Three-Dimensional Meshes Watermarking: Review and Attack-Centric Investigation

Kai Wang[1], Guillaume Lavoué[1], Florence Denis[2], and Atilla Baskurt[1]

[1] LIRIS, UMR 5205 CNRS, INSA-Lyon, F-69621 Villeurbanne, France
[2] LIRIS, UMR 5205 CNRS, Université Lyon 1, F-69622 Villeurbanne, France
`{kwang,glavoue,fdenis,abaskurt}@liris.cnrs.fr`

Abstract. The recent decade has seen the emergence of 3D meshes in industrial, medical and entertainment applications. Therefore, their intellectual property protection problem has attracted more and more attention in both the research and industrial realms. This paper gives a synthetic review of 3D mesh watermarking techniques, which are deemed to be a potential effective solution to the above problem. We begin with a discussion on the particular difficulties encountered in applying watermarking on 3D meshes. Then some typical algorithms are presented and analyzed, classifying them in two categories: spatial and spectral. Considering the important impact of the different attacks on the design of 3D mesh watermarking algorithms, we provide an attack-centric viewpoint of this state of the art. Finally, some special issues and possible future working directions are discussed.

Key words: 3D mesh, digital watermarking, copyright protection, authentication, attack, robustness.

1 Introduction

Recently, 3D meshes have been widely used in virtual reality, medical imaging, video games and computer aided design. Basically, a 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 essentially the positions (coordinates) of all its vertices, while the *connectivity* information provides the adjacency relations between the different elements. Figure 1 shows an example of 3D mesh. As illustrated by the close-up, 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 *de facto* 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 a low-level but effective model.

Digital watermarking has been considered as a potential efficient solution for copyright protection of various multimedia contents. This technique carefully

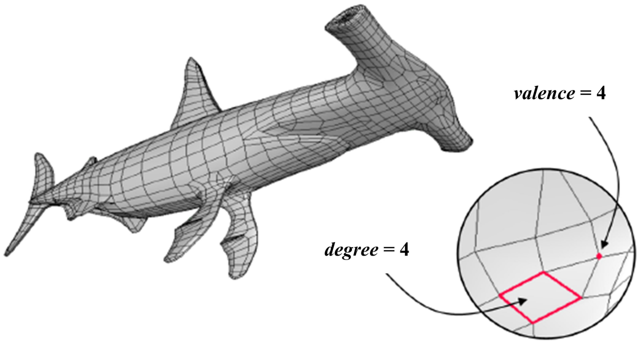

Fig. 1. Example of 3D mesh and a close-up illustrating the *valence* of a *vertex* and the *degree* of a *facet*.

hides some secret information in the cover content. Compared with traditional cryptography, digital watermarking technique is able to protect digital works after the transmission phase and the legal access. There exist different classifications of watermarking techniques. We distinguish *non-blind* and *blind* watermarking schemes depending on whether the original digital work is needed at extraction, or not. Usually, one hopes to construct a *robust* watermark, which is able to go through common malicious attacks, for copyright protection purpose. But sometimes, the watermark is intentionally designed to be *fragile* for authentication applications. Finally, researchers have the habit to group practical watermarking algorithms in two categories, to say *spatial* or *spectral*, according to the insertion domain.

This paper reviews the nearly 10-year history of the research on 3D meshes watermarking techniques since the publication of the first relevant algorithms in 1997 [24]. The remainder of this paper is organized as follows. Section 2 discusses the special difficulties encountered when watermarking 3D meshes, and provides an overview of the most important techniques proposed in the literature. Attacks on watermarked meshes play an important role in the elaboration of suitable watermarking algorithms. They are much more intractable than their counterparts on watermarked images. So section 3 is dedicated to analyze various possible attacks and discuss the corresponding solutions to resist them. Some open questions and possible research directions are given in the last section.

2 3D Meshes Watermarking Techniques

2.1 Difficulties and classification

There still exist few watermarking methods for 3D meshes, in contrast with the relative maturity of the theory and practices of image, audio and video watermarking. This situation is mainly caused by the difficulties encountered while handling the arbitrary topology and irregular sampling of 3D meshes, and the complexity of possible attacks on watermarked meshes.

We can consider an image as a matrix, and each pixel as an element of this matrix. This means that all these pixels have an intrinsic order in the image, for example the order established by row or column scanning. On the contrary, there is no simple robust intrinsic ordering for mesh elements, which often constitute the watermarking primitives. Some intuitive orders, such as the order of the vertices and facets in the mesh file, and the order of vertices obtained by ranking their projections on an axis of the objective coordinate system, are easy to be altered. In addition, because of their irregular sampling, we are still short of an efficient and effective spectral analysis tool for 3D meshes. This situation, as you can see in the following sections, makes difficult to put the "secure spread spectrum" watermarking schemes into practices.

