A Highly Adaptable Capacity and Invisibility 3D Watermarking Based on Four-Points Sets

Xifeng Gao[1] Caiming Zhang[1,2] Yu Wei[1]
Weitao Li[1]

1. School of Computer Science and Technology, Shandong University, Jinan, China
2. School of Computer Science and Technology, Shandong Economic University, Jinan, China
beimuxiao@hotmail.com

ABSTRACT

In this paper, we propose a fine tuneable capacity and invisibility novel blind watermarking method for 3D models with arbitrary topology in spatial domain. Our watermarking approach is based on a novel four-points sets construction and selection scheme to embed watermark in the vertices of the 3D models. Experimental results show that the capacity and invisibility of the watermarked models can be monotonically adjusted. To the best of our knowledge, our novel method can provide much better watermark invisibility than other state-of-the-art watermarking method, while maintain large capacity and strong robustness against various typical attacks including cropping, RST transformations and local attacks. The low computational complexity of both the embedding and the extraction processes makes it suitable for copyright protection of 3D models.

Categories and Subject Descriptors

H.4.m [**Information Systems Applications**]: Miscellaneous; I.3.5 [**Computing Methodologies**]: COMPUTER GRAPHICS—*Computational Geometry and Object Modeling*

General Terms

Algorithms, Security

Keywords

3D model watermarking, copyright protection, four-points set.

1. INTRODUCTION

With the widespread use of 3D models in various applications such as digital archives, visualization, entertainment, 3D gaming, and virtual reality, 3D watermarking for protecting the intellectual property rights and certificating the authentication of 3D models has been widely researched in recent years.

Existing watermarking methods are classified according to several criteria. Based on the purpose of a watermarking method, there are (semi-)fragile watermarking methods [4, 8, 9, 14, 21] used for model authentication, and robust watermarking methods [2, 3, 5, 7, 12, 13, 15, 16, 17, 18, 19, 22, 23, 1] used for copyright protection. Based on whether an extraction process only needs the private key or not, there are blind [5, 7, 13, 16, 17, 23, 1] and non-blind [2, 3, 12, 15, 18, 19, 22] watermarking methods. Based on where watermarks are added, there are watermarking methods applied in spatial domain [2, 3, 7, 13, 16, 17, 23, 1] and transform domain [5, 12, 15, 18, 19, 22] respectively. According to the above criteria, our proposed watermarking method is robust and blind, with watermarks added in the spatial domain.

For the purpose of comparison, researchers usually evaluate the performance of a watermarking method in the following aspects:

1. Generality. A watermarking method should be able to embed watermarks in models of all different types with various geometry and topological features.
2. Capacity. A watermarking method should be able to embed watermarks that are large enough to meet application requirements.
3. Invisibility. Embedded watermarks should be imperceptible and a watermarked model should not have obvious visual artifacts.
4. Robustness. Watermarks should be able to be extracted from models that are badly distorted.
5. Efficiency. A watermarking method should be computationally efficient with a low memory requirement.

However, because of the topological complexity and irregularity of 3D models, there are few existing watermarking methods which can provide adjustable embedding capacity and watermark invisibility and also protect intellectual property of 3D models from various attacks efficiently. In this paper, we propose a highly adaptable capacity and invisibility watermarking method for 3D models with arbitrary topology. It can extract full watermarks successfully from

MM&Sec'10, September 9–10, 2010, Roma, Italy.

models damaged by typical attacks and partial watermarks even when the models are severely damaged.

1.1 Related Work

In this section, we briefly describe the existing 3D robust watermarking methods by dividing them into transform domain methods and spatial domain methods.

When watermarks are added in the transform domain, most watermarking methods embed a watermark by modifying the transform coefficients of direct frequency analysis [5, 18] or multi-resolution analysis [12, 19, 22] of an input model. Based on Laplacian frequency analysis, Ohbuchi et al. [18] propose a non-blind watermarking method by modulating the low and medium frequency coefficients additively; Cayre et al. [5] give a blind watermarking method by quantizing the low and medium frequency coefficients. However, for watermarking methods based on Laplacian analysis, there are two well-known drawbacks: computational cost increases rapidly with mesh complexity and connectivity information is also needed in analysis procedure [20]. Using wavelet analysis, Kanai et al. [12] propose a non-blind watermarking method that modifies the ratio of the norm of a wavelet coefficient to the length of its supporting edge. Praun et al. [19] apply multi-resolution analysis described in [11] for a non-blind digital watermarking method. Based on the Burt-Adelson pyramid decomposition [10] of multi-resolution analysis, Yin et al. [22] propose a robust, but non-blind watermarking algorithm. Besides direct frequency analysis and multi-resolution analysis, by converting an original mesh model into the spherical parameterization domain, Li et al. [15] report a watermarking method that can handle various attacks using informed detection.

When watermarks are embedded in the spatial domain, most watermarking algorithms change the geometry of an input model. Tetrahedral volume ratio(TVR), one of the three watermarking methods proposed by Ohbuchi et al. in [16] and [17], is the first one that can resist affine transformations. TVR also uses affine invariants defined as the ratios of volumes of tetrahedrons generated of three "neighbored" triangles along a sequence of triangles. However, TVR is designed for triangular meshes only and can not be used for non-manifold models. In [2], Beneden describes a non-blind watermarking method that can resist simplification attack by modifying the normal distribution. Similar to [2], Cho et al. present two blind watermarking methods using the distribution of vertex norms in [7]: to shift the mean value of the distribution and to change the variance respectively. These two methods achieve robustness against many attacks by sacrificing embedding capacity. However, they are not applicable to small models and are vulnerable to cropping attacks and affine transformations. In [3], in order to achieve robustness against affine transformations and simplifications, a combination of three methods, vertex flood algorithm(VFA), affine invariant embedding(AIE) and normal bin encoding(NBE), is proposed by Benedens and Busch. However, this combined method is not completely blind since some information produced by the original model must be provided in the extracting process. In [23], Zefieiou et al. describe two methods based on principal component analysis. Although these two methods are blind and can survive similar transformations, they are vulnerable to cropping attacks and non-uniform transformations due to their dependence on the centroid of an input model. By embedding a given watermark into the grouped clusters, which are formed using a nearest neighbor heuristic, P. Agarwal and B. Prabhakaran in [1] proposed a blind watermarking method that is robust against uniform transformation and localized attacks. Based on the principle of moment-preserving [6], Kuo et al. present a blind watermarking method in [13] that modifies vertices on the creases and corners of a triangular mesh. However, this method can only be applicable to triangular meshes.

