3D IMAGE WATERMARKING ROBUST TO GEOMETRIC DISTORTIONS

A. Tefas G. Louizis I. Pitas

Department of Informatics, Aristotle University of Thessaloniki
Box 451, Thessaloniki 54006, GREECE, pitas@zeus.csd.auth.gr

ABSTRACT

A novel blind method for 3D image watermarking robust against geometric distortions is proposed. A ternary watermark is embedded in a grayscale or a color 3D volume. Construction of watermarks having appropriate structure enables fast and robust watermark detection even after several geometric distortions of the watermarked volume. Simulation results indicate the ability of the proposed method to deal with the aforementioned attacks. The proposed method is also robust against lossy compression up to a certain compression ratio. Experiments conducted indicate the superiority of the proposed method.

1. INTRODUCTION

In the last decades massive digitization of multimedia data such as photographs, paintings, speech, music, video, documents, etc., became very popular. New techniques for the representation, storage and distribution of digital multimedia information have been developed. At the same time, the amount of digital data that is distributed through international communication networks has increased rapidly. In such an environment original digital products can be easily copied, tampered and transmitted back to the network. Consequently, the design of robust techniques for copyright protection of multimedia data became necessary.

The main challenge in multimedia watermarking for copyright protection is the robustness of the watermarking techniques against several types of attacks. The attacks that are usually encountered in 3D volume watermarking methods are lossy compression and geometric distortions. Up to now, very little attention has been given to the development of 'real' 3-D voxel watermarking algorithms and this is reflected in the limited existing literature. A method based on spread spectrum watermarking of the 3D DCT coefficients is proposed in [1]. The watermarking technique is a straightforward extension of [2] to 3D data and thus it inherits all its inefficiencies. The watermark bits are first spread by a large spreading factor and then are modulated using pseudorandom noise. The 3D DCT coefficients of the watermark are added to the 3D DCT coefficients of the volume and by inverse 3D DCT the watermarked volume is obtained. In the detection phase the original unwatermarked 3D data is needed. The robustness of this method to geometric distortions seems to be limited. Furthermore, the technique is not blind. A similar approach that exploits embedding in the wavelet domain has been proposed in [3].

In this paper a novel technique for 3D image watermarking robust to geometric distortions is proposed. It is based on an established image watermarking technique [4, 5]. A watermark signal is embedded in the spatial domain using appropriate embedding functions. In the watermark detection the watermark signal is generated and its existence is examined using the corresponding detection functions. The original 3D volume is not necessary during the watermark detection. The novelty of the method is based on the design of a robust watermark having a specific structure that enables fast searching for geometrically distorted versions of the watermark. Thus, the watermark detection speed is increased significantly. The proposed watermarking technique is also robust against lossy compression of the 3D data.

2. WATERMARK GENERATION AND EMBEDDING

The watermark generation procedure aims at generating a three-valued watermark $w(\mathbf{x}) \in \{0, 1, 2\}$, from a volume $f(\mathbf{x})$, given a digital key K. The watermark is a random sequence of three-valued data, thus, it is usually produced by a pseudorandom number generator. An alternative to random number generators is to use chaotic mixing systems or sequences that are produced by chaotic maps having prespecified spectral properties [6, 7].

After the watermark generation we proceed to the watermark embedding by altering the voxels of the original (host) volume according to the following formula:

$$f_w(\mathbf{x}) = \begin{cases} f(\mathbf{x}) & \text{if } w(\mathbf{x}) = 0 \\ g_1(f(\mathbf{x}), \mathcal{N}(\mathbf{x})) & \text{if } w(\mathbf{x}) = 1 \\ g_2(f(\mathbf{x}), \mathcal{N}(\mathbf{x})) & \text{if } w(\mathbf{x}) = 2 \end{cases} \quad (1)$$

where g_1, g_2 are suitably designed functions based on $\mathbf{x}$ and $\mathcal{N}(\mathbf{x})$ denotes a function that depends on the neighborhood

This work has been supported by the European Project IST-1999-10987 CERTIMARK.

of the voxel $\mathbf{x}$. The functions g_1, g_2 are called *embedding functions* and they are selected so as to define an inverse detection function $G(f_w(\mathbf{x}), \mathcal{N}(\mathbf{x}))$. The detection function, when applied to the watermarked volume $f_w(\mathbf{x})$, gives the watermark $w(\mathbf{x})$:

$$G(f_w(\mathbf{x}), \mathcal{N}(\mathbf{x})) = w(\mathbf{x}) \tag{2}$$

Obviously several embedding functions and the appropriate detection function can be designed giving different watermarking schemes. The embedding function used in our method is based on a superposition of real quantities in the voxels to be signed:

$$g_1(f(\mathbf{x}), \mathcal{N}(\mathbf{x})) = \mathcal{N}(\mathbf{x}) \oplus \alpha_1 f(\mathbf{x}) \tag{3}$$

$$g_2(f(\mathbf{x}), \mathcal{N}(\mathbf{x})) = \mathcal{N}(\mathbf{x}) \oplus \alpha_2 f(\mathbf{x}) \tag{4}$$

where α_1, α_2 are suitably chosen constants and $\mathcal{N}(\mathbf{x})$ is local neighborhood operation of the voxels around $\mathbf{x}$. The sign of α_1, α_2 is used for the detection function and its value determines the watermark power.

