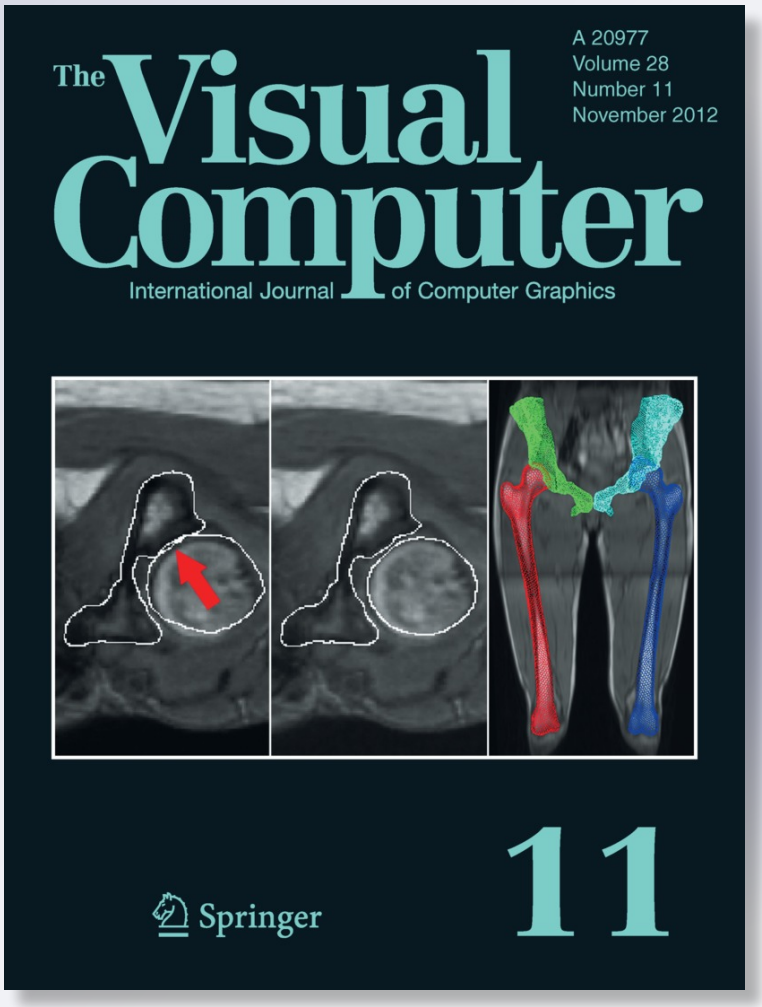
A robust confirmable watermarking algorithm for 3D mesh based on manifold harmonics analysis

Jinrong Wang, Jieqing Feng & Yongwei Miao

The Visual Computer
International Journal of Computer Graphics

ISSN 0178-2789
Volume 28
Number 11

Vis Comput (2012) 28:1049-1062
DOI 10.1007/s00371-011-0650-3



Springer

Your article is protected by copyright and all rights are held exclusively by Springer-Verlag. This e-offprint is for personal use only and shall not be self-archived in electronic repositories. If you wish to self-archive your work, please use the accepted author's version for posting to your own website or your institution's repository. You may further deposit the accepted author's version on a funder's repository at a funder's request, provided it is not made publicly available until 12 months after publication.

Springer

Author's personal copy

Vis Comput (2012) 28:1049–1062
DOI 10.1007/s00371-011-0650-3

ORIGINAL ARTICLE

A robust confirmable watermarking algorithm for 3D mesh based on manifold harmonics analysis

Jinrong Wang · Jieqing Feng · Yongwei Miao

Published online: 15 October 2011
© Springer-Verlag 2011

Abstract Owing to the manifold harmonics analysis, a robust non-blind spectral watermarking algorithm for a two-manifold mesh is presented, which can be confirmed by a trusted third party. Derived from the Laplace–Beltrami operator, a set of orthogonal manifold harmonics basis functions is first adopted to span the spectral space of the underlying three-dimensional (3D) mesh. The minimal number of the basis functions required in the proposed algorithm is also determined, which can effectively accelerate the spectrum computations. Then, to assert ownership and resist 3D mesh forging, a digital signature algorithm is adopted to sign the watermark in the embedding phase and to verify the signature in the extraction phase, which could optimize the robust non-blind spectral watermarking algorithm framework. To improve the robustness of the embedded watermark signature, the input 3D mesh will be segmented into patches. The watermark signature bits are embedded into the low-frequency spectral coefficients of all patches repeatedly and extracted with regard to the corresponding variations of their coefficients. Extensive experimental results demonstrate the efficiency, invisibility, and robustness of the proposed algorithm. Compared with existing watermarking algorithms, our algorithm exhibits better visual quality and is more robust to resist various geometric and connectivity attacks.

J. Wang · J. Feng (✉)
State Key Laboratory of Computer-Aided Design & Computer Graphics, Zhejiang University, Hangzhou 310058, P.R. China
e-mail: jqfeng@cad.zju.edu.cn

J. Wang
Hangzhou Institute of Service Engineering, Hangzhou Normal University, Hangzhou 310036, P.R. China

Y. Miao
College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, P.R. China

Keywords Non-blind watermarking · Manifold harmonics analysis · Spectral space · Public-key

1 Introduction

With the rapid development of acquisition facilities and processing techniques, three-dimensional (3D) models nowadays are widely applied to digital entertainment, film and television, 3D games, cultural heritage protection, etc. Meanwhile, the unauthorized duplication, modification, and spread of 3D models are becoming common. We are now facing the problem of protecting the copyright of 3D models, which is also an important topic in computer graphics and multimedia. In the cryptography field, digital signature technique is adopted to assert message ownership [1]. However, because the 3D model representation is quite different from the text document, it is not trivial work to extend the digital signature technique to 3D model copyright protection [2]. Therefore, as an alternative solution, digital watermarking techniques for 3D models based on the information hiding theory are proposed accordingly, which provide another effective means of copyright protection and ownership assertion [3, 4].

Digital watermarking hides secret message (called watermark) into a digital image, audio, video, or 3D model for copyright protection and ownership assertion. Recently, many watermarking algorithms have been proposed for 3D meshes [3]. Due to their different purposes and applications, watermarking algorithms can be classified into robust ones and fragile ones. A robust watermarking algorithm is usually designed for ownership claim, whereas a fragile one is designed for integrity verification [5–8]. According to their different extraction strategies, watermarking algorithms can

Author's personal copy

also be classified into non-blind ones and blind ones depending on whether they require the original 3D mesh or not.