Compared to spatial domain watermarking methods, although transform domain watermarking methods usually obtain good robustness against signal processing attacks, they often require a higher computational cost and extra information in watermark extraction. This is not favorable to applications where speed and efficiency are required (for example, 3D gaming over the Internet). In this paper, we propose a spatial domain watermarking method which achieves large capacity, great invisibility, strong robustness and low computational cost for copyright protection of 3D models.

1.2 Contributions and Overview

In this paper, we present a novel and efficient watermarking method for 3D models with arbitrary topology. Our approach is based on similarity transformation invariants defined as the length ratios of two segments of a diagonal intersected by the other one in a projected coplanar convex quadrilateral. For each vertex in an input model, we calculate its similarity transformation invariant length ratios in a carefully selected coplanar quadrilateral constructed by a four-points set within a local neighborhood of vertices. By slightly changing these ratios while keeping the quadrilateral coplanar, we embed pieces of a watermark (chopped into pieces beforehand) into the model. Watermark pieces are indexed and embedded multiple times. When a watermark is extracted, the same four-points set for each vertex is also selected as in the embedding process. Given these four-points sets, we calculate the same similarity transformation invariant length ratios, extract indices and watermark pieces accordingly, and reconstruct the entire watermark by majority voting of watermark pieces.

Our proposed method has the following features:

- **Topological Generality.** Compared to other watermarking algorithms, our approach can handle 3D models with any topology due to the fact that in general, a four-points set can always be obtained from a local neighborhood of vertices, no matter how complex an input model is.

- **Tunable Capacity.** In our proposed method, a watermark is chopped into pieces, and the length of each piece can be adjusted according to application requirements. The longer each watermark piece, the larger embedding capacity is.

- **Adjustable Invisibility.** Watermark pieces can be placed at different places of a length ratio such that a tradeoff between invisibility and robustness can be achieved.

- **Strong Robustness.** Models watermarked with our proposed method provide strong robustness against various attacks, since the proposed length ratios are similarity transformation invariants, watermark pieces

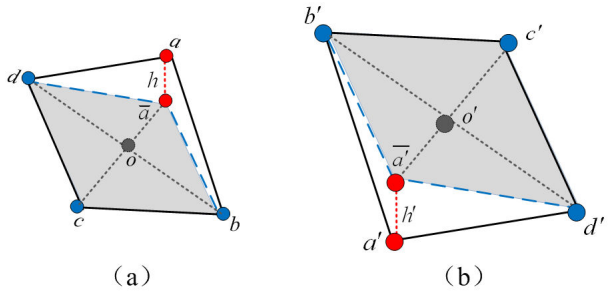


Figure 1: Projected length ratios are preserved under any similarity transformations.

are locally indexed and four-points sets are selected independently.

- **Computational Efficiency.** Our proposed method is quite simple for both the embedding and the extraction process, where a low computational cost is incurred.

In the following Section, we introduce the proposed similarity transformation invariant and describe its construction procedure for 3D models. In Section 3, we present the embedding and extraction process of our proposed method. Computational complexity and embedding capacity of the proposed method are discussed in Section 4. In Section 5, we provide experimental results and conclude our work in Section 6. Future work is discussed in Section 7.

2. SIMILARITY-TRANSFORMATION INVARIANTS

2.1 The Concept of Similarity-Transformation Invariants

Our definition of similarity-transformation invariants can be illustrated in Fig. 1. Let a, b, c, d be four points in three-dimension, where any three points are not collinear. Then $\bar{a}, b, c, d$ are four coplanar points, where $\bar{a}$ is the projected point from a to plane Δbcd (Fig. 1a). The diagonals of $\bar{a}c$ and bd meet at point o as illustrated in Fig. 1a. Let r_1 be the ratio of $\bar{a}o$ and $\bar{a}c$ and r_2 be bo/bd. Then r_1 and r_2 are preserved under any similarity transformations. Let a', b', c', d' and $\bar{a}'$ be the corresponding five points after any similarity transformations of $a, b, c, d, \bar{a}$, let $\bar{a}'c'$ and $b'd'$ meet at point o', $r_1' = \bar{a}'o'/\bar{a}'c'$ and $r_2' = b'o'/b'd'$. Then $\bar{a}'$ is the projection point from a' to plane $\Delta b'c'd'$ (as seen in Fig. 1b) and $r_1 = r_1'$ and $r_2 = r_2'$.

2.2 Construct Similarity-Transformation Invariants in 3D Models

A 3D model is comprised of a set of vertices V and a set of edges E between these vertices. Let v_i denote the i^{th} vertex. We define the $k-ring$ neighbors of v_i as $N_{v_i}^k = N_{v_i}^{k-1} \cup \{v_j | \exists v_l \in N_{v_i}^{k-1} \cap (v_j, v_l) \in E\}$, where $k > 0$. When $k = 0$, $N_{v_i}^0 = v_i$. The larger k is, the larger $N_{v_i}^k$. Since four-point sets are selected in $N_{v_i}^k$. A larger $N_{v_i}^k$ provides more candidates for four-point sets selection with a much higher computational cost. However, from various experiments, we observe that a larger local neighborhood has a little contribution to increasing embedding capacity and almost no benefit to improving watermark invisibility and efficiency. Therefore, we constantly keep k to be 1 throughout this paper. For convenience, we use $N(v_i)$ instead of $N_{v_i}^1$ in the rest of this paper.

