Table of Contents

Research Articles

1 A Marked Point Process Model Including Strong Prior Shape Information Applied to Multiple Object Extraction From Images
Maria Kulikova, INRIA Sophia-Antipolis, France
Ian Jermyn, INRIA Sophia-Antipolis, France
Xavier Descombes, INRIA Sophia-Antipolis, France
Elena Zhizhina, Institute of Information Transmission Problems (IITP), Russia
Josiane Zerubia, INRIA Sophia-Antipolis, France

14 A Robust Embedding Scheme and an Efficient Evaluation Protocol for 3D Meshes Watermarking
Saoussen Ben Jabra, Institut Superieure d’Informatique, Tunisia
Ezzeddine Zagrouba, Institut Superieure d’Informatique, Tunisia

31 Direct 3D Information Determination in an Uncalibrated Stereovision System by Using Evolutionary Algorithms
Alain Koch, Université de Bourgogne, France
Albert Dipanda, Université de Bourgogne, France
Claire Bourgeois-République, Université de Bourgogne, France

43 Construction of 3D Triangles on Dupin Cyclides
Bertrand Belbis, Université de Bourgogne, France
Lionel Garnier, Université de Bourgogne, France
Sebti Foufou, Université de Bourgogne, France, and Qatar University, Qatar

59 Evaluation Approach of Arabic Character Recognition
Hanan Aljuaid, University Technology Malaysia, Malaysia
Dzulkifli Mohamad, University Technology Malaysia, Malaysia
Muhammad Sarfraz, Kuwait University, Kuwait
A Robust Embedding Scheme and an Efficient Evaluation Protocol for 3D Meshes Watermarking

Saoussen Ben Jabra, Institut Superieur d’Informatique, Tunisia
Ezzeddine Zagrouba, Institut Superieur d’Informatique, Tunisia

ABSTRACT
This paper proposes two main contributions. In the first one, a 3D mesh watermarking using Maximally Stable Meshes detection and multi-signatures embedding is presented. The originality of this scheme is to detect the attack type applied on marked mesh. In plus, it is robust against numerous attacks, blind and invisible. The proposed scheme uses the Maximally Stable meshes (MSMs) to insert signature. After MSMs detection using an extension of Maximally Stable Efficient Regions, three MSMs are selected to be marked. Then, three different signatures are embedded using three different watermarking schemes. This embedding allows knowing the type of the applied attack by detecting which of the signatures resisted. In more, it maximizes robustness by profiting from advantages of every scheme. The second contribution is a new evaluation protocol for 3D watermarking which allows generating a performance score for 3D mesh watermarking schemes. This protocol is based on six criteria having different weights in performance score computing. Finally, this protocol is used to evaluate the proposed watermarking scheme and to compare it with other algorithms. The obtained results verified the good performances of the proposed algorithm which presents the highest score.

Keywords: 3D Meshes, Robustness, Signature, Stable Regions, Watermarking

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. Many 3D models used for online commerce or entertainment are examples of contents that developers and owners can’t distribute without control over piracy. However, due to the complexity of 3D objects, 3D watermarking is far from the maturity of watermarking algorithms dedicated to audio, image or video watermarking. Basically, watermarking process consists to embed a signature into data and to try to detect it after any manipulation done on marked data. Usually, signature must
be robust 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, and remeshing) and cropping (i.e. cutting part of the 3D model by a plane). Watermarking can be blind or non blind depending on whether the original digital image is needed at extraction, or not.

This paper is organized as follows: an overview of mesh watermarking techniques is provided first. The proposed watermarking scheme is described, and the proposed evaluation protocol for 3D watermarking methods is presented. Experimental results and evaluations are given along with conclusions and perspectives.

**MESH WATERMARKING OVERVIEW**

Recently, 3D meshes have been widely used in virtual reality, medical imaging, video games and computer aided design. A 3D mesh is a collection of polygonal facets targeting to constitute an appropriate approximation of a real 3D object. It possesses three different combinatorial elements: vertices, edges and facets. From another viewpoint, a mesh can also be completely described by two kinds of information. The geometry information gives the positions (coordinates) of all its vertices, while the connectivity information provides the adjacency relations between the different combinatorial elements. Although there are many other 3D representations, such as cloud of points, parametrized surface, implicit surface and voxels, 3D mesh has been a standard of numerical 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 effective model. This fact partially explains why much of the work in the area of 3D watermarking deals with 3D triangle meshes. Although some schemes have been proposed to watermark NURBS (Lee, 2002) and point-sampled surfaces (Cotting et al., 2004).