Besides the above point, robust watermarks have also to face to various delicate attacks. The reordering of vertices and facets do not have any impact on the shape of the mesh, while it can seriously desynchronize watermarks which rely on this straightforward ordering. The similarity transformations, including translation, rotation and uniform scaling, are supposed to be common operations through which a robust watermark should survive. Even worse, the original watermark primitives can disappear after a mesh simplification or remeshing. Such tools are available in many softwares, and they can totally destroy the connectivity information of the watermarked mesh while well conserving its shape. Usually, we distinguish geometric attacks, which only modify the positions of the vertices, and connectivity attacks, which also change the connectivity aspect. Section 3 provides a detailed investigation on these attacks and discusses the existing solutions to make the watermarks robust to them.

Watermarking 3D meshes in computer aided design applications introduces other difficulties brought by the design constraints. For example, the symmetry of the object has to be conserved and the geometric modifications have to be within a tolerance for future assembly. Under this situation, the watermarked mesh will no longer be evaluated only by the human visual system that is quite subjective, but also by some strict objective metrics.

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 connectivity) or in the spectral domain (by modifying some kind of spectral-like coefficients).

2.2 Spatial Techniques

As mentioned above, the spatial description of a 3D mesh includes geometry aspect and connectivity aspect. Most existing algorithms take the former as primitives, which shows superiority in both robustness and imperceptibility compared to the latter. This section will take more concerns on watermarking primitives than on robustness, which will be explored in detail in the next section.

Spatial Techniques Modifying the Geometry

Note that no matter the practical primitive is, all the techniques in this subsection are implemented by modifying the coordinates of involved vertices.

The algorithms that modify the vertices positions directly and individually are often fragile techniques. Yeo and Yeung [33] proposed such an algorithm that serves for mesh authentication. The basic idea is to search for a new position for each vertex where two predefined hash functions have an identical value, so as to make all vertices valid for authentication. At the extraction phase, they simply examine the validity of each vertex, and locate the possible attacks on the invalid vertices. In fact, this algorithm depends on a pre-established vertex order, which causes a causality problem. Lin et al. [21] solved this problem and also proposed a more analytic and controllable modification scheme with a better attack localization capability. Cayre and Macq [9] proposed a high-capacity blind data-hiding algorithm for 3D triangular meshes. By choosing the projection of a vertex on its opposite edge in a triangle as the primitive (see Figure 2), the theoretical capacity can attain 1 bit per vertex. The synchronizing mechanism relies on the choice of the first triangle by a certain geometrical criterion, and a further spreading scheme that is piloted by a secret key. Bors [8] also reported a blind algorithm. The primitive is the relative position of a vertex to its 1-ring neighbours. A two-state space division is established, and the vertex is assumed to be moved into the correct subspace according to the next watermark bit.

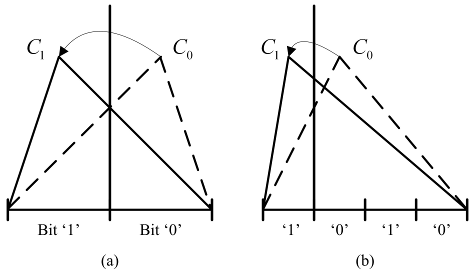

Fig. 2. Watermarking primitive in the algorithm of Cayre and Macq [9], the projection is moved to the nearest correct interval: (a) opposite edge is divided in two intervals; (b) opposite edge is divided in four intervals. The inserted bits are both '1'.

Some other algorithms choose positions of groups of vertices as watermarking primitives in order to strengthen the robustness. Yu et al. [35] gave a non-blind robust algorithm. Vertices are divided into N groups and in each of them is inserted one bit by modifying the length from its member vertices to the gravity centre of the mesh. The modulation scheme is a simple additive method with an adaptive intensity obtained by a local geometrical analysis of the mesh. The extraction is also quite simple, since it is sufficient to regroup the vertices and inverse the additive insertion model. However, to ensure a good robustness, a pre-processing step of registration and resampling is necessary, which makes the algorithm non-blind. In Benedens's "Vertex Flood Algorithm (VFA)" [5], after grouping vertices according to their distances to the centre of a designated triangle, the range of the group interval is then divided into $m = 2^n$ subintervals, and all the group vertices distances to the chosen triangle centre are altered so that the new distances all fall into a certain subinterval that stands for the next n watermark bits.

Facets have several interesting measures for watermarking. Ohbuchi et al. [25] chose the ratio between the height of a triangle and its opposite edge length as primitive to construct a watermarking technique that is intrinsically invariant to similarity transformations (Triangle Similarity Quadruple (TSQ) algorithm). Benedens [5] reported a blind algorithm in which the triangular facet height is quantized. By quantizing the distance of a facet to the mesh centre, Wu and Chueng [31] gave a fragile but high-capacity scheme. In another Benedens's method [4], the Extended Gaussian Image (EGI) of a mesh is established by clustering facets according to their normal directions, then in each "bin" of the EGI, the average normal direction of the group of facets is modified to carry one watermark bit. Since these average normal directions approximately describe the mesh shape, this scheme is demonstrated to be robust to simplification and remeshing. Instead of EGI, Lee et al. [19] adopted Complex EGI for watermarking. One inconvenience of this class of algorithms is that the modification of the positions of the involved vertices is indirect and sometimes quite complex, especially in the last two algorithms.