In our watermarking method, we employ the Similarity transformations invariant ratios described in Section 2.1 to embed watermarks for 3D models. In order to obtain length ratios, four-point sets have to be selected for vertices in an input model. Given $N(vi)$ of v_i and their sequence (*i*.e., the vertices indexes of the input model), let n_i be the number of vertices in $N(vi)$, then the total number of all four-point sets in $N(vi)$ is $C_{n_i}^4$. Note that n_i should be no less than 4 in most cases. For a four-point set a, b, c, d in $N(vi)$, there are four projection cases as shown in Fig. 2(b)-(e). Let $h_{\Delta bcd}^a$, $h_{\Delta acd}^b$, $h_{\Delta abd}^c$ and $h_{\Delta abc}^d$ be the corresponding projection distances. Then, the total number of all the projected quadrilaterals for v_i is $4 \times C_{n_i}^4$ and let H_{v_i} be the set of all projection distances. Our selection of the four-point set of v_i is very simple. We generate all these projected quadrilaterals one after another. And Given the $4 \times C_{n_i}^4$ quadrilaterals and H_{v_i}, we choose the convex quadrilateral projected by four points with the minimum distance (i.e. $h_{\Delta abe}^c$ in Fig. 2(f)). Then $\{a, b, c, e\}$ is the set we select for v_i.

3. WATERMARKING PROCESS FOR A 3D MODEL

After describing the applied similarity transformation invariant ratios and their construction procedures, we now illustrate the proposed watermarking method in detail.

3.1 Watermark Processing

A watermark can be produced by cryptographic hash functions or other transformations. Due to the fact that a watermark can always be expressed by a string of 0s and 1s, we address watermark sequences composed of 0s and 1s only in this paper. Given a string of 0s and 1s, we divide the octal sequence into sequential groups, each of which is identified by a unique index. Let w_i be the i^{th} group and (i, w_i) be the i^{th} watermark piece. Let W denote the set of all watermark pieces, then $W = \{(1, w_1), (2, w_2), \ldots, (n, w_n)\}$, where $i = 1, 2, \ldots, n$.

3.2 Embedding Watermark

In our proposed watermarking method, the embedding procedure consists of two major steps: four-points sets construction and selection (for details, refer to Section 2.2), and watermark pieces embedding. Watermark pieces are embedded into length ratios by slightly changing their values while keeping the quadrilaterals coplanar. Details of length ratio modification are given as follow.

Given a four-points set $\{a, b, c, d\}$ and a watermark piece (i, w_i), the length ratios to be used for watermark embedding are r_1, r_2 as defined in Section 2.1. Let L and H be the distances from decimal point to the low notion and the high notion respectively (as shown in Fig. 3). A watermark piece w_i and its individual index i are embedded into r_2 and r_1 by replacing their original decimal values from L to H with w_i and i respectively.

Suppose the corresponding convex quadrilateral of four-points set $\{a, b, c, d\}$ is $a, b, \bar{c}, d$ as shown in Fig. 4a, there are four candidate length ratios to be chosen for watermark embedding, i.e. $ao/a\bar{c}$, bo/bd, $\bar{c}o/a\bar{c}$ and do/bd. In order to

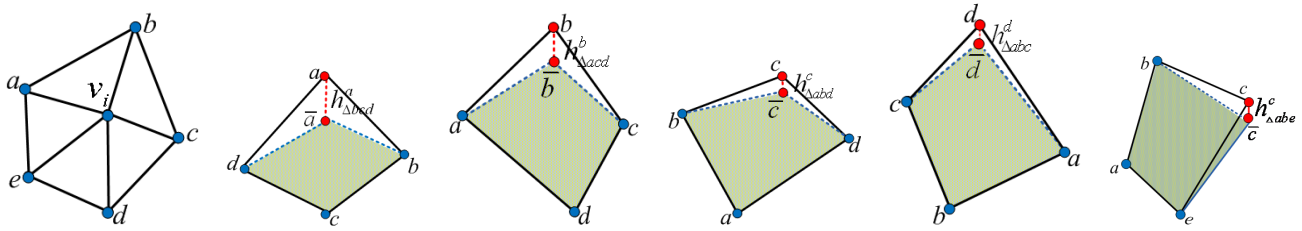


Figure 2: An example of four-points set construction and selection. (a) Neighborhood of v_i. (b) a is projected to the plane Δbcd. (c) b is projected to the plane Δacd. (d) c is projected to the plane Δabd. (e) d is projected to the plane Δabc. (f) Selected four-points set and for v_i.

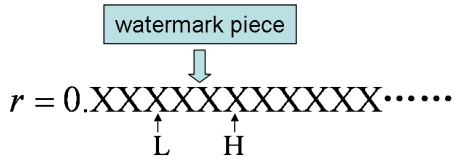


Figure 3: Replace the decimal notions between L and H with a watermark piece.

identify and differentiate r_1 and r_2 without any knowledge of vertex order, r_1 and r_2 are chosen to satisfy the following relationship:

$$r_1 < r_2 < 0.5. \tag{1}$$

In case any of those four length ratios equals to 0.5, we move the corresponding vertex outwards a little bit, following the direction of the diagonal it resides on. An example is shown in Fig. 4(b). Given the length ratios of different diagonals, if the decimal notion right before L is the same, we treat them as equal ratios (e.g. $ao/a\bar{c} = bo/bd$). In this case, we subtract 1 from the $\{L-1\}^{th}$ decimal notion of either $ao/a\bar{c}$ or bo/bd such that they are no longer equal. After these adjustment, it's guaranteed that there are two length ratios both of which are less than 0.5 and one is smaller than the other. Let the smaller length ratio be r_1 and the other be r_2. After a watermark piece is embedded, r_1 and r_2 are changed into r_1' and r_2' as illustrated in Fig. 4(c). Note that r_1' and r_2' still satisfy the relationship of $r_1' < r_2'$. This is because the decimal notions before L of r_1' and r_2' are not affected by the embedding of watermark piece. Since the change of r_1 and r_2 are done by adjusting the coordinates of a and b along the direction of diagonals they reside on, the coordinate of o keeps constant, and the change of r_1 and r_2 are mutual independent. Let a' and b' be the new vertices after adjusting a and b, respectively, then a' and b' are calculated as follow:

$$\begin{aligned} a' &= (o - \bar{c} \times r_1')/(1 - r_1'), \\ b' &= (o - d \times r_2')/(1 - r_2'). \end{aligned} \tag{2}$$

The distance of $||a' - a||$ between a' and a is calculated as

$$||a' - a|| = \frac{||r_1 - r_1'||}{1 - r_1'} ||\bar{c} - a||, \tag{3}$$

where $||\bar{c} - a||$ is the length of $a\bar{c}$ and $1 - r_1' > 0.5$.

