WATERMARKING DIGITAL 3D VOLUMES IN THE DISCRETE FOURIER TRANSFORM DOMAIN

Vassilios Solachidis, Ioannis Pitas

Department of Informatics, University of Thessaloniki
Thessaloniki 54124, Greece Tel, Fax: +30-2310996304
e-mail: {vasilis,pitas}@zeus.csd.auth.gr

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 important properties in terms of scaling and rotation invariance. Furthermore, a special symmetry of the watermark is exploited, in order to decrease the detection time. 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.

1. 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.

The limited existing literature with respect to 3D voxel-based watermarking manifests the little attention that has been given to this domain which is very important for medical image copyright protection. In [1], watermarking is used for medical image integrity verification. The watermark insertion is applied in the spatial domain and the extraction can be performed using cryptographic hash functions, parity control or linear block codes. In [2], a 3D voxel based watermarking method is proposed, which is an extension of the 2D watermarking methods in [3], [4]. In [5], another 3D voxel based watermarking method is introduced, which embeds the watermark into the 3D DCT domain of the volume. The watermarked volume is obtained by applying an inverse DCT. A similar approach is presented in [6], where the embedding is performed in the wavelet domain.

In this paper, a 3D volume-based watermarking method is presented. The watermark is embedded into the magnitude of the Fourier transform of the volume. However, the watermark is not embedded into the entire frequency domain, but it is localized between two homocentric spheres. The proposed 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 accelerates the detection procedure significantly, in the case that the watermarked volume has been rotated.

The use of the 3D (icosahedral) watermark symmetry to counter 3D rotation attacks and to reduce the search space for 3D rotation angles is the main novelty of this paper along with the use of the Fourier domain that results in the significant reduction of the detection time of the proposed blind method.

The paper is organized as follows. In Section 2, the properties of the 3D Fourier transform are described. Section 3 describes the watermark construction, embedding and detection procedures, as well as the performance evaluation process. In Section 4, 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 the Fourier transform towards that goal. Finally, in section 5, experimental results and conclusions are presented.

2. 3D FOURIER TRANSFORM PROPERTIES

The 3D Fourier transform has the following properties:

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

$$|DFT[v(n_1+d_1, n_2+d_2, n_3+d_3)]| = M(k_1, k_2, k_3) \quad (1)$$

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

$$DFT[v(sn_1, sn_2, sn_3)] = 1/sV\,(k_1/s, k_2/s, k_3/s) \quad (2)$$

  where s is the scaling factor.
- Rotation in the spatial domain causes the same rotation in the frequency domain:

$$DFT[v([[n_1, n_2, n_3]^T \mathbf{R}_{\theta_x\theta_y\theta_z}]^T)] = V([[k_1, k_2, k_3]^T \mathbf{R}_{\theta_x\theta_y\theta_z}]^T) \quad (3)$$

  where $\mathbf{x}^T$ denotes the transposed vector of $\mathbf{x}$ and $\mathbf{R}_{\theta_x\theta_y\theta_z}$ is the 3D rotation matrix by θ_x, θ_y and θ_z angles around the x, y and z axes respectively.

The work presented was developed within VISNET, a European Network of Excellence (http://www.visnet-noe.org), funded under the European Commission IST FP6 programme.

3. WATERMARK CONSTRUCTION, EMBEDDING, DETECTION AND METHOD EVALUATION

3.1. Watermark construction

The watermark W is a three dimensional bivalued signal, which takes one of the two values, 1 or -1. 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 affect 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 is in the center of the transform domain, the watermark is embedded in a region that covers the middle frequencies:

$$W(r,\phi,\theta) = \begin{cases} 0, & \text{if } r < R_1 \text{ and } r > R_2 \\ \pm 1, & \text{if } R_1 < r < R_2 \end{cases} \quad (4)$$

where $r = \sqrt{k_1^2 + k_2^2 + k_3^2}$, $\theta = \arctan(k_2/k_1)$, $\phi = \arctan\left(k_3/\sqrt{k_1^2 + k_2^2}\right)$. 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 choice of the embedding domain of the watermark, is its symmetry. We construct a symmetrical watermark in order to reduce the search space in the rotation domain $[\theta_x, \theta_y, \theta_z]$. More specifically, a regular polyhedron is selected as symmetrical watermark. Obviously, as the number of the polyhedron edges increases, the rotation search space decreases. Although in the corresponding 2D method [7], a 2D ring is divided into any desirable number of sectors, in the 3D case, the number of the regular polyhedron faces can not be arbitrary. Unfortunately, there is an upper limit for the number of the edges of a regular polyhedron. Hence, the icosahedron illustrated in Figure 1, is the selected regular polyhedron. It can be considered as a union of 20 pyramids where each pyramid has a common face with three others. 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 ($r = \frac{1+\sqrt{5}}{2}$). Thus, the watermark can be considered as an inner shell of an icosahedron, which consists of identical pyramids. The fast watermark detection resulting from the use of icosahedral symmetries is analyzed in Section 4.

