Journal of Physics: Conference Series

PAPER • **OPEN ACCESS**

Digital Image Recovery Based on Lifting Wavelet Transform

To cite this article: Taha Basheer Taha *et al* 2021 *J. Phys.: Conf. Ser.* **1962** 012021

View the article online for updates and enhancements.

This content was downloaded from IP address 185.206.172.59 on 05/09/2021 at 07:29

Digital Image Recovery Based on Lifting Wavelet Transform

Taha Basheer Taha[1], Dujan B. Taha[2], Ruzelita Ngadiran[3], Phaklen Ehkhan[4]

[1]IT Department, Faculty of Sciences, TISHK International University, Erbil, Iraq.
[2]Software Engineering Department, College of Computer Science and Mathematics, Mosul University, Iraq
[1,3,4] Centre of Excellence Advanced Computing (AdvComp), Faculty of Electronic Engineering Technology, University Malaysia Perlis, Perlis, Malaysia
Taha.Basheer@tiu.edu.iq, PhD.Taha@gmail.com

Abstract. Recently, with the wide distribution of digital media, the need for authenticating digital images was increased. Therefore, many image tamper detection and recovery algorithms were introduced in literature to detect malicious modifications and retrieve the original images. The process of detection and recovery, however, used to have complex operation which requires long processing time. In this paper, a simplified image recovery algorithm is presented by using lifting wavelet transform. In the proposed method, the approximation band is hidden inside the bits of the original image and to be retrieved without relying on source image. For images with hidden data, the average PSNR and SSIM values were 31.22 and 0.977 respectively, and images were successfully retrieved after block attack.

Index Terms—Tamper Detection, Image recovery, Lifting Wavelet Transform**.**

1. Introduction

Changing the contents of digital images became easy and fast after the wide distribution of digital images editing tools in personal computers or mobile applications. Many tampered images emerge in news items, scientific experiments and even legal evidences as criminal investigation and road accident imaging. Therefore, the authenticity of images should not be taken for granted [1]. Accordingly, one of the primary goals of digital image forensics is the authentication of the images and recover regions which have undergone some form of manipulation or alteration.

Many algorithms were specialized in verification of the credibility of digital images, and distinguishing the original images from faked images and establishing the authenticity of digital photographs have become some of the greatest challenges of the present time [2].

One of authentication methods is the use of fragile watermarks, where a fragile watermark, having important features of an image, is embedded into a cover image, and by comparing the fragile watermark and image features, so the image integrity can be authenticated [3]. Although the fragile watermarking methods is considered a feasible method for solving the problem of image authentication, but using external watermark will increase the payload of the algorithm by adding another image.

One important aspect in image recovery is the process of detection and retrieval is preferred to be done without the existing of the original image, i.e., the algorithm should have the ability of self-recovery. Another aspect that is preferred is the simplicity of the algorithm, which can make it easy to be executed in devices with limited processor speed or in real time applications.

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

According to mentioned criteria, in this paper, a low complexity, blind and simplified image recovery is proposed based on fast and integer lifting wavelet transformation by spreading the approximation band of the transform to entire image pixels and recover them to show the original image and recover the tampered pixels. It is also avoid using external watermark in detecting and recovering the tamper in images, as the authentication data will be generated from the image itself.

The paper is organized as follows; the next section is a literature review of previous studies on image tampering. Lifting wavelet transform was explained in section three followed by the proposed methodology in section four. Results were shown in section five and the paper was concluded in section six.

2. Literature Review

Different image recovery algorithm were presented in literature using time or frequency domain. In 2019, Rajput & Ansari proposed an algorithm in which the original image is reduced in size, copied four times and hidden in the original image's 4-LSB using four pseudo-random codes. Later on, these copies are used for tamper detection [4]. In [5], an image tamper localization scheme was proposed by Sreenivas & Kamakshiprasad in which chaotic maps are used to generate a 2×2 image block. The scheme is improved by including a self-recovery method to recover the tampered regions [5]. Hsu et.al proposed an algorithm that is used as a certain, not necessary, portion of the image to hide important information to improve the recovery process [6].

