Robust Invisible Watermarking of Volume Data

Yinghui Wu[1], *Xin Guan*[2], *Mohan S Kankanhalli*[1], *Zhiyong Huang*[1]
School of Computing[1] Dept. of Computational Science[2]
National University of Singapore, Singapore 119260
Email: huangzy@comp.nus.edu.sg

1 Introduction

Digitizing of visual data such as images and video has effected a dual impact. While on one hand it has enabled faster and more efficient storage, transfer and processing, on the other hand duplication and manipulation of such data has also become very easy and undetectable. Security concerns over copyright violation of visual data have also increased with the growth of computer networks that enable fast and error free movement of any unauthorized duplicate and possibly manipulated copy of visual information. The only solution appears to be to cement into the visual data a secondary signal that is not perceivable and is bonded so well with the original data that it is inseparable and survives any kind of signal processing. Techniques to embed/retrieve such a stamp or secondary information (*watermark*), that conveys some information about the intended recipient or the lawful owner of the original data, have been of considerable research interest [2, 6]. However, this work has been mostly confined to visual data such as digital images [8] and digital video [5]. Recently, there have been novel techniques proposed for watermarking computer graphics data such as arbitrary triangle meshes [1, 9]. However, there has been hardly any work in the watermarking of 3D volume data.

We would like to develop a technique for watermarking of 3D volume data which is *invisible* and *robust*. By "invisible", we mean that the 2D volume rendered image of this watermarked volume data should be *perceptually indistinguishable* from the 2D volume rendered image of the original volume data (assuming that all the other rendering parameters are unchanged). "Robust" watermarking implies that the embedded invisible watermark should be resistant to intentional or unintentional attacks such as:

- Geometrical distortions: spatial scaling, cropping of a region of the volume, translations, cut and paste to another volume.
- Addition of a constant offset to the voxel values.
- Addition of Gaussian or non-Gaussian noise.
- Linear filtering such as low pass or high pass filtering.
- Non-linear filtering such as median filtering.
- Local exchange of voxel rows/columns.
- Quantization and requantization.
- Digital to Analog and Analog to Digital conversion.

It must be noted that if a particularly strong attack manages to remove the watermark from the volume data, then the quality of its 2D volume rendered images should be sufficiently degraded so as to make this tampered data useless. We have developed a novel algorithm based on the spread-spectrum communication technique [4] that addresses these concerns.

2 The Volume Watermarking Technique

Watermarking a volume data-set is essentially the process of altering the voxel values in a manner that ensures that a viewer of its volume-rendered image does not notice any perceptual change between the original volume rendering and the watermarked volume rendering. We utilize the spread-spectrum technique in the frequency domain in order to achieve this effect [3, 4]. The purpose of utilizing the frequency domain is to make the watermark robust by hiding it in multiple frequencies. Assume that volume V that needs to be watermarked is of the size $n_x \times n_y \times n_z$. The basic scheme of our watermarking technique is outlined below:

1. A $4 \times 4 \times 4$ block-based 3D discrete cosine transform (DCT) transform [10] is applied to the volume V. The $4 \times 4 \times 4$ 3D DCT is computed using:

$$F(u,v,w) = \frac{1}{2\sqrt{2}} C(u)C(v)C(w)\Big[\sum_{x=0}^{3}\sum_{y=0}^{3}\sum_{z=0}^{3} f(x,y,z) * cos\frac{(2x+1)u\pi}{8} cos\frac{(2y+1)v\pi}{8} cos\frac{(2z+1)w\pi}{8}\Big]$$

where

$$C(u), C(v), C(w) = \begin{cases} \frac{1}{2\sqrt{2}} & u,v,w = 0 \\ 1 & otherwise \end{cases}$$

Note that in our case $f(x, y, z)$ corresponds to the voxel values and $F(u, v, w)$ corresponds to the 3D DCT coefficients. The $4 \times 4 \times 4$ block-size has been chosen as a trade-off between the computational complexity of the transform and the availability of sufficient frequencies to hide the watermark.

