Authentication of Volume Data

Mohan S. Kankanhalli Ee-Chien Chang Xin Guan Zhiyong Huang Yinghui Wu

School of Computing, National University of Singapore, Singapore 117543
mohan@comp.nus.edu.sg

3D volume data is being increasingly used in many applications. The digital nature of the data allows easy creation, copying and distribution. However, it also allows ease of manipulation which can enable wilful or inadvertent misrepresentation of the content. For an application like medical imaging, this can have serious diagnostic and legal implications. Thus there is a strong need to establish the integrity of a particular volume data set. The traditional data authentication mechanisms like digital signatures or cryptographic methods are not very useful in this context due to their extreme fragility. What is required is a method that can detect the integrity for allowable content-preserving manipulations.

In this work-in-progress report, we present a new technique for authenticating 3D volume data using a *robust content-based digital signature*. This signature is derived from the significant features of volume data so that if any of these features are altered significantly, the signature will not match the data set. The term *content-based* refers to the fact the important features of the data (whose integrity we are interested in certifying) should be somehow incorporated into the digital signature. The rationale being that if some important content feature is deleted/modified/added, then the digital signature should not match the doctored data set. The term *robust* refers to the fact that any manipulation which does not change the significant features should not affect the veracity of the signature. For such benign operations, the digital signature should indeed authenticate the data set. Common types of operations on volume data set are scaling, thresholding, cropping, cut-and-replace a sub-volume, filtering, addition/removal of noise and affine transformations. As long as these operations do not change the content features, they are considered benign. We use a novel wavelet-based foveation technique [1] to accurately and succinctly capture the significant content features. Moreover, the scheme allows a flexible threshold to be set which can determine the extent of the manipulations which can be considered benign.

We will now provide an overall description of the method for generating the robust content-based digital signature and the method for authenticating a volume data-set using this digital signature. For the generation of the digital signature, the following steps are required:

Partition of the voxel values by data analysis: First, all the voxel values are sorted in the non-descending order. Second, partition the sorted list using a threshold value.

The threshold value is specified by the user in our current implementation. However, heuristics can be applied if the domain knowledge is known for the particular class of volume data.

For many volume data sets, the density values of significant content components are distinguishable even though the voxels representing them are closely connected to each other. Sometimes, they may perhaps even have similar voxel values in which case domain knowledge could be utilized for distinguishing them. For example, human CT/MRI volumes can be partitioned by using the density values as well as anatomical knowledge.

Segmentation: From the partition, we derive a set of voxel values that partition different parts. These voxel values are used to derive the same number of sets of the isosurfaces. One segment of voxels can be formed if they are bounded as a closed sub-volume by (1) one isosurface, (2) several isosurfaces, or (3) one or several isosurfaces with the one or several border planes of the volume. It can be efficiently derived using the scan conversion algorithm, an extension of the standard scanline algorithm used in the rasterization and hidden-surface elimination, to derive and accumulate the intervals bounded by the isosurfaces and border planes iteratively.

Feature extraction: It is a process of selection of key voxels. A 3D Gaussian mask is applied on the volume several times as lowpass filtering. Due to the large size of volume data, we simulate the 3D Gaussian filtering as a windowed lowpass filtering dimension by dimension. In the highly blurred resulting volume, the key voxels are chosen to be local maximum voxels which are above a predefined threshold. The key voxels are then used as the input to the foveation procedure.

Wavelet-based foveation: To make sure that important content throughout the foreground is captured, we apply the foveation technique which is basically a space-variant filtering technique. We believe it is very important to use this since it *summarizes* all the important content throughout the foreground with the key voxels as the foci. Thus all significant features are compactly captured. Additionally since it is a many-to-one mapping, it offers security. Thus, this information can be used as a key.

The foveated volume is obtained from a uniform resolution volume through a space-variant smoothing process where the width of the smoothing function is small near the fovea but gradually increases towards the peripheral. The process of going from a uniform volume to a foveated volume is known as *foveation*. The *foveation* of a function $V : \mathbf{R}^d \to \mathbf{R}$ is determined by a *smoothing function* $g : \mathbf{R}^d \to \mathbf{R}$, and a *weight function* $w : \mathbf{R}^d \to \mathbf{R}_{\geq 0}$.

$$(TV)(\mathbf{x}) := \int_{\mathbf{R}^d} V(\mathbf{t}) w(\mathbf{x}) g\left(w(\mathbf{x}) \|\mathbf{t} - \mathbf{x}\|_2\right) d\mathbf{t}. \tag{1}$$

The weighting function w depends upon three parameters and takes the form

$$w(\mathbf{x}) = \left(\alpha \|\mathbf{x} - \gamma\|^d + \beta\right)^{-1}. \tag{2}$$

We call α the *rate* as it determines how fast resolution falling off, call γ the fovea as it determines the point of highest resolution, and call β the *foveal resolution* as it determines the resolution at the fovea. Both α and β are non-negative and the smoothing function g is normalized so that $\int_{R^d} g(\mathbf{x})\, d\mathbf{x} = 1$. In general, we could replace the weighting function by any non-negative function. Given

two weighting functions w_1,w_2, the blended w_3 is

$$w_3(\mathbf{x}) = \max\{w_1(\mathbf{x}), w_2(\mathbf{x})\}. \quad (3)$$

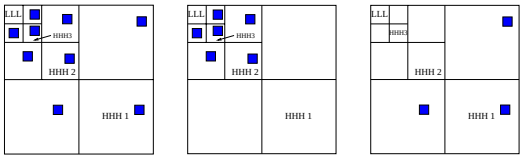
This generalization is useful when we are interested in volumes with multiple foveae.