However, there is still no standard benchmark to assess different 3D mesh watermarking algorithms. For robust watermarking algorithms, it is widely recognized that the following four aspects should be considered in general. *Invisibility*: The embedded watermark should be almost invisible and the visual quality of watermarked mesh should be altered as little as possible; *Robustness*: Enough bits of the embedded watermark can be extracted correctly after the mesh undergoes geometric processing; *Capacity*: The amount of embedded watermark should be large enough to introduce cryptograph technique for enhancing its security; *Computational efficiency*: A large-scale 3D mesh can be watermarked within a reasonable time.

In this paper, we proposed a robust non-blind confirmable spectral watermarking algorithm for a two-manifold mesh based on the manifold harmonics analysis, in which a digital signature algorithm is introduced. The main contributions of the proposed algorithm include the following:

- To assert ownership and resist 3D mesh forging, a digital signature algorithm is incorporated explicitly into both the watermark embedding and extraction phases, which could optimize the robust non-blind spectral watermarking framework.
- Without sacrificing of visual quality and robustness of the 3D watermarked mesh, we give the theoretical analysis of the minimal number of manifold harmonics basis functions required in the proposed algorithm. This can greatly facilitate the spectral analysis and watermark embedding of a large-scale 3D mesh with millions of vertices.
- The watermark signature bits are embedded in an absolutely embedding manner and extracted with regard to the corresponding variations of their coefficients in the proposed algorithm. Quite extensive experimental results show that the proposed algorithm is robust and can resist various geometric and connectivity attacks.

The remainder of the paper is organized as follows. Some previous works are reviewed in Sect. 2. In Sect. 3, the manifold harmonics analysis for 3D mesh is introduced briefly. In Sect. 4, the proposed algorithm is described in detail and automatic selection of the number of basis is given. In Sect. 5, the implementation results and the detailed comparisons with existing watermarking algorithms are given. Finally, conclusions are drawn and future research are indicated in Sect. 6.

2 Previous works

After the first 3D mesh watermarking algorithm was proposed by Ohbuchi et al. [9], various watermarking algorithms have been proposed for 3D meshes. These algorithms can be classified into spatial domain ones and spectral domain ones. A spatial domain algorithm embeds a watermark into a mesh by modifying its geometry information or topology connectivity information directly, such as vertex position and connectivity [9–12], normals [13], and local moments [14]. The spatial domain algorithm is simple, efficient and has high capacity. However, it is not robust enough to resist various attacks, especially for mesh simplification.

A spectral domain algorithm embeds a watermark into its low-frequency spectral coefficients of a 3D mesh. It exhibits better robustness than the spatial domain algorithm in general. Kanai et al. [15] proposed a blind watermarking algorithm based on wavelet transform and multi-resolution representation of 3D mesh. They modified the ratio of the norm of wavelet coefficient vector to the length of its support edge, which is invariant to the affine transformation. The watermarked mesh can resist the attacks of affine transformation, random noise, etc. However, the algorithm strictly requires the underlying 3D mesh with one to four subdivision connectivities. Praun et al. [16] presented a robust non-blind watermarking algorithm via multi-resolution analysis. It works for 3D meshes with arbitrary topology connectivity. Alternatively, Yin et al. [17] first performed a multi-resolution decomposition of a 3D mesh and then embedded the watermark into the low resolution components, which correspond to the global shape information.

Direct spectral analysis of a 3D mesh provides another kind of spectral domain [18]. Based on the Laplace basis functions, Ohbuchi et al. [19, 20] proposed a robust non-blind spectral watermarking algorithm (abbreviated as LBFs in our paper). They segmented a 3D mesh into patches and embedded the watermark into the low-frequency spectral coefficients of each patch, which can resist a wide class of attacks. However, because its basis functions correspond to the eigenvectors of a combinational Laplacian matrix, the visual quality of a watermarked mesh suffers from topology-based basis functions, especially for a 3D mesh with non-regular tessellation. The computational cost of the basis functions is also expensive. Wu et al. [21] proposed a robust non-blind spectral watermarking algorithm based on the radial basis functions (abbreviated as RBFs in our paper). They adopted mesh reconstruction difference to improve the visual quality of the watermarked mesh. Since only a small number of radial basis functions are adopted and the orthogonal basis functions are computed via singular value decomposition of a small-scale matrix, the RBFs can efficiently handle large-scale meshes even with more than 10^6 vertices. Despite the improvement in computational efficiency, the invisibility, capacity, and robustness are sacrificed to some extent due to its watermark embedding manner. Wang et al. [22] presented an improved 3D mesh watermarking algorithm based on radial basis functions. With an optimized center point set determination method and new

Author's personal copy

watermark embedding manner, the algorithm improves the visual quality of the watermarked mesh.

On the other hand, some interested blind spectral watermarking algorithms have been proposed in recent years. Liu et al. [23] presented a robust blind watermarking algorithm for two-manifold meshes. They modified the low-frequency amplitudes in an iterative embedding manner to embed the watermark bits into the mesh. Wang et al. [24] also proposed a blind watermarking algorithm using the manifold harmonics analysis. They embedded a 16-bit watermark into the amplitudes of the low-frequency coefficients using the 2-symbol scalar Costa scheme. The above two algorithms can resist similarity transformation, random noise, simplification and smoothing attacks. However, they can not resist cropping attacks or any combination attacks that include cropping. Moreover, these two algorithms are of a low bit-capacity, for example, only 5 bits in [23] and 16 bits in [24]. With the proposed segmentation method and the Laplace basis functions, Luo et al. [25] proposed a relatively high bit-capacity (64 bits) blind watermarking algorithm for 3D mesh. However, since they compute all eigenvalues and the eigenvectors of a Laplacian matrix for each patch, the computational costs for their proposed algorithm are expensive. Moreover, because each patch is embedded one watermark bit for the highest robustness, its bit-capacity is still low and it also can not resist cropping attacks.

The watermark extraction of blind spectral watermarking algorithm is more convenient than that of the non-blind one. In addition, the robustness is not affected by mesh alignment and re-sampling operations, which are essential for the robust non-blind spectral watermarking algorithm. However, it is generally believed that the non-blind algorithm can provide better robustness to various attacks than the blind one [4, 14].

In this paper, we focus on the robust non-blind spectral watermarking algorithm for a two-manifold mesh. Furthermore, the proposed algorithm is more suitable for the 3D meshes in graphics applications than in CAD/ CAM applications, whereas the latter one requires more efforts on geometric feature preservation.

