BLIND AND ROBUST WATERMARKING OF 3D MODELS: HOW TO WITHSTAND THE CROPPING ATTACK?

Patrice Rondao Alface, Benoit Macq

Université catholique de Louvain
2, Place du Levant
B-1348 Louvain-La-Neuve, Belgium

François Cayre

Laboratoire des Images et des Signaux
961 rue de la Houille Blanche - BP46
F-38402 Saint Martin d'Hres cedex, France

ABSTRACT

State-of-the-art blind and robust 3D watermarking schemes already withstand combinations of a wide variety of attacks (e.g. noise addition, simplification, smoothing, ...) except cropping. This attack is however very common and should be dealt with in a copyright protection framework. In this paper, we propose a technique which enables to extend the robustness of such schemes to cropping. Our algorithm proceeds by the automatic detection of robust shape feature points which are then used for the embedding of a watermark in a local neighborhood. We show that robustness against cropping and other common attacks is achieved provided that at least one feature point as well as its corresponding local neighborhood are retrieved.

Index Terms— 3D watermarking, Shape feature points

1. INTRODUCTION

Robust watermarking has been proposed as part of the solution to the protection of the intellectual property rights (IPR) attached to audiovisual contents such as sound, image, video etc. Focusing on the specific case of copyright protection, robust watermarking aims at ensuring that the identifier (i.e. the *watermark*) of the audiovisual content buyer or licenser will always be present and detected.

In this context, the requirements of watermarking are mainly *imperceptibility* (the identifier should not alter the use of the content to be protected) and *robustness* (the watermark should resist any combination of attacks until the content becomes too much degradated to be used).

In this paper the audiovisual content we focus on relates to 3D models. A 3D model is usually represented by a 3D mesh which is composed of two sets : the *geometry* which is the set of 3D points and their coordinates and the *connectivity* which is the set of edges and polygons connecting the points of the geometry. The mesh only approximates the perceived smooth surface which is the content that owners generally want to protect against illegal distribution. This means that modifying the number of points or polygons of a watermarked mesh while preserving its perception not prevent from detecting the watermark.

In the case of blind detection schemes, which directly detect the watermark on the suspect mesh without the availability of the original data, the state-of-the-art robustness usually fails at dealing with combinations of all classes of watermarking attacks (see [1] for an extensive survey). Spectral- [2] and wavelet-based [3] blind watermarking schemes resist combinations of rigid transforms (rotation, translation and uniform scaling), smoothing, noise addition and compression. Feature points extension of the spectral decomposition has led to robustness to simplification [4] and, finally, histogram-based spatial watermarking schemes [5, 6] have proved to be able to withstand all combinations of commonly tested 3D watermarking attacks *except cropping*. This weakness is caused by the construction of these schemes which is based on the histogram of euclidian distances from each point of the mesh to the mesh center of gravity (CoG). Cropping attacks and non-uniform resampling attacks modify the CoG position and do not allow the decoder to retrieve the same histogram and, subsequently, the watermark.

The main contribution of this paper is a technique which enables to extend the robustness of histogram-based watermarking schemes to the cropping attack. Furthermore, several improvements of the histogram construction lead to a better robustness to non-uniform resampling of 3D meshes.

The organisation of this paper is as follows. Section 2 presents the overview of the watermarking scheme we propose. This scheme is based on the detection of robust feature points which is described in Section 3. Section 4 is dedicated to the detection of robust neighborhoods and Section 5 to our modified local histogram-based watermark embedding. Results are then illustrated and commented in Section 6.

2. WATERMARKING SCHEME OVERVIEW

The blind and robust watermarking scheme proposed in this paper is composed of three different steps:

1. feature points detection

2. local and robust neighborhood detection

3. histogram-based embedding of each feature point neighborhood

The main idea of our scheme is to exploit and improve the very good robustness properties of histogram-based watermarking schemes while extending them to robustness against cropping. As previously mentioned, the weakness of these schemes is related to modifications of the CoG position. We overcome this problem by restricting the histogram construction to some local parts (a.k.a. patches or charts) of the mesh which are each watermarked. These patches are given by the robust neighborhood of robust feature points and usually do not cover the entire mesh. If a cropping occurs, it will change the global mesh CoG and cut some feature points and their neighborhoods but it will not affect the CoG position and watermark of each robust neighborhood that has been preserved by the attack.

