A New Approach of 3D Watermarking Based on Image Segmentation

Saoussen Ben Jabra and Ezzeddine Zagrouba

Institut Supérieur d’informatique,
Abou Raihane Bayrouni, 2080 l’Ariana, Tunisia.
Ezzeddine.Zagrouba@fsm.rnu.tn

Abstract

In this paper, a robust 3D triangular mesh watermarking algorithm based on 3D segmentation is proposed. In this algorithm three classes of watermarking are combined. First, we segment the original image to many different regions. Then we mark every type of region with the corresponding algorithm based on their curvature value. The experiments show that our watermarking is robust against numerous attacks including RST transformations, smoothing, additive random noise, cropping, simplification and remeshing.

1. Introduction

Recently, 3D images have been widely used in virtual reality, medical imaging, video games and computer aided design. They are mostly represented by polygonal meshes. Basically, a mesh is a collection of polygonal facets. It possesses three different combinatorial elements: vertices, edges and facets. It can also be completely described by two kinds of information: The geometry information defines essentially the coordinates of all its vertices, while the connectivity (topology) information describes the adjacency relations between the different elements. The degree of a facet is the number of its component edges, and the valence of a vertex is defined as the number of its incident edges. Although there are many other 3D representations (such as cloud of points, parametric surface, implicit surface and voxels), 3D mesh has been the most popular used representation of 3D objects thanks to its simplicity and usability. Furthermore, it is quite easy to convert other representations to 3D mesh, which is considered as an efficient low-level model.

Digital watermarking, derived of the steganography, has been considered as a good technique to resolve the problem of copyright. It consists of inserting (generally under invisible shape) a signature into an image, then to try to get it back after any possible attacks on the image. It can be blind or non blind depending on whether the original digital image is needed at extraction, or not. Usually, the signature must be robust it means that it must resist against the malicious attacks; this type of watermarking is designed to copyright protection applications. The watermarking can also be fragile for authentication applications. Robustness is often measured in terms of the number of watermarking attacks categories the watermark is able to resist. Most common categories of attacks are RST transformations (rotation, translation, scaling), geometrical attacks (noise addition, surface smoothing), resampling attacks (connectivity modifications such as simplification, subdivision, remeshing) and cropping (i.e. cutting part of the 3D model by a plane).

The remaining sections of this paper are organized as follows. A brief review of the 3D watermarking schemes is given in Section 2. The proposed watermarking embedding scheme is described in section 3 and the experimental results are provided in section 4. Finally, section 5 summaries the proposed work and present the future work.

2. Overview of 3D watermarking

Compared to other audiovisual multimedia such as image, audio and video, 3D watermarking is relatively new and is not yet a mature technology. This situation is caused by the complexity of the meshes and the possible manipulations which can attack the watermarked meshes. Existing techniques concerning 3D meshes can be classified in two main categories, depending whether the watermark is embedded in the spatial domain (by modifying the geometry or the topology) or in the spectral domain (by modifying the spectral coefficients of the mesh).

2.1. Spatial methods

They may be classified in two main categories: the first modify the geometry and the second modify the topology.
2.1.1. Spatial methods modifying geometry. These schemes modify the point positions. Harte et al. [1] have proposed a blind watermarking scheme to embed a watermark in the point positions. One bit is assigned to each point: 1 if the point is outside a bounding volume defined by its point neighborhood and 0 otherwise. This bounding volume may be either defined by a set of bounding planes or by a bounding ellipsoid. During embedding and decoding, points are ranked using their distance to their neighborhood center. The Vertex Flood Algorithm (VFA) [2] embeds information in point positions. Given a point p in the mesh, all points are clustered in subsets (Sk) accordingly with their distance to p. This point is the barycenter of a reference triangle R whose edges are the closest to a predefined edge length ratio. Each non-empty subset is subdivided in m + 2 intervals. The distance of each point in a subset is modified in order to encode m bits.

Geometric algorithms can resist to geometrical attacks (translation, rotation, zooming and a combination of them) but they don’t resist against remeshing or simplification. For extraction, geometric watermarking mostly can be blind.

