

## DIGITAL WATERMARKING OF 3D MEDICAL VISUAL OBJECTS

M. N. Favorskaya<sup>1,\*</sup>, E. I. Savchina<sup>1</sup>

<sup>1</sup> Reshetnev Siberian State University of Science and Technology, Institute of Informatics and Telecommunications, 31, Krasnoyarsky Rabochy ave., Krasnoyarsk, 660037 Russian Federation - favorskaya@sibsau.ru, ms.oreshkina@inbox.ru

Commission II, WG II/10

**KEY WORDS:** Digital Watermarking, 3D Medical Object, Digital Wavelet Transform, Digital Hadamard Transform

### ABSTRACT:

At present, medical equipment provides often 3D models of scanning organs instead of ordinary 2D images. This concept is supported by Digital Imaging and COmmunications in Medicine (DICOM) standard available for telemedicine. This means that the confidential information under transmission ought to be protected by special techniques, particularly digital watermarking scheme instead of textual informative files represented, for example, on CD disks. We propose a multilevel protection, for which a fragile watermark is the first level of protection. The Region Of Interest (ROI) watermark and textual watermarks with information about patient and study (the last ones can be combined as a single textual watermark) form the second level of protection. Encryption of the ROI and textual watermarks using Arnold's transform is the third level of protection. In the case of 3D models, we find the ROI in each of 2D sliced images, apply the digital wavelet transform or digital shearlet transform (depending on the volume of watermarks) for the ROI and textual watermarks embedding, and embed a fragile watermark using digital Hadamard transform. The main task is to find the relevant regions for embedding. To this end, we develop the original algorithm for selecting relevant regions. The obtained results confirm the robustness of our approach for rotation, scaling, translation, and JPEG attacks.

### 1. INTRODUCTION

Enhancement of digital processing methods and telecommunication networks led to use medical data in a digit format. On the one hand, representation, storage, and distribution of digital content are simplified but, on the other hand, these advances facilitate to simplicity of data destruction. Digital watermarking as one of the popular ways for protection of digital multidimensional content is rapidly developed. Recently, 3D medical images are becoming increasingly important in healthcare environment that causes a study of their protection by novel watermarking approaches. However, watermarking of 3D models is a weekly investigated scope with the impressive restricts respect to the ordinary watermarking of 1D and 2D data. Often 3D models are 3D polygonal mesh models with the following challenges:

1. A number of vertexes in 3D mesh model is around a few thousand points, while an image has a resolution in several million pixels. Thus, a capacity for embedding in 3D mesh models is low.
2. A grid of vertexes in 3D mesh model is not regular as a regular grid of pixels for 2D data. Thus, an explicit ordering of data representing by vertexes, edges, and polygonal surfaces does not exist.
3. Any conventional transform of 3D mesh model is not invariant to possible geometrical or topological changes of 3D model. This means that robustness to attacks is low.
4. The local areas for embedding imply that any conventional transform used for embedding cannot be robust to the geometrical and topological attacks.
5. It is enough easy to distort 3D mesh model by complex geometrical or topological transforms.

It should be noted that the Internet attacks aiming to destroy or remove a watermark in 3D mesh model are principally different

from the geometrical and common image processing attacks for audio, image, or video data. Such specific attacks can be the following ones: mesh simplification in order to change the coordinates of vertex, mesh smoothing by deleting high-frequency components of the model, re-triangulation using another sampling mesh, vertex randomization, topology changing of the triangular mesh, adding noise into the coordinates of vertexes, and local deformation of 3D model. Note that the most complex geometrical attacks (for any dimension of data) include shearing, non-uniform scaling along arbitrary axes, projections, and global deformations (e.g. twisting or bending). Such distortions break down visual quality and usability of the watermarked image.

Nowadays, the robust watermarking schemes for 3D mesh models do not invented, and this task comes down to watermarking of 2D images. Fortunately, another representation of 3D medical models is available, viz. slicing representation. Thus, a radiological 3D model of jaw aiming a dental supervision provides a set of sliced images in DICOM format (files with extension .dcm).

The rest of this paper is organized as follows. Section 2 briefly reviews the related work. Section 3 describes a procedure for creation of watermarks respect to levels of protection. Selecting regions for embedding is discussed in Section 4. Embedding and extraction schemes are reported in Section 5. Finally experimental results and conclusions are given in Sections 6 and 7, respectively.

### 2. RELATED WORK

The first investigations in watermarking schemes of 3D triangular mesh models can be referred to 2000s (Yu et al., 2003). This approach embedded a watermark by perturbing the distance from a vertex to the center in each section by weighing

scheme with respect to the local geometry of the model. The authors claimed that this approach was invariant to common attacks on 3D models (mesh simplification, addition of noise, model cropping, as well as their combinations). The great majority of encryption protocols are based on optical encryption methods, such as digital holography, diffractive imaging, integral imaging, multiple cameras, and detector photogrammetry (Muniraj et al., 2014; Mehra et al., 2015; Jiao et al., 2019). In spite of optical encryption methods have some advantages, such as parallel processing and data handling in various domains, these algorithms are difficult in efficient software implementation.

