Color Image Steganography using Dual Wavelet Transforms

Mahdi Abbasi
Department of Computer Engineering, Engineering Faculty
Bu-Ali Sina University
Hamedan, Iran

ABSTRACT
Steganography is the art and science of covert communication. The secret information can be concealed in content such as image, audio, or video. This paper provides a novel image steganography technique which hides both image and key in color cover image using Discrete Wavelet Transform (DWT) and Integer Wavelet Transform (IWT). The cover image and secret image coefficient values are embedded by using a fusion technique. The cover image is a color image and the secret image is a grayscale image. This algorithm first separates RGB color planes of the cover image. Next, the algorithm extracts either DWT or IWT coefficients of both R-plane of the cover image and secret image. These two extracted coefficient values are fused into a single image by using a wavelet-based fusion technique. By taking IDWT/IIWT transform of the fused image the stego image is obtained. Different combinations of DWT/IWT transforms were performed on the scrambled secret image and cover image. Experimental results shows that the proposed method can produce stego images with high level of perceptual invisibility and security.

General Terms
Image Processing, Steganography, Wavelet

Keywords
Color image, steganography, Discrete Wavelet Transform, Integer Wavelet Transform.

1. INTRODUCTION
Steganography is the art of hiding information in such a way that, keeps the existence of the message secret [1, 2]. The wavelet domain is growing up very quickly. The wavelet transform is a very powerful tool and it is used in many diverse fields, including approximation theory; signal processing, physics, astronomy, and image processing [3-7]. There are many advantages of using Wavelet transform domain for steganography and it is proved by different practice tests. The use of such transform mainly increases the capacity and robustness of the Information Hiding system. Here the steganography is implemented in the Wavelet domain [1-8].

The major objective of steganography is to prevent some unintended observer from stealing or destroying the confidential information. Figure 1illustartes the triangle of information hiding. The capacity, robustness and the security are three related features of an information hiding system. There are some factors to be considered when designing a steganography system [2, 9-11]:

1. *Invisibility:* Invisibility is the ability to be unnoticed by the human eye.
2. *Security:* Even if an attacker realizes the existence of the information in the stego object it should be impossible for the attacker to detect the information. The closer the stego image to the cover image, the higher the security. It is measured in terms of PSNR. High PSNR value indicates high security.
3. *Capacity*: The amount of information that can be hidden relative to the size of the cover object without deteriorating the quality of the cover object.
4. *Robustness*: It is the ability of the stego to withstand manipulations such as filtering, cropping, rotation, compression etc.

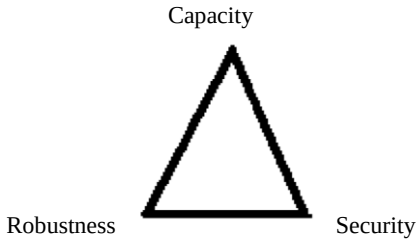


Figure 1: Information hiding system features

2. RELATED WORK
The steganography is done in both spatial domain and transform domain [1, 3, 8, 9, 11, 12]. The main difference is in the way that the secret message gets embedded in the cover image. In the spatial domain, the secret image is embedded in the coefficients of the transform of the cover image whereas in the transform domain, the secret message is embedded by changing the image pixels [9, 11, 12]. Each of these methods have special advantages and disadvantages. Methods in the transform domain would provide high security, but they cannot embed considerable information as compared to the spatial domain techniques. The main weakness of the spatial domain techniques is their problematic security[1]. For this reason, transform-based steganography methods have been interested much more than spatial domain techniques. Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT or Discrete Wavelet Transform (DWT) are used in transform domain steganography [4-6, 13].

In the last few years, numerous methods/algorithms have been developed for steganography using Wavelet Transform. Therefore, the review of related work has been conducted on the researches which have used discrete wavelet transformation and have combined it with integer wavelet transformation for hiding secret image information in digital color images. A comprehensive review of the literature of steganography may be found in [2, 11, 12].

Nilanjan Dey et al. [14] proposed a stenographic technique for hiding multiple images in a color image based on DWT and DCT. This Technique gives satisfactory PSNR value to establish the robustness of the work. Since only selected high-frequency components are modified for hiding method so

there must be some constraints on the secret image size.

