Comparative Analysis of 2-Level and 4-Level DWT for Watermarking and Tampering Detection

(Tulasi M R, Vardhini R Narasimhan, Shilpa R, Neha Anjum) [1],
(Ms. Manjushree K Chavan, Assistant Professor) [2]
[1, 2]*(Department of Electronics and Communication, Dr. T. Thimmaiah Institute of Technology, Kolar Gold Fields-563 120, India)*

ABSTRACT : With the advancement in the technology, there has been increase in the volume of information. This has led to the copying and illegal data hacking. Watermarking has become a serious issue in the network security. Attackers are using the different tools for the data extraction. Duplicating of images is also a major issue in the present world. Hence, to overcome from this problem, the DWT and the SPIHT algorithm is used for the watermarking and hash vectors are generated to detect the tampers. There are different techniques for the watermarking process; among these DWT seems to be the most efficient method. The 2- Level and 4-Level DWT operation is performed on the image, where 4-Level and 2-Level MSE and PSNR values are compared. From the comparison, it will be theoretically proved that 4-level is more accurate and secure than 2-Level.

KEYWORDS –2-Level DWT, 4-Level DWT, SPIHT Algorithm, Tampering Detection, Watermarking.

1. INTRODUCTION

Watermarking is a process of hiding the information. Watermarking can be done in two domains. One is spatial domain and the other is transform domain. Spatial domain transformation is the easy way to insert the watermark and is less complex. And it is not robust against the attacks. Transform domain transformation is bit complex compared to the spatial domain; they are robust and uses simple image processing operations. In transform domain, DWT is preferred because the transformation is done in the wavelet domain and the image security increases. For the watermarking process, we consider two images they are host image and watermark image. The host image coves the watermark image and hence the embedded information is not visible. Even if the data is extracted by different means like fax, mail, messages and the image format is changed by cropping, resizing the data hidden is not lost. Digital watermarking helps in protection of illegal authorization, duplication and alterations. Tampering detection is the process of detecting the changes with respect to the original image. The change that has occurred are said to be the tampers. For the detection of tamper, we consider to images. One is host image and the other is the tampered image. The host image is the watermark image and tampered image is the watermarked image. The hash vectors are generated and 64 features are extracted from the image.

2. METHODOLOGY FOR WATERMARKING

For the watermarking the two images are considered. The watermark image is embedded by host image. The flow of digital watermarking is as shown in the Fig. 2.1. In this stage, the RGB components i.e. Red, Green, and Blue components are separated and DWT operation is applied separately for both the host image and watermark image. The SPIHT encoding and decoding operation is applied only to the watermark image. The resultant components of the host image are added with the watermarked image by multiplying scaling factor to the watermark image. And finally the inverse DWT operation is performed to the newly obtained watermarked image. The filtering operation is performed to remove the noise added during the transformation. The filter used here is median filter; it is a non-linear and is very effective at removing noise. There are different parameters to theoretically prove the image efficiency and robustness. Among these MSE and PSNR values of the watermarked image is calculated. The MSE is the average of the squares of the difference between the deviations from the original. PSNR is the ratio of the maximum power of the signal to the power of the corrupting noise. The DWT operation and the SPIHT algorithm will be further explained in detail. The watermarking process is done using two-level DWT and four-level DWT separately [1].

