A Watermarking Framework for Subdivision Surfaces

Guillaume Lavoué, Florence Denis, Florent Dupont, and Atilla Baskurt

Université Claude Bernard Lyon 1, INSA de Lyon, Laboratoire LIRIS UMR 5205
8 boulevard Niels Bohr, 69622 Villeurbanne Cedex, France
{glavoue, fdenis, fdupont, abaskurt}@liris.cnrs.fr

Abstract. This paper presents a robust watermarking scheme for 3D subdivision surfaces. Our proposal is based on a frequency domain decomposition of the subdivision control mesh and on spectral coefficients modulation. The compactness of the cover object (the coarse control mesh) has led us to optimize the trade-off between watermarking redundancy (which insures robustness) and imperceptibility by introducing two contributions: (1) Spectral coefficients are perturbed according to a new modulation scheme analyzing the spectrum shape and (2) the redundancy is optimized by using error correcting codes. Since the watermarked surface can be attacked in a subdivided version, we have introduced a so-called *synchronization* algorithm to retrieve the control polyhedron, starting from a subdivided, attacked version. Through the experiments, we have demonstrated the high robustness of our scheme against both geometry and connectivity alterations.

1 Introduction

Watermarking provides a mechanism for copyright protection or ownership assertion of digital media by embedding information in the data. There still exist few watermarking methods for three-dimensional models compared with the amount of algorithms available for traditional media such as audio, image and video. Most of the existing methods concern polygonal meshes and can be classified into two main categories, depending if the watermark is embedded in the *spatial* or in the *spectral* domain. *Spatial* techniques [1,2] are quite fast and simple to implement, but do not yet provide enough robustness and are rather adapted for blind fragile watermarking or steganography. *Spectral* algorithms decompose the target 3D object into a spectral-like (or multi-resolution) domain using wavelets [3], multi-resolution decomposition [4,5] or spectral analysis [6,7,8] in order to embed the watermark by modifying kinds of spectral coefficients. Our objective is to propose an efficient watermarking algorithm for subdivision surfaces, which have not been, for the moment, considered in existing 3D techniques. A subdivision surface is a smooth (or piecewise smooth) surface defined as the limit surface generated by an infinite number of refinement operations using a subdivision rule on an input coarse control mesh. Hence, it can model a smooth

B. Gunsel et al. (Eds.): MRSC 2006, LNCS 4105, pp. 223–231, 2006.

surface of arbitrary topology while keeping a compact storage and a simple representation. Figure 1 shows an example of subdivision surface (Catmull-Clark rules [9]), at each iteration, the base mesh is linearly subdivided and smoothed. A lot of algorithms exist to convert a 3D mesh into a subdivision surface [10,11] because this model is much more compact, in term of amount of data, than a dense polygonal mesh.

Basically, every existing polygonal mesh watermarking technique could be applied on subdivision surfaces since corresponding control polyhedrons *are* polygonal meshes. However these surfaces have two specificities which cannot be ignored to design a real efficient applicable watermarking scheme:

1. For a given 3D shape, this representation is much more compact than a polygonal mesh. Thus there is much less available space to embed the watermark.
2. The possible attacks against the watermarked subdivision surface can occur on different states: against the control polyhedron or against a subdivided version (see Figure 1).

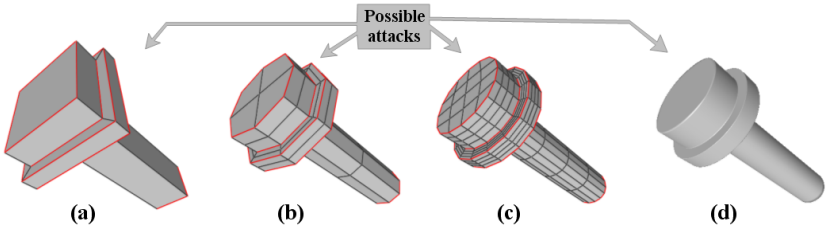


Fig. 1. Example of subdivision surface with sharp edges (in red). (a) Control mesh, (b,c) one and two subdivision steps, (d) limit surface.

Our principal objective is the robustness of the mark, thus we have chosen a spectral domain to embed the watermark; among existing decomposition schemes, the spectral analysis, used by Ohbuchi et al. [6,7], leads to the best decorrelation really close to a theoretical Fourier analysis (see section 2.1). The compactness of the watermarking support (a coarse control polyhedron) has led us to optimize the efficiency of the insertion, in two different ways:

- We propose an extension of the widely used additive modulation scheme [6][7], by increasing embedding strength on low frequency components, in which alterations are less visible for human eyes (see section 2.2).
- In [6] and [7], the mark is repeated several times to increase the robustness. We have investigated a more sophisticated technique, coming from telecommunication theory using convolutional encoding (see section 2.3).