3.2. Watermark embedding

Let $v(n_1, n_2, n_3)$ be a $N \times N \times N$ grayscale original volume and $V(k_1, k_2, k_3)$ its Discrete Fourier Transform (DFT). Let also $M(k_1, k_2, k_3) = |V(k_1, k_2, k_3)|$ be the magnitude, $P(k_1, k_2, k_3)$ the phase of $V(k_1, k_2, k_3)$ 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:

$$\begin{aligned} &M'(k_1,k_2,k_3) = \\ &M(k_1,k_2,k_3) + M(k_1,k_2,k_3)W(k_1,k_2,k_3)\cdot p = \\ &M(k_1,k_2,k_3)(1 + W(k_1,k_2,k_3)\cdot p) \end{aligned} \quad (5)$$

where p is a factor that determines the watermark strength. The embedding is performed in a multiplicative way, because this corresponds to a simple watermark masking, i.e., the watermark amplitude increases as the Fourier coefficient magnitude increases.

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

$$v' = IDFT(V'), \quad V' = M'(cos(P) + i\ sin(P)). \quad (6)$$

3.3. Watermark detection

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

$$c = \sum_{k_1=1}^{N}\sum_{k_2=1}^{N}\sum_{k_3=1}^{N} W(k_1,k_2,k_3)M'(k_1,k_2,k_3). \quad (7)$$

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

$$\begin{aligned} c = \sum_{k_1=1}^{N}\sum_{k_2=1}^{N}\sum_{k_3=1}^{N} &(W(k_1,k_2,k_3)M(k_1,k_2,k_3) + \\ &pW(k_1,k_2,k_3)W'(k_1,k_2,k_3)M(k_1,k_2,k_3)) \end{aligned} \quad (8)$$

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

$$\begin{aligned} c = \sum_{k_1=1}^{N}\sum_{k_2=1}^{N}\sum_{k_3=1}^{N} &(W(k_1,k_2,k_3)M(k_1,k_2,k_3) + \\ &pW^2(k_1,k_2,k_3)M(k_1,k_2,k_3)) \end{aligned} \quad (9)$$

Assuming that;

- W, W', M are independent and identically distributed random variables,
- W, W' have zero mean value and are orthogonal to each other,

the mean value μ_c of c is given by:

$$\mu_c = \begin{cases} K \cdot p \cdot \mu_M & \text{if } W = W' \\ 0 & \text{if } W \neq W' \\ 0 & \text{if no watermark is present} \end{cases} \quad (10)$$

where μ_M and σ_M^2 are the mean value and the variance of M, 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 μ_M, we can use $\mu_{M'}$, because:

$\mu_{M'} = \overline{M}(k_1,k_2,k_3) + p\overline{W}(k_1,k_2,k_3))\overline{M}(k_1,k_2,k_3) = \overline{M}(k_1,k_2,k_3) = \mu_M$

3.4. Performance evaluation of the watermarking method

For the performance evaluation of the proposed method, false alarm and false rejection probabilities are used. The watermark detection rule is:
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 a 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 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 detection with erroneous keys (set A) and one for detection with correct keys (set B). In order to estimate the above mentioned probability errors, we approximate the empirical pdf of c_n with a continuous distribution. Assuming that the detector summation terms in (7) are independent and identically distributed (i.i.d.) and using the central limit theorem, it can be derived that both detector output sets (A, B) follow the Gaussian distribution. Given the estimated detector output pdfs, the resulting ROC (Receiver Operating Characteristic) curves are constructed. In order to construct the ROC, the following intervals have to be calculated

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

where $f_1(x)$ and $f_2(x)$ are the theoretical detector output distributions of detector output 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 several values of T.

4. GEOMETRICAL ATTACKS

In this section the effect of geometrical distortions on the embedded watermark are examined and recovery mechanisms are presented. The spherical symmetry is exploited to counter 3D rotation attacks.

4.1. Rotation

The watermark is constructed in such a 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 accelerate the watermark detection process.

Suppose that we have a watermarked volume, rotated by angles θ_x, θ_y and θ_z around x, y and z axes, respectively. Prior to the detection procedure, the watermarked volume should be rotated 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.

4.2. Scaling

Scaling in the spatial domain causes inverse scaling in the frequency domain (2). If 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.

