COPYRIGHT PROTECTION OF 3D IMAGES USING WATERMARKS OF SPECIFIC SPATIAL STRUCTURE

Giorgos Louizis, Anastasios Tefas and Ioannis 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.

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.

Robustness of the watermarking techniques against several types of attacks is the main challenge in multimedia watermarking for copyright protection. 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 3D image (voxel-based) 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

The watermark generation procedure aims at generating, primary, a three-valued basic watermark $w(\mathbf{x}) \in \{-1, 0, 1\}$ of size $\mathbf{S} = [S\ S\ S]^T$ 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 generation of $w(\mathbf{x})$, a watermark volume $w_f(\mathbf{x})$ of specific structure is constructed from $w(\mathbf{x})$ in three steps. The volume $w_f(\mathbf{x})$ has the same size $\mathbf{F} = [F_1\ F_2\ F_3]^T$ as the original (host) volume $f(\mathbf{x})$ to be watermarked, where F_1, F_2, F_3 are the dimensions of the original volume.

In the first step, the basic watermark $w(\mathbf{x})$ is shaped into

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

sphere as follows:

$$w_s(\mathbf{x}) = \begin{cases} w(\mathbf{x}) & \text{if } ||\mathbf{x} - \frac{\mathbf{S}}{2}|| \leq \frac{S}{2} \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

where $||\cdot||$ is the Euclidean distance. This shaping ($w(\mathbf{x}) \rightarrow w_s(\mathbf{x})$) is performed in order to avoid data loss after rotation of the basic watermark.

In the second step an intermediate watermark volume $w_m(\mathbf{x})$ of size $\mathbf{M} = [M\ M\ M]^T$, $M > S$, is constructed from $w_s(\mathbf{x})$. The volume $w_m(\mathbf{x})$ is comprised of several non-overlapping copies of $w_s(\mathbf{x})$. These copies are rotated versions of the original $w_s(\mathbf{x})$ by angles multiple of a step angle ϑ. The structure of the intermediate watermark $w_m(\mathbf{x})$ is formed as follows:

$$w_m(\mathbf{x}) = w_s(\ R(\ \mathbf{x} \bmod S,\ \vartheta\ [(\mathbf{x} \operatorname{div} S) - \boldsymbol{\alpha}]\ )\ ) \quad (2)$$

where $R(\mathbf{v}, \boldsymbol{\varphi})$ is a function rotating vector $\mathbf{v}$ by angle $\boldsymbol{\varphi}$ and $\boldsymbol{\alpha} = (\frac{\mathbf{M}}{2} \operatorname{div} S)$.

Finally, in the third step $w_f(\mathbf{x})$ is constructed by covering the entire volume with non-overlapping copies of $w_m(\mathbf{x})$.

$$w_f(\mathbf{x}) = w_m(\mathbf{x} \bmod M) \quad (3)$$

3. WATERMARK EMBEDDING

After the watermark generation we proceed to the watermark embedding by altering the voxels of the host volume $f(\mathbf{x})$ according to the following formula:

$$f_w(\mathbf{x}) = \begin{cases} f(\mathbf{x}) & \text{if } w_f(\mathbf{x}) = 0 \\ m(\mathbf{x}, f(\mathbf{x})) \oplus p\ w_f(\mathbf{x}) & \text{if } w_f(\mathbf{x}) = \pm 1 \end{cases} \quad (4)$$

where $m(\mathbf{x}, f(\mathbf{x}))$ denotes a function that depends on the neighborhood of voxel $\mathbf{x}$ in volume $f(\mathbf{x})$. The embedding formula used in our method is based on superposition ($\oplus$) of real quantities on the voxels to be signed, and p is a suitably chosen constant whose value determines the watermark power.

The size of the region of $f(\mathbf{x})$ around $\mathbf{x}$ used for the calculation of $m(\mathbf{x}, f(\mathbf{x}))$ is important for the watermarking procedure. Moreover, the number of voxels used for the calculation of $m(\mathbf{x}, f(\mathbf{x}))$ 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 $3 \times 3 \times 3$).