2.1.2. Spatial methods modifying topology. There exist very few watermarking methods using the mesh topology. Among this class of watermarking schemes, Ohbuchi et al. [3] have proposed four different watermarking algorithms. These schemes are Triangle Similarity Quadruple (TSQ), Tetrahedral Volume Ratio (TVR), Triangle Strip Peeling Sequence (TSPS) and Macro Density Pattern (MDP). TSQ modifies ratios between triangle edge lengths or triangle height and basis lengths. The invariant used by TVR is the ratio between an initial tetrahedron volume and the volume of tetrahedron given by an edge and its two incident triangles. These ratios are slightly modified to embed the watermark. The third scheme, TSPS, encodes data in triangle strips given the orientation of the triangles. Finally, Ohbuchi’s MDP is a visual watermarking method which embeds the signature by changing the local density of points. The Triangle Flood Algorithm (TFA) is another connectivity-driven watermarking scheme developed by Oliver Benedens [4]. This scheme uses connectivity and geometric information to generate a unique traversal of all the mesh triangles. Point positions are modified to embed the watermark by altering the height of the triangles and also to enable the regeneration of the traversal.

Topologic algorithms can resist to topologic attacks (simplification and remeshing). For extraction, topologic watermarking mostly can be blind.

2.2. Spectral methods

These methods embed information in a mesh transform domain. These transforms can be the mesh spectral decomposition, the wavelet transform or the spherical wavelet transform. Ohbuchi et al. [5] proposed a spectral watermarking which embeds the signature on low pseudo-frequency coefficients. Kanai et al. [6] have proposed the first scheme embedding in the wavelet transform domain. The watermark bits are embedded by modifying the least significant bits of the wavelet coefficients modulus.

These schemes are robust against filtering and cropping and their extraction depends on the used transform.

2.3. Attribute based watermarking

The watermarking can use other proprieties of the 3D mesh like texture, 3D silhouettes... A texture is coded as a picture attached to each of the facets of the object 3D. The signature can be inserted using the texture. [7] separate the texture from the original 3D mesh and uses a 2D watermarking to insert the signature in the texture. Bennour et al. [8] embed the watermark in 3D silhouettes of the mesh and retrieve it in 2D rendered views of the model. Therefore, no 3D data is necessary at the decoding side. These schemes are robust against the 2D attacks.

2.4. NURBS representation based watermarking

Mechanics industry produces two main kinds of surfaces: functional surfaces, which enable the manufactured product to operate its function; and free surfaces, for an esthetical purposes. Free surfaces are created with CAD software by making use of parametric surfaces. A NURBS surface is composed by a set of control points denoted by P, a vector of weights denoted by w, and a knot vector denoted by U. The principle in [9] is to change the weight and the knot vectors so as to preserve the overall geometry. When marking CAD models, the algorithm required the smallest alteration of the geometry because they can cause errors in production.

These algorithms are robust to the geometric attacks and simplification and they aren’t blind.

2.5. Comparative study

According to the study of existing methods, we can notice that every type of insertion possesses its own
limitations and its own advantages. Table 1 presents a comparison of different schemes based on the most important criteria of watermarking: invisibility (1), robustness (2) and type of detection (3).

Table 1. Comparison of watermarking schemes

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Class 1</th>
<th>Class 2</th>
<th>Class 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geometric</td>
<td>+</td>
<td>Geometric attacks</td>
<td>Blind</td>
</tr>
<tr>
<td>Topologic</td>
<td>+</td>
<td>Remeshing + Simplification</td>
<td>Blind</td>
</tr>
<tr>
<td>Spectral</td>
<td>+</td>
<td>Cropping + Compression + filtering</td>
<td>Depends on the used transform</td>
</tr>
<tr>
<td>NURBS</td>
<td>+</td>
<td>Geometric attacks + simplification</td>
<td>Non blind</td>
</tr>
<tr>
<td>Other attributes</td>
<td>+</td>
<td>2D attacks</td>
<td>Non blind</td>
</tr>
</tbody>
</table>

3. The proposed watermarking

Many schemes have been developed but mostly of them are not blind and they cannot resist against all the attacks. The idea that we conceived consists in marking image with a method which uses many types of insertion to benefit from multiple advantages of each type. This can be achieved after an unrefined segmentation of the image to be marked which transform the image in various zones and every zone will be marked using a different type of insertion chosen according to the characteristics of the region.

The general algorithm of insertion decomposes into several stages: segmentation, curvature estimation, marking of regions and reconstitution of the marked image. The detection of the signature decomposes also into several stages where the two first of which are identical to those used in the insertion. Indeed, after the segmentation and the classification of regions of the given image, the adequate detector will be applied on every region according to its type to verify the presence of the signature.

3.1. Image segmentation

The segmentation decomposes a 3D mesh into connected subsets of mesh. The chosen algorithm that we have implemented was proposed by L.Guillaume[10]. It decomposes the object into almost constant curvature triangle regions with precise edge boundaries. Firstly, discrete curvature is calculated for each vertex according to the work of Meyer et al[11]. Then, vertices are classified into clusters according to their principal curvatures values. A region growing algorithm is then processed assembling triangles into connected labeled regions according to the vertex clusters. Holes between regions are filled taking into account boundary criteria. Finally a region adjacency graph is processed and reduced in order to merge similar regions according to several criteria (curvature similarity, size, common perimeter).