3. ROBUST FEATURE POINTS

Several papers (e.g. [7]) have explored the *protrusion* function to develop perceptual segmentation algorithms. The protrusion of a point is an estimation of how much it is "geodesically" distant to the set of all other points of the shape. Large protrusion values indicate the point is an extremity of the shape (a.k.a. *prongs*), low values indicate the point belongs to the core of the shape (see Fig. 1). This protrusion function

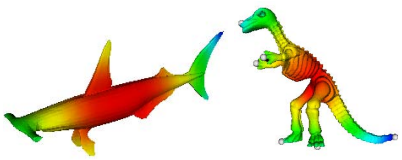

Fig. 1. On the left, the protrusion function of the *Hammerhead* model, low protrusion values (the core) are represented in red and high values in blue. On the right, the protrusion function and prongs of the *Dinosaur* model.

is usually defined on a 3D mesh representation M of a surface S as follows:

$$\mu(v) = \frac{1}{area(M)} \sum_{p_i \in M} g(v, p_i)^2 area(p_i), \qquad (1)$$

with

$$area(M) = \sum_{p_i \in M} area(p_i), \qquad (2)$$

where $g(v, p_i)$ is the geodesic distance between points v and p_i; $area(p_i)$ is the area of the neighborhood of point p_i and $area(M)$ is the sum of the area contributions of each point of the mesh M. The weighting areas can be chosen in many different ways with similar results but most approaches are based on the area of the 1-ring neighborhood (the set of points which are connected to a given point by one edge).

The *geodesic distance* between points p_i and p_j on a surface mesh M is given by the length of the *shortest path* on M linking these points. In practice, we compute its approximation by the *fast marching algorithm* [8].
Since it is an integrative function, the protrusion is robust to noise addition, smoothing and resampling. Its local maxima are also robust to cropping if the cropping plane does not cut their 1-ring neighborhood. However, in our work, we restrict the definition of a prong as a point $p \in M$ satisfying the following conditions:

1. p belongs to the convex hull of M

2. $\forall q \in N_k(p), \mu(p) > \mu(q)$

3. p is not on the border of M

where $N_k(p)$ is the set of k geodesically nearest neighbors of p. We impose the prongs to belong to the convex hull of the surface in order to avoid the detection of local maximas in the core region of the mesh. We thus select geodesic extremities of the shape which are also euclidian extremities of the shape. Moreover, we reject shape boundaries. Indeed, all the points of a border are geodesically far from the other points of the shape and should then be considered as prongs. As we want to resist cropping attacks, it is important to avoid the borders these attacks create. This definition loses some intuitive prongs that do not belong to the convex hull or the borders but enables to filter undesirable local maxima.

4. ROBUST LOCAL NEIGHBORHOODS

Now that the prongs have been detected, we must define their neighborhood. These neighborhoods are patches that do not have to entirely cover the shape. Since these patches are hosts of the watermarking technique we have selected, their shape must satisfy some conditions:

1. the patch is a geodesic circle centered on the prong,

2. the geodesic radius of the patch cannot be superior to R_g: the half of the geodesic distance value to the nearest prong,

3. the line intersecting each point of the patch to its CoG cannot intersect with other points of the patch (a.k.a. star-shape condition). The minimal geodesic distance value at which this problem occurs is denoted R_s.

Considering a prong v, let us denote R_{max} the geodesic distance to the most distant point from v. We thus compute for a given prong v, the values R_g and R_s which are set to R_{max} if they do not exist. This occurs when only one prong is detected or when the shape has always a star shape behavior (i.e.

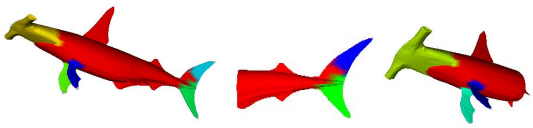

Fig. 2. On the left, example of prong neighborhoods for the *Hammerhead* model. Patch neighborhoods which are selected for watermarking have a different color corresponding to their prong. The red region is not watermarked. On the right, the detected neighborhoods on the two remaining sides of the model after a cropping attack by a vertical plane.