The robust and blind mesh watermarking based on the geometric volume moments as the watermarking primitive was represented in (Wang et al., 2011). Then, the normalized mesh was decomposed into patches and the watermark was embedded through a quantization of the zero-order volume moments of selected candidate patches. Fuzzy C-means clustering technique for selection vertices in 3D mesh model was adopted in (El Zein et al., 2017). These authors claimed that their watermarked 3D mesh models were resistant to several attacks (similarity transforms, noise addition, cropping, and mesh smoothing). Zhang et al. (Zhang et al., 2019) proposed reversible data hiding method for 3D mesh models based on prediction-error expansion and smooth sorting. Instead of partial prediction, they used a ring prediction context in the neighbour vertices respect to central vertex. The smooth cells obtained a top priority for data embedding. The vertices, candidate and reference, may be changed for increasing embedding capacity. Encryption protocol for 3D biomedical objects consisting of two phases was developed in (del Rey et al., 2016). In the confusion phase, the voxels' positions are permuted by discretized chaotic map, whereas in the diffusion phase, the value of each voxel using cellular automaton was changed.

A security enhanced DICOM image sharing through the local area network had been proposed in (Arumugham et al., 2018). Details of patient history and QR code of patient ID were encrypted by chaotic maps and Lorenz attractor with good level of confidentiality. The encrypted patient details were embedded in Region Of Non-Interest (RONI) region of the DICOM images applying Digital Wavelet Transform (DWT). Transmission of the DICOM images used three-layer authentication: username – password, face recognition and one time password confirmation. The authors allowed storage of the DICOM images in cloud environment.

Fragile reversible watermarking scheme for digital radiographic images was suggested in (Pan et al., 2018). The originality is in that a fragile watermark is represented as an image quantum noise, the dominant noise in radiographic images. Fragile watermark is embedded into RONI, black background, using the well-known histogram shifting modulation applied to wavelet coefficients.

Scrambling is one of the best techniques to decorrelate the watermarked image. For this purpose, the chaotic-based methods, among which Arnold's transform (Arnold and Avez, 1968), 2D logistic maps (Chai et al., 2017), chaotic Baker map (Chen et al., 2014), 3D Lorentz chaotic system (Saini et al., 2017), are successfully applied.

### 3. CREATION OF WATERMARKS

Section 3.1 includes a procedure of forming textual watermarks. Section 3.2 presents an automatic method of ROI watermarks segmentation in a set of 2D sliced images. Application of Arnold's transform is discussed in Section 3.3.

#### 3.1 Textual watermarks

The DICOM information model (DICOM, 2018) involves around 4,600 reserved data elements. However, four entities mentioned below are very important. Among them, there are entity "Patient" (with attributes *PatientID*, *PatientName*, *PatientBirthDay*, *PatientSex*, *PatientAge*, *PatientBodyMassIndex*, *PatientWeight*, and *PatientAddress*), entity "Study" (with attributes *StudyIDIssuer*, *StudyDate*, *StudyTime*, *ReferringPhysicianName*, *ReferringPhysicianAddress*), entity "Series" (with attributes *SeriesID*, *SeriesDate*, *SeriesTime*, *EquipmentModality*, *ManufacturerModelName*), and entity "Image" (with attributes *ImageNumber* and *ImageType*). Let us group the attributes associating them with two textual watermarks: information about patient  $WM_{PT}$  so called Electronic Patient Record (EPR) and information about study  $WM_{ST}$ : provided by equations 1 and 2:

$$WM_{PT} = \{PatientID, PatientName, PatientBirthDate, PatientSex, PatientAge, PatientBodyMassIndex, PatientWeight, PatientAddress\} \quad (1)$$

$$WM_{ST} = \{StudyIDIssuer, StudyDate, StudyTime, ReferringPhysicianName, ReferringPhysicianAddress, SeriesID, SeriesDate, SeriesTime, EquipmentModality, ManufacturerModelName, ImageNumber, ImageType\} \quad (2)$$

Note that for simplicity we join the watermarks  $WM_{PT}$  and  $WM_{ST}$  as one textual watermark.