3.2. Curvature estimation

The classification of the different regions given by the segmentation is achieved by using two measures: Gaussian and mean curvature. In fact, these two measures permit to classify the regions in three classes: convex regions having positive mean curvature and positive Gaussian curvature, concave regions having a negative mean curvature and positive Gaussian curvature and plane regions having Gaussian curvature almost equal to zero. Estimating the mean curvature on a triangulated surface can be done by using the following formula:

\[ K_m(X) = \frac{1}{2}A \sum_{j \in N(i)} (\cot \alpha_j + \cot \beta_j) (X_j-X) \]  

(1)

Where angles \( \alpha_j \) and \( \beta_j \) are two angles opposite to the edge \( e(i,j) \), \( A \) is the Voronoi surface in the point \( X \) and \( N(i) \) is the neighbourhood of the point \( X \). The Gaussian curvature can be calculated using the following formula:

\[ K_g(X) = \frac{1}{2}A (2\pi - \sum_{i=1,n} v_i) \]  

(2)

Where \( n \) is the number of triangles and \( i \) is a component.

3.3. Adaptation of watermarking algorithms

Our main goal is to obtain a scheme of watermarking robust against the maximum of attacks, blind and invisible. For robustness, to get the maximum, our idea was to profit from the advantages of many classes of watermarking. So, we choose to use three schemes in one algorithm. These three schemes are: geometric, topologic and spectral scheme. These three schemes are chosen because the first permit to get robustness against geometric attacks, the second permit to the signature to be robust against remeshing and simplification and the last scheme allow obtaining robustness against filtering and compression. In more, the repetition of the signature in many regions helps us to detect the signature after a cropping of the marked image. In the other hand, the use of these three schemes allows to obtain a blind extraction because
these algorithms don’t need the original image at the time of the detection.

In the comparative study, we observed that spectral watermarking give the maximum of invisibility when the insertion is done in low frequencies which correspond to the plane regions so we choose to mark this type of regions with spectral watermarking. For the two others types of regions, we choose to mark concave regions with geometric watermarking and convex regions with topologic watermarking. This choice is based on experimental study. In fact, we have tested the two propositions and we have obtained the better visibility where we apply geometric algorithm on the concave regions and topologic algorithm on the convex regions. The table 2 presents the choice of the algorithm according to the type of the region.

### Table 2. Choice of watermarking

<table>
<thead>
<tr>
<th>Curvature estimation</th>
<th>Type of region</th>
<th>Watermarking algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Km&gt;0 and Kg&gt;0</td>
<td>convex</td>
<td>topologic</td>
</tr>
<tr>
<td>Km&lt;0 and Kg&gt;0</td>
<td>concave</td>
<td>geometric</td>
</tr>
<tr>
<td>Kg ≈ 0</td>
<td>plane</td>
<td>spectral</td>
</tr>
</tbody>
</table>

### 3.4. Decoding

The detection of the signature decomposes in many stages. First, the marked image will be segmented using the same algorithm in insertion. After, mean and gaussian curvature of the obtained regions will be calculated to classify the regions to three types like insertion. After classification, the adequate algorithm of detection will be applied on every region. So a geometric detector will be applying to concave regions, a topologic detector will be applying to convex regions and spectral detector to the plane regions. Every detector will give ‘1’ if the signature will be found in the region else it gives ‘1’. If all the detectors give ‘0’ so we decide that the image is not marked. These detectors are all blind they don’t need the original image to detect the signature so our detector is blind.

### 4. Experimentation

We give in this section the results of segmentation and watermarking.

### 4.1. Segmentation results

We have tested the segmentation on four images: the first “Fandisk” with 6475 points and 12946 triangles we obtained 24 regions. The second “Cow” with 2903 points and 5804 triangles we obtained 20 regions. The third Porsche with 5247 points, 10474 triangles and 51 regions and finally “Teapot” with 530 points and 1024 triangles and we obtained 4 regions. We have chosen these images because they have different proprieties of number of points, number of regions and triangles and they have different proprieties of curvature. Figure 1 represents the segmentation results.

![Figure 1. Segmentation results](image)

### 4.2. Watermarking results

We have tested our approach of watermarking on the four images used in segmentation. The three algorithms which are implemented are: the scheme of Harte et al [1] for the geometric class, the TSQ [3] scheme for topologic class and the scheme of Ohbuchi et al [4] for spectral class. We obtained the results represented in figure 2.