Existing techniques concerning 3D meshes can be classified in two main categories, depending on whether the watermark is embedded in the spatial domain (by modifying the geometry or the connectivity) or in the frequency domain (by modifying some kind of mesh transformation like spectral decomposition or wavelet transformation).

**Spatial Schemes**

They can be classified in two main categories: geometric schemes which modify vertices coordinates and topologic schemes which modify vertices connectivity.

**Geometric Schemes**

Harte et al. (2002) 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. The Vertex Flood Algorithm (VFA) (Benedenes, 1999) embeds also information in point positions. Given a point p in the mesh, all points are clustered in subsets S, accordingly with their distance to p. Each non-empty subset is subdivided in m + 2 intervals in order to encode m bits. The distance of each point in a subset is modified so that it is placed on the middle of one of the m+2 intervals.

**Topologic Schemes**

Among the topologic class of watermarking schemes, Ohbuchi et al. (1998) 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 (Benedens, 1999). 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.

Frequency Schemes

These schemes embed signature by modifying some mesh transformation like spectral decomposition, wavelet transformation, spherical wavelet...

The first scheme based on spectral decomposition has been proposed by Ohbuchi et al. (2002). An additive watermark is embedded on low pseudo-frequency coefficients (P;Q;R) (the three spectra are embedded in the same way). The decoding retrieves the partition and the correspondence between the original connectivity and the watermarked geometry. Kobbelt and Wu (2005) reported an algorithm that is based on radial basis functions. The construction of these basis functions is relative to the geometric information. This kind of analysis seems effective because it can give a good approximation of the original mesh with just a very limited number of basic functions.

Uccheddu et al. (2004) described a blind one-bit watermarking algorithm with the hypothesis of the statistical independence between the wavelet coefficients norms and the inserted watermark bit string. Thanks to a remeshing step, the above analysis could be extended to irregular meshes. With this idea, Cho et al. (2005) built a fragile watermark to accomplish authentication task in the wavelet domain. This remeshing step can also be done in spherical parameterized space. Jin et al. (2004) used such a technique to insert a watermark into both the coarsest representation and the spherical wavelet coefficients of an irregular mesh.

Attributes Based Schemes

There exist other mesh watermarking techniques that modify some attributes of original mesh. Among these techniques, Li et al. (2004) converted the initial mesh in spherical parameterization domain and watermarked its 2D spherical harmonic transformation coefficients. In fact, parameterization transforms a 3D mesh into a bi-dimensional description, thus probably permits making use of the existing 2D image watermarking algorithms. Bennour et al. (2007) propose to insert signature in the 2D contours of 3D objects and retrieve it in 2D rendered views of the model. Therefore, no 3D data is necessary at the decoding side. At last, Fing et al. (2007) proposed a scheme which embed signature in feature points of original mesh. These feature points are detected from contours of the regions obtained after segmentation of original mesh. These watermarking techniques are robust against 2D attacks and they are usually not blind.

NURBS Representation Based Schemes

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 prin
principle (Lee, 2002) 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.

**Comparative Study**

In this paper, we restrict our work to watermarking methods using 3D mesh representation because only three watermarking classes are used in the proposed approach: geometric, topologic and frequency classes. 3D watermarking overview shows that every class presents robustness against a particular class of attacks. In fact, geometric schemes are generally robust against remeshing and simplification and are usually blind. Contrary, the most topologic schemes can’t resist to remeshing and simplification attacks but they resist to geometric transformations and they are usually blind. Finally, frequency methods can resist to smoothing and noise attacks and their detection can be blind depending on the used transformation. Table 1 presents robustness comparison between these three watermarking classes.

<table>
<thead>
<tr>
<th>Attack / scheme</th>
<th>Geometric</th>
<th>Topologic</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Translation</td>
<td>-</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Rotation</td>
<td>-</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Zooming</td>
<td>-</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Remeshing</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Simplification</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Noise</td>
<td>-</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>Smoothing</td>
<td>-</td>
<td>-</td>
<td>+</td>
</tr>
</tbody>
</table>

**PROPOSED APPROACH OF 3D WATERMARKING**

In this paper, a new approach of mesh watermarking is presented. This approach embeds three different signatures into three stable regions of original mesh. Each signature is inserted using a different watermarking algorithm. This allows obtaining a good robustness by profiting from advantages of every algorithm. In plus, if the mesh is attacked, the type of used attack can be known by detecting which of the signatures resisted.

