# Simulation Model Medical Images Watermarking using Complex Hadamard Transform

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

***Abstract* – A simulation model of algorithm for digital watermarking of medical images using complex Hadamard transform is presented. The model is implemented on a signal processor TMS 320C6713 and its experiments indicate it can be used in real-time systems. The developed algorithm for watermarking allow high detection of unauthorized access or attacks on the included watermark. 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, Complex Hadamard Transform, Unitary Transforms, Matlab Simulation.**

## 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.

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].

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 [8].

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.

In the class of transparent watermarks they may be further categorize techniques as robust or fragile. A robust mark is designed to resist attacks that attempt to remove or destroy the mark. Such attacks include lossy compression, filtering, and geometric scaling. A fragile mark is designed to detect slight changes to the watermarked image with high probability. The main application of fragile watermarks is in content authentication. Most of the work, as reported in the literature, in watermarking is in the area of robust techniques [4], [8], [9]. Many important applications could benefit from the use of fragile watermarks [10]-[15].

A fragile watermark is a mark that is readily altered or destroyed when the host image is modified through a different image transformation techniques. Fragile marks are not suited for enforcing copyright ownership of digital images - an attacker would attempt to destroy the embedded mark and fragile marks are, by definition, easily destroyed. The sensitivity of fragile marks to modification leads to their use in image authentication [10].

The fragile watermarking techniques in spatial domain mainly include manipulation of the LSB by different methods – vector quantization, chaos theory and etc. [11].

Frequency domain techniques have proved to be more effective than spatial domain techniques in achieving high robustness against attacks and can embed more bits of

[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

watermark. Commonly used frequency domain transforms are Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Discrete Fourier transform (DFT) and genetic algorithms [12], [13], [14].

The idea to use the Complex Hadamard transformation for watermarking was first presented by Mironov and Kunchev in [16] and is further developed for still images and video sequences in a number of subsequent publications. In the present work a simulation model of developed by the authors' simulation model for digital watermarking of medical images using Complex Hadamard Transform (CHT) is described [15].

The developed model 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 with median filters and average filters. The developed on the MATLAB Simulink simulation model is experimented by the personal computer with 3.2GHz Core-i5 processor and specialized signal processor board - TMS 320C6713 DSK.

## II. Simulation Model Description

The common results and properties, obtained from the one dimensional Complex Hadamard Transform (CHT) [16], 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:

$$\begin{cases} [Y] = [CH_N][X][CH_N] \\ [X] = \dfrac{1}{N^2}[CH_N][Y][CH_N] \end{cases} \quad (1)$$

The Hadamard transformation is simple for implementation, 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 properties of complex Hadamard transform matrices and its applications in digital image processing are described in detail in article [16].

The algorithms on which are based the developed models for embedding and extraction of watermark are described in article [15]. The principal block scheme of simulation model, representing the embedding of the watermark, developed using MATLAB Simulink environment is presented in Fig.1.

The presented model was developed basically with standard modules from the Simulink library, which allows it to be used in the implementation on a signal processor boards of the TMS family. The difference is only in the blocks where the complex transformations are performed because they do not exist in existing Simulink implementations. The most important blocks are:

- Subsystem "*Embedding*";
- Subsystem "*Marking*";
- Subsystem "*F/M Matrix*";
- Subsystem "*Watermarking*".

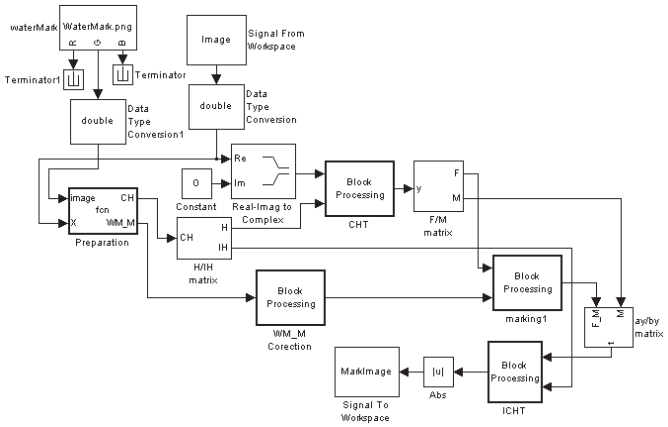


Fig.1. Simulation model, representing the embedding of the watermark using CHT

In the Subsystem "*Embedding*", shown in Fig.2, the input image and the sign image (in subblock "*Preparation*") are preparing for watermarking.

