Watermarking digital 3D volumes in the Discrete Fourier Transform domain

Vassilios Solachidis, *Member, IEEE*, and Ioannis Pitas, *Fellow, IEEE*

Abstract

In this paper, a robust blind watermarking method for 3D volumes is presented. A bivalued watermark is embedded in the Fourier transform magnitude of the 3D volume. The Fourier domain has been selected because of its scaling and rotation invariance. Furthermore, in order to decrease the detection time, a special symmetry of the watermark is exploited. The proposed method is proven to be resistant to 3D lowpass filtering, noise addition, scaling, translation, cropping and rotation. Experimental results prove the robustness of this method against the above-mentioned attacks.

Index Terms

3d volume watermarking, Fourier transform, icosahedron.

I. Introduction

MULTIMEDIA data can be easily copied, reproduced and sometimes maliciously processed in a networked environment. Thus, protection of multimedia information has attracted a lot of attention during the last few years. Watermarking has been proposed as an efficient tool for copyright protection. The related research has exhibited tremendous growth in the past decade. The basic concept behind any watermarking technique is the insertion of an invisible signal (watermark) in the original data. This signal conveys copyright information about the owner or authorized user. A watermark should fulfill some basic requirements. These can be summarized as follows:

- *Imperceptiblity:* Watermark perceptibility not only decreases the media quality, but also easies watermark localization and removal.
- *Robustness:* The watermark should be detected even after intentional or unintentional processing attacks.
- *Noninvertibility:* The watermark should be localized within a watermarked signal.

This work has been partially supported by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT.

- *Media dependency:* Although a single key produces a single watermark, a watermark should be signal-dependent to avoid collusion attacks.
- *Trustworthy detection:* False alarm and false rejection probabilities should be sufficiently low.

A general watermarking framework for copyright protection has been presented in [1], [2] and describes all these issues in detail. Watermarking has recently become a very active research area and numerous methods dealing with audio [3], image [4] - [9] or video watermarking [10]-[14] have appeared in the literature to date. Overview papers on existing multimedia watermarking methods can be found in [15], [16].

The limited existing literature, with respect to 3D volumetric data watermarking, manifests the little attention that has been given to this domain, which is very important particularly for medical image copyright protection. Both spatial and transform domain techniques have been proposed for 3D volume watermarking. In [17], a 3D voxel based watermarking method is proposed, which is an extension of the 2D watermarking methods [6],[18]. In [19], a 3D voxel based watermarking method is proposed. The watermark is embedded into the 3D DCT domain of the volume and then, the watermarked volume is obtained by applying an inverse DCT. This method is robust against geometric attacks but it is not blind since the original volume is subtracted from the watermarked one. A similar approach is presented in [20]. In this case, the embedding is performed in the wavelet domain.

Volumetric watermarking can be performed using two categories of watermarking techniques. The first one includes slice-based techniques, which are similar to the classical 2D watermarking methods. The main idea behind this group of techniques is that the watermark is embedded separately into each 2D slice. The second category of watermarking techniques consists of volume-based ones. The major difference of the latter group of techniques is that they treat the volume as a 3D signal instead of a set of 2D signals (slices). In attempting a brief comparison between the two different categories, one can argue that slice-based techniques are simpler, faster and less computationally intensive. On the other hand, slice-based techniques can not cope with 3D geometrical attacks that do not have an equivalent 2D attack. For example, if z is the axis that is perpendicular to the slices, then 3D rotation around this axis is equivalent to 2D rotations of all slices around the intersection point of the z axis and each slice. Any other type of 3D rotation does not have an equivalent set of 2D slice rotations resulting in watermark detection failure. 3D rotation, as well as 3D scaling, changes the number of the volume slices. Thus, these attacks can not be handled by slice-based techniques. Volume-based techniques, can cope more efficiently with the above mentioned 3D attacks, although being more computationally complex.

Generally, there are many ways in the literature that the researchers cope with the watermark robustness against geometric attacks issue. One way is the use of a pattern (or template) in the watermark construction. Thus, due to the existence of redundant

information the issue of watermark resynchronization becomes much easier. Such examples can be found in [21]-[24]. Another way is the use of a geometric invariant domain such as the Fourier-mellin and Radon transform, the Fourier magnitude and the Zernike moments. Most of these ideas where inspired from image registration methods. These watermarking methods can be found in [25] -[28]. Finally, another approach is the geometric attack estimation through embedded features. The main idea is the feature embedding in order to be able to detect them even after a geometric attack. After the successful features detection, it is easy to estimate the geometric attacks performed to the watermark media, invert the geometric transformation and then detect the watermark. Unfortunately, the main drawback of these approach is that these features can be detected also for an attacker and then eliminated. Furthermore, the attacks can add some other features in order to confuse the detector regarding the embedded features. In [29]- [31] watermarking feature based approaches can be found.

In this paper, a volumetric data watermarking method for 3D volumes is presented. The watermark is embedded in the magnitude of the Fourier transform of the volume. The watermark is not embedded on the entire frequency domain, but it is located between two homocentric spheres. This watermarking method is blind, which implies that the original (unwatermarked) volume is not needed in the detection procedure. Therefore, if the volume is geometrically transformed (rotated, translated, scaled or cropped), the detection procedure is relatively slow. However, the special watermark structure and the fact that the watermark is embedded in the Fourier magnitude accelerates the detection procedure, because the geometrical properties of the Fourier domain are exploited. More specifically, the watermark is designed in such a way as to obtain icosahedral symmetry. This property, as it will be seen later on, accelerates the detection procedure significantly, in the case that the watermarked volume has been rotated. Thus, this method could be associated in both pattern watermarking methods as well as to the geometric invariant ones.

A corresponding symmetry in the 2D (image) watermarking case could be exploited if a ring consisting of identical sectors was chosen as the embedded watermark. In such a case, the rotation search space would decrease from $[0, 2\pi]$ rad to $[0, \frac{2\pi}{s}]$, where s denotes the number of the identical sectors.

However, in the 3D (volume) watermarking case, the fact that there exist 3 rotation angles increases the search space significantly and poses a challenge, in the sense that the watermark is selected to exploit symmetries to minimize the search space. One way to tackle this problem would be to extend the aforementioned 2D watermarking symmetry case, selecting a spherical shell as a watermark and exploiting the icosahedral symmetry in the watermark values.

3D volume watermarking differs significantly from the watermarking of 1D or 2D signals. For example in audio watermarking there is no rotation attack and translation attack is simpler since that the signal can be translated only to one dimension. In the 2D watermarking, translation can be performed in two dimensions and also rotation attack is an applicable attack. Finally, in

the 3D case the attacks depend on the application. For example, in video watermarking rotation attack can not be applied in video data along the time axis. Scaling may be applied but frame size (scaling in the x-y axis) and frame rate (scaling in the t-axis) may be assumed known before the embedding and detection procedures. On the other hand in 3D volume watermarking 3D rotation, 3D translation and scaling are much more rich since they are defined on a 7 parameter space.

Thus, if we had applied a 2D watermarking method in a 3D volume (by embedding 2D different watermarks in each volume slice) then this method would not be robust against scaling and rotation. In the case of scaling, the number of slices would be changed (according to the scale factor) and we could not detect the watermarks since that the number of slices will be different than the number of the embedded watermarks.

