A Fragile Watermarking Scheme for Authentication of Semi-regular Meshes †

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

Abstract

This paper presents a fragile watermarking scheme for authentication of 3D semi-regular meshes. After one wavelet decomposition, the watermark is inserted by slightly modifying the norms and orientations of the obtained wavelet coefficient vectors. The inserted watermark is robust to the so-called content-preserving attacks including vertex reordering and similarity transformations. However, it is vulnerable to others attacks such as local and global geometric modifications and remeshing since the objective is to check the integrity of the mesh. Additionally, according to the watermark extraction result, these attacks can be precisely located on the surface of the attacked mesh in a blind way. Sufficient security level is also achieved by introducing secret keys and by using scalar Costa quantization scheme with appropriate parameter values. Experimental results demonstrate the efficacy of the proposed watermarking scheme.

Categories and Subject Descriptors (according to ACM CCS): I.3.5 [Computer Graphics]: Computational Geometry and Object Modeling - Surface Representations.

1. Introduction

Digital watermarking is the art of hiding a piece of secret information within the functional part of another content that can be an image, an audio or video clip, a 3D mesh, and so forth. One can distinguish between robust watermarking used for copyright protection and fragile watermarking used for authentication (integrity verification). The former should be able to survive through various unintentional operations and intentional attacks on the watermarked content, while the latter should be fragile to even very slight modifications. A valuable fragile scheme should also offer the capability of locating the modified parts of the content to be authenticated. Practically, this localization capability is a particular advantage of the authentication based on watermarking compared to that based on cryptography.

A semi-regular mesh is a piecewise regular structure since it consists of a patchwork of large regular regions; hence it owns regular vertices (valence 6 in the case of triangular mesh) almost everywhere. 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 highly attractive for many applications involving level of details management such as filtering, texturing, rendering and particularly compression. Along with the popular use of semi-regular meshes mainly thanks to the research on remeshing techniques, users are seeking for an effective technique for their authentication. The authentication based on fragile watermarking appears a very attractive solution, with its potential precise attack localization capability.

One may think that a fragile watermark should be vulnerable to all possible attacks since the objective is to detect any malicious modifications on the watermarked mesh. However, some so-called content-preserving attacks, including vertex reordering and similarity transformations (i.e. translation, rotation, uniform scaling and their combination), have theoretically no impact on the mesh shape; therefore, they are often not considered as attacks but as routine operations against which even a fragile watermark is required to be able

† 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.

to stand. Hence, the typical requirement for a fragile watermark of 3D mesh [WLDB07] is that it should be robust to the aforementioned content-preserving attacks while being vulnerable to the other attacks. In addition, the attack localization capability, as precise as possible, is always desired.

To our knowledge, the fragile watermarking of semi-regular meshes has only been addressed by Cho et al. [CLLP04]. They first apply several wavelet decompositions on the original 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 inputs of these two functions are invariant to similarity transformations. However, it seems there exist two problems: first, the causality problem occurs because the modification of the current to-be-watermarked facet can influence the validities of its already watermarked neighbouring 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.

The fragile watermarking for authenticating arbitrary 3D meshes is studied in several references [YY99, LLLL05, CT06, WC06]. In these four algorithms, either vertex coordinates or the relative position of a vertex to its traversed 1-ring neighbours (in a certain vertex traversal algorithm) 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.

2. Proposed fragile watermarking scheme

The proposed fragile watermarking scheme is based on wavelet transform of semi-regular meshes [LDW97]. Fig. 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 Fig. 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 Fig. 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 subdivision connectivity and the dual synthesis algorithm can accomplish the inverse reconstruction.

Following subsections will detail the different steps of the watermark embedding and extraction procedures of the proposed scheme. Our scheme is robust to both vertex reordering and similarity transformations. Meanwhile, the causality problem is avoided and the algorithm's security can be ensured. The blindness of the watermark extraction, which is mandatory for an authentication algorithm, is also achieved. Finally, the endured attacks can be precisely located based on the watermark extraction result. Although we consider triangular semi-regular meshes, our method is easy to extend to any semi-regular mesh with arbitrary facet degree.