#### 3.2 ROI watermark

Also expert ought to mention ROI for its embedding in one 2D slice aiming a protection from internet attacks. The ROI in other slices are detected automatically. This watermark  $WM_{ROI-3D}$  is a set of watermarks in each slice  $WM_{ROI_i}$  provided by equation 3:

$$WM_{ROI-3D} = \{I_{ROI_i}\}, i=1\dots N \quad (3)$$

where  $N$  = number of slices

The watermark  $WM_{ROI_i}$  is a set of pixels defined by equation 4:

$$WM_{ROI_i} = \{SubjectRelativePositionInImage\} \quad (4)$$

Also we create a fragile watermark  $WM_{FR}$  in order to understand the internet attacks happened or not. A fragile watermark has a property to be destroyed under any type of attack. A fragile watermark contains visible or invisible small popular image, logotype, or message:

$$WM_{FR} = \{SetOfLogoPixels\} \quad (5)$$

During embedding and extraction, additional task respect to automatic segmentation of ROI<sub>i</sub>,  $i \in 1, \dots, n$ , in each of  $i$ th slice appears. An automatic segmentation is executed using the energy model based on the method of Local and Global Intensity Fitting (LGIF) (Wang et al., 2009) with the following Bregman iterative procedure (Goldstein and Osher, 2009). Energy model LGIF joins the advantages of Chan and Vese (CV) model (Vese and Chan, 2002) and Local Binary Fitting (LBF) model (Li et al., 2007). Let  $\Omega \subset \Re^2$  be an image and  $u_0 : \Omega \rightarrow \Re$  be a given gray level. The CV model does not use information about gradients; it searches such gray level  $u_0$ , which approximate the intensities inside and outside respect to contour  $C$  with accuracy to constants  $c_1$  and  $c_2$ . Energy  $F_{CV}(\cdot)$  is minimized using equation 6:

$$\begin{aligned} F_{CV}(C, c_1, c_2) = & \lambda_1 \int_{in(C)} |u_0(\mathbf{x}) - c_1|^2 d\mathbf{x} \\ & + \lambda_2 \int_{out(C)} |u_0(\mathbf{x}) - c_2|^2 d\mathbf{x} + v|C| \end{aligned} \quad (6)$$

where  $in(C)$  = the inside regions respect to contour  $C$   
 $out(C)$  = the outside regions respect to contour  $C$   
 $|C|$  = the length of contour  
 $\lambda_1, \lambda_2$ , and  $v$  = the positive constants

The LBF model has a view of equation 7:

$$\begin{aligned} F_{LBF}(C, f_1, f_2) = & \lambda_1 \int \left[ \int_{in(C)} K_\sigma(\mathbf{x} - \mathbf{y}) |I(y) - f_1(\mathbf{x})|^2 dy \right] d\mathbf{x} \\ & + \lambda_2 \int \left[ \int_{out(C)} K_\sigma(\mathbf{x} - \mathbf{y}) |I(y) - f_2(\mathbf{x})|^2 dy \right] d\mathbf{x} \\ & + v|C| \end{aligned} \quad (7)$$

where  $K_\sigma$  = a kernel function, usually Gaussian kernel  
 $f_1(\mathbf{x})$  and  $f_2(\mathbf{x})$  = two functions that fit image intensities near the point  $\mathbf{x}$

Then, the LGIF model is defined by equation 8 (Wang et al., 2009):

$$\begin{aligned} F_{LGIF}(\phi, f_1, f_2, c_1, c_2) = & \omega F_{GIF}(\phi, c_1, c_2) \\ & + (1 - \omega) F_{LBF}(\phi, f_1, f_2) \end{aligned} \quad (8)$$

where  $F_{GIF}$  = the transformed CV model  
 $F_{LBF}$  = the transformed LBF model  
 $\omega$  = a positive constant,  $0 \leq \omega \leq 1$

The LGIF model segments an image more accurate than the CV and the LBF models. However, it is enough difficult to find a value of positive constant  $\omega$  in order to balance two models. We can improve the obtained results using split Bregman method, which is formulated as L2-regularization:

$$\min_{u,d} |\vec{d}|_1 + H(u) + \frac{\lambda}{2} \|\vec{d} - \Phi(u)\|^2 \quad (9)$$

where  $H(u)$  and  $\Phi(u)$  = the convex functionals  
 $d = E(u, d) - H(u)$   
 $E(u, d)$  = the energy function

$\lambda$  = the positive constant  
 $\|\cdot\|_2$  = the L2-norm

Bregman iterative procedure is calculated using equations 10–11:

$$\begin{aligned} (\bar{u}^{k+1}, \bar{d}^{k+1}) = & \arg \min_{u,d} \left( |\vec{d}|_1 + H(u) \right. \\ & \left. + \frac{\lambda}{2} \|\vec{d} - \Phi(u) - b^k\|^2 \right) \end{aligned} \quad (10)$$

$$b^{k+1} = b^k + (\Phi(\bar{u}^{k+1}) - \bar{d}^{k+1}) \quad (11)$$

where  $\bar{u}^{k+1}$  = a solution at step  $k + 1$   
 $b^k$  = additional variable at step  $k$

The iterative procedure converges under  $k \rightarrow \infty$ ,  $\|\vec{d} - \Phi(u)\| \rightarrow 0$ ,  $\|\bar{u}^{k+1} - u^*\| \rightarrow 0$ , where  $u^*$  is some solution. Thus, Bregman procedure guarantees the efficient segmentation of convex visual objects.

