International Journal of Engineering & Technology, 7 (3.29) (2018) 65-69

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Multipurpose watermarking based on hybrid strategies

P. Sivananthamaitrey [1] *, P. Rajesh Kumar [1]

[1] Andhra University College of Engineering, Visakhapatnam
**Corresponding author E-mail: psmaitrey@gmail.com*

Abstract

Dual digital watermarking has emerged as a successful solution for copyright protection, tamper detection and localization. However, several problems related to the robustness, capacity, tampered area detection still mystifying. This paper presents a high capacity dual watermarking mechanism for digital colour images. An invisible robust watermark is embedded in the Green component of the host image by using a hybrid combination of Stationary Wavelet Transform (SWT) and Singular Value Decomposition (SVD) for copyright protection. A fragile invisible watermark based on the Least Significant Bit (LSB) replacement approach is embedded in the Blue composition of the image for tamper detection and localization. The proposed technique focuses on robustness and imperceptibility while maximizing embedding capacity that makes this technique a multipurpose watermarking scheme.

Keywords: *Digital Watermarking; Stationary Wavelet Transform (SWT); Singular Value Decomposition (SVD); the Least Significant Bit (LSB).*

1. Introduction

The one of the most importance given in signal processing iThe rapid growth in internet technology makes a huge amount of multimedia data easily accessible for everyone. Nevertheless, the digital content also suffers by unlawful operations such as unauthorized copying, duplication, editing and tampering by intruders. The protection of intellectual property rights is another increasingly important concern. This indispensable issue can be better addressed by using digital watermarking technique wherein a logo image or text is used for embedding into a cover image that needs authentication.

The requirements of watermarking are imperceptibility, Robustness, capacity and Security. Although, many digital watermarking algorithms proposed, a little attention is received on dual watermarking algorithms where two watermarks usually a robust and a fragile are used. The main purpose of robust watermark is ownership identification or copyright protection. Fragile watermark is used to verify the integrity of the received images and can also locate tampered regions in an image. This paper proposes a simple and efficient dual watermarking technique for authentication, integrity verification and tamper localization. The robust watermark is embedded in the green component of the cover image by using Stationary wavelet transform (SWT) and singular value decomposition (SVD). The fragile watermark is inserted in the LSB plane of the blue component of the image.The rest of the paper is organized as follows: Literature survey is presented in section II followed by embedding and extracting process in section III. The results of the proposed method, analysis and the comparison with other recent techniques are shown in section IV and this approach is concluded in described in section V.

2. Related work

This section briefly presents the previous literature on dual watermarking. All of the literature references that are mentioned have been either used extensively in several applications or cited by other research. A blind robust watermarking technique to embed two watermarks into a cover image is proposed [1]. In this technique two binary watermarks are merged and then embedded into a host image. Sixteen merged-watermark bits are embedded into sixteen low-frequency band Discrete Wavelet Transform (DCT) coefficients of the host image. This process allows dual watermarks to be embedded many times in the host image which increases the robustness against several attacks.

A dual watermarking approach using Redundant Discrete Wavelet Transform (RDWT), block based singular value decomposition (SVD) and Arnold transforms [2] is presented. This scheme has the high embedding capacity and a little degradation in the image. A medical image watermarking with Discrete Wavelet Transform(DWT) and Singular Value Decomposition (SVD) with optimization using Firefly algorithm [3] is proposed. In this method, one watermark image (Patient information) is embedded by modifying the left singular vector while the other watermark (patient image) is embedded by modifying singular values. The watermarks are scrambled using Fibonacci-Lucas Transform. Firefly algorithm is used for optimizing PSNR and NCC.

An Image tamper detection and recovery method based on self-embedding Watermarks is proposed in [4]. The watermark used in this method is simply the down-sampled version of the cover image. Two identical watermarks are embedded into the LSB plane of the original image. This approach focuses on tampering, but failed to address copyright protection. A blind watermarking algorithm that embeds two watermarks in the host image for authentication and tamper detection is presented in [5] . It uses a Unique Identification Code (UIC) as first robust watermark which is then embedded using the 2-level DWT and a hash code of host image is used as secondary watermark for tamper detection.