Han et al. [7] proposed a spatial domain method in which the host image is divided into blocks, and the characteristics of each block is hidden in the same block. The hidden characteristics are extracted and compared with that block to detect the existence of tampering. Chang et al. [8] proposed a fragile watermarking scheme in which the authentication data of an image, as the eight-pixel values surrounding the center of the block, the block number, the user secret key, and user ID is inserted into adaptive least significant bits of the embedded pixels. And the least significant bit selection was determined by the corresponding block type. When authenticating image integrity, the first authenticated information is retrieved from the least significant bits of each center block. Then, a new authenticated message of the test image is generated in the same manner.

Qi et.al used discrete wavelet transform (DWT) to embed the image features in the approximation sub band to high frequency bands, however, the recovery process was not clarified [9]. Sarika et.al employed both wavelet and singular value decomposition (SVD) to detect image tampering. In wavelet, both transmitted and extracted are compared to check whether the image is altered or not, while the SVD is used to recover the original image's content [10]. SVD was used in [11], by generating two distinct tamper detection keys based on SVD of the image blocks. Each generated tamper detection and self-recovery key is distinct for each image block and is encrypted using a secret key.

Some literature studies consider watermarks existing as an important factor to investigate authentication and integrity [12], as a consequence, it is involved in many tamper detection attempts in literature where different algorithms are proposed for detecting image forgery and self-recovery. Many surveys are presented to summarize such attempts as [13] and [14].

As shown in literature, many of transform domain studies are relied on DWT, SVD or other floating-point transforms. Floating number calculations are considered time consuming complex operations especially when the design required real time response or to be achieved by limited processor embedded systems. In addition, using of watermarks requires extra capacity for the watermark. In this paper, the proposed model based on simple and integer calculations, which make it fast and consumes less memory, that ease its usage in embedded and real time systems.

3. Lifting Wavelet Transform

In 1994, Sweldens [10] proposed the second generation of wavelet transform, Lifting Wavelet Transform (LWT) in the purpose of efficiently constructing wavelet coefficients using simple and integer calculations. The computation complexity in LWT implementation is simple and requires less resources in compare to filter banks methods is used in composing DWT. LWT is an integer-to-integer computation that makes it suitable to be used in real time and embedded systems. LWT can be performed using three major steps [10, 16]:

3.1 Split

In the Split step (which is also called lazy wavelet), the signal is divided into two smaller subsets. It is used to be divided to odd samples and even samples.

3.2 Predict

A pixel value in an odd position (Xo) will be predicted by values of its two neighbors at even positions (Xe). The difference between the predicted value of a pixel in an odd position and its actual value is stored in the location of odd samples. The signal after the prediction step represents the detailed band, Dn. In gradient and smooth areas, where the intensity of the pixels is linearly changing, predicted values will be near to real values, so, values of detailed band coefficients are close to zero. However, in places of large variation of intensities, detail band coefficients will have higher values, accordingly, the larger coefficient value in a certain area is the larger divergence in pixels values at that area. This feature was exploited in the proposed texture mask. Equation (1) shows the predict step calculation.

$$Y2n+1=Xo- \text{PREDICT } (Xe) \quad (1)$$

3.3 Update

If the average of each two samples in a signal is considered instead of entire samples, the energy of this signal can be decreased to half while maintaining its overall structure [17]. In update step, the average of each two sequenced odd samples is considered the value of the even sample between them. However, because of the non-linearity nature of the pixels, the even sample value should to be updated with the difference between the real value and the predicted value in the predict steps. The obtained signal after updating is called the approximation band because it is approximately similar to the original signal but with half the number of samples (Equation 2). According to its similarity with the original signal, the approximation band is used to extract edges from the images in the proposed method.

$$Y2n=Xe + \text{UPDATE } (Y2n+1) \quad (2)$$

The three steps will produce the detailed and approximation coefficients (Figure 1). To reconstruct the original signal, the inverse of lifting wavelet transform (ILWT) is performed by applying the same LWT equation in reverse order [16], (Figure 2).

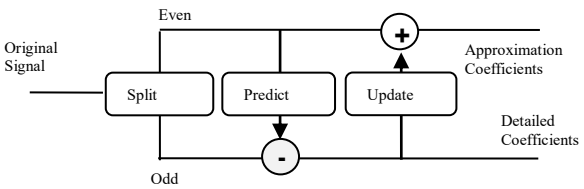

Figure 1. Forward lifting wavelet transform.