In the rotation case, only if the rotation performed around z-axis, the 2D watermarks would be robust, since rotation around z-axis would result in 2D rotation of each volume slice. If the rotation would performed around other axis different than the z one, then the 2D rotation would not be robust.

The paper is organized as follows. The properties of the 3D Fourier transform are described in section II. Then, watermark construction is outlined in section III. In the next two sections, IV and V, the watermark embedding and detection procedures are illustrated. In section VI, special reference is given to the robustness of the method against geometrical distortions and to the contribution of the watermark structure and the properties of Fourier transform towards that goal. In section VII, experimental results are presented. Finally, conclusions are drawn in section VIII.

II. 3D Fourier transform properties

In this section the important Fourier transform properties will be presented that will be exploited in the watermark embedding and detection procedure. Let $v(n_1, n_2, n_3)$ be a $N \times N \times N$ grayscale original volume. Its Discrete Fourier Transform is given by:

$$V(k_1, k_2, k_3) = \sum_{n_1=0}^{N-1} \sum_{n_2=0}^{N-1} \sum_{n_3=0}^{N-1} v(n_1, n_2, n_3) e^{-j2\pi n_1 k_1/N - j2\pi n_2 k_2/N - j2\pi n_3 k_3/N} \tag{1}$$

Let also $M(k_1, k_2, k_3) = |V(k_1, k_2, k_3)|$ be the magnitude of $V(k_1, k_2, k_3)$. The 3D Fourier transform has the following properties:

- Circular shifts in the spatial domain do not effect the magnitude of the Fourier transform:

$$|DFT[v(n_1 + d_1, n_2 + d_2, n_3 + d_3)]| = M(k_1, k_2, k_3) \tag{2}$$

- Scaling in the spatial domain causes inverse scaling in the frequency domain:

$$DFT[v(sn_1, sn_2, sn_3)] = \frac{1}{s^3} V\left(\frac{k_1}{s}, \frac{k_2}{s}, \frac{k_3}{s}\right) \tag{3}$$

where s is the scaling factor.

- Rotation in the spatial domain causes the same rotation in the frequency domain:

$$DFT[v([[n_1, n_2, n_3]^T R_{\theta_x\theta_y\theta_z}]^T)] = V([[k_1, k_2, k_3]^T R_{\theta_x\theta_y\theta_z}]^T) \tag{4}$$

where $[]^T$ denotes the transpose operator and $R_{\theta_x\theta_y\theta_z}$ is the 3D rotation matrix by θ_x, θ_y and θ_z angles around x, y and z axes respectively.

III. Watermark construction

The watermark W is a 3 dimensional bivalued 1, -1 signal. The number of $1s$ has to be identical to the number of $-1s$, so that the watermark signal has a zero mean value. To proceed, one should observe that modifications in the low frequencies of the Fourier transform will cause visible changes in the spatial domain of the 3D volume. Furthermore, usual lowpass filtering operations mostly affects the high frequencies of the Fourier transform. Thus, the watermark should be added in the middle frequencies, because, if carefully designed, it will be both robust against lowpass filtering and perceptually invisible. Considering that the zero frequency term $I(0,0,0)$ is in the center of the transform domain, the watermark is embedded in a region that covers the middle frequencies:

$$W(r,\phi,\theta) = \begin{cases} 0, & \text{if } r < R_1 \text{ and } r > R_2 \\ \pm 1, & \text{if } R_1 \leq r \leq R_2 \end{cases} \tag{5}$$

where $r = \sqrt{k_1^2 + k_2^2 + k_3^2}$, $\theta = \arctan\left(\frac{k_2}{k_1}\right)$, $\phi = \arctan\left(\frac{k_3}{\sqrt{k_1^2+k_2^2}}\right)$

The watermark W is a spherical shell of inner radius R_2 and outer radius R_1, having values ± 1.

Another important issue, besides the determination of its embedding domain, is 3D watermark symmetry. We construct a symmetrical watermark in order to reduce the search space in the rotation domain $[\theta_x, \theta_y, \theta_z]$.

This symmetrical watermark support region is selected to be a regular polyhedron. Obviously, as the number of the polyhedron edges increases, the rotation search space decreases. Although in the corresponding 2D method, a 2D ring divided into any desirable number of sectors is required [32], in the 3D case the number of the polyhedron faces can not be arbitrary. Unfortunately, there is an upper limit for the number of the edges of a regular polyhedron [33]. This polyhedron is the icosahedron and it is illustrated in Figure 1. It can be considered as a union of 20 pyramids where each individual pair of pyramids have a common face. The coordinates of the 12 icosahedron vertices can be given by: $(\pm\frac{1}{2}, 0, \pm\frac{r}{2})$, $(\pm\frac{r}{2}, \pm\frac{1}{2}, 0)$, $(0, \pm\frac{r}{2}, \pm\frac{1}{2})$, where r is the golden ratio ($r = \frac{1+\sqrt{5}}{2}$) (proposition 16 of [33]).

Thus, the watermark shell can be considered as an inner sphere of an icosahedron, which consists of identical pyramids. The use of icosahedral symmetries in fast watermark detection is analyzed in section VI.

IV. Watermark embedding

Let $P(k_1, k_2, k_3)$ be the phase of the Fourier transform of the volume $V(k_1, k_2, k_3)$ and $W(k_1, k_2, k_3)$ the watermark. The watermark is embedded in the volume Fourier magnitude coefficients, according to the following embedding rule:

$$\begin{aligned} M^W(k_1, k_2, k_3) &= f(M(k_1, k_2, k_3), p) \\ &= M(k_1, k_2, k_3) + M(k_1, k_2, k_3)W(k_1, k_2, k_3)p \\ &= M(k_1, k_2, k_3)(1 + W(k_1, k_2, k_3)p), \end{aligned} \tag{6}$$

where p is a factor that determines the watermark strength. The embedding has been performed in a multiplicative way, because this corresponds to a simple watermark masking i.e. the watermark amplitude increases as the Fourier coefficient magnitude increase. It is obvious that, due to the fact that M^W represents the Fourier magnitude, its values should be positive. Therefore, p should be selected to be smaller than 1.

The watermarked volume $v^W(n_1, n_2, n_3)$ is produced by taking the inverse Fourier transform of the watermarked magnitude $M^W(k_1, k_2, k_3)$ and the phase of the original volume $P(k_1, k_2, k_3)$:

$$v^W = IDFT(V^W), \;\; V^W = M^W(cos(P) + i\, sin(P)). \tag{7}$$

V. Watermark detection and method evaluation

A. Watermark detection

Let V' be a possibly watermarked volume and M' its DFT magnitude. The correlation c between the possibly watermarked coefficients M' and the watermark W can be used to detect the presence of the watermark:

$$c = \sum_{k_1=1}^{N} \sum_{k_2=1}^{N} \sum_{k_3=1}^{N} W(k_1, k_2, k_3) M^{'}(k_1, k_2, k_3). \tag{8}$$

If the volume V' is watermarked by another watermark W', $W \neq W'$, then the correlation c is given by:

$$c = \sum_{k_1=1}^{N} \sum_{k_2=1}^{N} \sum_{k_3=1}^{N} (W'(k_1, k_2, k_3)M(k_1, k_2, k_3) + pW(k_1, k_2, k_3)W'(k_1, k_2, k_3)M(k_1, k_2, k_3)) \tag{9}$$