A dual watermarking Algorithm is proposed in [6], in this paper, the first watermark is embedded into the high-frequency part of DWT. Using visual cryptography, they process the second watermark to generate two shares, then one of them is embedded into the low-frequency part of DWT and another is protected by the copyright. Imprecise reversible dual watermarking scheme is presented

Copyright © 2018 P. Sivananthamaitrey, P. Rajesh Kumar. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

in [7], This work proposes inserting a lossless reversible visible watermark in spatial domain based on pixel mapping method and another invisible watermark by modifying singular values in transform domain of the host image.
An eigenface is taken as the robust watermark embedded into the low frequency subband LL while the fragile watermark is based on LSB substitution to detect the tamper and locate the damaged region [8] the corresponding region of eigenface is used to recover the image. A modified dual watermarking scheme [9], this paper presents watermarks generation from the host image itself. The robust watermark inserted into the region of interest (ROI) based on Integer Wavelet Transform (IWT) and the secondary watermark is embedded by the LSB substitution for tamper localization and recovery.
A visual watermark method of implanting Quick Response (QR) Code image onto the grayscale image [10] is proposed. The insertion method changes the pixel values by adding positive random values to them, such that the altered results are visible. Subsequently, the watermark information is concealed in the gray image by a reversible steganographic procedure. The watermark information can be extracted to recover the watermarked images.
A dual watermarking technique based on Contourlet and SVD is proposed in [11]. Here, two watermarks are inserted into the low frequency and high frequency components of the host image and using SVD. While extraction the two watermarks are compared with the original watermarks and the one whose similarity is higher is adopted as the required watermark. A dual digital watermarking technology for digital rights management is presented in [12], in this paper, the first watermark for copyright protection of the owner is embedded in the low and middle frequency of DCT coefficients of the cover image. The second watermark belongs to the customer is embedded in the DC coefficients.
A Dual watermarking method for secure image authentication and recovery [13] is proposed. In this paper, The first watermark is binary and is used to accurately authenticate the content and determine and classify the manipulations. The second watermark (image digest); highly compressed version of the host image, is used to recover the approximation of the image. Both the IDCT and IWT are utilized to generate and embed the watermarks. Huffman coding is used to reduce the capacity of the image digest. Both of the watermarks are embedded in suitable wavelet coefficients.
A blind dual watermarking mechanism for digital color images is presented in [14]. Here, invisible robust and fragile watermarks are embedded for copyright protection and image authentication respectively. The robust watermark is embedded by using DWT in YCbCr color space, and the fragile watermark is based on an improved least significant bit (LSB) replacement approach in RGB planes.
A DWT based spread-spectrum watermarking algorithm [15] is proposed that uses medical image as the cover. The image watermark representing health center name in binary image format is embedded into intermediate frequency sub-bands (HL1 and LH1) of the first level DWT coefficients and the patient's identity/reference as text watermark is embedded into selected sub-band DWT coefficients (HL2 and LH2) of the second level.
All the above works primarily focused on the robustness of the watermark and imperceptibility of the host image. Some of them also focused on the recovery of the original image from tampering. Moreover, the stationary wavelet transform (SWT) has not been used so far in the dual watermarking system despite its time invariance property. The proposed technique uses SWT and also concentrates on robustness and imperceptibility while maintaining maximum embedding capacity which can be employed in applications such as embedding complete patient image and information into corresponding medical images.

3. Proposed algorithm

This section elaborates the proposed watermarking mechanism in detail. In order to achieve copyright protection and tamper detection, a simple, efficient dual watermarking technique for colour images is presented. The two watermarks both of them are of 512×512 size are inserted in the host image of 512×512 size. In order to compare the experimental results with other recent works, the proposed method is applied on standard image 'Lena' and is implemented using MATLAB. The details of dual watermark embedding and extraction processes are described in the below subsections.