3 Manifold harmonics analysis

Manifold harmonics basis functions are the eigenfunctions of the following Laplace–Beltrami operator, which is an extension of the classical Laplacian operator onto a two-manifold M with a metric g.

$$\Delta_M = \mathrm{div} \cdot \mathrm{grad} = \sum_i \frac{1}{\sqrt{|g|}} \frac{\partial}{\partial x_i} \sqrt{|g|} \frac{\partial}{\partial x_i} \tag{1}$$

where $|g|$ denotes the determinant of g. These eigenfunctions are denoted as pairs $\{(\lambda_k, \boldsymbol{H^k})\}$ that satisfy the following manifold harmonics equation.

$$-\Delta \boldsymbol{H} = \boldsymbol{\lambda H} \tag{2}$$

Vallet and Levy [26] employed the Finite Element Method (FEM) to discretize the above eigenfunction problem for a two-manifold mesh. The harmonics equation (2) can be re-written as the following generalized eigenvalue problem.

$$-\boldsymbol{Q H} = \boldsymbol{\lambda B H} \tag{3}$$

where

$$Q_{ij} = \begin{cases} (\cot \beta_{ij} + \cot \beta'_{ij})/2 & : \quad edge(i, j) \\ -\sum_j Q_{ij} & : \quad i = j \end{cases},$$

$$B_{ij} = \begin{cases} (|t| + |t'|)/12 & : \quad edge(i, j) \\ (\sum_{t \in St(i)} |t|)/6 & : \quad i = j \end{cases}.$$

In the above equations, the $|t|$ and $|t'|$ are the areas of triangles t and t', respectively, which share the edge (i, j), and $\boldsymbol{Q}$ is the stiffness matrix with cotangent weights. The β_{ij} and β'_{ij} are two angles corresponding to the edge (i, j) in the triangles t and t', respectively. The term $\cot \beta'_{ij} = 0$ if the edge(i, j) is a boundary edge of the mesh. The $St(i)$ denotes a set of one-ring neighboring triangles around vertex i. By lumping the mass matrix $\boldsymbol{B}$, one can obtain a diagonal mass matrix $\boldsymbol{D}$, whose elements are

$$D_{ii} = \sum_j B_{ij} = \left(\sum_{t \in St(i)} |t| \right) /3. \tag{4}$$

If the matrix $\boldsymbol{B}$ in (3) is replaced with the diagonal matrix $\boldsymbol{D}$, then (3) can be reformulated as

$$-\boldsymbol{Q H} = \boldsymbol{\lambda D H}. \tag{5}$$

By solving (5) for the leading m eigenvalues and their eigenvectors, we can obtain a set of eigenpairs $\{(\lambda_k, \boldsymbol{H}^k)\}$ $(0 \le k \le m - 1)$ with $\lambda_0 = 0 \le \lambda_1 \cdots \le \lambda_{m-1}$. We will discuss how to determine the number "m" in Sect. 4.3. Finally, each vector $\boldsymbol{H}^k$ is $\boldsymbol{D}$-relative normalized as: $\bar{\boldsymbol{H}}^{\boldsymbol{k}} = \boldsymbol{H}^k / \sqrt{(\boldsymbol{H}^k)^T \boldsymbol{D} \boldsymbol{H}^k}$. The orthogonalized vectors $\{(\lambda_k, \bar{\boldsymbol{H}}^{\boldsymbol{k}}) | 0 \le k \le m - 1\}$ are called the Manifold Harmonics Basis (MHB). With the help of publicly available libraries APPACK [27] and TAUCS [28], a band-by-band spectrum computing algorithm [26] is employed to compute the MHB in our algorithm.

Let the original mesh have n vertices, then the Manifold Harmonics Transformation (MHT) of a coordinate vector $\boldsymbol{x} = [x_0, \ldots, x_{n-1}]^T$ means the expansion of the vector $\boldsymbol{x}$ under MHB functions. The spectral coefficient vector