The size of the region around $\mathbf{x}$ used for the calculation of $\mathcal{N}(\mathbf{x})$ is important for the watermarking procedure. Moreover, the number of voxels used for the calculation of $\mathcal{N}(\mathbf{x})$ determines the upper bound of the number of watermarked voxels in a volume. If a voxel to be signed is contained in the neighboring region of another signed voxel, the related watermark detection may be affected by the neighboring voxel alterations, thus resulting in a false detection. To avoid such problems we should use small watermark embedding neighborhoods (i.e., of size 3 × 3 × 3). The maximum number of voxels that can be signed in a host volume of dimensions $N \times N \times N$ by using blocks of $(2r+1) \times (2r+1) \times (2r+1)$ for calculating $\mathcal{N}(\mathbf{x})$ is given by:

$$k = \frac{N^3}{(r+1)^3} \tag{5}$$

3. WATERMARK DETECTION

In the detection procedure we generate first the watermark $w(\mathbf{x})$ according to the watermark key K. The detection function resulting from (3,4) is defined by:

$$G(f_w(\mathbf{x}), \mathcal{N}(\mathbf{x})) = \begin{cases} 1 & \text{if } f_w(\mathbf{x}) - \mathcal{N}(\mathbf{x}) > 0 \\ 2 & \text{if } f_w(\mathbf{x}) - \mathcal{N}(\mathbf{x}) < 0 \end{cases} \tag{6}$$

The detection function is valid if $\alpha_1 > 0$ and $\alpha_2 < 0$. This fact should be accounted for the design of the embedding functions. By employing the detection function in the watermarked volume a bi-valued detection volume $d(\mathbf{x})$ is produced:

$$d(\mathbf{x}) = G(f_w(\mathbf{x}), \mathcal{N}(\mathbf{x})) \tag{7}$$

Based on the watermark $w(\mathbf{x})$ and the detection volume $d(\mathbf{x})$, we can decide whether the watermark under investigation is embedded in the volume or not. The detection is based on the voxel to voxel comparison for the nonzero voxels in $w(\mathbf{x})$. By comparing the watermark $w(\mathbf{x})$ and the detection volume $d(\mathbf{x})$ we form the false detection volume:

$$e_w(\mathbf{x}) = \begin{cases} 1 & \text{if } \ w(\mathbf{x}) \neq 0 \ \text{ and } \ w(\mathbf{x}) \neq d(\mathbf{x}) \\ 0 & \text{otherwise} \end{cases} \tag{8}$$

The false detection volume has value 1 (white voxels) if a watermarked voxel is falsely detected and 0 otherwise. The detection ratio is given by the ratio of the correctly detected voxels to the sum of the watermarked voxels in the image.

$$D_w = 1 - \frac{\text{card}\{e_w(\mathbf{x})\}}{\text{card}\{w(\mathbf{x})\}} \tag{9}$$

The embedding functions are designed in such way, so as the probability p of a voxel to be detected as signed with g_1 or g_2, for an unwatermarked volume, to be 0.5. Thus, the detection ratio in an unwatermarked volume forms a binomial distribution. The cumulative distribution function (*cdf*) of the watermark detection ratio is given by:

$$P_n = p^k \sum_{i=0}^{n} \frac{k!}{i!(k-i)!} \tag{10}$$

where k is the total number of the watermarked voxels and n is the number of correctly detected watermarked voxels.

The decision about the volume ownership is taken by comparing the watermark detection ratio of the volume to a predefined threshold T. The value of the threshold determines the minimum acceptable level of watermark detection.

4. ROBUSTNESS TO GEOMETRIC DISTORTIONS

The proposed watermarking algorithm is adequate for progressive watermark detection. By the term progressive watermark detection we mean that under certain conditions the watermark detection procedure is not necessary to be performed to the entire volume. That is, the watermark detection in a small region of the volume is sufficient for deciding whether the volume is watermarked or not. The minimum size of the search region depends on the minimum number of watermarked voxels needed for the detection procedure. In order to estimate the minimum number of watermarked voxels needed for the detection procedure we can condition the minimum acceptable false watermark acceptance probability. Let us denote by ϵ_1 the upper bound of false watermark acceptance probability (ϵ_1 is usually set equal to 10^{-4}):

$$Pr\left\{D_{w_i} > T\right\} < \epsilon_1, \quad \forall w_i \neq w \tag{11}$$

where T is the watermark detection threshold and w is the correct watermark.