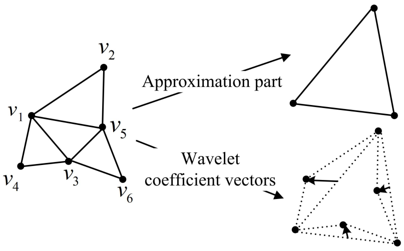

Figure 1: *Illustration of one iteration of the lazy wavelet decomposition mechanism.*

2.1. Watermark embedding

The first step is to carry out one iteration of wavelet decomposition on the original non-watermarked semi-regular mesh $\mathcal{M}_0$. Then, we obtain a coarser mesh $\mathcal{M}_1$ and a set of N wavelet coefficient vectors denoted by $\mathcal{C} = \{\mathbf{c_1}, \mathbf{c_2}, ..., \mathbf{c_N}\}$, where N is also the number of edges in $\mathcal{M}_1$. Each coefficient vector $\mathbf{c_i}$ is associated with an edge $\mathbf{e_i}$ in $\mathcal{M}_1$. It is worthwhile noting that the embedding procedure is independent of these indices so they can be assigned arbitrarily. In our algorithm, we take the edges in $\mathcal{M}_1$ as raw authentication primitives; and then we derive the validity of each vertex in the dense mesh based on these edges' authentication results.

The basic idea of the watermark embedding is to find two watermarking primitives for each edge $\mathbf{e_i}$ and then slightly modify them in order to insert in both of them a same watermark symbol s_i. 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 may be modified independently, and the primitives of different edges may also 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. We have found two such primitives: the one is the acute angle between $\mathbf{c_i}$ and $\mathbf{e_i}$ that is denoted by θ_i as illustrated by Fig. 2; the other is the ratio between the norm of $\mathbf{c_i}$ and the length of $\mathbf{e_i}$ that is denoted by $r_i = \|\mathbf{c_i}\| / \|\mathbf{e_i}\|$. Both primitives are theoretically invariant to similarity transformations so that the robustness against them can be achieved.

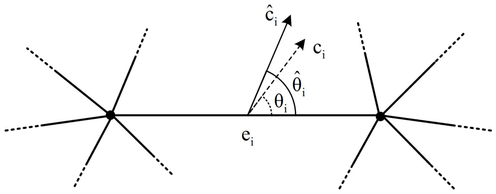

Figure 2: *Illustration of the watermarking primitives and the modification of the norm and orientation of a wavelet coefficient vector.*

The next step is the watermark symbol insertion. This symbol s_i can be any of the item in the symbol set $\mathcal{A} =$

$\{a_1, a_2, ..., a_M\}$, where M is the number of legal symbols. In practice, θ_i and r_i are both quantized by using the M-symbol Scalar Costa Scheme (SCS) [EBTG03]. θ_i 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_i for edge $\mathbf{e_i}$ and therefore for the future quantization of r_i. Furthermore, this quantization also ensures a sufficient robustness of the implied symbol of θ_i to similarity transformations, which can cause slight perturbation of θ_i due to calculation and storage precision limits. The reason for taking out symbol-preserving quantization on θ_i rather than on r_i is that θ_i is more sensitive to similarity transformations and its modification is less imperceptible than r_i.

The practical quantization procedure is as follows: first, a component-wise random codebook is established for each θ_i as given by Equ. 1, where Δ_θ is the quantization step, $z \in \mathbb{Z}^+$ 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}, and t_{θ_i} is a pseudo-random dither signal. Note that each code word u implies a symbol in $\mathcal{A}$ that is the mapped symbol of value l in u's derivation.

$$\mathcal{U}_{\theta_i,t_{\theta_i}} = \bigcup_{l=0}^{M-1} \left\{ u = z.\Delta_\theta + l\frac{\Delta_\theta}{M} + t_{\theta_i}, 0^\circ \leq u \leq 90^\circ \right\} \quad (1)$$

Then we find the nearest code word u_{θ_i} to θ_i in this codebook and take its implied symbol as s_i. The quantized value $\hat{\theta}_i$ is calculated according to Equ. 2, where $\alpha_\theta \in (0, 1]$ is a compensation factor. In our scheme, α_θ will partially drive the induced distortion and the watermark security. The security is measured by the information leakage of the secret parameters of the watermarking system through observations. A perfect security of the quantization can be gained if an appropriate value of α_θ has been selected [PFCPG05].

$$\hat{\theta}_i = \theta_i + \alpha_\theta \left(u_{\theta_i} - \theta_i \right) \quad (2)$$

Finally, as shown in Fig. 2, the orientation of $\mathbf{c_i}$ is modified by rotating it around the midpoint of $\mathbf{e_i}$ in the 2D plane engendered by $\mathbf{c_i}$ and $\mathbf{e_i}$ to reach the expected angle value $\hat{\theta}_i$.