**Embedding Algorithm**

General algorithm of embedding decomposes to several stages. Given an original mesh M, stable regions R1 are detected using an extension of the well known MSER (Maximally Stable Efficient Regions) (Matas et al., 2002). Three regions R1, R2 and R3 are selected to be marked. These last ones must have the maximum of vertices number to maximize the visual quality of marked mesh. Then, three signatures S1, S2 and S3 are embedded respectively into R1, R2 and R3. S1 is embedded with a topologic scheme, S2 with a geometric scheme and S3 with spectral scheme. Finally, marked meshes are obtained by considering these three marked regions.
Maximally Stable Meshes Detection

Maximally Stable Meshes (MSMs) present an extension of Maximally Stable Extremal Regions (MSER) detector from Matas et al. (2002), which has proven to be one of the best interest point detectors in computer vision. Evaluations by Mikolajczyk and Schmid (2004) as well as Fraundorfer and Bischof (2005) revealed that the MSER detector performs best on a wide range of test sequences. An MSER is a connected region which can be detected in any image whose pixel values are of a totally ordered set. Therefore, MSER detection can be applied to any gray scale image or to any color image, whose RGB values are ordered. All MSERs are detected by an extremal property of the intensity function in the region and on its outer boundary. MSERs have properties that form their superior performance as stable local detector.

Donoser et al. (2006) proposed an extension of MSER for volumetric data and they named them Maximally Stable Volumes MSVs. Each detected MSV provides sets of connected regions (at least one region) within consecutive images of the sequence and, in addition, temporal correspondence information between them. As for MSERs, MSVs present high properties of stability. The authors applied the MSVs for 3D segmentation of medical images.

In the proposed extension, curvature measure is used instead of intensity measure and vertices instead of pixels. The general algorithm used for stable regions detection decomposes into several steps: vertices sorting, extremal regions extraction, area variation computing for every region and MSMs extraction.

In first step, vertices are sorted in the increasing order. The input is a mesh \( M = \{V,F\} \) where \( V \) is a set of vertices: \( V=\{v_i\}, \) \( v_i \in \mathbb{R}^3 \) and \( F \) is a set of edges: \( F \subset V. \) An adjacency (neighborhood) relation \( A \subset V \times V \) is defined: \( v_i \) and \( v_j \) are adjacent \( (v_i A v_j) \) if \( \{v_i,v_j\} \in F. \) In MSER’s definition, the pixels are ordered using intensity values. In the proposed approach, vertices Gaussian curvature measure is used. In fact, curvature estimation is a fundamental tool for analyzing and describing a surface’s behavior. The discrete Gaussian curvature \( K(v) \) of a given vertex \( v \) can be defined as:

\[
K(v) = 2\pi - \sum_{i=1}^{n} \alpha_i
\]

Let \( \alpha_i \) denotes the angle between two successive edges. Every vertices Gaussian curvature presents a threshold.

In second step, extremal regions will be detected. A region \( R \) is a contiguous subset of \( M, \) where for each vertices \( v_i, v_j \in R \) there is a sequence \( v_i, v_1, v_2, ..., v_k, v_j \) and \( v_1Av_2, v_2Av_3, ..., v_kAv_j. \) For every threshold, regions which compose the original mesh are determined but vertices having Gaussian curvature lower or equal to the threshold are only considered. The set of the obtained regions for all thresholds presents the set of extremal meshes.

