Hierarchical Watermarking of Semi-regular Meshes Based on Wavelet Transform

Kai Wang*, Guillaume Lavoué, Florence Denis, and Atilla Baskurt

***Abstract*—This paper presents a hierarchical watermarking framework for semi-regular meshes. Three blind watermarks are inserted in a semi-regular mesh with different purposes: a geometrically robust watermark for copyright protection, a high-capacity watermark for carrying a large amount of auxiliary information, and a fragile watermark for content authentication. The proposed framework is based on wavelet transform of the semi-regular mesh. More precisely, the three watermarks are inserted in different appropriate resolution levels obtained by wavelet decomposition of the mesh: the robust watermark is inserted by modifying the norms of the wavelet coefficient vectors associated with the lowest resolution level; the fragile watermark is embedded in the high resolution level obtained just after one wavelet decomposition by modifying the orientations and norms of the wavelet coefficient vectors; the high-capacity watermark is inserted in one or several intermediate levels by considering groups of wavelet coefficient vector norms as watermarking primitives. Experimental results demonstrate the effectiveness of the proposed framework: the robust watermark is able to resist all the common geometric attacks even with relatively strong amplitude; the fragile watermark is robust to content-preserving operations, while sensitive to other attacks of which it can also provide the precise location; the payload of the high-capacity watermark increases rapidly along with the number of watermarking primitives.**

***Index Terms*—Hierarchical watermarking, semi-regular mesh, copyright protection, high capacity, authentication.**

I. Introduction

THE basic idea of digital watermarking technique [1], [2] is to embed an amount of secret information in the functional part of a cover content. This content can be an image, an audio or video clip, a 3D model, an integrated circuit, a code fragment, and so forth. This technique has attracted much attention from both academic and industrial sectors since the mid of 1990s. According to different specific objectives, we can generally distinguish between *robust* watermarking used for copyright protection and *fragile* watermarking used for content authentication (integrity verification). In robust watermarking, the embedded watermark should be as resistant as possible against both routine operations and malicious attacks. In fragile watermarking, the inserted watermark should be vulnerable to even very slight modifications and furthermore provide some supplementary information, such as the location and the nature of the endured modifications. Sometimes, the purpose of a watermark is simply to hide some information that is related to the cover content, for instance the patient's information of a 3D image obtained by a CT scan. In such applications, instead of the robustness (or the fragility), the *capacity* may be the main concern. These applications are similar to steganography; however, one significant difference is that in steganography the inserted information is more important than the cover content and has normally no relationship with it, while here the inserted information serves as auxiliary information of the cover content and is secondary.

Three-dimensional mesh [3] has become the *de facto* standard for the representation of 3D objects because of its simplicity and usability. A 3D mesh contains three different combinatorial elements: *vertices*, *edges* and *facets*. The coordinates of the vertices give the geometry information of the mesh, while the edges and facets (*i.e.* adjacency relationships between vertices) describe the connectivity information. Actually, more and more 3D meshes are used in applications such as computer aided design, medical imaging, film special effect making and video games mainly due to the processing capability improvement of ordinary PCs and the bandwidth increase of the network infrastructure. Two important concepts concerning a 3D mesh are the *valence* and the *degree*. The *valence* of a vertex is the number of its incident edges, while the *degree* of a facet is the number of its component edges. A 3D mesh is *regular* if all its vertices have a same valence (usually, the valence is 6 in the case of triangular meshes). A *semi-regular* mesh is a piecewise regular structure and consists of a patchwork of large regular regions; hence, it owns regular vertices almost everywhere.

In this paper, a hierarchical watermarking framework is proposed for 3D semi-regular meshes. Three different watermarks (robust, high-capacity and fragile) are inserted simultaneously in a semi-regular mesh, serving for different applications (copyright protection, content enrichment and content authentication). These applications are not mutually exclusive. For instance, we can imagine the following scenario: a manufacturer designs a complex car part represented by a semi-regular mesh, then he may wish to embed in this part a piece of copyright information for intellectual property protection against possible forgery; he may also want to insert a fragile watermark so as to ensure that any modification can be easily detected by authorized clients; and finally he may like to embed into the object some description information, such as the part design norm and its applicable car models. Indeed, the concept of multiple (or multipurpose) watermarking [4], [5]

K. Wang* (corresponding author), G. Lavoué, and A. Baskurt are with LIRIS, UMR 5205 CNRS, INSA-Lyon, Villeurbanne, F-69621 France. (e-mails: {kwang, glavoue, abaskurt}@liris.cnrs.fr, phone: 33-472436097, fax: 33-472437117)

F. Denis is with LIRIS, UMR 5205 CNRS, Université Lyon 1, Villeurbanne, Université de Lyon, F-69622 Lyon France. (e-mail: fdenis@liris.cnrs.fr)

Manuscript received Jan. 18, 2008, accepted Sep. 13, 2008. This work is partially supported by China Scholarship Council of Chinese government and the region of Rhône-Aples, France, under the contract of ISLE cluster's SYSECUR project.

has been investigated for a long time and several techniques have been proposed for images [6] and audios [7]. To the authors' knowledge, this paper presents the first attempt on multiple watermarking for 3D meshes. According to [5], in general, the multiple watermarking system seems as secure as the individual underlying algorithms; on the contrary, the robustness, imperceptibility and capacity of individual underlying algorithms are generally degraded by the embedding of the other watermarks. In our system, there is not any inter-infection between the different watermarks so that their individual performances are kept as much as possible.

All the three watermarks in our hierarchical multiple watermarking system are blind and invariant to the so-called content-preserving attacks including vertex reordering and similarity transformations (*i.e.* translation, rotation, uniform scaling and their combination), which theoretically do not have any influence on the mesh shape. The robust watermark is resistant to all the common geometric attacks and serves for copyright protection. The fragile watermark is robust to the aforementioned content-preserving attacks. However, it is vulnerable to others attacks such as local and global geometric modifications since the objective is to check the integrity of the mesh. Additionally, at extraction, these attacks can be precisely located on the surface of the attacked mesh in a blind way. The high-capacity watermark is used to carry a large amount of auxiliary information about the semi-regular mesh. Its capacity increases rapidly with the number of watermarking primitives.

The remainder of this paper is organized as follows: section II provides an overview of the proposed hierarchical watermarking framework; section III briefly reviews the related work in the literature; sections IV, V and VI detail the embedding and extraction procedures of the robust, high-capacity and fragile watermarking schemes, respectively; the experimental results are presented in section VII; section VIII concludes the paper and points out some future working directions.

II. Overview of the hierarchical watermarking framework

As mentioned previously, a semi-regular mesh is a patchwork of large regular regions. Such a mesh is built starting from a coarse-level irregular mesh that is recursively refined through iterative subdivisions and displacements forming a multi-resolution hierarchical structure. Semi-regular meshes allow for wavelet transform and therefore are particularly attractive for many applications involving level of details management such as filtering, texturing, rendering and particularly compression where a lot of work has been done [8], [9] even for dynamic mesh sequences [10]. Accordingly, even very recently a lot of remeshing techniques have been proposed for constructing such multi-resolution semi-regular models starting from 3D volumetric models [11] or irregular meshes [12] even gigantic [13]. Along with the more and more popular use of these semi-regular meshes, their intellectual property protection and authentication problems have attracted more and more attention. Naturally, as promising techniques, robust and fragile watermarking algorithms appear as good candidates to solve these problems. Meanwhile, a high-capacity watermark is sometimes very useful to carry a large amount of auxiliary information, such as the mesh generation information, a description, a related website address, or even animation parameters.

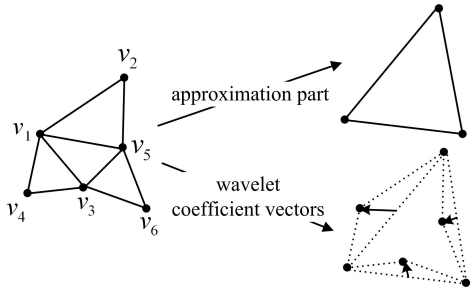


Fig. 1. Illustration of one iteration of the lazy wavelet decomposition mechanism on triangular semi-regular meshes.

The proposed hierarchical watermarking framework is based on wavelet transform of semi-regular meshes [14]. Figure 1 illustrates one iteration of the lazy wavelet decomposition mechanism. A group of four triangles is merged in one and three of the six initial vertices (*even* vertices, v_2, v_4, v_6 in Figure 1) are conserved in the lower resolution. The wavelet coefficients are calculated as the prediction errors for all the deleted vertices (*odd* vertices, v_1, v_3, v_5 in Figure 1) and they are 3D vectors associated with each edge of the coarser mesh. A straightforward prediction is used here, which is the midpoint of the two even vertices having been incident to the odd vertex. Such an analysis can be iteratively applied on a dense mesh with semi-regular connectivity and can finally provide a very coarse irregular mesh that represents the basic shape (low frequencies) and several sets of wavelet coefficient vectors (WCVs) that stand for details information at different resolution levels (median and high frequencies). The dual synthesis algorithm can accomplish the inverse reconstruction. Note that the obtained coarsest-level mesh cannot be further decomposed (since it is irregular) and that its complexity depends on the remeshing technique that has produced the semi-regular hierarchical structure. Obviously, this is only a simple intuitive introduction to the wavelet transform of semi-regular meshes, readers could refer to [14] for its strict mathematical formulation.

Such a multi-resolution analysis based on wavelet transform is a very suitable tool for hierarchical multiple watermarking: first, there is no inter-infection between different watermarks if they are inserted in WCVs of different levels; secondly, also more importantly, these watermarks can be inserted at different appropriate resolution levels according to their specific objectives. Figure 2 illustrates the proposed framework: the fragile watermark is embedded in a dense resolution level obtained just after one wavelet decomposition of the original mesh, by modifying the orientations and norms of the corresponding WCVs; the robust watermark is inserted by modifying the norms of the WCVs associated with the lowest resolution level; the high-capacity watermark is inserted in one or several intermediate levels by considering groups of WCV norms as watermarking primitives. In practice, the robust watermark is first inserted after a thorough decomposition, then the high-

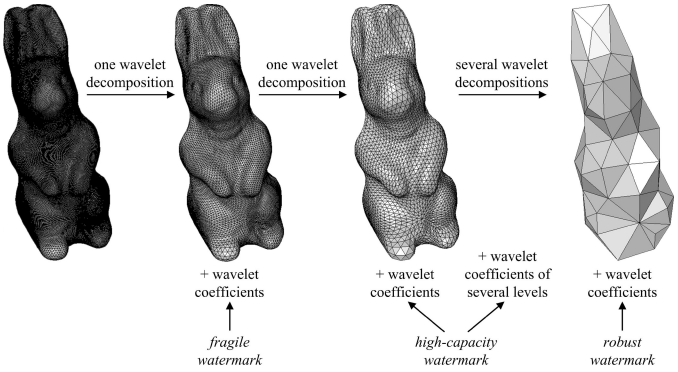


Fig. 2. Illustration of the proposed hierarchical multiple watermarking framework.

capacity watermark and the fragile watermark are inserted successively during the reconstruction procedure. This workflow effectively prevents the posteriorly inserted watermark from impacting the anteriorly inserted one(s) and follows the principle proposed in [4], which points out that the most robust watermark should be inserted at first while the most fragile one should be inserted at last. By using this embedding order, we also make assumption that the embedding of the first two watermarks does not obviously degrade the functional quality (especially for CAD objects [15]) and the perceptual quality of the mesh, so as to make the authentication based on the fragile watermark meaningful. The main contributions of this work can be summarized as follows: first, the robust watermark demonstrates better performances compared to the existing semi-regular mesh watermarking schemes; secondly, to our knowledge, the fragile watermark is the first on this topic that is robust to all the content-preserving operations while providing a precise attack localization capability; thirdly, although the high-capacity watermark is somewhat fragile, its particular embedding method provides the highest payload in the literature of 3D mesh watermarking; fourthly, for these three schemes, we explicitly take the watermarking security [16], [17] into account, which is measured by the potential information leakage of the secret parameters of the watermarking system through observations.

