International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-5, June 2020

A Juxtaposition Between Integer Wavelet Transform and Discrete Wavelet Transform for Secure Image Steganography

Ravi Ranjan, Subham Thirani, M.Jasmine Pemeena Priyadarsini, G.K.Rajini, A.Jabeena

Abstract: ***Image steganography is a technique that is used to hide information. The information can be of various types like image, video, or audio. Steganography is done so that no one apart from the correct receiver can retrieve the information. This paper consists of all advantages and highlights of the wavelet transform but with the additional features like randomness and some default values that are already built-in it. Various algorithms can be used in steganography and they provide good hiding capacity and low detectability. Here we have hidden the image into the cover image using Integer Wavelet Transform (IWT) and also using Discrete Wavelet Transform (DWT) and compared which technique gives better results. It is very difficult to predict the presence of a hidden image inside the stego image since it looks exactly like the cover image. There is no loss in quality from the secret image to the extracted image since the PSNR (Peak Signal to noise ratio) is high for both of them. This process was done using both DWT and IWT and the results prove that that the IWT technique is not only simpler but also more efficient than the DWT technique since it gives higher PSNR values. Through the proposed algorithm, an increase in the strength and imperceptibility is noticed and it can also maintain various transformations such as scaling, translation, and rotation with algorithms that already exist. The final results, after comparing both the transforms prove that the algorithm which is being proposed in IWT is indeed effective***

Keywords: Discrete Wavelet Transform, Integer Wavelet Transform, MSE, PSNR, Steganography.

I. INTRODUCTION

Nowadays, hiding information is an extremely important aspect of information security. There are various techniques to provide security and one of them is steganography. Earlier there weren't many security issues except copyright protection. But nowadays due to an increase in computer networks, we need to hide the information into some other medium such as image, audio, or video [1]. Steganography of the image using the transform domain approach transforms the hidden image into the image of the cover embedding the secret image in it.

Revised Manuscript Received on June 15, 2020.
* Correspondence Author
Ravi Ranjan*, School of Electronics Engineering,, Vellore Institute of Technology, Vellore, India. E-mail: ravi.ranjan2016@vitstudent.ac.in
Subham Thirani, School of Electronics Engineering,, Vellore Institute of Technology, Vellore, India, E-mail: subham.thirani2016@vitstudent.ac.in
M.Jasmine Peemena Priyadarsini, School of Electronics Engineering,, Vellore Institute of Technology, Vellore, India, E-mail: jasmin@vit.ac.in
G.K.Rajini, School of Electronics Engineering,, Vellore Institute of Technology, Vellore, India, E-mail: rajini.gk@vit.ac.in
A.Jabbena, School of Electronics Engineering,, Vellore Institute of Technology, Vellore, India, E-mail: ajabeena@vit.ac.in

They're inserted in the cover picture frequency bands to reinforce them and make them more resilient for attacks. That also makes the exchange of confidential information much more appropriate. The original image is known as the cover image. The cover image along with the hidden image is known as stego image. Any unauthorized user will not be able to identify that there is a hidden image within the stego image [20]. Only the authorized recipient will be able to retrieve the confidential information. Steganography systems can be categorized into various transform domain and spatial domain methods [15]. Here, we use IWT and DWT to design the steganographic system and then compare the two methods.

A. Integer Wavelet Transform

Maximum information hiding techniques perform their embedding process by changing the contents of various media like image, video, and audio [6]. Due to this, there is some distortion in the cover image during extraction and as a result of this an analyzer can try to extract the confidential information [18]. These attacks can be prevented by using an Integer Wavelet Transform (IWT). To avoid distortion, IWT is a very efficient method because it maps integers to integers [9]. There are four sub-bands LL, LH, HL, and HH [14]. Among these four layers, in IWT, the LL subband is a very close copy of the original image on a smaller scale. Several methods of concealing data perform information embedding by modifying the composition of a source media. As a result, while extraction it causes some distortion in the cover image and thus the steganalyzer can try to extract the secret information [3]. This can be avoided by using Integer Wavelet Transform. The proposed algorithm uses the wavelet to convert coefficients to embed messages into four subbands of transforming a two-dimensional wavelet [19]. We used Integer Wavelet Transform to prevent problems with floating-point precision of the wavelet filters

B. Discrete Wavelet Transform

DWT offers information on frequency and time domain simultaneously. Firstly, the time domain is passed through both low-pass and high-pass filters so that we can extract both low and high frequencies respectively [4]. This process is repeated many times and each time some part of the signal is drawn out.DWT mainly utilizes scaling and wavelet functions which are associated with low pass and high pass filters [10].

