Algorithms for Digital Watermarking of the Health System Images with Hadamard Transform

Rumen P Mironov, Stoyan Kushlev
Faculty of Telecommunications
Technical University of Sofia
Boul. Kl. Ohridsky 8, Sofia 1000
Bulgaria
{rmironov@tu-sofia.bg}, {skushlev@mail.bg}

ABSTRACT: *In this work we have presented using a complex hadamard transform an algorithm for digital watermarking of health system images. We are able to detection the unauthorized access and attacks in the watermarking with the help of the newly introduced algorithms. The experimental results of the some attacks over the test medical images are drawn made on the base of mean-squared error and signal to noise ratio of the reconstructed images.*

Keywords: Medical Image Watermarking, Complex Hadamard Transform, Orthogonal Transforms

Received: 2 September 2020, Revised 28 November 2020, Accepted 5 December 2020

DOI: 10.6025/jmpt/2021/12/1/18-25

1. 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.

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], and [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 nontransparent.

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 whit high transparency and robustness. Using transformations on the watermarks themselves assures high security agents 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 command 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 complex Hadamard transform is described. The developed algorithm allow high detection of unauthorized access or attacks on the included watermark. The obtained experimental results for some simulated attacks over the 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.

2. Mathematical Description

The common results and properties, obtained from the one dimensional Complex Hadamard Transform, described in [9], can be generalized for two-dimensional Complex Hadamard Transform. In this case the 2D signals (images) can be represented by the input matrix [X] with the size *N*x*N*. The result is a spatial spectrum matrix [Y] with the same size. The corresponding equations for the forward and the inverse 2D CHT are:

$$\left| \begin{array}{l} [Y] = [CH_N][X][CH_N] \\ [X] = \frac{1}{N^2}[CH_N][Y][CH_N] \end{array} \right. \qquad (1)$$

The Hadamard transformation is simple for implementation transformation, there for it is used for compression and watermarking of information. The proposed complex Hadamard transform matrix has the advantages of having similar structure as the well know real Hadamard matrix. The complex Hadamard matrix consists of only four values {1; -1; j; -j}. The properties of complex Hadamard transform matrices and its applications in digital image processing are described in detail in [9], [10].

The developed algorithm for embedding of watermark is made in the following steps:

- **Step 1:** Preparation of the image – the image is prepared for embedding using the forward complex Hadamard transformation.

- **Step 2:** Embedding the watermark into the image – the embedding process of the watermark is based upon modifying the phase of the spectrum coefficients.

- **Step 3:** Reconstruction of the image – the reconstruction of the image is done using the reverse complex Hadamard transformation.

The extraction of the watermark is made by the following steps:

- **Step 1:** Preparation of the watermark image – same as in the embedding the image is prepared using the forward complex Hadamard transformation.

- **Step 2:** Preparation of the non-watermarked image – for the extraction of the watermark in the decoder a non-watermark copy of the image is used. The non watermark image is prepared using the forward complex Hadamard transformation.

- **Step 3:** Extracting the watermark from the image.

- **Step 4:** Reconstruction of the extracted watermark – the reconstruction of the extracted watermark is done using the reverse complex Hadamard transformation.

- **Step 5:** Estimating if the acquired watermark is valid – estimates if there were attacks agents the integrity of the watermark.

3. Experimental Results

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

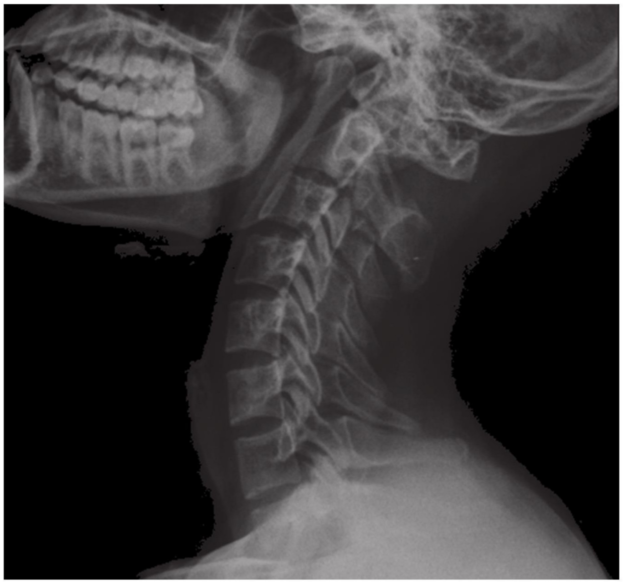


Figure 1. (*a*) Input X-ray test image “Spine 1”