### 3.3 Application of Arnold's transform

The Arnold's transform refers to the chaotic transforms (Arnold and Avez, 1968). It is successfully applied as a technique to scramble a watermark in order to increase the robustness against the cropping attacks. This transform disorders a watermark matrix and makes a watermark obscured. The 2D Arnold's transform has a view of equation 11:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\text{mod } N_w) \quad (11)$$

where  $(x, y)$  = the pixel's coordinates of the original watermark

$(x', y')$  = the pixel's coordinates of the scrambled watermark

$p, q$  = the coefficients of transform

$N_w \times N_w$  = the sizes of a watermark (values of the width and length ought to be equaled)

In practice, equation 11 is replaced by simplified version, so called the Arnold's cat map:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\text{mod } N_w) \quad (12)$$

The transformation includes three steps during the one iteration:

- Shear in the OX direction by a factor of 1
- Shear in the OY direction by a factor of 1
- Evaluate the modulo

The Arnold's transform is a periodic and invertible mapping. A full number of iterations that leads to appearing the original image is known as the Arnold's period. At the same time, a chosen number of iterations provides a secret key. During decryption, if a scrambled image is iterated enough times (the Arnold's period minus value of secret key), then the original image will be reconstructed successfully. For color watermarks, the YCbCr color space (Y is a luminance, Cb and Cr are chrominance components) is recommended. In this case, only

Y-channel is processed by the Arnold's transform. The scrambling procedure can be complicated by the multi-regional scrambled (with different parameters) parts of a watermark.

#### 4. SELECTING REGIONS FOR EMBEDDING

The radiological medical image includes the gray textural and black areas on the borders. If we embed all types of watermarks distributed in an image uniformly, we may obtain a noisy watermarked image. In general, three factors influence on embedding quality, viz. imperceptibility, robustness, and capacity, which conflict with each other. Imperceptibility means the minimum errors during embedding. Robustness is a capability to resist different types of attacks. Capacity refers to the total number of bits embedded in the host image. To satisfy these requirements, we ought to select carefully regions for embedding and corresponding type of transform for embedding. Note that automatic segmentation of ROI in each slice allows us to set the sizes of ROI watermark in a view of rectangle.

The strategy is such that a fragile watermark is embedded into a fixed small area of medical image. The remaining part of image is segmented into “black” (boundary) part and “gray-scale” (textural) part without ROI mentioned by expert. Textual watermarks are embedded into “black” part, while ROI is embedded into “gray-scale” part. Depending on the ROI volume, we use the DWT or more capacious due to larger number of coefficients Digital Shearlet Transform (DST). The bits of textual watermarks are uniformly embedded into coefficients of the DWT in “black” part of an image. The conducted experiments confirmed the proposed strategy for selecting regions for embedding.

#### 5. EMBEDDING AND EXTRACTION SCHEMES

For multilevel protection, four types of watermarks ought to be embedded in the host image. Among them, there are fragile watermark as the first level of protection, which shows any implemented distortion, two textual watermarks with information about patient and study, respectively, and visual watermark with ROI pointed by expert manually. We may consider a ROI visual watermark as the second level of protection. In the case with a set of 2D sliced images, first, we find the ROI in a given projection in each of sliced images related to 3D model of a single tooth, 3D models of several teeth, or 3D model of a whole jaw. Second, we apply a conventional watermarking algorithm for embedding the segmented ROI in textural regions of each sliced image (Favorskaya et al., 2018a). Third, the textual watermark with private information is embedded into the border regions mostly. In 2D sliced representation, a set of images is grouped as an archive file, and we may embed fragile watermark and textual watermark in any 2D image one time. However, this information can be duplicated due to a relatively huge amount of the sliced images. This means that the process of embedding/extraction of watermarks increased dramatically but the robustness for attacks is grown in times. Application of Arnold's transform, especially to the ROI and textural watermarks means the third level of protection.

The embedding scheme is the following. First, a host slice is divided into  $8 \times 8$  blocks. Each block is marked as a textural or black region forming two chains. The ROI and consistent area for a fragile watermark do not considered. The textural chain is applied for embedding of ROI watermark, while the black chain is used for embedding of the textual information with the EPR

and study information. Due to large volume of these watermarks, the DWT or the DST are utilized. Note that the DST is better than the DWT due to its invariant to translation and scaling attacks. A fragile watermark is a stable in sizes watermark, and we may use a simpler transform for embedding, i.e. the Digital Hadamard Transform (DHT) (Favorskaya et al., 2018b). The DHT allows to control a degree of fragile watermark visibility by tuning of a scale factor. Such separated areas for embedding lead to complexity of secrete key, which ought to contain the positions of fragile and ROI watermarks, as well as two chains with “black” and “gray-scale” blocks. The extraction scheme is ordinary except of necessity to select the corresponding blocks regarding different watermarks.