This feature is useful in bisecting time reparability [17].

Here we use the Haar wavelet which operates on data by computing the sums and differences of adjacent elements. [8] It first operates on adjacent horizontal elements and later on horizontal elements. An excellent property of the Haar wavelet transform is that the transform is equal to its inverse. [7]. in 1-level DWT, with the help of high pass filter and low pass filter inputs are convolved. In 2-level DWT, initially 1-level DWT is applied to all rows and then to all columns [12].

II. METHODOLOGY

A. Taking Input

- We take a 256 x 256 secret gray scale image and 512 x 512 cover image. We also give an embedding coefficient as input.

B. Embedding Process

- Split RGB color image in three cover planes i.e. Red, Green, and Blue.
- Take the green plane of the cover image and compute DWT and IWT by operating on it.
- Divide the output image of the DWT and IWT into wavelet sub-bands i.e. Low Low (LL), Low High (LH), High Low(HL), High High(HH).
- Take the secret image and divide it and the LL sub-band of IWT and DWT into non-overlapping blocks of equal size.
- Embed the secret image into LL sub-bands of IWT AND DWT using the expression:

  ((1-alpha)*block1)+ (alpha*block2)

  Block 1 represents the block of LL subband of IWT and DWT of the cover image, Block 2 represents the block of the secret image, Alpha represents the embedding coefficients [13].

C. Performing Inverse Transform

- Compute IIWT and IDWT and stego image with respect to a green plane is obtained and then combine Red and Blue plane information to the stego image.
- Stego output image of 512 X 512 image is obtained and it is a color image.

D. Extraction Process

- On the stego image compute IWT and DWT.
- The extraction process is performed using

  (par1-((1-alpha)*par2))./alpha

  Par 1 represents LL band of stego image, par2 represents secret image, Alpha represents embedding coefficient, Hidden image is extracted from stego image

E. Parameters Calculation

- PSNR and MSE values for stego and the secret image is calculated

F. Comparison Of Both Methods

- Comparisons of IWT and DWT method of steganography are compared based on PSNR and MSE values.