The pseudo-random dither signal t_{θ_i} is generated by using a secret key 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, which in a broad sense also belong to the security issue. Usually, an ordering for all the watermarking primitives is established and the pseudo-random numbers can then be assigned one by one to the ordered primitives. However, we cannot adopt such a mechanism for θ_i, because we want the robustness to vertex reordering and the precise attack localization capability. To resolve this issue, a look-up table has been introduced, which gives the correspondence between value ranges of a local geometric ratio gr_i for each edge $\mathbf{e_i}$ and the sequential pseudo-random numbers generated by using a key K_θ. Practically, gr_i is the ratio between $\mathbf{e_i}$'s length and the length sum of $\mathbf{e_i}$'s incident triangles' midlines that pass the midpoint of $\mathbf{e_i}$; this ratio is invariant to similarity transformations. The 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_{s_1} to reinforce the security. For each θ_i, a number is selected from this table as t_{θ_i} according to the real value of gr_i.

The quantization of the norm-length ratio r_i is similar by using a different appropriate quantization step Δ_r and three different secret keys K_{m_2}, K_r and K_{s_2}. The significant difference is the use of a constrained codebook (given by Equ. 3, l_{s_i}'s mapped symbol is s_i) to carry out the quantization so that the quantized value $\hat{r}_i$ implies the same symbol s_i as $\hat{\theta}_i$. Keeping the orientation of the rotated $\mathbf{c_i}$ unchanged, we can modify its norm in order to reach the expected ratio value $\hat{r}_i$. Note that all the quantities involved in the quantizations (θ_i, r_i, gr_i) are local to edge $\mathbf{e_i}$ and independent of any element ordering; hence, the precise attack localization capability and the invariance to vertex reordering are ensured.

$$\mathcal{U}_{s_i,r_i,t_{r_i}} = \left\{ u = z.\Delta_r + l_{s_i}\frac{\Delta_r}{M} + t_{r_i}, u \geq 0 \right\} \quad (3)$$

Once the two quantization procedures are accomplished, an equality relationship between the two inserted watermark symbols has been established for each edge in $\mathcal{M}_1$. Then a watermarked dense mesh $\hat{\mathcal{M}}_0$ can be reconstructed by applying one wavelet synthesis on the coarser mesh $\mathcal{M}_1$ with the modified wavelet coefficient vectors $\hat{\mathbf{c}}_\mathbf{i}, 1 \leq i \leq N$.

2.2. Watermark extraction and mesh authentication

The watermark extraction does not need the original non-watermarked mesh and is quite simple with the knowledge of the six secret keys. Note that the values of Δ_θ, Δ_r and M can be fixed for all the meshes without seriously affecting the algorithm's performances. The first step is to carry out one wavelet decomposition of the semi-regular mesh to be authenticated. Then two codebooks for θ_i and r_i can be reconstructed for each edge $\mathbf{e_i}$ in the obtained coarser mesh by using the acquired keys. The two symbols can then be easily extracted by seeking the nearest code words to the actual values of θ_i and r_i. 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 (see Fig. 1) is determined by the following rule: if any of its incident edges in the coarser mesh is invalid, then it is considered as invalid; otherwise as valid. The validity of an *odd* vertex is simply the validity of the edge that is associated with its corresponding wavelet coefficient vector. This decision procedure has an effect of weak dilatation morphology operation for the real invalid vertices. We adopt such a mechanism in order to handle the false positive issue, whose occurring probability is about $1/M$. In this way, false positive can be generally avoided but some valid vertices may be marked as invalid (false negative). However, false negative is broadly thought as much more acceptable in authentication compared to false positive, especially under judicial applications.

3. Experimental results

Above all, it is worthwhile noting that it is crucial to select appropriate values for the algorithm's parameters. For instance, the quantization steps should be selected so that the watermark can just resist the precision errors introduced by similarity transformations (or by any tolerable geometric compression) while being vulnerable to other non-tolerable modifications. In this way, the quantization steps are also usually small enough to ensure the watermark imperceptibility. Furthermore, the compensation factors should also be appropriately selected in order to ensure a sufficient security level and the correctness of the quantizations. The value ranges for gr_i should be carefully determined to avoid obvious information leakage. A proper number of legal symbols is also important to achieve a good trade-off between the induced distortion and the false positive rate.

The proposed scheme has been implemented and tested on several semi-regular meshes. The watermark embedding and extraction procedures can be accomplished within a very short time (less than 15 seconds for a 2.8 GHz processor with 2GB memory for meshes having about 100K vertices). Fig. 3 and Fig. 4 illustrate the experimental results on a rabbit mesh having about 70K vertices. The used parameter values are as follows: $M = 32$, $\Delta_\theta = 60^\circ$, $\Delta_r = 0.004$, $\alpha_\theta = 0.80$, and $\alpha_r = 0.99$. The watermark is imperceptible (Fig. 3) and invariant to similarity transformations (Fig. 4.a). According to the watermark extraction result, we can successfully locate the invisibly noised part (Fig. 4.b) or the deformed part (Fig. 4.c) on the modified meshes, and can also detect a global modification (such as a remeshing in Fig. 4.d).