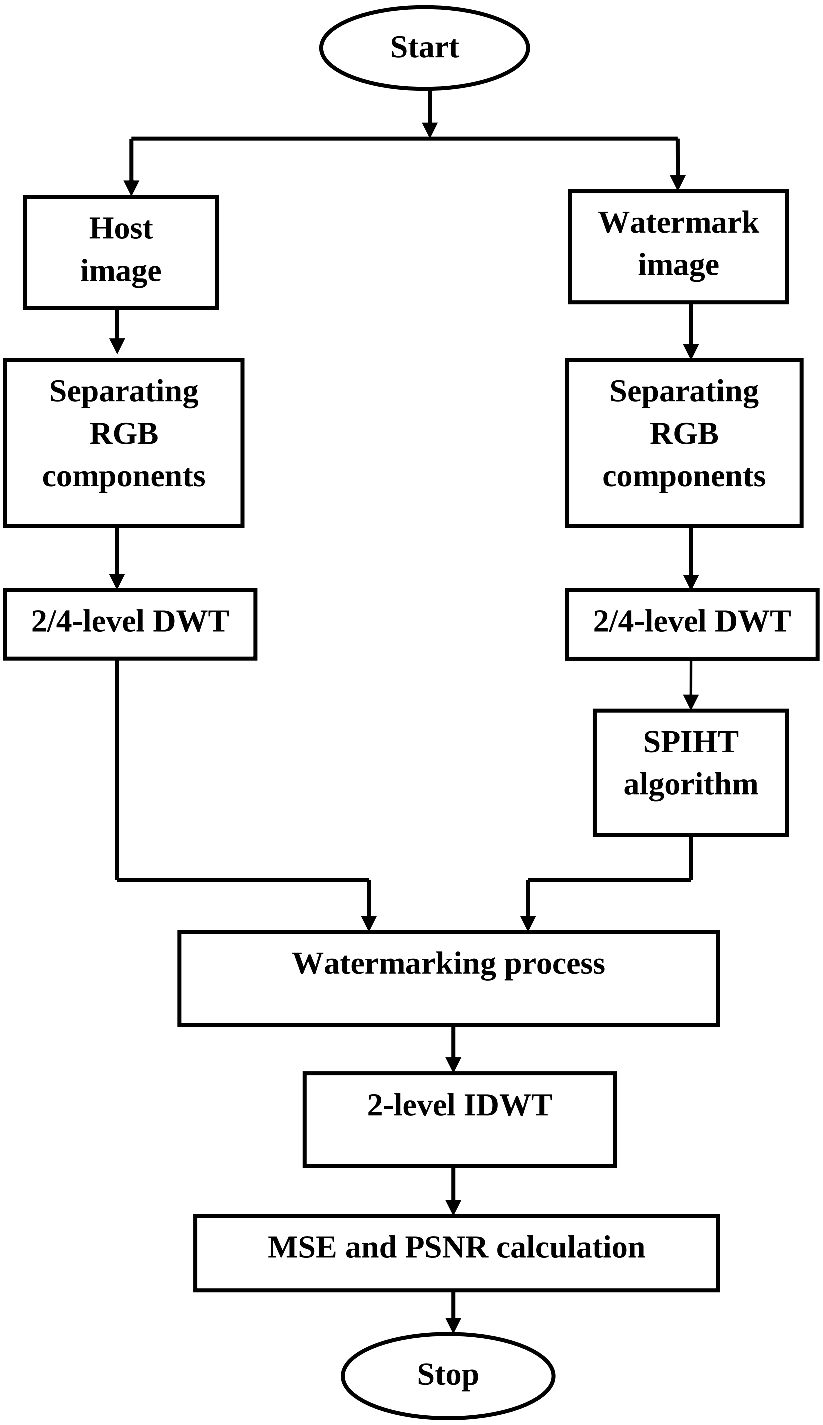

Fig. 2.1: Flow of Watermarking

2.1 Discrete Wavelet Transform

Discrete Wavelet Transform (DWT) is a mathematical tool for decomposing an image. The transformation is based on small waves called wavelets. The wavelets are of varying frequency. Wavelet domain is a secure domain for watermarking. The DWT decomposes the original image into mainly three spatial directions i.e. horizontal, diagonal and vertical in result separating the image into four components that is Low-Low, Low-High, High-Low and High-High. For our transformation only the low frequency components are considered since it contains the maximum information. For second level decomposition the Low-Low component is further decomposed into four-levels is as shown in the Fig. 2.2. For the third level decomposition LL2 sub-band is decomposed into four-levels. For four-level DWT transformation, LL3 sub-band is further decomposed into four levels as shown in Fig. 2.3. At every level of decomposition, the magnitude of DWT is larger in lower bands and smaller in the other three bands. Human visual system (HVS) is extra sensitive to the low frequency parts, so the watermark is embedded in the Low-Low sub-band. The advantage of this method is that the features of an image that are not detected at one resolution may be easily detected at another [2].