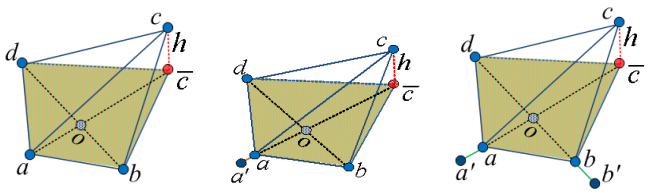


Figure 4: Embed watermark pieces into length ratios. (a) Four-points set and its projected convex quadrilateral. (b) Adjust the values of ratios $ao/a\bar{c}$ and $\bar{c}o/a\bar{c}$ by moving a outward a bit. (c) Modified vertices to change length ratios after embedding watermark piece i, w_i.

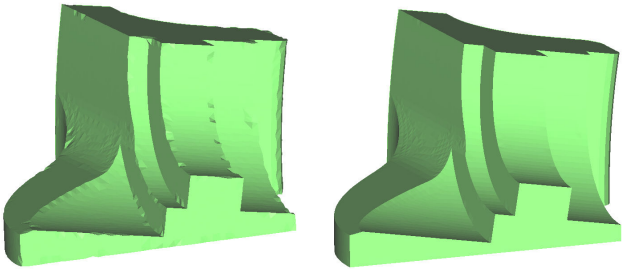


Figure 5: The impact of L on the visual effect of the Fandisk model. (a)Visible artifact is observed when $L = 2$. (b)No visible artifact is shown when $L = 3$.

Given L and H, we have

$$||a' - a|| \approx 2 \times P \times ||\bar{c} - a||, \tag{4}$$

where $P = (10^{-L}x_l + 10^{-L-1}x_{l+1} + \cdots + 10^{-H+1}x_{h-1} + 10^{-H}x_h)$. $x_l, x_{l+1}, \cdots x_{h-1}, x_h$ are the corresponding decimal notions of $||r_1 - r_1'||$.

From (4), we can see that the invisibility of our proposed method mainly depends on the value of L. It is clear that as the value of L decreases, the distance of $||a' - a||$ increases. That is, as watermark pieces are placed closer to decimal point, more distortion can be observed in a watermarked model. This effect is demonstrated by Fig. 5, which shows two watermarked Fandisk models with $L = 2$ and $L = 3$, respectively.

As to the robustness to noise, the performance of our proposed method is affected by not only the value of L but also the value of H. Given the value of H, when the strength of

attacking noise is above $10^{-H} \times ||\bar{c} - a||$, extracted watermarks start to show errors. In general, as H gets smaller, the robustness to noise increases. A detailed discussion of L and H selection is performed in Section 5.

The pseudo code for embedding a watermark is demonstrated here:

1. Set the tags of all the vertices in V as "un-used" and initialize the set of four-points sets Ω as $\emptyset$.
2. For each vertex v_i in V,
   (a) Construct its local neighborhood of $N(v_i)$. Note that if the tags of some vertices in $N(v_i)$ are "used", we discard them from $N(v_i)$.
   (b) Construct all coplanar quadrilaterals in $N(v_i)$ using the method described in Section 2.2.
   (c) Select the four-points set as described in Section 2.2 and set the tags of the four points as "used" and add this four-points set to Ω.
3. Embed a watermark piece into every four-points set in Ω employing the method described above.

Note that multiple copies of a watermark are embedded into a 3D model in our proposed method. The purpose is to enhance the robustness of a watermarked model against various attacks.

3.3 Extracting Watermark

Similar to the embedding procedure, the extraction process can be described with the following steps:

1. Set the tags of all the vertices as "un-used" and initialize the set of watermark pieces W as $\emptyset$.
2. For each vertex v_i in V,
   (a) Construct its local neighborhood of $N(v_i)$. Same as the embedding procedure, if the tags of some vertices in $N(v_i)$ are "used", we discard them from $N(v_i)$.
   (b) Select the four-points set as described in Section 2.2 and set the tags of the four points as "used".
   (c) Extract a watermark piece with its corresponding index from the length ratios of the four-points set and add it to W. Note that the selected length ratios here should satisfy (1). Otherwise, we simply believe this four-points set is severely damaged and discard it.
3. Sort the extracted w_i according to i, and then translate the set of watermark pieces W into original watermark by majority voting.

The watermark extraction procedure of our proposed method is blind and simple, where no extra information is needed and its computational cost is low.

Table 1: The Number of Four-Points Sets Collected in Our Experiments and the Capacity for Five Models When $L = 2, H = 4$

Model	Fandisk	Dragon	Maple	Buddha	Bunny
Ω	1516	4943	6008	6998	7541
Capacity	13644	44487	54072	62982	67869

4. ALGORITHM ANALYSIS

4.1 Time Complexity

Considering a model with V vertices, the most computationally expensive operations of the proposed method are Local Neighborhood Construction ($O(3V)$), Four-Point Set Selection($O(KV)$), and Watermark Embedding and Extracting ($O(PV)$), where K and P are both constants. Therefore, the proposed method has a computational complexity of $O(3V) + O(KV) + O(PV) = O(V)$ altogether.

4.2 Embedding Capacity

Embedding capacity is the amount of data embedded for watermarking. However, in the proposed watermarking method, indices of watermark pieces are also embedded in length ratio r_1. Therefore, when embedding capacity is considered, we only count the amount of watermark pieces embedded in r_2 as the real watermarking data. Embedding capacity of the proposed method is calculated in (5).

