Medical Images Watermarking using Wavelet Transform and DCT

Rumen P. Mironov[1], Stoyan Kushlev[2]

***Abstract* – An algorithm for digital watermarking of medical images using Wavelet transform and DCT is presented. The developed algorithm ensures high transparency of the watermark and is resistant to various types of malicious attacks. The obtained experimental results for some attacks over the test medical images are made on the base of mean-squared error and signal to noise ratio of the reconstructed images.**

***Keywords* – Medical Image Watermarking, Wavelet Transform, DCT, Unitary Transforms.**

I. INTRODUCTION

Recent technological advances in Computer Science and Telecommunications introduced a radical change in the modern health care sector, including: medical imaging facilities, Picture Archiving and Communications System (PACS), Hospital Information Systems (HIS), information management systems in hospitals which forms the information technology infrastructure for a hospital based on the DICOM (Digital Imaging and Communication in Medicine) standard. These services are introducing new practices for the doctors as well as for the patients by enabling remote access, transmission, and interpretation of the medical images for diagnosis purposes [1], [2], [3].

Digital watermarking has various attractive properties to complement the existing security measures that can offer better protection for various multimedia applications [4]. The applicability of digital watermarking in medical imaging is studied in [5] and a further justification of the watermarking considering the security requirements in teleradiology is discussed in [2].

The new medical information systems required medical images to be protected from unauthorized modification, destruction or quality degradation of visual information. The other problem is a copyright protection of disseminated medical information over Internet. In this regard three main objectives of watermarking in the medical image applications: data hiding, integrity control, and authenticity are outlined in [5], which can provide the required security of medical images.

[1]Rumen P. Mironov is with the Faculty of Telecommunications, Technical University of Sofia, Boul. Kl. Ohridsky 8, Sofia 1000, Bulgaria. E-mail: rmironov@tu-sofia.bg

[2]Stoyan Kushlev is with the Faculty of Telecommunications, Technical University of Sofia, Boul. Kl. Ohridsky, 8, Sofia 1000, Bulgaria. E-mail: skushlev@mail.bg

Every system for watermarking can be characterized with invisibility of the watermark, security of the watermark, robustness of the watermark and the ability for reversible watermarking. The importance of each depends on the application and how it is used [6], [7]. For the needs of medicine the main watermarking characteristics are:

- Invisibility of the watermark – the embedded watermark should be invisible without reducing the quality of the original images;
- Security of the watermark – secrecy to unauthorized persons of the information for the embedded watermark;
- Robustness and fragility of the watermark – robust watermarking is resistant to possible attacks such as image processing and on the other hand fragile watermarks will allow high detection of unauthorized access or attacks on the watermark;
- Reversibility of the watermark – removing of the embedded watermark should not reduce the quality of the original images.

Based on processing domain, watermark techniques can be separated as watermarking in spatial domain, watermarking in frequency domain and watermarking in phase domain of the input signal. According to the way of watermark preprocessing, discern two groups of methods: the first one is when the watermark is transformed in the domain of the input image and the second one is when the watermark is not transformed in the domain of the input image. Another classification is based upon the transparency of the watermark into the input images - the watermark is transparent or non- transparent.

Watermarking in spatial domain allow easy realization of the algorithms for watermarking. The disadvantage of using the spatial domain is that the watermarks have low efficiency and robustness. Using frequency and phase domain allow watermarks with high transparency and robustness. On the other hand using transformations on the watermarks themselves assures high security agents against unauthorized attacks.

The best way to test the watermark robustness is by simulating of unauthorized attacks. Unauthorized attacks are attacks against the integrity of the watermark. The most used attacks are unauthorized removal, adding or detection of watermark. The removal and adding of watermarks are active attacks while the detections of watermarks are passive attacks.

An outline of the medical image watermarking field that uses various techniques to embed watermark data and utilize various functions to detect tampered regions is given below in the paper [8].

In the present work an algorithm for digital watermarking of medical images using Wavelet transform and DCT is described. The developed algorithm ensures high transparency of the

watermark and is resistant to various types of malicious attacks. The obtained experimental results for some simulated attacks over the three test medical images are made on the base of mean-squared error and signal to noise ratio of the reconstructed images. The robustness of the watermark against some attacks are tested with the post processing of watermarked images by adding of Salt and Pepper noise, Gaussian noise, filtration whit median filters and average filters.