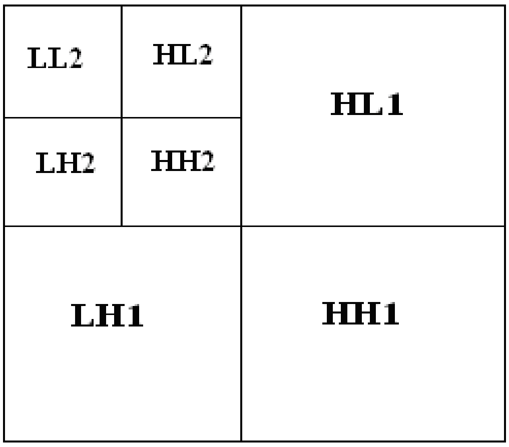

Fig. 2.2: Two-Level DWT

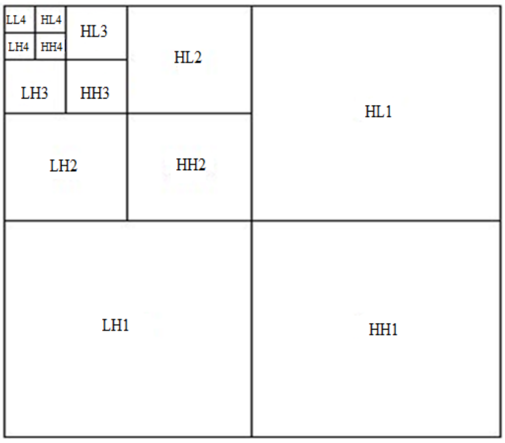

Fig. 2.3: Four-Level DWT

2.2 SPIHT Algorithm

SPIHT (Set Partitioning in Hierarchical Trees) is an efficient method for encoding and decoding the image using wavelet transformation. SPIHT is an embedded compression algorithm with adaptive output rates. SPIHT algorithm is efficient, completely embedded. It is simple and fast. This algorithm can truncate output bit stream at any desired rate. The SPIHT algorithm sorts the rounded multi-resolution wavelet transform coefficients according to their magnitudes and transmits them based on significant bit order. The operation is performed in two stages, one is sorting pass and other is refinement pass [3].

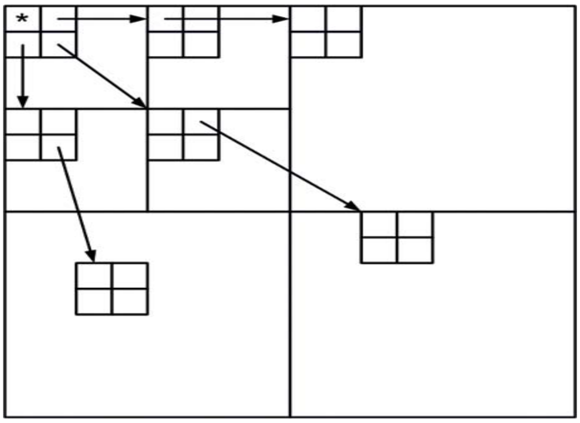

Fig. 2.4: Wavelet Transforms Spatial Orientation Trees

The SPIHT exploits the similarities across different sub-bands wavelet transform. These similarities can be found through wavelet transform spatial orientation trees as shown in Fig. 2.4. SPIHT encoding supports the images of larger dimensions, it results in lossless compression. SPIHT algorithm provides inherent characteristics. It has very precise rate control [4].