#### 6. EXPERIMENTAL RESULTS

The experimental results were conducted into two directions, viz. automatic segmentation of the ROI in a set of 2D sliced images and multilevel protection under typical attacks. Two ways for ROI detection, manual and automatic, are depicted in Figure 1. Figure 2 presents the automatic ROI detection in slices (through 15 slices for better visibility).

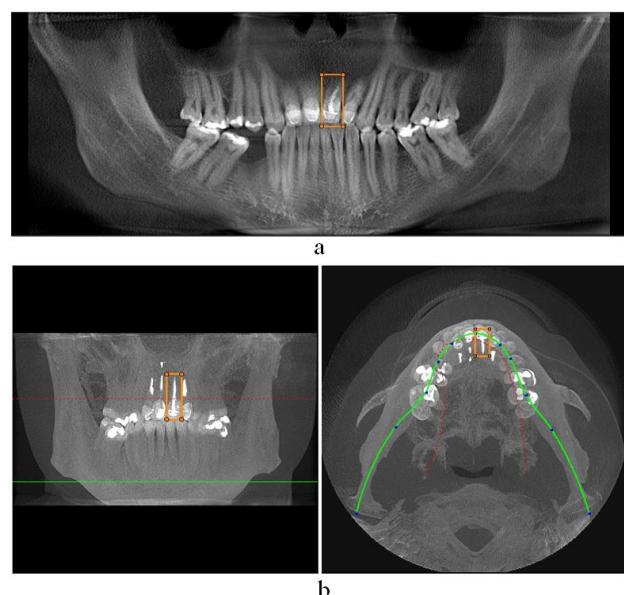


Figure 1. ROI detection: a manually by expert in panoramic image, b automatically based on the main projections

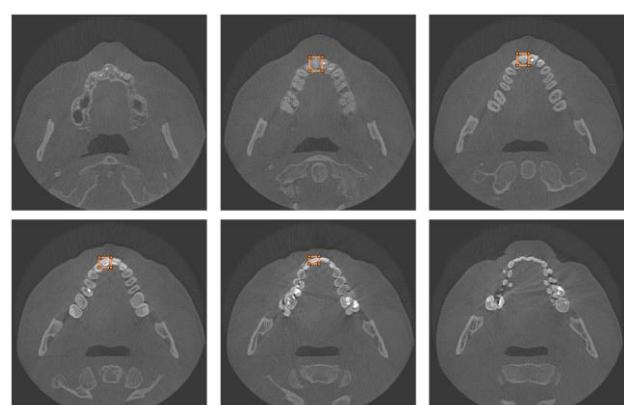


Figure 2. Automatic ROI detection in slices

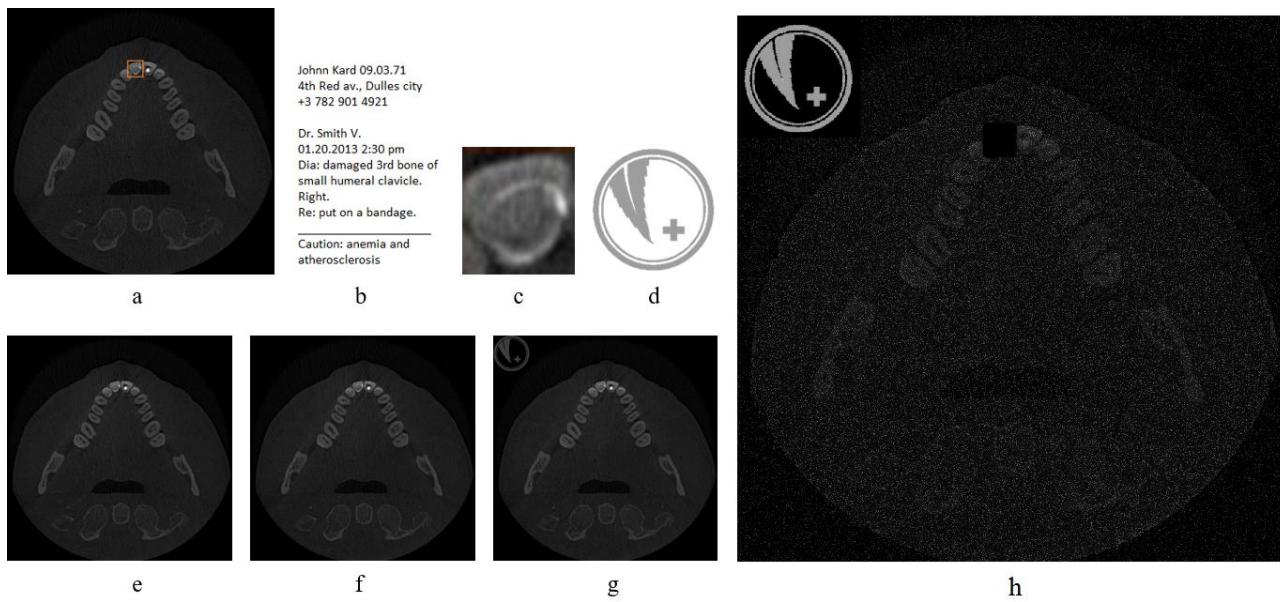


Figure 3. Initial data and visual examples of watermarking process: a original slice for embedding, b textual watermark, c ROI watermark (increased in 3 times), d fragile watermark, e watermarked slice after embedding of ROI watermark, f watermarked slice after embedding of ROI and textual watermarks, g watermarked slice after embedding of ROI, textual, and fragile watermarks, h increased difference map between original and watermarked images