Watermark embedding can be done in a spherical coordinate system, especially in the distance component $r_i = \sqrt{x_i^2 + y_i^2 + z_i^2}$. We can benefit to elaborate some similarity-transformation-invariant algorithms if the distance component is relative to the mesh centre. Since the component r_i represents the shape of the mesh, its modification is supposed to be more robust than a single x_i, y_i, or z_i component modification. These are two main reasons for why numerous researchers chose to watermark in spherical coordinate system [11, 22, 36].

There exist other spatial techniques that modify the geometry. Ohbuchi et al. [25] presented the "Tetrahedral Volume Ratio Embedding" algorithm that is invariant to affine transformation. Li et al. [20] 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 bidimensional description, thus probably allows to make use of the existing 2D image watermarking algorithms. At last, Bennour et al. [7] propose to insert watermarks in the 2D contours of 3D objects.

To summarize, the main drawback of the techniques that modify the geometry is the relative weak robustness to both geometric and connectivity attacks. For blind schemes, the synchronization issue is really a difficult problem. However, these methods have the advantages of high capacity and localization ability of malicious attacks.

Spatial Techniques Modifying the Connectivity

Actually, there are very few 3D meshes watermarking techniques based on connectivity modification. On the one hand, this kind of watermark is obviously fragile to connectivity attacks, and on the other hand, the introduced modification can be very easy to detect. Ohbuchi et al. [24] presented two such algorithms. In the first one, the local triangulation density is changed to insert a visible watermark. The second algorithm first cuts one band of triangular facets off the mesh, and then glues it to the mesh with just one edge. This facet band can be a meaningful pattern or simply determined by a secret key. Both methods are visible and fragile, but the local distribution of the embedded watermark stops them from being a useful fragile watermark for integrity authentication.

2.3 Spectral Techniques

Most of the successful image watermarking algorithms are based on spectral analysis. A better imperceptibility can be gained thanks to the “spread spectrum” principle. It has a dilution effect of the inserted watermark bits in all the spatial and spectral parts of the carrier. A better robustness can also be achieved if the watermark is inserted in the low and median frequency parts. Unfortunately, for 3D meshes, we haven’t yet an efficient and robust spectral analysis tool. Moreover, the lack of a natural parameterization makes spectral analysis even more difficult. As it can be seen in the following subsections, almost all the existing tools have their limitations. Besides the algorithms that embed watermarks in the spectrum obtained by a direct frequency analysis, we also present here the class of algorithms that are based on multiresolution analysis. The basic idea behind both of them is the same: modification of some spectral-like coefficients.

Spectral Techniques Based on Direct Frequency Analysis

Researchers have tried different types of basis functions for this direct frequency analysis. For Laplacian basis functions, a matrix of dimension $n \times n$ (n being the number of vertices) is constructed based on mesh connectivity. Then $3n$ spectral coefficients are calculated as the projections of the three coordinates vectors of all the vertices on the eigenvectors of this Laplacian matrix. Based on this analysis, Ohbuchi et al. [27] proposed a non-blind method (additive modulation of the low and median frequency coefficients) while Cayre et al. [10] gave a semi-blind one (quantization of the low and median frequency coefficients). There exist two serious problems with the Laplacian frequency analysis. The computation time increases rapidly with mesh complexity due to the diagonalization of the $n \times n$ Laplacian matrix. Moreover, the analysis procedure depends on the mesh connectivity information. The first problem forced the authors to cut the original mesh into several patches possessing fewer vertices. To overcome the fragility to connectivity change, the authors proposed a pre-processing step of resampling at the extraction to recover exactly the same connectivity as the cover mesh.

Wu and Kobbelt [32] 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 basis functions. So calculation time can be greatly saved. In spite of this improvement, the algorithm remains sensible to various attacks, that's why the authors still proposed to do registration and resampling before the real extraction. With the similar objective to solve the computation performance issue, Murotani and Sugihara [23] proposed to watermark the singular spectral coefficients. In this method, the matrix to be diagonalized has a much lower dimension.

Although current 3D mesh spectral analysis tools are not efficient enough, they provide the opportunity to directly transplant the existing mature spectral watermarking techniques of digital images.

Spectral Techniques Based on Multiresolution Analysis

Multiresolution analysis is a useful tool to reach an acceptable trade-off between the mesh complexity and the capacity of the available resources. Such an analysis produces a coarse mesh which represents the basic shape (low frequencies) and a set of details information at different resolution levels (median and high frequencies). These methods also allow to realize a synthesis process during which multiple representations with different complexities can be created.