4. WATERMARK DETECTION

In the detection procedure we generate, first, the basic watermark volume $w_s(\mathbf{x})$ according to the watermark key K. Then, the bi-valued detection volume $d(\mathbf{x})$ is produced:

$$d(\mathbf{x}) = \begin{cases} 1 & \text{if } f_w(\mathbf{x}) - m(\mathbf{x}, f_w(\mathbf{x})) > 0 \\ -1 & \text{if } f_w(\mathbf{x}) - m(\mathbf{x}, f_w(\mathbf{x})) < 0 \end{cases} \quad (5)$$

Based on the basic watermark $w_s(\mathbf{x})$ 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 non-zero voxels of $w_s(\mathbf{x})$. By comparing the watermark $w_s(\mathbf{x})$ with the detection volume $d(\mathbf{x})$, the false detection volume $e(\mathbf{x})$ is formed. Usually, the size of $f_w(\mathbf{x})$, and therefore the size of $d(\mathbf{x})$, is greater than that of $w_s(\mathbf{x})$. Thus, $w_s(\mathbf{x})$ must be compared to every possible shifted version of $d(\mathbf{x})$. That is, $\forall\ \mathbf{i} \in [\mathbf{0},\ \mathbf{F} - \mathbf{S}]$:

$$e_{\mathbf{i}}(\mathbf{x}) = \begin{cases} 1 & \text{if } w_s(\mathbf{x}) \neq 0 \text{ and } d(\mathbf{x} + \mathbf{i}) \neq w_s(\mathbf{x}) \\ 0 & \text{otherwise} \end{cases} \quad (6)$$

The false detection volume has value 1 if a watermarked voxel is falsely detected and 0 otherwise. The detection ratio $D_{\mathbf{i}}$, for each $\mathbf{i}$, is given by the ratio of correctly detected voxels to the sum of watermarked voxels in the volume caused by the embedding of one basic watermark $w_s(\mathbf{x})$.

$$D_{\mathbf{i}} = 1 - \frac{\operatorname{card}\{e_{\mathbf{i}}(\mathbf{x})\}}{\operatorname{card}\{w_s(\mathbf{x})\}} \quad (7)$$

The detection ratio D of the detection procedure on the entire volume $f_w(\mathbf{x})$ is:

$$D = \max_{\mathbf{i}} D_{\mathbf{i}} \quad (8)$$

The embedding formula is designed in such way, so as the probability of a voxel to be detected as signed with $w_s(\mathbf{x}) = -1$ or $w_s(\mathbf{x}) = 1$, for an unwatermarked volume, to be 0.5. Thus, the detection ratio in an unwatermarked volume forms a binomial distribution [4].

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

5. 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 and is theoretically computed in [4].

The *Receiver Operating Characteristic* (ROC) curves for several sizes S of $w_s(\mathbf{x})$, after JPEG compression of the watermarked volume slices with 90 quality factor, are plotted in Figure 1. 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^{-25}. The number of watermarked voxels ($\mathrm{card}\{w_s(\mathbf{x})\}$) used for detection in that case is approximately 300 and depends on the watermark key.

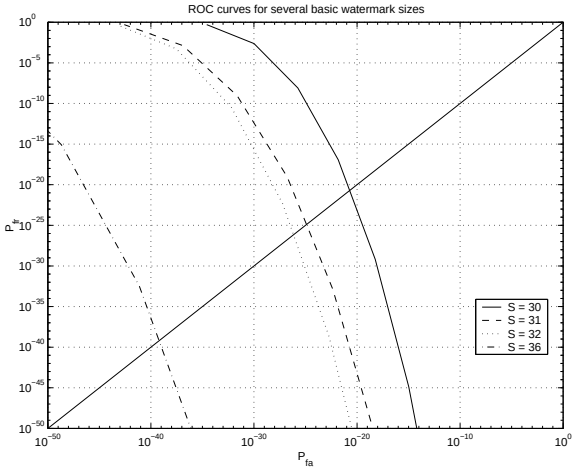

Figure 1: Minimum number of watermarked voxels needed for progressive detection. ROC curves for several basic watermark sizes.

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 basic watermark $w_s(\mathbf{x})$ of size $\mathbf{S} = [31\ 31\ 31]^T$ 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 $w_s(\mathbf{x})$ in the test volume. Accordingly, the watermark detection for several geometric distortions, like scaling and rotation, of the watermarked image is completed in $\approx 1\mathrm{min}$.

The speed of the proposed algorithm is further improved by the specific structure of the watermark signal proposed in Section 2. Thus, searching for rotated versions of the basic 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 volume $w_m(\mathbf{x})$ of size $\mathbf{M} = [128\ 128\ 128]^T$ can be embedded. In a watermark $w_m(\mathbf{x})$ of this size, a basic watermark $w_s(\mathbf{x})$ of size $\mathbf{S} = [31\ 31\ 31]^T$ can be inserted 125 times with partial overlapping. Thus, 125 rotated versions of $w_s(\mathbf{x})$ can be embedded in the volume. The basic watermark $w_s(\mathbf{x})$ of size $\mathbf{S} = [31\ 31\ 31]^T$ is robust against rotation of $\pm 2^\circ$ in all directions. Thus, by setting ϑ equal to 4° in (2), the constructed watermark $w_m(\mathbf{x})$ that comprises of 125 basic watermarks is robust against rotation of $\pm 10^\circ$ in all directions.