2. To embed the watermark information bits $a_j \in \{1, -1\}$ the bits are first spread by a large spread factor cr , called the chiprate [4]. For spreading the information, the bit pattern is repeated in a raster-scan order to tile the entire volume of size $n_x \times n_y \times n_z$. This improves its robustness to geometrical attacks such as cropping. The spreading provides for spatial redundancy by embedding the information bits into cr number of voxels:

$$b_i = a_j \quad \forall i = j \times K \tag{1}$$

and K varying from 1 to cr. The spread bits b_i are then modulated with a pseudo-random-noise (PN) sequence.

$$p_i \text{ where } p_i \in \{-1, 1\} \tag{2}$$

This forms the basic watermark sequence.

3. The modulated signal, i. e. the watermark sequence w_i where $w_i = b_i \cdot p_i$, thus forms a volume W of size $n_x \times n_y \times n_z$. This watermark volume W is also transformed into the frequency domain by using a $4 \times 4 \times 4$ block-based 3D DCT transform.

4. For every DCT block $b_i^V \in V$ and the corresponding DCT block $b_i^W \in W$, the corresponding coefficients are added to form a watermarked block $b_i^{V'} = b_i^V + b_i^W$ which constitute the watermarked volume V'_{DCT} in the frequency domain.

5. The 3D inverse DCT is performed on V'_{DCT} to obtain a $n_x \times n_y \times n_z$ size volume V'. The inverse 3D DCT is done using:

$$f(x,y,z) = \frac{1}{2\sqrt{2}}[\sum_{u=0}^{3}\sum_{v=0}^{3}\sum_{w=0}^{3} C(u)C(v)C(w)F(u,v,w) * cos\frac{(2x+1)u\pi}{8} cos\frac{(2y+1)v\pi}{8} cos\frac{(2z+1)w\pi}{8}]$$

This new volume V' is the watermarked volume data corresponding to the original volume data V.

For any given set of volume rendering parameters, the 2D image produced by volume rendering on V' will be perceptually indistinguishable from the 2D image produced using V. Since a pseudo-noise sequence is used for modulation, the watermark sequence is also noise-like which ensures that the watermark is difficult to detect, locate and manipulate without compromising on the corresponding volume-rendered image quality.

2.1 Watermark Detection

For detecting the existence of the watermark, the DCT-transformed original volume data is subtracted from the DCT-transformed watermarked volume data $\hat{V}'$ (we use $\hat{V}'$ instead of V' because it may have been subjected to attacks) to obtain the residual volume data DCT coefficients, i.e. $V^r = \hat{V}' - V$. The 3D inverse DCT is performed on this residual data V^r to obtain the residual watermark sequence $\hat{w}_i$. This $\hat{w}_i$ is then analyzed by correlating it with the same pseudo-noise sequence that was used in the embedding phase where correlation can be understood as demodulation followed by summation over the correlation window. The correlation window for each bit is the chiprate. If the peak of correlation is positive, the corresponding watermark bit is $+1$ else it is -1. Considering one subset of the watermark values $\hat{w}_i$ over the correlation window where $i \in 1 \ldots cr$

$$s_j = \sum_{i=1}^{cr} p_i \cdot \hat{w}_i = \sum_{i=1}^{cr} p_i^2 \cdot b_i + \Delta \tag{3}$$

Δ being the error term which can be due to intentional or unintentional attacks. But by choosing a large cr we have adequate redundancy and the summation can be approximated as :

$$s_j = \sum_{i=1}^{cr} p_i \cdot \hat{w}_i \approx cr \cdot a_j \tag{4}$$

The required information bit $\hat{a_j}$ (i.e. the detected watermark bit) is

$$\hat{a_j} = sign(s_j) \tag{5}$$

Thus, to retrieve the watermark, the original volume data and the same unshifted pseudo-noise sequence that was used at the embedder are required.

