

Image Steganography Scheme Using Neural Network in Wavelet Transform Domain

Anamika Sharma¹, Ajay Kushwaha²

¹M.Tech Scholar Computer Science, Rungta College of Engineering, Bilhailai, Durg, Chhattisgarh, India

²Assistant Professor, Rungta College of Engineering, Bilhailai, Durg, Chhattisgarh, India

Abstract: 'Steganography is a art, which enforcing for obscure one part of data or information within another'. This paper proposed an image steganography scheme which based on neural network fusion in wavelet transform domain. The cover and stego image is dividing in its frequency coefficients components by wavelet transform domain, and neural network used as classifier. Proposed method trying to accomplish satisfactory imperceptibility, robustness and appraise the performance of the several attacks by using different type of wavelet families. All experimental result for this proposed method will be performed in MATLAB language.

Keywords: Steganography, Wavelet Transform, Neural Network, Fusion Process

1. Introduction

The phrase Steganography comes out from Greek 'Stegano' based on cover or secret and 'Graphy' based on drawing or writing. Steganography's main objective is cover-media hide a confidential message in such a manner that cannot recognize by other compartment of the hidden message.

Types of Steganography

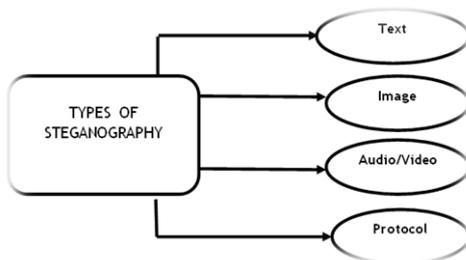


Figure 1: Classification of Steganography

1.1. Text Steganography

It is a most important method of steganography to hide information's in form of texts. Secret message can be hidden in every text message's nth letter of every word. It has decreased its importance after Internet prosperous and different formats type of digital file. Because the text files have a small amount of repeated digital data files is not used in using text stenography.

1.2. Image Steganography

As the popular cover objects in steganography images are used in teas. In a digital image, secret key a message is embedded through an embedding algorithm. The resulted stego image can be send to the receiver. On the other side, the same key is processed by the extraction algorithm. During the stego image transmission, unauthenticated persons only noticed the image transmission but can't guess that hidden Image message is exist. Steganography techniques can broadly categorize: Spatial-domain based Transform domain based Steganography.

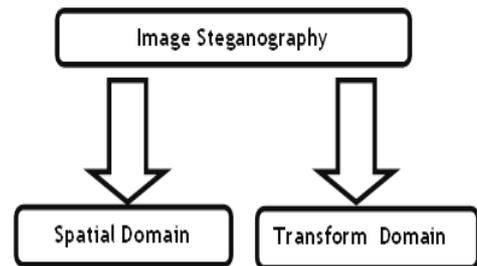


Figure 2: Image Steganography Classification

1.2.1. Spatial Domain Method

In spatial Domain Method, the secret message is immediate (embedded) planted. The LSB insertion method is most uncomplicated & normally use for this steganography. In this technique, pixels's least sign bit are substituted by the message bits which are transposed before embedding.

1.2.2. Transform Domain Method

In this method, we can hide a large amount of high security data, so secret messages have good invisibility with no loss. The digital image is compounded by low and high frequency constituents. Low frequency content map by blend and plane region, high frequency components contribute the sharp and edge transitions importantly. Low frequency regions are more sensitive; whatever change in them will be transparent to the human visual system. Hence, in both low & high frequency parts, it's not viable to hide an equal amount of data. Also, pixel in the low frequency area is strongly correlated with its neighbours whereas it greatly varies from its neighbours in high frequency areas. With this it concludes that analyzes and obtains the image in the frequency domain which help to achieve efficient embedding data. And at last the observable states that transform domain schemes are less prone to attacks.

DWT based Steganography: Description of wavelet transformation can be applied as multiresolution process decomposition in terms of an image elaborated onto a lot of basis wavelet functions. DWT shows its own, property of excellent frequency space localization. In each dimension image processing is filtered by 2D filter & corresponding result can be applied to 2D DWT images. The input image classified by filters in 4 non-overlapping multiresolution

sub-band, LL (Approximated coefficient), LH (vertical), HL (horizontal) and HH (diagonal).