Foveated volumes can also be treated as the approximation of an volume using a fixed number of bit, using a weighted norm as the underlying measure. This weighted norm can be derived from (1) and has the form,

$$\|V\|_w = \int_{\mathbf{R}^d} \frac{V(\mathbf{x})}{w(\mathbf{x})} d\mathbf{x}, \quad (4)$$

where the weighting function w is the function in (2).

Wavelet bases have important applications in mathematics and signal processing due to their ability to build sparse representation for large classes of functions and signal [2]. It is a natural choice for foveated volume due to their locality in space and frequency. Interesting, the choice of the weighting function (2) gives a self-similarity across scales [1], which is illustrated in Fig 1. This property leads to a simple but fast extraction algorithm [1].



(a) (b) (c)

Figure 1: Allowable Lowpass Filtering: (a) Original wavelet coefficients (C_w); (b) After allowable lowpass filtering (C'_w); (c) Remaining coefficients ($C_w{}^*$). $C_w - C'_w = C_w{}^*$.

Extracting the coefficients: Recall that the first part of the signature (S, W) is the highly compressed volume. To obtain S, one could first compute the foveation (1) with respect to the multi-foveae weighting function, and then compress the foveated volume using a known lossy or lossless compression technique for uniform volumes. Because computing (1) directly is computational intensive, we use the approximation (5).

$$(T^{\text{fov}} I) \approx \text{IDWT}(M\ \text{DWT}(I)), \quad (5)$$

where DWT is the discrete wavelet transformation and IDWT is its inverse. M is a predetermined mask.

In our implementation, S is extracted from the volume by quantizing the wavelet coefficients M DWT(I), followed by a lossless compression using `gzip`.

Note that `gzip` is a general lossless compression tool, which does not exploit properties of volumes, especially the coherence of wavelet coefficients across space and scale. Thus it is not the best technique for our application. A possible improvement can be done by incorporating the well-known zero-tree algorithm [3] into our scheme.

Encryption: For additional security, public-key cryptography [4] is utilized to encrypt the key derived in the previous step. Basically, the secret key of the owner of the volume data is used to encrypt the feature key obtained. For the purpose of authentication, the public-key of the owner can be used to decrypt this information and the feature key can be thus recovered. Since this step is well-understood, we will not discuss it further in this paper.

For authenticating a particular volume data-set, the following steps are performed:

Affine transformation parameters recovery: Since, one of the benign manipulations could be the affine transformation of the volume, the transform parameters are computed first. *Matching*: The content features of the transformed volume are compared with the content features of the original data-set (obtained from the digital signature after decryption using the owner's public key). A match value between the original features and the transformed volume features is computed. If this match value exceeds a certain threshold, then the volume is certified as genuine else it is considered untrustworthy.

We have conducted experiments on two volume data sets, SKULL ($68 \times 64 \times 64$) and TOMATO ($64 \times 208 \times 216$) (Figure 2). In the selection of key voxels, we used a windowed lowpass filtering for five times with the window size 9 and the threshold 1.5. The resulting numbers of key voxels are 25 for SKULL and 124 for TOMATO. The sizes of the signatures are 8KB and 19KB respectively. Five experiments were done with these two volume data sets. The first three experiments examine the signature robustness under global manipulation like low-pass filtering, sharpening, and lossy compression, whereas the last two experiments consider local manipulation like cropping and localized modification. One experiment result of adding Gaussian noise is shown in Figure 3. In this experiment, for SNR of the noise as low as 14.70dB, the volume was still authenticated. Other experimental results are also promising.

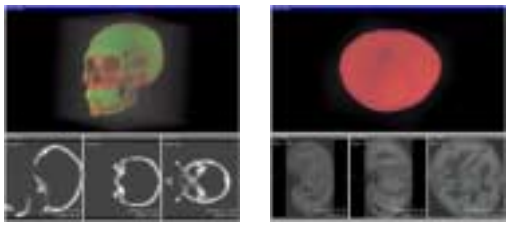


Figure 2: Two volume data sets.

References

[1] E-.C. Chang, S. Mallat, and C. Yap. Wavelet foveation. *Journal of Applied and Computational Harmonic Analysis*, 9(3):312–335, 2000.

[2] S. Mallat. A Wavelet Tour of Signal Processing. *Academic Press*. 1998.

[3] J.M. Shapiro. Embedded image coding using zerotrees of wavelet coefficients. *IEEE Trans. on Signal Processing*. vol. 41, no. 12, December 1993, 3445-3462.

[4] W. Stallings. Cryptography and Network Security: Principles and Practice. *Prentice-Hall Inc.* Second Edition, 1998.

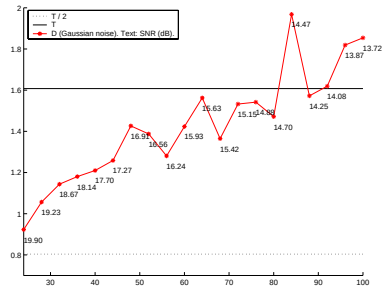


Figure 3: An experiment result: distortion vs. SNR.