Author's personal copy

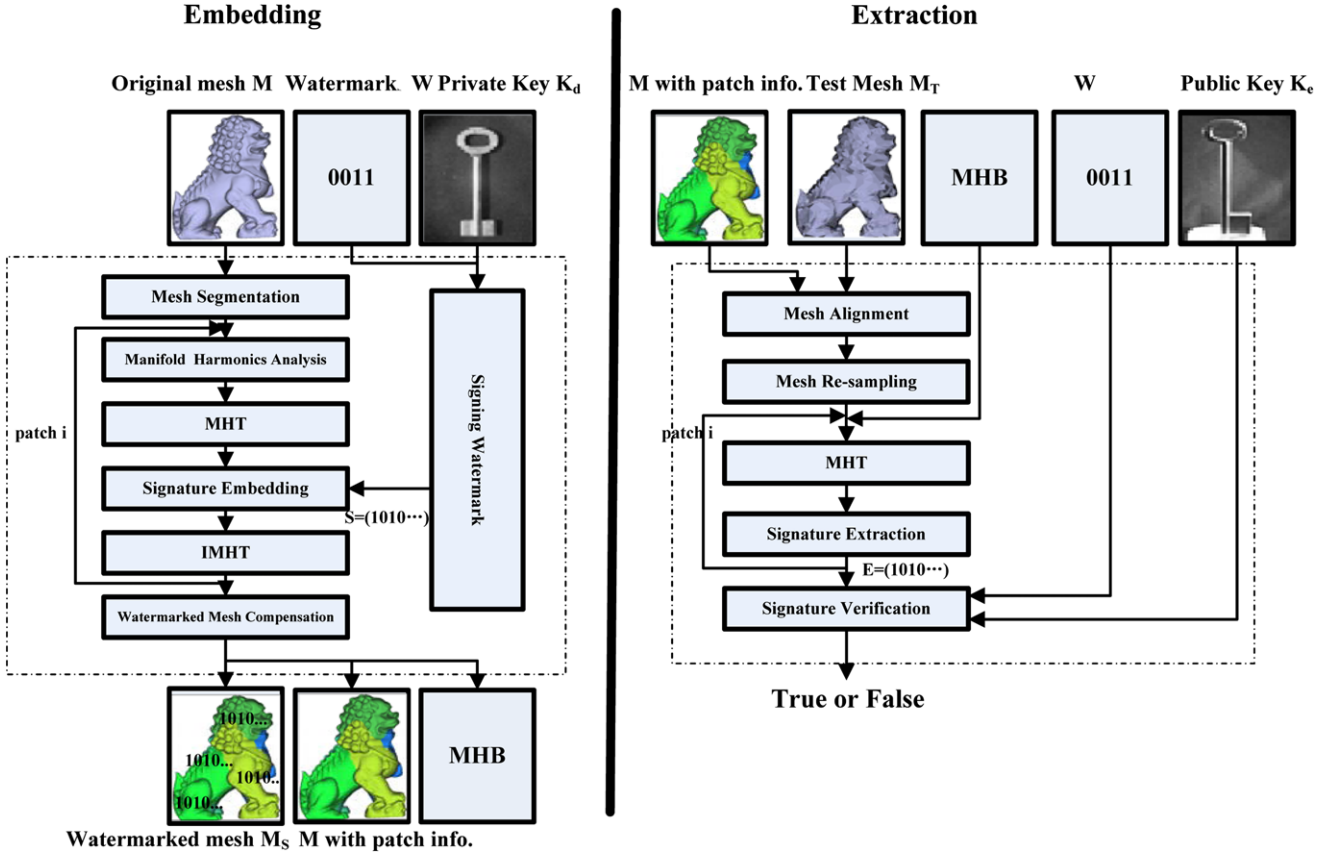


Fig. 1 The framework of the proposed watermarking algorithm

$\tilde{\boldsymbol{x}} = [\tilde{x}_0, \ldots, \tilde{x}_{m-1}]^T$ of $\boldsymbol{x}$ in the spectral space can be evaluated using the following formula [26].

$$\tilde{x}_k = x^T \boldsymbol{D}\bar{\boldsymbol{H}}^{\boldsymbol{k}} = \sum_{i=0}^{n-1} x_i D_{ii} \bar{H}_i^k \tag{6}$$

where $0 \leq k \leq m-1$. The $\tilde{\boldsymbol{y}}$ and $\tilde{\boldsymbol{z}}$ can be evaluated similarly. The Inverse MHT (IMHT) means the reconstruction of the vertex coordinate vector from its spectral coefficient vector as follows [26].

$$x_i' = \sum_{k=0}^{m-1} \tilde{x}_k \bar{H}_i^k \tag{7}$$

where $0 \leq i \leq n-1$. It is similar for the $\boldsymbol{y}$ and $\boldsymbol{z}$ coordinate vectors.

Due to the truncation of MHB functions, the reconstructed mesh via IMHT will suffer from the loss of the underlying geometric information. To alleviate this deficiency, we evaluate the reconstruction difference ΔM between the original mesh M and the reconstructed mesh M' using the following (8).

$$\Delta M = M - M'. \tag{8}$$

The reconstruction difference ΔM is helpful to improve the visual quality of watermarked mesh in the subsequent sections.

4 The robust non-blind confirmable watermarking algorithm

4.1 Framework of the proposed algorithm

The framework of the proposed algorithm is illustrated in Fig. 1. To resist cropping attack, a large mesh is first segmented into several patches, which helps equilibrate the MHB computational cost. For each patch, the manifold harmonics analysis is performed to compute the leading m MHB functions. The geometric information of each patch can then be transformed from spatial domain to its spectral domain via MHT. In the present work, the watermark is signed by the Elliptic Curve Digital Signature Algorithm (ECDSA) [29]. A signature S is generated with a private key, and then a modified S is modulated with the low-frequency spectral coefficients of each patch. Finally, a watermarked mesh can be reconstructed via IMHT using modulated spectral coefficients. Furthermore, the loss of geometry informa-

Author's personal copy

tion in watermarked mesh can be compensated by adding the reconstruction difference.

As a non-blind watermarking algorithm, the extraction phase requires the test mesh, the original unwatermarked mesh, MHB (optional), the patch information, and the public key. The test mesh is first aligned with the original mesh and then re-sampled according to the original mesh. Then the MHT is applied to the re-sampled test mesh and the original mesh, respectively, which will generate two spectral coefficient vectors. The extracted signature is then obtained by comparing the two coefficient vectors. Finally, after performing the signature verification step with the public key, we can draw the ownership assertion, i.e., true or false. The details of these steps are illustrated in Fig. 1.

4.2 Watermark embedding

4.2.1 Mesh segmentation

As described in Sect. 3, the performance bottleneck in the proposed algorithm is the eigenvalue-eigenvectors decomposition, which is always expensive for a large-scale mesh. To reduce the computational cost and to resist cropping attacks, a large-scale mesh is segmented into several patches. Meanwhile, considering the robustness and visual quality of watermarked mesh, the watermark signature should be spread to all patches uniformly. Due to the large-scale of the underlying mesh which may be up to millions of vertices, the speed of patch generation should be fast. Thus, we adopt the MeTiS [30] to segment the mesh such that each patch contains less than 30 k vertices. Naturally, the users can interactively determine whether a small-scale mesh needs to be segmented according to whether it can resist the cropping attacks or not.

4.2.2 Signing watermark

In this step, the ECDSA is applied to the watermark W to generate an l bits signature S. We will discuss how to determine the signature length "l" in Sect. 4.3. A digital signature algorithm proves that a particular message, i.e., watermark W, is valid. For the selection of hashing function which is the indispensable component in ECDSA, the IEEE P1363 standard [31] suggests SHA-1 defined by NIST [32]. The length of its input data should be no more than 2^{64}, while the length of its output data is 160 bits. The signature algorithm is briefly described as follows.

First, two integers a_2 and a_6 are selected interactively to create an elliptic curve EC: $y^2 + xy = x^3 + a_2x^2 + a_6$, which is defined on Galois Field GF($2^{l/2}$) [29, 33]. Let the order d define as the number of points in an elliptic curve group and A is the base point of order d on the curve EC. The public key K_e is then determined as: $K_e = k_d A$ after the mesh owner specifies private key k_d.

Then a point $R = (x_R, y_R) = rA$ is computed via a random integer r $(0 < r < d)$. The watermark hash is $h = SHA1(W)$. After the field element x_R is converted to an integer $\bar{x}_R$, the first signature component in ECDSA becomes the modulus of $\bar{x}_R$ with respect to the curve order d as

$$S_0 = \bar{x}_R \ mod \ d. \tag{9}$$

Here, the second component can be obtained via the following formula:

$$S_1 = r^{-1}(h + k_d S_0) \ mod \ d. \tag{10}$$

Finally, an l bits signature $S = (S_0, S_1)$ can be obtained, which is a 0 and 1 bit string.