The LL sub-band can further continue to receive next scale of wavelet coefficients, until final scale N is gain. Once N is accomplish, we'll have $3N+1$ sub-bands which is lie on multi-resolution sub-bands (LLN), (LHX), (HLX) and (HHX) where X ranges start from 1 to N. Image energy almost stored by these drops.

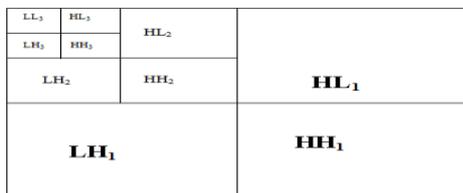


Figure 3: Three level decomposition using DWT

IWT based Steganography: A Nonlinear transform having a social organisation of lifting scheme and rate deformation is known as Integer Wavelet Transform. IWT performance based on the representation of integers to integers and they also allow perfect reconstruction of original pictures. IWT transforms an integer data into another set of integer data.

In DWT, wavelet filters hide data in floating point coefficients, floating point pixel values transform on integers so that some hidden information may be less. Which may directly failure of the data hiding scheme?

1.3 Protocol Steganography

Protocol Steganography refers as embedding information technique within network protocols & messages used on the transmission network. Sometimes may be information can be hide in the TCP/IP packet header or never applied in any subject areas.

1.4 Audio Steganography

Also we can apply another form that is Audio Files for hiding secret data. Where secret messages embedded in the digital audio form. timing is an another unique and different technique for audio coding, where properties work for human ear to hide unnoticeable information. Another audible louder sound is whenever present then significant audible sound is unreachable. In this properties allow to select the channel where information can be hiding. [1-4]

2. Neural Network

The neural network is an optimization technique. Neural is being used as a classifier. Neural networks are being organized in layers. When an element of the neural network fails, Neural Network can continue without any problem because of their parallel nature. An artificial neural network consists of an interconnected group of nodes called neurons. Each circular node represents an artificial neuron and an arrow represents a connection from the output of one neuron to the input of another. Neural is composed of three layers. Input layer means Training set and trained target which passed as input to neural. Hidden layer concerned

with the number of iterations at which given the best result. Output layer are generate final result.

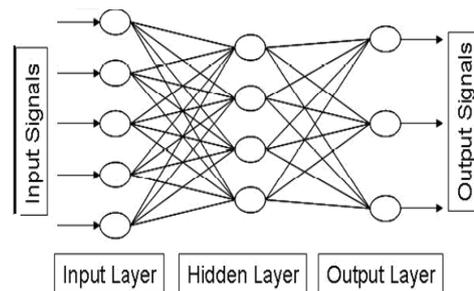


Figure 4: Structure of Neural Network

Neural network are classified as both feed-forward and feed-back network. There are some neural network techniques are given for learn the network.

2.1. Back Propagation Network

It is a feed forward technique, which calculate and minimize the generated error during network learning.

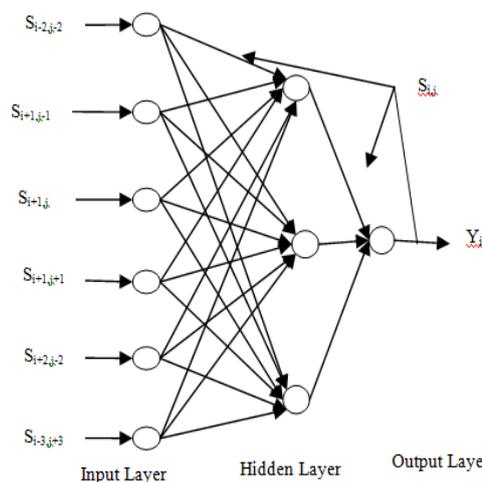


Figure 5: Back Propagation Neural Network

2.2. Fuzzy Neuro System

Fuzzy neuro system has two different types:

- A) Fuzzy logic designing for neural network
- B) Neural network designing for fuzzy logic.