6. 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 the experiments presented in this section. The watermark embedding power used in all the experiments 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 70, 75, 80 and 85 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 $= 70$), the EER of the system is 10^{-4}.

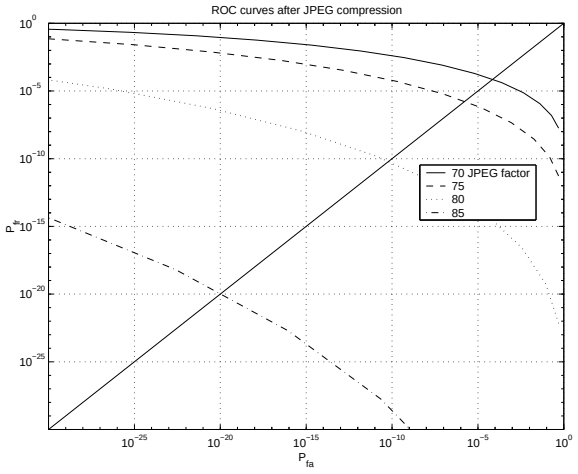

Figure 2: Detector performance after JPEG compression of the watermarked volume slices.

Robustness against geometric distortions of the watermarked volume is achieved by searching for the basic watermark in a reduced space as described in Section 5.

The efficiency of the special structure of $w_f(\mathbf{x})$ was tested by searching for $w_s(\mathbf{x})$ in rotated (with first order interpolation) versions of the watermarked volume. The results of this experiment are shown in Figure 3. It is obvious from the plots that the system performs well even after 10° rotation of the watermarked volume (EER $\approx 10^{-6}$).

In order to test the performance of the proposed method against scaling attacks, the watermarked volume was scaled with factor h, rescaled with factor $1/h$ and the final volume was exhaustively searched for basic watermark existence

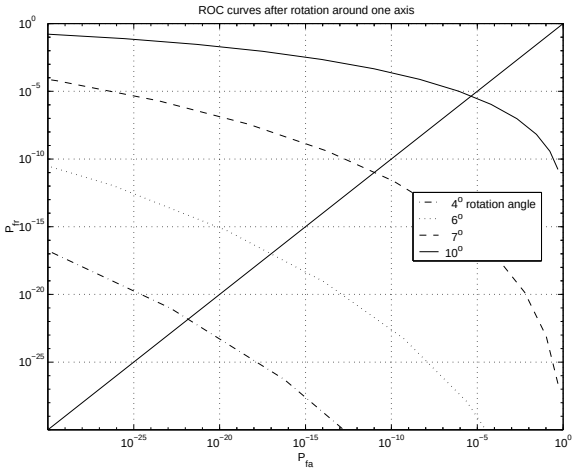

Figure 3: Detector performance after rotation of the watermarked volume.

(first order interpolation has been used in all scaling transformations). The corresponding ROC curves are shown in Figure 4. It can be easily observed that the method's performance in upsampling ($h > 1$) is very high. However, the performance decreases for $h < 1$ due to information loss caused by downsampling. Robustness to downsampling is increased when the watermark embedding power is raised (e.g., to PSNR ≈ 40dB).

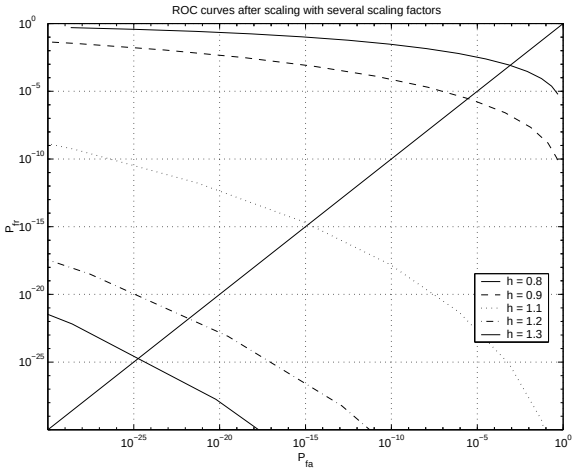

Figure 4: Detector performance after scaling of the watermarked volume.

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.

7. CONCLUSIONS

A blind 3D image watermarking method in the spatial domain has been proposed for copyright protection. A watermark signal of specific structure has been presented. 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.

8. 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.