4.2.3 Signature embedding

In this subsection, the signature S is embedded in the spectral domain of the 3D mesh by slightly modifying the low-frequency spectral coefficients. According to the spectral analysis [20], the low-frequency components account for the global shape information, while the high-frequency components contribute to the local shape information. Thus, a slight disturbance of the low-frequency spectral coefficients will not obviously introduce shape appearance distortion.

Assuming that the original mesh M is segmented into n_p patches, the patch j $(0 \le j \le n_p - 1)$ has a set of $3m$ spectral coefficients $\{\tilde{\boldsymbol{x}}_j, \tilde{\boldsymbol{y}}_j, \tilde{\boldsymbol{z}}_j\}$. These coefficients are modulated with $S = (s_0, s_1, \ldots, s_{l-1})$ under the chip rate c, the modulation amplitude α, and the axis-aligned bounding box size $\varphi_{j,x}, \varphi_{j,y}, \varphi_{j,z}$ of the patch j.

To balance the spectrum energy of each patch, the signature S composed of $\{0, 1\}$ is converted to another bit string $S' = (s'_0, s'_1, \ldots, s'_{l-1})$, where $s'_i = -1$ if $s_i = 0$; otherwise, $s'_i = 1$. Then the S' is duplicated c (chip rate) times to generate the final embedded signature as follows:

$$S'' = (\underbrace{S', S', \ldots, S'}_{c}). \tag{11}$$

Then we modulate the low-frequency spectral coefficients of each patch $\{(\tilde{x}_{j,k}, \tilde{y}_{j,k}, \tilde{z}_{j,k}) | 0 \le j \le n_p - 1, 1 \le k \le m - 1\}$ beginning from the second $(k = 1)$ three coefficients. This is because the eigenvalue corresponding to the first three coefficients is zero and its eigenvector is constant. The duplicated signature $S'' = (s''_0, s''_1, \ldots, s''_{lc-1})$ is embedded into all patches repeatedly. The modulating formula are

$$\begin{cases} \tilde{x}'_{j,k} = \tilde{x}_{j,k} + \alpha s''_{3(k-1)} \varphi_{j,x} \\ \tilde{y}'_{j,k} = \tilde{y}_{j,k} + \alpha s''_{3(k-1)+1} \varphi_{j,y} \\ \tilde{z}'_{j,k} = \tilde{z}_{j,k} + \alpha s''_{3(k-1)+2} \varphi_{j,z} \end{cases} \tag{12}$$

Author's personal copy

for $1 \le k \le \lceil lc/3 \rceil$, and

$$\begin{cases} \tilde{x}'_{j,k} = \tilde{x}_{j,k} \\ \tilde{y}'_{j,k} = \tilde{y}_{j,k} \\ \tilde{z}'_{j,k} = \tilde{z}_{j,k} \end{cases} \tag{13}$$

for $k = 0$ or $\lceil lc/3 \rceil + 1 \le k \le m - 1$.

4.2.4 *Watermarked mesh compensation*

After the signature is embedded, the IMHT is performed to generate the watermarked mesh via the modulated spectral coefficients. To compensate for the loss of geometric information of watermarked mesh M'_S, the reconstruction difference ΔM, defined in (8), is added on the M'_S. Finally, the watermarked mesh M_S becomes

$$M_S = M'_S + \Delta M. \tag{14}$$

4.3 Parameters discussion

The parameters in the proposed algorithm include patch information, digital signature parameters, and embedding parameters. Patch information includes the patch number n_p and the patching topology. In our implementations, the patch number is $n_p = [n/30000] + 1$, where n is the vertex number of the mesh. Digital signature parameters include the length of Galois Field and the base point A in an elliptic curve group. The length of Galois Field is 162 bits, which is long enough for practical applications and the base point A is generated in random with regard to the degree d [29].

Embedding parameters include the number of manifold harmonics basis m, the signature length l, the modulation amplitude α, and the chip rate c. Theoretically, the embedding signature length l could be no more than $3(m-1)$. However, only low-frequency spectral coefficients are modulated with the signature for the sake of robustness. Meanwhile, the longer the embedded signature is, the more serious the distortion of watermarked mesh will be. Owing to the 162-bith length of Galois Field in Sect. 4.2.2, the signature length l is adopted as 324 bits in our paper. In theory, a large chip rate c can increase robustness in the case of exact computation. Similarly, a large α helps extract the signature and thus increase the robustness, but it tends to introduce shape distortion. An example of different αs is shown in Fig. 2. Therefore, we must trade off the robustness and visual quality when choosing the parameters c and α in practice.

Finally, we discuss the most important embedding parameter m, i.e., the number of MHB functions. Intuitively, a large number m may be helpful to increase the robustness and visual quality of watermarked mesh. However, according to the following Theorem 1, the answer is negative.

(a) original mesh (b) α=0.005 (c) α=0.001

Fig. 2 Watermarked eros (476 k vertices) using our algorithm with different parameter αs. The distortion in (**b**) is more notable than that in (**c**)

Theorem 1 *Given the chip rate c and modulation amplitude* α, *the watermark signature* $S = (s_0, \ldots, s_{l-1})$ *is embedded into the spectral coefficients* $\{(\tilde{x}_k, \tilde{y}_k, \tilde{z}_k) | 1 \le k \le \lceil lc/3 \rceil\}$ *by using the embedding process in* (12) *and* (13). *Given two integers* $m_1 = \lceil lc/3 \rceil + 1$ *and* $m_1 \le m_2 \le n - 1$, *then the watermarked meshes* $M_S^{(m_1)} = M_S^{(m_2)}$, *where* $M_S^{(m_1)}$ *and* $M_S^{(m_2)}$ *are generated using* $\boldsymbol{MHB}^{(m_1)} = \{(\lambda_k, \bar{\boldsymbol{H}}^{k,m_1}) | 0 \le k \le m_1 - 1\}$ *and* $\boldsymbol{MHB}^{(m_2)} = \{(\lambda_k, \bar{\boldsymbol{H}}^{k,m_2}) | 0 \le k \le m_2 - 1\}$, *respectively.*

The proof of Theorem 1 is given in the Appendix. According to Theorem 1, if $M_S^{(m_1)}$ and $M_S^{(m_2)}$ undergo the same attack, then their extraction signatures are the same. Therefore, without sacrificing of the robustness and visual quality of the 3D watermarked mesh, the minimal number of MHB can be set as $m = \lceil lc/3 \rceil + 1$, i.e., $m = 325$ in our paper. Here a small number m will introduce shape distortion in the reconstructed mesh. However, the distortion can be greatly compensated by introducing the reconstruction difference as described in Sect. 4.2.4. Thus, the computational costs for the MHB are decreased efficiently in our algorithm.