III. Related Work

Actually, relatively few watermarking schemes have been proposed for 3D meshes. This situation is due to the difficulties introduced by the irregular representation of 3D mesh and the existence of various intractable attacks. These difficulties include watermark resynchronization, robustness to connectivity attacks and causality problem, especially when we want to devise a blind and robust algorithm. Formally, the *causality problem* means that the insertion of the posterior watermark bits impacts the synchronization and/or the modulation of the anteriorly inserted ones; hence, the extracted bits can be different from the original ones, even in the absence of attacks. In the following, we will briefly review the existing 3D mesh watermarking techniques, particularly for semi-regular meshes. Interested readers could refer to [18] and [19] for two comprehensive surveys on 3D mesh watermarking.

A. Robust techniques

The attacks that a robust 3D mesh watermark should be able to resist include mainly the geometric attacks and the connectivity attacks. The former consists of similarity transformations, conventional signal processing (*i.e.* noise addition, smoothing, enhancement, lossy compression, etc.) and local deformation. The latter mainly consists of cropping, simplification and vertex resampling. Note that connectivity attacks would generally destroy the intrinsic multi-resolution connectivity of the semi-regular mesh and thus also destroy its intrinsic attractiveness. Therefore, in our opinion, for a semi-regular mesh, even its robust watermark may not have to be resistant to these destructive attacks.

The robust watermarking of semi-regular meshes was first discussed by Kanai *et al*. [20]. They proposed a non-blind algorithm based on lazy wavelet transform. The watermarking primitive is the ratio between the norm of a WCV and the length of its support edge, which is invariant to similarity transformations. Uccheddu *et al*. [21] described a blind one-bit watermarking algorithm with hypothesis of the statistical independence between WCV norms and inserted watermark bit string. Watermark synchronization is realized by carrying out blind mesh self-registration at both embedding and detection sides based on principal component analysis. Their scheme shows relatively good robustness against geometric attacks.

Kim *et al*. [22], [23] studied the robust watermarking of arbitrary mesh based on irregular wavelet transform [24]. In [22], a similar correlation-based scheme as in [21] is used to insert watermark bits in bins (groups) of WCVs. This scheme is fragile to connectivity attacks due to the vulnerability of the adopted synchronization mechanism under such attacks. In [23], the authors apply the robust histogram-based watermarking technique proposed in [25] on a coarser mesh obtained after irregular wavelet decomposition. The watermark can be extracted from the reconstructed (and possibly attacked) dense mesh without carrying out wavelet analysis. However, this scheme seems less robust than the original technique that inserts watermark directly in the dense mesh.

More generally, for arbitrary meshes, researchers have tried to use spatial primitives [26], [27], direct spectral analysis tools [28]–[31] and multi-resolution analysis tools [22], [23], [32] to design robust watermarking techniques. The methods based on statistical mesh descriptors [25], [33], [34] and the content-based algorithms [35], [36] seem promising to achieve robustness against all types of attacks while keeping the technique blind.

B. Fragile techniques

The typical requirement for a fragile mesh watermark is that it should be robust to the aforementioned content-preserving attacks while being vulnerable to the other ones; additionally, it should also offer the capability of locating the attacks endured by the watermarked mesh.

To our knowledge, the fragile watermarking of semi-regular meshes has only been addressed by Cho *et al*. [37]. They first apply several wavelet decompositions on the original triangular mesh and then consider the facets in the obtained

coarser mesh as authentication primitives. The basic idea is to slightly modify each facet so that the values of two predefined functions are the same, in order to make all these facets valid for authentication. Both function inputs are invariant to similarity transformations. However, it seems that two problems exist: first, the causality problem occurs because the modification of the current to-be-watermarked facet can influence the validities of its already watermarked neighboring facets, and this problem is not mentioned by the authors; secondly, the watermark is inserted in a relatively coarse mesh obtained after several wavelet decompositions, which seems disadvantageous to provide precise attack localization capability.

Fragile watermarking for authenticating arbitrary 3D meshes has been studied in several references [38]–[41]. In these algorithms, either vertex coordinates or the relative position of a vertex to its traversed neighbors (in a certain vertex transversal order) is considered as watermarking primitive. However, none of these algorithms attains the robustness to both vertex reordering and similarity transformations. This situation is due to the difficulties introduced by the causality problem and by the requirement of a precise attack localization capability.

C. High-capacity techniques

To our knowledge, there is no high-capacity watermarking method specifically proposed for semi-regular meshes. More generally, for arbitrary meshes, individual vertex coordinates are commonly used to construct high-capacity approaches. Cayre and Macq [42] proposed a high-capacity blind data hiding algorithm for 3D triangular meshes. The watermarking primitive is the projection of a vertex on its opposite edge in a triangular facet, and the theoretical capacity attains 1 bit/vertex. A higher capacity, which is about 3 bits/vertex, is achieved in [43] by applying a multi-level embedding procedure. This procedure consists in modifying successively the parallel, vertical and rotary positions of a vertex related to its opposite edge in a triangular facet. Benedens [44] reported a high-capacity ($\approx$1 bit/facet) algorithm in which the height of each triangular facet is quantized. By quantizing the distance from a vertex or a facet to the mesh gravity center, Wu and Chueng [41], [45] gave two other schemes whose capacity can reach 1 bit/vertex or 1 bit/facet, respectively.

IV. Blind and Robust Watermark

A. Objective and basic idea

Our objective is to construct a blind watermark that is robust to all the common geometric attacks. One critical problem of blind mesh watermarking schemes is their relatively weak robustness. Technically, the synchronizing mechanism is difficult to design and is often fragile. Even worse, sometimes, the watermark insertion procedure itself can modify the established order of the watermarking primitives; this is one typical example of the causality problem and it is also the reason why the author of [27] introduced a post-processing step after watermark insertion to rectify the synchronization order. One possible solution to the synchronization issue is the indexing scheme, in which the index of each watermark bit is explicitly embedded along with the bit; one such example is given in [26]. However, this solution needs a large watermark payload while keeping a sufficient robustness, which seems difficult. Our proposal is to use a certain robust aspect to synchronize the embedded bits: the edges in the coarsest-level mesh obtained by a thorough wavelet decomposition are sorted according to their lengths; this order is experimentally fairly robust to geometric attacks. Then the watermark bits are inserted one by one by modifying the norms of WCVs associated with these sorted edges. Moreover, in this way, the synchronizing primitives (edge lengths) and the watermarking primitives (WCV norms) are separated, so the causality problem is avoided.

B. Watermark embedding

The first step of the embedding procedure is to carry out a thorough wavelet decomposition (supposing that it consists of J iterations) on the original non-watermarked semi-regular mesh $\mathcal{M}_0$. Then, we obtain a coarsest-level irregular mesh $\mathcal{M}_J$ and J sets of WCVs. For robust watermark embedding, we only consider the set of N_J WCVs associated with $\mathcal{M}_J$, where N_J is also the number of edges in $\mathcal{M}_J$.

In the next step, all the edges in $\mathcal{M}_J$ are sorted by descending order of their lengths. Thus, the longest edge in $\mathcal{M}_J$ is denoted by $\mathbf{e_1^J}$, the second longest edge is denoted by $\mathbf{e_2^J}$, and so forth. The WCV associated with $\mathbf{e_1^J}$ is denoted by $\mathbf{c_1^J}$, the one associated with $\mathbf{e_2^J}$ is denoted by $\mathbf{c_2^J}$, etc. Thus, an order of all the edges (also of all the WCVs) has been established. Note that $\mathbf{e_i^J}, 1 \le i \le N_J$ is defined as the coordinate difference of its two incident vertices and thus is considered as a 3D vector.

The watermark is a readable bit sequence $w_1, w_2, ..., w_R$. These bits are inserted by quantifying the norms of $\mathbf{c_i^J}, 1 \le i \le N_J$. First of all, we have to fix a quantization step Δ_{rob} for these norms: the average edge length is calculated as $l_{av} = \frac{1}{N_J}\sum_{i=1}^{N_J}\left\|\mathbf{e_i^J}\right\|$ and Δ_{rob} is fixed as l_{av}/ϵ_{rob}, where ϵ_{rob} is a control parameter to achieve an expected trade-off between robustness and imperceptibility. An appropriate value of ϵ_{rob} can be found through experimental study so that it can be fixed for most of the semi-regular meshes without seriously affecting the algorithm's performances.

The next step is watermark bit embedding. The bit w_i is inserted by quantifying $\left\|\mathbf{c_i^J}\right\|$ through the 2-symbol scalar Costa scheme (SCS) [46]. The practical quantization procedure is as follows: first, a component-wise random codebook is established for each $\left\|\mathbf{c_i^J}\right\|$ as given by Equation 1, where Δ_{rob} is the pre-fixed quantization step, $z \in Z^+$ can be any of the non-negative integers, $l \in \{0, 1\}$ each stands for a legal watermark bit, and $t_{\left\|\mathbf{c_i^J}\right\|}$ is an additive pseudo-random dither signal.

$$\mathcal{U}_{\left\|\mathbf{c_i^J}\right\|, t_{\left\|\mathbf{c_i^J}\right\|}} = \bigcup_{l=0}^{1}\left\{u = z.\Delta_{rob} + l\frac{\Delta_{rob}}{2} + t_{\left\|\mathbf{c_i^J}\right\|}, u \ge 0\right\} \quad (1)$$

Note that each code word u in $\mathcal{U}_{\left\|\mathbf{c_i^J}\right\|, t_{\left\|\mathbf{c_i^J}\right\|}}$ implies a watermark bit, which is the value of l in u's derivation. The

dither signal $t_{\|\mathbf{c_i^J}\|}$ is generated by using a secret key K_{rob} and is introduced to achieve randomization of the codebook. For a watermarking system, introduction of randomization by using secret key is an effective way to prevent non-authorized watermark extraction and optimal watermark removal. As an example, $t_{\|\mathbf{c_i^J}\|,1\leq i\leq N_J}$ can form a simulation sequence of a random variable T_{rob} that follows the uniform distribution between $\left(-\frac{\Delta_{rob}}{4},\frac{\Delta_{rob}}{4}\right)$ (*i.e.* $T_{rob}\sim U\left(-\frac{\Delta_{rob}}{4},\frac{\Delta_{rob}}{4}\right)$), and they can be generated by inputting K_{rob} to an appropriate pseudo-random number generator.

Then we find the nearest code word $u_{\|\mathbf{c_i^J}\|}$ to $\|\mathbf{c_i^J}\|$ in this codebook that implies the correct watermark bit w_i (*i.e.* w_i should be equal to the l's value of $u_{\|\mathbf{c_i^J}\|}$). The quantized value $\|\hat{\mathbf{c_i^J}}\|$ is calculated according to Equation 2, where $\alpha_{rob}\in(0,1]$ is a compensation factor. Usually, we choose $\alpha_{rob}\geq 0.50$ in order to ensure the correctness of the watermark extraction when there is no attack.

$$\|\hat{\mathbf{c_i^J}}\| = \|\mathbf{c_i^J}\| + \alpha_{rob}\left(u_{\|\mathbf{c_i^J}\|} - \|\mathbf{c_i^J}\|\right) \tag{2}$$

In our scheme, α_{rob} will partially drive the induced distortion and the watermark security. A perfect security of the SCS quantization (*i.e.* the secrecy of K_{rob}) can be gained if an appropriate value of α_{rob} has been selected [47] (here $\alpha_{rob}=0.50$ for a perfect security).