In third step, the area variation for every region \( R \) is measured. This area variation is defined as:

\[
\rho(R, \Delta) = \left( \left\| R_{\Delta} \right\| - \left\| R_{-\Delta} \right\| \right) / \left\| R \right\|
\]

Where \( |.| \) is the cardinality, \( \Delta \) is a parameter of the function and \( R_\Delta \) presents the smallest extremely mesh that contains \( R \) and has Gaussian curvature which exceeds of at least by \( \Delta \) the curvature of \( R. \) Similarly, let \( R_\Delta \) be the biggest extremely mesh containing \( R \) that has Gaussian curvature which is exceeded by at least \( \Delta \) by \( R. \)

In the last step, a region \( R \) is considered as a Maximally Stable Mesh MSM if its variation ratio \( \rho(R, \Delta) \) presents a local minimum. This means that \( \rho(R, \Delta) \) must be lower than variation ratio of any region directly contained in \( R \) or any region which contains \( R. \)

To test the stability of the obtained MSMs, the original mesh is attacked by many rotations.
with different angles, many translations according to the three axis $x$, $y$ and $z$ and many zooming in and out using different percentages. Then, the defined method of MSM detection is applied on every attacked mesh. The same regions are obtained before and after attacks. This improves the stability of detected regions against tested attacks. Figure 1 presents detection results applied on two test images: “porsche” and “cow” while Figure 2 presents detection results after different rotations and different zooming.

After stable regions detection, the obtained regions are sorted by their vertices number in increase order. Three regions which have maximum vertices number are selected to be marked. The output of this stage is three stable regions $R_1$, $R_2$ and $R_3$.

Maximally Stable Meshes Marking

Given three different signatures ($S_1$, $S_2$ and $S_3$), they are embedded in $R_1$, $R_2$ and $R_3$, using three different watermarking algorithms. $S_i$ is a random sequence with zero mean and unit variance. Every stable region is considered as a mesh and will be marked. $R_1$ is marked by $S_1$ with a topologic algorithm, $R_2$ is marked by $S_2$ with a geometric algorithm and $R_3$ is marked by $S_3$ using a spectral algorithm. The combination of these three algorithms allows obtaining robustness against maximum of attacks.

The first chosen algorithm which embeds the signature $S_1$ is the topologic scheme of Benedens (1999). This algorithm is based on a global traversal of mesh connectivity. Given an
initial triangle, vertices which form a triangle with an adjacent edge of the initial triangle are selected. Then, the heights of adjacent triangles are ordered to determine the order of triangles traversal. This step is repeated for adjacent triangles. The embedding is done by altering the height of the triangles. This algorithm is robust against rotation, translation and uniform scaling and it is blind.

The second algorithm which embeds the signature $S_2$ is the geometric scheme of Harte and Bors (2002). It embeds the 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. During embedding points are ranked with respect to their distance to their neighborhood center. This scheme is robust against topologic transformations (simplification and remeshing) and it is blind.

The last algorithm which embeds signature $S_3$ is the spectral scheme of Cayre et al. (2003). It is a substitutive watermarking scheme based on the flipping of spectral coefficient triplets $(P;Q;R)$. Low pseudo-frequencies are avoided to improve the imperceptibility of the embedding. The watermark is on the contrary inserted on middle and high pseudo-frequencies. This scheme resists against noise and smoothing and it is blind.

The output of this stage is three marked regions $R_1'$, $R_2'$, and $R_3'$ and the marked mesh $M'$ will be reconstituted by these three marked regions. Figure 3 presents the general architecture of embedding stage.

**Detection Algorithm**

General algorithm of detection also decomposes to several stages where the two first ones are similar to those of insertion. In fact, given a test mesh $M''$, stable regions are detected using the same method applied during embedding. Then, the three regions $(R_1'', R_2'', R_3'')$ having the maximum of vertices number are selected. In the next step, the adequate detector is applied on every stable region: the topologic detector is applied to $R_1''$, the geometric detector is applied to $R_2''$ and the spectral detector is applied to $R_3''$. These three detectors are blind because they don’t need original mesh at extraction step. Every detector can fail to find signature and gives 0 as output else it succeeds and gives two type of information as output: 1 (for watermarking confirmation) and the signature which resisted after attacks. The final detection result can contain two information types: failure or success of detection and the resisted signature. This result is 0 (failure) if all detectors fail to find signature and 1 (success) if at least one of detectors gives 1. In this second case, the resisted signature is known and the type of attacks applied on marked images is detected. In fact, if only $S_1$ is detected it means that marked image has been attacked with geometric attacks because $S_1$ is embedded with a topologic scheme which is robust against these attacks. In the same way, if only $S_2$ is detected it means that marked image has been attacked with a geometric attack. Finally, if only $S_3$ is found it means that marked image has been attacked with a smoothing or a noise. Figure 4 presents the general architecture of detection stage.