If the volume V' is watermarked by W, the correlation c is:

$$c = \sum_{k_1=1}^{N} \sum_{k_2=1}^{N} \sum_{k_3=1}^{N} (W(k_1, k_2, k_3)M(k_1, k_2, k_3) + pW^2(k_1, k_2, k_3)M(k_1, k_2, k_3)). \tag{10}$$

Assuming that:

- W, W', M are independent and identically distributed random variables,

- W, W' have zero mean value,
- W, W' are orthogonal to each other,

the mean value μ_c of c is given by:

$$\mu_c = \begin{cases} Kp\,\mu_{_M} & \text{if } W = W' \\ 0 & \text{if } W \neq W' \\ 0 & \text{if no watermark is present} \end{cases} \tag{11}$$

where $\mu_{_M}$ and $\sigma^2_{_M}$ are the mean value and the variance of $M(k_1, k_2, k_3)$, respectively, and K is the number of the volume voxels in the spherical shell $K = \frac{4}{3}\pi(R_2^3 - R_1^3)$. The correlator c can also be expressed in a normalized form: $c_n = c/\mu_c$. In this case, the mean value μ_c depends on the magnitude of the Fourier transform of the original volume $M(k_1, k_2, k_3)$, which is unknown. Instead of $\mu_{_M}$, we can use $\mu_{_{M'}}$, because:

$$\mu_{_{M'}} = \overline{M}(k_1, k_2, k_3) + p\overline{W}(k_1, k_2, k_3))\overline{M}(k_1, k_2, k_3) = \overline{M}(k_1, k_2, k_3) = \mu_{_M} \tag{12}$$

The mean value of the normalized correlator c_n is expected to be 1 for every watermarked volume, when calculated for the correct watermark W. Most often, the watermarks that are produced by random generators do not have a zero mean value. Thus, the correlator should be modified in order to avoid this problem. The modified correlator is of the form:

$$c_n = \left(\frac{\sum\limits_{M' \in M'_+} M'(k_1, k_2, k_3)}{N_+} - \frac{\sum\limits_{M' \in M'_-} M'(k_1, k_2, k_3)}{N_-} \right) \frac{N_+ + N_-}{2 \cdot p \sum\limits_{M' \in M_+ \cup M_-} M'(k_1, k_2, k_3)}$$

$$= \left(\frac{\sum\limits_{M \in M_+} M(k_1, k_2, k_3) + M(k_1, k_2, k_3) \cdot p}{N_+} - \frac{\sum\limits_{M \in M_-} M(k_1, k_2, k_3) - M(k_1, k_2, k_3) \cdot p}{N_-} \right)$$

$$\frac{1}{2\,p\,\mu_M}$$

$$\mu_{c_n} = (\mu_{_{M_+}} + p \cdot \mu_{M_+} - \mu_{_{M_-}} + p \cdot \mu_{M_-}) \frac{1}{2\,p\,\mu_M} = 1,$$

where: $M_+ = \{M(k_1, k_2, k_3) \mid W(k_1, k_2, k_3) = 1\}$, $M_- = \{M(k_1, k_2, k_3) \mid W(k_1, k_2, k_3) = -1\}$,

and N_+, N_- are the cardinalities of M_+ and M_- respectively. We assume that $\mu_{_{M_+}} = \mu_{_{M_-}} = \mu_{_M}$ Practically, we calculate two sums, the sum of the $M'(k_1, k_2, k_3)$ where the corresponding watermark values equal 1 and the sum of the $M'(k_1, k_2, k_3)$ where the corresponding watermark values equal -1. The quantity in the brackets is the weighted difference between the first and the second sum. Then, this is divided by the quantity in the last fraction in order to achive unity mean.

B. Performance evaluation of the watermarking method

For the performance evaluation of the proposed method, false alarm and false rejection probabilities will be used. The watermark detection rule could be:

H_0: V' is watermarked by W, if $c_n \geq T$

H_1: V' is not watermarked by W, if $c_n < T$.

Considering that T is the detection threshold, two error probabilities must be estimated, namely the false alarm probability P_{fa} (which is the probability of detecting a watermark in an unwatermarked volume) and the false rejection probability P_{fr}, i.e., the probability of not detecting the watermark in the watermarked volume.

In order to estimate these error probabilities (P_{fa} and P_{fr}), a watermark is embedded in the volume and then, detection is performed using firstly the correct key (the key that was used in the embedding) and then an erroneous key. This is performed for L different pairs of correct and erroneous keys. As a result, two sets of detector outputs are produced, one for the detection with the erroneous key (set A) and one for detection with the correct key (set B). The next step is to calculate the detection errors by counting the detector values of set A which are higher than threshold T, denoted by A_0 and the detector values of set B that are lower than T, denoted by B_0. The estimates of the probabilities of the detection errors for a particular threshold T are given by: $\hat{P}_{fa} = \frac{B_0}{L}$ and $\hat{P}_{fr} = \frac{A_0}{L}$.

Unfortunately, this performance estimation can produce errors of order of $1/L$. If the desired order is 10^{-L}, we have to perform the above experiments for 10^L keys. For large L values, the number of the experiments is not feasible. Thus, in order to estimate the above mentioned probability errors, we approximate the empirical pdf of c_n with a continuous distribution. Assuming that the the detector summation terms in (8) are independent and using the central limit theorem, it can be derived that both detector output sets (A, B) follow the Gaussian distribution. Then, given the estimated detector output pdfs, the resulting ROC (Receiver Operating Characteristic) curves are constructed. The ROC curve is the graphical plot of the false alarm vs false rejection errors for several values of the detection threshold. In order to construct the ROC, the following intervals have to be calculated

$$P_{fa} = \int_T^{\infty} f_1(x)dx,$$
$$P_{fr} = \int_{\infty}^{T} f_2(x)dx.$$

where $f_1(x)$ and $f_2(x)$ are the theoretical detector output distributions of sets A and B respectively. Each threshold value T corresponds to a pair of (P_{fa}, P_{fr}). The ROC curve consists of all the pairs of (P_{fa}, P_{fr}) calculated for many values of T. Usually, T values lie between the mean values of $f_1(x)$ and $f_2(x)$. Another useful measure is the Equal Error Rate (EER)

that is the point in the ROC curve where both errors are equal ($P_{fa} = P_{fr}$).

VI. Geometrical attacks

In this section, the attacks of geometrical distortions to the embedded watermark will be examined and recovery mechanisms will be presented. The spherical symmetry will be employed to counter 3D rotation attacks.

A. Rotation

The watermark is constructed in such way that the detection procedure of a rotated watermarked volume becomes simpler and faster. The main idea is to restrict the search space $[\theta_x, \theta_y, \theta_z]$ and, consequently, to make the watermark detection process faster.

Suppose that we have a watermarked volume, rotated by angles θ_x, θ_y and θ_z around x, y and z axes, respectively. Before we perform the detection procedure, we should rotate the watermarked volume backwards to its initial position. However, since the method is blind, the initial unwatermarked volume is unknown. Consequently, the rotation angles are unknown as well. Because of the icosahedral symmetry of the watermark, the detection will be successful not only for the initial position of the watermarked volume but for a total of 20 different rotated positions.