2.3 Extraction of Watermark

The extraction process is performed on watermarked image in order to get back the embedded watermark. The flow of extraction is shown in Fig. 2.5. For the extraction process two input images are considered. The first input is host image and the second is watermarked image. The RGB components are separated for both the images and then DWT transformation is applied. The extraction process is done by subtracting host image from the watermarked image and dividing by a scaling factor. The inverse DWT is applied for the extracted watermark. The two-level and four-level DWT operation is done separately. The watermark extracted from the four-level contains more information and is more efficient than compared to the two-level.

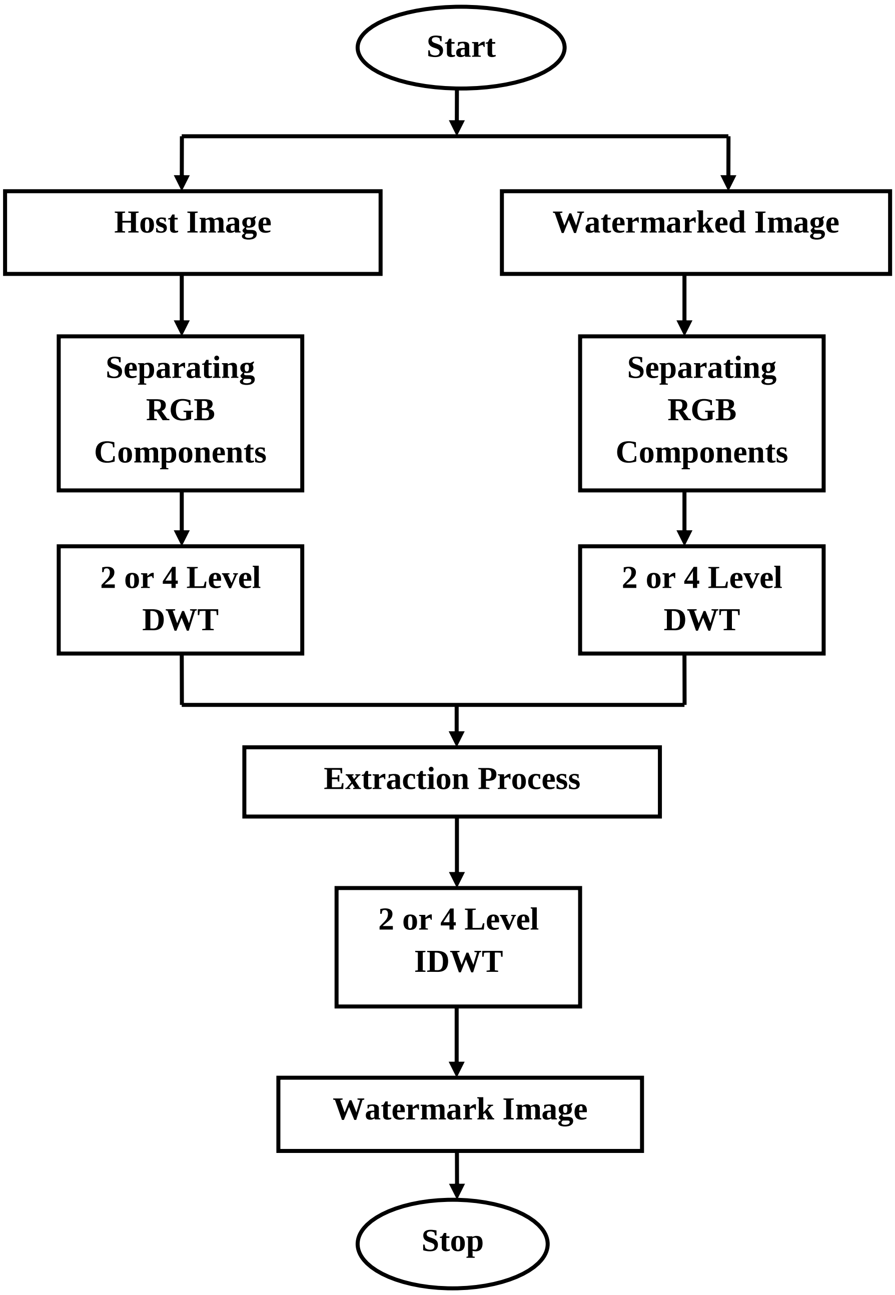

Fig. 2.5: Flow of Watermark Extraction

3. METHODOLOGY FOR TAMPERING DETECTION

Thetampering detection is a process that easily detects the unauthorized access. The image feature based hash generation is a popular technique for tampering detection. The flow of tampering is as shown in the Fig. 3.1. For the tampering detection two images are considered one is watermark image and other is watermarked image. The image features are extracted for both the images. The feature points can be of any number; here 64 features are extracted for the detection of tampers. The hash vectors are generated separately. The comparison is done by matching the features through distance function. If the feature points of the watermark image matches with the watermarked image, we conclude that tampering has not occurred. If the feature points of the watermark image do not match with the watermarked image, we conclude that tampering has occurred. The tampering detection is accomplished by finding the difference between the hash matrices corresponding to tampered image and original image [5].