a) Robust watermark embedding process for copyright protection

It is verified in the literature, a watermark is more robust when it is embedded in the transform domain. In order to enhance the watermark holding capacity of the image, the stationary wavelet transform (SWT) is used as it produces the equivalent sized bands as that of host image. The algorithm is given below.
Step1: A 512×512 color image is resolved into Red, Green and Blue components and a 512×512 gray image is considered for watermark.
Step2: SWT using Haar wavelet is applied at the Green component of the host image and gray watermark image as
given in Eq.1 and Eq.2

$$[LL, LH, HL, HH] = SWT(Green) \quad (1)$$

$$[LL', LH', HL', HH',] = SWT(\ watermark) \quad (2)$$

Step3: Singular Value Decomposition (SVD) is applied on HH and HH' bands as given by Eq.3 and Eq.4. The eigen values, thus obtained are mixed using a scaling factor ' α ' given by Eq.5

$$[U, S, V] = SVD(HH) \quad (3)$$

$$[, U', S', V'] = SVD(HH') \quad (4)$$

$$Snew = \ S + \alpha * S' \quad (5)$$

Step4: The inverse SVD and ISWT are computed to obtain the watermarked Green plane as given by Eq.6 and Eq.7

$$HH'' = \ U * Snew * V^T \quad (6)$$

$$Green' = ISWT(LL, LH, HL, HH'')$$

The block diagram of the complete embedding process is shown in figure 1.

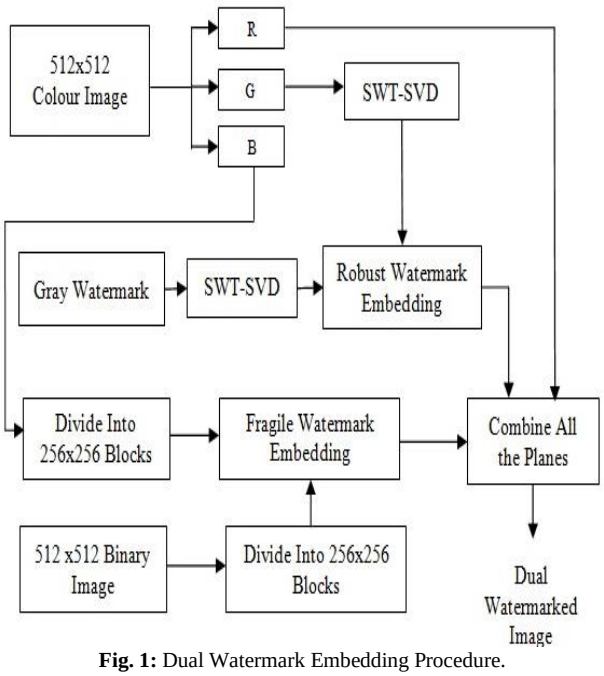


Fig. 1: Dual Watermark Embedding Procedure.

b) Fragile watermark embedding process for tamper detection and localization

In order to identify any malicious changes made to the original images, the watermark need to be very sensitive to the tampers. The following steps describe the process.

Step1: A 512×512 binary watermark is divided into four 256×256 sub images.

Step2: The Blue plane of the host image is also divided into four 256×256 sub planes.

Step3: Each sub plane is embedded with the corresponding sub watermark by least significant bit (LSB) substitution technique.

Step4: All the sub planes are combined to get watermarked Blue plane.

Finally, all the R, G and Blue planes are combined to get a dual watermarked image.

c) Fragile Watermark extraction

The process of fragile watermark extraction is given below

Step1: The watermarked image is resolved into Red, Green and Blue components.

Step2: The 512×512 Blue component is divided into four sub images of 256×256.

Step3: The least significant bits of a sub images are used to obtain the four parts of the watermark

Step4: All the extracted parts from the sub images are then combined to form the binary watermark.

The complete extraction procedure is depicted in figure2.

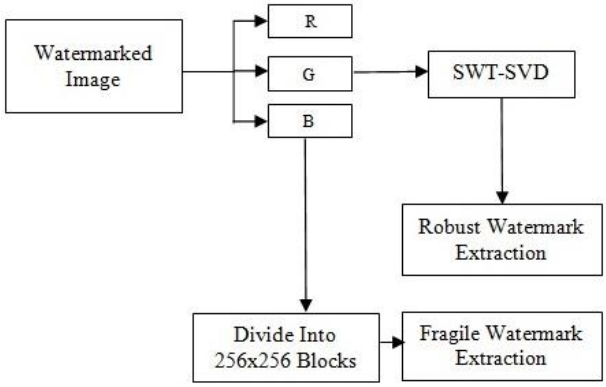


Fig. 2: Dual Watermark Extracting Procedure.

d) Robust watermark extraction

The procedure for extraction of robust watermark is described here.