However, the aforementioned symmetry is not adequate. All pyramids of the icosahedron are identical and are filled with randomly generated voxels. The pyramid bases (faces of the icosahedron) are denoted by capital letters. Figure 2a depicts the initial position of the watermark. For illustration purposes, arrows indicate the orientation of the pyramid. Suppose that we rotate the initial watermark in such a way that the resulting watermark domain is the one depicted in Figure 2b. Due to the rotation, faces E,B,A,F of the icosahedron in Figure 2a correspond to faces D,G,C,A, respectively, in Figure 2b.

Even though the faces can be matched using appropriate rotation, the orientation of the corresponding pyramids is not the same. This implies that an additional symmetry issues should be exploited to cope with this problem. More specifically, each pyramid is divided into three identical pyramidal elements as shown in Figure 3. Each pyramidal element is symmetrical to the line connecting the center of the mass of the 'mother' pyramid to the three vertices of the base and the center of the icosahedron. Thus, the above mentioned matching can be applied, with the resulting orientation of the corresponding pyramids becoming the same.

Suppose that we wish to search for the point A_1, where A_1 is the metacenter of the shaded face in Figure 1. Let, A_i $i = 2, ..., 20$, be the metacenter of the rest of the icosahedron faces. Because of the symmetry, it is adequate to match A_1 with any of the points $A_i,\ i = 1, ..., 20$. In the shaded area, there exists exactly one A_i. Thus, we can limit out search in this area. If the watermark is appropriately rotated so that point A_1 is matched with any of A_i, then, only the symmetric point

of A_1 with respect to O, is also matched, where O is the center of the icosahedron. However, the rest of the points should be matched as well. This could only be performed by rotating the watermark around the A_1O axis. Because of the symmetry of each pyramid of the icosahedron, the rotation should not be performed in the interval $[0, 2\pi)$, but in the interval $[0, 2\pi/3)$. Thus, in order to find out the best matching, we correlate (in the Fourier domain) the volume with the rotated watermark for all the rotated versions according the the previous analysis. When we get the maximum correlation value, we assume that the watermark is matched with the volume. It should be noted that the aforementioned procedure is iterative: each step involves rotation in order to match the A_1 point followed by rotation around the A_1O axis (in the interval $[0, 2\pi/3)$) in order to match the rest points. This procedure is mandatory, since watermark matching can not be determined only by A_1 matching, but can be verified only if all the voxels are matched.

Therefore, if we want to detect a rotated volume, it is sufficient to detect any rotations that occur around the z axis for angles lying in the interval $[0, 2\pi/5]$, and around the y axis for angles lying in the interval $[0, \pi/3]$ rad. This is illustrated more clearly in Figure 4. In this Figure, the surface of the watermark sphere is shown. Rotation around y and z axes corresponds to translation of the surface in Figure 4. Thus, in order to match a point A_1 with any of the points $A_i,\ i = 1, ..., 20$, we have to rotate only in the above-mentioned intervals. Following that, we should detect rotations around the A_1O axis for angles between 0 and $2\pi/3$, due to the pyramid symmetry. For more advanced detection, each pyramid is divided in sectors as can be seen in Figure 5. Hence, as far as the rotation around the AO axis is concerned, the watermark can be detected not only for the correct angle ω, but also for angles lying in the interval $[\omega - x, \omega + x]$. x depends on the sector dimensions of the pyramids.

1) Special case: Rotation around z axis: In medical imaging applications the most usual rotation that is applied is the rotation around z axis. In the case of a non-symmetrical watermark the search space would be the interval $[0, 2\pi]$. However, in our case, because of the symmetry, the search space around z axis is limited to the $[0, 2\pi/5]$, that is the one fifth of the search space in the non-symmetrical case. This significant search space reduction minimizes the detection time.

B. Scaling

Scaling in the spatial domain causes inverse scaling in the frequency domain (3). Suppose that the size of the initial volume is $N \times N \times N$ and the radii (internal and external) of the watermark (in the frequency domain) are R_1 and R_2 respectively. Suppose that we scale the watermarked volume by a scale factor $s,\ (s > 0)$. Then, the scaled volume size is $sN \times sN \times sN$, but the size of the watermark of the scaled volume remains unaltered in the frequency domain. This means that the watermarked coefficients will still lie within the spherical shell of radii R_1 and R_2.

Thus, in the case of a scaled volume watermark detection, we only have to calculate the correlation between the watermark

and the watermarked volume magnitude, since R_1 and R_2 are absolute values. Furthermore, because of the normalization, the correlation output does not depend on the scale factor s.

C. Cropping

Cropping in the spatial domain results in a change in the frequency sampling step. Thus, in order to detect the watermark, we firstly have to change the frequency sampling step of the cropped volume and then compute the correlation. Unfortunately, since the method is blind, the size of the original (non-cropped) volume is not known. Therefore, correlation has to be computed for several sampling steps and the maximum correlator output should be selected.

D. Translation

In the medical imaging domain, all the useful information lies within the volume objects. Usually, the volume background consists of voxels of uniform luminance (typically around zero). Thus, any translation of the volume content that does not lead to object truncation is equivalent to a 3D circular shift. The proposed method is robust against this kind of attack. Due to the translation property of the Fourier transform, as illustrated in equation (2), the Fourier magnitude remains unaltered, if a circular shift in the spatial domain has been performed. Rotation around an arbitrary center is equivalent to rotation around the volume center, followed by translation. Therefore, the proposed method is robust to such an attack.

VII. Experimental results

This method has been applied in a number of 3D medical volumes. A gray scale $256 \times 256 \times 256$ volume coming from the Visible Human Project [34] was used as a host volume in this paper (Figure 6a). The number of the non zero voxels of this volume is equal to $4.671.878$, that is only the 27.85% of the total number of the volume voxels. The watermark is finally embedded onto the non-zero voxels only. Thus, after the embedding procedure, all the voxels of the watermarked volume will be converted to zero valued voxels if the corresponding original voxels in the original volume are zero. Of course, this corresponds to a form of arbitrary region cropping.

In Figure 6b, the watermarked volume is presented. The embedding power p that was used was equal to 0.3. The parameters R_1 and R_2 that were used are equal to 26 and 102 respectively. For better visual comparison of the original and the watermarked volumes, the same (namely the 133th) frame of each volume is presented in Figures 7a and 7b respectively. There is no visible difference between the two frames. The absolute difference between the original and the watermarked frame is shown in Figure 8. Note in order the differences to be visible the absolute difference has been multiplied by 20. The SNR of the watermarked volume is 31 dB. Therefore, the watermark is expected to be invisible. In Figure 8 the absolute difference between the original

and watermarked frames. Since that the difference is small, the resulted frame would appear totally black. Thus, we multiplied it by the factor 20 in order to make visible the differences between the original and the watermarked frames. In Figure 9 another example of original-watermarked volume pair is shown and in Figure 11 the ROC curve for this volume is illustrated.