II. Mathematical Description

The common block scheme of the developed algorithm for watermarking is shown on Fig.1.

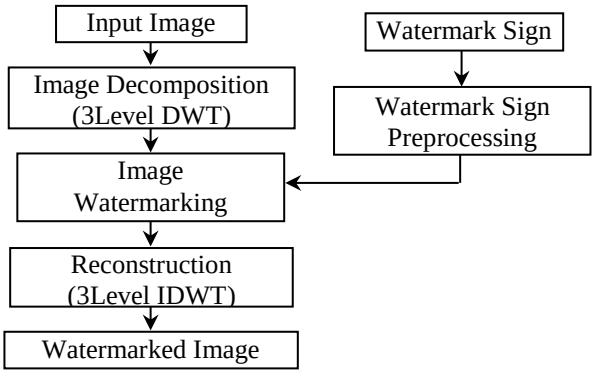


Fig.1. Common block scheme of watermarking.

The input image is decomposed into 3 levels via two dimensional Discrete Wavelet Transform (2D DWT). The transformed by the 2D discrete cosine transform (DCT) image of the digital watermark is included in one of the three 2D DCT transformed blocks from the 3th level of the 2D DWT – LH3, HL3 or HH3. The choice of the watermark insertion block with size PxQ is based on the maximum of entropy. Watermarking is performed by the following formula:

$$C_{k'} = C_k + a \times V_k, k = 1, 2, \dots, P \times Q \quad , \qquad (1)$$

where: C_k are the coefficients of the transformed insertion block, V_k are the coefficients of the transformed watermark, k is the consecutive number of the coefficients and a is parameter which determines the depth of watermarking. The value of the coefficient a must satisfy the markup threshold. The threshold is dynamically determined in relation to the input image, which is 10 percent lower than the entropy of the selected block. In reconstruction block the inverse wavelet transform (2D IDWT) is applied and the output watermarked image is obtained.

The developed decoder is informed. The transformed images - marked and original are including at the input. The purpose of the decoder is to determine what message (sign) is included in the watermarked image. The information about the block where the watermark is written, the markup threshold, and the markup factor is recorded in the header of the format used. The watermark is retrieved by the following formula:

$$V_{k'} = (C_{k'} - C_k)/a, k = 1, 2, \dots, P \times Q \quad , \qquad (2)$$

where: $C_{k'}$ are the coefficients of the transformed insertion block of the watermarked image, C_k are the coefficients of the transformed correspondent block of the original image, $V_{k'}$ are the coefficients of the transformed watermark. The watermark is received in the reconstruction unit. Over the data received by the decoder applies inverse discreet wavelet transform.

III. Experimental Results

For the analyses of efficiency of the developed algorithm for watermarking of medical images three test images, shown in Fig.1a, b, c, with size 512x512 and 256 gray levels are used.

Fig.1a. Input X-ray test image “Spine 1”.

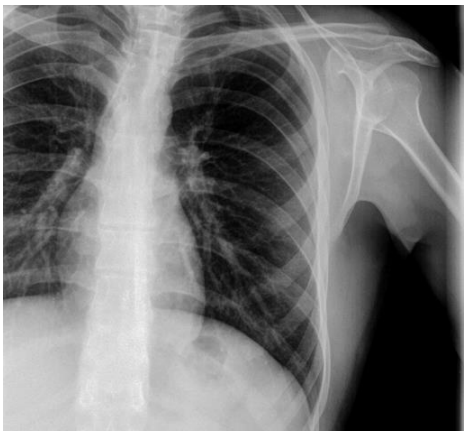


Fig.1b. Input X-ray test image “Spine 2”.