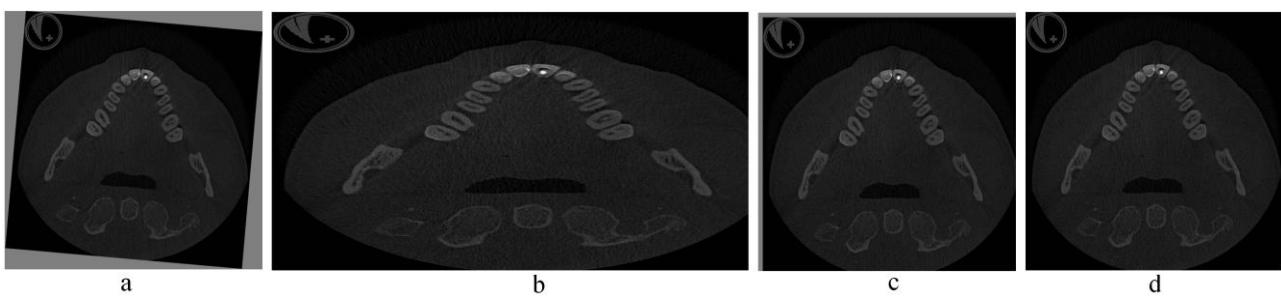


Figure 4. Examples of attacks: a rotation, b scaling, c translation, d JPEG

Visual example of multilevel protection is depicted in Figure 3. Original slice and three types of watermarks are represented in Figure 3a-3d. The main idea is a non-intersection between areas for embedding. It should be noted that the ROI and textural watermarks are tuned into Arnold's transform before embedding. First, we embed the ROI watermark into texture area except of ROI (Figure 3e). Second, we add textual watermark into black area of slice (Figure 3f). Third, fragile watermark is enclosed into the predefined area (Figure 3g). The increased difference map between original and watermarked images is depicted in Figure 3h. This procedure is implemented for each slice after extraction of ROI automatically as it is shown in Figure 2. The extraction process is executed in the inverse order. Fragile watermark shows the existence of attacks.

Possible types of attacks, which can be applied for some or all slices, are mostly directed on Rotation, Scaling, Translation (RST), and JPEG compression. Examples of attacks are depicted in Figure 4. During experiments, the watermarked slices were exposed to rotation, scaling, translation, and JPEG attacks. After that, a metric Bit Correct Ratio (BCR), which estimates the robustness to attacks, was calculated for the original and extracted watermarks according to equation 13:

$$BCR(x, y) = \frac{\sum_{x=1}^M \sum_{y=1}^N f(x, y) \oplus f'(x, y)}{M \times N} \quad (13)$$

where  $f(x, y)$  = values of functions at position  $(x, y)$   
 describing the original watermark

$f'(x, y)$  = values of functions at position  $(x, y)$   
 describing the extracted watermark

$\oplus$  = the Exclusive-OR operation

$M \times N$  = the sizes of watermark

We calculated the BCR values for the original and extracted watermarks for each type of attack. The BCR value (in percentages) ranges in [0...100], where values close to 100 means that the extracted watermark is similar with the original watermark and the robustness is high. Hereinafter, for each type of attack the corresponding diagram and table are provided.

First of all, the watermarked slices were distorted by clockwise rotation attacks on 3°, 5°, 8°, and 10°. The estimates are depicted in Figure 5 and Table 1.

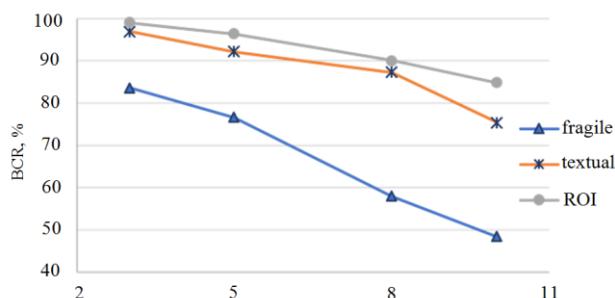


Figure 5. Watermark distortions under rotation attacks

Watermark	Degree, °			
	3	5	8	10
Fragile watermark	83.6	76.7	58.0	48.5
Textual watermark	96.9	92.2	87.3	75.4
ROI	99.1	96.4	90.1	84.8

Table 1. BCR estimates under rotation attacks

As it follows from Figure 5 and Table 1, the ROI watermark is the most robust regarding other watermarks. Only after rotation on 10°, a number of error bits exceeded 15%. At this time, a fragile watermark changed instantly on any rotation angle.