Finally, keeping the orientation of $\mathbf{c_i^J}$ unchanged, we modify its norm to realize the norm quantization. If the edge number N_J is greater than the watermark bit number R, a redundant embedding will be carried out in order to enhance the robustness. Two repetition schemes are possible: the first is to sequentially divide the ordered edges in several groups each having R edges, and the watermark sequence is repeatedly embedded in each group; the second is to sequentially divide the edges in R equal parts and repeatedly insert one bit in each part. The second scheme is experimentally less robust due to the vulnerability of the last few watermark bits inserted in the shortest edges. The embedding in these edges is naturally less robust than in the longer ones since their associated WCVs usually represent higher frequencies. Hence, the first repetition scheme was adopted.

Once the quantization of all the WCVs is accomplished, we apply wavelet synthesis on $\mathcal{M}_J$ with the modified WCVs until the resolution level where the high-capacity watermark is to be embedded.

Algorithm 1 summarizes the blind and robust watermark embedding procedure.

C. Watermark extraction

With the knowledge of the secret key K_{rob} used during the watermark embedding, the watermark extraction is blind and quite simple. It is sufficient to carry out a thorough wavelet analysis, reestablish the edge order, calculate the quantization step, reconstruct the component-wise codebook for each WCV and finally find out its designated bit by looking for the nearest code word in this codebook to the actual value of the WCV norm. If redundant insertion is used during watermark embedding, a simple majority voting strategy is adopted at extraction to deduce the watermark bit values.

Algorithm 1 Blind and robust watermark embedding procedure

1: Do wavelet analysis of the original semi-regular mesh until the coarsest level
2: Do descending sort of all the edges in this level according to their lengths
3: Calculate the average length l_{av} of the edges and fix the WCV norm quantization step as l_{av}/ϵ_{rob}
4: **for** each edge in the descending sort **do**
5: Calculate the norm of its associated WCV
6: Quantize this norm according to Equation 2 by using scalar Costa quantization scheme
7: **end for**
8: Do mesh reconstruction until the level where the high-capacity watermark is to be embedded

D. Analysis and discussion

This robust watermark is theoretically invariant to similarity transformations, because the real watermarking primitive is the ratio between the norm of a WCV and the average length of all the edges in the coarsest-level mesh, which is invariant to these transformations. The induced distortion for each odd vertex (see Figure 1) in the reconstructed $(J-1)$-level mesh $\hat{\mathcal{M}}_{J-1}$ is the norm difference between the quantized and the original WCV that represents its prediction error. It is easy to deduce that the upper limit of this distortion is equal to $\alpha_{rob}\times\frac{\Delta_{rob}}{2}$. This distortion will later propagate to the odd vertices introduced by the following reconstruction steps. The robust watermarking scheme fails if the synchronization mechanism fails or if the watermark modulation scheme fails. Practically, the former usually demonstrates stronger robustness than the latter under geometric attacks. Obviously, the watermark will generally be destructed under connectivity attacks, which yet can be omitted in semi-regular mesh watermarking. If we want also the robustness against connectivity attacks, one possible solution is to devise a robust remeshing technique that is insensitive to connectivity changes. Before watermark extraction, the attacked mesh could be first remeshed to reconstruct a semi-regular mesh with the same connectivity configuration as the one in which the watermark is initially inserted. Such a remeshing technique could possibly rely on a blind and robust feature points detection algorithm but its development seems difficult. One special connectivity attack is the cropping. We guess that a partial wavelet analysis is still possible on the intact regions of a cropped semi-regular mesh, so that the watermark can still be successfully extracted because of the redundant embedding. The principle would be first calculating the autocorrelation function of the extracted bit sequence from the intact parts of the coarsest-level mesh, then it would be possible to resynchronize the watermark according to the cyclic peaks of this autocorrelation function. One limitation of our robust scheme is that it will probably fail for the regular or semi-regular meshes where the edges in the coarsest-level representation have almost the same length. In such a case, other metrics have to be used to sort these coarsest-level edges, such as the areas or the roughness of the regions [48] in the original dense mesh that correspond to the incident facets of these edges.

V. Blind and High-capacity Watermark

In this section, a new high-capacity watermarking scheme is introduced for semi-regular meshes. In this scheme, the watermark is no longer inserted bit by bit, but globally.

A. Watermark embedding

For a mesh $\hat{\mathcal{M}}_H$ at a certain level of the wavelet synthesis procedure carried out after the robust watermark embedding, we suppose that its N_H WCVs are indexed according to the lengths of their associated edges in $\hat{\mathcal{M}}_H$, in the same way as in the last section. This means that the WCV indexed by i is associated with the ith longest edge in $\hat{\mathcal{M}}_H$.

Then we combine each WCV $\mathbf{c_i^H}$ with another number denoted by $order_o(i)$. To obtain this number, we first calculate the residue of the norm $\left\|\mathbf{c_i^H}\right\|$ divided by a control parameter p as $res(i) = \left\|\mathbf{c_i^H}\right\| \%p$; $order_o(i)$ is the order (ascending) of the value $res(i)$ among the residues of all the WCVs at the same level. Like in the robust watermark, the control parameter is fixed as $p = l_{av}/\epsilon_{hc}$ and is also related to the average length of the edges (but at a different resolution level). The first five lines of Table I show one simple example of this calculation, where $N_H = 5$ and $p = 0.1$. For instance, $res(1)$ of $\mathbf{c_1^H}$ is equal to 0.08, which is the largest among all the residues of the five WCVs, thus $order_o(1)$ is set to be 5.

These numbers are listed successively as $order_o(1), order_o(2), ..., order_o(N_H - 1), order_o(N_H)$, along with the ascending order of the index i (as shown by the fifth line of Table I). This sequence is a permutation of the N_H numbers ranging from 1 to N_H and thus has $N_H!$ different possibilities. As a consequence, each permutation can potentially represent a watermark of $\lfloor \log_2(N_H!) \rfloor$ bits (*i.e.* the largest integer less than or equal to $\log_2(N_H!)$). The correspondence between watermarks ($\lfloor \log_2(N_H!) \rfloor$-bit strings) and possible order sequences (N_H-number permutations) is established according to the following rule: for two permutations, the one with a bigger first number (from left) represents a bigger bit string (in terms of its binary value); and if the first numbers are the same, we compare the second, and so on. Under this rule, the permutation $1, 2, 3, ..., N_H - 1, N_H$ represents the smallest bit string $0, 0, ..., 0, 0$; and the permutation $1, 2, 3, ..., N_H, N_H - 1$ designates the second smallest bit string $0, 0, ..., 0, 1$.

With this rule, each possible watermark bit string can be represented by a permutation. Thus, it seems natural to substitute the original permutation by a new one in order to insert a given watermark. This new permutation is established by modifying the WCV norms so as to alternate their norm residues' orders. The new WCV norm is determined by Equation 3, where $order(i)$ is the new expected norm residue order of the WCV $\mathbf{c_i^H}$ that is associated with the ith longest edge.

$$\left\|\hat{\mathbf{c}}_\mathbf{i}^\mathbf{H}\right\| = \left\lfloor \frac{\left\|\mathbf{c_i^H}\right\|}{p} \right\rfloor .p + \frac{order(i).p}{N_H + 1} \tag{3}$$

The last three lines of Table I give one simple example of the substitutive watermarking procedure. It can be seen that only the residue of the WCV norm is substituted, while the difference between the WCV norm and the residue is kept unchanged.

Practically, the N_H edges are divided into several ordered groups of G edges (in each group are inserted $\lfloor \log_2(G!) \rfloor$ bits) in order to make the watermark less fragile. Thus, the practical capacity of this method is $\left\lfloor \frac{N_H}{G} \right\rfloor . \lfloor \log_2(G!) \rfloor$ bits. The simplest grouping is adopted: putting the edges indexed by 1 to G in the first group, the ones indexed by $(G + 1)$ to $2G$ in the second group, and so forth. It is possible to carry out a compensation modulation similar as in Equation 2 for the new WCV norms. After the compensation, a secret key K_{hc} can also be used to introduce pseudo-random additive dither signals to the established WCV norms. Algorithm 2 summarizes the embedding procedure of the proposed high-capacity watermarking scheme.

Algorithm 2 Blind and high-capacity watermark embedding procedure

1: Do wavelet synthesis after robust watermark embedding until a certain appropriate level
2: Do descending sort of all the edges in this level by their lengths
3: Calculate the average length l_{av} of the edges and fix the control parameter p as l_{av}/ϵ_{hc}
4: Divide the edges in several ordered groups of G edges according to their length sorting
5: **for** each ordered edge group **do**
6: Translate the next $\lfloor \log_2(G!) \rfloor$ bits in the watermark sequence to a corresponding permutation
7: **for** each descending sorted edge in the current group **do**
8: Substitute the norm of its associated WCV according to Equation 3 in order to assign it an expected norm residue order in the desired permutation
9: Modify the new norm by applying a compensation scheme similar to Equation 2 and by introducing a dither signal generated by using secret key K_{hc}
10: **end for**
11: **end for**
12: Do mesh reconstruction until the second densest level where the fragile watermark is to be embedded

B. Watermark extraction

Like in the robust watermark, the extraction of the high-capacity watermark is simple and blind with the knowledge of the secret key K_{hc}. After dividing the edges in several ordered groups and for each group establishing a permutation according to the WCV norm residues' ordering, we can find out the watermark bit substring implied by each group. Finally, all the extracted substrings are concatenated to construct the complete watermark bit string.

C. Analysis and discussion

If all the WCVs in all the J resolution levels are considered for high-capacity watermarking (with no robust and fragile watermarks embedded), the capacity upper limit of our method is $\left\lfloor \frac{N_0^v - N_J^v}{G} \right\rfloor . \lfloor \log_2(G!) \rfloor$, where N_0^v and N_J^v are the numbers of vertices in $\mathcal{M}_0$ and $\mathcal{M}_J$, respectively (remember that each deleted vertex has a corresponding WCV). Considering that N_J^v is normally negligible compared to N_0^v, the capacity limit

TABLE I
EXAMPLE OF THE HIGH-CAPACITY WATERMARK EMBEDDING STEPS ($N_H = 5$)

Edges lengths	3.2	3.0	2.7	2.1	1.8
Edge / WCV indices (i for $\mathbf{c_i^H}$ and $\mathbf{e_i^H}$)	1	2	3	4	5
WCV norms ($\left\|\mathbf{c_i^H}\right\|$)	0.28	0.35	0.24	0.21	0.22
Residues of the norms divided by $p = 0.1$ ($res\,(i)$)	0.08	0.05	0.04	0.01	0.02
Original WCV orders ($order_o\,(i)$)	5	4	3	1	2
Expected WCV orders ($order\,(i)$)	3	4	5	2	1
New residues ($\frac{order(i).p}{N_H+1}$)	0.0500	0.0667	0.0833	0.0333	0.0167
New WCV norms ($\left\|\hat{\mathbf{c}}_\mathbf{i}^\mathbf{H}\right\|$)	0.2500	0.3667	0.2833	0.2333	0.2167

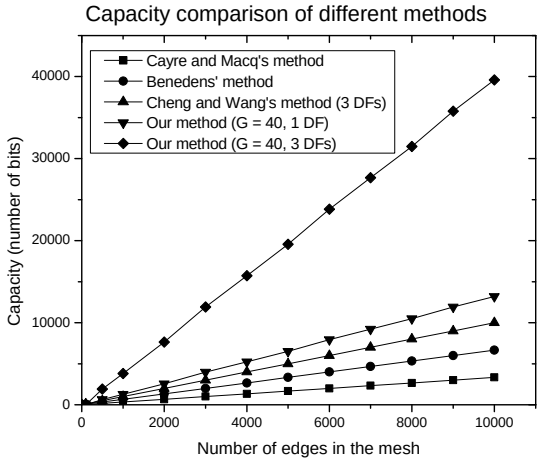


Fig. 3. Capacity comparison of different high-capacity algorithms.

can be approximated by $\left\lfloor \frac{N_0^v}{G} \right\rfloor . \lfloor \log_2 (G!) \rfloor$. If we want a higher capacity, the other two degrees of freedom (DF) of the WCV (*e.g.* the two angles of the WCV in the local spherical coordinate system) can also be modified independently from its norm with a similar scheme.