K B Raja et al. [3] proposed a dual transform technique for robust steganography for secret and secure communication. This technique employed error detection and correction coding technique to increase robustness which has excellent PSNR with high levels of security.

Sushil Kumar et al.[15] proposed a multi-layered secure, robust and high capacity image steganography algorithm. This algorithm achieved three layers of security, better in terms of imperceptibility, robustness and embedding capacity.

M. Fahmy Tolba and Al-said Ghonemy [6, 7] proposed the high capacity image steganography using wavelet-based fusion. This method combines the DWT coefficients of both cover image and secret image. There, color images are used for steganography.

In the following, a new method is presented that uses the combinations of the Wavelet transform to achieve stego images with maximum level of quality.

3. PROPOSED METHOD

In this section, the steps of the proposed method are described comprehensively.

3.1 Preprocessing

Pre-processing methods use a small neighborhood of a pixel in an input image to get a new brightness value in the output image. All the pixels of an image in the spatial domain are multiplexed by embedding strength factors alpha. Image preprocessing deals with before the fusion can be performed. Most of the time images are misaligned registration is used to establish a spatial correspondence between sensor images and to determine spatial geometric transformation called wrapping which aligns the images[16].

3.2 Cover Image

It is defined as the original image into which the required secret message is embedded. It is also termed as the 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 grayscale image to color image in the uncompressed format.

3.3 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[16].

3.4 Discrete Wavelet Transform

In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled[6, 7]. As with other wavelet transforms, a key advantage it has over Fourier transforms is the temporal resolution: it captures both frequency and location information. Wavelets are special functions which used as Bessel functions for representing signals. DWT is applied to the entire image or to its subparts. The embedding process is done by modifying some coefficients that are selected according to the type of protection needed. If one wants the message to be imperceptible, he/she should choose a high range of frequency. If one wants the message to be robust, he/she should choose a low range of frequency. DWT provides an appropriate basis for separating the noise from an image. As the wavelet transform is good at energy compaction, the small coefficients more likely represent noise, and large coefficients represent important image features [17-19].

DWT is used for digital images. Many DWTs are available. Depending on the application appropriate one should be used[20]. The simplest one is Haar transform. To hide text message integer wavelet transform can be used. When DWT is applied to an image it is decomposed into four subbands: LL, HL, LH, and HH. The LL part contains the most significant features. Hence, if the information is hidden in LL part the stego image can withstand compression or other manipulations. But sometimes distortion may be produced in the stego image and then other subbands can be used. The decomposition of the Lena image by two levels of 2D-DWT is shown in Figure 2.

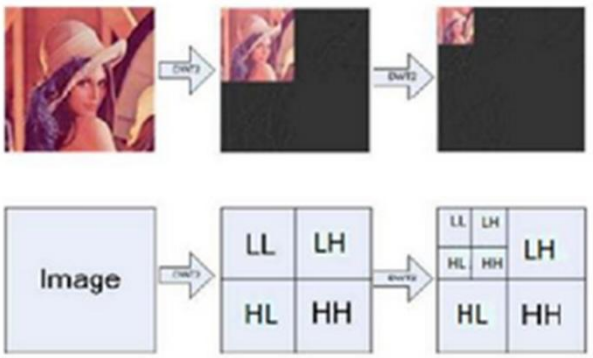


Fig 2: Two-level two-dimensional DWT

3.5 Integer Wavelet Transform

Integer Wavelet Transform is a nonlinear transform having a structure of lifting scheme and as its rate-distortion performance similar to DWT Wavelet transforms that map integers to integers allows perfect reconstruction of the original image. 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 the data is hided 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 into the failure of the data hiding system. The lifting scheme (LS) allows a low complexity and efficient implementation of the DWT. This allows new transforms to be used. One is the LS- based integer wavelet transform (IWT) scheme. Although IWT is very interesting because of the previously cited advantages, its main drawback is that the most image coefficients after IWT has smaller dynamic change and worse energy compaction than DWT, which would degrade the performances of the Lossy coding[6, 21-23].

3.6 Image Fusion

The objective of image fusion is to combine information from multiple images of the same scene. Image fusion needs image registration [7, 24]. The goal of image registration is to find a transformation that aligns one image to another. Fusion can be performed on pixel, feature or decision level[24]. Fusion methods such as arithmetic and logical operation can be performed in steganography. Image fusion provides an effective way of reducing the increasing volume of information while at the same time extracting all the useful information from the source images. Image fusion becomes essential sub-topic in the digital image processing area. Image fusion is nothing but a process of combining two or more different images into a new single image retaining important

features from each image.