![Figure 2. Watermarking results](image)
4.2.1. Visibility. The term of visibility refers to the visual degradation of a 3D object due to the embedding of the watermark. Naturally, the watermarking process should not introduce suspicious perceptible artifacts. In some other words, a human observer should not be able to detect if some digital data has been watermarked or not. Some techniques have been introduced to measure objectively whether a distortion due to embedding is perceptible or not. To evaluate our watermarking we tested the most used measure: the signal to noise ratio SNR. The maximum value of SNR obtained for the four tested images is $6.32 \times 10^{-3}$ for Fandisk image which has 6475 vertices. No differences can be observed between the original and marked image.

To evaluate the visibility of our approach we measured the SNR for the same four images marked with the three watermarking (geometric, topologic and spectral). Figure 3 presents the variation of the SNR for the four tested images using our approach and the three other classes.

![Figure 3. Variation of the SNR](image)

According to the diagram of the SNR, our approach gives a good visibility because the values of SNR are not high and they are very near to the SNR of the other approaches. The little augmentation of the SNR of our algorithm is caused by the repitition of the signature in many regions.

4.2.2. Robustness. First, we have evaluated our watermarking algorithm against RST attacks (translation, scaling and rotation). We noticed the success of the retrieval of the signature after these three attacks. After, we have studied additive random noise on the vertices coordinates and Laplacian smoothing of the mesh. For every attack, we give in the table 3 the robustness of the watermarking and we give the maximum parameter value that can resist the signature. Considering noise addition, we have focused on the noise power as the attack parameter for example fandisk image can resist to the noise attack if the noise power is lower to 0,33. The parameter for smoothing is the number of iterations of the smoothing algorithm. For the four tested images the robustness is achieve if this parameter is lower to 20 iterations. Finally we cropped the 3D mesh by cutting 15% of vertices and we changed the meshing and we removed 1/8 of vertices. We observed that our algorithm is also able to detect the presence of signature after these two attacks.

<table>
<thead>
<tr>
<th>Table 3. Robustness against attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>RST</td>
</tr>
<tr>
<td>Smoothing</td>
</tr>
<tr>
<td>noise</td>
</tr>
<tr>
<td>Reme-shing</td>
</tr>
<tr>
<td>Cropping</td>
</tr>
<tr>
<td>Simplification</td>
</tr>
</tbody>
</table>

![Figure 3. Variation of the SNR](image)
In table 4, we give the number of regions for which, the detector find the signature. We give this number when the marked image is modified with different attacks. We observed that, for every tested image, our detector find the signature in many regions.

Table 4. Number of detected regions

<table>
<thead>
<tr>
<th>Description</th>
<th>Number of Regions</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 attacks</td>
<td>24 4 51 20</td>
</tr>
<tr>
<td>Translation</td>
<td>22 4 45 18</td>
</tr>
<tr>
<td>Rotation</td>
<td>17 4 40 17</td>
</tr>
<tr>
<td>Zooming</td>
<td>15 2 41 13</td>
</tr>
<tr>
<td>Smoothing</td>
<td>17 2 42 14</td>
</tr>
<tr>
<td>Noise</td>
<td>19 3 39 15</td>
</tr>
<tr>
<td>Remeshing</td>
<td>16 2 35 13</td>
</tr>
<tr>
<td>Cropping</td>
<td>10 1 24 9</td>
</tr>
<tr>
<td>Simplification</td>
<td>18 2 27 14</td>
</tr>
</tbody>
</table>

5. Conclusion and perspectives

In this paper, we have presented a new approach of 3D image watermarking which combines three classes of insertion. This combination allows benefiting from the multiple advantages of each class. This is realized by segmenting the 3D image in unrefined regions having different values of curvature and by adapting every region to a class of insertion to obtain the maximum of invisibility of the mark. We have presented first, existing methods using the two possible domains of insertion: spatial (geometric and topologic), spectral and the other types of watermarking. Then, we have presented our method which is based on an hybrid watermarking using the 3D segmentation. A quantitative evaluation in terms of “SNR” was used to measure the quality of the marked image. The robustness of our new method was verified after application of various types of attacks such as RST transformations (rotation, scaling and translation), smoothing, random noise added to vertex coordinates, cropping vertices, simplification and remeshing. This is obtained through to the capacity of our detector to find signature from marked and attacked image.

In perspective, this work can be completed by other studies which can improve it. Indeed, we can find new invariant parameters to the segmentation algorithm. It means that we choose the invariant regions from the original image to mark them. These regions allow us to improve the robustness of the scheme.

6. References