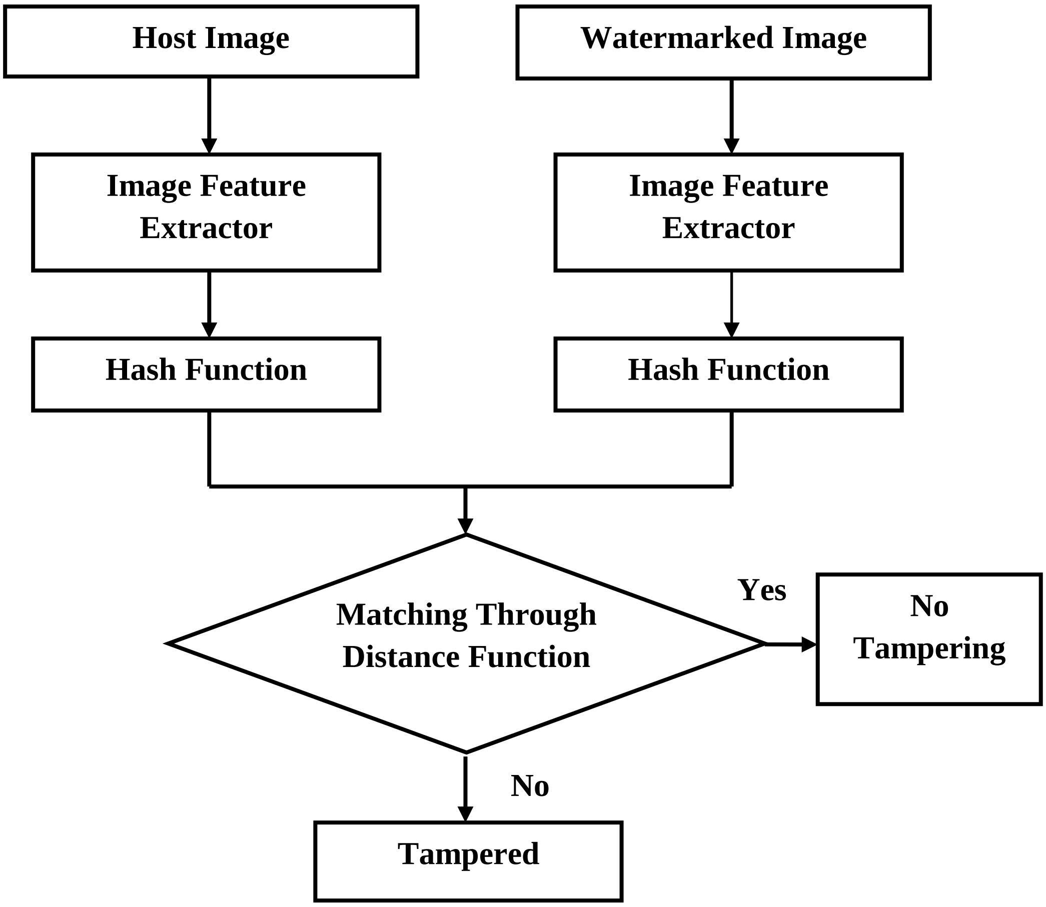

Fig. 3.1: Flow of Tampering Detection

4. RESULTS AND COMPARISION

The results and resultant images after performing the watermarking process and extraction process are given below. The watermarking process and extraction process are performed separately for two-level and four-level DWT.

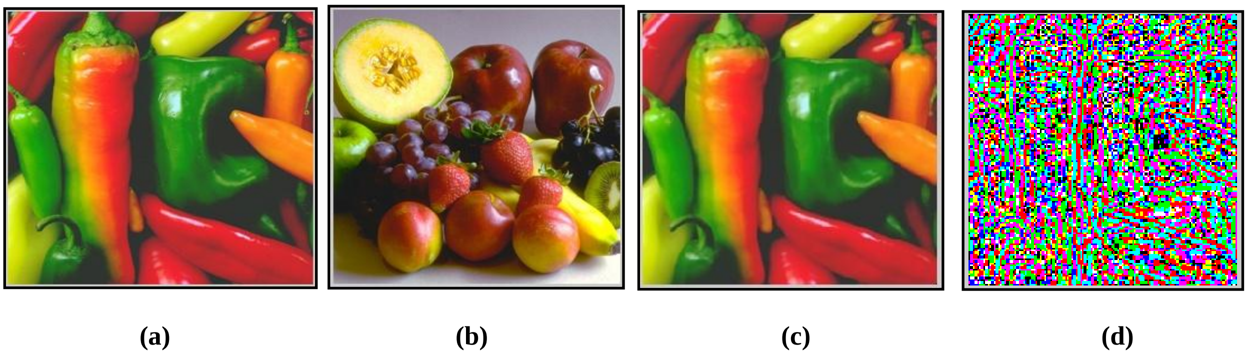

Fig. 4.1: (a) Host image, (b) Watermark image, (c) Watermarked image, (d) Extracted image using two-level DWT

The two images are considered, one is host image as shown in Fig. 4.1 (a) and the other is watermark image as shown in Fig. 4.1 (b). The image after