Our extraction process needs to compare the watermarked subdivision control polyhedron with the original one. However attacks can occur on a subdivided version of the watermarked surface. Thus we propose an algorithm to retrieve the control polyhedron, starting from a subdivided, attacked version: the control mesh *synchronization* (see section 2.4).

2 Subdivision Surface Watermarking Algorithm

2.1 Spectral Analysis

The control mesh spectrum is obtained by projecting the vertices coordinates on the eigenvalues of the *Laplacian matrix*. We consider the Bollabás [12] definition for the computation of such a matrix which leads to an easier eigenvalues decomposition. The Laplacian matrix L is defined by $L = D - A$, where D is a diagonal matrix whose each diagonal element d_{ii} corresponds to the valence of the vertex i (i.e. the number of edges connected to this vertex) and A is the adjacency matrix of the mesh whose each element a_{ij} is equal to 1 if vertices i and j are adjacent and 0 otherwise. For a mesh with n vertices, matrices A, D and L have a $n \times n$ size. The eigenvalues decomposition of the Laplacian Matrix L gives n eigenvalues λ_i and n eigenvectors w_i. By sorting the eigenvalues in an ascending order, the n corresponding eigenvectors form a set of basis functions with increasing frequencies, only depending on the mesh connectivity. We call W the $n \times n$ projection matrix constructed with the juxtaposition of the n ordered column eigenvectors.

The geometry information of the mesh, containing n vertices $v_i = (x_i, y_i, z_i)$, can be represented by three vectors $X = (x_1, x_2, ..., x_n)$, $Y = (y_1, y_2, ..., y_n)$ and $Z = (z_1, z_2, ..., z_n)$. The spectral coefficient vectors P, Q and R, computed as follows, form three mesh spectra corresponding to the three orthogonal coordinate axes in the spectral domain.

$$P = W \times X,\ Q = W \times Y,\ R = W \times Z. \tag{1}$$

The geometry can be retrieved using spectral coordinates and inverse matrix W^{-1}. The amplitude spectrum can be obtained by computing coefficients $s_i = \sqrt{(p_i^2 + q_i^2 + r_i^2)}$ for each vertex. Figure 2.b presents the amplitude spectrum obtained for the *SubRabbit* control mesh (200 vertices) which shows a very fast decrease, since most of the geometric information is concentrated in low frequencies. We have not represented the first coefficient which corresponds to the continuous component (i.e. the position) of the object and is not considered in the watermarking process.

2.2 Spectral Coefficient Modulation

Our watermarking algorithm embeds the mark by modulating the amplitude of the coefficients of the mesh spectra P, Q and R. For a given modulating vector $V = (v_1, v_2, ..., v_m)$, $v_i \in \{-1, 1\}$, there exist several schemes to perturb spectral coefficients c_i, introduced notably by Ohbuchi et al. [6][7] and Wu and Kobbelt [8]. Ohbuchi et al. consider a simple additive scheme: $\hat{c_i} = c_i + v_i.\alpha$, with $\hat{c_i}$ the watermarked spectral coefficient, c_i the original one, and α the global watermarking strength. The main drawback is that the low frequency coefficients are disturbed with the same amplitude than the higher frequency ones, which involve a larger visual distortion. At the opposite, the modulating scheme from Wu and Kobbelt is basically the following: $\hat{c_i} = c_i + c_i.v_i.\alpha$. Thus the modulating amplitude is directly proportional to the coefficient value, therefore it will

rapidly converge toward zero. Thus, only very low frequency coefficients will be considered in the watermarking process.

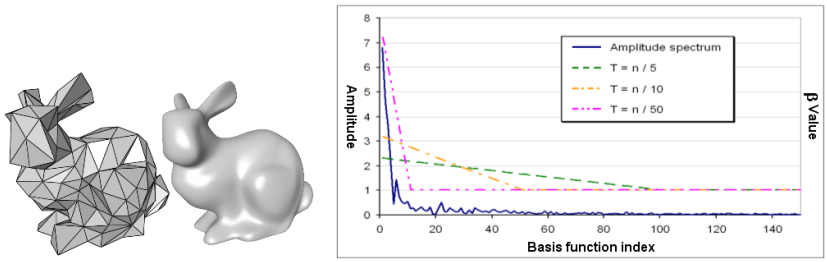
In order to avoid both drawbacks we introduce a new coefficient modulation scheme: the *Low Frequency Favouring* (LFF) modulation, which favours low frequencies but also modulate higher ones:

$$\hat{c_i} = c_i + v_i.\alpha.\beta_i \tag{2}$$

with β_i, the local watermarking strength which adapts the modulation amplitude to the frequency:

$$\beta_i = \begin{cases} 1 & if\ i \geq T \\ g * i + (1 - g * T) & if\ i < T \end{cases} \tag{3}$$