The most interesting point of multiresolution analysis for watermarking is its flexibility. There are different available locations allowing to meet different application demands. For example, insertion in the coarsest mesh ensures a good robustness, while embedding in the details parts provides an excellent capacity. The insertion in low resolution can be both more robust and more imperceptible thanks to a dilution effect. The insertion in high resolution level may permit to construct some effective fragile watermarks with a precise localization ability of the attacks.

Wavelets are a common tool for such a multiresolution analysis. Figure 3 shows the wavelet decomposition of a dense rabbit mesh, the watermark can be inserted either in the coarsest mesh, or in the wavelet coefficients at different levels. In fact, these wavelet coefficients are 3D vectors associated with each edge of the corresponding coarser mesh. Note that this kind of wavelet analysis is applicable only on semi-regular triangular meshes. Based on this wavelet analysis, Kanai et al. [15] proposed a non-blind algorithm that modifies the ratio between a wavelet coefficient norm and the length of its support edge, which is invariant to similarity transformations. Uccheddu et al. [29] 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. [12] extended the algorithm of Yeo and Yeung in the wavelet domain. This remeshing step can also be done in spherical parameterized space. Jin et al. [14] used such a technique to insert a watermark into the coarsest representation and the spherical wavelet coefficients of an irregular mesh. Using a direct irregular mesh wavelet analysis tool without any assistant remeshing step, Kim et al. [16] elaborated a blind algorithm. Other multiresolution analysis tools, such as the edge-collapse iterations technique [28] and the

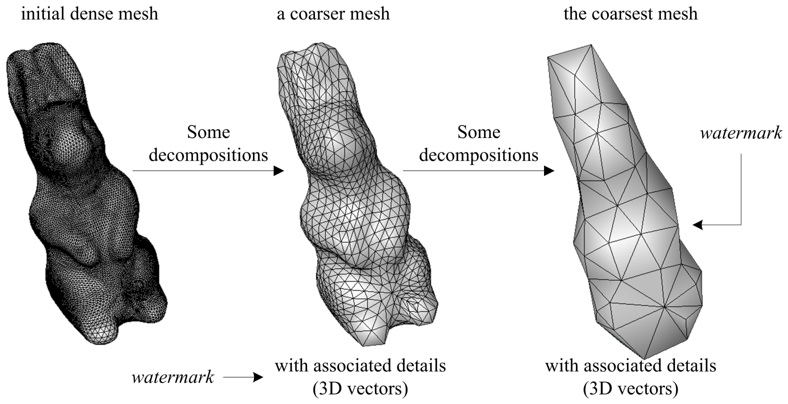

Fig. 3. 3D mesh watermarking techniques based on wavelet analysis.

Burt-Adelson pyramid decomposition [34], are employed to develop robust 3D mesh watermarking algorithms.

Nonetheless, as the current direct spectral analysis tools, the available multiresolution analysis schemes have either connectivity restrictions or robustness deficiencies (especially to connectivity attacks). And for majority of these techniques, registration and resampling are recommended to ensure a sufficient robustness. But this inevitably makes the algorithms non-blind.

3 Attack-Centric Investigation

As mentioned in subsection 2.1, attacks constitute an indispensable factor when designing 3D meshes watermarking algorithms. In this section, we carefully discuss three types of attacks and introduce the existing solutions in the literature.

3.1 Robustness to Geometric Attacks

This kind of attacks only modifies the geometric part of the watermarked mesh. No matter what is the nature of the geometric change, the attack is reflected by a modification of vertices positions.

Similarity Transformations. Similarity transformation is considered to be a common operation rather than an attack, against which even a fragile watermark should be able to stand. It includes translation, rotation, uniform scaling, and the combination of the above three operations. Generally speaking, there are three different strategies to build a watermark that is immune to this attack.

The first solution is to use some primitives that are invariant to similarity transformations. Ohbuchi et al. [24] gave a list of such primitives. The most utilized is the ratio between two measures of a triangle (height or edge length). The primitives in most of the blind spatial techniques are also invariant to similarity transformations, like the primitives in the methods of Cayre and Macq

[9], Bors [8], and Cho et al. [11]. Practically, these primitives are all some relative measures between several absolute and individual ones, and they embody the similarity between different meshes. The similarity transformation, like its name, will always keep these relative measures unchanged. Fortunately, not only the watermarking primitives are kept unchanged, but also most synchronization schemes are insensible to this kind of attack. Moreover, if we expect a robustness even to affine transformations, the Nielson-Foley norm can be a good primitive candidate [6, 30].

The second solution is to watermark in an invariant space. One such space can be obtained by doing the following steps [22, 36].

1. Translate the origin of the coordinate system to the mesh gravity centre.
2. Calculate the principal axes of the mesh and rotate the object so that they coincide with axes of the coordinate system.
3. Do a uniform scaling so that the whole mesh is bounded in a unit sphere/cube.

Then the watermark is inserted in this new space. But the causality problem arises because the variables used in precedent steps, such as the gravity centre and principle axes orientations are probably changed after watermark insertion. So there will possibly exist some extent of errors when reconstructing this space at the extraction. If a precise extraction is demanded, we have to memorize these original values, but this will make the technique at least semi-blind.