Figure 3 graphically compares the capacity of our method with different high-capacity methods in the literature (without any robustness consideration): Cayre and Macq's method (1 bit/vertex) [42], Benedens' method (1 bit/facet) [44], Cheng and Wang's method (3 bits/vertex, 3 DFs) [43], and ours ($G = 40$ with only the WCV norm watermarked and with all the three WCV DFs watermarked). For this comparison, it is assumed that for a manifold triangular mesh, we usually have $e = 1.5f$ and $f \approx 2v$, where v, e, f are the numbers of vertices, edges, and facets of the dense mesh, respectively.

If the control parameter p here is equal to the quantization step Δ_{rob} from the robust algorithm (last section), the WCV norm distortion in the worst situation is comparable for these two algorithms. However, the value p is subdivided into G subintervals instead of 2 for Δ_{rob}, and the high-capacity watermark relies on the relationship between norms of different WCVs, so even a little norm attack much smaller than p could seriously disrupt the established orders. That is the principal reason for the relative fragility of this watermark.

VI. FRAGILE WATERMARK

We recall that the objective of the fragile watermark is to be invariant to content-preserving attacks while being vulnerable to other ones. Meanwhile, the endured attacks have to be precisely located on the watermarked mesh according to the extraction result. The blindness of the watermark extraction, which is mandatory for an authentication algorithm, has also to be achieved.

A. Watermark embedding

The first step is to carry out the wavelet synthesis after robust and high-capacity watermark embeddings until the second densest level (level 1). Then, we obtain a relatively dense mesh $\hat{\mathcal{M}}_1$ and a set of N_1 WCVs denoted by $\mathbf{c_1^1}, \mathbf{c_2^1}, ..., \mathbf{c_{N_1}^1}$. Each WCV $\mathbf{c_k^1}$,$_{1 \le k \le N_1}$ is associated with an edge $\mathbf{e_k^1}$ in $\hat{\mathcal{M}}_1$. Note that, differently from the last two sections, the fragile watermark embedding procedure is independent of these indices so they can be assigned arbitrarily. In our algorithm, we take the edges in the less dense mesh $\hat{\mathcal{M}}_1$ as raw authentication primitives; then we derive the validity of each vertex in the watermarked (and possibly attacked) dense mesh $\hat{\mathcal{M}}_0$ based on the authentication results of these edges.

The basic idea of the watermark embedding is to find two watermarking primitives for each edge $\mathbf{e_k^1}$ and then slightly modify them in order to insert in both of them a same watermark symbol s_k. Thus, each edge is made valid for authentication by establishing an equality relationship between the two symbols implied by the two modified primitives. Ideally, these two primitives have to be modified independently, and the primitives of different edges have also to be modified independently. In this way, the causality problem (within an individual edge and between different edges) is prevented and the invariance to vertex/facet reordering is attained. Practically, we have found two such primitives: the one is the acute angle between $\mathbf{c_k^1}$ and $\mathbf{e_k^1}$ that is denoted by θ_k as illustrated by Figure 4; the other is the ratio between the norm of $\mathbf{c_k^1}$ and the length of $\mathbf{e_k^1}$ that is denoted by $r_k = \left\|\mathbf{c_k^1}\right\| / \left\|\mathbf{e_k^1}\right\|$. Both primitives are theoretically invariant to similarity transformations so that the robustness against them can be achieved.

The next step is the watermark symbol embedding. This symbol s_k can be any of the item in the symbol set (alphabet) $\mathcal{A} = \{a_1, a_2, ..., a_M\}$, where M is the number of legal symbols. θ_k and r_k are both quantized by using the M-symbol scalar Costa scheme [46]. θ_k is first quantized; as shown in the following, its quantization does not modify the symbol implied by its initial value. Indeed, the objective here is to find this initially implied symbol and fix it as s_k for edge $\mathbf{e_k^1}$ and therefore for the future quantization of r_k.

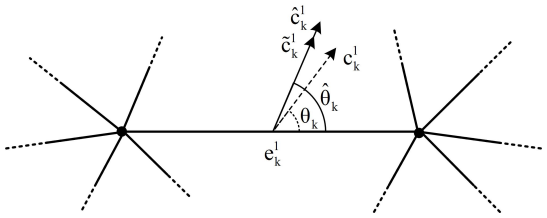


Fig. 4. Illustration of the fragile watermarking primitives and the modification of the norm and orientation of a WCV.

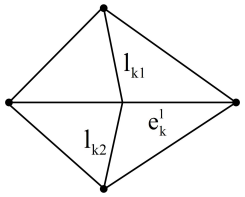


Fig. 5. The geometric ratio gr_k used to construct the look-up table. In manifold mesh, each $\mathbf{e_k^1}$ is incident to two facets (one for a border edge), and $\mathbf{l_{k1}}$, $\mathbf{l_{k2}}$ are the midlines of these facets passing the midpoint of $\mathbf{e_k^1}$. gr_k is calculated as the length ratio $\left\|\mathbf{e_k^1}\right\| / (\|\mathbf{l_{k1}}\| + \|\mathbf{l_{k2}}\|)$.

This quantization also ensures a sufficient robustness of the implied symbol of θ_k to similarity transformations, which can cause slight perturbation of θ_k due to calculation and storage precision limits. The reason for taking out symbol-preserving quantization on θ_k rather than on r_k is that θ_k is more sensitive to similarity transformations and its modification is less imperceptible than r_k.

The practical quantization procedure of θ_k is as follows: first, a component-wise random codebook is established for each θ_k as given by Equation 4, where Δ_θ is the quantization step, $z \in Z^+$ can be any of the non-negative integers, $l \in \mathcal{L} = \{0, 1, ..., M-1\}$ each stands for one of the M legal symbols in $\mathcal{A}$ and the bijective mapping between $\mathcal{L}$ and $\mathcal{A}$ is determined by a secret key K_{m_1} (this mapping is introduced in order to prevent evident watermark forgery while trying to modify the watermarked mesh), and t_{θ_k} is a pseudo-random and uniform-distributed dither signal. Note that each code word u in $\mathcal{U}_{\theta_k, t_{\theta_k}}$ implies a symbol in $\mathcal{A}$ that is the mapped symbol of the value l in u's derivation.

$$\mathcal{U}_{\theta_k, t_{\theta_k}} = \bigcup_{l=0}^{M-1} \left\{ u = z.\Delta_\theta + l\frac{\Delta_\theta}{M} + t_{\theta_k}, 0^\circ \le u \le 90^\circ \right\} \tag{4}$$

Then we find the nearest code word u_{θ_k} to θ_k in this codebook and take its implied symbol as s_k. The quantized value $\hat{\theta}_k$ is calculated according to Equation 5, where $\alpha_\theta \in (0, 1]$ is a compensation factor.

$$\hat{\theta}_k = \theta_k + \alpha_\theta \left(u_{\theta_k} - \theta_k\right) \tag{5}$$

Finally, as shown by Figure 4, the orientation of $\mathbf{c_k^1}$ is modified by rotating it around the midpoint of $\mathbf{e_k^1}$ in the 2D plane engendered by $\mathbf{c_k^1}$ and $\mathbf{e_k^1}$ to obtain an intermediate temporary vector $\tilde{\mathbf{c}}_\mathbf{k}^\mathbf{1}$ that reaches the expected angle value $\hat{\theta}_k$.

Like $t_{\|\mathbf{c_i^J}\|}$ in Equation 1, t_{θ_k} is also introduced to achieve randomization of the codebook. Usually, an ordering for all the watermarking primitives is established and the generated pseudo-random numbers can then be assigned one by one to the ordered primitives, such as in the last two sections. However, we cannot adopt such a mechanism for θ_k, because we want a precise attack localization capability, for which a global ordering (synchronization) is not appropriate. To resolve this issue, we consider a local geometric ratio gr_k between $\mathbf{e_k^1}$'s length and the length sum of $\mathbf{e_k^1}$'s incident triangles' midlines that pass the midpoint of $\mathbf{e_k^1}$ (see Figure 5, and note that this ratio is invariant to similarity transformations). A look-up table is introduced, which gives the correspondence between value ranges of gr_k for each edge $\mathbf{e_k^1}$ and the sequential pseudo-random numbers generated by using a key K_θ. In our implementation, these pseudo-random numbers form a simulation sequence of a uniform-distributed random variable $T_\theta \sim U\left(-\frac{\Delta_\theta}{2M}, \frac{\Delta_\theta}{2M}\right)$. Furthermore, the value ranges in the look-up table can be scrambled by another key K_{t_θ} to reinforce the security. For each θ_k, a number is selected from this table as t_{θ_k} according to the real value of gr_k.

The quantization of the norm-length ratio r_k is similar by using a different appropriate quantization step Δ_r and three different secret keys K_{m_2}, K_r and K_{t_r}. The significant difference is the use of a constrained codebook (given by Equation 6, l_{s_k}'s mapped symbol is s_k) to carry out the quantization so that the quantized value $\hat{r}_k$ implies the same symbol s_k as $\hat{\theta}_k$.

$$\mathcal{U}_{s_k, r_k, t_{r_k}} = \left\{ u = z.\Delta_r + l_{s_k}\frac{\Delta_r}{M} + t_{r_k}, u \ge 0 \right\} \tag{6}$$

Keeping the orientation of $\tilde{\mathbf{c}}_\mathbf{k}^\mathbf{1}$ unchanged, we can modify its norm in order to obtain the watermarked WCV $\hat{\mathbf{c}}_\mathbf{k}^\mathbf{1}$ that reaches the expected ratio value $\hat{r}_k$. Note that all the terms involved in the quantizations (θ_k, r_k, gr_k) are local to edge $\mathbf{e_k^1}$ and independent of any element ordering; hence, the precise attack localization capability and the invariance to vertex reordering are ensured.

Once the two quantizations are accomplished, an equality relationship between the two inserted watermark symbols has been established for each edge in $\hat{\mathcal{M}}_1$. Then a watermarked dense mesh $\hat{\mathcal{M}}_0$ can be reconstructed by applying one wavelet synthesis on $\hat{\mathcal{M}}_1$ with the modified WCVs $\hat{\mathbf{c}}_\mathbf{k}^\mathbf{1}, 1 \le k \le N_1$.