**Proposed Evaluation Protocol for 3D Mesh Watermarking**

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. Nevertheless, the results developed in the diverse publications present only partial tests led 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 type 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.

Existing Evaluation Protocols

There exist many evaluation tools for image watermarking, video watermarking and audio watermarking such as Checkmark, Certimark, StirMark, and Optimark, etc. Concerning 3D watermarking, the evaluation of the existing techniques presents an important problem but often untidy. Based on our knowledge, there exist only one evaluation tool for 3D mesh watermarking proposed by Bennour et al. (2007). 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. This choice is based on the fact that these five examples present a variety in terms of mesh size (vertices and triangles number), mesh curvature, etc. Besides, the authors presented a list of usual attacks and gave a score which must be calculated to estimate the robustness of the methods. In this score, the authors considered that the various attacks have the same importance. This score is calculated by using the following equation:

$$S_{robust} = \sum \sum \sum R_e s_{extraction}$$

This robustness score is a number included between 0 and 20. They defined three levels of security: low level where honest manipulations of the 3D object do not have to invalidate the
extraction of the mark, moderated where the watermarking scheme has to resist to manipulations which can be hostile and top where the power of attacks for this level of security is relatively high. For every level, the authors defined, for every attack, the values of parameters which they have to respect.

Concerning the invisibility, this protocol opts for the Hausdorff distance to calculate the distortion between original and marked meshes.

Proposed Evaluation 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. Figure 5 presents the proposed evaluation protocol.

3D Meshes Models

The performances of 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 6 presents these chosen 3D meshes in their simplified form: Bunny (34835 vertices), Dragon (50000 vertices), Venus (100759 vertices), Horse
Figure 5. Proposed evaluation protocol

Figure 6. Proposed 3D models
(112642 vertices), rabbit (70658 vertices) and cow (2904 vertices).

**Invisibility Estimation**

Invisibility estimation of a 3D watermarking scheme consists in estimating the similarity between two 3D objects: the original and the modified object. This estimation presents an important necessity in many applications such as simplification, compression, matching and recently watermarking applications. Several metrics for estimating the difference between two 3D models were proposed. Among these metrics, we can notice the Hausdorff distance (Gueziec, 2001), volume based measures (Al- liez & Schmitt, 1999), minimal energy based measures and curvature based measures (Kim & Kim, 2001).

In the proposed protocol, the Hausdorff distance is used. The symmetric Hausdorff distance $H(M_1,M_2)$ between two meshes denoted $M_1$ and $M_2$ is defined as:

$$
\max(\max_{a \in M_1} \min_{b \in M_2}(d(a,b)), \max_{a \in M_2} \min_{b \in M_1}(d(a,b)))
$$

Where $d(a,b)$ stands for the Euclidian distance between points $a$ and $b$ in the 3-D space. This metric is well correlated to perception for quite similar meshes, guaranteeing a specific error bound between two meshes.

**Mark 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 in 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. For the techniques with capacity, the method to estimate the capacity of a 3D watermarking system is to calculate the ratio between the extracted message size and the number of the mesh polygons.

**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.

**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.

**Geometric Attacks**

In a geometry attack, only the vertex coordinates are modified while the mesh connectivity is kept unchanged. Our evaluation protocol proposes to test the following geometry attacks:

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.
Noise addition: In the most of the tests realized in the diverse publications, the authors indicate the robustness of their approach to the addition of a noise (Gaussian noise, random uniform noise, etc.). In the proposed protocol, we propose to add a random uniform noise with different percentages and the robustness is evaluated by the maximum percentage values that can resist the watermarking.

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 (Taubin, 2000) on watermarked meshes, with different iteration numbers N.

Topologic Attacks

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

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.

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. The proposed protocol is designed to robust watermarking algorithms so the remeshing attack must be considered as an important attack. We propose to change the original mesh by inverting some edges of the marked mesh to minimize the angle for a given triangle.

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. Our evaluation protocol proposes to test many cropping with different percentages.

Complexity

The complexity presents the time of the running embedding step and detection step. The complexity is not an important factor in the most of watermarking applications but it is better to reduce the complexity while it doesn’t affect the performances of the watermarking.