Step1: SWT followed by SVD computed on the Green plane of the watermarked image as given by Eq.7 and Eq.8

$$[LL, LH, HL, HH''] = SWT(Green') \tag{7}$$

$$[, U'', S'', V''] = SVD(HH'') \tag{8}$$

Step2: The constant 'α' is used to get the eigen values of the watermark from the eigen values of the Green plane and is shown in Eq.9

$$Swm = (S'' - S)/\alpha \tag{9}$$

Step3: Inverse SVD is computed using the eigen values obtained in Step2 followed by Inverse SWT to get the robust watermark as given by Eq.10 and Eq.11

$$HX'' = U' * Swm * V'^{T} \tag{10}$$

$$Robust = ISWT(LL, LH, HL, HX'') \tag{11}$$

4. Results and analysis

a) Imperceptibility and Robustness Test

The proposed algorithm is implemented in MATLAB and the performance of the technique is evaluated by applying various image processing attacks and geometric transformations on watermarked image. This section presents the obtained results and comparison with the other significant dual watermarking techniques. The imperceptibility of watermarked image is evaluated by the following equations. The mean square error (MSE) between original image f and watermarked image f^' is calculated using Eq. (12) which in turn used to evaluate

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(f(i,j) - f'(i,j)\right)^2 \tag{12}$$

The peak signal to noise ratio (PSNR) is calculated from Eq. (13).

$$PSNR = 10\,log[(255)^2/MSE] \tag{13}$$

The robustness of the proposed technique is evaluated by using normalized correlation coefficient (NCC) which is evaluated by Eq. (14). The NCC values represent the similarity between original watermark W and extracted watermark W'.

$$NCC = \frac{\sum_i \sum_j W(i,j).W'(i,j)}{\sum_i \sum_j w^2(i,j)} \tag{14}$$

Table 1 compares the imperceptibility (PSNR) of the proposed technique with methods of Singh et al. (2017), Sejpal et al. (2016) and Liu et al. (2016).

Table 1: Comparison of PSNR Values of Other Methods with the Proposed Method

	Singh et al [15]	Sejpal et al [3]	Liu et al[14]	Proposed Method
PSNR(dB)	32.48	84.51	40.85	55.88

To verify the watermark imperceptibility and robustness of the proposed method, all watermarked images are subjected to some common image processing operations such as adding Gaussian noise, adding Salt-and-Pepper noise, median filtering, blurring, JPEG compression, sharpening and histogram equalization and geometrical distortions such as resizing, rotation, and cropping).The attacked watermarked images and corresponding extracted watermarks are presented in Figure 3.



Fig. 3: Attacked Images on the Top and the Corresponding Extracted Watermark Images at the Bottom.

The robustness performance in terms of NCC is compared

with the other techniques and the imperceptibility performance in terms of PSNR of the proposed method by subjecting the watermarked image to various attacks is presented in Table 2.

Table 2: Comparison of Robustness Performance Results of Other Methods with the Proposed Method Along with PSNR Subjecting to Various Attacks.