$$C = (H - L + 1) \times \Omega \tag{5}$$

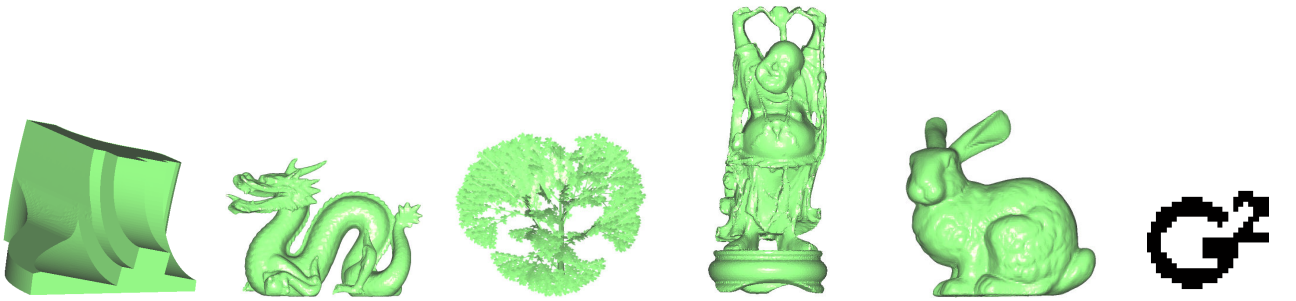
where C denotes the pure embedding capacity. Based on this calculation, we can easily say that the embedding capacity of our proposed method purely depends on the total number of selected four-points sets (denoted by Ω) and the length of embedding positions in similarity-transformation invariant length ratios (denoted by $H - L + 1$). Table 1 lists the number of four-points sets for five models used in our experiments. (5) also tells us that as $H - L$ increases, C increases monotonically. Therefore, we can fine tune the capacity to the special requirements.

5. EXPERIMENTS AND ANALYSIS

In this section, we conduct a series of experiments to test the invisibility and the robustness of the proposed watermarking algorithm. As shown in Fig. 6(a)-(e), four manifold models (*i*.e., Fandisk, Dragon, Buddha and Bunny) and one non-manifold model (*i*.e., Maple-tree) are used in our experiments. As shown in Fig. 6(f), the watermark image used in our experiments is 24×24 pixels (576 Bits). If not otherwise specified, the parameters for the tests of the robustness to cropping, similarity transformations, and noise attacks are set as $H = 3$ and L=2.

5.1 Watermark Invisibility

Although there is no standardized metric for the measurement of invisibility, two types of approaches have usually been adopted to evaluate the watermark invisibility of a 3D watermarking algorithm - subjective perception and objective measurement of geometry distortion.



(a)6475 vertices 12946 faces | (b)22998 vertices 47794 faces | (c)45499 vertices 43530 faces | (d)32328 vertices 67240 faces | (e)35947 vertices 69451 faces | (f)24 × 24 pixels

Figure 6: Original models and watermark. (a) Fandisk. (b) Dragon. (c) Maple-tree. (d) Buddha. (e) Bunny. (f) Watermark image.

5.1.1 *Subjective Perception*

In order to demonstrate the watermark invisibility of the proposed 3D watermarking algorithm, we show in Fig. 7 the visual renderings of various 3D models at different values of L, where Fig. 7(a) and Fig. 7(b)-(d) give the models before and after the watermarking, respectively. With the increase of L, the artificial effects in watermarked models are gradually imperceptible. Actually, even when $L = 2$, we can hardly perceive any visual difference between the models (Dragon, Maple-tree, Buddha, and Bunny) before and after watermarking. However, visual effect is obvious for Fandisk model when $L = 2$, and the reason for this is explained in Section 5.1.2.

5.1.2 *Geometry Distortion Measurement*

In our experiments, we employ the commonly used signal-to-noise ratio (SNR)as means of measuring the geometrical difference between the watermarked and original models. In general, the larger the SNR, the better is the invisibility.

We perform a series of tests on the Fandisk, Dragon, Maple-tree, Buddha, and Bunny models to observe the impact of L and H on the SNR, and illustrate the results in Fig. 8. Fig. 8(a) illustrates that given $H = L + 2$, as L increases, the SNR increases almost monotonically. It's also shown that the values of SNR have a large gap between the Fandisk and the other four models. This is mainly due to the fact that the average length of embedding-cell diagonals of the Fandisk model is larger than those of the other models. The corresponding visual effect of the five models at different L are shown in Fig. 7. Similarly, Fig. 8(b) shows that for a given L, as H increases, the SNR decreases accordingly. When H is larger than 6, this change is much less obvious. This phenomenon can be explained by (4).

Compared to other methods in the literature, our proposed algorithm can achieve super good watermark invisibility while maintaining high capacity as shown in Table 1. Because of this attractive property, our proposed watermarking algorithm is suitable for common applications that have high requirements on the fidelity of watermarked 3D models.

5.2 Robustness

In order to demonstrate the robustness of the proposed method, in our experiments, we use various types of attacks including geometrical transformations (*e.g.*, similarity transformation), topological transformations (*e.g.*, cropping) and signal processing algorithms (*e.g.*, noising). We employ BER [12, 13, 21], the ratio of the incorrectly extracted bits of a watermark to its total bits, as the metric to evaluate the robustness of our proposed watermarking algorithm.

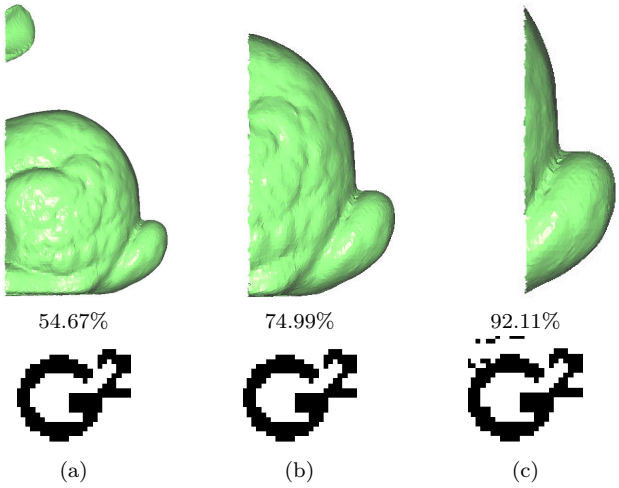


Figure 9: Watermarks extracted from Bunny at different cropping ratios.

5.2.1 *Robustness against Cropping*

Since watermark pieces are embedded into mutual independent four-points sets and we embed multiple copies of the same watermark into the model, the watermark can survive much more serious cropping attacks than any other existing watermarking methods.

In our experiments, for each cropped model, the corresponding cropping ratio is measured by counting the percentage of cut vertices with respect to the total number of vertices in the original model. A few cropped Bunny models are shown in Fig. 9 which demonstrates that, even when the cropping ratio goes as high as 92.11%, our algorithm can still extract a quite distinguishable image of the embedded watermark.