T is a user defined threshold (usually fixed to $\frac{n}{10}$, with n the number of coefficients), and g is the gradient of the linear approximation of the amplitude spectrum between coefficients 1 and T. The main idea is to have a constant watermark strength(α) for middle and high frequency coefficients (index$> T$) and then to increase linearly the strength for low frequencies. The gradient g is calculated from a linear approximation of the amplitude spectrum in $[1, T]$ in order to adapt the watermarking function to the considered object. Figure 2 shows an example of the β functions for the *SubRabbit* shape and for different T values.



(a) **(b)**

Fig. 2. (a) Subdivision surface *SubRabbit*, (b) Amplitude spectrum of the control mesh and evolution of the watermarking strength according to parameter T

Increasing the watermarking strength for low frequency coefficients does not increase the visual distortion since the human eye is much more sensible to normal variations than to geometric modifications. Moreover, a high frequency distortion applied on a subdivision control mesh implies a low frequency distortion on the limit surface since a control mesh can be consider as a coarse low frequency version of its associated limit surface. This fact allows us to consider the whole spectra to embed the mark, contrary to existing algorithms which consider only very low frequency coefficients [8], or the first half [7], in the embedding process.

2.3 Message Sequence Generation

Most of the existing algorithms ensure robustness to high frequency attacks by watermarking only very low frequencies [8,4,5]. However these methods are not so robust to low frequency attacks like non uniform scaling or other global deformations. In a different way Ohbuchi et al. [6] repeat the mark along the spectra, and then average the extracted marks. We add redundancy in a better way noting that a watermarking system can be viewed as a digital communication system: the 3D object represents the communication channel and the objective is to insure the reliable transmission of the watermark message through this channel. Thus it seems natural to consider the use of error correcting codes (ECC), to increase the robustness of the transmission. A lot of different ECC exist in the field of telecommunication. We have chosen to consider convolutional coding associated with soft decision Viterbi decoding. The significant superiority of this ECC for watermarking application was highlighted by Baudry et al. [13] within the field of 2D image.

2.4 Control Mesh Synchronization

The watermarked subdivision surface, can be captured and/or attacked in a subdivided version, thus we have to be able to retrieve the mark even in such a case. So, starting from the reference original subdivision surface, a *control mesh synchronization* moves iteratively its control points in order to match it with the suspect smooth surface. For a given target smooth surface (attacked subdivided watermarked surface) (see Figure 3.a) and a given reference subdivision control mesh (see Figure 3.b), our process displaces control points by minimizing a global error between the corresponding limit surface and the target one, based on the quadratic distance approximants defined by Pottmann and Leopoldseder [14]; This algorithm, used for subdivision surface approximation by Lavoué et al. [11] and Marinov and Kobbelt [10] allows a quite accurate and rapid convergence.

Figure 3.a presents a smooth surface coming from 4 subdivisions (and possibly attacks) of a watermarked control mesh (Catmull-Clark rules). The watermark strength has been exagerated for this experiment. The reference original subdivision surface is shown in Figures 3.b (control mesh) and 3.e (limit surface). After only 5 synchronization iterations, the limit surface (Figure 3.g) is perfectly fitted with the suspect one (Figure 3.a). Resulting errors are respectively 3.84×10^{-3} and 0.03×10^{-3} after 2 and 5 iterations (surfaces were normalized in a cubic bounding box of length equal to 1). Thus after 5 iterations we have retrieved the shape of the watermarked control mesh (see Figure 3.d), and we are able to launch the watermark extraction.

3 Experiments and Results

We have conducted experiments on several subdivision surfaces. Examples are given for three typical objects: *SubPlane* (154 control points) (see Figure 4.a), *SubRabbit* (200 control points) (see Figure 2.a) and *SubFandisk* (86 control