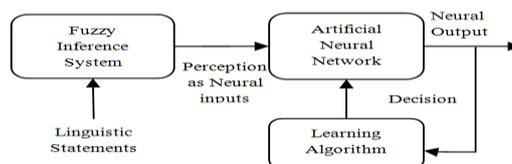


Figure 6: Fuzzy Neuro System

3. Related Work

G. Prabhakaran et.al [5] propose their research on the concentration for perfecting the visible effect of stego image and robustness against several approaches by applying fusion process of DWT & IWT .they conclude that, dual approach observe the combination of DWT & IWT, and execute better visible quality, embedding capacity

and computational capacity. Embedding methods for both DWT & IWT obtain PSNR & high imperceptibility values placed between 35-54 db.

Ramamurthya N. et.al [6] proposed method worked on image watermarking based back propagation neural network in DWT domain, this paper worked on 8*8 bitmap image. Their work was robust for noising, compression, and rotation etc.

Aradhana Sharma et.al [7] proposed and told about the work on an image steganography technique which combines the DWT and DCT. According to them research on 3 level wavelet decomposition carrying a single level of cover image and processing the image as 4x4 blocks with DCT. Regarding all methods and their observations it is conclude that this approach combination is capable for accomplish more imperceptibility & security. As per their study of 3 levels DWT and DCT provide a deep depth value to hide the secret image with PSNR values ranged between 43-48 db.

With the help of IWT, colour cover image hide the multiple secret image and keys, **Hemalatha S et.al [8]** research paper provide a steganography image technique, where no visual difference between cover and stego image. The extracted secret images look similar as original secret images. Also observed that, in single colour image two secret images can be hide.

Hemalatha S et.al [9] performed their work and proposed that secret image could be hidden by considering the three separate colour component. But secret image hidden by keys that are generated using the corresponding colour components and the keys are hidden in the respective colour components of the cover image. Secret image can be extracting by using keys. IWT is using for hide the keys. Their result shows the technique gives good quality stego images with better PSNR values compared to similar other techniques.

Neda Raftari et.al [10] proposed work suggesting for transform the cover & secret images from both spatial into frequency domain IWT is uses, assignment algorithm is use for find good match between blocks for embedding. In which secrete image is embedded by different coefficient band cover image. At last with the conclusion the results shows that after applying attacks on stego images, the secret images have good value of PSNR and acceptable visual quality. In addition, for extracting the embedded secret image original cover image does not require.

S.K.Muttoo et.al [11] According to their works, they propose a revocable steganographic image embedding algorithm, consist of three parts. Firstly, original text message are compress or encoded, they use self-synchronization variable codes, T-codes. Secondly, again encrypted the gain encoded binary string by AES improved method. In high frequency bands embed encrypted message, which is obtaining by apply DD DT DWT 1-level decomposition from cover image. This algorithm is comparing with DWT based corresponding algorithm and where is founded that it is good embedding capacity, robustness and imperceptibility.

Jagadeesh B.et.al [12] proposed a combination method of fuzzy logic and artificial neural. Fuzzy neuro system is use for this method. That method was experimented on various image attacks, which gave better robustness as result.

H S Manjunatha Reddy et.al [13] stated that, cover image is sectioned in 4*4 cells & DWT or IWT will be applying on apiece cell. HH band of 2*2 cell of DWT or IWT are consider and manipulating by payload bit pairs (by using identity) matrix to obtain stego image. Key is uses for payload pairs bit extracted at the destination. For all image formats IWT compare by DWT & it is observed that PSNR values are better. The proposed algorithm is robust since the payload is embedding into the transform cover image indirectly. In future the algorithm can be tested with some more transform domain techniques which will be improved the performance.

Seongho Cho a et.al [14] experiment tells about a Traditional image steganalysis which conducted by the entire image frame respectively. In this work, they differentiate a stego image from its cover image based on the decomposition of images into smaller blocks, and then the whole image will be obtain by all image blocks integrating results via decision fusion. After the observation and results they concluded that the performance of this image steganalysis is less sensitive for decision fusion methods but more sensitive for the classifier choice.

Juned Ahmed Mazumder et.al [16], presented a DWT using high security steganographic technique & optimized message propogeting method. Here they used Haar wavelet which decomposes both cover image into high and low frequency information. Where high frequency contains information about the edges, corners etc. Secret Message is introduced into high frequency sub-band R, G, B colour components which started from each of the colour component's last column from top bottom approach depend on the message length. To measuring the imperceptibility of the method they used MSE and PSNR. For this experiment we have taken four image formats: PNG, BMP, JPEG and TIFF. Their experimental result state that compare from other methods the Capacity & MSE are amended with satisfactory PSNR.