Attack Type	Depth	Singh et al.[15] NCC	Sejpal et al.[3] NCC	Liu et al.[14] NCC	Proposed Method NCC	Proposed Method PSNR
No Attack		1.0000	1.0000	1.0000	1.0000	55.88
Gaussian Noise	0.01	0.7335	0.9269	0.9664	0.9889	20.17
	0.05	0.6964	--	--	0.9786	19.31
	0.1	--	0.8868	--	0.9580	17.38
	0.3	--	--	0.9171	0.9390	10.9
	0.5	--	--	0.8735	0.9093	7.46
Salt and Pepper Noise	0.01	--	0.9431	0.9990	0.9997	25.18
	0.02	0.7391	--	0.9981	0.9994	22.11
	0.04	--	--	0.9959	0.9985	19.19
	0.08	--	--	0.9893	0.9967	16.16
	0.1	0.7155	0.9064	--	0.9859	15.16
Median filtering	2×2	0.6736	0.8995	--	0.9698	29.21
	3×3	0.2216	0.9033	--	0.9499	33.79
Scaling	25%	--	--	--	0.9398	28.62
	50%	--	--	0.5188	0.9698	32.98
	200%	0.7394	--	0.9998	0.9999	42.19
Rotate	45^0	--	--	--	0.9999	7.36
	90^0	--	--	--	1.0000	11.51
Blur	0.1	--	--	0.9997	1.0000	55.87
	0.2	--	--	0.9514	1.9889	55.87
	0.3	--	--	0.8735	1.9656	55.84
JPEG Compression	90	0.7394	--	0.9967	0.9999	34.74
	80	0.7394	0.9941	0.9842	0.9997	33.59
	70	0.7394	0.9835	0.9711	0.9899	32.89
	60	0.7364	--	0.8687	0.9699	32.40
	40	0.7335	--	--	0.9497	31.52
Crop	10%	--	--	0.9998	1.0000	14.80
	30%	--	--	0.9989	0.9997	9.87
Sharpen	0.1	0.7394	--	--	1.0000	48.87
HE		0.7394	0.9949	--	1.0000	14.22
Brighten	50	--	--	0.9904	1.0000	14.49
	80	--	--	0.9806	0.9998	10.82
Darken	50	--	--	0.9655	0.9999	14.36
	80	--	--	0.8813	0.9998	10.5

It can be inferred from Table.1 and Table 2 that the performance of the proposed method is superior to Singh et al.[15] and Liu et al.[14] in terms of both imperceptibility and robustness .The technique proposed by Sejpal et al.[3] is superior in imperceptibility and inferior in robustness to the proposed method .

b) Tamper detection and Localization Test

The watermark embedded in the Blue component of the host image is fragile, i.e., very sensitive to any image processing and geometric attacks as it is inserted in the LSB positions of the plane. This feature of fragility is exploited in determining whether the image has been tampered or not (Image authentication or Integrity) and also to locate the tampered region of the image.

The proposed method divides the fragile watermark into four parts as shown in Fig 4. Before being embedded and the four parts are assigned with a nomenclature of top-left, top-right, bottom-left and bottom-right.

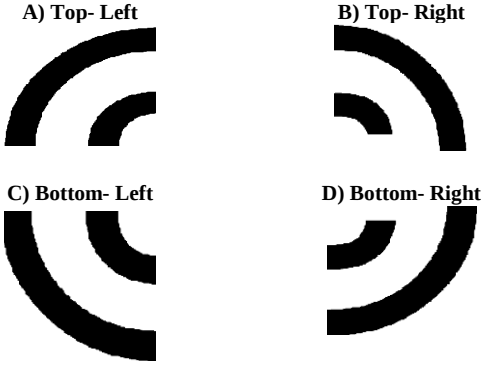


Fig. 4: The Four Parts of the Watermark.

The watermarked image is tampered with various attacks such as mosaic effect, blurring, median filtering and flipping some portion of the image. The extracted watermarks clearly show the locations where the image actually got tampered. The watermarked images are tampered with using XnView software and are shown in Fig.5 (a), (b), (e) and (f). The extracted watermarks are shown in Fig.5 (c), (d), (g) and (h).

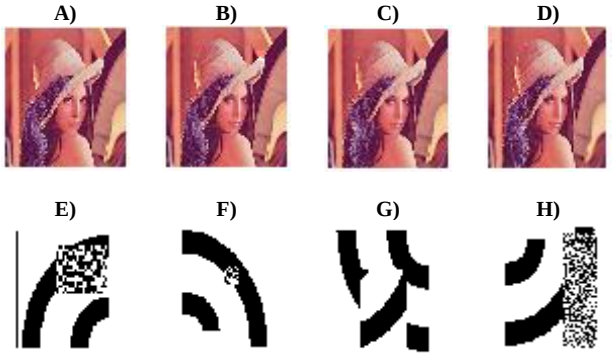


Fig. 5: A) Image Tampered by Mosaic Effect on the Hat. B) Image Blurred at the Front Tip of the Hat. C) Image Tampered by Flipping a Part of Hair. (D) Image Tampered in the Mirror by Median Filtering by 13×13 Mask.(E) Extracted Watermark from the Top-Left Portion of the Image Showing the Tampered Location .(F) Extracted Watermark From the Top-Right Portion of the Image Showing the Tampered Location.(G) Extracted Watermark From the Bottom-Left Portion of the Image Showing the Tampered Location. (H) Extracted Watermark from the Bottom-Right Portion of the Image Showing the Tampered Location.

