity with low visual quality. We discuss each of these cases in next section.

3.1 PROPOSED ALGORITHM:

The block diagram of the embedding procedure is shown in Fig. 2 and extraction algorithm in Fig. 3. The blocks of the proposed algorithm explained in the following steps:

Step 1: Feeding input image as two dimensional arrays
Step 2: Introduction of IWT to prevent the gray scale value ranges >255 or smaller than O.
Step 3: Remap input image into 8x8 non overlapping blocks.
Step 4: Using IWT four sub bands transformation takes places, resulting LLI, LHI, HLI and HHI.

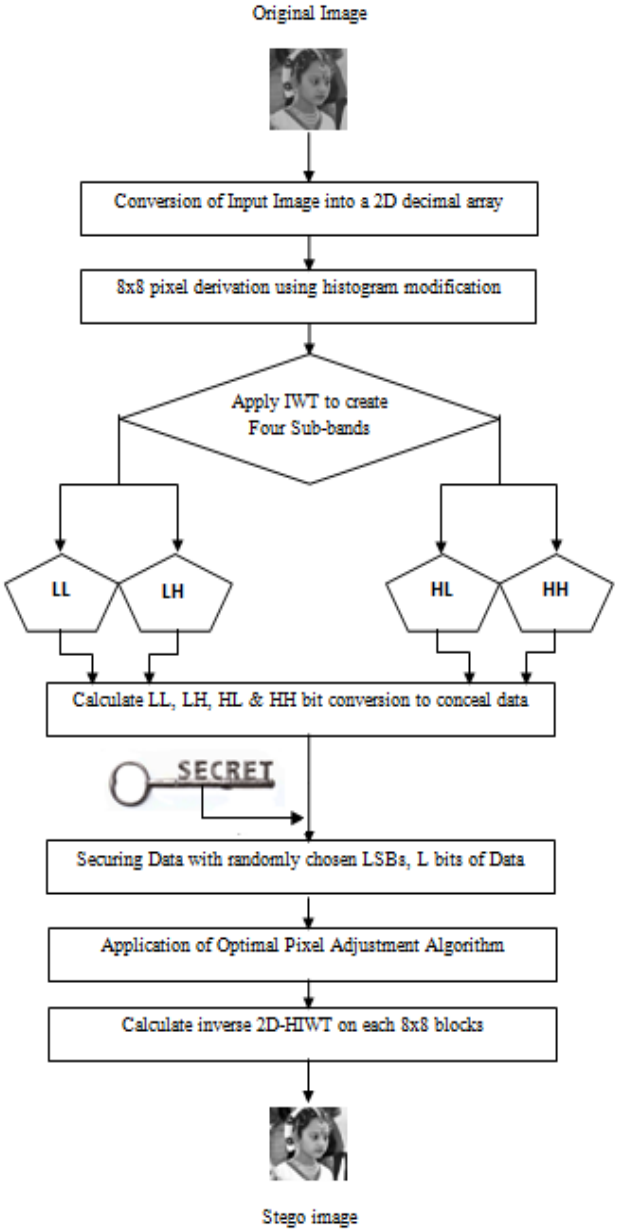

Figure 2: Original image Modification with Secret Key using 2D-HIWT

Step 5: Compute the length of LSBs, LSBs forms different values of k which divide the system into 3 cases based on the value of K
Step 5.1: If k is 1 this case provides low hiding capacity with high visual quality of the resultant-image.
Step 5.2: if k is 3 provide average hiding capacity with reasonable visual quality.
Step 5.3: if k is 4 provides high visual quality of the resultant image which is not important and the user requires only high hiding capacity.
Step 6: embed L bit of message with different coefficient and the coefficient is responsible for security of the message
Step 7: Use OPA where vale of L is calculated with respect to the value of wavelet coefficient. Here it is mainly used to minimize the error
Step 8: finally, calculate the inverse integer wavelet transform on each 8x8 block to restore the image to spatial domain.