4.4 Watermark extraction

The watermarked mesh M_S may be distributed with licenses and will undergo potential attacks. The extraction phase can assert ownership of the test mesh M_T. As a non-blind watermarking algorithm, the extraction phase requires the test mesh M_T, original mesh M, MHB (optional), the patch information, and the public key. To extract the watermark signature from the test mesh M_T and verify the signature, we should recover an intermediate mesh according to the test mesh using mesh alignment and re-sampling operations.

4.4.1 *Mesh alignment and re-sampling*

To resist simple but common similarity transformation attacks, the test mesh M_T should be first aligned with the orig-

Author's personal copy

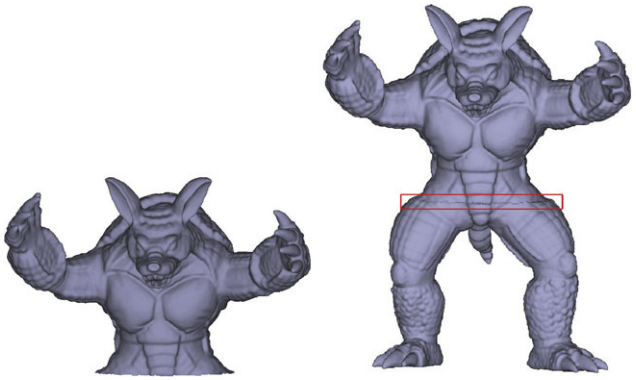


Fig. 3 Watermarked armadillo (173K) via a cropping attack (*left*) and its re-sampled one (*right*). After mesh re-sampling, the cropping boundary on the mesh is obvious in the model on the right (enclosed by a red rectangle)

inal mesh M. The Iterated Closest Point (ICP) method [34], i.e., a popular alignment technique, is adopted after an approximate transformation via coarse alignment is defined. The coarse alignment requires at least three corresponding point-pairs on the M_T and original mesh M, which can be specified interactively or generated automatically. For the automatic correspondence, the 4-Points Congruent Sets (4PCS) can be employed [35]. To speed up the ICP method, we construct a kd-tree to facilitate the nearest point searching.

After the test mesh M_T is aligned with the original mesh M, M_T is re-sampled according to M such that the re-sampled M_T has the same topology as that of M. First, the normal vector at each vertex of M is estimated as an angle-weighted average of the neighboring triangle normals. Then the re-sampled vertex on M_T is defined as the intersection between the mesh M_T and each normal vector of M. If the distance between the re-sampled vertex on M_T and the corresponding vertex on M is greater than a user-defined threshold or there is no intersection (in the case of cropping attacks), the corresponding vertex on the original mesh M will be adopted as the intersection. Thus, the alignment and re-sampling steps can deal with cropping and connectivity attacks. An example of a cropped watermarked mesh is shown in Fig. 3. The ray-triangle intersection is accelerated using the Binary Space Partition (BSP) in our algorithm.

4.4.2 Signature extraction

After the alignment and re-sampling steps, the MHT step is performed for each patch-pair of the original mesh M and the re-sampled test mesh M_T. Then we can obtain two sets of $3m$ spectral coefficients $\{\tilde{\boldsymbol{x}}_j, \tilde{\boldsymbol{y}}_j, \tilde{\boldsymbol{z}}_j\}$ and $\{\tilde{\boldsymbol{x}}'_j, \tilde{\boldsymbol{y}}'_j, \tilde{\boldsymbol{z}}'_j\}$ for patch-pair j. The parameter m is set as $\lceil lc/3 \rceil + 1$ which is discussed in Sect. 4.3.

Next, the signature bits are extracted with regard to the corresponding variations of their coefficients. The summations of the coefficient variations for the signature bits s_{3k}, s_{3k+1}, s_{3k+2} $(0 \le k \le \lceil l/3 \rceil - 1)$ are defined as follows:

$$\begin{cases} q_{3k} = \sum_{j=0}^{n_p-1} \sum_{i=0}^{c-1} (\tilde{x}'_{j,k+1+il/3} - \tilde{x}_{j,k+1+il/3}) \\ q_{3k+1} = \sum_{j=0}^{n_p-1} \sum_{i=0}^{c-1} (\tilde{y}'_{j,k+1+il/3} - \tilde{y}_{j,k+1+il/3}) \\ q_{3k+2} = \sum_{j=0}^{n_p-1} \sum_{i=0}^{c-1} (\tilde{z}'_{j,k+1+il/3} - \tilde{z}_{j,k+1+il/3}). \end{cases} \tag{15}$$

Ideally, if there is no attack for the test mesh M_T and no numerical error in the computations, the above q_{3k}, q_{3k+1}, q_{3k+2} should equal

$$\begin{cases} q_{3k} = c\alpha\varphi_x s_{3k} \\ q_{3k+1} = c\alpha\varphi_y s_{3k+1} \\ q_{3k+2} = c\alpha\varphi_z s_{3k+2}, \end{cases} \tag{16}$$

where $0 \le k \le \lceil l/3 \rceil - 1$ and $\varphi_x = \sum_{j=0}^{n_p-1} \varphi_{j,x}$, $\varphi_y = \sum_{j=0}^{n_p-1} \varphi_{j,y}$, $\varphi_z = \sum_{j=0}^{n_p-1} \varphi_{j,z}$. Since c, α, φ_x, φ_y, φ_z are always positive, and $s_{3k} \in \{-1, 1\}$, thus the extracted signature bit e_{3k} can be determined as

$$e_{3k} = \begin{cases} 1 & : \quad q_{3k} \ge 0 \\ 0 & : \quad q_{3k} < 0 \end{cases} \tag{17}$$

which is similar for e_{3k+1} and e_{3k+2}.

To evaluate the robustness of watermarking algorithms, the Extraction Rate (ER) between the watermark signature $S = (s_0, s_1, \ldots, s_{l-1})$ and the extracted signature $E = (E_0, E_1) = (e_0, e_1, \ldots, e_{l-1})$ is defined as

$$ER = \frac{1}{l} \sum_{i=0}^{l-1} (e_i = s_i). \tag{18}$$

If each signature bit is extracted successfully, ER is 100%.