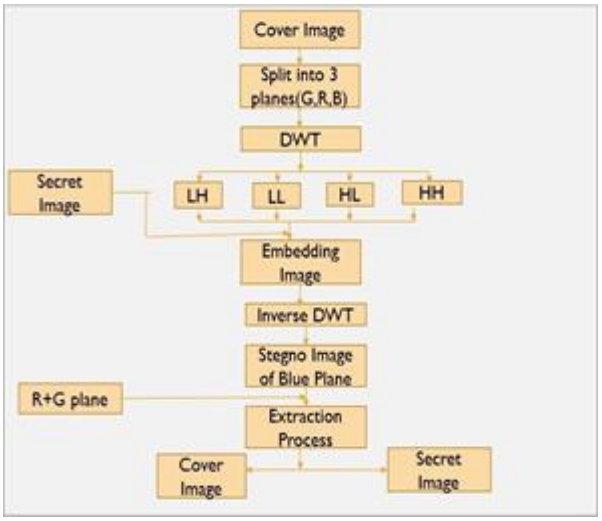

Fig 1: Proposed Algorithm for the DWT method

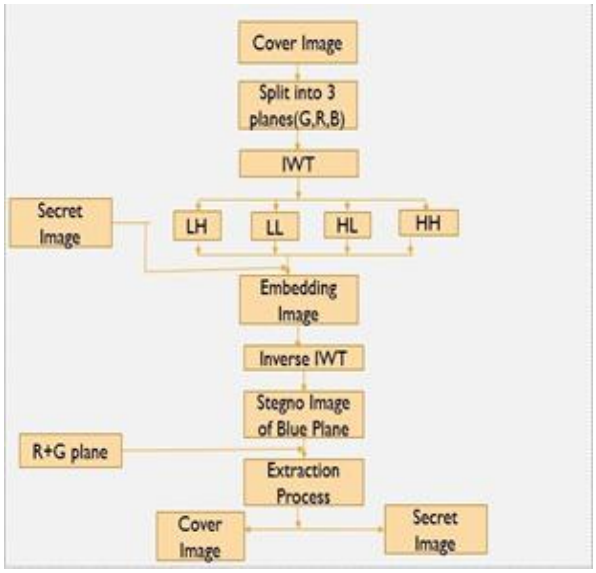

Fig 2: Proposed Algorithm for IWT method

III. RESULT AND ANALYSIS

We need to compare and evaluate both the algorithms used for image steganography. To analyze it we will use Fabirc.jpg as an input image and Mandi.tif as a secret image. The cover image is of size 512 x 512 pixels and the secret image has a size of 256 x 256 pixels [5]. They are shown in Fig 2 a and b respectively. One level DWT and IWT is performed on the blue plane of the cover image and is shown in Fig 3. As we know that almost all the energy is concentrated in the Low-low (LL) band, hence it is taken for embedding the LL band [2]. The LL band of the IWT and DWT is shown in Fig 4. The secret image is embedded into the LL band of the DWT and IWT of the cover image using the formula (1) and after that IIWT (Inverse Integer Wavelet transform) and IDWT (Inverse Discrete Wavelet Transform) is performed. As a result, a stego image is obtained which contains both cover image and secret image as shown in Fig 5 and 6 respectively.

Unauthorized users will not be able to recognize the secret picture embedded inside the cover image. The stego image is rather imperceptible and stable and the changes in the images are not detected. The extraction process is performed to get the hidden image from the stego image, and the secret image is obtained as a result [16]. The extracted image is shown in Fig. The performance of both the algorithms is evaluated and proves that IWT is superior to DWT.

(a)Cover image of size 512 x 512 (b)Secret image of size 256 x 256

Fig 3: Cover image and Secret image

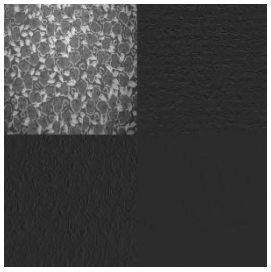

Fig 4: One-level IWT of Cover image

Fig 5: LL band of DWT of Cover image

Fig 6: Stego image

Fig 7: Extracted Secret Image

Performance measures: The efficiency of the technique proposed is estimated using commonly used metrics such as PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error) [11].

Performance comparison of IWT and DWT: The evaluation of performance measure of IWT and DWT for different cover and secret images are done.

PSNR for stego image for both DWT and IWT is shown in Table 1. PSNR for extracted image for both DWT and IWT is shown in Table 2. MSE for stego image for both DWT and IWT is shown in Table 3. MSE for extracted image for both DWT and IWT is shown in Table 4.

	DWT			IWT		
Cover Image	Secret Image			Secret Image		
	Trees	Mandi	Camera- man	Trees	Mandi	Camera- man
Fabric	290.1	290.8	290.7	309.3	309.28	309.16
Pepper	291.1	291.07	291.14	311.02	311.06	311.014
Pears	285.7	285.85	285.80	305.694	305.89	305.767

Table 1: PSNR for stego image for both DWT and IWT

	DWT			IWT		
Cover Image	Secret Image			Secret Image		
	Trees	Mandi	Camera - man	Trees	Mandi	Camera - man
Fabric	40.64	42.05	42.758	36.64	37.80	38.50
Pepper	40.33	41.56	40.679	36.26	37.49	36.560
Pears	34.83	35.76	37.09	30.076	31.62	33.051

Table 2: PSNR for extracted image for both DWT and IWT

	DWT			IWT		
Cover Image	Secret Image			Secret Image		
	Trees	Mandi	Camera - man	Trees	Mandi	Camera - man
Fabric	5.59	4.068	3.446	14.705	10.774	9.193
Pepper	6.022	4.499	5.547	15.50	11.60	14.35
Pears	21.27	17.528	12.692	54.337	44.2413	32.553

Table 3:MSE for stego image for both DWT andIWT

	DWT			IWT		
Cover Image	Secret Image			Secret Image		
	Trees	Mandi	Camera - man	Trees	Mandi	Camera - man
Fabric	5e-25	5e-25	3.5e-25	7.6e-27	7.5e-27	7.88e-27
Pepper	5e-25	5e-25	4.9e-25	4.8e-27	5.1e-27	5.2e-27
Pears	1e-24	1e-24	1.7e-24	1.7e-26	1.6e-26	1.7e-26

Table 4:MSE for stego image for both DWT andIWT

Analysis of different frequency sub-bands for IWT and DWT: In the Fig-7 shown below, it can be seen that LL and LH sub-band for IWT performance is better than DWT [14] but it is contrasting in HL and HH sub-band.