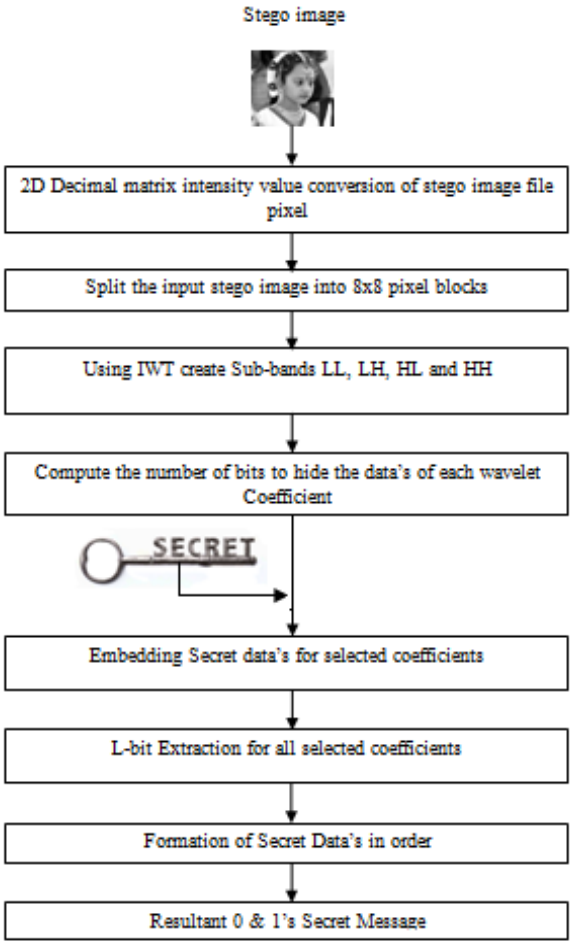

Figure 3: Embedding Stego Image using Wavelet Filters

4 EXPERIMENTAL RESULTS

The proposed system was applied to two typical 512x512 8-bit grayscale images shown in fig 2, it achieved satisfactory results against other systems using wavelet transform.

Volume: 6 Issue: 5 Pages: 2464-2467 (2015) ISSN: 0975-0290

The program was implemented using Matlab 7.5 running on 3.46 G dual core processor under Windows Vista. The secret message to embed is a randomly generated binary stream with the same length as the calculated hiding capacity.

V. CONCLUSIONS

In this paper we proposed a novel data hiding scheme that hides data into the integer wavelet coefficients of an image. The system combines an adaptive data hiding technique and the optimum pixel adjustment algorithm to increase the hiding capacity of the system compared to other systems. The proposed system embeds secret data in a random order using a secret key only known to both sender and receiver. It is an adaptive system which embeds different number of bits in each wavelet coefficient according to a hiding capacity function in order to maximize the hiding capacity without sacrificing the visual quality of resulting stego image. The proposed system also minimizes the difference between original coefficients values and modified values by using the optimum pixel adjustment algorithm. The proposed scheme was classified into three cases of hiding capacity according to different applications required by the user. Each case has different visual quality of the stego-image. Any data type can be used as the secret message since our experiments was made on a binary stream of data. There was no error in the recovered message (perfect recovery) at any hiding rate. From the experiments and the obtained results the proposed system proved to achieve high hiding capacity up to 48% of the cover image size with reasonable image quality and high security because of using random insertion of the secret message. On the other hand the system suffers from low robustness against various attacks such as histogram equalization and JPEG compression. The proposed system can be further developed to increase its robustness by using some sort of error correction code which increases the probability of retrieving the message after attacks, also investigating methods to increase visual quality of the resultant-image (PSNR) with the obtained hiding capacity.

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 image Steganographic Method Using Tri-way Pixel-Value Differencing," Journal of Multimedia, Vol. 3, No.2, June 2008.

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

[5] 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.

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

[7] P. Chen, and H. Lin, "A DWT Approach for image Steganography," International Journal of Applied Science and Engineering 2006. 4, 3: 275:290.

[8] 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.

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

[10] G. Xuan, J. Zhu, Y. Q. Shi, Z. Ni, and W. Su., "Distortion less data hiding based on integer wavelet transform," IEE Electronic Letters, 38(25): 1646--1648, Dec. 2002.

[11] Lillo M. Shih, "Generalizations of Pixel-Value Differencing Steganography for Data Hiding in images", Fundamental Informaticae, vol. 83, no, pp. 319-335, 2008.

Author Biography

Indra Gandhi Raman is a researcher for more than 18 years, specializing in the field of character distortion. She has completed her doctorate in Computer Science and also holds post graduation degrees in four different departments namely Mathematics, Computer Science, Management and Psychology. Her area of interests includes AI, Neural Network, Cryptography and Software Engineering. She did her Ph.D., research on Distorted Character Recognition using Neural Networks. She can be contacted through Email:shambhavi.rajesh@gmail.com

Dr.K.P.Kaliyamurthie is self-directed, enthusiastic educator with a commitment on student development. He is with Bharath University, Chennai, Tamil Nadu, India as Professor and Head of the Department of Computer Science and Engineering. He has over 24 years of rich experience in teaching along with student administration. He has guided more than 300 UG, PG projects and organized various national level conferences. He served as Senior Chair, Technical advisor in various national level conferences and Technical Committee member in International Conferences. He is an active member in CSI, IEEE, ISTE, ACM etc., His area of interests includes Data Mining and Warehousing, Networks and Software Engineering. He can be contacted through Email:kpkaliyamurthie@gmail.com