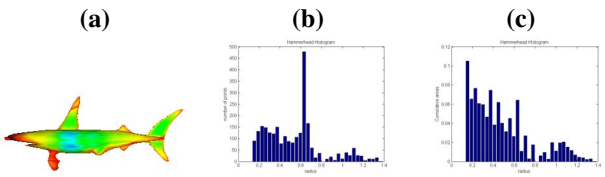

Fig. 3. Improvement of the shape histogram construction. (a) The *Hammerhead* model density is not uniform (red to blue for decreasing values of density), (b) Corresponding histogram computed by [6] shows an undesirable peak near radius bins of high density sampling, (c) Corresponding histogram computed by our method.

the shape is convex). The neighborhood is therefore defined by the surface region covered by the wavefront of radius R which is given by:

$$R = min(R_g, R_s) \leq R_{max}. \tag{3}$$

In case the nearest prong has been lost after a (cropping) attack, R_{max}, R_s and R_g can be modified and the robustness of the patch is not ensured. Therefore, a limitation of our approach is that we must recover a pair of prongs that are nearest neighbors. However in practice, if the geometry implies $R = R_s$ because of condition 3, the presence of the nearest prong would not be necessary to recover the correct patch. An example of neighborhoods is given in Fig. 2.

5. PATCH RADIAL WATERMARKING

This Section is dedicated to the third step of our algorithm. Our watermarking technique is inspired by works of Zafeiriou et al. [5] and Cho et al. [6] for 3D blind spatial robust watermarking. These similar schemes are both based on a representation of the geometry in spherical coordinates with respect to the shape CoG. Their robustness results are similar and very good against most watermarking attacks. The disadvantage of their techniques is that the CoG is not correctly estimated after cropping and some resampling attacks and the watermark detection fails. We use the prongs and their corresponding patches to retrieve at least a prong and its local shape. Then the CoG of this patch is correctly retrieved as well as the embedded watermark. Moreover, we propose some modifications of the scheme of Cho et al. to better withstand resampling.

5.1. Robust Center of Gravity Estimation

First of all, we must define the CoG C_g of the shape M. Following [5, 6], this point is simply estimated by the mean of the geometry. For a regularly sampled mesh M (i.e. points are uniformly distributed on the shape), this estimation of C_g is correct. However, if the shape is irregularly sampled, the estimation of C_g is biased, and its position is shifted towards the part of the shape which has the highest density of points. We propose to use different weights to estimate the position of C_g:

$$C_g = \frac{1}{area(M)} \sum_{p_i \in M} area(p_i) p_i, \tag{4}$$

where $area(p_i)$ is the third of the area of the 1-ring neighborhood of p_i and $area(M)$ is given by the sum of the $area(p_i)$. The estimation of C_g is now robust against resampling attacks.

5.2. Shape Histogram

The *radius shape histogram* (a.k.a. shape histogram) of a star shape is the histogram of the distance between each point of the shape and its CoG. The distance between a point p and the CoG C_g is noted $\rho(p)$ and is simply given by their euclidian distance. The histogram can be represented by regrouping ρ values in bins and is characterized by a minimal radius ρ_{min} and a maximal radius ρ_{max} as illustrated on Fig. 3.

In order to build the histogram, several choices are possible. Cho et al. propose to simply count the number of points in a given bin. This however implies a certain sensitivity to resampling. Here, we propose to add for each point the ratio between its 1-ring area and the cumulated area of the shape. Taking the areas into account allows invariance of the histogram with respect to local point sampling density variations and therefore to resampling attacks (see Fig. 3).

5.3. Watermark Embedding

The watermarking embedding consists in modifying the distribution of points in each of the $N + 2$ bins of the shape histogram. For that purpose, each histogram is subdivided in two sub-intervals that carry a 0 or a 1 information bit. The mean of the distribution of points in this interval is displaced or not towards the other sub-interval accordingly to the watermark bit to embed. This displacement is simply performed by moving points along the line which link them to the CoG so that their new distance corresponds to the correct sub-interval.

The extremity bins (i.e. those containing ρ_{min} or ρ_{max}) are not modified for imperceptibility reasons as well as for preventing a modification of the bins construction. Likewise Cho et al. [6] we embed $N = 64$ bits.