V.Meiamai et.al [18] proposed the uses of pixel indicator channel which is deciding uses of histogram technique to secret message file that has to be embedded in the highest color intensity plane. Their result after observing the method efficiency can be enhanced by authenticating the user with a key.

4. Proposed Work

Proposed work tells about the dual transform technique by applying fusion process which may include arithmetic operations and logical operations.itz significance is that even with the large messages size there is high invisibility. This proposed method will be implemented in MATLAB language.

A. Embedding Process:

1) In existing algorithm, G. Prabhakaran et.al [5] embedded cover & stego image by DWT or IWT.

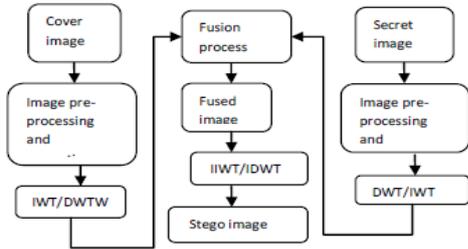


Figure 7: Existing Embedding Model

2) Proposed embedding process Algorithm:

- a) Firstly Read the cover image as C. Convert cover image pixel values into image (CG).
- b) Apply image pre-processing and then process correction to get colour cover image (CG).
- c) Read the secret image (S).
- d) Apply image reprocessing and correction process to get a image as (SG).
- e) Apply dual transforms technique into both cover & secret image.
- f) By applying Wavelet Transform, extract the approximated coefficients of matrix of the cover image (CG1).
- g) By applying Wavelet Transform, extract the approximated coefficients of matrix of the secret image (SG1).
- h) Neural Fusion operation will be applying on image CG1 and SG1 to getting merge image.
- i) Fused image will be performing by 2-D Inverse Wavelet Transform to get the stego image.

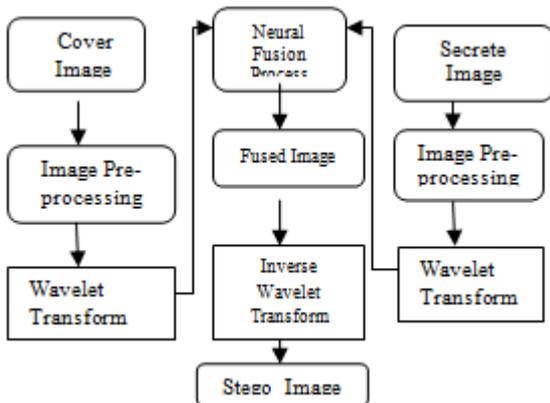


Figure 8: Purposed Embedding Method

B. Extracting Process:

1) In existing algorithm, G. Prabhakaran et.al [5] extracted cover & stego image by DWT or IWT wavelet.

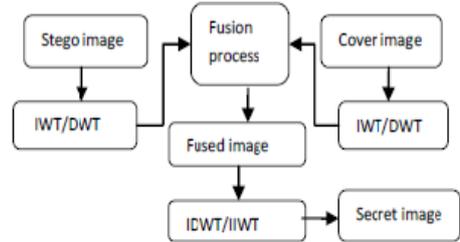


Figure 9: Based Extracting Model

2) Algorithm for proposed extracting process:

- a) Firstly get the stego image. And a 2-D Wavelet Transform will be performing at both cover and stego image level.
- b) Neural Fusion process will be applied on stego and cover images to getting fused image.
- c) Wavelet coefficients will be separated and applied Inverse Wavelet Transform on the fused image to recover the secret image.

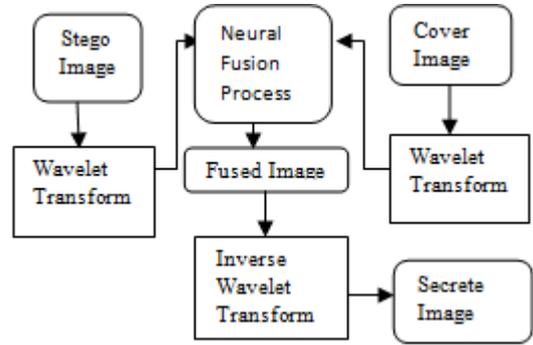


Figure 10: Purposed Extracting Method

5. Expected Result



Figure 11 (a): Cover Image



Figure 11 (b): Secret Image



Figure 11 (c): Stego Image

Performance Analysis: Performance analysis of these transforms is done based on below parameters.