4.4.3 Signature verification

To verify the extraction signature $E = (E_0, E_1)$ on the watermark W, according to the IEEE P1363 standard [31], we should compute three integers, t, t_1, t_2 after we obtain the hash $h = SHA1(W)$ as follows:

$$\begin{aligned} t &= E_1^{-1} \ mod \ d \\ t_1 &= ht \quad mod \ d \\ t_2 &= tE_0 \ mod \ d \end{aligned}. \tag{19}$$

Then a point R' on the public elliptic curve EC (in Sect. 4.2.2) is computed using t_1, t_2:

$$R' = t_1 A + t_2 K_e. \tag{20}$$

Finally, the x coordinate $x_{R'}$ of R' is converted to an integer $\bar{x}_{R'}$. If the modulus of $\bar{x}_{R'}$ to the curve order d equals the integer E_0, then the extraction signature $E = (E_0, E_1)$ equals the embedded signature $S = (S_0, S_1)$ and the result of verification is true; otherwise, the result of verification is false.

Author's personal copy

5 Experimental results and discussion

Each watermark bit should be blindly embedded into several spectral coefficients for the watermark extraction, hence, the blind spectral watermarking algorithms [23–25] need more spectral coefficients to embed the same length watermark bits (such as 324 bits in our paper) than our algorithm. It will be difficult to balance computational efficiency, visual quality, and robustness. Thus, compared with the three algorithms, our algorithm has advantages of computational efficiency, high bit-capacity, and well-balanced visual quality and robustness, especially for the cropping attacks.

Therefore, we have implemented the proposed algorithm (noted as MHBs) and the other two robust non-blind spectral watermarking algorithms, i.e., LBFs [20] and RBFs [21], for various scales of 3D meshes. We compare three algorithms comprehensively in terms of their efficiency, visual qualities, and robustness under various attacks. All of the examples are implemented on a PC with Intel CPU i7 (920) processor, 2.67 GHz, 4 G RAM, and Window 7 (64 bits).

According to the parameters discussion in Sect. 4.3, and also for the sake of fair comparison, the embedding parameters are set as follows: $l = 324$ for all algorithms; for LBFs: $\alpha = 0.001$, $c = 1$; for RBFs: $\alpha = 0.01$, $c = 1$; for MHBs: $c = 3$, and $\alpha = 5 \times 10^{-6}$ for bunny model, $\alpha = 0.0002$ for teddy model, $\alpha = 0.001$ for the other models. Note that the chip rates $c = 3$ for MHBs and $c = 1$ for LBFs mean the same length of embedded signature due to the different embedding mechanism. For RBFs, if $\alpha < 0.01$ or $c > 1$, the robustness of the algorithm will worsen.

5.1 Security discussion

In the proposed algorithm, to assert ownership and resist 3D mesh forging, the robust non-blind spectral watermarking framework is optimized by introducing the ECDSA both in the embedding phase and in the extraction phase. The private key k_d is uniquely held by the mesh owner, then only the owner can embed the watermark W into the 3D mesh validly. The trusted third party (confirmer) can then confirm with the mesh owner of watermarked mesh using the owner's public key K_e and watermark W. The signatures in different watermarked meshes even via the same private key may be different because of a random value r in signing the watermark. Therefore, our algorithm can both assert ownership and resist forging.

In the proposed algorithm, if ER is 100%, the signature verification is true, and the ownership is claimed. This is the strictest ownership assertion. Of course, we can define different security grades according to different ER values. For example, if the ER is greater than a threshold (e.g., 56.1%, it will be discussed in Sect. 5.5), we can also affirm that the test mesh contains the originally embedded watermark signature.

Table 1 Runtime statistics of MHBs, where the number m of MHB computed is **325**. The table includes vertex number n, patch number n_p, runtime for computing MHB (MHB), embedding runtime (Emb.) and extraction runtime (Ext.)

Models	n	n_p	MHB	Emb.	Ext.
bunny	35 k	1	31.331 s	0.140 s	1.341 s
teddy	46 k	1	42.021 s	0.218 s	1.132 s
Chinese lion	153 k	5	129.786 s	0.546 s	3.291 s
armadillo	173 k	6	149.170 s	0.577 s	4.164 s
eros	476 k	16	409.096 s	1.607 s	12.039 s
Asia dragon	1 M	33	845.477 s	2.978 s	23.034 s

Table 2 Runtime statistics for LBFs, which include patch number n_p, the number m of LBF computed, runtime for computing LBF (LBF), embedding runtime (Emb.), and extraction runtime (Ext.)

Models	n_p	m	LBF	Emb.	Ext.
bunny	1	5 k	6 m 19 s	1.576 s	3.480 s
teddy	1	3.5 k	7 m 19 s	4.290 s	1.430 s
Chinese lion	5	4 k	26 m 49 s	14.602 s	4.396 s
armadillo	6	4 k	30 m 16 s	16.567 s	5.347 s
eros	16	4 k	1 h 26 m 3 s	45.536 s	15.283 s
Asia dragon	33	4 k	2 h 53 m 39 s	102.779 s	30.932 s

5.2 Computational efficiency

Computational costs of the spectral algorithms are mainly determined by the construction of spectral spaces. The computational efficiency is largely improved because we give a method to determine the minimal number of basis functions without scarifying the visual quality and robustness of the watermarked mesh. Table 1 shows the runtime statistics of the proposed algorithm for various scale 3D meshes. Compared with dominated runtime for computing MHB, the runtimes for signing watermark and signature verification can almost be neglected. Even for the mesh with over 1 M vertices, the whole watermarking embedding runtime is less than 15 minutes because only a minimal number of MHB are computed under the same security conditions. In comparison, for the LBFs, it will take about 3 hours as shown in Table 2. For the RBFs algorithm, it will take about 16 minutes for $m = 108$ ($m = 325$ in our algorithm) as shown in Table 3. Thus, the proposed algorithm have the advantage on computational efficiency compared with LBFs.