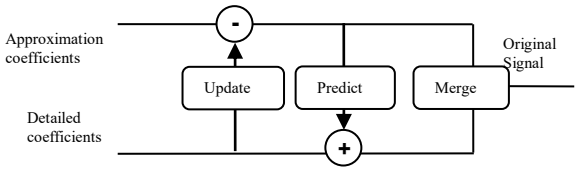

Figure 2. Inverse lifting wavelet transform

4. Proposed Method

The proposed method is divided into approximation band distribution and detection, and recovery processes.

4.1 Approximation band spread

The approximation band distribution is depicted in Figure 3. The first step is to read the original image and apply LWT on it. The size of the test image is 512×512, accordingly, the size of the approximation band after applying two LWT decompositions is 128×128 or 16384 coefficients. These coefficients have the important feature of the image; hence, they will be hidden inside the original image pixels. As a grey image, each coefficient is consisting of eight bits. These bits will be separated by bit planes each plane carries one bit, for example, plane 1 will have the MSB of all approximation band coefficients, plane 2 will have the second MSB bit of all approximation band coefficients. However; according to the limitation of the size, only the most five significant bits will be used to be embedded, as they are the most important bits. Five-bit planes will be extracted from the approximation band, which means 128×128×5=81,920 bits to be hidden.

The original image of 512×512 size will be used to hide the five pixels of bit planes. For each three pixels, for example 1, 2, 3, the average of one and three will be found, and the value of 2 will be set as the resultant average. Then, the value of the bits in bit planes will be added to or subtracted from that average. If the value of the bit plane is 1, then a fixed number, the embedding power, is added to the average of the two pixels, and if the value of the plane bit is zero then the average will be subtracted by the embedding power. Experimentally, the embedding power is set to 5.

As the original image is of 512×512 pixel, or 262,144, and one bit can be hidden in each three bits, hence the maximum number of bits is 262,144 /3 = 87,381, which is sufficient to embed five-bit planes of size 81,920.

1	((1+3)/2) ± embedding power	3

4.2 Image Recovery

The recovery process is achieved by applying the LWT on the target image and compare it with the embedded approximation band. The embedded approximation band will be determined from the average of each two odd original pixels, if the even pixel value is more than the average of its two odd neighbors' values, then the bit plane on that location is one, otherwise it is zero. Then after combining all bit planes, the approximation band (The five MSB) will be retrieved. The comparison between the two retrieved approximation band and the target one will show any tampering process that is applied to the image. Then the pixels of the retrieved approximation band will replace the tapered one, and then after applying the ILWT the original image will be displayed. The flowchart in Figure 4 shows the recovery process.