The watermark detection ratio, for a watermark other than the one embedded in the volume or for an unwatermarked volume, follows (10). Thus, equation (11) can be rewritten as:

$$\frac{1}{2^m} \sum_{i=Tm}^{m} \frac{m!}{i!(m-i)!} < \epsilon_1 \tag{12}$$

By using DeMoivre-Laplace theorem [8] it follows that:

$$\mathbf{G}\left\{\frac{Tm - 0.5m}{0.5\sqrt{m}}\right\} > 1 - \epsilon_1 \tag{13}$$

and the minimum number m of watermarked voxels needed for the watermark detection is:

$$m > \left(\frac{\text{erfinv}(0.5 - \epsilon_1)}{2T - 1}\right)^2 \tag{14}$$

where erfinv is the inverse function of the error function:

$$\text{erf}\, x = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-y^2/2} dy \tag{15}$$

The *Receiver Operating Characteristic* (ROC) curves for several basic watermark sizes are plotted in Figure 1.

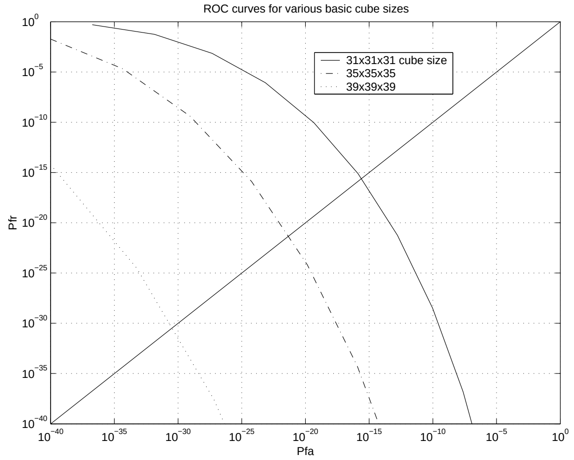

Fig. 1. Minimum number of watermarked voxels needed for progressive detection. ROC curves for several basic watermark sizes.

It is obvious from the plots that a region of approximately $31 \times 31 \times 31$ is sufficient for watermark detection. The Equal Error Rate (EER) in this case is 10^{-16}. The number of watermarked voxels used for detection in that case is approximately 300 and depends on the watermark key.

The proposed algorithm allows very fast watermark detection thus enabling correct watermark detection for several geometric distortions of the watermarked volume. Specifically, the detection of a watermark of size $31 \times 31 \times 31$ shifted to every voxel of a volume is performed in a few seconds. That is, robustness against image cropping is achieved by exhaustive search of the watermark in the test volume. Accordingly, the watermark detection for several geometric distortions, like scaling and rotation, of the watermarked image is completed in ≈ 1min.

The speed of the proposed algorithm is further improved by constructing watermark signals of specific structures. That is, the watermark is embedded more than one times in the host volume since its size is much smaller than the size of the host volume. If the host volume is larger than the watermark then the watermark is embedded at several non-overlapping regions of the host volume until the entire volume is covered. The copies of the watermark that are embedded in the volume are rotated versions of the original basic watermark. Thus, searching for rotated versions of the watermark in the detection procedure can be applied in a reduced search space, enabling faster detection. For example in a volume of size $128 \times 128 \times 128$ a watermark of size $31 \times 31 \times 31$ can be embedded 125 times with partial overlapping. Thus, 125 rotated versions of the original watermark can be embedded in the volume. The watermark of size $31 \times 31 \times 31$ is robust against rotation of $\pm 2°$ in all directions. Thus, the constructed watermark that comprises of 125 basic watermarks is robust against rotation of $\pm 10°$ in all directions.

5. EXPERIMENTAL RESULTS

The proposed 3D image watermarking technique has been tested in real medical data. A test volume comprised of 128 slices of size 128×128 has been used for testing the algorithm. The watermark embedding power used was 45dB in PSNR. Using this embedding power the watermark is perceptually invisible.

The proposed watermarking method has been tested for robustness against JPEG compression of the volume slices. That is, each slice of the watermarked volume has been JPEG compressed with 80, 85 and 90 quality factor before watermark detection. ROC curves for this test are shown in Figure 2. As illustrated in the figure, the performance of the method decreases as the compression ratio increases. However, even in the case of 1:15 JPEG compression ratio (JPEG factor = 80), the EER of the system is 10^{-4}.