Then the watermarked slices were distorted by scaling attacks with ratios 0:2, 2:0, 2:2, and 0.5:1.5 (the first and second digits in ratio mean stretching and contraction factors, respectively). The estimates are depicted in Figure 6 and Table 2.

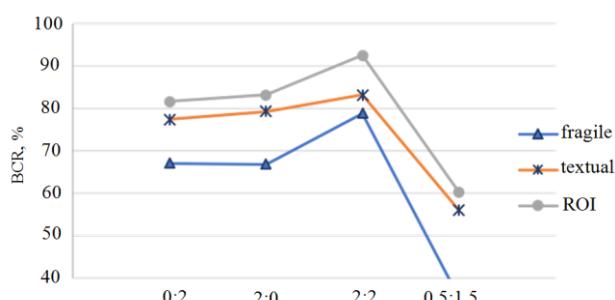


Figure 6. Watermark distortions under scaling attacks

Watermark	Scaling coefficients			
	0:2	2:0	2:2	0.5:1.5
Fragile watermark	67.1	66.8	78.8	35.3
Textual watermark	77.4	79.2	83.1	56
ROI	81.6	83.1	92.5	60.2

Table 2. BCR estimates under scaling attacks

This experiment demonstrates low values under non-proportional stretching and the lowest values under scaling with stretching and contraction simultaneously. The ROI watermark is the most robust to scaling attacks due to applied DWT/DST.

In the following experiment, the watermarked slices were distorted by translation attacks on 5, 10, 15, and 20 pixels. The estimates are depicted in Figure 7 and Table 3.

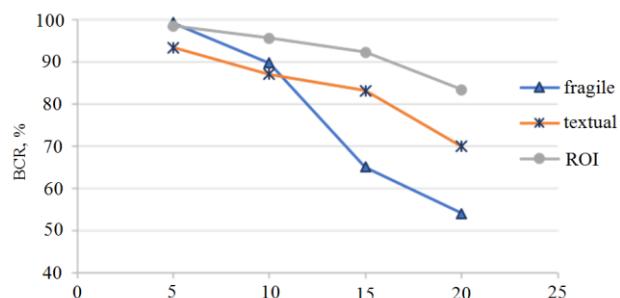


Figure 7. Watermark distortions under translation attacks

Watermark	Pixels			
	5	10	15	20
Fragile watermark	99.2	89.7	65.1	54.1
Textual watermark	93.3	87.0	83.1	69.9
ROI	98.4	95.5	92.2	83.3

Table 3. BCR estimates under translation attacks

This experiment differs by behavior of fragile watermark. Translation on 5 pixels influenced on its quality lesser than in other experiments. This fact is explained by location of fragile watermark: such non-significant translation does not capture an area of fragile watermark. Note that each slice has a resolution 776×776 pixels.

Lastly, the watermarked slices were distorted by JPEG attacks of watermarked slice. The estimates are depicted in Figure 8 and Table 4.

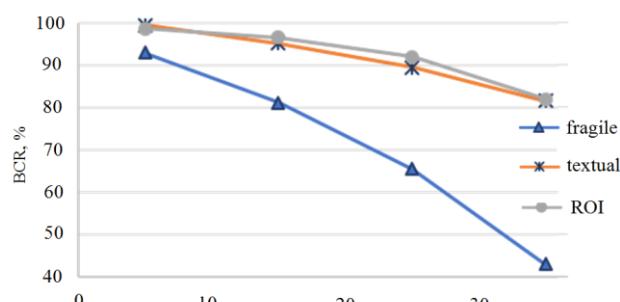


Figure 8. Watermark distortions under JPEG attacks

Watermark	Compression, %			
	5	15	25	35
Fragile watermark	93.0	81.2	65.6	43.1
Textual watermark	99.5	95.2	89.5	82.7
ROI	98.7	96.6	91.0	82.1

Table 4. BCR estimates under JPEG attacks

The ROI and textual watermarks are more robust to JPEG attacks with regard to other types of attacks due to applied DWT/DST. However, fragile watermark is destroyed as usually.

## 7. CONCLUSIONS

In this research, we propose a multilevel protection of 3D medical images with regard to RST and JPEG attacks. Due to great volume of embedded medical information, the methods of 3D watermarking techniques are not suitable directly. We reduced a dimension of medical images from 3D to a set of 2D

slices. In each slice, three types of watermarks are embedded in frequency domain. Additionally, this procedure is enforced by Arnold's transform of ROI and textual watermarks. Experimental results show a relatively good robustness of the ROI watermark under RST and JPEG attacks due to the applied frequency transforms, DWT or DST depending on the total volume of embedded information. Fragile watermark embedded by DHT confirms its main function, viz. indication of presence of attacks.