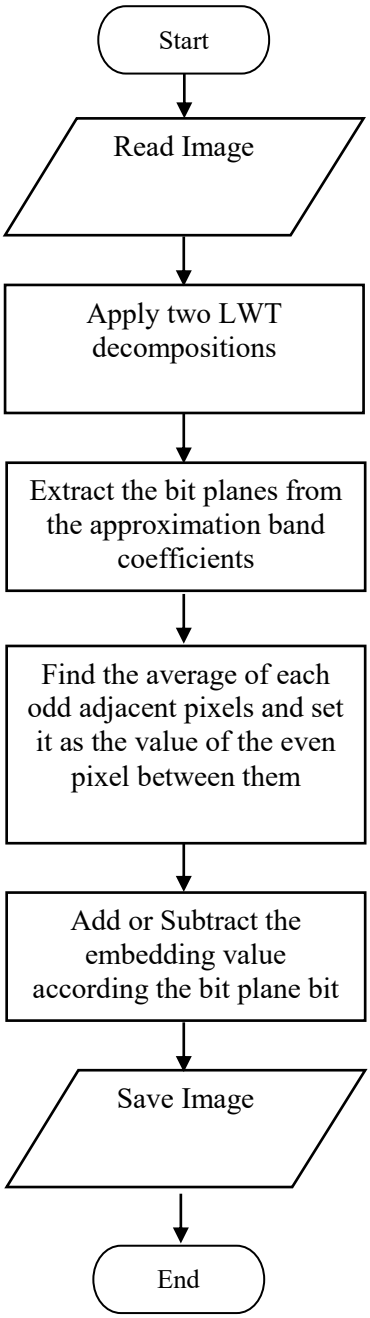

Figure 3. Approximation band distribution

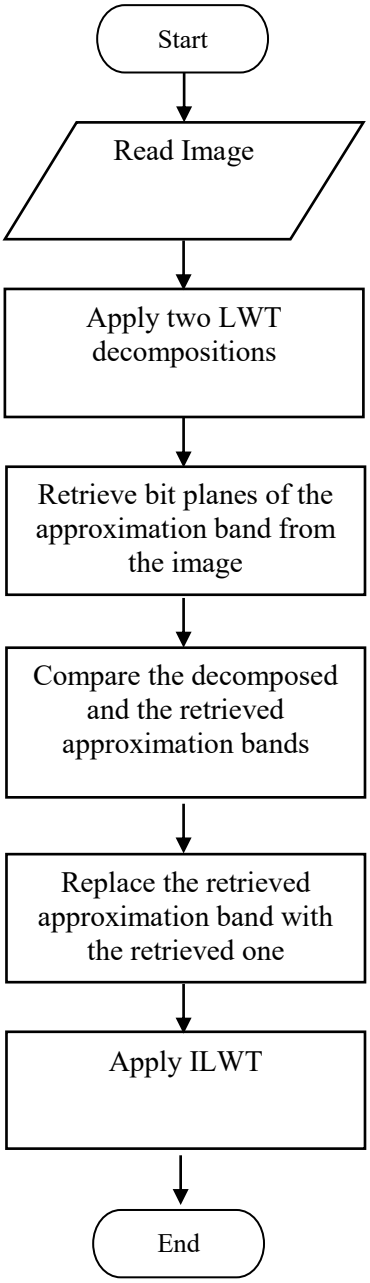

Figure 4. Image recovery process

5. Experimental Results

In order to check the performance of the algorithm, the quality of the produced images and the recovery of tampered areas were evaluated.

5.1 Image Quality

For quality assessment of the produced images, two quality measures were used, Peak signal to noise ratio (PSNR) is considered a simple objective pixel-based method in image quality evaluation. PSNR is logarithmic transformation of the mean square error (MSE). PSNR equation is given as:

$$\mathrm{PSNR} = 20\log_{10}\left(\frac{\mathrm{MAX}}{\mathrm{MSE}}\right) \tag{3}$$

and

$$\mathrm{MSE} = \frac{1}{m * n} + \sum_{x=0}^{m-1}\sum_{y=0}^{n-1} \| \mathrm{I}(x,y) - \mathrm{I}'(x,y) \|^2 \tag{4}$$

Where m, n are image dimensions and I and I' are host and direct image, respectively.

In addition to PSNR, structural similarity index (SSIM) [15] is used as more reliable measurements. The equation of SSIM is given by:

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2+\mu_y^2 + C_1)(\sigma_x^2+\sigma_y^2 + C_2)} \tag{5}$$

Where x and y are non-negative original and modified image signals, respectively. μ_x, μ_y, are the mean intensity, σ_x, σ_y are the standard deviations for the original and distorted images respectively, C1, and C2 are constants.

Eight images were used for quality evaluation where their thumbnails are shown in Figure 5.

Figure 5. Thumbnails of tested images, numbered from left to right up to bottom as img1, img2... img8

Figure 6: Original images (left), block attack (Center) and recovered images

Table 1. PSNR and SSIM result for tested image.

Image	PSNR	SSIM
Img1	30.2264	0.9836
Img2	32.6039	0.9789
Img3	32.7919	0.9826
Img4	31.4596	0.9812
Img5	25.6008	0.9580
Img6	31.7047	0.9726
Img7	33.9038	0.9914
Img8	31.4765	0.9702
Average	31.22095	0.9773125

According to Table 1, PSNR values are high and SSIM values for all tested images were larger than 0.95, which indicates that the images are in accepted and high quality [16-18].

5.2 Block Tamper Recovery

Figure 6 shows test images with blocking a certain part of each of them, and Figure 6b shows the recovered images after the blocking. The recovery process was made without using reference images, which reduce the complexity of the system in terms of memory usage. The results show that the algorithm can recover images and shows an accepted level of hidden parts.