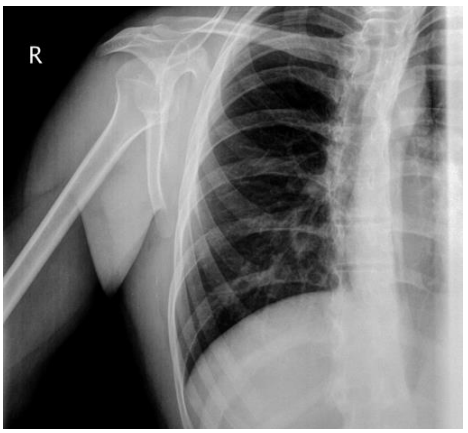


Fig.1c. Input X-ray test image “Spine 3”.

Based on the described sequence in Section II, algorithm for embedding of watermark and algorithm for extraction of the watermark have been developed and have been simulated by the developed with MATLAB programs.

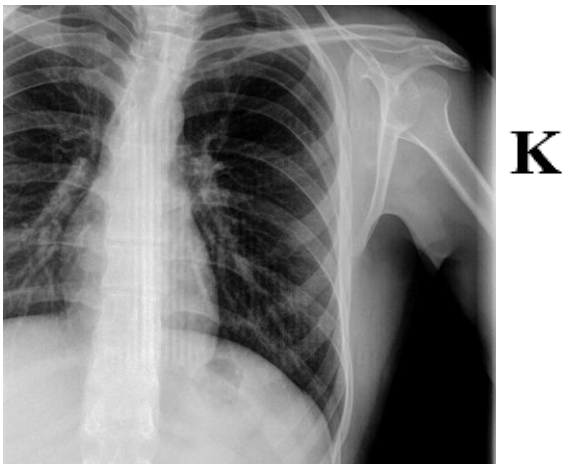
The test images shown in Fig.1 are transformed by the 3 levels 2D DWT and the input watermark (letter K) is embedded into the transformed block (LH3, HL3 or HH3) with maximum entropy of each image.

The robustness of the watermark against some popular attacks are simulated with the post processing of watermarked images by adding 100% of Gaussian noise with mean 0 and variance 0.01; adding 100% of Salt and Pepper noise; filtration with median filter with size 3x3; filtration of Gaussian noisy image with average filter; filtration of Salt and Pepper noisy image with median filter. The obtained results for the test images are summarized in Tabl.1.

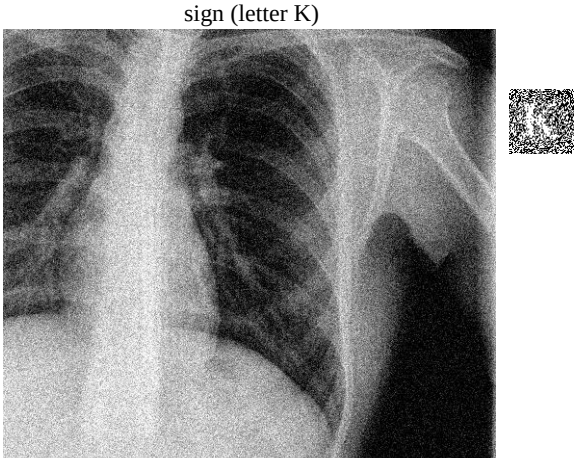
Tabl.1

Test Images	"Spine 1"	"Spine 2"	"Spine 3"
Reconstructed Watermarked image			
SNR, dB	19.86	18.16	18.71
PSNR, dB	45.8	42.72	43.49
MSE	1.71	3.48	2.91
NMSE	0.01	0.015	0.01
NMSE, %	1	1.5	1
NC	0.57	0.53	0.55
NC, %	57	53	55
Watermarked image with Gaussian noise			
SNR, dB	4.66	4.67	4.69
PSNR, dB	30.6	29.22	29.47
MSE	56.67	77.74	73.55
NMSE	0.34	0.34	0.34
NMSE, %	34	34	34
NC	0.34	0.46	0.42
NC, %	34	46	42
Watermarked image with Salt and Pepper noise			
SNR, dB	14.54	14.02	14.27
PSNR, dB	40.48	38.57	39.05
MSE	5.82	9.04	8.1
NMSE	0.035	0.04	0.038
NMSE, %	3.50	4	4
NC	0.36	0.41	0.39
NC, %	36	41	39
Watermarked image with median filtration			
SNR, dB	16.13	17.4	17.99
PSNR, dB	45.07	41.95	42.77
MSE	2.02	4.15	3.44
NMSE	0.012	0.018	0.016
NMSE, %	1.20%	1.80%	1.60%
NC	0.57	0.52	0.55
NC, %	57%	52%	55%
Watermarked image with Salt and Pepper noise and median filtration			
SNR, dB	18.55	16.99	17.6
PSNR, dB	44.49	41.54	42.38
MSE	2.31	4.57	3.76
NMSE	0.01	0.02	0.017
NMSE, %	1%	2%	1.70%
NC	0.56	0.52	0.55
NC, %	56%	52%	55%
Watermarked image with Gaussian noise and average filtration			
SNR, dB	8.86	8.6	8.6
PSNR, dB	34.8	33.15	33.38
MSE	21.51	31.49	29.88
NMSE	0.13	0.14	0.14
NMSE, %	13%	14%	14%
NC	0.34	0.43	0.41
NC, %	34%	43%	41%