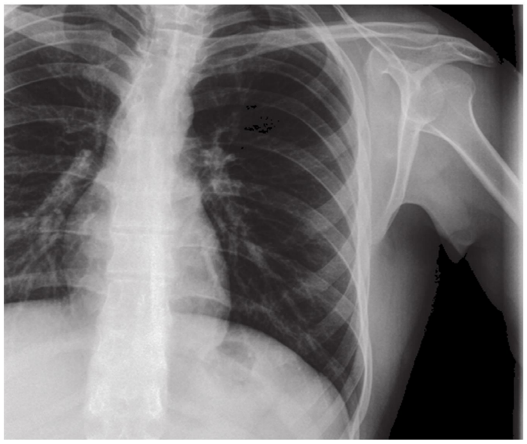


Figure 1. (*b*) Input X-ray test image “Spine 2”

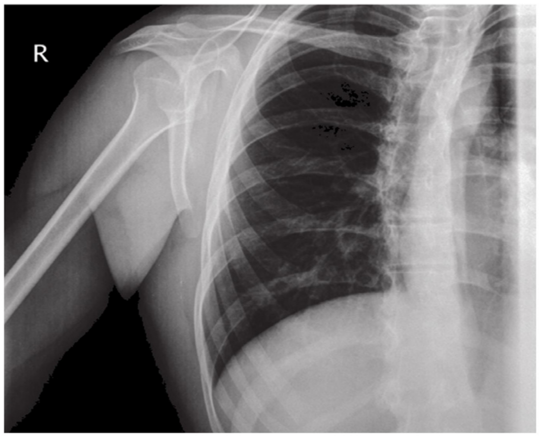


Figure 1. (*c*) Input X-ray test image “Spine 3”

These images are transformed by the 2D CHT with kernel 32x32. By this way the input image is divided on 256 subimages with size 32x32, the input watermark (letter K) is embedded into the phase spectrum of some sub-images and the algorithm is simulated by the developed MATLAB program.

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.

Test Images	**“Spine 1”**	**“Spine 2”**	**“Spine 3”**
Reconstructed Watermarked image			
SNR, dB	83.06	84.51	83.57
PSNR, dB	93.07	89.95	89.13
MSE	3.20E-	05 6.58E-05	7.95E-05
NMSE	4.94E-	09 3.54E-09	4.39E-09
NMSE, %	4.94E-	07 3.54E-07	4.39E-07
NC	0.76	0.89	0.87
NC, %	75.66	89.21	86.89