The robustness of the 3D watermarking system to various attacks is shown in Figures 10-17, where we plot the detector output pdfs for the two hypothesis H_0, H_1 and the resulting ROC (defined in section V-B). As shown in Figures 10-17, in all the performed experiments, c_n is always bigger than the chosen threshold T ($T = 0.055$) in case of detection using the correct key, and lower that T, when the detection is performed with an erroneous key (even if the volume is distorted, compressed or geometrically transformed). Thus, according to the experimental results, both false alarm and false rejection errors are equal to zero ($P_{fa} = P_{fr} = 0$). In order to estimate the above errors more accurately, we will follow the procedure mentioned in the end of subsection V-B. For that reason, the errors that are presented in the next paragraphs are very small, even though the number of experiments can not justify so large accuracy.

In Figure 10, the ROC curve of the detector output is shown in the case of no attack. The two empirical pdfs are very well separated and the EER is very small (10^{-30}). In the next two Figures, 12 and 13, ROC curves of the detector output are shown in the cases of median and moving average filtering respectively. The window size in the filtering processes is $3 \times 3 \times 3$. The robustness is very good and the EER is $5.5 \cdot 10^{-4}$ and $4.1 \cdot 10^{-4}$ for the median and moving average filtering respectively. In Figure 14, the ROC curve of the detector output on the histogram equalized volume is presented. In this case, the results are even better compared with the no attack case (Figure 10). This happens because histogram equalization amplifies middle frequency noise, and therefore, the watermark itself. According to this observation, we can apply histogram equalization or high-pass filtering or an image whitening operation as a pre-detection process, in order to improve the detection results, i.e. to decrease the false alarm and false rejection errors.

In Figure 15, the ROC curve in the case of a translation attack is illustrated. The volume has been translated by 5 voxels in the x-axis, 10 voxels in the y-axis and 15 voxels in the z-axis. The EER in this case equals 10^{-27}.

In the next two Figures 16a, b the watermarking method robustness against JPEG compression is examined. This is a 2-dimensional attack that is performed separately in every frame. The quality of the compressed images is rather low and equals 60. The method performance is very good since the EER is 10^{-24}.

In Figure 17, the ROC curve in the case of a scaling attack is illustrated. The scale factors are equal to 0.5. Because of scaling, the high frequencies of the volume are attenuated. Generally, the frequencies that will be deleted depend on the downsampling factor. Hence, the bigger the downsampling factor is, the bigger the number of the high frequencies that will be deleted is. Despite this fact, robustness is good with $EER = 10^{-4}$.

Apart from the isotropic scaling, we have performed non-isotroping scaling. In Figure 18 the detector output for anisotropic scaling attack is shown. In this case, we performed scaling only along y and z axis. More specifically, we used scaling factors $s_x = 1$, $s_y = s_z = a$, for $a = 1$ to 1.035. Although that the method is not robust against anisotropic scaling, the watermark can be detected for small scaling factors $(a < 1.01)$.

In the Figures 19a,b, the watermarked volume output in the case of a combined geometric attack is presented. More specifically, the watermarked volume has been scaled from size $256 \times 256 \times 256$ to $307 \times 307 \times 307$ (scaling factor 1.199). Then, the scaled volume has been cropped to the size $256 \times 256 \times 256$. As it is illustrated in these Figures, the resulting volume has been scaled and cropped (the lower part of the face, the neck and the shoulders as well as the nose have been cropped). The detection has been performed according to the procedure described in subsection VI-C. Thus, we have to detect the watermark for several sampling steps and then select the highest value of the correlator. An example is shown in the Figure 19c. Due to the fact that the highest value of the detector is selected to be the max value of correlator outputs for the several sampling steps, the distribution mean of the correlator output in the case of erroneous watermark detection is slightly bigger than zero. It should be noted that, in this case, a full watermark search would be very complicated computationally, if it would require detection for several scaling factors as well as for translations in x, y and z axis. Using the proposed method, the search has to be limited only to the different sampling steps. In the Figure 20a, the ROC curve is shown. Although the errors are slightly bigger than in the no attack case due to the errors imported by the attacks (interpolation by scaling attack and deduction of watermark energy by cropping), the detection performance is still very good (EER=$2.4\ 10^{-4}$).

Finally, the results with respect to a rotation attack are presented in Figure 21a. More specifically, the watermarked volume is rotated using suitable angles, so that, due to the watermark symmetry, the detector output will be expected to be above the threshold. This experiment has been performed for all the combinations of the following angles: $0, 2\pi/5, 4\pi/5, 6\pi/5, 8\pi/5$ around the x-axis, $0, \pi/3, 2\pi/3, 4\pi/3, 5\pi/3$ around the y-axis and $0, 2\pi/3, 4\pi/3$ around the AO axis. As depicted in Figure 21a, for all the above angles the produced detector output shows that the watermark (due to symmetry) remains unaltered.

In order to show the method sensitivity on the search step size we performed the following experiment. We performed detections by rotating the watermark using small rotation angles. The results are shown in Figure 21b. It can be seen that the method it quite robust against ± 2 degrees rotation.

The watermark symmetry accelerates the watermark detection but, at the same time, it reduces the watermark capacity. One way to estimate the watermark capacity is to calculate the false alarm errors. The false alarm errors come from the existence of similar watermarks in watermark set. If the capacity is big enough, then the false alarm errors are small. Thus, according to the experimental results presented in this section, due to the fact that the false alarm errors are very small we conclude that

the watermark capacity is satisfactory.

A. Complexity

It is obvious that in the case that the watermarked volume has not undergone geometrical attacks, the watermark is synchronized with the watermarked volume. Thus, the only operation needed is the calculation of the Fourier magnitude of the watermarked volume and then the correlation between the watermarked magnitude and the watermark. The same stands also in the case of translation since that translation does not affect the Fourier magnitude. In the case of scaling attack, again no further operations are needed. Of course, if the scaling factor is greater than one, then just a part of the watermarked magnitude will be correlated with the watermark. If the scaling factor is lower than one, then a part of the watermark has to be correlated with the watermarked magnitude. In the case of cropping, the search has to be performed for several sampling steps (Figure 19c). Finally, in the case of rotation, the procedure is presented in subsection VI-A. The watermark is matched, if the A_1 point of the watermark is matched with one of the A_i points of the watermarked signal, and subsequently, if the rest of the points are matched. In order to match the point A_1, we have to search for all the combinations of rotations that moves the point A_1 inside a spherical triangle (Figure 4). Then, in order to match the rest of the points we have to rotate the watermark around the A_1O axis in the interval $[0, 2\pi/3)$. Thus, the total number of searches (correlations), for the rotation case, equals the product of the rotations for the matching of the point A_1 times the rotations for the matching of the rest of the points. The number of the rotations depends on the incremental step of the rotation angle. Each watermark pyramid can be constructed in such a way as to increase the incremental step and consequently decrease the number of rotations and the detection time. For example, the pyramid in Figure 5 is constructed in such a way that the rotations around the A_1O axis can be done using a quite large incremental search (3 degrees), because the pyramid is highly correlated with its rotated versions around A_1O axis for small angles. Furthermore, the pyramid in this Figure is constructed in a such a way that decreases the incremental search for the cropping searches. In Figure 19c, we achieve high correlator values for two sampling steps that allows us to double the sampling step and consequently decrease the number of searches.