To summarize, Algorithm 3 lists the main steps of the fragile watermark embedding procedure.

B. Watermark extraction and mesh authentication

The first step is to carry out one wavelet decomposition of the semi-regular mesh to be authenticated. Then two codebooks for θ_k and r_k can be reconstructed for each edge $\mathbf{e_k^1}$ in the obtained less dense mesh by using the acquired keys. Two symbols can then be easily extracted by seeking the nearest code words in the codebooks to the actual values of θ_k and r_k. If these two symbols are equal, the current edge is marked as valid, otherwise as invalid.

Then the task is to derive the validity for each vertex in the dense mesh. The validity for an even vertex in the dense mesh (see Figure 1) is determined at first by the following rule: if any of its incident edges in the less dense mesh is

Algorithm 3 Fragile watermark embedding procedure

1: Do wavelet synthesis after robust and high-capacity watermark embeddings until level 1
2: Generate two pseudo-random dither signals t_{θ_k} and t_{r_k} by using secret keys K_θ and K_r
3: Construct two look-up tables giving correspondences between value ranges of the geometric ratio gr_k and the pseudo-random dither signals t_{θ_k} and t_{r_k}
4: **for** each edge $\mathbf{e_k^1}$ in this resolution level **do**
5: Do symbol-preserving SCS quantization for θ_k with the established look-up table between gr_k and t_{θ_k}
6: Do SCS quantization for r_k with the look-up table between gr_k and t_{r_k}, so that the two quantized values both imply a same symbol s_k
7: **end for**
8: Do one iteration of wavelet synthesis in order to obtain the watermarked dense mesh $\hat{\mathcal{M}}_0$

invalid, then it is considered as invalid; otherwise as valid. The validity of an odd vertex in the dense mesh (see Figure 1) is then determined according to the validities of its two neighboring even vertices: if either of these two vertices is invalid, it is considered as invalid; otherwise as valid. We adopt such a mechanism in order to handle the false positive issue under attacks. Actually, each edge in the less dense mesh has a false positive probability (the edge is considered as valid but in fact it is not) that is about $\frac{1}{M}$ under attacks. By using the above decision rule, the false positive rate for an even vertex (supposed of valence 6) is decreased to $\left(\frac{1}{M}\right)^6$ if it is in the middle of an attacked region, and that of an odd vertex is also considerably decreased (to $\left(\frac{1}{M}\right)^{11}$ if it is in the middle of an attacked region). Contrarily, some valid vertices may be wrongly marked as invalid (false negative). As in the existing methods [39], [40], this false negative only concerns the vertices that are neighboring to the real invalid vertices and seems inevitable if we want the invariance to similarity transformation. Finally, the authentication results on vertices are displayed to the users.

C. Analysis and discussion

The upper limit of the distortion induced by fragile watermark embedding for each odd vertex in $\hat{\mathcal{M}}_0$ can be approximated by Equation 7, where $\alpha_\theta \frac{\Delta_\theta}{2M} \left\|\mathbf{c_k^1}\right\|$ approximates the maximum possible distortion introduced by the quantization of θ_k (distance between $\tilde{\mathbf{c}}_\mathbf{k}^\mathbf{1}$ and $\mathbf{c_k^1}$, see Figure 4), and $\alpha_r \frac{\Delta_r}{2} \left\|\mathbf{e_k^1}\right\|$ is the maximum possible distortion introduced by the quantization of r_k (distance between $\hat{\mathbf{c}}_\mathbf{k}^\mathbf{1}$ and $\tilde{\mathbf{c}}_\mathbf{k}^\mathbf{1}$, see Figure 4).

$$D^{fr} \approx \sqrt{\left(\alpha_\theta \frac{\Delta_\theta}{2M} \left\|\mathbf{c_k^1}\right\|\right)^2 + \left(\alpha_r \frac{\Delta_r}{2} \left\|\mathbf{e_k^1}\right\|\right)^2} \tag{7}$$

The minimum quantization steps Δ_θ^{min} and Δ_r^{min} that ensure robustness against vertex coordinate distortions of amplitude Dis can be calculated according to Equations 8 and 9.

$$\Delta_\theta^{min} = Dis. \frac{2M}{\alpha_\theta \left\|\mathbf{c_k^1}\right\|} \tag{8}$$

TABLE II
INFORMATION ABOUT THE USED SEMI-REGULAR MESHES

	Venus	Rabbit	Horse	Feline
Maximum resolution level (J)	6	5	5	4
Edges in $\mathcal{M}_0$	491520	211968	337920	193536
Edges in $\mathcal{M}_J$	120	207	330	756

$$\Delta_r^{min} = Dis. \frac{2}{\alpha_r \left\|\mathbf{e_k^1}\right\|} \tag{9}$$

Similarity transformation and tolerable geometric compression can both be modeled as slight vertex coordinate distortion; thus, the quantization steps can be selected so that the watermark possesses a desired level of robustness against these tolerable operations, while being vulnerable to other non-tolerable modifications. In this way, these quantization steps are also usually small enough to ensure the watermark imperceptibility. The number of legal symbols M is supposed to be large enough in order to ensure a small distortion (see Equation 7), a low false positive rate (see the discussion in the above subsection) and a high security level (*e.g.* to make it difficult to break out the symbol mapping mechanism). However, M cannot be too large due to the calculation and storage precision limitation and to the desired robustness to tolerable operations. Once selected, these parameters can be fixed for all the meshes without seriously affecting the algorithm's performances.

Our scheme can also be used as high-capacity data hiding algorithm: bits can be inserted independently in the quantized angle value and norm-length ratio.

VII. EXPERIMENTAL RESULTS

A. Basic simulations

The proposed hierarchical watermarking framework is implemented and tested on several semi-regular meshes. Figure 6 illustrates four of them: Venus, Rabbit, Horse and Feline. Table II lists some detailed information about these models. All the four meshes are obtained by using the remeshing technique proposed in [49] and are furthermore normalized within a unit sphere. Concerning the parameter setting, for robust and high-capacity watermarks, the control parameters ϵ_{rob} and ϵ_{hc} are fixed at 19 and 100 respectively, which appear to provide good performances for most of the models. After fixing ϵ_{rob}, for each mesh, we increase the compensation factor α_{rob} as large as possible until visible distortion appears. α_{rob} values may also be fixed adaptively for different mesh regions according to their local properties, such as the roughness measurement proposed in [48]. This adaptive setting may lead to a more robust watermark with less perceptual distortions. The improvement on this point constitutes one part of our future work. For fragile watermark, the used parameter values are as follows: $M = 32$, $\Delta_\theta = \frac{1}{3}\pi = 60°$, $\Delta_r = 0.004$, $\alpha_\theta = 0.80$, and $\alpha_r = 0.99$.

Figure 7 illustrates the watermarked meshes (under the same viewpoints as in Figure 6) and Figure 8 shows some close-ups of the watermarked and non-watermarked meshes. From these two figures, we can see that there exist nearly no perceptible distortions introduced by the watermark embedding, especially

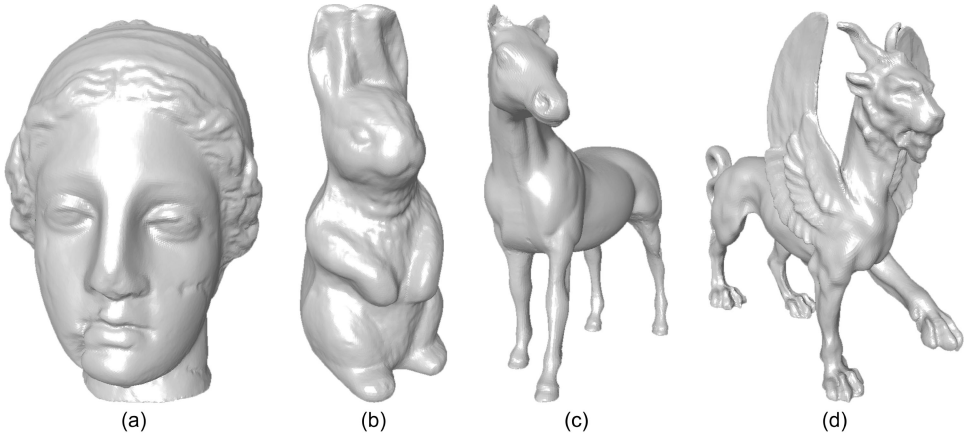


Fig. 6. The original non-watermarked semi-regular meshes used for experiments: (a) Venus, (b) Rabbit, (c) Horse, (d) Feline.

on relatively rough regions. However, on very smooth regions (*e.g.* the body of the Horse), some scar-like artifacts can appear, even under a very low watermarking strength. It is actually a common problem for 3D mesh watermarking. This problem also emphasizes the importance of studying perceptual assessment of mesh watermarking algorithms [50]–[52], which can help to devise a perceptually adaptive watermark with different strengths in different spatial areas.

Table III lists the baseline evaluations of the hierarchical watermarking framework. All the tests have been carried out on a Pentium IV 2.8GHz processor with 2GB memory. The objective distortion between watermarked and original meshes is measured by Metro [53] in terms of maximum root mean square error (MRMS) and Hausdorff distance (HD). A "perceptual" distance between them is evaluated by the mesh structural distortion measure (MSDM) proposed in [51]. Its value tends toward 1 (theoretical limit) when the measured objects are visually very different and is equal to 0 for identical ones. One advantage of the robust watermark is that it can introduce relatively high-amplitude objective modifications while keeping them perceptually invisible (the induced MSDM is less than 0.1), since these modifications are rather of low frequencies. It is well known that for 3D mesh watermarking, the lower frequency component modifications are both more imperceptible and more robust. The MSDM remains low even after the insertion of all the three watermarks, which demonstrates the good imperceptibility of the whole hierarchical watermarking system. Note that for the first three models, the maximum possible repetition rate is used for the 64-bit robust watermark. Contrarily, for Feline model, although its has 756 edges in the coarsest-level, only the 64 longest edges are used for watermarking. Actually, the edges in the coarsest representation are very numerous so that they tend to have similar lengths and their associated WCVs become of rather intermediate frequencies, thus the synchronization mechanism and the WCV norm quantization become less robust and the watermark repetition no longer improves the robustness. This will not introduce ambiguity at extraction since we can easily estimate whether there exists bit repetition by simply examining the autocorrelation function of the extracted bit sequence from all the coarsest-level edges.

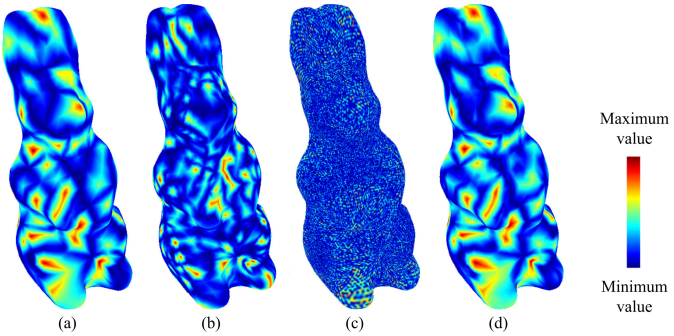


Fig. 9. Maps of the objective distortions introduced by (a) the robust watermark, (b) the high-capacity watermark, (c) the fragile watermark, and (d) all the three watermarks on the Rabbit mesh.

Figure 9 illustrates the maps of the objective distortions introduced by different watermarks on the Rabbit mesh. The distortion pattern varies from relatively low frequency for robust watermark, to intermediate frequency for high-capacity watermark, and finally to high frequency for fragile watermark.