In the "C-BER" column of Table 2 lists the BERs of the extracted watermark images at different cropping ratios for the five tested models. From this table, we observes that as the cropping ratio gets higher, the BER rises simultaneously.

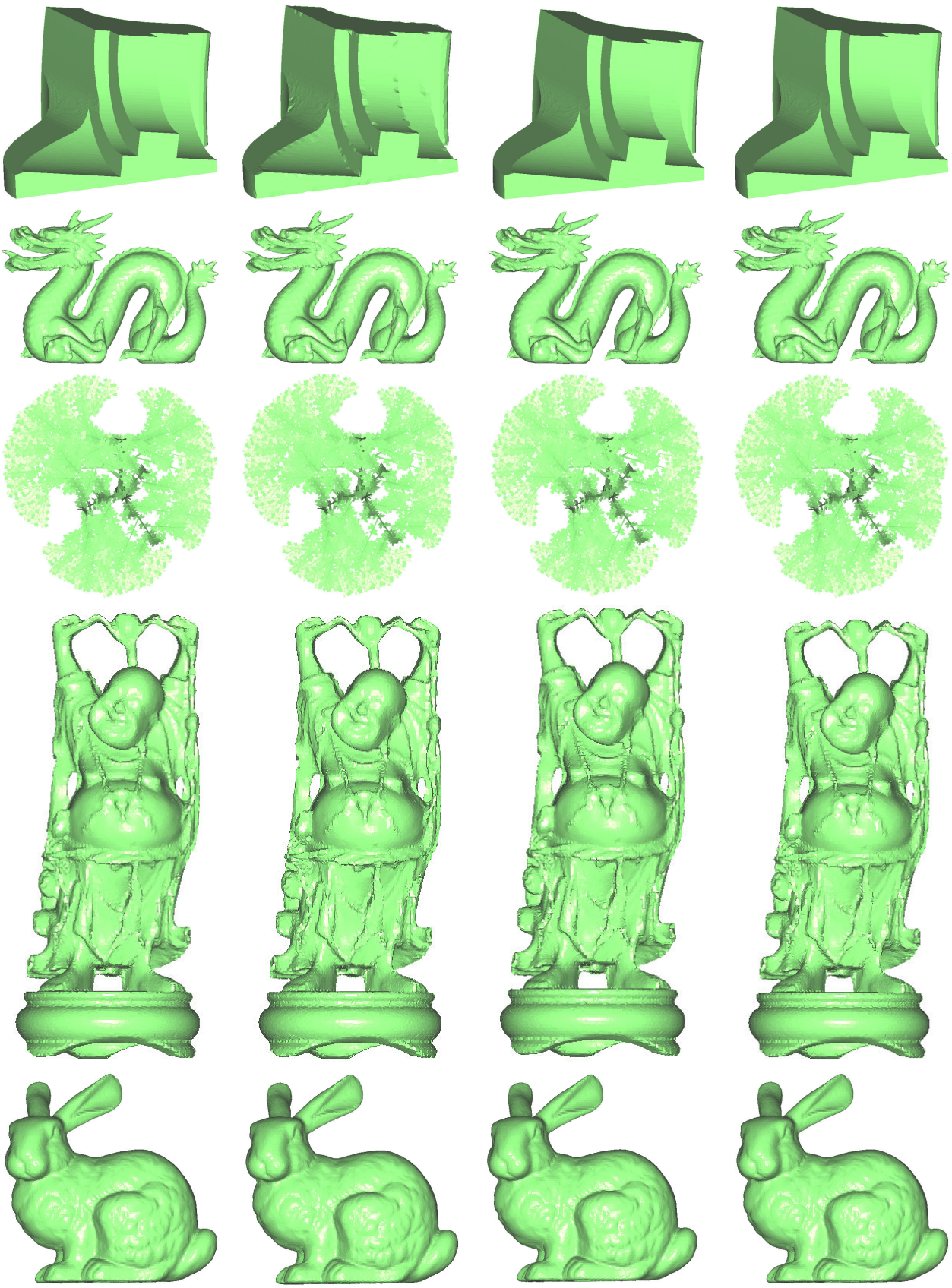


Figure 7: Visual effects of the watermarked models at different L while $H = L + 2$. (a) $L = 2, H = 4$. (b) $L = 3, H = 5$. (c) $L = 4, H = 6$. (d) $L = 5, H = 7$.

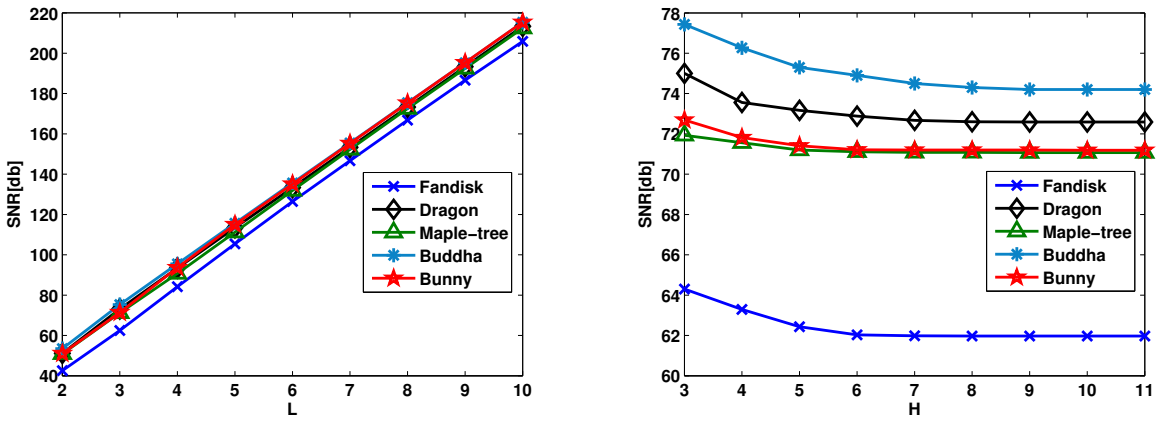


Figure 8: Geometry distortion comparison. (a) Variation of SNR as L increases (with $H = L+2$).(b) Variation of SNR as H increases (with $L = 3$).