Detected Information Nature

The extraction result can contain different information types: the inserted signature or a simple confirmation of watermarking (yes or no) or other information related to the marked mesh. In the last case, with a watermarking confirmation, the detection can give other information like attack type applied on the marked mesh.

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 has to have the bigger 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 (Bennour, 2007). This classification defines three levels: high, moderate and low. For every attack we present in Table 2 the values of the evaluation parameters for every level.

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

$$S_r = \sum_{meshes} \left( \frac{1}{8} \sum_{all v} v \right)$$

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, there are two levels: good and moderate. If the Haussdorff distance is lower than 0.03 the invisibility is high else it is moderate. The detection type can be blind or not. Blindness score is $S_b = 1$ if detection is blind else $S_b = 0$.

**EXPERIMENTAL RESULTS**

The proposed watermarking is evaluated using the proposed protocol. First the embedding is done on the selected models with different signature having different lengths 16 bits to 64 bits.

**Invisibility Results**

Figure 7 presents watermarking results:

Table 3 presents Haussdorff Distance for every tested model:

This table shows that invisibility for all tested meshes is lower than 0.03 and it is considered as high. This high invisibility is evident because only three regions of the original mesh are marked.

**Robustness Results**

The described attacks are applied on marked meshes and the detection step is applied on attacked meshes. The robustness results are described in Table 4.

Table 4 presents the evaluation parameters values for every attack and each tested mesh. The results show that for RST attacks the robustness level is high for all meshes. This high robustness is evident because the embedding is down on Maximally Stable regions which are stable by translation, rotation and zooming. For noise attack, the robustness, smoothing and simplification, robustness is high or moderate and this depends on the mesh complexity. For cropping, only Horse model presents a low robustness level. This low level is due to the choice of the marked stable meshes which are concentrated in the same part for this model.

<table>
<thead>
<tr>
<th>Attack</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(in)</td>
<td>1/6(out), 6(in)</td>
</tr>
<tr>
<td>Noise</td>
<td>5%</td>
<td>20%</td>
<td>40%</td>
</tr>
<tr>
<td>Smoothing</td>
<td>5-10</td>
<td>10-30</td>
<td>30-50</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 remeshing</td>
<td>2-5 remeshing</td>
<td>6-10 remeshing</td>
</tr>
</tbody>
</table>
Using this table, the robustness score $S_r$ can be calculated and we obtained $S_r = 5.33$. This robustness score is very good and prove that the proposed watermarking has high robustness performances.

**Detection Type**

The extraction don’t need the original mesh presence so the proposed watermarking is blind and the blindness score $S_b = 1$. 

**Table 3. Haussdorff distance for all tested meshes**

<table>
<thead>
<tr>
<th>Mesh</th>
<th>Dhaus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bunny</td>
<td>0.0128</td>
</tr>
<tr>
<td>Dragon</td>
<td>0.0154</td>
</tr>
<tr>
<td>Venus</td>
<td>0.0203</td>
</tr>
<tr>
<td>Horse</td>
<td>0.0232</td>
</tr>
<tr>
<td>Rabbit</td>
<td>0.0178</td>
</tr>
<tr>
<td>Cow</td>
<td>0.0211</td>
</tr>
</tbody>
</table>

**Table 4. Robustness results**

<table>
<thead>
<tr>
<th>Attack/mesh</th>
<th>Bunny</th>
<th>Dragon</th>
<th>Venus</th>
<th>Horse</th>
<th>Rabbit</th>
<th>Cow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Translation</td>
<td>15</td>
<td>10</td>
<td>10</td>
<td>15</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>Rottion</td>
<td>180°</td>
<td>180°</td>
<td>180°</td>
<td>180°</td>
<td>180°</td>
<td>180°</td>
</tr>
<tr>
<td>Zooming</td>
<td>1/4, 3</td>
<td>1/6,6</td>
<td>1/6,5</td>
<td>1/6,6</td>
<td>1/4,3</td>
<td>1/6,6</td>
</tr>
<tr>
<td>Noise</td>
<td>20%</td>
<td>30%</td>
<td>20%</td>
<td>40%</td>
<td>20%</td>
<td>20%</td>
</tr>
<tr>
<td>Smoothing</td>
<td>30</td>
<td>40</td>
<td>30</td>
<td>30</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>Simplification</td>
<td>40%</td>
<td>40%</td>
<td>30%</td>
<td>50%</td>
<td>30%</td>
<td>20%</td>
</tr>
<tr>
<td>Cropping</td>
<td>1/3</td>
<td>1/2</td>
<td>1/3</td>
<td>1/8</td>
<td>1/2</td>
<td>1/2</td>
</tr>
<tr>
<td>Remeshing</td>
<td>6</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>6</td>
<td>2</td>
</tr>
</tbody>
</table>
Detected Information Nature

