A new evaluation protocol for robust 3D mesh watermarking

Saoussen Ben Jabra
SIVREC unit of research
Institut Supérieur d'Informatique ISI
Ariana, Tunisia
saoussen.bj@laposte.net

Ezzeddine Zagrouba
SIVREC unit of research
Institut Supérieur d’Informatique ISI
Ariana, Tunisia
ezzeddine.zagrouba@fsm.rnu.tn

Abstract—This paper presents a new evaluation protocol for robust mesh watermarking schemes. This protocol allows comparing different mesh watermarking techniques by measuring their performances score. The last one is based on numerous criteria which are: robustness in front attacks, invisibility, detection type, detected information nature, capacity and complexity. For every criterion, the proposed protocol defines the best and the lowest values and calculates its evaluation score. Finally, a performance score of the given scheme is defined based on these evaluation scores. To evaluate the proposed protocol, we use it to calculate the performances scores for five existing schemes to compare them. Experimental results show that the proposed protocol is simple to use and allows obtaining an efficient comparison of existing mesh watermarking schemes.

I. INTRODUCTION

The recent decade has seen the emergence of 3D meshes in industrial, medical and entertainment applications. Therefore, their protecting from piracy and illegal use has attracted more and more attention in both the research and industrial domains. The solution is watermarking which consists to insert a signature into model and to try to detect it after different manipulations done on marked model. The evolution of 3D watermarking techniques is very fast. Indeed, these techniques are more and more numerous as well as the number of the publications relied to these techniques. These techniques can be geometric (using vertices coordinates to insert signature) [1], or topologic (using mesh facets to mark the mesh) [2] or spectral (using spectral decomposition or wavelet transformation to insert signature) [3,4]. Other techniques are proposed and permit to insert signature by modifying some mesh attributes like texture [5] or silhouette [6]. A comprehensive survey of 3D watermarking techniques can be found in [7].

Nevertheless, the results developed in the diverse publications present only partial tests based on the solution without any effective comparison of the various algorithms. To have this comparison, it is often necessary to reprogram the existing algorithms. This not guaranteed that the realized implementation is also successful as those of the initial authors. By comparing the 3D mesh watermarking with other types of watermarking such as image or audio or video watermarking, we can notice that the other watermarking types already know several protocols which allow estimating effectively the performances of the various algorithms. For the 3D watermarking, the comparison is considered as a difficult process because the 3D objects can have several models of representations as well as the manipulations on 3D objects are very different from an evaluation to the other one.

Based on our knowledge, there exist only one evaluation tool for 3D mesh watermarking proposed by Bennour et al. [8]. This protocol is only based on three main criteria which are: the invisibility, the capacity and the robustness. In this protocol, the authors presented a list of 3D objects which they consider sufficient for the evaluation. Besides, the authors presented a list of usual attacks and gave a score which must be calculated to estimate the robustness of the methods. This score is based on invisibility, robustness and capacity. Concerning the invisibility, this protocol opts for the Hausdorff distance to calculate the distortion between original and marked meshes.

In this paper, a new evaluation protocol is presented. This protocol is based on six criteria. For every criteria an evaluation score is defined depending on its weight in the protocol. In fact, for a robust watermarking scheme, the robustness is the most important criterion so it must have the highest weight in this score. The other criteria are classified based on their importance in watermarking evaluation. Using these evaluation scores, a final score is calculated to evaluate the performances of a given scheme. We also present a list composed by six 3D models selected for the evaluation process. These models are chosen thanks to their different proprieties of vertices and facets number, curvature, etc. Finally, to test the proposed protocol, it is applied for comparing several existing watermarking schemes.

The remainder of this paper is organized as follows: in the next section, the proposed protocol is described by giving the list of test meshes, selected attacks and different evaluation scores. Next, an experimental comparison of six existing watermarking schemes is presented and obtained results are discussed. Finally, conclusions and perspectives are drawn.

II. THE PROPOSED PROTOCOL

An evaluation system must present a maximum of simplicity and flexibility to be easily used and accepted by many researchers. In the proposed protocol, the goal is to
provide a generic and standard tool allowing estimating the performances of 3D watermarking algorithms by taking into account several aspects which are: capacity, invisibility, robustness, complexity, detection type and nature of the detected information. Fig 1 presents the proposed evaluation protocol.

A. Selected meshes

The performances of a 3D watermarking algorithm depend on 3D used models. In fact, some algorithms are dedicated to a specific 3D objects type and other algorithms are more generic. A robust evaluation system needs to define a list of varied 3D models to test the performances of proposed watermarking. We have selected several representative meshes (with different numbers of vertices and different shape complexities) as the test models. Figure 2 presents these chosen 3D meshes in their simplified form: Bunny (34835 vertices), Dragon (50000 vertices), Venus (100759 vertices), Horse (112642 vertices), rabbit (70658 vertices) and cow (2904 vertices).