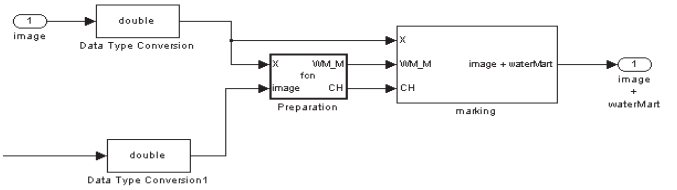


Fig.2. Simulation Subsystem "*Embedding*"

In the Subsystem "*Marking*" show in Fig. 3, the watermarking process is executed.

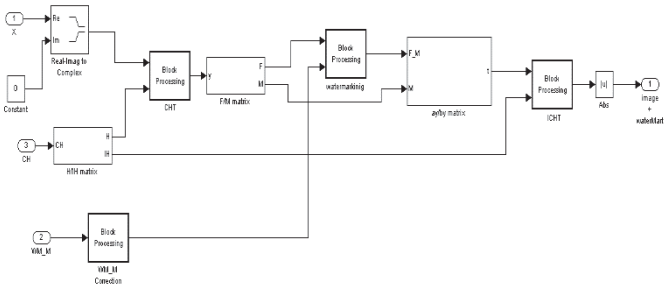


Fig.3. Simulation Subsystem "*Marking*"

The "*H/IH*" subsystem specifies direct Complex Hadamard Matrix and its inverse matrix for the input image. The "*F/M Matrix*" matrix subsystem (shown in Fig.4) defines complex and real parts of amplitude-frequency and phase-frequency components on the base of equations, described in [15].

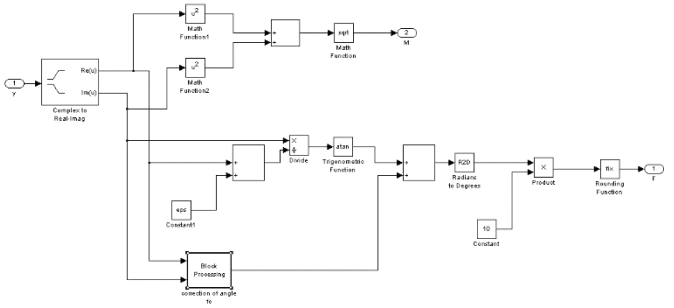


Fig.4. Simulation Subsystem "*F/M Matrix*"

Through the "*WM_M Correction*" block, watermark coefficients are limited to marker block coefficients in order to avoid oversaturation. The "*Watermarking*" subsystem adds the resulting watermark to the converted input image.

In the subblocks "*CHT*" and "*ICHT*", the direct and inverse complex Hadamard matrices are created respectively based on the examinations made in [16].

The principal block scheme of simulation model, representing the extraction of the watermark is developed using MATLAB Simulink environment and is presented in Fig.5.