Table 2: The BERs of the Tested Models at Different Cropping Ratios and Noise Strengths

Model	Cropping	C-BER	Noise	N-BER
Fandisk	31.78%	0.00%	10^{-5}	11.06%
	67.03%	1.38%	10^{-4}	32.32%
	79.29%	7.69%	10^{-3}	48.96%
Dragon	51.21%	0.00%	10^{-5}	0.00%
	68.66%	0.00%	10^{-4}	18.31%
	92.36%	11.81%	10^{-3}	40.13%
Maple-tree	48.16%	0.00%	10^{-5}	0.00%
	72.15%	0.00%	10^{-4}	19.41%
	90.81%	0.52%	10^{-3}	38.89%
Buddha	33.18%	0.00%	10^{-5}	0.00%
	71.36%	0.00%	10^{-4}	20.75%
	88.81%	5.20%	10^{-3}	42.25%
Bunny	54.67%	0.00%	10^{-5}	0.00%
	74.99%	0.00%	10^{-4}	20.34%
	92.11%	2.77%	10^{-3}	39.07%

However, even if the cropping ratio is large enough to be over 80%, the BER still keeps low (around 10%).

5.2.2 *Robustness against Similarity Transformations*

Since the proposed algorithm employs the similarity transformation invariants, the extracted watermark is preserved under any similarity transformations involving translation, rotation, uniform scaling, and their combinations as is shown in Fig. 10.

5.2.3 *Robustness against Noise*

In our experiments, random uniform noise distributed in the interval of $[-a, a]$, where a is the strength of noise, is added to the Cartesian coordinates of the vertices in an input model. Here, we set $L = 3, H = 4$ for the Fandisk model

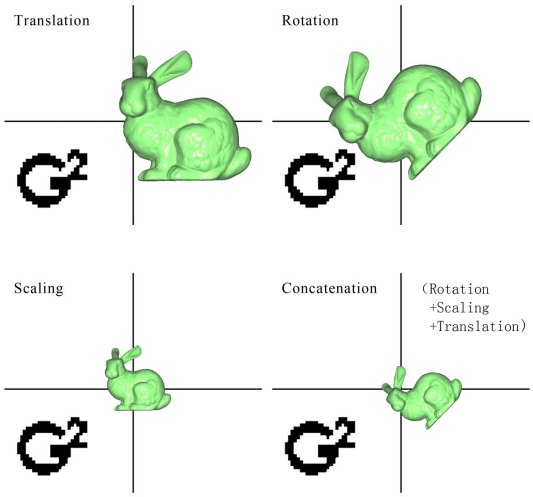


Figure 10: Watermark images can be completely extracted from watermarked models after several similarity transformations.

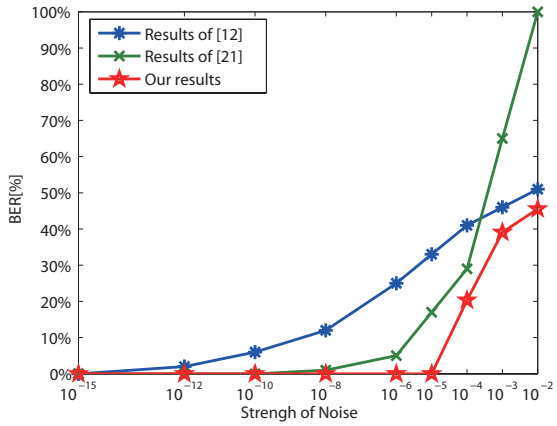


Figure 11: Comparison of robustness against noise with [12] and [21].

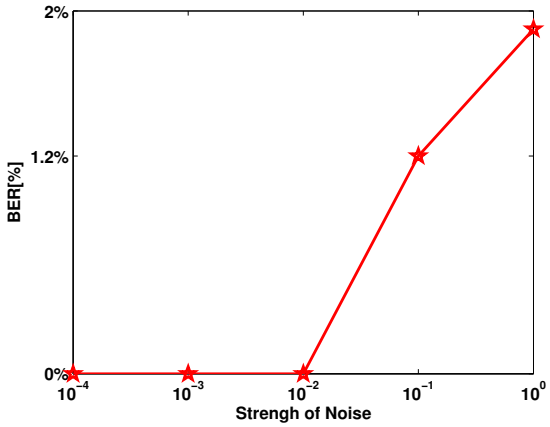


Figure 12: The BERs for different strengths of noise when 50% vertices are attacked.

so as to tradeoff the visual effect of watermarked model and the robustness against noise.

Using the same watermark and the Bunny model, we compare the robustness against noise of our proposed algorithm to [12] and [21] and illustrate the results in Fig. 11. In Fig. 11, the horizontal axis represents the noise strength, and the vertical axis represents the BER results after the previously described noise attack is applied to all the vertices. As shown in Fig. 11, the wavelet-based watermarking method described in [12](the blue curve) is sensitive to noise, whose watermark is not intact even when the noise strength is as weak as 10^{-13}. While in our proposed method, the BER starts to show only when the noise strength is larger than 10^{-5}. The integral-based method described in [21] (the green curve) is relatively less sensitive to noise than the wavelet-based method, but more vulnerable to noise than ours. Compared to [12, 21], our proposed method provides a superior robustness against noise with a much lower BER at given strength of noise.

Experimental results for the five test models under three different noise strengths are given in column "N-BER" of Table 2. From the table we can see that our method is fairly robust to noise attacks under a strength of 10^{-4}, but the quality of the embedded watermark starts to devastate for a noise strength of 10^{-3} or higher. This is because decimal values indicated by L in similarity transformation invariant length ratios are affected by vertex displacement caused by additive noise. Note that, the performance for the Fandisk model is not as good as that for the other models, since H is set to be 4 for the Fandisk model which is more sensitive to noise. However, if we embed watermark pieces into binary notions of the length ratios, we can adjust parameters for the Fandisk more precisely for a comparable robustness against noise with the other four models.