B. Invisibility estimation

Invisibility estimation of a 3D watermarking scheme consists in estimating the similarity between two 3D objects: the original and the marked object. Several metrics for estimating the difference between two 3D models were proposed. Among these metrics, we can notice the Hausdorff distance \[9\], volume based measures \[10\], minimal energy based measures and curvature based measures \[11\]. In the proposed protocol, the symmetric Hausdorff distance is used. This metric is chosen because it is well correlated to perception for quite similar meshes, guaranteeing a specific error bound between two meshes.

C. Signature capacity

The capacity is the information quantity which can be hided in a 3D model. The number of bits which we can insert is strictly related to the object nature and to the aimed application. Usually, 16 to 64 bits are enough to assure a copyright protection application but not to hide explicit data as the logo of a society or to assure the integrity of the document.

D. Extraction type

There exist two mark extraction types: blind if the original model is needed at detection or not otherwise. At non blind detection, the original object must be present with the marked object to extract the mark. This detection type limits the application domains of the corresponding watermarking and also increases the complexity of the extraction step. In a blind extraction, only the key used for insertion must be present at extraction. This second detection type is more interesting than the first type.

E. Selected attacks

For all applications of 3D watermarking, the robustness is a fundamental criterion to be taken into account during the conception of a watermarking algorithm. However, it is necessary to notice that a technique of watermarking can never be robust to all attacks. We selected for the proposed evaluation protocol a set of attacks from the tests realized in the different publications. These selected attacks can be classified in two main classes: geometric attacks and topologic attacks. In a geometry attack, only the vertex coordinates are modified while the mesh connectivity is kept unchanged. The proposed evaluation protocol proposes to test the following geometry attacks:
1) **RST attacks**: these attacks include rotation, scaling and translations. A robust or a fragile watermarking should be able to survive after these three attacks or after their combination. These attacks always keep the mesh shape intact. For each attack, the robustness is calculated by giving the maximum of the attack parameter value that can resist the signature. This parameter is presented by the angle of the applied rotation, by the value of translation for every axis and by zooming percentage.

2) **Noise addition**: The noise addition (Gaussian noise or random uniform noise, etc.) is an important attack. In the proposed protocol, we add a random uniform noise with different percentages and the robustness is evaluated by the maximum percentage values that can resist the watermarking.

3) **Smoothing**: Smoothing aims to remove the noise introduced during the mesh generation process through 3D scanning. For the proposed evaluation protocol, we choose to carry out Laplacian smoothing [12] on watermarked meshes, with different iteration numbers.

   In a connectivity attack, the adjacency relationship between vertices is changed. For this class of attacks, the following attacks are chosen:

4) **Simplification**: This manipulation allows accelerating the transmission of the 3D model on the network. It is often considered as the most competitive attack within the community of 3D watermarking. To test the robustness of this attack, we reduce the vertices number with many percentages and robustness is measured by the maximum of simplification percentage that can resist the signature.

5) **Remeshing**: Some complex treatments which may be done on 3D meshes need a particular connectivity (regular connectivity with a defined valence or a connectivity of subdivision, etc.). A pre-treatment is so necessary: the original object will be remeshed to have the needed connectivity. This attack also modifies the representation of the mesh and presents a dangerous manipulation for watermarking schemes. We propose to change the original mesh by inverting some edges of the marked mesh.

6) **Cropping**: Concerning this attack, one part of the watermarked mesh is cut off and thus lost. A robust watermarking algorithm should resist to this attack. The proposed evaluation protocol proposes to test many cropping with different percentages.

**F. Final score**

Given that the proposed protocol is intended for robust watermarking methods thus the robustness criterion in front of attacks is considered as the most important parameter in this protocol. Therefore, this parameter must have the biggest coefficient in the calculation of the final score. This last one should take into account several criteria which are in the increasing degree of importance: the robustness in front of attacks, invisibility, detection type, detected information nature, capacity and lastly the complexity because for this last parameter it is important only if the watermarking process is designed for an application which need a minimal calculation time. So, we begin by calculate the robustness score.

Eight attacks are applied on marked meshes and every attack presents an evaluation parameter which can define the level of robustness of the watermarking to the corresponding attack. We improve the classification of robustness levels used in [8]. This classification defines three levels: high, moderate and low. For every attack we present in table 1 the values of the evaluation parameters for every level.