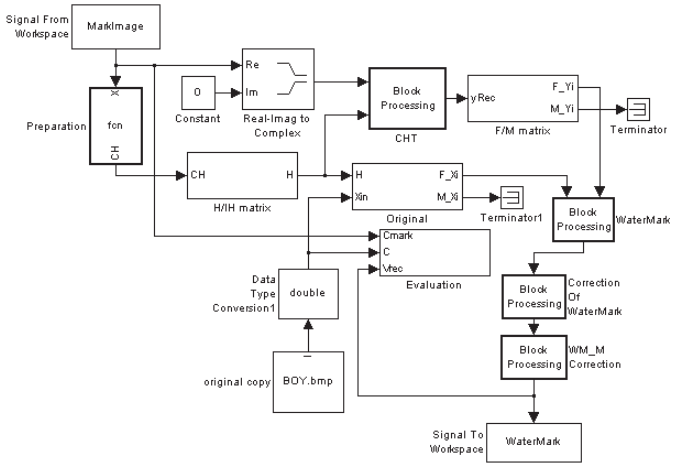


Fig.5. Simulation model representing the extraction of the watermark using ICHT

The marked image is loaded from the workspace using the subblock "*Signal from Workspace*". In the subblock "*Preparation*" the preparation of the complex matrix of Hadamard is carried out. In the Subsystem "*Extracting*", show in Fig. 6, the extraction of watermark is done.

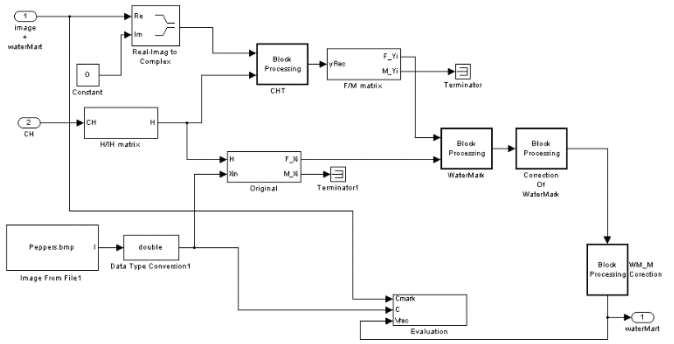


Fig.6. Simulation model of Subsystem "Extracting"

The "*H/IH*" subsystem specifies direct Complex Hadamard Matrix and its inverse matrix for the input image. The "*CHT*" subsystem performs a complete complex transformation of Hadamard onto the tagged image. The "*F/M Matrix*" matrix subsystem (shown in Fig.4) defines complex and real parts of amplitude-frequency and phase-frequency components on the base of equations, described in [15].

The Subsystem "*Original*" performs the functions of "*CHT*" and "*F/M Matrix*" blocks, but applied to a copy of the original image. The "*Water Mark*" subblock performs the extraction of the watermarked image. The "*Correction of Water Mark*" and "*WM_Correction*" subblocks make a retrograde correction of the watermark coefficients that stopped the coder. The "Evaluation" subsystem calculates the SNR, PSNR, MSE, NMSE and normalized cross-correlation metrics.

## III. Experimental Results

For the analyses of efficiency of the developed model for watermarking of medical images three test images, shown in Fig.7a, b, c, with size 512x512 and 256 gray levels are used.

Fig.7a. Input X-ray test image "Spine 1".

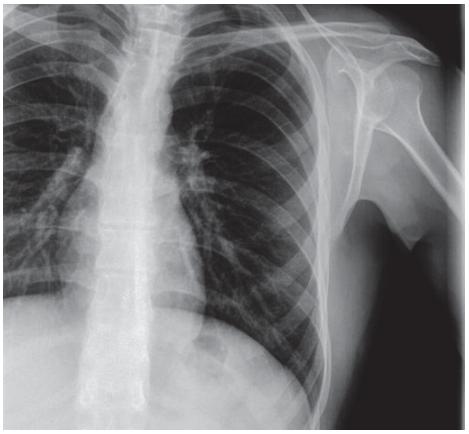

Fig.7b. Input X-ray test image "Spine 2".