Future investigations are directed on compensation of RST desynchronization attacks in medical images.

## ACKNOWLEDGEMENTS

The reported study was funded by the Russian Fund for Basic Researches according to the research project № 19-07-00047.

## REFERENCES

- Arnol'd, V.I., Avez, A., 1968. Ergodic problems of classical mechanics. *Mathematical physics monograph series*. New York, Benjamin.
- Arumugham, S., Rajagopalan, S., Rayappan, J.B.B., Amirtharajan, R., 2018. Networked medical data sharing on secure medium – A web publishing mode for DICOM viewer with three layer authentication. *Journal of Biomedical Informatics*, 86, pp. 90-105.
- Chai, X., Chen, Y., Broyde, L., 2017. A novel chaos-based image encryption algorithm using DNA sequence operations. *Optics and Lasers in Engineering*, 88, pp. 197-213.
- Chen, J.-X., Zhu, Z.-L., Fu, C., Zhang, L.-B., Zhang, Y., 2014. Cryptanalysis and improvement of an optical image encryption scheme using a chaotic Baker map and double random phase encoding. *Journal of Optics*, 16(12), no. 125403.
- del Rey, M.A., Pastora, H.J.L., G. Rodríguez Sanchez, R.G., 2016. 3D medical data security protection. *Expert Systems with Applications*, 54, pp. 379-386.
- DICOM: Digital Imaging and Communications in Medicine. Available at: <https://www.dicomstandard.org/current/> (18 December 2018)
- El Zein, O.M., El Bakrawy, L.M., Ghali, N.I., 2017. A robust 3D mesh watermarking algorithm utilizing fuzzy C-means clustering. *Future Computing and Informatics Journal*, 2(2), pp. 148-156.
- Favorskaya, M.N., Jain, L.C., Savchina, E.I., 2018a. Perceptually tuned watermarking using non-subsampled shearlet transform. In: Favorskaya M.N., Jain L.C. (Eds.) *Computer Vision in Control Systems-3*, ISRL, Vol. 136, pp. 41-69.
- Favorskaya, M., Savchina, E., Popov, A., 2018b. Adaptive visible image watermarking based on Hadamard transform. In: *Advanced Technologies in Aerospace, Mechanical & Automation Engineering (MIST Aerospace 2018)*, Vol. 450, pp. 052003-1–052003-6.
- Goldstein, T., Osher, S., 2009. The split Bregman method for L1 regularized problems. *SIAM Journal on Imaging Sciences*, 2(2), pp. 323-343.
- Jiao, S., Zhou, C., Shi, Y., Zou, W., Li, X., 2019. Review on optical image hiding and watermarking techniques. *Optics and Laser Technology*, 109, pp. 370-380.
- Li, C., Kao, C., Gore, J., Ding, Z., 2007. Implicit active contours driven by local binary fitting energy. In: *IEEE Conference on Computer Vision and Pattern Recognition*, Minneapolis, MN, USA, pp. 1-7.
- Mehra, I., Singh, K., Agarwal, A.K., Gopinathan, U., Nishchal, N.K., 2015. Encrypting digital hologram of three-dimensional object using diffractive imaging. *Journal of Optics*, 17(3), Article ID: 035707.
- Muniraj, I., Kim, B., Lee, B.G., 2014. Encryption and volumetric 3D object reconstruction using multispectral computational integral imaging. *Applied Optics*, 53(27), pp. 25-32.
- Pan, W., Bouslimi, D., Karasad, M., Cozic, M., Coatrieux, G., 2018. Imperceptible reversible watermarking of radiographic images based on quantum noise masking. *Computer Methods and Programs in Biomedicine*, 160, pp. 119-128.
- Saini, I., Singh, P., Yadav, A.K., 2017. Analysis of Lorenz-chaos and exclusive-OR based image encryption scheme. *International Journal of Social Computing and Cyber-Physical Systems*, 2(1), pp. 59-72.
- Vese, L.A., Chan, T.F., 2002. A multiphase level set framework for image segmentation using the Mumford and Shah model. *International Journal of Computer Vision*, 50(3), pp. 271-293.
- Wang, L., Li, C., Sun, Q., Xia, D., Kao, C., 2009. Active contours driven by local and global intensity fitting energy with application to brain MR image segmentation. *Computerized Medical Imaging and Graphics*, 33(7), pp. 520-531.
- Wang, K., Lavoue, G., Denis, F., Baskurt, A., 2011. Robust and blind mesh watermarking based on volume moments. *Computers and Graphics*, 35(1), pp. 1-19.
- Yu, Z., Ip, H.H.S., Kwok, L.F., 2003. A robust watermarking scheme for 3D triangular mesh models. *Pattern Recognition*, 36(11), pp. 2603-2614.
- Zhang, G., Song, X., Wen, T., Fu, C., 2019. Reversibility improved data hiding in 3D mesh models using prediction error expansion and sorting. *Measurement*, 135, pp. 738-746.