<table>
<thead>
<tr>
<th>Attack/level</th>
<th>low</th>
<th>moderate</th>
<th>high</th>
</tr>
</thead>
<tbody>
<tr>
<td>Translation</td>
<td>2</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>Rotation</td>
<td>2</td>
<td>20</td>
<td>180</td>
</tr>
<tr>
<td>Zooming</td>
<td>3/4(out), 4/3(in)</td>
<td>1/3(out), 2/3(in)</td>
<td>1/6(out), 1/6(in)</td>
</tr>
<tr>
<td>Noise</td>
<td>2%</td>
<td>20%</td>
<td>40%</td>
</tr>
<tr>
<td>Simplification</td>
<td>10%</td>
<td>30%</td>
<td>70%</td>
</tr>
<tr>
<td>Cropping</td>
<td>1/8</td>
<td>1/3</td>
<td>1/2</td>
</tr>
<tr>
<td>Remeshing</td>
<td>1</td>
<td>2-3</td>
<td>6-10</td>
</tr>
</tbody>
</table>

The robustness score $S_r$ is defined by the following equation:

$$S_r = \sum_{\text{meshes}} \left( \frac{1}{n} \sum_{\text{attacks}} v \right)$$

Where $v=1/3$ if the level is low, 2/3 if level is moderate and 1 if level is high. If the watermarking can’t resist in front of all attacks then $v=0$. The robustness score is a scalar included in $[0,6]$. $S_r=0$ if the detection fails for every attack and $S_r=6$ if the robustness level is high for every attack.

For invisibility score, it depends on obtained Hausdorff distances values. If these values are lower than 0.03 then invisibility is high and invisibility score $S_{inv}=3$. If these values are included between 0.03 and 0.06, invisibility is considered as good and $S_{inv}=2$. Finally, if invisibility is higher than 0.06 it is considered as moderate and $S_{inv}=1$.

For detection type criterion, it can be blind or not. If it is blind, blindness score $S_{blind}=1$ and $S_{blind}=0$ otherwise.

The next criterion is the nature of detected information. This information can be a simple confirmation of watermarking and in this case, the corresponding score $S_{ind}=1$. The detection result can contain other information like attack type done on marked image and in this case $S_{ind}=2$.

For complexity, $S_{com}=0.5$ if it is lower than one minute else $S_{com}=0$. Finally, for capacity, $S_{cap}=0.5$ if the signature contains more than 64 bits and $S_{cap}=0$ otherwise.

Based on the evaluation scores ($S_r$, $S_{inv}$, $S_{blind}$, $S_{ind}$, $S_{com}$ and $S_{cap}$), the final performances score can be calculated. The six scores haven’t the same weight. For example, the robustness score $S_r$ can achieve the value 6 so $S_r$ has the maximum ponderation in the final score calculation. This score is equal to the sum of all evaluation scores and is presented by a float included between 0 and 13 and it is defined by the following equation:

$$\text{Final score} = S_r + S_{inv} + S_{blind} + S_{ind} + S_{com} + S_{cap}$$


III. COMPARATIVE STUDY

To test the proposed protocol, it is applied to compare five existing watermarking schemes: geometric [1], topologic [2], spectral [3], geometric based on maximally stable meshes [13] and hybrid watermarking based on maximally stable meshes detection and multi-signatures embedding [14]. Figure 3 presents Haussdorff distances obtained for the five schemes. This figure shows that the two last schemes ([13] and [14]) present the best invisibility. This good result is obtained because only stable regions are marked in this two schemes.

![Fig. 3. Invisibility comparison](image)

Table 2 presents different evaluation scores and final performances scores obtained for every scheme. These schemes present different scores included between 7,25 and 11,33. The best final score is achieved by [14] thanks to the use of a combination of several watermarking schemes and this permits to profit from their advantages.

**TABLE II**

<table>
<thead>
<tr>
<th>Scheme</th>
<th>$S_{rob}$</th>
<th>$S_{inv}$</th>
<th>$S_{det}$</th>
<th>$S_{cmp}$</th>
<th>$S_{com}$</th>
<th>$S_{final}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>[14]</td>
<td>3</td>
<td>5,33</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>[13]</td>
<td>3</td>
<td>4,5</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>9,5</td>
</tr>
<tr>
<td>[11]</td>
<td>2</td>
<td>2,25</td>
<td>1</td>
<td>0</td>
<td>0,5</td>
<td>7,25</td>
</tr>
<tr>
<td>[2]</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0,5</td>
<td>8</td>
</tr>
<tr>
<td>[3]</td>
<td>2</td>
<td>3,33</td>
<td>1</td>
<td>0</td>
<td>0,5</td>
<td>8,33</td>
</tr>
</tbody>
</table>

In figure 4, the variation of final score of different compared schemes is presented. We can notice that no scheme can have a final score equal to the maximum value (13). This is evident because when a criterion is increased, the other criteria can be decreased. In more, every watermarking scheme is designed for a different application domain and it need to verify some criteria and don’t need to satisfy others.

![Fig. 4. Final scores variation](image)

IV. CONCLUSION

In this paper, a new evaluation protocol for robust 3D mesh watermarking schemes is presented. This protocol is based on six criteria: robustness, invisibility, detection type, detected information nature, complexity and capacity. This protocol permits to calculate for every criterion an evaluation score and to generate a final score which presents the performances measure of the watermarking scheme. To test this protocol, several schemes are compared and their final score are calculated to evaluate their performances. Experimental results prove that the proposed protocol allows comparing efficiently different schemes. In more, it is easy to use.

As future work, this protocol can be improved by adding other criteria related to fragile schemes and to schemes designed to image indexing.

REFERENCES