6. Conclusion

In this paper, a new image tamper detection and recovery algorithm is presented. The algorithm considers the approximation band of the second LWT decomposition to be used as a reference image, as it has the most important features of the image. The approximation band is converted to binary bit planes and hidden inside even image pixels after they will be changed to the average of the two adjacent odd pixels. When the plane bit value is one, then a certain value called the embedding strength is added to the average, and if it is zero, then the average is subtracted by the embedding strength. In detection, LWT is applied again and the decomposed approximation band is compared with the recovered one, the difference will show the altered locations and the change will be detected and recovered. Experimental results show that the produced images have accepted quality measures, PSNR and SSIM average values are 31.22095 and 0.9773125 respectively. It also shows good recovery of the image after blocking attack. The current work is to enhance the presented algorithm by using perceptual masks to determine the best embedding strength according to image features.

References

[1] Wang, W., Dong, J., & Tan, T. (2009, August). A Survey of Passive Image Tampering Detection. In IWDW (Vol. 9, pp. 308-322).
[2] Mishra, M., & Adhikary, F. (2013). Digital image tamper detection techniques-a comprehensive study. arXiv preprint arXiv:1306.6737.
[3] Hsu, C. S., & Tu, S. F. (2010). Probability-based tampering detection scheme for digital images. Optics Communications, 283(9), 1737-1743.
[4] Rajput, V., & Ansari, I. A. (2019). Image tamper detection and self-recovery using multiple median watermarking. Multimedia Tools and Applications, 1-17.

[5] Sreenivas, K., & Kamakshiprasad, V. (2017). Improved image tamper localisation using chaotic maps and self-recovery. Journal of Visual Communication and Image Representation, 49, 164-176.
[6] Hsu, C. S., & Tu, S. F. (2016). Image tamper detection and recovery using adaptive embedding rules. Measurement, 88, 287-296.
[7] Han, S., Jin, H. L., Fujiyoshi, M., & Kiya, H. (2006, December). Lossless data hiding in the spatial domain for image tamper detection. In Intelligent Signal Processing and Communications, 2006. ISPACS'06. International Symposium on (pp. 760-763). IEEE.
[8] Chang, C. C., Hu, Y. S., & Lu, T. C. (2006). A watermarking-based image ownership and tampering authentication scheme. Pattern Recognition Letters, 27(5), 439-446.
[9] Qi, X., Xin, X., & Chang, R. (2009, November). Image authentication and tamper detection using two complementary watermarks. In Image Processing (ICIP), 2009 16th IEEE International Conference on (pp. 4257-4260). IEEE.
[10] Bhosale, S., Thube, G., Jangam, P., & Borse, R. (2012, August). Employing SVD and Wavelets for Digital Image Forensics and Tampering Detection. In Advances in Mobile Network, Communication and its Applications (MNCAPPS), 2012 International Conference on (pp. 135-138). IEEE.
[11] Dadkhah, S., Abd Manaf, A., Hori, Y., Hassanien, A. E., & Sadeghi, S. (2014). An effective SVD-based image tampering detection and self-recovery using active watermarking. Signal Processing: Image Communication, 29(10), 1197-1210.
[12] Liew, S. C., & Zain, J. M. (2011). Tamper localization and lossless recovery watermarking scheme. In Software Engineering and Computer Systems (pp. 555- 566). Springer Berlin Heidelberg.
[13] Arun Anoop, M. (2015, March). Image forgery and its detection: A survey. In Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on (pp. 1-9). IEEE.
[14] Qazi, T., Hayat, K., Khan, S. U., Madani, S. A., Khan, I. A., Kołodziej, J., ... & Xu, C. Z. (2013). Survey on blind image forgery detection. Image Processing, IET, 7(7), 660- 670.
[15] Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: from error visibility to structural similarity. Image Processing, IEEE Transactions on, 13(4), 600-612.
[16] Su, Q. (2016). Novel blind colour image watermarking technique using Hessenberg decomposition. IET image processing, 10(11), 817-829.
[17] Hsu, L.-Y., & Hu, H.-T. (2015). Blind image watermarking via exploitation of inter-block prediction and visibility threshold in DCT domain. Journal of Visual Communication and Image Representation, 32, 130–143. http://doi.org/10.1016/j.jvcir.2015.07.017.
[18] Zong, T., Xiang, Y., Natgunanathan, I., Guo, S., Zhou, W., & Beliakov, G. (2015). Robust histogram shape-based method for image watermarking. IEEE Transactions on Circuits and Systems for Video Technology, 25(5), 717-729.