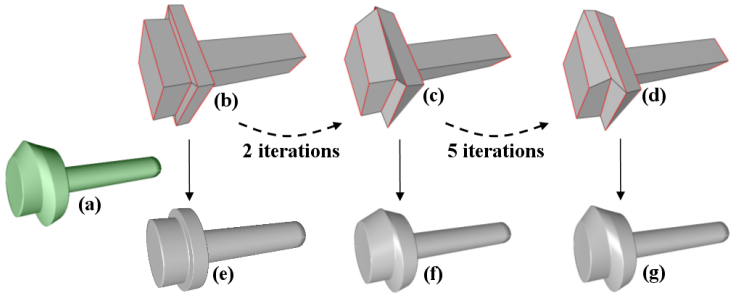


Fig. 3. Example of *synchronization*. (a) Suspect smooth surface, (b,c,d) Reference control polyhedron after 0, 2 and 5 synchronization iterations. (e,f,g) Corresponding limit surfaces.

points) (see Figure 5.a). The robustness is verified for diverse attacks directed against both the control mesh and subdivided versions. In all the experiments, we have considered the embedding of a watermark of length $k = 32$ bits, and with parameters $T = 10$ and $\alpha = 0.005$. The rate of the convolutional coder is 1/3 (96 coefficients are watermarked, on each coordinate spectrum) and every object is scaled to a unit bounding box.

Attacks Against the Control Mesh

Our watermarking scheme can be considered as an improvement of the mesh watermarking algorithm from Ohbuchi et al. [6], by firstly introducing a new modulation algorithm (the *Low Frequency Favouring* scheme) and secondly by modulating the binary message by convolutional encoding. Thus we have established the efficiency of these improvements by checking robustness against two types of real world attacks which alter different parts of the object spectrum: noise addition (rather high frequencies) and non-uniform scaling (rather low frequencies). For each attack, we consider four algorithms:

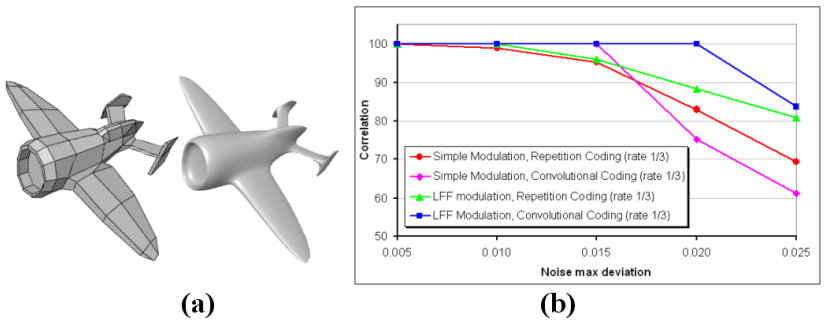


Fig. 4. (a) Subdivision surface *SubPlane*, (b) Watermarking correlation (%) under noise addition attacks, with increasing maximum deviations

- Simple Modulation, Repetition Coding (basically, the Ohbuchi scheme).
- Simple Modulation, Convolutional Coding.
- Low Frequency Favoring (LFF) Modulation, Repetition Coding.
- Low Frequency Favoring (LFF) Modulation, Convolutional Coding (basically, our complete scheme).

In the following results, for each presented correlation value, we have repeated 100 times the insertion, the attack and the extraction, with random bit patterns of length 32 bits and then averaged the obtained correlations.

For the noise addition attack, we modify the three coordinates of each vertex of the control mesh, according to a randomly chosen offset between 0 and a maximum deviation E_{max}. Figure 5 shows the extracted average correlation, according to increasing E_{max} values, for the SubPlane object. The LFF modulation and the watermark convolutional encoding bring a real gain in robustness. For SubRabbit and SubPlane, the correlation reaches 100% for $E_{max} = 0.020$ (four times the value of the watermark strength α!) while the basic scheme (simple modulation, repetition coding) gives respectively 90% and 85%.

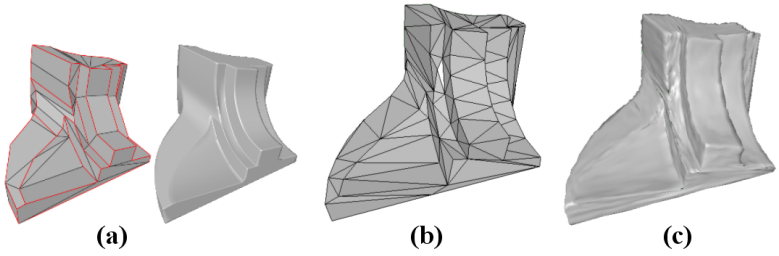


Fig. 5. (a) Subdivision surface *SubFandisk* and Watermarked subdivided objects after (b) simplification (from 4498 vertices to 110) and (c) noise addition. The extracted correlation is 100%.

Concerning the non-uniform scaling attack, we multiply each coordinate (X,Y and Z) by a scaling value, randomly chosen between $1 - S_{max}$ and $1 + S_{max}$. For $S_{max} = 0.3$ we obtain a correlation value of 92% for SubRabbit with our scheme, against 72% with the basic scheme and 100% for SubPlane against 75%.