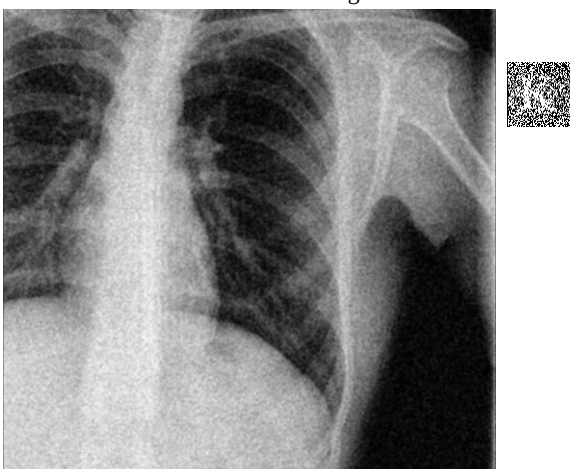
To estimating the efficiency of the developed algorithms for watermarking of medical images the following metrics are used: peek signal to noise ratio (PSNR) estimate how transparent is the watermark to the human eyes; normalize cross-correlation (NC) is used to determinate how close the extracted watermark is compared to the original. High value of NC means that there are little differences between them; mean square error (MSE) and normalized mean square error (NMSE) are used to determinate how much the watermark image has change compared to the original.



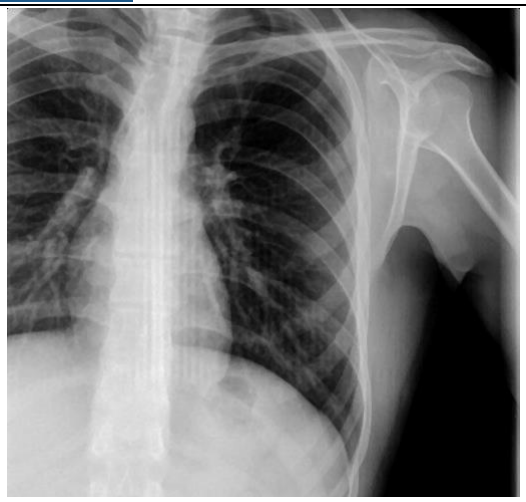
a. Input watermarked image and original watermark sign (letter K)



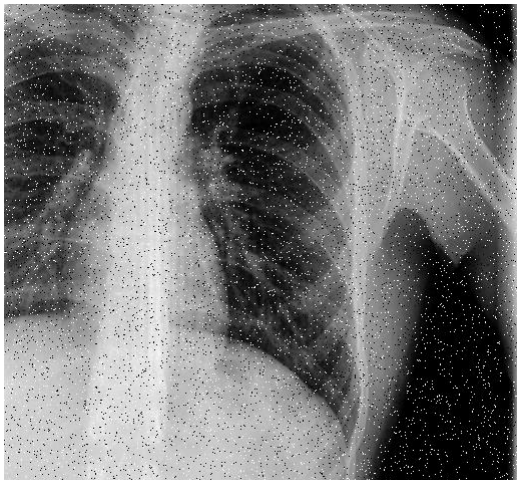
b. Input watermarked image with Gaussian noise and extracted watermark sign