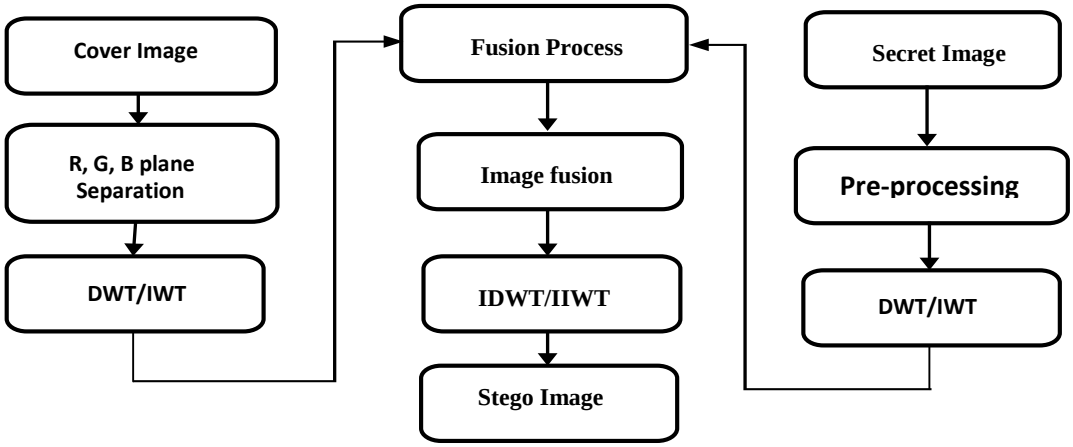


Fig 3: Embedding process

Here, wavelet-based fusion is used. It is used to hide the secret image into the cover image. It involves merging of the wavelet coefficients of both the cover image and the secret image into a single image called a fused image. In a normalized image, the pixel components take on values that span a range between 0.0 and 1.0 instead of the integer range of [0,255]. Hence, the corresponding wavelet coefficients will also range between 0.0 and 1.0.

The wavelet-based fusion actually merges the wavelet coefficients of both the cover image and the secret image into a single fused result using the following equation:

$$f'(x,y) = f(x,y) + \alpha\, g(x_m, y_m) \quad (1)$$

Where, f' is the modified DWT coefficient, f is the original DWT coefficient, g is the message coefficient, and α is the embedding strength (ranging from 0.0 to 1.0).

4. PROPOSED METHOD

4.1 Embedding Process

During the proposed embedding process, IWT/DWT is performed on both the cover image and the secret image. By using the fusion process the fused image is gotten. The IIWT/IDWT is applied according to the following algorithm on the fused image to get a stego image. The steps are illustrated in figure 3. The steps would be summarize as:

1) Get Color Cover Image as C (Cover).
2) Separate Cover Image into R, G, and B Channel (CR, CG, and CB Channels) and take CR Channel.
3) Get Grayscale Secret Image as SG.
4) Apply combinational transforms on CR plane (of Color Cover image) and SG (Gray scale Secret Image).
5) By applying IWT/DWT, extract the approximation coefficients of matrix LL1 and detail Coefficients matrices LH1, HL1, HH1 of R Channel Cover Image as CR1.
6) By applying DWT/IWT extract the approximation coefficients of matrix LL1 and detail coefficient matrices LH1, HL1, HH1 of the Secret Image as SG1.
7) Perform fusion operation on image CR1 and SG1 get fused image.
8) Finally apply IIWT/IDWT on fused image to form the stego image as ST.

4.2 Extracting Process

During the proposed extracting process, the recovered stego image and known cover image are reconstructed with IWT/DWT transform domain and followed by the fusion process. Next, IDWT/IIWT is performed to rebuild the secret image. Finally, the secret image is obtained, which is similar to the original secret image. The steps are illustrated in figure 4. The steps would be summarize as:

1. Extracts the DWT/IWT coefficient values of stego image and cover image.
2. Apply inverse fusion process to get fused image.
3. Take IDWT/IIWT of the fused image to reconstruct the secret image.