The third solution is to carry out registration of the input mesh at extraction with the original non-watermarked one. Low-precision registration methods use singular spectral coefficients [23], eigenvectors of the vertices correlation matrices [26], inertial moments [27], and characteristic points [32] of the two meshes. High-precision methods often need user interactions to determine a good initial condition and the registration is realized by iteratively minimizing a sum of local errors [27, 34]. This solution will obviously make the algorithms non-blind, but provides a better robustness.

Signal Processing Attacks. A mesh can be considered as a signal in a three-dimensional space. There are counterparts of the traditional one-dimensional signal processing techniques for 3D meshes, such as random additional noise, smoothing, enhancement, and lossless compression (usually realized by quantization). Figure 4.b and 4.c illustrate two examples. Although these operations can be very harmful to inserted watermarks, they are really common manipulations in animation and special effects applications.

Random noise, smoothing, and enhancement can be modeled in the spectral domain by a modification of the high-frequency part. Quantization can be thought as a certain form of noise, but its effect is somewhat complicated. Generally speaking, the spectral watermarking techniques that modify the low and median frequency parts are more robust to these attacks, as demonstrated by Praun et al. [28]. Their method is among the most robust in the literature. Note that for the additive watermarking scheme, insertion in the low frequency part is both more robust and more imperceptible. Different modulation schemes have

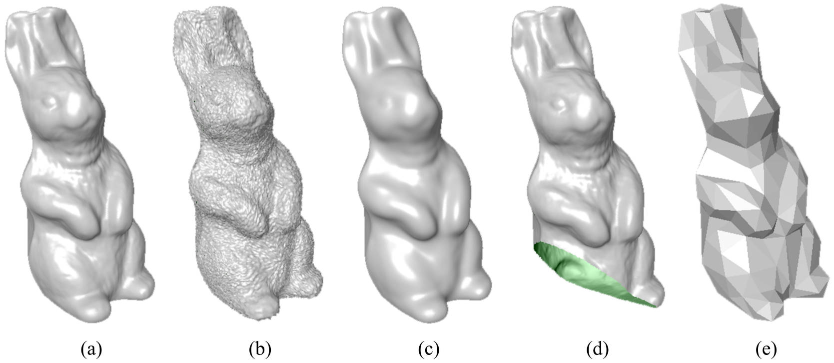

Fig. 4. Original mesh and four examples of attacked meshes: (a) original rabbit mesh; (b) random additive noise; (c) smoothing; (d) cropping; (e) simplification.

been developed. Ohbuchi et al. [26] proposed to repeat the watermark insertion in the first half of the spectrum with a constant intensity. Wu and Kobbelt [32] watermarked only the very low frequency coefficients and proposed an adaptive insertion intensity that is proportional to the absolute value of the coefficient. Lavoué et al. [18] gave another modulation scheme, in which the intensity is linear for the low and median frequency coefficients and constant for the high frequency part.

Spatial techniques are less robust to signal processing attacks. One good measure is to search for an adaptive spatial insertion intensity founded on local geometric analysis. This analysis can be based on the average length of the incident edges of a vertex [3], the geometric distortion introduced by a vertex split operation [28], the minimal incident edge length of a vertex [34], or the possible normal direction variance of the incident facets of a vertex after insertion [35]. The basic idea is to increase the watermarking intensity where are located the significant parts of the mesh shape, while keeping the visual quality. At last, redundant insertion [26] and use of error correction code [18] can sometimes significantly reinforce the robustness to these attacks.

Local Deformation Attacks. A local deformation is sometimes imperceptible if we haven't the original mesh for comparison, but it can seriously disturb the watermark, especially the synchronization process. One natural solution is to divide the mesh into several patches and repeat the watermark insertion in each patch. This division can be based on curvature or semantic analysis. As mentioned previously, division in patches may also decrease the insertion time for some spectral techniques.

3.2 Robustness to Connectivity Attacks

This class of attacks includes cropping, remeshing, subdivision and simplification. In general, they are quite difficult to handle.

Cropping is a special attack (see Figure 4.d for an example), and some researchers prefer to regard it as a geometric attack because its consequence is quite similar to the one caused by local deformation. Watermark repetition in different patches seems the most efficient way to resist cropping.

As far as the other attacks (Figure 4.e illustrates an example of simplification), the algorithms which take the average normal direction of a group of facets [4, 19], or the distances of a group of vertices to the mesh centre [11] as primitives, seem less sensible. Their primitives are approximately conserved after connectivity modification. Other spatial techniques are less robust by reasons of both the geometric change of the primitives and the desynchronization problem. The basis function construction and the frequency coefficients calculation in direct spectral analysis are either dependent to vertices order or to mesh connectivity. The existing multiresolution analysis tools often have connectivity restrictions, and the remeshing step is not robust enough to connectivity change. So, to attain a sufficient robustness for these methods, the authors usually recommend doing a pre-processing step of connectivity restoration before extraction. This restoration procedure can be considered as a resampling of the extraction input mesh (objective mesh) so as to obtain the same connectivity configuration as the cover mesh [27, 34, 35] or the non-attacked stego-mesh [32] (reference mesh). The task is to find, for each vertex in the reference mesh, a corresponding point on the surface of the objective mesh. This correspondence can be established by the nearest neighbour criterion [32], ray intersection [27, 35], or iterations targeting to minimize a particular cost function [34].