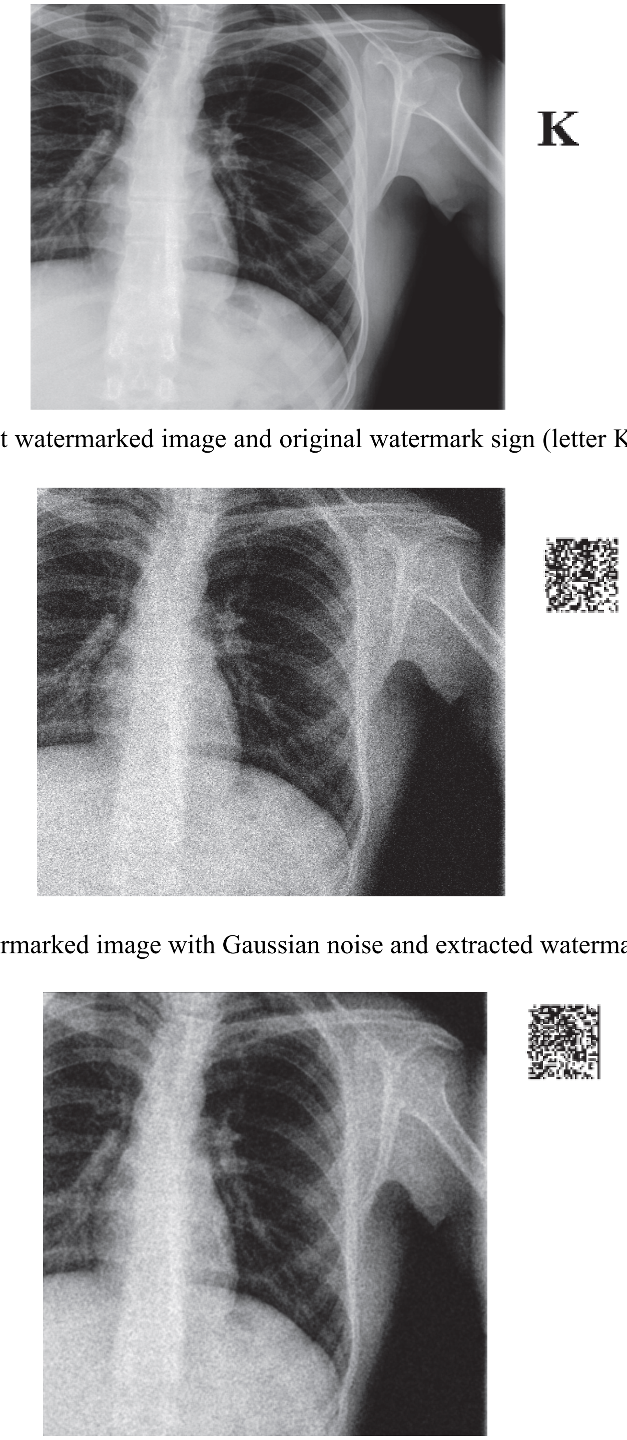
Watermarked image with Gaussian noise			
SNR, dB	10.96	14.97	14.96
PSNR, dB	20.98	20.40	20.51
MSE	5.19E+02	5.93E+02	5.78E+02
NMSE	8.01E-02	3.18E-02	3.19E-02
NMSE, %	8.01E+00	3.18E+00	3.19E+00
NC	0.67	0.63	0.63
NC, %	66.99	62.54	62.67
Watermarked image with Salt and Pepper noise			
SNR, dB	7.32	12.34	12.29
PSNR, dB	17.33	17.78	17.84
MSE	1.20E+03	1.09E+03	1.07E+03
NMSE	1.85E-01	5.83E-02	5.90E-02
NMSE, %	1.85E+01	5.83E+00	5.90E+00
NC	0.65	0.59	0.58
NC, %	64.89	58.92	58.2
Watermarked image with median filtration			
SNR, dB	33.31	35.20	34.76
PSNR, dB	43.33	40.64	40.31
MSE	3.02E+00	5.62E+00	6.05E+00
NMSE	4.66E-04	3.02E-04	3.34E-04
NMSE, %	4.66E-02	3.02E-02	3.34E-02
NC	0.51	0.58	0.57
NC, %	51.19	58.35	57.22
Watermarked image with Salt and Pepper noise and median filtration			
SNR, dB	32.15	33.80	33.46
PSNR, dB	42.16	39.24	39.01
MSE	3.95E+00	7.75E+00	8.17E+00
NMSE	6.10E-04	4.17E-04	4.51E-04
NMSE, %	6.10E-02	4.17E-02	4.51E-02
NC	0.51	0.58	0.57
NC, %	50.56	57.95	56.59
Watermarked image with Gaussian noise and average filtration			
SNR, dB	18.16	22.62	22.37
PSNR, dB	28.17	28.05	27.92
MSE	9.91E+01	1.02E+02	1.05E+02
NMSE	1.53E-02	5.50E-03	5.80E-01
NMSE, %	1.53E+00	5.50E-01	5.80E+01
NC	0.69	0.63	0.64
NC, %	68.74	63.08	64.36

Table 1

To estimating the efficiency of the presented algorithm 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.