Attacks Against a Subdivided Version

Since a suspect subdivision surface can be retrieved in a subdivided form, we have tested the robustness of the watermarking scheme to the synchronization process and to some attacks against a subdivided watermarked surface. For this experiment, we have watermarked the SubFandisk control mesh ($\alpha = 0.005$ and $rate = 1/2$) and then applied three subdivision iterations. We have then considered two attacks: a rather strong simplification (see Figure 5.b) and a noise addition (max deviation = 0.4%) (see Figure 5.c). We obtain for both cases a 100% correlation, after the synchronization and the mark extraction.

4 Conclusion

We have presented a robust watermarking scheme for subdivision surfaces, based on the modulation of spectral coefficients of the subdivision control mesh. Due to the compactness of the cover object (a coarse control mesh), our algorithm optimizes the trade-off between watermarking redundancy and imperceptibility by modulating coefficients according to a new scheme (LFF) and by using error correcting codes. Experiments have shown an average 20% improvement of the robustness, compared with a standard modulation scheme [7].

Since a watermarked subdivision surface can be captured and/or attacked in a subdivided (i.e. smooth) version, we have also introduced a synchronization process allowing to retrieve the corresponding control mesh and to correctly extract the mark. This process provides efficient robustness against remeshing or simplification attacks.

Concerning future work, it should be useful to modelize the spectral distortion introduced by the different types of attacks (noise addition, quantization, scaling etc.) in order to construct specific error correcting codes. We also plan to conduct a deeper analysis of the visual distorsion introduced by our algorithm. Several authors have proposed perceptual metrics [15] or evaluation protocols [16] to properly benchmark watermarking schemes.

References

1. Benedens, O.: Geometry-based watermarking of 3d models. IEEE Computer graphics and application **19** (1999) 46–55
2. Cayre, F., Macq, B.: Data hiding on 3-d triangle meshes. IEEE Transactions on Signal Processing **51** (2003) 939–949
3. Kanai, S., Date, H., Kishinami, T.: Digital watermarking for 3d polygons using multi-resolution wavelet decomposition. In: IFIP WG 5.2 International workshop on geometric modeling: fundamental and application (GEO-6). (1998) 296–307
4. Praun, E., Hoppe, H., Finkelstein, H.: Robust mesh watermarking. In: Siggraph. (1999) 69–76
5. Yin, K., Pan, Z., Shi, J., hang, D.: Robust mesh watermarking based on multiresolution processing. Computers and Graphics **25** (2001) 409–420
6. Ohbuchi, R., Takahashi, S., Miyazawa, T., Mukaiyama, A.: Watermarking 3d polygonal meshes in the mesh spectral domain. In: Graphic interface. (2001) 9–17
7. Ohbuchi, R., Mukaiyama, A., Takahashi, S.: A frequency-domain approach to watermarking 3d shapes. Computer graphic forum **21** (2002) 373–382
8. Wu, J., Kobbelt, L.: Efficient spectral watermarking of large meshes with orthogonal basis functions. The Visual Computers **21** (2005) 848–857
9. Catmull, E., Clark, J.: Recursively generated b-spline surfaces on arbitrary topological meshes. Computer-Aided Design **10** (1978) 350–355
10. Marinov, M., Kobbelt, L.: Optimization methods for scattered data approximation with subdivision surfaces. Graphical Models **67** (2005) 452–473
11. Lavoué, G., Dupont, F., Baskurt, A.: A framework for quad/triangle subdivision surface fitting: Application to mechanical objects. Computer Graphics Forum **25** (2006)

12. Bollabás, B.: Modern graph theory. Springer (1998)
13. Baudry, S., Delaigle, J.F., Sankur, B., Macq, B., Maitre, H.: Analyses of error correction strategies for typical communication channels in watermarking. Signal Processing **81** (2001) 1239–1250
14. Pottmann, H., Leopoldseder, S.: A concept for parametric surface fitting which avoids the parametrization problem. Computer Aided Geometric Design **20** (2003) 343–362
15. Lavoué, G., Drelie Gelasca, E., Dupont, F., Baskurt, A., Ebrahimi, T.: Perceptually driven 3d distance metrics with application to watermarking. In: SPIE Applications of Digital Image Processing XXIX. (2006)
16. Benedens, O., Dittmann, J., Petitcolas, F.: 3d watermarking design evaluation. In: SPIE Security and Watermarking of Multimedia Contents V. Volume 5020. (2003) 337–348