PSNR is used for measuring the quality of the Secret image (reconstructed image) that usually expressed as decibels (db), which is a logarithmic scale. Cause of lack of a universal image quality measurement tool us always using PSNR to evaluate the deformation between the stego & original cover images.

MSE representing the difference Between of the original colour cover image which has $M \times N \times$ size and the get stego image which has $M \times N \times$ size, and the pixel $(x_{j,k}$ and $x'_{j,k}$) are located on the j th row of the k th column of images (cover) x and (stego) x' , respectively.

There are following quality metrics formulas are given,

1) Mean Square Error

$$MSE = \frac{1}{MN} \sum_{j=1}^M \sum_{k=1}^N (x_{j,k} - x'_{j,k})^2 \quad (1)$$

2) Pick Signal To Noise Ratio

$$PSNR = 10 \frac{\log_{10}(255)^2}{MSE} \text{ dB} \quad (2)$$

3) Normalized Cross Correction

$$NCC = \frac{\sum_{j=1}^M \sum_{k=1}^N (x_{j,k} - x'_{j,k})}{\sum_{j=1}^M \sum_{k=1}^N (x'_{j,k})^2} \quad (3)$$

4) Average Difference

$$AD = \frac{\sum_{j=1}^M \sum_{k=1}^N (x_{j,k} - x'_{j,k})}{MN} \quad (4)$$

5) Structural Content

$$SC = \frac{\sum_{j=1}^M \sum_{k=1}^N (x_{j,k})^2}{\sum_{j=1}^M \sum_{k=1}^N (x'_{j,k})^2} \quad (5)$$

6) Maximum Difference

$$MD = \text{MAX}(|x_{j,k} - x'_{j,k}|) \quad (6)$$

7) Normalized Absolute Error

$$NAE = \frac{\sum_{j=1}^M \sum_{k=1}^N |x_{j,k} - x'_{j,k}|}{\sum_{j=1}^M \sum_{k=1}^N |x'_{j,k}|} \quad (7)$$

6. Conclusion

This proposed technique mainly concentrates on to gain better robustness and imperceptibility based on several

image attacks like cropping, rotation, and noising. The result will also check visual perfection quality of stego image. In this method colour image will be converted into grey image. It is applicable on to hide online content distribution system, secret communication, internet security & medical imaging systems.

References

- [1] Mangesh Ghonge¹, Ankita Dhawale², Atul Tonge³. "REVIEW OF STEGANOGRAPHY TECHNIQUES" International Journal of Advent Research in Computer & Electronics (IJARCE) Vol.1, No.1, March 2014 35.
- [2] Mansi S. Subhedara^{*}, Vijay H. Mankarb "CURRENT STATUS AND KEY ISSUES IN IMAGE STEGANOGRAPHY: A SURVEY" 1574-0137/© 2014 Elsevier.
- [3] Kanzariya Nitin K., Nimavat Ashish V. "COMPARISON OF VARIOUS IMAGES STEGANOGRAPHY TECHNIQUES" International Journal of Computer Science and Management Research Vol 2 Issue 1 January 2013 ISSN 2278-733X
- [4] Banasthali Vidyapith, "IMAGE STEGANOGRAPHY TECHNIQUES: A REVIEW ARTICLE" ACTA Technica Cornvinensis July-September 2013.
- [5] G. Prabakaran, Dr. R. Bhavani, K Kanimozhi "DUAL TRANSFORM BASED STEGANOGRAPHY USING WAVELET FAMILIES AND STATISTICAL METHODS" International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 21-22 978-1-4673-5845-3/13/\$31.00©2013 IEEE
- [6] Ramamurthya N., Varadarajanb S. "THE ROBUST DIGITAL IMAGE WATERMARKING SCHEME WITH BACK PROPAGATION NEURAL NETWORK IN DWT DOMAIN" INTERNATIONAL CONFERENCE ON MODELLING OPTIMIZATION AND COMPUTING elsevier 2012 Volume 38, 2012, Pages 3769-3778
- [7] Aradhana Sharma¹, Ahmed Mohammed "THREE LEVEL WAVELET DECOMPOSITION HYBRID TRANSFORM IMAGE STEGANOGRAPHY" International Journal Of Advanced Electronics & Communication Systems Approved By Csir-Niscair Issn No: 2277-7318 Issue 2 Vol 3, Apr-May-2014 Paper Id 84-117-1-S
- [8] Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath, "A SECURE AND HIGH CAPACITY IMAGE STEGANOGRAPHY TECHNIQUE" Signal & Image Processing : An International Journal (SIPIJ) Vol.4, No.1, February 2013 DOI : 10.5121/sipij.2013.4108 83
- [9] Hemalatha S., U Dinesh Acharya, Renuka A. and Priya R. Kamath, "AN INTEGER WAVELET TRANSFORM BASED STEGANOGRAPHY TECHNIQUE FOR COLOR IMAGES" International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 3, Number 1 (2013), pp. 13-24
- [10] Neda Raftari and Amir Masoud Eftekhari Moghadam "DIGITAL IMAGE STEGANOGRAPHY BASED ON INTEGER WAVELET TRANSFORM AND