B. Robustness evaluation

The resistance of the robust watermark is tested under different geometric attacks, including vertex reordering, similarity transformation, noise addition, smoothing and quantization. The robustness is measured by the normalized correlation between the extracted watermark bit string and the originally inserted one. This correlation value varies between -1 (orthogonal strings) and +1 (identical strings). The distortion induced by attacks is also measured by MRMS, HD and MSDM (third to fifth columns of Tables IV to VI). In our simulations, the maximum amplitude of the uniform additive noise is relative to the average distance from the vertices to the mesh center. For each amplitude, we perform five experiments using different seeds to generate different noise patterns and report the average as the final result. In smoothing attacks, the mesh is processed by Laplacian smoothing [54] with different iteration numbers while fixing the scaling factor λ as 0.10. In quantization attacks, the distance from a vertex to the mesh center is quantized: an 8-bit quantization implies that this distance is quantized to one of the 256 possible levels.

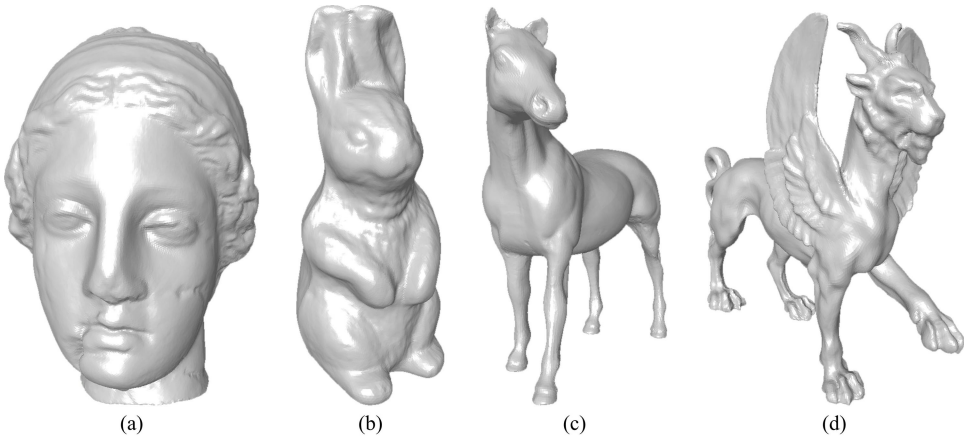


Fig. 7. The watermarked semi-regular meshes: (a) Venus, (b) Rabbit, (c) Horse, (d) Feline.

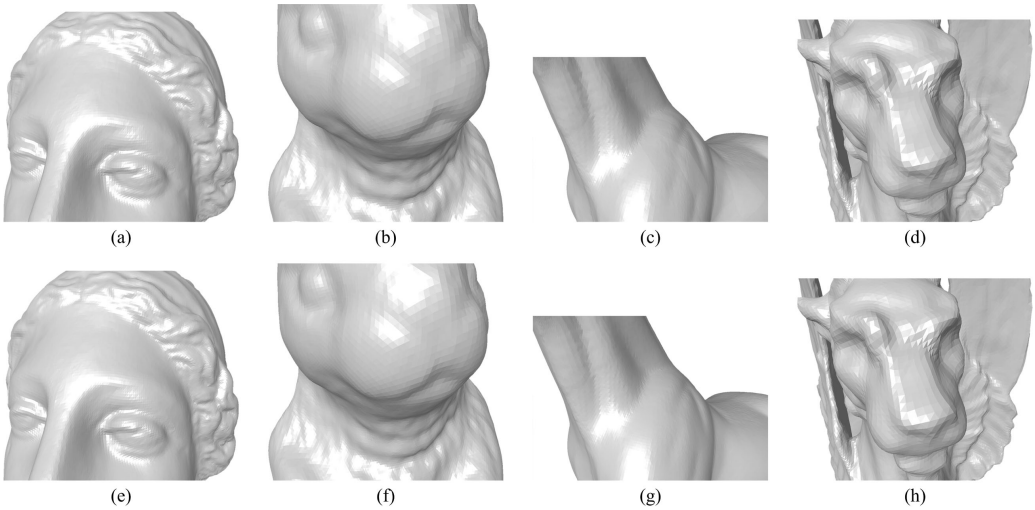
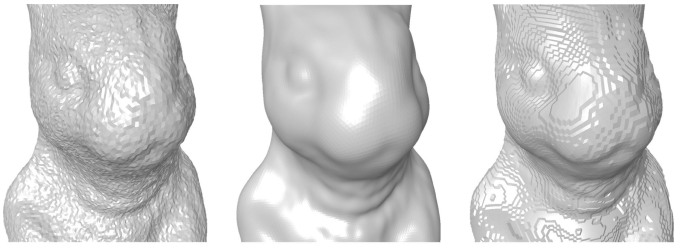


Fig. 8. Close-ups of the watermarked meshes: (a) Venus, (b) Rabbit, (c) Horse, (d) Feline. The corresponding non-watermarked close-ups are also provided as (e)-(h) for comparison.

TABLE III
BASELINE EVALUATIONS OF THE HIERARCHICAL WATERMARKING FRAMEWORK

	Venus	Rabbit	Horse	Feline
Embedding time of three WMs (s)	61.23	26.30	41.54	23.55
Extraction time of three WMs (s)	14.44	8.33	10.61	5.92
MRMS by three WMs (10^{-3})	1.24	1.15	0.67	0.72
HD by three WMs (10^{-3})	5.87	3.99	2.65	3.93
MSDM by three WMs	0.056	0.077	0.11	0.10
Payload of the robust WM (bits)	64	64	64	64
Value of α_{rob}	0.50	0.70	0.50	0.85
Repetition time of the robust WM	1	3	5	1
MRMS by robust WM (10^{-3})	1.21	1.12	0.64	0.71
HD by robust WM (10^{-3})	5.87	3.99	2.65	3.97
MSDM by robust WM	0.039	0.070	0.098	0.096
Embedding level of the H-C WM	4	4	4	3
Edges in that level	1920	828	1320	3024
Payload of the H-C WM (K bits)	7.632	3.18	5.247	11.925
MRMS by H-C WM (10^{-3})	0.22	0.20	0.15	0.12
HD by H-C WM (10^{-3})	1.07	1.00	0.78	0.67
MSDM by H-C WM	0.045	0.039	0.058	0.047
MRMS by fragile WM (10^{-3})	0.01	0.01	0.01	0.02
HD by fragile WM (10^{-3})	0.14	0.10	0.18	0.21
MSDM by fragile WM	0.025	0.023	0.032	0.032

*'WM' stands for 'watermark', and 'H-C' stands for 'high-capacity'.



(a) (b) (c)

Fig. 10. Some attacked Rabbit models for the robust watermark test: (a) by a 0.25% noise, (b) by a Laplacian smoothing of 30 iterations ($\lambda = 0.10$), and (c) by an 8-bit quantization.

The robust watermark is experimentally invariant to vertex reordering and similarity transformations. Table IV, V and VI present the robustness evaluations against noise addition, smoothing and quantization. Figure 10 illustrates several attacked Rabbit meshes. Our scheme works better for Venus, Rabbit and Horse models than for Feline model. The main reason is that Feline has too many edges in its coarsest-level irregular mesh, thus the corresponding WCVs belong to rather intermediate frequency and their modifications are less robust. The second reason may be that the actual parameter setting is not very suitable for a mesh possessing so many edges in its coarsest-level representation.

More precisely, under noise addition, the performance of our scheme begins to decline when the MRMS error introduced by an attack attains half of the MRMS distortion caused by watermark embedding. This is reasonable because the watermark is inserted via a 2-symbol quantization. The scheme shows better performance under smoothing and quantization than under noise addition for similar attack-induced MRMS errors. It can also be observed from the tables that our robust watermark can withstand an attack that introduces a much higher MSDM distance (*i.e.* visual difference) than that caused by the watermark embedding.

Experimentally, the induced distortion increases as ϵ_{rob} decreases or α_{rob} increases. A perfect security is gained when $\alpha_{rob} = 0.50$, then the quantity of the leaked information increases as α_{rob} increases. One interesting point is the robustness variation along with the values of ϵ_{rob} and α_{rob}. When ϵ_{rob} is fixed, under a certain attack, it seems that there exists an optimum value for α_{rob} that maximizes the robustness. When α_{rob} is fixed, in general, the robustness is experimentally improved under small-amplitude attacks as ϵ_{rob} decreases. However, under moderate or strong attacks, robustness may not certainly be improved when ϵ_{rob} decreases. The main reason is that the robustness is also related to α_{rob}, to the number of payload and to the error correction coding.

In general, the robustness of our scheme outperforms the early non-blind algorithm of Kanai *et al.* [20]. It is difficult to compare our readable watermarking scheme with the detectable (one-bit watermarking) scheme of Uccheddu *et al.* [21]; nonetheless, the critical attack amplitude (*e.g.* for which the correlation is equal to 0.70) in our algorithm seems comparable with the maximum tolerable attack amplitude in their method. Compared with the recent blind scheme of Cho *et al.* [25], it appears that our scheme shows better robustness under smoothing but is less robust under noise addition. Concerning the introduced distortion, both schemes have their advantages: in the scheme of Cho *et al.*, the distortion is rather of high frequency but the watermark can resist attacks that induce much higher objective distortion than it; in our scheme, the distortion is rather of low frequency and relatively high objective distortion can be introduced by watermark embedding while keeping it imperceptible. Our technique has a higher security level than their method that is based on vertex norm histogram modification. Finally, it is important to note that the current parameter setting of our scheme is very conservative and in favor of the watermark imperceptibility and security instead of the robustness.

As anticipated, the high-capacity watermark is robust to vertex reordering and similarity transformation, but somewhat fragile to other attacks. It can resist until about 0.002% to 0.004% ramdom additive noise. The maximum resistable noise amplitude seems inversely propotional to the edge number of the resolution level where the high-capacity watermark is embedded. In the current implementation, the imperceptibility of the high-capacity watermark mainly depends on the value of ϵ_{hc}: when ϵ_{hc} decreases, the watermark becomes more visible. For example, when the watermark is embedded in level 4 of Rabbit, the critical value for ϵ_{hc} is about 70 beyond which the watermark becomes visible. The watermark payload depends on the parameter G, which has an upper limit due to the limited vertex coordinate storage precision. This precision is fixed as 6 digits per coordinate in our experiments. If the watermark is inserted in level 4 of Rabbit with $\epsilon_{hc} = 70$, G can be increased up to the total edge number of this level (828 edges) so as to permit a payload of $6.837K$ bits. On the contrary, if the watermark is embedded in level 3 that has 3312 edges, with $\epsilon_{hc} = 70$, G cannot be greater than 750 (then the payload is $24.34K$ bits) in order to ensure the watermark correctness under a 6-digit vertex coordinate storage precision.