5. IMPLEMENTATION AND EVALUATION

MATLAB is a high performance tool for technically computation that integrates computation, visualization and programming in an easy to use environment. MATLAB 2014 is a numerical computing environment and fourth-generation programming language. A set of color and gray-scale images of size 256*256 were used for experimental test. For example, the well-known test images of Lena and Cameraman were used. Lena image is vector color image which is used as the cover image and Cameraman image is a gray-scale image which is used as secret image.

By using transform combination technique for steganography, the stego images were generated. In all experiments there were four combinations of two transforms including: DWT-DWT, DWT-IWT, IWT-DWT, and IWT-IWT. Out of those combinations, the results of each of combinations are shown in figure 5 and figure 6. In both figures results up to Embedding process are shown.

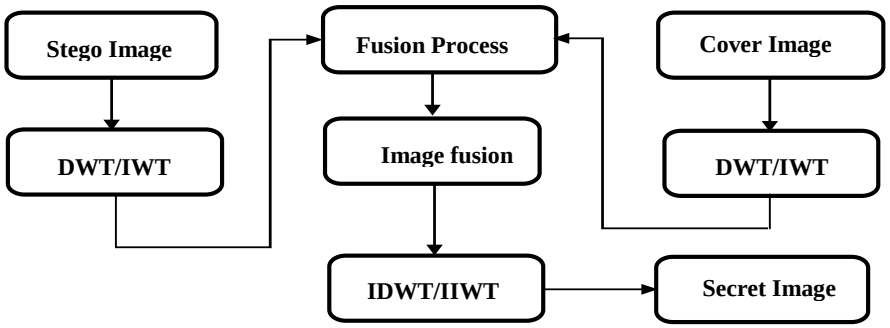


Fig 4: Extraction process

Fig 5: Results of IWT-DWT, (a) Cover Image, (b)Secret image, (c)IWT of Secret Image, (d)DWT of Cover Image, (e) Stego Image, (f) Extracted Image

5.1 Performance Parameter Evaluation

To retain the image quality and provide a stronger robustness and security of an image steganography scheme, the statistical parameters are further considered. The value of statistical parameters not only reduces the image perceptibility but also enhances the robustness to resist attacks. The PSNR and MSE are used to measure the distortion between the original cover image and the stego image.

5.1.1 Mean Square Error (MSE)

The distortion in the image can be measured using MSE and can be defined as the measure of average of the squares of the difference between the intensities of the stego image and the cover image. It is popularly used because of the mathematical tractability it offers. It is represented as follows:

$$MSE = \frac{1}{MN}\sum_{j=1}^{M}\sum_{1}^{N}(X_{j,k} - X'_{j,k})^2 \qquad (2)$$

In equation (2), $X_{j,k}$ and $X'_{j,k}$ denote the intensities of the corresponding pixels of the stego image and the cover image, respectively

5.1.2 Peak Signal to Noise Ratio (PSNR)

It is the measure of the quality of the image by comparing the cover image with the stego image. It measures the statistical difference between the cover and stego image. The PSNR depicts the measure of reconstruction of the transformed image. This metric is used for discriminating between the cover and stego image and is formulated as below.