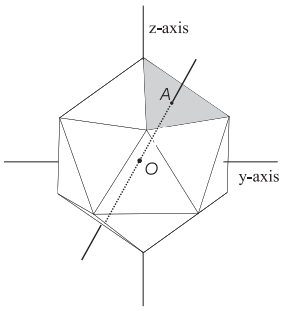

Fig. 1. Icosahedron.

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 constant values. Furthermore, because of the correlator normalization, the correlation output does not depend on the scale factor s.

4.3. 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.

4.4. Translation

In many domains (e.g. medical imaging) where 3D volumes are used, all the useful information lies within the volume objects. Usually, the volume background consists of voxels of uniform luminance (typically 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 (1), the Fourier magnitude remains unaltered after the applying of a circular shift in the spatial domain. Rotation around an arbitrary center is equivalent to rotation around the volume center, followed by translation. Therefore, the proposed method is also robust against such an attack.

5. EXPERIMENTAL RESULTS AND CONCLUSIONS

This method was applied in a number of 3D medical volumes. A gray scale $256 \times 256 \times 256$ volume was used as a host volume in this paper. The watermark was embedded in the object voxels only (non zero), whereas the background voxels (zero) remained unaltered. The number of the non zero voxels of the volume is equal to $4.671.878$, which is only the 27.85% of the total number of the volume voxels. Thus, after the embedding procedure, all the voxels of the watermarked volume were converted to zero valued voxels, if the corresponding voxels of the original volume were zero valued.

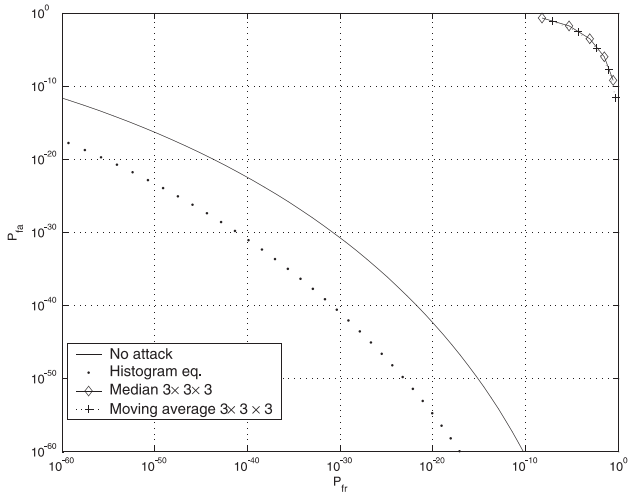

Fig. 2. ROC curves illustrating algorithm performance against attacks.

The embedding power p that was used was equal to 0.3. The SNR during embedding is 31 dB. Therefore, the watermark is expected to be invisible.

It should be noted that 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 filtered or geometrically transformed. Thus, $\hat{P}_{fa} = \hat{P}_{fr} = 0$.

If we approximate the empirical distributions with the continuous ones (subsection 3.4), we can calculate the ROC curves more accurately. The robustness of the 3D watermarking system to various attacks is shown in Figure 2, where ROC curves are plotted. The solid line corresponds to the ROC curve of the detector output in the case of no attack. The dotted line indicates the ROC curve after a histogram equalization attack. In the latter case, the results are better than the no attack one which occures because histogram equalization amplifies middle frequencies and hence the watermark itself. Based on 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. The other two ROC curves correspond to median and moving average filtering. The window size in both filtering processes is $3 \times 3 \times 3$. As can be seen from the figure, the algorithms performance is almost the same after applying these two filtering attacks in the watermarked volume.

Additional tests were performed in order to show the algorithm's efficiency. In case of a translation attack, the method's performance is very good since the EER equals 10^{-27}. The algorithm was also tested against scaling attacks. Experiments were performed using a scale factor equal to 0.5. Because of the fact that the watermark is embedded in the middle frequencies, the detection is robust with an EER equal to 10^{-4}. Furthermore, we have to underline that detection time is not affected by scaling, due to the Fourier properties there is no need for detection for several sampling steps [8].

Finally, in the case of rotation attacks we performed the following tests. The watermarked volume was rotated using suitable angles, so that, due to the watermark symmetry, the detector output would be expected to be greater than 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. For all the above angles, the produced detector output is greater than the threshold, which illustrates that the proposed watermark is robust (due to its symmetry).

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

6. REFERENCES

[1] G.Coatrieux, B.Sankur, and H.Maitre, "Strict integrity control of biomedical images," in *Proceedings of SPIE*, San Jose, CA, USA, January 22-25 2001, vol. 4314.

[2] 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.

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.