5. Conclusion

A multipurpose watermarking scheme for both copy right protection, authentication and tamper detection has been presented in this paper. The proposed scheme has four special features:

1) It embeds two watermarks both of size equivalent to that of host image while maintaining significantly higher PSNR which makes this scheme a high capacity and high imperceptibility dual watermarking technique.
2) The SWT and SVD hybrid strategy has been proven from NCC values that this scheme achieves better robustness over the other significant works of similar kind.
3) As the fragile watermark is inserted using LSB substitution method, it is more vulnerable to any malicious attacks which make the detection and localization of tampers becomes easy.
4) This scheme does not involve any complex calculations hence it is clearly understood and easy to implement even on hardware. Despite its simplicity, this scheme has proven to be efficient in terms of imperceptibility and robustness. This is the first technique that combines both robust and fragile watermarks of same size as that of host image.

References

[1] Lu, Chun-Shien and Hong-Yuan Mark Liao. "Multipurpose watermarking for image authentication and protection." IEEE transactions on image processing: a publication of the IEEE Signal Processing Society 10 10 (2001): 1579-92.

[2] Sachin Gaur, Vinay Kumar Srivastava "A RDWT and Block-SVD based dual watermarking scheme for digital images".

[3] Sejpal, Shveti & Shah, Nikesh. (2016). "A novel multiple objective optimized dual watermarking scheme based on DWT-SVD using Firefly algorithm." 46-51. 10.1109/CAST.2016.7914938.

[4] Kiatpapan, Sawiya and Toshiaki Kondo. "An image tamper detection and recovery method based on self-embedding dual watermarking." 2015 12th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON) (2015): 1-6.

[5] Saiyyad, Mohmmad Ali M. and Nitin N. Patil. "Authentication and tamper detection in images using dual watermarking approach." Proceedings of third International Conference on Reliability, Infocom Technologies and Optimization (2014): 1-5.

[6] Han, Yanyan et al. "DWT-Domain dual watermarking algorithm of color image Based on Visual Cryptography." 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (2013): 373-378.

[7] Mehra, Neelesh & Shandilya, Madhu. (2013). "Imprecise reversible dual watermarking scheme." Journal of Advances in Information Technology. 4. 10.4304/jait.4.4.166-171.
[8] Qi Han, Lei Han, Erfu Wang, Jie Yang "Dual Watermarking for Image Tamper Detection and Self-recovery".
[9] Tashk, A., Danyali, H.M., & Alavianmehr, M.A. (2012). "A modified dual watermarking scheme for digital images with tamper localization/detection and recovery capabilities." 2012 ninth International ISC Conference on Information Security and Cryptology, 60-65.
[10] Hsu, Fu-Hau, Min-Hao Wu and Shiuh-Jeng Wang. "Dual-Watermarking by QR-code applications in image processing." 2012 ninth International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing (2012): 638-643.
[11] Zhang, Jianhong & Yang, Xiaoming & Xie, Xiaofei. (2010). "Dual-watermarking algorithm based on Contourlet." International Conference on Intelligent Control and Information Processing (ICICIP). 10.1109/ICICIP.2010.5564207.
[12] Liao, Yeqing and Quan Liu. "Applying dual digital watermarking technology in digital rights management." The third International Conference on Information Sciences and Interaction Sciences (2010): 616-619.
[13] Chamlawi, Rafiullah, Imran Usman and Asifullah Khan. "Dual watermarking method for secure image authentication and recovery." 2009 IEEE 13th International Multitopic Conference (2009): 1-4.
[14] X. L. Liu, C. C. Lin and S. M. Yuan, "Blind dual watermarking for color images' authentication and copyright protection," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 28, no. 5, pp. 1047-1055, May 2018.
[15] Singh A.K., Kumar B., Singh G., Mohan A. (2017) "Secure Spread Spectrum Based Multiple Watermarking Technique for Medical Images." Medical Image Watermarking. Multimedia Systems and Applications. Springer, Cham.