In the proposed watermarking, two types of information are detected at extraction step: the watermarking confirmation and the type of attack done on marked mesh. This is obtained thanks to the use of three different signatures which are embedded using three different watermarking algorithms. Every used algorithm presents robustness against a class of attacks and so, from the detected signature, we can know the attack type applied on marked mesh.

Watermarking Capacity and Complexity

These two criteria are not considered as priority criteria for the proposed watermarking. For the capacity, the signature can’t exceed 64 bits because the embedding is done only on regions which can have a little size. The complexity is not minimal because the watermarking process is decomposed to several steps: MSMs detection, research of feature regions and regions watermarking. The complexity of the watermarking can achieve ten minutes for some test models.

Comparative Study

To improve the performances of the proposed watermarking, it is compared with others algorithms: the three used classic watermarking algorithms and a recent watermarking using maximally stable meshes (Zagrouba & Ben Jabra, 2009). This last one insert the signature in all obtained MSMs using a geometric watermarking. In Figure 8, a comparison of invisibility in term of Haussdorff distance is presented. This figure shows that the proposed watermarking

---

**Figure 8. Invisibility comparison**

---

**Table 5. Performances comparison of different watermarking algorithms**

<table>
<thead>
<tr>
<th>Approach/parameter</th>
<th>$S_1$</th>
<th>$S_2$</th>
<th>Detected information</th>
<th>capacity</th>
<th>complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed approach</td>
<td>5.33</td>
<td>1</td>
<td>Confirmation + attack</td>
<td>&lt;= 64 bits</td>
<td>&gt;= 5 min</td>
</tr>
<tr>
<td>Geometric + MSMs</td>
<td>4.5</td>
<td>1</td>
<td>Confirmation</td>
<td>&lt;= 64 bits</td>
<td>&gt;= 5 min</td>
</tr>
<tr>
<td>Geometric</td>
<td>2.25</td>
<td>1</td>
<td>Confirmation</td>
<td>&gt;= 128 bits</td>
<td>&lt;= 2 min</td>
</tr>
<tr>
<td>Topologic</td>
<td>3</td>
<td>1</td>
<td>Confirmation</td>
<td>&gt;= 128 bits</td>
<td>&lt;= 2 min</td>
</tr>
<tr>
<td>Spectral</td>
<td>3.33</td>
<td>1</td>
<td>Confirmation</td>
<td>&gt;= 128 bits</td>
<td>&lt;= 2 min</td>
</tr>
</tbody>
</table>
presents the lower Hausdorff distance values and so presents the better invisibility.

In Table 5, the robustness score, blindness score, detected information, capacity and complexity for every watermarking are given. Experimental results prove that the proposed watermarking presents the better performances in terms of robustness, blindness and detected information. For complexity and capacity, they are moderate.

CONCLUSION

Robustness and invisibility are usually a trade-off in a watermarking system. However, to satisfy both conditions, this paper proposes a new approach of 3D mesh watermarking which embeds the signature in Maximally Stable Meshes (MSMs) of original 3D mesh. This insertion allows benefiting from the invariance criteria of MSMs. In fact, these regions permit to obtain the same segmentation results before and after attacks thanks to their stability. After MSMs detection, the obtained regions are sorted by their vertices number. Three MSMs which present maximum number of vertices are selected to be marked using three different watermarking algorithms (topologic, geometric and spectral) to profit from their robustness. Every watermarking algorithm embeds a different signature. This allows knowing the attack type applied on marked image. In the second part of this paper, a new evaluation protocol for robust 3D mesh watermarking is proposed. This protocol is based on several criteria and permits to compare different watermarking algorithms. A comparative study between different watermarking using the proposed protocol proved that the new watermarking presents the better performances especially in terms of invisibility and robustness. In more, it permits to obtain additional information at detection.

The future work will attempt to minimize the complexity of MSMs detection to optimize the performances of the proposed watermarking.

REFERENCES