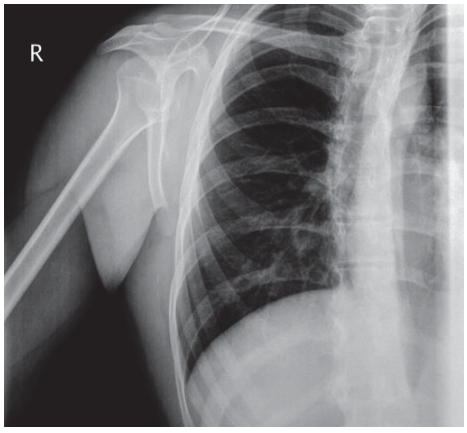


Fig.7c. Input X-ray test image "Spine 3".

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

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.

To estimating the efficiency of the presented simulation model 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 results obtained from the tests shows that the efficiency of the developed on Matlab Simulink environment model with regard to watermark quality, its invisibility to the user and its resistance to some of the most commonly used attacks is the same as the program implementation developed by the authors and shown in [15]. There are no differences between the results obtained through program simulation and simulation made with Simulink.

This is due to the fact that in modules using complex Hadamard transform are included software blocks (Math blocks) as there are no standard blocks for this transform in Matlab Simulink Blockset.

The developed in the MATLAB Simulink environment model was tested on a personal computer with 3.2GHz Core-i5 processor and on a specialized signal processor board - TMS 320C6713 DSK.

The results, obtained from the simulation of Matlab, show that time coding for different images varies between 3.1 and 3.36 seconds. The decoding process is about 1.93 seconds.. Simulation on the signal processor TMS 320C6713 takes place over a real time scale, requiring about one second to load and prepare each image individually.

## IV. Conclusion

A simulation model 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, signal to noise ratio and normalized cross-correlation of the reconstructed images. They show that the developed model 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. This will allow to a great extent to verify the reliability of the medical data transmitted and recorded as images.

Experimental results obtained from the simulation of signal processor TMS 320C6713 show that the developed model can be implemented and hardware used in systems for the protection of medical imaging systems against unauthorized access in real time.

All this leads to the conclusion that the developed models for watermarking can be used successfully for watermark protection of medical data.

## V. 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] Neha Singh, Mamta Jain, Sunil Sharma, “A Survey of Digital Watermarking Techniques”, *International Journal of Modern Communication Technologies & Research*, August 2013.

[9] 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.

[10] S. Radharani, M. L. Valarmathi . “A study of watermarking scheme for image authentication”. *International Journal of Computer Applications*, 2010, Vol. 2, No.4, pp. 24-32.

[11] Pragya Jain, Anand S. Rajawat. “Fragile Watermarking for Image Authentication: Survey”. *International Journal of Electronics and Computer Science Engineering (IJECSE)*, pp. 1232-1237. ISSN 2277-1956.

[12] Huang-Chi Chen, Yu-Wen Chang, Rey-Chue Hwang. “A Watermarking Technique based on the Frequency Domain”, *Journal of Multimedia*, 2012, Vol. 7, No. 1, pp. 82-89.

[13] A. Kannammal, K. Pavithra, S. Subha Rani. “Double Watermarking of Dicom Medical Images using Wavelet Decomposition Technique”. *European Journal of Scientific Research*, 2012, Vol. 70, No. 1, pp. 46-55.

[14] K. Sreenivas, V. Kamkshi Prasad. “Fragile watermarking schemes for image authentication: a survey”. *International Journal of Machine Learning and Cybernetics*, July 2018, Volume 9, Issue 7, pp 1193–1218.

[15] R. Mironov, St. Kushlev. “Medical Images Watermarking using Complex Hadamard Transform”. *LII International Scientific Conference Information, Communication and Energy Systems and Technologies (ICEST’2017)*, June 28-30 2017, Niš, Serbia, Proc. of ICEST'2017, pp.52-55. ISSN: 2603-3259 (Print), ISSN: 2603-3267 (Online).

[16] R. Kountchev, R. Mironov. Audio Watermarking in the Phase-Frequency Domain. *XXXIX International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST 2004)*, Bitola, Macedonia, June 16-19, 2004, pp.123-126. ISBN: 9989-786-38-0.