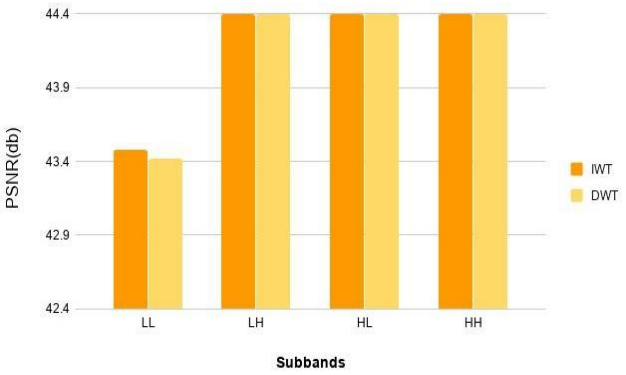

Fig 8: Comparison of IWT and DWT for different subbands

IV. CONCLUSION

In this paper, the secret image can be extracted from the original image without any distortion using both the algorithms. The higher the PSNR value, the less distortion. IWT is a more powerful way of concealing classified knowledge without distortion. Integer to Integer mapping is done in IWT. Whereas in DWT the resulting output does not consist of integers if the input consists of integers. The resulting output can be labeled with integers altogether in the case of IWT which can be seen in the PSNR value of both the algorithms. Thus IWT is better than DWT. Hence, it will allow us to independently transmit the secret information to the receiver, making it almost impossible for any unintended users to extract the secret information and recover the original host image when they access the Stego image.

This approach provides good Stego-image efficiency with lower PSNR values compared to other approaches. This method, however, will allow us to independently transmit the secret information to the receiver, making it almost impossible for any unintended users to extract the secret information and recover the original host image when they access the Stego image. Hence, secret information can be transmitted safely without altering the original cover image.

REFERENCES

1. Katzenbeisser, S. and Petitcolas, F.A.P., " Information Hiding Techniques for Steganography and Digital Watermarking." Artech House, Inc., Boston, London,2000.
2. Ahmed A. Abdelwahab and Lobna A. Hassaan, "A Discrete Wavelet Transform Based Technique For Image Data Hiding", 25th National Radio Science Conference, 2008.
3. Anitha Gnana selvi. J, Maria kalavathy.G, 2019. Probing Image and Video Steganography based On Discrete Wavelet and Discrete Cosine Transform: 589-595.
4. International Telecommunication Union (ITU), 1992. Information Technology- Digital Compression and Coding of Continuous-Tone Still Images- T.81. ITU Sept. 1992.
5. M.F. Tolba, M.A. Ghonemy, I.A. Taha, A.S. Khalifa, " Using Integer Wavelet Transforms in Colored Image-Steganography", International Journal on Intelligent Cooperative Information Systems, Vol.4,pp.75-85.2004.
6. Neda Raftari and Amir Masoud Eftekharu Moghadam, "Digital Image Steganography based on IWT', 6th Asia Modelling Symposium, pp.87-92, 2012.
7. S. Mallat, W. L. Hwang. "Singularity detection and processing with wavelets." IEEE Trans. on Information Theory, 1992,38(2): 617-643
8. El Shazl Yemad, Abdel Wahab Safey, 2018. "Image steganography using least significant bit and integer wavelet transform" pp:265-273.
9. S.Thenmozhi, Dr.M.Chandrasekaran, 2012. "Novel Approach for Image Steganography Based on Integer Wavelet Transform"456-469.
10. T. Narasimmalou, Allen Joseph .R, Optimized Discrete Wavelet Transform based Steganography,2012
11. S. V. Narasimhan, N. Basumallick, and S. Veena, Introduction to Wavelet Transform: A Signal Processing Approach, 1 ed.: Alpha Science Intl Ltd, 2011.
12. S. Mallat, "A Wavelet Tour of Signal Processing (Wavelet Analysis & Its Applications),"2nd ed.: Academic Press, 1999.
13. E. Elbasi, A. M. Eskicioglu. "A DWT-Based Robust Semi-Blind Image Watermarking Algorithm Using Two Bands" IS&T/SPIE's 18th Annual Symposium on Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII Conference. San Jose, CA. January 2006.
14. Neda Raftari and Amir Masoud Eftekhari Moghadam, "Digital Image Steganography Based on Integer Wavelet Transform and Assignment Algorithm", Sixth Asia Modelling Symposium, 2012, pp 87-92.
15. Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee, and Poulami Das, "A Tutorial Review on Steganography" (IC3–2008 UFL & JIITU, p. no. 105-114).
16. S.Dewitte, J.Cornelis, "Lossless Integer Wavelet Transform", IEEE Signal Processing Letters, Vol.4, pp.158-160, 2002.