Robustness against geometric distortions of the watermarked volume is achieved by searching for the basic watermark in a reduced space as described in Section 4.

In order to test the performance of the proposed method against scaling attacks the watermarked volume was scaled with factor f, rescaled with factor $1/f$ and the final volume was exhaustively searched for basic watermark existence (first order interpolation has been used in all scaling transformations). The corresponding ROC curves are shown in Figure 3. It can be easily observed that the method's perfor-

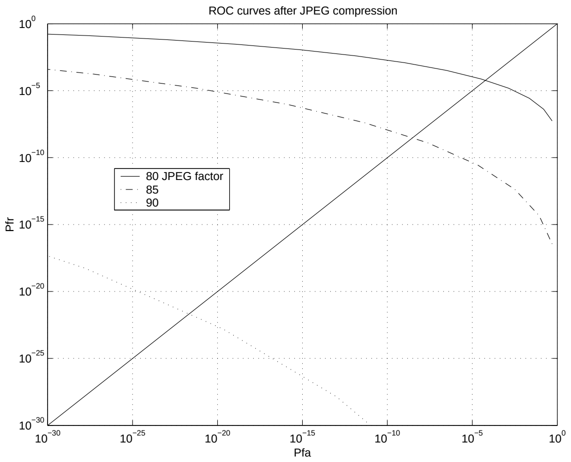

Fig. 2. Detector performance after JPEG compression of the watermarked volume slices.

mance in upsampling ($f > 1$) is very high. However, the performance decreases for $f < 1$ due to information loss caused by downsampling. Robustness to downsampling is increased when the watermark embedding power is raised (e.g., to PSNR≈40dB).

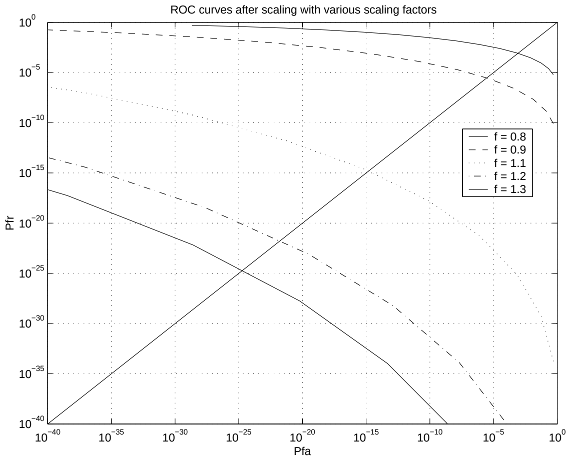

Fig. 3. Detector performance after scaling the watermarked volume.

Robustness against scaling is achieved by searching for the basic watermark in scaled versions of the test volume. The scaled versions are created successively by varying the scaling factor, using a certain step. The maximum allowable value of that step was computed to be $9/256$.

It is worth noting that for medical images the visual quality of the image sequences should be very high. Thus, the acceptable compression and downsampling usually lie in a range at which the quality of the image sequence is not degraded much. At this range the proposed method's robustness is sufficient for reliable watermark detection.

6. CONCLUSIONS

A blind 3D image watermarking method has been proposed for copyright protection. The minimum number of watermarked voxels needed for reliable watermark detection has been theoretically derived and embedding of rotated versions of a smaller basic watermark has been enabled. A progressive watermark detection technique for fast and robust watermark detection after several geometric distortions of the watermarked volume has also been proposed. The major advantage of the proposed method is its robustness against geometric distortions and lossy compression up to a certain compression ratio.

7. REFERENCES

[1] 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. Computer Graphics International CGI 2001*, July 2001, pp. 347–350.

[2] 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.

[3] X. Guan, M.S. Kankanhalli Y. Wu, and Z.Y. Huang, "Invisible watermarking of volume data using wavelet transform," in *International Conference on Multimedia Modeling MMM2000*, Nagoya, Japan, November 2000, pp. 153–166.

[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, 7-11 May 2001.

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

[6] N. Nikolaidis, S. Tsekeridou, A. Nikolaidis, A. Tefas, V. Solachidis, and I. Pitas, "Applications of chaotic signal processing techniques to multimedia watermarking," in *Proceedings of the IEEE workshop on Nonlinear Dynamics in Electronic Systems*, Catania Italy, May 18-20 2000, pp. 1–7.

[7] A. Tefas, A. Nikolaidis, N. Nikolaidis, V. Solachidis, S. Tsekeridou, and I. Pitas, "Statistical analysis of markov chaotic sequences for watermarking applications," in *2001 IEEE International Symposium on Circuits and Systems (ISCAS 2001)*, Sydney, Australia, May 6-9 2001.

[8] A. Papoulis, *Probability, Random Variables and Stochastic Processes*, McGraw-Hill, New York, 1991.