VIII. Conclusions

In this paper, a blind watermarking method for 3D volumes is presented. In order to decrease the detection time, a symmetrical watermark is constructed. The embedding-detection procedures are performed in the Fourier domain of the volume and more specifically, in the Fourier magnitude. By inserting the watermark in the Fourier magnitude, the frequencies that are watermarked can be easily determined, resulting in robustness against filtering attacks and compression. Furthermore, due to the Fourier

magnitude properties, the method is also robust against geometrical distortions. The spherical symmetry of the embedded watermark is used to reduce the search space after rotation attacks.

REFERENCES

[1] G. Voyatzis and I. Pitas, "Protecting digital-image copyrights: A framework," *IEEE Computer Graphics and Applications*, vol. 19, no. 1, pp. 18–24, January/February 1999.

[2] G. Voyatzis and I. Pitas, "The use of watermark in the rotection of digital multimedia products," *IEEE Proceedings Special issue on Identification and protection of multimedia information*, vol. 87, no. 7, pp. 1197–1207, July 1999.

[3] M.D. Swanson, B.Zhu, A.H. Tewfik, and L. Boney, "Robust audio watermarking using perceptual masking," *Elsevier Signal Processing, Sp. Issue on Copyright Protection and Access control*, vol. 66, no. 3, pp. 337–355, 1998.

[4] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," *Elsevier Signal Processing, Sp. Issue on Copyright Protection and Access control*, vol. 66, no. 3, pp. 385–403, May 1998.

[5] I. Pitas, "A method for watermark casting in digital images,," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 8, no. 6, October 1998.

[6] G. Voyatzis and I. Pitas, "Digital image watermarking using mixing systems," *Computer & Graphics*, vol. 22, no. 3, 1998.

[7] M. Barni, F. Bartolini, V. Cappelini, and A. Piva, "A DCT-domain system for robust image watermarking," *Elsevier Signal Processing*, vol. 66, no. 3, pp. 357–372, 1998.

[8] C.-T. Hsu and J.-L. Wu, "Hidden digital watermarks in images," *IEEE Trans. on Image Processing*, vol. 8, no. 1, pp. 58–68, January 1999.

[9] D. Kundur and D. Hatzinakos, "Improved robust watermarking through attack characterization," *Optics Express*, vol. 3, no. 12, pp. 485–490, December 1998.

[10] R.B. Wolfgang, C.I. Podilchuk, and E.J. Delp, "Perceptual watermarks for digital images and video," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1108–1126, July 1999.

[11] W. Zhu, Z. Xiong, and Y. Zhang, "Multiresolution watermarking for images and video," *IEEE Trans. on Cirsuits and Systems for Video Technology*, vol. 9, no. 4, pp. 545–550, June 1999.

[12] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," *Elsevier Signal Processing, Sp. Issue on Copyright Protection and Access control*, vol. 66, no. 3, pp. 283–301, 1998.

[13] I.J. Cox, J. Kilian, F.T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, December 1997.

[14] M.D. Swanson, B. Zhu, and A.H. Tewfik, "Multiresolution scene-based video watermarking using perceptual models," *IEEE Journal of Selected Areas of Communications*, vol. 16, no. 4, pp. 540–550, May 1998.

[15] "Special issue on identification & protection of multimedia information," *Proceedings of the IEEE*, vol. 87, no. 7, 1999.

[16] "Special issue on copyright & privacy protection," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, May 1998.

[17] G.Louizis, A.Tefas, and I.Pitas, "Copyright protection of 3d images using watermarks of specific spatial structure," in *Proc. of IEEE Int. Conf. on Multimedia and Expo 2002(ICME2002)*, Lausanne, Switzerland, August 26-295 2002.

[18] A.Tefas and I.Pitas, "Robust spatial image watermarking using progressive detection," in *Proc. of 2001 IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP 2001)*, Salt Lake City, Utah, USA, May 7-11 2001.

[19] Y.H. Wu, X. Guan, M. S Kankanhalli, and Z.Y. Huang, "A robust invisible watermarking of volume data using the 3d dct," in *Proc. of Computer Graphics Interna-tional CGI 2001*, Hong Kong, China, July 03-06 2001, pp. 347 – 350.

[20] X. Guan, M. S Kankanhalli, Y.H. Wu, and Z.Y. Huang, "Invisible watermarking of volume data using wavelet transform," in *Proc. of International Conference on Multimedia Modeling MMM2000*, Nagoya, Japan, November 13-15 2000, p. 153166.

[21] M. Kutter, "Watermarking resisting to translation, rotation and scaling," in *Proc. of SPIE*, Boston, USA, November 1998.

[22] S. Pereira and T. Pun, "Robust template matching for affine resistant image watermarks," *IEEE Trans. on Image Processing*, vol. 9, no. 6, pp. 1123–1129, June 2000.

[23] S. Voloshynovskiy, F. Deguillaume, and T. Pun, "Multibit digital watermarking robust against local nonlineargeometrical distortions," *Image Processing, 2001. Proceedings. 2001 International Conference on*, vol. 3, 2001.

[24] S. Stankovic, I. Djurovic, and I. Pitas, "Watermarking in the space/spatial-frequency domain usingtwo-dimensional Radon-Wigner distribution," *Image Processing, IEEE Transactions on*, vol. 10, no. 4, pp. 650–658, 2001.

[25] J.K. Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Elsevier Signal Processing, Sp. Issue on Copyright Protection and Access control*, vol. 66, no. 3, pp. 303–317, 1998.

[26] C.Y. Lin, M. Wu, JA Bloom, IJ Cox, ML Miller, and YM Lui, "Rotation, scale, and translation resilient watermarking for images," *Image Processing, IEEE Transactions on*, vol. 10, no. 5, pp. 767–782, 2001.

[27] V.Solachidis and I.Pitas, "Circularly symmetric watermark embeddong in 2-d dft domain," *IEEE Transactions on Image Processing*, vol. 10, no. 11, pp. 1741–1753, 2001.

[28] D. Simitopoulos, DE Koutsonanos, and MG Strintzis, "Robust image watermarking based on generalized Radon transformations," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 13, no. 8, pp. 732–745, 2003.

[29] P. Bas, J.M. Chassery, and B. Macq, "Geometrically invariant watermarking using feature points," *Image Processing, IEEE Transactions on*, vol. 11, no. 9, pp. 1014–1028, 2002.

[30] M. Kutter, SK Bhattacharjee, and T. Ebrahimi, "Towards second generation watermarking schemes," *Image Processing, 1999. ICIP 99. Proceedings. 1999 International Conference on*, vol. 1, 1999.

[31] Jin S. Seo and Chang D. Yoo, "Localized image watermarking based on feature points of scale-space representation.," *Pattern Recognition*, vol. 37, no. 7, pp. 1365–1375, 2004.

[32] V. Solachidis and I. Pitas, "Self-similar ring shaped watermark embedding in 2-d dft domain," in *Proc. of EUSIPCO'00*, Tampere, Finland, September 4-8 2000.

[33] Euclid, *Elements*, vol. 13.

[34] Visible Human Project, "U.s. national library of medicine, 8600 rockville pike, bethesda, md 20894," http://www.nlm.nih.gov/research/visible/visible_human.html.