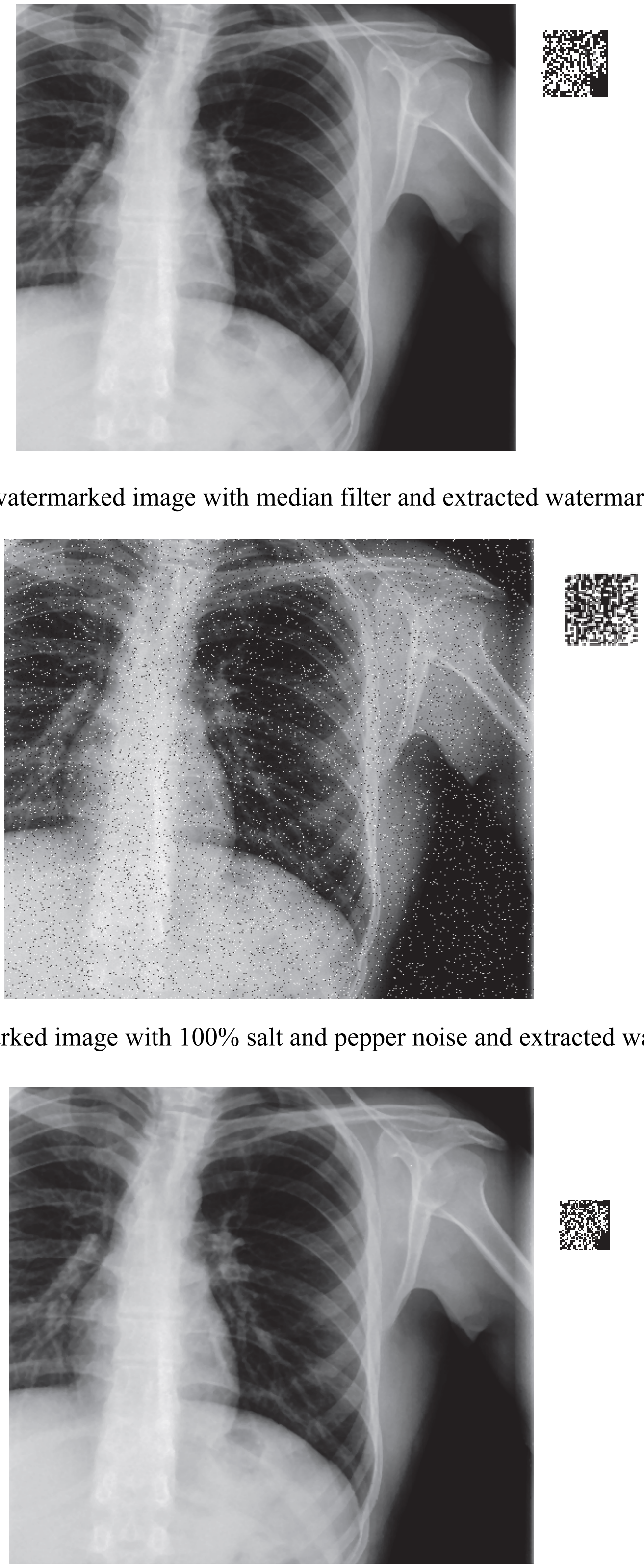
The obtained results for the test images are summarized in Table 1.



(*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

Figure 2. Results for watermarked image “Spine 2” with different post processing attacks

In Figure 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.

4. Conclusion

An algorithm for digital watermarking of medical images using complex Hadamard transform is presented. 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. They show that the developed algorithm allows high detection of unauthorized access or attacks on the included watermark. On the other hand the embedded watermark is practically invisible for the doctors and retains largely the information in the original images. All this leads to the conclusion that the developed algorithm for watermarking can be used successfully for watermark protection of medical data.

Acknowledgement

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

References

[1] Koushik, P., Ghosh, G., Bhattacharya. M. (2012). 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, 2(2), p 29-37.

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

[3] Siau-Chuin, L., Zain, J. M. (2010). Reversible Medical Image Watermarking for Tamper Detection and Recovery, 3*rd IEEE* International Conference on Computer Science and Information *Technology*, 2010, vol. 5, p 417-420.

[4] Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T. (2007). *Digital Watermarking and Steganography*, 2nd Edition, Elsevier, Burlington, 2007.

[5] Coatrieux, G., Maitre, H., Sankur, B., Rolland, Y., Collorec, R. (2000). Relevance of Watermarking in Medical Imaging, IEEE EMBS International Conference on Information *Technology Applications in Biomedicine*, 2000, p 250–255.

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

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

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

[9] Mironov, R., Kountchev, R. (2006). Analysis of Complex Hadamard Transform Properties, *XLI International Scientific* Conference on Information, Communication and Energy *Systems and Technologies*, *ICEST 2006*, 26 June - 1, July, Sofia, Bulgaria, 2006, p 173-176.

[10] Falkowski, B., Rahardja, S. (2004). Complex Hadamard Transforms: Properties, Relations and Architecture, *IEICE Trans. Fundamentals*, vol. E87-A (8), August 2004.