5.4. Watermark Decoding

The watermark is simply read in the histogram bins by determining whether the bin distribution mean is in the 0 or 1 subinterval. Since the watermark is repeated in each prong neighborhood, we compute the final retrieved watermark by a simple majority rule over the watermark bits retrieved in each neighborhood.

6. ROBUSTNESS EXPERIMENTAL RESULTS

We have tested the robustness of the prong detection under a wide set of attacks. The robustness of the neighborhoods under the cropping attacks has not been deeply tested because of the lack of similarity or error measure between surfacic patches. A visual confirmation is provided by Fig. 2. This choice is motivated by the fact that it is more interesting to directly test the robustness of the watermarking scheme itself.

The results of the prong robustness benchmark are given in Fig. 4 with the corresponding robustness of the whole watermarking schemes as well. We can see the prongs are more robust than the umbilical points proposed in a former work [4]. This can be explained by the fact that these points are detected by the maxima of an integral function while umbilical points are based on a differential function. These preliminary results show the robustness of the whole scheme. The indicated values are those from which higher intensities of the attack lead to a non-null bit error rate. It can be seen that the scheme resists all classes of watermarking attacks but with small attack amplitudes.

	Hammerhead	Bunny	Dinosaur
noise	.14%(.3%)	.09%(.4%)	.01%(.35%)
smoothing	15(200)	10(100)	15(120)
decimation	10%(25%)	15%(20%)	12%(30%)
subdivision	1	1	1
rigid	OK	OK	OK
cropping	OK	OK	OK

Fig. 4. Robustness of the watermarking scheme against most common watermarking attacks. An indication of the prong robustness is given between parentheses when it differs from the whole scheme robustness values. The cropping attack is performed with a vertical plane intersecting the center of gravity of the models. Values correspond to the attack maximal amplitude for which the watermark (or the prongs position) is correctly retrieved. The noise attack amplitude is measured in percentage of the bounding box diagonal; smoothing and subdivision in number of iterations and decimation in percentage of removed points.

7. CONCLUSIONS

This paper has presented a way to extend the robustness of blind and robust watermarking schemes to the difficult cropping attack. At this stage, the watermark robustness is far from beeing as robust as the prong detection. However, the watermarking scheme can afford some center of gravity displacements which are due to small prong displacements if the sampling density is sufficient. Some optimizations should be developed to improve the watermarking scheme. However, this blind scheme is very promising as it is the first to withstand cropping and resampling attacks (of small amplitude).

8. REFERENCES

[1] P. Rondao Alface and B. Macq, "From 3d mesh data hiding to blind and robust 3d shape watermarking," *LNCS Transactions on Data Hiding and Multimedia Security*, 2006, accepted.

[2] F. Cayre, P. Rondao Alface, F. Schmitt, B. Macq, and H. Maître, "Application of spectral decomposition to compression and watermarking of 3d triangle mesh geometry," *Image Communications*, vol. 18, no. 4, pp. 309–319, 2003.

[3] F. Uccheddu, M. Corsini, and M. Barni, "Wavelet-based blind watermarking of 3d models," in *Proc. of the 2004 multimedia and security workshop*, 2004, pp. 143–154.

[4] P. Rondao Alface and B. Macq, "Blind watermarking of 3d meshes using robust feature points detection," in *Int. Conf. on Image Proc. (ICIP05), Genova, Italy, 11-14 September*, 2005, vol. 1, pp. 693–696.

[5] S. Zafeiriou, A. Tefas, and I. Pitas, "Blind robust watermarking schemes for copyright protection of 3d mesh objects," *IEEE Trans. Vis. Comput. Graph.*, vol. 11, no. 5, pp. 596–607, 2005.

[6] J.W. Cho, M.S. Kim, R. Prost, H.Y. Chung, and H.Y. Jung, "Robust watermarking on polygonal meshes using distribution of vertex norms," in *Proc. of IWWM'05, volume LNCS 3304, Siena, Italy*, 2005, pp. 283–293.

[7] S. Valette, I. Kompatsiaris, and M. Strinzis, "A polygonal mesh partitioning algorithm based on protrusion conquest for perceptual 3d shape description," in *SVE 2005, Villars, CH, March 11-18*, 2005, pp. 68–76.

[8] G. Peyré and L. Cohen, "Geodesic re-meshing and parameterization using front propagation," in *Proc. of VLSM'03*, 2003, pp. 33–40.