We also test our proposed method when noise is applied to portions of original vertices only, and show the results for the Bunny model in Fig. 12. In this figure, the vertical axis represents the BER values corresponding to the situation where noise is applied to 50% randomly selected vertices from the original model. When the noise strength is less than 10^{-1}, the values of BER are zero because the extracted watermark image is the same to the original one. Although little disturbance starts to appear in the extracted watermark images when the noise strength gets stronger than 10^{-1}, the BER is still very low when the noise strength is as high as 10^{0}. The robustness against local noise attacks of our algorithm is very strong for the reason that watermark pieces are embedded in neighborhoods that are mutually independent.

6. CONCLUSIONS

In this paper, we propose a novel watermarking method which embeds/extracts watermarks blindly and robustly for 3D models with arbitrary topology, including manifold and non-manifold. This proposed method embeds watermarks in an input model's geometry by imperceptibly modifying its similarity transformation invariant length ratios. The proposed method not only provides highly flexible embedding capacity and watermark invisibility, but also is robust against various attacks including cropping, similarity transformations, noises and local attacks. Due to its simplicity (Four-points sets) and efficiency (with the computational complexity $O(V)$), the proposed watermarking method is suitable for copyright protection of 3D models.

7. FUTURE DISCUSSION

There are several ways to extend the current research. First, in our current implementation, four-points sets are used without any classification. We may improve the robustness against global noise by choosing four-points sets with longer diagonals. We may further increase watermark invisibility by selecting projection congruent four-point sets in the embedding process circumventing sharp edge and high curvature. Other interesting directions of future work include watermarking 3D models of continuous LODs and gigantic model watermarking.

8. ACKNOWLEDGEMENTS

This work is supported by National 863 High-Tech programme of China (2009AA01Z304), the National Natural Science Foundation of China (60933008čň60633030), National Research Foundation for the Doctoral Program of Higher Education of China (20070422098).

9. REFERENCES

[1] P. Agarwal and B. Prabhakaran. Robust blind watermarking of point sampled geometry. In *Proc. of the 9th Workshop on Multimedia & Security.*, Sep. 2007.

[2] O. Benedens. Geometry-based watermarking of 3d models. *IEEE Computer Graphics and Applications, special issue on image security*, 19(1):45–46, Jan./Feb. 1999.

[3] O. Benedens and C. Busch. Towards blind detection of robust watermarks in polygonal models. In *Proc. Eurographics '00*, pages C199–C208, Aug. 2000.

[4] F. Cayre, O. Deviller, F. Schmitt, and H. Maître. Watermarking 3d triangle meshed for authentication and integrity. Inria researchreport rr-5223, June 2004.

[5] F. Cayre, P. Rondao-Alface, F. Schmitt, B. Macqb, and H. Matîre. Application of spectral decomposition to compression and watermarking of 3d triangle mesh geometry. *Signal Processing*, 8(4):309–319, 2003.

[6] S. C. Cheng and T. L. Wu. Subpixel edge detection of color images by principal axis analysis and moment-preserving principle. *Pattern Recognition*, 38(4):527–537, 2005.

[7] J. W. Cho, R. Prost, and H. Y. Jung. An oblivious watermarking for 3d polygonal meshes using distribution of vertex norms. *IEEE Trans. Signal Processing*, 55(1):142–155, 2007.

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

[9] C. M. Chou and D. C. Tseng. Affine-transformation-invariant public fragile watermarking for 3d model authentication. *IEEE Computer Graphics and Applications*, 29:72–79, Mar./Apr. 2009.

[10] I. Guskov, W. Sweldens, and P. Schröder. Multiresolution signal processing for meshes. In *Proc. ACM SIGGRAPH'99*, pages 325–334, 1999.

[11] H. Hoppe. Progressive mesh. In *Proc. ACM SIGGRAPH'96*, pages 99–108, Aug. 1996.

[12] S. Kanai, H. Date, and T. Kishinami. Digital watermarking for 3d polygons using multiresolution wavelet decomposition. In *Proc. Sixth IFIP WG 5.2 Int'l Workshop Geometric Modeling*, pages 296–307, 1998.

[13] C. T. Kuo, S. C. Cheng, D. C. Wu, and C. C. Chang. A blind robust watermarking scheme for 3d triangular mesh models using 3d edge vertex detection. *Asian Journal of Health and Information Sciences*, 4(1):36–63, 2009.

[14] S. K. Lee and Y. S. Ho. A fragile watermarking scheme for three-dimensional polygonal models using triangle strips. *IEICE Trans. Comm.*, 87(9):2811–2815, 2004.

[15] L. Li, D. Zhang, Z. G. Pan, J. Shi, K. Zhou, and K. Ye. Watermarking 3d mesh by spherical parameterization. *Computers & Graphics*, 28(6):981–989, 2004.

[16] R. Ohbuchi, H. Masuda, and M. Aono. Watermarking three-dimensional polygonal models. In *Proc. Fifth ACM Int'l Conf. Multimedia (Multimedia '97)*, pages 261–272, 1997.

[17] R. Ohbuchi, H. Masuda, and M. Aono. Watermarking three-dimensional polygonal models through geometric and topological modifications. *IEEE J. Selected Areas in Comm.*, 16(4):551–560, 1998.

[18] R. Ohbuchi, A. Mukaiyama, and S. Takahashi. A frequency-domain approach to watermarking 3d shapes. In *Proc. Eurographics'02*, pages 373–382, 2002.

[19] E. Praun, H. Hoppe, and A. Finkelstein. Robust mesh watermarking. In *Proc. ACM SIGGRAPH'99*, pages 325–334, 1999.

[20] K. Wang, G. Lavou, F. Denis, and A. Baskurt. A comprehensive surevy on three dimensional mesh watermarking. *IEEE Trans. Multimedia*, 10(8):309–319, Dec. 2008.

[21] Y. P. Wang and S. M. Hu. A new watermarking mehthod for 3d models based on integral invariants. *IEEE Trans. Visualization and Computer Graphics*, 15(2):285–294, Mar./Apr. 2009.

[22] K. K. Yin, Z. G. Pan, J. Y. Shi, and D. Zhang. Robust mesh watermarking based on multiresolution processing. *Computers & Graphics*, 25(3):409–420, 2001.

[23] S. Zafeiriou, A. Tefas, and I. Pitas. Blind robust watermarking schemes for copyright protection of 3d mesh objects. *IEEE Trans. Visualization and Computer Graphics*, 11(5):596–607, Sep./Oct. 2005.