Two other possibilities to handle connectivity attacks are to find a robust transformation or parameterization domain that is independent to connectivity, and to watermark some robust mesh shape descriptors.

3.3 Robustness to Other Attacks

This group contains mainly three attacks: file attack, format attack, and representation attack. The file attack simply consists of reordering the vertices and/or the facets in the mesh description file. The mesh file format conversion attack may alter the underlying mesh data structure, so the intrinsic processing order of the vertices and facets can also be changed. To be invariant to these two attacks, it just needs to turn the synchronization scheme independent to these intrinsic orders. The representation conversion may be the most destructive attack to 3D mesh watermarks, because after such an attack, the mesh itself will no longer exist (for example, an approximation of a mesh with a NURBS model). Until now, no researcher has mentioned robustness to this attack. In our opinion, the two ideas given at the end of the last subsection can also be potential solutions to this serious attack.

4 Discussions and Perspectives

Table 1 presents a comparison of some typical algorithms of each class. The values in the column “Inserted bits” are the ones reported in the original papers. Most robustness performances are evaluated by a sign ranging from '−−', which means the least robust, to '++', which stands for the most robust. In our opinions, there exist many valuable research topics in 3D meshes watermarking:

Classic Problem: Trade-off between Capacity, Robustness, and Imperceptibility. These measures are often contradictory. For example, an important watermarking intensity gives a better robustness, but normally degrades the visual quality of the watermarked mesh and risks to make the watermark perceptible. The redundant insertion could considerably strengthen the robustness, but meanwhile unavoidably decreases the capacity. Local adaptive geometric analysis seems favorable to find optimal watermarking parameters in order to achieve a well compromise between these indicators.

Algorithms Evaluation. So far, the research community has been lacking of a widely used performance evaluation system of the existing algorithms. We need a standard attack benchmark and distortion measurement. The distortion introduced by watermarking can be either evaluated by objective geometric distortion, or by perceptual distortion measure [1, 13, 17].

Construction of Robust and Blind Algorithms. The elaboration of such an algorithm attracts the attention of many researchers considering its satisfactory flexibility and reliability. In our opinion, this requires at least to overcome two difficulties. The first one is to build a robust and secure synchronization mechanism, especially for spatial techniques. Using certain robust aspect of the mesh to locate and index the watermarking primitives seems a good idea. At the same time, the separation of synchronization primitives from watermarking primitives can prevent the causality problem. The second difficulty is to avoid the registration and resampling pre-processing steps, which target to ensure the robustness. As mentioned before, global and robust shape descriptors or transformations, like geometric moments, spherical harmonic transformation, can be a good start point. Another possibility is to introduce a remeshing step at both insertion and extraction sides. First of all, the cover mesh (possibly irregular) is remeshed to generate a corresponding semi-regular mesh with a similar geometrical shape. Then watermarks are inserted in this semi-regular mesh. For extraction, we suppose that a mesh with the same semi-regular connectivity can be reconstructed. Here, the connectivity issue is supposed to be solved, and the watermarks in the semi-regular mesh are assumed to be blind and geometrically robust. The key point lies in elaborating a remeshing scheme which is insensitive to connectivity change. Alface and Macq have done some work in this direction [2].

Other Perspectives. Other research topics include informed 3D mesh watermarking techniques, hierarchical watermarks, 3D mesh digital fingerprints, and the interplay between compression and watermarking, or between subdivision and watermarking.

Table 1. Comparison of different 3D mesh watermarking techniques.

Categories	Algorithms	Clearly controllable intensity	Inserted bits	Blind	Local adaptability
Spatial techniques on vertices	Yeo and Yeung [33]	No	1 bit/vertex	Yes	No
	Lin et al. [21]	Yes	1 bit/vertex	Yes	No
	Cayre and Macq [9]	Yes	1 bit/vertex	Yes	No
	Yu et al. [35]	Yes	≈50 bits	No	Yes
	VFA [5]	Yes	≈900 bits	Yes	No
	Bors [8]	No	0.2 bits/vertex	Yes	Yes
	Cho et al. [11]	Yes	≈50 bits	Semi	No
Spatial techniques on facets	TSQ [24, 25]	No	1.2 bits/facet	Yes	No
	Benedens [4]	Yes	≈30 bits	Semi	No
	Lee at al. [19]	Yes	≈50 bits	Semi	Yes
Other spatial techniques	Li et al [20]	No	24 bits	No	No
	Bennour et al. [7]	Yes	≈500 bits	No	No
Direct spectral techniques	Ohbuchi et al. [27]	Yes	32 bits	No	No
	Cayre et al. [10]	Yes	64 bits	Semi	No
	Wu and Kobbelt [32]	Yes	24 bits	No	No
	Alface and Macq [2]	Yes	64 bits	Yes	No
Multiresolution spectral techniques	Kanai et al. [15]	Yes	≈620 bytes	No	No
	Uccheddu et al. [29]	Yes	Not clear	Yes	No
	Praun et al. [28]	Yes	50 bits	No	Yes
	Yin et al. [34]	Yes	250 bits	No	Yes