17. Prasad Nizampatnam, Kishore Kumar Tappeta, "Bandwidth extension of narrowband speech using integer wavelet transform", IET Signal Processing, Vol.11,pp.437-445, 2017
18. Dong Li, Chengxiang Zhang, Hongqing Liu, Jia Su, Xiaoheng Tang, Qinghua Liu, Guisheng Liao, " A Fast Cross-Range Scaling Algorithm for ISAR Images Based on the 2-D Discrete Wavelet Transform and Pseudopolar Fourier Transform", IEEE Transactions on Remote Sensing, Vol.57, pp. 4231-4245, Jan. 2019
19. Adam Nevriyanto, Sutarno Sutarno, Sri Desy Siswanti, Erwin Erwin, "Image Steganography using a combine of Discrete Wavelet Transform and Singular Value Decomposition for more Robustness and Higher Peak Signal Noise Ratio", International Conference on Electrical Engineering and Computer Science, Oct. 2018
20. Mohamad Anwar, Moechammad Sarosa, Erfan Rohadi, "Image Steganography using Lifting Wavelet Transform and Dynamic Key", International Conference of Artificial Intelligence and Information Technology, March. 2019

AUTHORS PROFILE

Ravi Ranjan, an undergraduate student in Electronics and Communication Engineering Department from VIT University, Vellore, Tamil Nadu, India

Subham Thirani, an undergraduate student in Electronics and Communication Engineering Department from VIT University, Vellore, Tamil Nadu, India

Dr. M. Jasmine Pemeena Priyadarsini obtained B.E. degree from Madras University in 1992 and M.E. degrees from Madurai Kamaraj University, Madurai in 1995. She earned his Ph.D. from Vellore Institute of Technology, Vellore, INDIA in 2014. She has published more than 45 research papers in National and International journals and reputed conferences. She has a teaching experience of about 25 years in Vellore Institute of Technology, Vellore in India. Presently, she is serving as Professor at Vellore Institute of Technology, India. She is a life member of Indian Society for Technical Education, IEEE society Membership, Fellow of Institution of Engineers, Fellow of Institution Electronics and Telecommunication Engineers. She has authored about four technical books. His research areas include Digital Image Processing, Digital signal processing, Optical Signal Processing, Light wave Communication Systems, Optical Coding Theory and Biometric Image Processing. She is a reviewer of several international conferences and journals.

Dr.G.K.Rajini working as Associate Professor,Vellore Institute of Technology,Vellore from July 2011 to till date and has 25 years of teaching expereince & 4 years of industrial expereince. Pursued Ph.D in S.V.University, Tirupati and M.Tech (Sensor Systems Technology), VIT University, Vellore, 2005. B.E (ECE). Thanthai Periyar Govt.Institute of Technology, Madras University, Vellore,1992. She has published various 50 papers in reputed journals and conferences.

Dr. A. Jabeena is an Associate Professor in School of Electronics Engineering, VIT University, Vellore. She has completed her B.E [Electronics and Communication Engineering in Bhrathiar University, Coimbatore, M.E., in Applied Electronics and received her PhD in Optical communication, Vellore Institute of Technology, Vellore. She has more than 25 years of teaching experience and her Research Interest includes application of Evolutionary algorithms to optimization problems in Wireless Optical Communication, Satellite communication, Optical Sensors and visible light communication. She is a member of Indian Society for Technical Education, IEEE, Institution of Engineers and Indian Science Congress Association. She has published more than 60 of her contributions in Scopus indexed journals and IEEE conferences. She is also reviewer of several international conferences and International journals