3 Results and Discussion

We have implemented the volume watermarking technique as a C++ program and we have used the *PKVox* software [7] for performing the volume rendering. The quality of the watermarked image appears unaltered as in fig 1. The images on the left-side are volume rendered images of the *original* skull volume data set whose size is $64 \times 64 \times 64$. A 170-byte watermark was embedded into this volume data set using the proposed technique. The images on the right are the volume rendered images of the *watermarked* skull volume data set. Our initial experimentation suggests that the watermarking technique is robust to the attacks outlined in the introduction. We have done extensive experiments which indicate that the perceptual quality of the volume-rendered images of the watermarked volume data sets is largely unchanged. We are still refining our technique and doing further experiments to test the robustness against various attacks.

References

[1] O Benedens. Geometry-based Watermarking of 3D Models. *IEEE Computer Graphics & Applications*, Vol. 19, No.1, pp. 46-55. January/February 1999.

[2] L Boney, A H Tewfik and K Hamdy. Digital Watermarks for Audio Signals. *Proceedings of 1996 IEEE International Conference on Multimedia Computing and Systems ICMCS'96*, Hiroshima Japan, pp. 473-480, July 1996.

[3] I Cox, J Killian, 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.

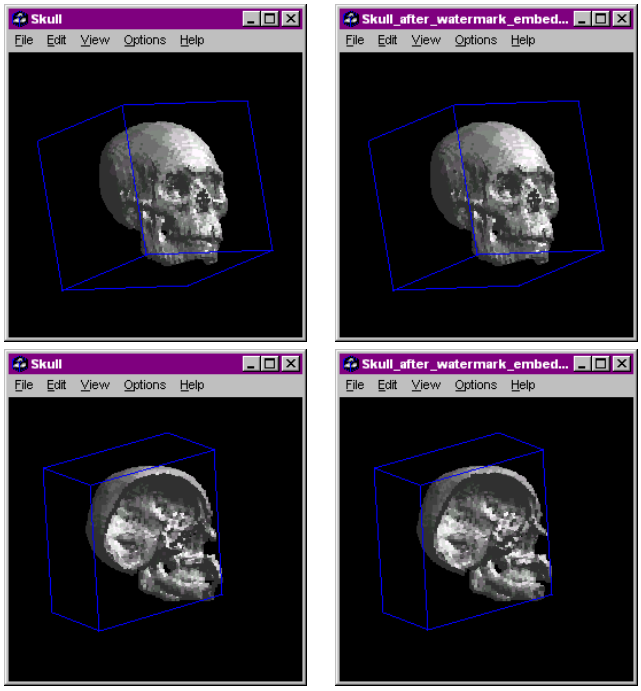

Figure 1: Volume rendered images of original volume (left) and watermarked volume (right)

[4] I Cox, M Miller and A McKellips. Watermarking as Communications with Side Information. *Proceedings of the IEEE*, Vol. 87, No. 7, pp. 1127-1141, July 1999.

[5] J Dittman, M Stabenau and R Steinmetz. Robust MPEG Video Watermarking Technologies. *Proceedings of the Sixth ACM International Multimedia Conference – ACM MM'98*, Bristol, UK, pp. 71-80, September 1998.

[6] F Hartung and M Kutter. Multimedia Watermarking Techniques. *Proceedings of the IEEE*, Vol. 87, No. 7, pp. 1079-1107, July 1999.

[7] P Kahler. PKVox: Advanced Volumetric Data Manipulation Software. (http://www.oakland.edu/~phkahler/vox/index.html)

[8] M S Kankanhalli, Rajmohan, and K R Ramakrishnan. Content-based Watermarking of Images. *Proceedings of the Sixth ACM International Multimedia Conference – ACM MM'98*, Bristol, UK, pp. 61-70, September 1998.

[9] E Praun, H Hoppe and A Finkelstein. Robust Mesh Watermarking *Computer Graphics – SIGGRAPH 1999 Proceedings*, pp. 69-76, September 1999.

[10] K Rao and P Yip. *Discrete Cosine Transform: Algorithms, Advantages, Applications*. Academic Press Inc., 1990.