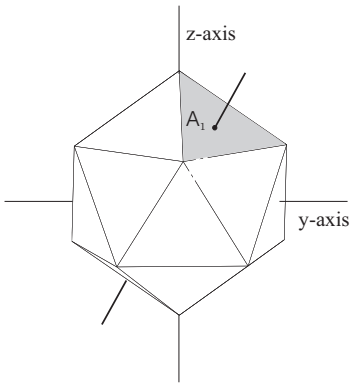
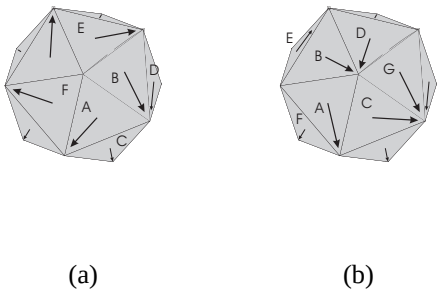


Fig. 1. Icosahedron.



(a) (b)

Fig. 2. Two different views of an icosahedron. The non-identical orientation of the corresponding pyramids is shown.

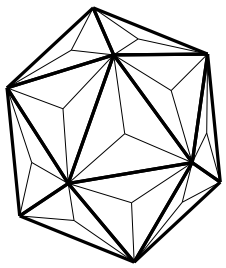


Fig. 3. Icosahedron split in pyramidal elements.

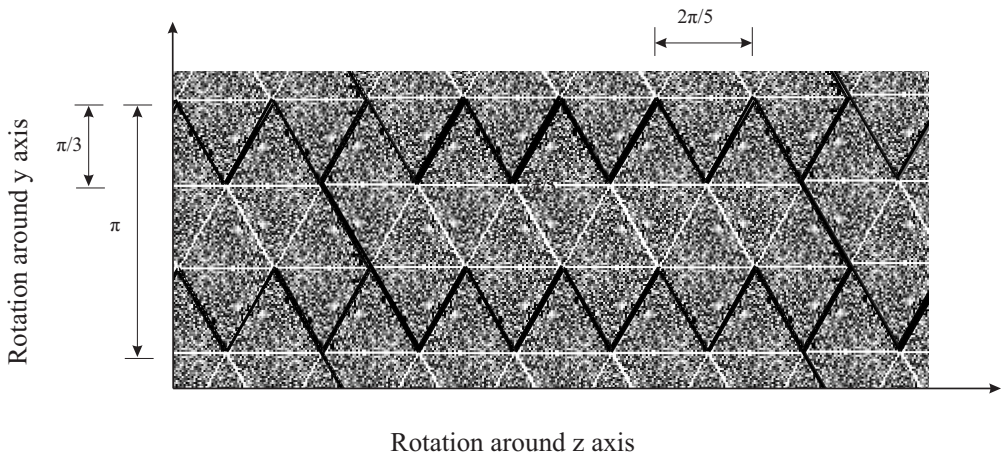


Fig. 4. Surface of the watermark sphere. Because of the symmetry, the rotation around z and y axis should be performed only in the intervals $[0, 2\pi/5]$ and $[0, \pi/3]$ respectively.

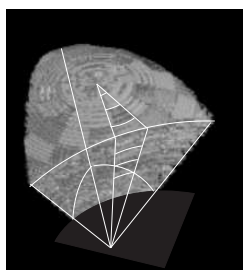
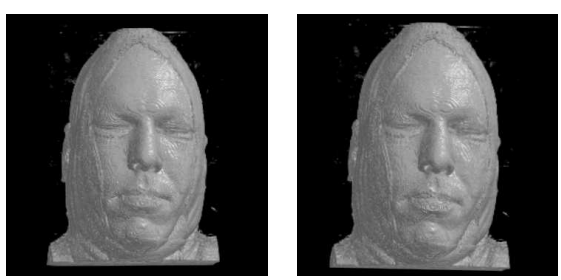
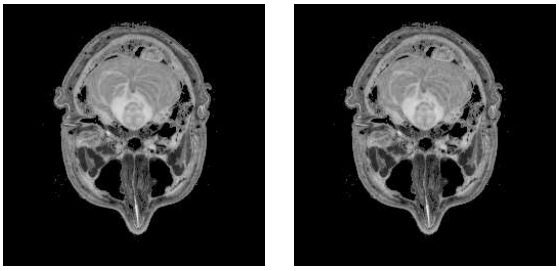


Fig. 5. Pyramid.



(a) (b)

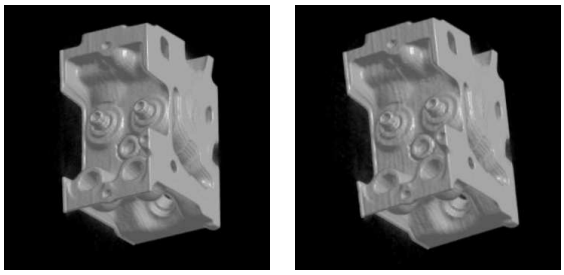
Fig. 6. Frame number 133 of the (a) original volume (b) watermarked



(a) (b)

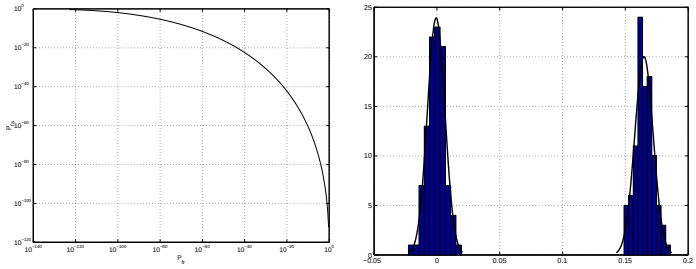
Fig. 7. Frame number 133 of the (a) original volume (b) watermarked

Fig. 8. Absolute difference between Frame number 133 of the original volume and the watermarked volumed multiplied by 20.



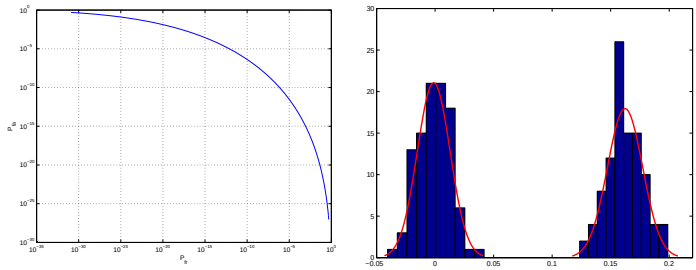
(a) (b)

Fig. 9. Watermarked volume rendering (engine volume)



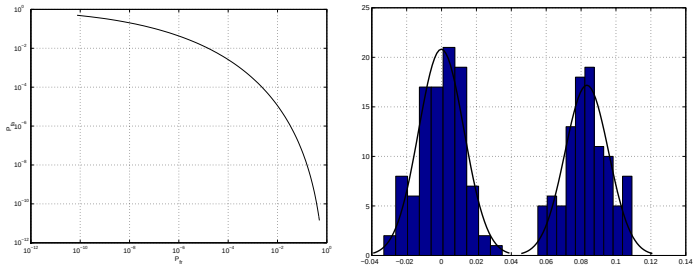
(a) (b)

Fig. 10. ROC curve and histogram of the correlator output (for the head volume)