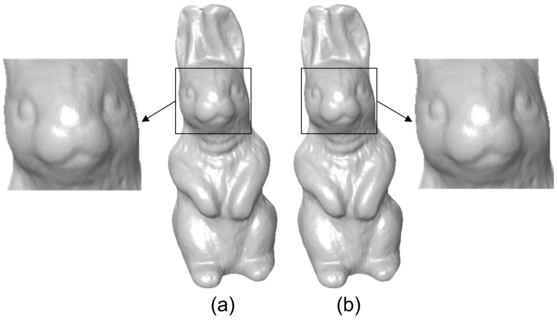

Figure 3: *The original rabbit mesh (a) and the watermarked rabbit mesh (b) with close-ups at the head. The normalized* L_2 *mean distance is* 1.1×10^{-4} *between the two meshes.*

4. Conclusion and future work

In this paper, a new fragile watermarking scheme is proposed for the authentication of 3D semi-regular meshes. To the authors' knowledge, it is the first algorithm on this topic that is robust to all the content-preserving attacks, while providing a precise attack localization capability. Our scheme can also be used as high-capacity data hiding method. Future work consists of theoretical analysis of the algorithm's performances, the application of our method under real-world network environment, and the design of such a fragile watermark for 3D irregular meshes.

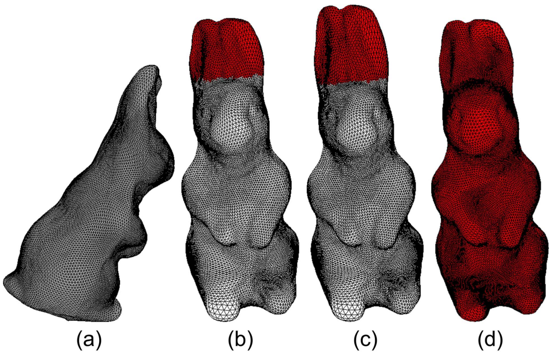

Figure 4: *Visualization of the authentication results under several attacks: (a) similarity transformation, (b) an invisible noise of 0.0003% of the vertex coordinates on the ears, (c) a local deformation on the ears that have been pulled up, and (d) a global remeshing. The valide parts are rendered in white, while the invalid parts are rendered in red.*

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

[CLLP04] Cho W. H., Lee M.-E., Lim H., Park S.-Y.: Watermarking technique for authentication of 3-D polygonal meshes. In *Proc. of the International Workshop on Digital Watermarking* (2004), pp. 259–270.

[CT06] Chou C.-M., Tseng D.-C.: A public fragile watermarking scheme for 3D model authentication. *Computer-Aided Design 38*, 11 (2006), 1154–1165.

[EBTG03] Eggers J. J., Bauml R., Tzschoppe R., Girod B.: Scalar costa scheme for information embedding. *IEEE Transactions on Signal Processing 51*, 4 (2003), 1003–1019.

[LDW97] Lounsbery M., DeRose T. D., Warren J.: Multiresolution analysis for surfaces of arbitrary topological type. *ACM Transactions on Graphics 16*, 1 (1997), 34–73.

[LLLL05] Lin H.-Y. S., Liao H.-Y. M., Lu C.-S., Lin J.-C.: Fragile watermarking for authenticating 3-D polygonal meshes. *IEEE Transactions on Multimedia 7*, 6 (2005), 997–1006.

[PFCPG05] Pérez-Freire L., Comesaña P., Pérez-González F.: Information-theoretic analysis of security in side-informed data hiding. In *Proc. of the International Workshop on Information Hiding* (2005), pp. 131–145.

[WC06] Wu H.-T., Cheung Y. M.: A high-capacity data hiding method for polygonal meshes. In *Proc. of the International Workshop on Information Hiding* (2006), pp. 188–200.

[WLDB07] Wang K., Lavoué G., Denis F., Baskurt A.: Three-dimensional meshes watermarking: Review and attack-centric investigation. In *Proc. of the International Workshop on Information Hiding* (2007), pp. 50–64.

[YY99] Yeo B.-L., Yeung M. M.: Watermarking 3D objects for verification. *IEEE Computer Graphics and Applications 19*, 1 (1999), 36–45.