Continuation of Table 1. Robustness to different attacks

Algorithms	Similarity transform.	Signal processing attacks	Local deform. and cropping	Connectivity attacks	Elements reordering
Yeo and Yeung [33]	−−	−−	Localization*	−−	Fragile
Lin et al. [21]	−−	−	Localization*	−−	Invariant
Cayre and Macq [9]	++	−	−	−−	Invariant
Yu et al [35]	Registration	+	−	Resampling	Invariant
VFA [5]	+	−	−	−	Invariant
Bors [8]	++	−	+	−−	Invariant
Cho et al. [11]	++	+	+	−	Invariant
TSQ [24, 25]	++	−	+	−−	Invariant
Benedens [4]	Registration	+	−	+	Invariant
Lee et al. [19]	Registration	+	+	+	Invariant
Li et al. [20]	+	+	+	Resampling	Invariant
Bennour et al. [7]	Registration	+	+	−	Invariant
Ohbuchi et al. [27]	Registration	++	++	Resampling	Resampling
Cayre et al. [10]	+	+	++	−−	Fragile
Wu and Kobbelt [32]	Registration	++	++	Resampling	Resampling
Alface and Macq [2]	+	+	++	+	Fragile
Kanai et al. [15]	+	−	−	−−	Invariant
Uccheddu et al. [29]	−	+	−	−	Invariant
Praun et al. [28]	Registration	++	++	Resampling	Resampling
Yin et al. [34]	Registration	+	−	Resampling	Resampling

* "Localization" means the ability of localizing attacks for the fragile algorithms.

Acknowledgments. The research work of the first author is funded by China Scholarship Council of Chinese government.

References

1. Alface P.R., Craene M.D., and Macq B., Three-Dimensional Image Quality Measurement for the Benchmarking of 3D Watermarking Schemes, Proceedings of SPIE-IS and T Electronic Imaging, vol. 5681, 2005, pp. 230-240
2. Alface P.R., and Macq B., Feature-Based Watermarking of 3D Objects Towards Robustness against Remeshing and De-synchronization, Proceedings of SPIE-IS and T Electronic Imaging, vol. 5681, 2005, pp. 400-408
3. Ashourian M., and Enteshary R., A New Masking Method for Spatial Domain Watermarking of Three-Dimensional Triangle Meshes, Proceedings of IEEE Region 10 Annual International Conference, vol. 1, 2003, pp. 428-431
4. Benedens O., Geometry-Based Watermarking of 3D Models, IEEE Computer Graphics and Applications, vol. 19, no. 1, 1999, pp. 46-55
5. Benedens O., Two High Capacity Methods for Embedding Public Watermarks into 3D Polygonal Models, Proceedings of the Multimedia and Security-Workshop at ACM Multimedia, 1999, pp. 95-99
6. Benedens O., and Busch C., Towards Blind Detection of Robust Watermarks in Polygonal Models, Computer Graphics Forum, vol. 19, no. 3, 2000, pp. 199-208
7. Bennour J., Garcia E., and Dugelay J.L., Watermark Recovery from 2D Views of a 3D Object Using Texture or Silhouette Information, Journal of Electronic Imaging, July-August 2007 (to appear)
8. Bors A.G., Watermarking Mesh-Based Representations of 3-D Objects Using Local Moments, IEEE Transactions on Image Processing, vol. 15, no. 3, 2006, pp. 687-701
9. Cayre F., and Macq B., Data Hiding on 3-D Triangle Meshes, IEEE Transactions on Signal Processing, vol. 51, no. 4, 2003, pp. 939-949
10. Cayre F., Alface P.R., Schmitt F., Macq B., and Maitre H., Application of Spectral Decomposition to Compression and Watermarking of 3D Triangle Mesh Geometry, Signal Processing, vol. 18, no. 4, 2003, pp. 309-319
11. Cho J.W., Kim M.S., Prost R., Chung H.Y., and Jung H.Y., Robust Watermarking on Polygonal Meshes Using Distribution of Vertex Norms, Proceedings of International Workshop on Digital Watermarking, 2005, pp. 283-293
12. Cho W.H., Lee M.E., Lim H., and Park S.Y., Watermarking Technique for Authentication of 3-D Polygonal Meshes, Proceedings of International Workshop on Digital Watermarking, 2005, pp. 259-270
13. Gelasca E.D., Ebrahimi T., Corsini M., and Barni M., Objective Evaluation of the Perceptual Quality of 3D Watermarking, Proceedings of International Conference on Image Processing, vol. 1, 2005, pp. 241-244
14. Jin J.Q., Dai M.Y., Bao H.J., and Peng Q.S., Watermarking on 3D Mesh Based on Spherical Wavelet Transform, Journal of Zhejiang University: Science, vol. 5, no. 3, 2004, pp. 251-258
15. Kanai S., Date H., and Kishinami T., Digital Watermarking for 3D Polygons Using Multiresolution Wavelet Decomposition, Proceedings of IFIP WG, 1998, pp. 296-307
16. Kim M.S., Valette S., Jung H.Y., and Prost R., Watermarking of 3D Irregular Meshes Based on Wavelet Multiresolution Analysis, Proceedings of International Workshop on Digital Watermarking, 2005, pp. 313-324