- ASSIGNMENT ALGORITHM" 978-0-7695-4730-5/12 \$26.00 © 2012 IEEE DOI 10.1109/AMS.2012.15
- [11] Tanmay Bhattacharya, Nilanjan Dey, S. R. Bhadra Chaudhuri Professor, "A SESSION BASED MULTIPLE IMAGE HIDING TECHNIQUE USING DWT AND DCT" International Journal of Computer Applications (0975 – 8887) Volume 38– No.5, January 2012 18
- [12] Jagadeesh B., Praveen Kumar D. "Fuzzy-Neuro based Robust Digital Image Watermarking Technique" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 7, July 2014
- [13] S.K. Muttoo, Sushil Kumar, "A MULTILAYERED SECURE, ROBUST AND HIGH CAPACITY IMAGE STEGANOGRAPHIC ALGORITHM" .World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 1, No. 6, 239-246, 2011 239
- [14] Sherin Youssef, Ahmed Abu Elfarag, Reta Raouf, "A ROBUST STEGANOGRAPHY MODEL USING WAVELET-BASED BLOCK-PARTITION MODIFICATION" International Journal of Computer Science & Information Technology (IJCSIT) Vol 3, No 4, August 2011 DOI : 10.5121/ijcsit.2011.3402 15
- [15] H S Manjunatha Reddy, K B Raja. "WAVELET BASED NON LSB STEGANOGRAPHY" Int. J. Advanced Networking and Applications 1203 Volume: 03; Issue: 03; Pages:1203-1209 (2011)
- [16] Seongho Cho, Byung-Ho Cha, Martin Gawecki a, C.-C. Jay Kuo , "BLOCK-BASED IMAGE STEGANALYSIS: ALGORITHM AND PERFORMANCE EVALUATION" 1047-3203/\$ - see front matter 2013 Elsevier Inc. All rights reserved.
- [17] Elham Ghasemi, Jamshid Shanbehzadeh, and Nima Fassihi "HIGH CAPACITY IMAGE STEGANOGRAPHY BASED ON GENETIC ALGORITHM AND WAVELET TRANSFORM", in Electrical Engineering 110, DOI 10.1007/978-1-4614-1695-1 30, © Springer Science+Business Media, LLC 2012
- [18] Juned Ahmed Mazumder, Kattamanchi Hemachandran, "COLOR IMAGE STEGANOGRAPHY USING DISCRETE WAVELET TRANSFORMATION AND OPTIMIZED MESSAGE DISTRIBUTION METHOD", International Journal of Computer Sciences and Engineering Vol.-2(7), PP(90-100) July 2014, E-ISSN: 2347-2693
- [19] V.Meiamai, A.Minu, R.Anushia Devi "HISTOGRAM TECHNIQUE WITH PIXEL INDICATOR FOR HIGH FIDELITY STEGANOGRAPHY" International Journal of Engineering and Technology (IJET) Vol 5 No 3 Jun-Jul 2013