performing watermarking process is shown in Fig. 4.1 (c). The image after performing extraction process is shown in Fig. 4.1 (d). The same process is repeated for four-level DWT as given below.

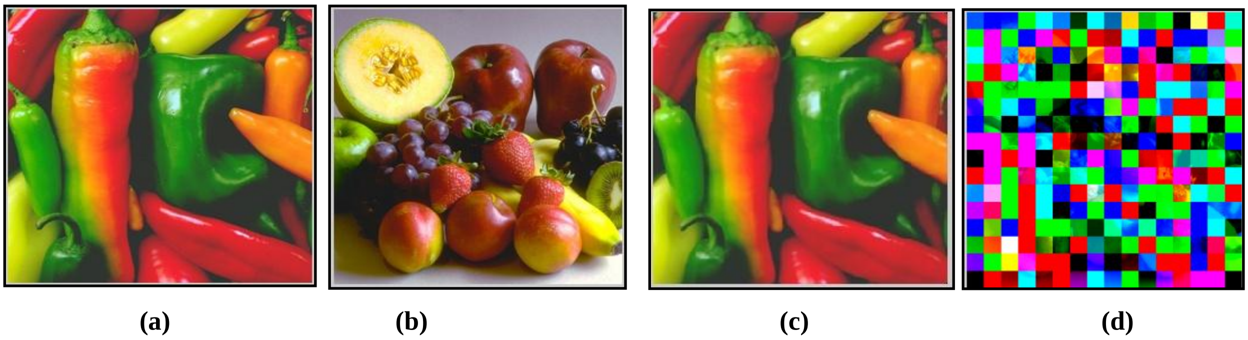

Fig. 4.2: (a) Host image, (b) Watermark image, (c) Watermarked image, (d) Extracted image using four-level DWT

The two images are considered, one is host image as shown in Fig. 4.2 (a) and the other is watermark image as shown in Fig. 4.2 (b). The image after performing watermarking process is shown in Fig. 4.2 (c). The image after performing extraction process is shown in Fig. 4.2 (d).