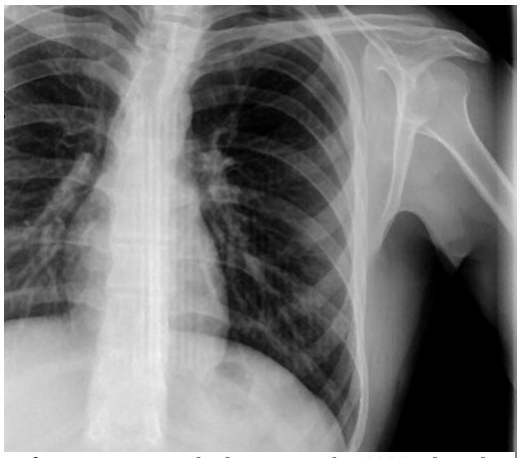
c. Input watermarked image with Gaussian noise and average filter and extracted watermark sign



d. Input watermarked image with median filter and extracted watermark sign



e. Input watermarked image with 100% salt and pepper noise and extracted watermark sign



f. Input watermarked image with 100% salt and pepper noise and median filter and extracted watermark sign

Fig.2. Results for watermarked image "Spine 2" with different post processing attacks

In Fig.2 a-f the visual results for watermarked image "Spine 2" with different post processing attacks are shown. On the right corner of each image is shown the extracted watermark.

IV. Conclusion

An algorithm for digital watermarking of medical images using Wavelet transform and DCT is presented. The obtained experimental results for some attacks over the three test medical images are made on the base of mean-squared error, signal to noise ratio and normalized cross-correlation of the reconstructed images. They shows that the developed algorithm for watermarking allows high robustness to possible attacks based on image processing operations as transforms, filtrations and etc. On the other hand the embedded watermark is practically invisible for the doctors and retains largely the information in the original images. This will allow to a great extent to verify the reliability of the medical data transmitted and recorded as images.

All this leads to the conclusion that the developed algorithm can be used successfully for watermarking not only of medical but on other type of data presented as images.

V. Acknowledgement

The author thank the National Fund for Scientific Research of the Bulgarian Ministry of Education and Science for the financial support by the contract I-02/1.

VI. References

[1] P. Koushik, G. Ghosh, M. Bhattacharya. "Biomedical Image Watermarking in Wavelet Domain for Data Integrity Using Bit Majority Algorithm and Multiple Copies of Hidden Information". *American Journal of Biomedical Engineering*, 2012, vol. 2(2), pp. 29-37.

[2] H. Nyeem, W. Boles, C. Boyd. "A Review of Medical Image Watermarking Requirements for Teleradiology". *Journal Digital Imaging*, 2013, vol. 26, pp.326–343.

[3] L. Siau-Chuin, J.M. Zain. "Reversible medical image watermarking for tamper detection and recovery", *3rd IEEE International Conference on Computer Science and Information Technology*, 2010, vol. 5, pp. 417 – 420.

[4] I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker. *Digital watermarking and steganography*. 2nd Edition, Elsevier, Burlington, 2007.

[5] Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec. "Relevance of watermarking in medical imaging". *Proceeding of IEEE EMBS International Conference on Information Technology Applications in Biomedicine*, 2000, pp. 250–255.

[6] W. K. Pratt. *Digital Image Processing*, 4th Ed., John Wiley & Sons. Inc., Hoboken, New Jersey, 2007.

[7] R. C. Gonzalez, R. E. Woods. *Digital Image Processing*, Third Ed., Pearson Education Inc., 2008.

[8] A. Ustubioglu, G. Ulutas. "A New Medical Image Watermarking Technique with Finer Tamper Localization". *Journal of Digital Imaging*. Springer International Publishing, 2017, pp.1-17.

[9] Mahasweta, J. Joshi et al. "Watermarking in DCT-DWT Domain", *International Journal of Computer Science and Information Technologies* (IJCSIT), Vol. 2 (2), 2011, pp. 717-720.

[10] Neha Singh, Mamta Jain, Sunil Sharma, "A Survey of Digital Watermarking Techniques", *International Journal of Modern Communication Technologies & Research*, August 2013