C. ROC analysis

In this subsection, we consider our robust scheme as a detectable algorithm with a watermark presence decision step after the watermark bit extraction. The receiver operating characteristics (ROC) of the detectable robust algorithm under noise and smoothing attacks have been experimentally analyzed. To complete the ROC curves, we have first prepared 100 watermarked meshes of the same object (Rabbit) using different random watermarks and random keys. The algorithm parameter values are the same as mentioned above. We have then attacked these models (noise and smoothing); for each attacked model, two detections are carried out: one with the right watermark and the right key, and the other with a wrong watermark and a wrong key. Then, for each kind of attack with different amplitudes, the false positive and false negative curves are drawn by varying the correlation threshold value that is used to decide the watermark presence. These curves are approximated to Gaussian distributions and the ROC curves that represent the relationship between the false negative value P_{fn} and the false positive value P_{fp} are obtained. According to the experimental results presented in Figure 11 where the

TABLE IV
RESISTANCE OF THE ROBUST WATERMARK AGAINST RANDOM NOISE ADDITION

Model	Noise	MRMS (10^{-3})	HD (10^{-3})	MSDM	Correlation
Venus	0.05%	0.17	0.62	0.28	0.85
	0.25%	0.84	3.15	0.70	0.59
	0.50%	1.67	6.25	0.83	0.31
Rabbit	0.05%	0.11	0.41	0.18	0.92
	0.25%	0.55	2.06	0.60	0.59
	0.50%	1.10	4.04	0.77	0.31
Horse	0.05%	0.11	0.41	0.23	0.96
	0.25%	0.55	2.03	0.64	0.50
	0.50%	1.10	4.07	0.78	0.08
Feline	0.05%	0.13	0.47	0.16	0.78
	0.25%	0.63	2.33	0.53	0.39
	0.50%	1.26	4.73	0.69	0.02

TABLE V
RESISTANCE OF THE ROBUST WATERMARK AGAINST LAPLACIAN SMOOTHING ($\lambda = 0.10$)

Model	Iterations	MRMS (10^{-3})	HD (10^{-3})	MSDM	Correlation
Venus	10	0.27	5.65	0.15	0.74
	30	0.68	9.75	0.27	0.71
	50	1.01	12.20	0.34	0.62
Rabbit	10	0.24	2.77	0.15	0.90
	30	0.65	6.93	0.26	0.71
	50	1.03	10.29	0.31	0.45
Horse	10	0.21	5.67	0.15	0.97
	30	0.54	9.97	0.23	0.50
	50	0.80	12.95	0.28	0.35
Feline	5	0.33	7.61	0.12	0.74
	10	0.63	12.47	0.18	0.50
	30	1.59	21.45	0.31	-0.02

TABLE VI
RESISTANCE OF THE ROBUST WATERMARK AGAINST COORDINATE QUANTIZATION

Model	Quantization	MRMS (10^{-3})	HD (10^{-3})	MSDM	Correlation
Venus	9-bit	0.93	1.95	0.49	0.93
	8-bit	1.85	3.90	0.66	0.70
	7-bit	3.70	7.80	0.79	0.63
Rabbit	9-bit	0.76	1.95	0.44	0.84
	8-bit	1.55	3.90	0.61	0.59
	7-bit	3.10	7.80	0.76	0.05
Horse	9-bit	0.68	1.95	0.44	0.61
	8-bit	1.35	3.90	0.60	0.25
	7-bit	2.70	7.80	0.73	0.17
Feline	10-bit	0.30	0.97	0.16	0.70
	9-bit	0.60	1.95	0.29	0.53
	8-bit	1.20	3.90	0.44	0.50

equal error rates (EER) of the curves are also indicated, our method demonstrates satisfying performance under both attacks, even with relatively strong amplitude. For instance, under 0.15% noise, an appropriate threshold value can be found so that false positive and false negative probabilities are both equal to 10^{-5}.

D. Fragile watermark test

We have fixed the parameters of the fragile watermark so as to resist an angle distortion until about 1° and a WCV norm distortion until about 0.2% of the minimum edge length (see Equations 8 and 9). In order to verify its effectiveness, several attacked models have been prepared. These attacks include similarity transformation, local invisible noise addition, local deformation, local rotation and global geometric processing. Figure 12.(a)-(e) show the attacked Rabbit models. Their corresponding authentication results are illustrated in Figure 12.(f)-(j). The watermark is practically invariant to similarity transformations (Figure 12.(f)). According to the watermark extraction results, we can successfully locate the noised part (Figure 12.(g)) and the deformed part (Figure 12.(h)) on the modified models. We can also report a possible local rotation (in Figure 12.(i), the neck of the Rabbit is invalid since the head has be rotated) and detect a global modification (such as a smoothing in Figure 12.(j)).

VIII. CONCLUSION AND FUTURE WORK

A new hierarchical watermarking framework has been proposed in this paper. Three different watermarks (robust, high-capacity and fragile) are simultaneously embedded in a same semi-regular mesh. The robust watermark is able to resist common geometric attacks even with a relatively high amplitude. For the high-capacity watermark, we demonstrate the possibility of embedding much more bits by relying on

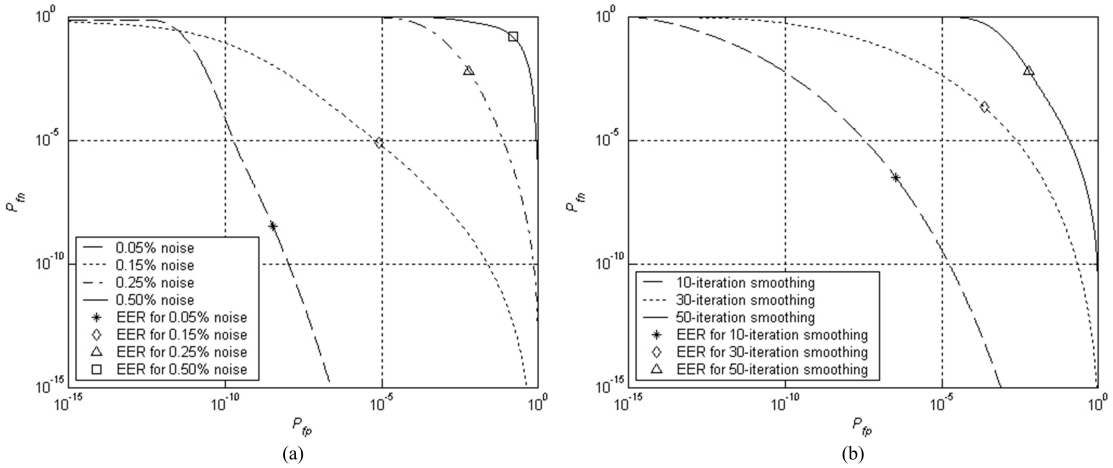


Fig. 11. ROC curves of the robust watermarking algorithm under (a) random noise addition and (b) Laplacian smoothing ($\lambda = 0.10$). The tests have been carried out on the Rabbit model.

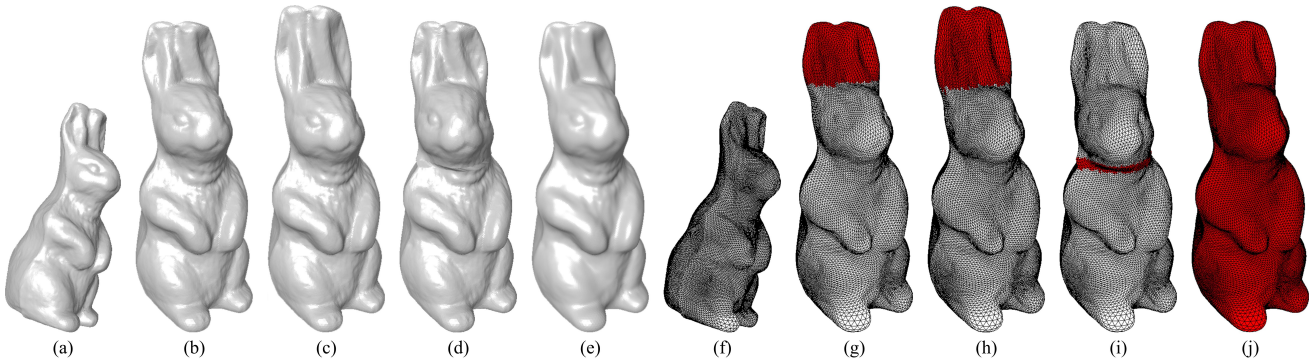


Fig. 12. Some attacked Rabbit models for the fragile watermark test: (a) by a similarity transformation, (b) by a 0.0005% binary invisible noise on the ears, (c) by a local deformation where the ears have been pulled up, (d) by a local rotation where the head has been rotated for $15°$, and (e) by a 10-iteration Laplacian smoothing with $\lambda = 0.10$. The corresponding authentication results are visulized in (f)-(j), where valid parts are rendered in white, while the invalid parts are rendered in red.

the relative relationship between the different watermarking primitives. To our knowledge, the fragile watermark is the first in the literature that is robust to all the content-preserving operations and at the same time provides a precise attack localization capability. Meanwhile, during the algorithms' design process, we have explicitly taken the watermarking security into account.

Concerning the future work, in short terms, we plan to implement some improvements for the three watermarking schemes: for the robust watermark, we want to combine our scheme with more advanced error correction coding methods in order to enhance robustness; for the high-capacity watermark, we intend to design an error correction code for the adopted permutation coding so as to make it less fragile; a study on the optimum and adaptable parameter setting of these three schemes for different meshes is also in schedule; finally, we plan to use local mesh geometric properties to synchronize the robust and high-capacity watermarks and to determine locally adaptable watermarking strengths in different parts of the mesh. In long terms, we look forward to devising a fully working fragile watermark for arbitrary 3D meshes based on our current work on semi-regular meshes; the design of a robust remeshing technique is also of our interest so as to generalize our robust algorithm to arbitrary meshes; finally, it is interesting to exploit the interplay between the robust and the fragile watermarks, because the fragile one may provide some information about the reliability of the robust one in different regions of an attacked model.

ACKNOWLEDGMENT

The authors would like to thank Céline Roudet for her help on the wavelet analysis and synthesis of three-dimensional semi-regular meshes.

REFERENCES

[1] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. Morgan Kaufmann Publishers Inc., 2001.

[2] M. Barni and F. Bartolini, *Watermarking Systems Engineering: Enabling Digital Assets Security and other Applications*. Marcel Dekker Inc., 2004.

[3] M. Botsch, M. Pauly, L. Kobbelt, P. Alliez, B. Lévy, S. Bischoff, and C. Rössl, "Geometric modeling based on polygonal meshes," in *Proc. of the ACM SIGGRAPH Course Notes*, 2007.

[4] F. Mintzer and G. W. Braudaway, "If one watermark is good, are more better?" in *Proc. of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, 1999, pp. 2067–2069.

[5] N. P. Sheppard, R. Safavi-Naini, and P. Ogunbona, "On multiple watermarking," in *Proc. of the International Workshop on Multimedia and Security*, 2001, pp. 3–6.

[6] C.-S. Lu and H.-Y. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Transactions on Image Processing*, vol. 10, no. 10, pp. 1579–1592, 2001.

[7] C.-S. Lu, H.-Y. Liao, and L.-H. Chen, "Multipurpose audio watermarking," in *Proc. of the International Conference on Pattern Recognition*, vol. 3, 2000, pp. 282–285.

[8] A. Khodakovsky, P. Schröder, and W. Sweldens, "Progressive geometry compression," in *Proc. of the ACM SIGGRAPH*, 2000, pp. 271–278.

[9] F. Payan and M. Antonini, "Mean square error approximation for wavelet-based semiregular mesh compression," *IEEE Transactions on Visualization and Computer Graphics*, vol. 12, no. 4, pp. 649–657, 2006.

[10] J.-H. Yang, C.-S. Kim, and S.-U. Lee, "Semi-regular representation and progressive compression of 3-D dynamic mesh sequences," *IEEE Transactions on Image Processing*, vol. 15, no. 9, pp. 2531–2544, 2006.