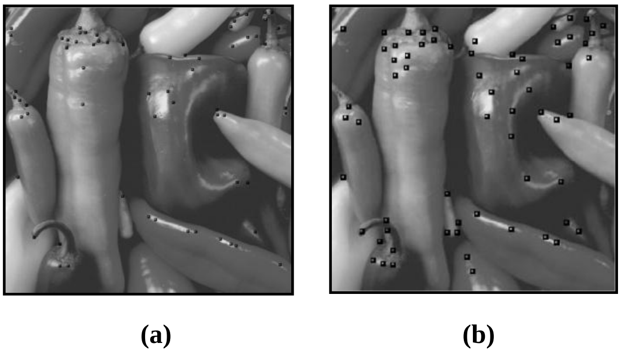

Fig. 4.3: (a) Watermark image, (b) Watermarked image

The resultant image of tampering detection is as shown in Fig. 4.3. From the Fig. 4.3 we can see that the watermark image is having different pixel values form that of the watermarked image. The difference is represented by extracting 64 feature points as shown in the Fig. 4.3.

Table 4.1: PSNR and MSE values of 2-level and 4-level DWT for RGB Components

Color Components / Parameters	2-level DWT			4-level DWT		
	R	G	B	R	G	B
MSE	20.3437	31.5606	33.7854	1.5704	1.0006	0.3707
PSNR	35.0465	33.1394	32.8435	46.1708	48.1284	52.4402

The MSE and PSNR values are calculated for the separate RGB components of two-level and four-level. From this we can tell that the four-level DWT is more efficient than two-level DWT. Has the MSE value decreases, the PSNR value increases. The error occurred in four-level is less compared to two-level DWT.

5. CONCLUSIONAND FUTURE WORK

The watermarking technique using two-level and four-level DWT is an efficient method. The security level and robustness of the image is increased. Using the wavelet domain transformation, the data hiding capacity decreased. To change the data format and to extract the data is very difficult even by using the different photo editing tools. It can be concluded that watermarking and tampering detection is very important for image authenticity and protecting the data against attacks. This kind of watermarking and tampering detection is performed only on the stationary images. This can be further extended to audios and videos. In future it can be enhanced to 8-level DWT, where the robustness of the image increases.

REFERENCES

[1] MadhuriRajawat and D S Tomar proposed “A Secure Watermarking and Tampering detection technique on RGB Image using 2 Level DWT”, in 2015 at Fifth International Conference on Communication Systems and Network Technologies.

[2] Swamy T N et al “A New Technique to Digital Image Watermarking Using DWT for Real Time Applications”, Int. Journal of Engineering Research and Applications ISSN: 2248-9622, Vol. 4, Issue 8, August 2014, pp. 102-107.

[3] Saeed Sarreshtedari and Mohammad Ali Akhaee developed “A Source-Channel Coding Approach to Digital Image Protection and Self-Recovery”, IEEE Transactions On Image Processing, Vol. 24, No. 7, July 2015.

[4] Said and W. A. Pearlman, “A new, fast, and efficient image codec based on set partitioning in hierarchical trees,” IEEE Trans. Circuits Syst. Video Technol., vol. 6, no. 3, pp. 243–250, Jun. 1996.

[5] Minati Mishra and Dr. M. C. Adhikary proposed “Digital Image Tamper Detection Techniques - A Comprehensive Study”, in 2013.