$$PSNR = 10\frac{\log_{10} 255^2}{MSE} \qquad (3)$$

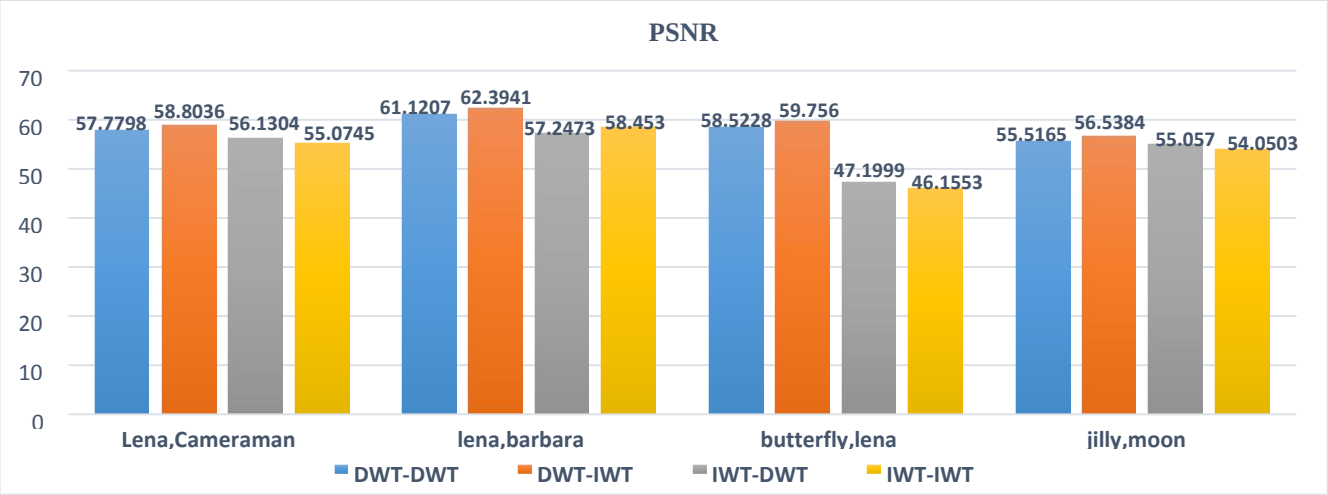
Table 1 shows performance evaluation of all four combination of wavelet transforms with images of different file formats and sizes. All combinations gives better results. But by comparing all PSNRs corresponding to all combinations as illustrated in figure 7, the DWT-IWT gives the best result considering the value of PSNR. This means the DWT-IWT combination provides the best-quality stego image.

Fig6: Steganography using DWT-IWT combination of wavelet transforms

Fig 7: PSNR of the result of steganography using four different sets of cover and secret images

Table 1: Performance evaluation with images of size 256*256 of different file formats

Image	size	DWT-DWT		DWT-IWT		IWT-DWT		IWT-IWT	
		PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
Lena.png (cover)	256×256	57.7798	1.2953	***58.8036***	***1.7801***	56.1304	1.1739	55.0745	1.8491
Cameraman.png (secret)	256×256								
Lena.jpg (cover)	256×256	61.1207	1.0703	***62.3941***	***0.2812***	57.2473	0.0318	58.4530	1.3743
Barbara.bmp (secret)	256×256								
Baboon.jpg (cover)	256×256	58.3724	1.9899	***59.5343***	***1.7801***	52.2149	1.0248	51.6017	1.8491
Cameraman.png (secret)	256×256								
Butterfly.png (cover)	256×256	58.5228	0.1490	***59.756***	***0.1151***	47.1999	1.0642	46.1553	1.2047
Lena.gif(secret)	256×256								
Jilly.tif (cover)	256×256	55.5165	0.1799	***56.5384***	***1.6951***	55.0570	1.1038	54.0503	1.7155
Moon.tif (secret)	256×256								
Baboon.jpg (cover)	256×256	56.7858	0.1139	***57.8117***	***0.1026***	51.2132	0.1540	51.3120	1.1281
House.png(secret)	256×256								
Butterfly.png (cover)	256×256	59.1044	1.1870	***60.2262***	***0.6951***	47.9771	0.9963	46.9297	1.7155
Moon.tif (secret)	256×256								
Jilly.tif (cover)	256×256	55.6363	1.2184	***59.6984***	***1.1026***	53.6981	1.2405	52.4890	1.1281
House.png(secret)	256×256								



6. CONCLUSION

In this paper, secret image is hide into two different domains of IWT (Integer Wavelet Transform) and DWT (Discrete Wavelet Transform). The cover image and secret image coefficient values are embedded in images of size 256*256 using a fusion technique.

This paper presents embedding steps of the proposed dual wavelet transform based color image steganography. The RGB color image is used as cover image and the secret image is a grayscale image. DWT/IWT coefficients are extracted of cover image (R-plan) and secret image. Then, these extracted coefficient values are embedded by a fusion technique. Then, stego image is obtained by taking inverse transform of fused image. All combination of DWT and IDW were experimented on images with different sizes and file formats. The PSNR and MSE were used to measure the distortion between the original cover image and the stego image. All combinations produce acceptable results. But comparing all combinations shows the DWT-IWT combination gives the best result with highest PSNR.

The proposed algorithm can be tested with more combinations of transform domain. Also, enhancing the visual effect of the stego image and the increasing the robustness of the proposed methods against the various attacks would extend the strength of the method.