17. Lavoué G., Gelasca E.D., Dupont F., Baskurt A., and Ebrahimi T., Perceptually Driven 3D Distance Metrics with Application to Watermarking, SPIE Applications of Digital Image Processing, 2006, pp. 63120L
18. Lavoué G., Denis F., and Dupont F., Subdivision Surface Watermarking, Computers and Graphics, vol. 31, no.3, 2007 (to appear)
19. Lee J.W., Lee S.H., Kwon K.R., and Lee K.I., Complex EGI Based 3D-Mesh Watermarking, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E88, no. 6, 2005, pp. 1512-1519
20. Li L., Zhang D., Pan Z., Shi J., Zhou K., and Ye K., Watermarking 3D Mesh by Spherical Parameterization, Computers and Graphics, vol. 28, no. 6, 2004, pp. 981-989
21. Lin H.S., Liao H.M., Lu C., and Lin J., Fragile Watermarking for Authenticating 3-D Polygonal Meshes, IEEE Transactions on Multimedia, vol. 7, no. 6, 2005, pp. 997-1006
22. Maret Y., and Ebrahimi T., Data Hiding on 3D Polygonal Meshes, Proceedings of the Multimedia and Security Workshop, 2004, pp. 68-74
23. Murotani K., and Sugihara K., Watermarking 3D Polygonal Meshes Using the Singular Spectrum Analysis, Proceedings of IMA International Conference, 2003, pp. 85-98
24. Ohbuchi R., Masuda H., and Aono M., Watermarking Three-Dimensional Polygonal Models, Proceedings of the ACM International Multimedia Conference and Exhibition, 1997, pp. 261-272
25. Ohbuchi R., Masuda H., and Aono M., Data Embedding Algorithms for Geometrical and Non-geometrical Targets in Three-Dimensional Polygonal Models, Computer Communications, vol. 21, no. 15, 1998, pp. 1344-1354
26. Ohbuchi R., Takahashi S., Miyazawa T., and Mukaiyama A., Watermarking 3D Polygonal Meshes in the Mesh Spectral Domain, Proceedings of Graphics Interface, 2001, pp. 9-17
27. Ohbuchi R., Mukaiyama A., and Takahashi S., A Frequency-Domain Approach to Watermarking 3D Shapes, Computer Graphics Forum, vol. 21, no. 3, 2002, pp. 373-382
28. Praun E., Hoppe H., and Finkelstein A., Robust Mesh Watermarking, Proceedings of the ACM SIGGRAPH Conference on Computer Graphics, 1999, pp. 49-56
29. Uccheddu F., Corsini M., and Barni M., Wavelet-Based Blind Watermarking of 3D Models, Proceedings of the Multimedia and Security Workshop, 2004, pp. 143-154
30. Wagner M.G., Robust Watermarking of Polygonal Meshes, Proceedings of Geometric Modeling and Processing, 2000, pp. 201-208
31. Wu H.T., and Chueng Y.M., A Fragile Watermarking Scheme for 3D Meshes, Proceedings of the Workshop on Multimedia and Security, 2005, pp. 117-124
32. Wu J., and Kobbelt L., Efficient Spectral Watermarking of Large Meshes with Orthogonal Basis Functions, Visual Computer, vol. 21, no. 8-10, 2005, pp. 848-857
33. Yeo B., and Yeung M.M., Watermarking 3D Objects for Verification, IEEE Computer Graphics and Applications, vol. 19, no. 1, 1999, pp. 36-45
34. Yin K., Pan Z., Shi J., and Zhang D., Robust Mesh Watermarking Based on Multiresolution Processing, Computers and Graphics, vol. 25, no. 3, 2001, pp. 409-420
35. Yu Z., Ip H.H.S., and Kwok L.F., A Robust Watermarking Scheme for 3D Triangular Mesh Models, Pattern Recognition, vol. 36, no. 11, 2003, pp. 2603-2614
36. Zafeiriou S., Tefas A., and Pitas I., A Blind Robust Watermarking Scheme for Copyright Protection of 3D Mesh Models, Proceedings of International Conference on Image Processing, vol. 3, 2004, pp. 1569-1572