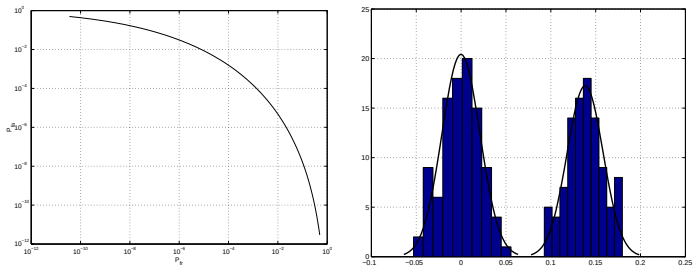
(a) (b)

Fig. 11. ROC curve and histogram of the correlator output (for the engine volume)



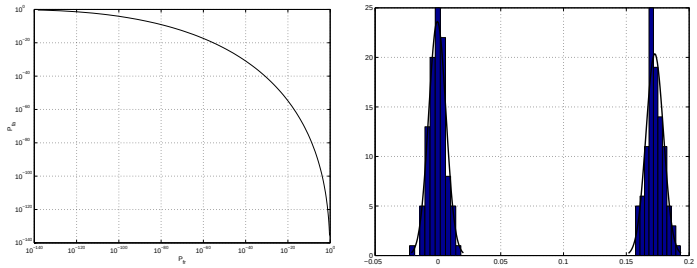
(a) (b)

Fig. 12. ROC curve (a) and distributions (b) of the correlator output after median filtering with window size : $3 \times 3 \times 3$.



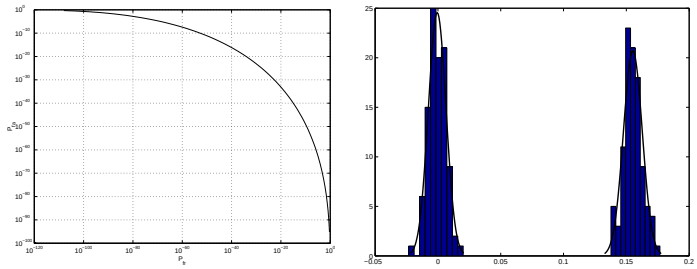
(a) (b)

Fig. 13. ROC curve (a) and distributions (b) of the correlator output after moving average filtering with window size : $3 \times 3 \times 3$.



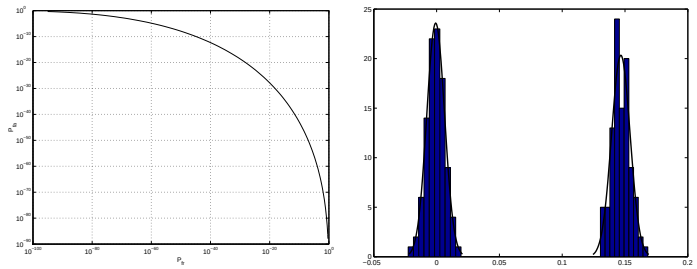
(a) (b)

Fig. 14. ROC curve (a) and distributions (b) of the correlator output after histogram equalization.



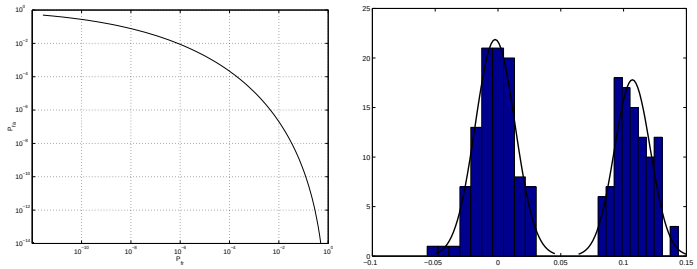
(a) (b)

Fig. 15. ROC curve (a) and distributions (b) of the correlator output after translation of 5 voxels in the x-axis, 10 voxels in the y-axis and 15 voxels in the z-axis.



(a) (b)

Fig. 16. ROC curve (a) and distributions (b) of the correlator output after JPEG compression of each volume frame (frame quality: 60).



(a) (b)

Fig. 17. ROC curve (a) and distributions (b) of the correlator output after 3D scaling (scale factor $\times$ 0.5).

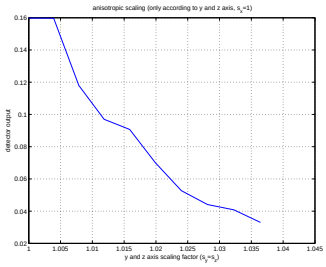
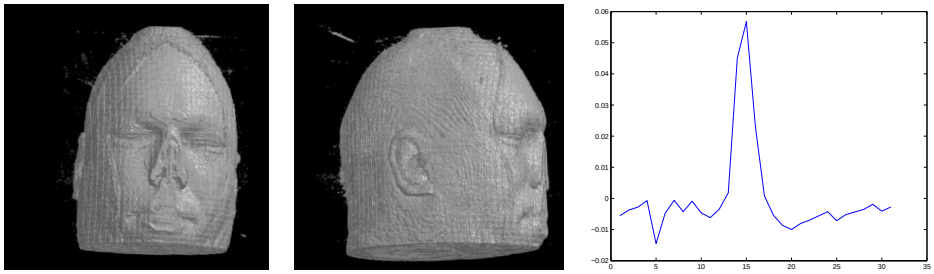
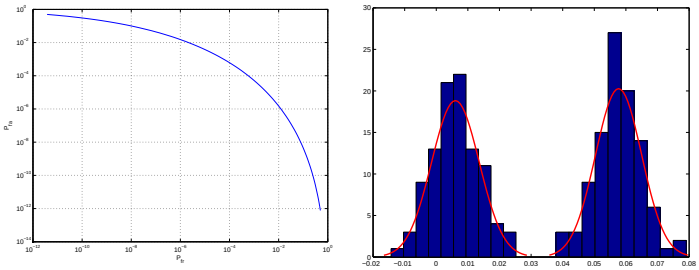


Fig. 18. Detector output after anisotropic scaling attack.



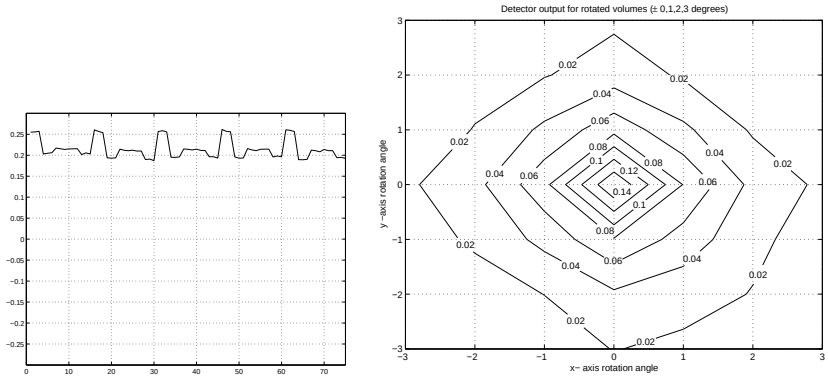
(a) (b)

Fig. 19. Combination attack (3D scaling and cropping) (a,b) attacked volume (two different views), c) detector output for several sampling steps



(a) (b)

Fig. 20. ROC curve (a) and distributions (b) of the correlator output after 3D scaling and cropping (scale factor $\times$ 1.2, cropping 83%)



(a) (b)

Fig. 21. (a)Detector output for various rotations (b) Detector output after small rotation around x and y axis.