[11] Z. J. Wood, P. Schröder, D. Breen, and M. Desbrun, "Semi-regular mesh extraction from volumes," in *Proc. of the IEEE Visualization*, 2000, pp. 275–282.

[12] I. Guskov, "Manifold-based approach to semi-regular remeshing," *Graphical Models*, vol. 69, no. 1, pp. 1–18, 2007.

[13] M. Ahn, I. Guskov, and S. Lee, "Out-of-core remeshing of large polygonal meshes," *IEEE Transactions on Visualization and Computer Graphics*, vol. 12, no. 5, pp. 1221–1228, 2006.

[14] M. Lounsbery, T. D. DeRose, and J. Warren, "Multiresolution analysis for surfaces of arbitrary topological type," *ACM Transactions on Graphics*, vol. 16, no. 1, pp. 34–73, 1997.

[15] R. Ohbuchi and H. Masuda, "Managing CAD data as a multimedia data type using digital watermarking," in *Proc. of the IFIP TC5 WG5.2 Workshop on Knowledge Intensive CAD to Knowledge Intensive Engineering*, 2001, pp. 103–116.

[16] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: Theory and practice," *IEEE Transactions on Signal Processing*, vol. 53, no. 10, pp. 3976–3987, 2005.

[17] P. Comesaña, L. Pérez-Freire, and F. Pérez-González, "Fundamentals of data hiding security and their application to spread-spectrum analysis," in *Proc. of the International Workshop on Information Hiding*, 2005, pp. 146–160.

[18] P. Rondao-Alface and B. Macq, "From 3D mesh data hiding to 3D shape blind and robust watermarking: A survey," *LNCS Transactions on Data Hiding and Multimedia Security*, vol. 2, pp. 99–115, 2007.

[19] K. Wang, G. Lavoué, F. Denis, and A. Baskurt, "Three-dimensional meshes watermarking: Review and attack-centric investigation," in *Proc. of the International Workshop on Information Hiding*, 2007, pp. 50–64.

[20] S. Kanai, H. Date, and T. Kishinami, "Digital watermarking for 3D polygons using multiresolution wavelet decomposition," in *Proc. of the International Workshop on Geometric Modeling: Fundamentals and Applications*, 1998, pp. 296–307.

[21] F. Uccheddu, M. Corsini, and M. Barni, "Wavelet-based blind watermarking of 3D models," in *Proc. of the ACM International Workshop on Multimedia and Security*, 2004, pp. 143–154.

[22] M.-S. Kim, S. Valette, H.-Y. Jung, and R. Prost, "Watermarking of 3D irregular meshes based on wavelet multiresolution analysis," in *Proc. of the International Workshop on Digital Watermarking*, 2005, pp. 313–324.

[23] M.-S. Kim, J.-W. Cho, R. Prost, and H.-Y. Jung, "Wavelet analysis based blind watermarking for 3-D surface meshes." in *Proc. of the International Workshop on Digital Watermarking*, 2006, pp. 123–137.

[24] S. Valette and R. Prost, "Wavelet-based multiresolution analysis of irregular surface meshes," *IEEE Transactions on Visualization and Computer Graphics*, vol. 10, no. 2, pp. 113–122, 2004.

[25] J.-W. Cho, R. Prost, and H.-Y. Jung, "An oblivious watermarking for 3D polygonal meshes using distribution of vertex norms," *IEEE Transactions on Signal Processing*, vol. 55, no. 1, pp. 142–155, 2007.

[26] R. Ohbuchi, H. Masuda, and M. Aono, "Data embedding algorithms for geometrical and non-geometrical targets in three-dimensional polygonal models." *Computer Communications*, vol. 21, no. 15, pp. 1344–1354, 1998.

[27] A. G. Bors, "Watermarking mesh-based representations of 3-D objects using local moments." *IEEE Transactions on Image Processing*, vol. 15, no. 3, pp. 687–701, 2006.

[28] R. Ohbuchi, A. Mukaiyama, and S. Takahashi, "A frequency-domain approach to watermarking 3D shapes," *Computer Graphics Forum*, vol. 21, no. 3, pp. 373–382, 2002.

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

[30] G. Lavoué, F. Denis, and F. Dupont, "Subdivision surface watermarking," *Computers & Graphics*, vol. 31, no. 3, pp. 480–492, 2007.

[31] J. Wu and L. Kobbelt, "Efficient spectral watermarking of large meshes with orthogonal basis functions," *The Visual Computer*, vol. 21, no. 8-10, pp. 848–857, 2005.

[32] E. Praun, H. Hoppe, and A. Finkelstein, "Robust mesh watermarking," in *Proc. of the ACM SIGGRAPH*, 1999, pp. 49–56.

[33] O. Benedens, "Geometry-based watermarking of 3D models," *IEEE Computer Graphics and Applications*, vol. 19, no. 1, pp. 46–55, 1999.

[34] S. Zafeiriou, A. Tefas, and I. Pitas, "Blind robust watermarking schemes for copyright protection of 3D mesh objects," *IEEE Transactions on Visualization and Computer Graphics*, vol. 11, no. 5, pp. 596–607, 2005.

[35] P. Rondao-Alface and B. Macq, "Blind watermarking of 3D meshes using robust feature points detection," in *Proc. of the IEEE International Conference on Image Processing*, 2005, pp. 693–696.

[36] P. Rondao-Alface, B. Macq, and F. Cayre, "Blind and robust watermarking of 3D models: How to withstand the cropping attack?" in *Proc. of the IEEE International Conference on Image Processing*, 2007, pp. V465–V468.

[37] W.-H. Cho, M.-E. Lee, H. Lim, and S.-Y. Park, "Watermarking technique for authentication of 3-D polygonal meshes," in *Proc. of the International Workshop on Digital Watermarking*, 2004, pp. 259–270.

[38] B.-L. Yeo and M. M. Yeung, "Watermarking 3D objects for verification," *IEEE Computer Graphics and Applications*, vol. 19, no. 1, pp. 36–45, 1999.

[39] H.-Y. S. Lin, H.-Y. M. Liao, C.-S. Lu, and J.-C. Lin, "Fragile watermarking for authenticating 3-D polygonal meshes," *IEEE Transactions on Multimedia*, vol. 7, no. 6, pp. 997–1006, 2005.

[40] C.-M. Chou and D.-C. Tseng, "A public fragile watermarking scheme for 3D model authentication," *Computer-Aided Design*, vol. 38, no. 11, pp. 1154–1165, 2006.

[41] H.-T. Wu and Y.-M. Cheung, "A high-capacity data hiding method for polygonal meshes," in *Proc. of the International Workshop on Information Hiding*, 2006, pp. 188–200.

[42] F. Cayre and B. Macq, "Data hiding on 3-D triangle meshes," *IEEE Transactions on Signal Processing*, vol. 4, no. 51, pp. 939–949, 2003.

[43] Y.-M. Cheng and C.-M. Wang, "A high-capacity steganographic approach for 3D polygonal meshes," *The Visual Computer*, vol. 22, no. 9, pp. 845–855, 2006.

[44] O. Benedens, "Two high capacity methods for embedding public watermarks into 3D polygonal models," in *Proc. of the ACM Workshop on Multimedia and Security*, 1999, pp. 95–99.

[45] H.-T. Wu and Y.-M. Cheung, "A fragile watermarking scheme for 3D meshes," in *Proc. of the ACM Workshop on Multimedia and Security*, 2005, pp. 117–124.

[46] J. J. Eggers, R. Bauml, R. Tzschoppe, and B. Girod, "Scalar costa scheme for information embedding," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 1003–1019, 2003.

[47] L. Pérez-Freire, P. Comesaña, and F. Pérez-González, "Information-theoretic analysis of security in side-informed data hiding," in *Proc. of the International Workshop on Information Hiding*, 2005, pp. 131–145.

[48] G. Lavoué, "A roughness measure for 3D mesh visual masking," in *Proc. of the ACM Symposium on Applied Perception in Graphics and Visualization*, 2007, pp. 57–60.

[49] I. Guskov, K. Vidimce, W. Sweldens, and P. Schröder, "Normal meshes," in *Proc. of the ACM SIGGRAPH*, 2000, pp. 95–102.

[50] P. Rondao-Alface and B. Macq, "Shape quality measurement for 3D watermarking schemes," in *Proc. of the SPIE-IS and T Electronic Imaging, Security and Watermarking of Multimedia Contents*, vol. 6072, 2006, pp. 622–634.

[51] G. Lavoué, E. D. Gelasca, F. Dupont, A. Baskurt, and T. Ebrahimi, "Perceptually driven 3D distance metrics with application to watermarking," in *Proc. of the SPIE-IS and T Electronic Imaging*, vol. 6312, 2006, p. 63120L.

[52] M. Corsini, E. D. Gelasca, T. Ebrahimi, and M. Barni, "Watermarked 3-D mesh quality assessment," *IEEE Transactions on Multimedia*, vol. 9, no. 2, pp. 247–255, 2007.

[53] P. Cignoni, C. Rocchini, and R. Scopigno, "Metro: Measuring error on simplified surfaces," *Computer Graphics Forum*, vol. 17, no. 2, pp. 167–174, 1998.

[54] G. Taubin, "Geometric signal processing on polygonal meshes," in *Proc. of the Eurographics State-of-the-art Reports*, 2000, pp. 81–96.

Kai Wang received the B.E. degree in Telecommunication Engineering from Xi'an Jiaotong University, China, in 2003. From 2001 to 2006, he participated in a double diploma project agreed between Chinese and French governments. Therefore in 2006, he received the M.E. degree in Pattern Recognition and Intelligent System from Xi'an Jiaotong University, China, and the Generalist Engineer degree from Ecole Centrale de Lyon, France, respectively.

He is currently pursuing the Ph.D. degree at INSA of Lyon, France. His research interests include multimedia signal processing, digital watermarking of images and 3D meshes, and pattern recognition.

Guillaume Lavoué received in 2002 the Engineer degree in Electronic, Telecommunication and Computer Science from CPE-Lyon, France, and the M.S. degree in Image Processing from Université Jean Monnet de St-Etienne, France. In 2005, he obtained the Ph.D. degree in Computer Science from Université Lyon 1, France. From February to April 2006, he was a postdoctoral fellow at Signal Processing Institute in Switzerland.

He is currently an Associate Professor of Computer Science at INSA of Lyon, France. His research interests include 3D digital image processing, 3D digital watermarking, geometric modeling and more precisely 3D compression and subdivision surfaces.

Florence Denis was born in Marseille, France, in 1962. She received the B.S. degree in 1985, the M.S. degree in 1985 and the Ph.D. degree in 1990, all from INSA of Lyon, France.

She is currently an Associate Professor at Université Lyon 1, France. She is also a member of the image processing group at the LIRIS Laboratory. Her research interests are in the fields of 2D and 3D image processing, segmentation and watermarking.

Atilla Baskurt was born in Ankara, Turkey, in 1960. He received the B.S. degree in 1984, the M.S. degree in 1985 and the Ph.D. degree in 1989, all in Electrical Engineering from INSA of Lyon, France.

Since December 2007, he is the Vice Chair of the research center LIRIS. He leads his research activities in two teams of LIRIS: the IMAGINE team and the M2DisCo team. These teams work on image and 3D data analysis and segmentation for image compression, image retrieval, shape detection and identification. His technical research and experience include digital image processing, 2D-3D data analysis, compression, retrieval and watermarking, especially for multimedia applications. He is also "Chargé de mission" on Information and Communication Technologies at the French Research Ministry.