7. REFERENCES

[1] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. S. Ho, and K.-H. Jung, "Image steganography in spatial domain: A survey," Signal Processing: Image Communication, vol. 65, pp. 46-66, 2018/07/01/ 2018.

[2] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," Neurocomputing, vol. 335, pp. 299-326, 2019/03/28/ 2019.

[3] H. M. Reddy and K. Raja, "Wavelet based non LSB steganography," International Journal of Advanced networking and applications, vol. 3, p. 1203, 2011.

[4] M. I. S. Reddy and A. P. S. Kumar, "Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm," Procedia Computer Science, vol. 85, pp. 62-69, 2016/01/01/ 2016.

[5] M. S. Subhedar and V. H. Mankar, "Image steganography using redundant discrete wavelet transform and QR factorization," Computers & Electrical Engineering, vol. 54, pp. 406-422, 2016/08/01/ 2016.

[6] M. Tolba, M. Ghonemy, I. Taha, and A. Khalifa, "Using integer wavelet transforms in colored image steganography," International Journal on Intelligent Cooperative Information Systems, vol. 4, pp. 230-235, 2004.

[7] [M. F. Tolba, M.-S. Ghonemy, I.-H. Taha, and A. S. Khalifa, "High capacity image steganography using wavelet-based fusion," in Proceedings. ISCC 2004. Ninth International Symposium on Computers And Communications (IEEE Cat. No. 04TH8769), 2004, pp. 430-435.

[8] T. Liu and Z.-d. Qiu, "A DWT-based color image steganography scheme," in 6th International Conference on Signal Processing, 2002., 2002, pp. 1568-1571.

[9] S. A. El_Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information," Computers & Electrical Engineering, vol. 70, pp. 380-399, 2018/08/01/ 2018.

[10] S. K. Sabnis and R. N. Awale, "Statistical Steganalysis of High Capacity Image Steganography with Cryptography," Procedia Computer Science, vol. 79, pp. 321-327, 2016/01/01/ 2016.

[11] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," Computer Science Review, vol. 13-14, pp. 95-113, 2014/11/01/ 2014.

[12] Y. Liu, S. Liu, Y. Wang, H. Zhao, and S. Liu, "Video steganography: A review," Neurocomputing, vol. 335, pp. 238-250, 2019/03/28/ 2019.

[13] U. D. Acharya and P. R. Kamath, "A secure color image steganography in transform domain," arXiv preprint arXiv:1304.3313, 2013.

[14] T. Bhattacharya, N. Dey, and S. Chaudhuri, "A session based multiple image hiding technique using DWT and DCT," arXiv preprint arXiv:1208.0950, 2012.

[15] S. Muttoo and S. Kumar, "A multilayered secure, robust and high capacity image steganographic algorithm," World of Computer Science and Information Technology Journal, vol. 6, pp. 239-246, 2011.

[16] A. Yahya, "Steganography Techniques," in Steganography Techniques for Digital Images, ed: Springer, 2019, pp. 9-42.

[17] S. Mallat, A wavelet tour of signal processing: Elsevier, 1999.

[18] S. G. Mallat, "A theory for multiresolution signal decomposition: the wavelet representation," IEEE Transactions on Pattern Analysis & Machine Intelligence, pp. 674-693, 1989.

[19] C. Torrence and G. P. Compo, "A practical guide to wavelet analysis," Bulletin of the American Meteorological society, vol. 79, pp. 61-78, 1998.

[20] N. Solanki, S. Khandelwal, S. Gaur, and D. Gautam, "A Comparative Analysis of Wavelet Families for Invisible Image Embedding," in Emerging Trends in Expert Applications and Security, ed: Springer, 2019, pp. 219-227.

[21] A. Calderbank, I. Daubechies, W. Sweldens, and B.-L. Yeo, "Wavelet transforms that map integers to integers," Applied and computational harmonic analysis, vol. 5, pp. 332-369, 1998.

[22] A. R. Calderbank, I. Daubechies, W. Sweldens, and B.-L. Yeo, "Lossless image compression using integer to integer wavelet transforms," in Proceedings of International Conference on Image Processing, 1997, pp. 596-599.

[23] 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, pp. 321-330, 2007.

[24] J. Ma, Y. Ma, and C. Li, "Infrared and visible image fusion methods and applications: A survey," Information Fusion, vol. 45, pp. 153-178, 2019