5.3 Visual quality comparison

Owing to the adoption of the manifold harmonics analysis and the new watermark embedding manner, the loss of visual quality of the watermarked mesh made by the proposed algorithm is decreased. The geometry disturbance or

Author's personal copy

Table 3 Runtime statistics for RBFs, where the number m of radial basis functions computed is **108** and patch number $n_p = 1$. The table includes runtime for computing RBF (RBF), embedding runtime (Emb.) and extraction runtime (Ext.). "*" means the out-of-core approach is adopted to compute RBF for the large-scale of mesh

Models	n	RBF	Emb.	Ext.
bunny	35 k	1.482 s	0.031 s	1.011 s
teddy	46 k	1.966 s	0.063 s	1.102 s
Chinese lion	153 k	6.614 s	0.172 s	3.229 s
armadillo	173 k	7.504 s	0.156 s	4.053 s
eros	476 k	19.513 s	0.430 s	11.873 s
Asia dragon	1 M	949.330 s(∗)	4.568 s	22.973 s

shape distortion in the watermarked mesh compared with the original mesh is an important factor to assess a mesh watermarking algorithm. To evaluate the small difference between two meshes, there are two criteria: subjective and objective. The subjective criterion is related to psychology and cognition of human being. Some interesting objective methods for watermarked mesh quality assessment are proposed, such as Hausdorff metric [36, 37], surface roughness metric [38], structural similarity metric [39] and Shape-DNA metric [40]. Due to space constraints, we will access the visual qualities of the watermarked meshes generated by different algorithms in terms of visual appearance, Hausdorff metric, and Shape-DNA metric.

The root mean square error of the forward Hausdorff distance between two meshes M_S and M is defined as [37]

$$d_{\text{rmse}}(M_S, M) = \sqrt{\frac{1}{|M_S|}\iint_{p\in M_S} d(p, M)^2\, dM_S} \tag{21}$$

where $|M_S|$ denotes the area of M_S, and $d(p, M)$ is the minimum Euclidean distance from a sampling point p on M_S to M. The sampling interval is 0.05% of the major bounding box diagonal length of M_S in our paper. The detailed statistics of d_{rmse} between the mesh and the watermarked meshes via LBFs, RBFs, and MHBs can be found in Table 4.

Reuter et al. [40] proposed a method to measure similarity between two meshes by taking the eigenvalues of its Laplace–Beltrami operator into account. Let M be a two-manifold mesh with a metric g. The spectrum of (M,g) is

$$spec(M, g) = \{\lambda_0 \le \lambda_1 \le \cdots\}, \tag{22}$$

where λ_i is the eigenvalue of (3). The cropped spectrum contains only the leading $m + 1$ eigenvalues

$$cspec_m(M, g) = \{\lambda_0 \le \lambda_1 \le \cdots \le \lambda_m\} \tag{23}$$

which is called Shape-DNA of (M,g). Let $\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_m)$ and $\boldsymbol{\lambda}^{(S)} = (\lambda_1^{(S)}, \lambda_2^{(S)}, \ldots, \lambda_m^{(S)})$ are two

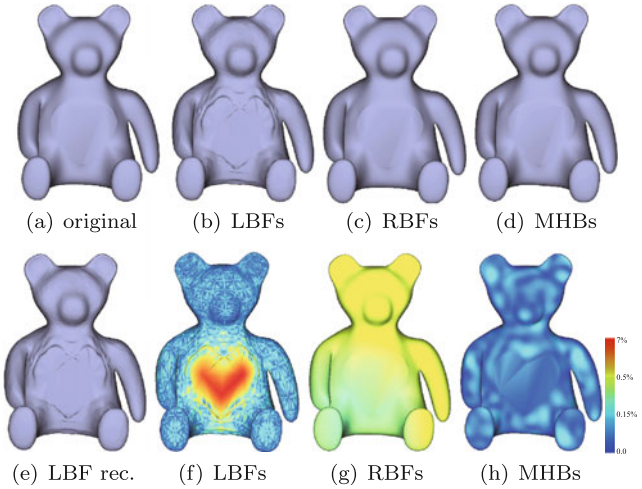


Fig. 4 Watermarked teddy (46 k vertices). (**a**) is the original mesh, (**b**)–(**d**) are watermarked meshes using LBFs with $\alpha = 0.001$, RBFs with $\alpha = 0.01$, and MHBs with $\alpha = 0.0002$, respectively and their robustness values can be found in Table 4. (**e**) is the reconstructed mesh using LBF with $m = 3500$. The $d_{2,50}$ for (**b**)–(**d**) are: 4.131043, 0.616213, and 0.238395. (**f**)–(**h**) are the mesh difference color maps (blue minimum and red maximum) of (**b**)–(**d**), which are coded according to relative distances between the watermarked ones and original ones

m-dimensional normalized Shape-DNAs for M and M_S, respectively, where λ_i and $\lambda_i^{(S)}$ are normalized by dividing their first non-zero eigenvalue. To evaluate the shape similarity between the original mesh M and its watermarked mesh M_S, the similarity metric between two meshes can be defined as

$$d_{p,m}(M_S, M) = \left(\sum_{i=1}^{m} (\lambda_i^{(S)} - \lambda_i)^p\right)^{1/p}. \tag{24}$$

Using the Euclidean distance $d_{2,50}$ of the normalized leading 50-dimensional vectors of eigenvalues, we can assess the geometry loss in the watermarked mesh. The detailed statistics of $d_{2,50}$ between the mesh and the watermarked meshes via LBFs, RBFs, and MHBs can be found in Table 4.

The visual appearance comparison between the mesh and the watermarked meshes via LBFs, RBFs, and MHBs can be found in Figs. 4 and 5. Figure 4 shows the visual quality comparison of the teddy watermarked using LBFs, RBFs, and MHBs. According to Fig. 4(b), Fig. 4(e), and Fig. 4(f), we can observe that the mesh watermarked using LBFs tends to be distorted because the teddy mesh contains slim triangles on the chest, as shown in Fig. 8(a). As we know, the LBF depend only on mesh connectivity while the watermarked meshes using RBFs and MHBs are slightly affected by the mesh irregularity, as shown in Fig. 4(c) and Fig. 4(d). The geometry difference color maps in Fig. 4(f)–4(h) also prove that the proposed algorithm can achieve satisfactory visual quality for the watermarked mesh. A similar conclusion can be drawn from a segmented mesh model in Fig. 5.

Author's personal copy

Table 4 Robustness comparisons, i.e., ER (%) under different attacks, where "ST" means similarity transformations, "LS5" means Laplacian smoothing for five steps, "TS" means Taubin smoothing, "Loop" means Loop subdivision for one time. Note that original mesh is used for the mesh alignment and re-sampling steps in LBFs and MHBs while watermarked mesh is used in RBFs

Models	Types	d_{rmse}	$d_{2,50}$	ST	noise		smoothing		re-meshing	Loop	simplification			
					0.5%	0.1%	LS5	TS			50%	10%	5%	1%
bunny	RBFs	.282	.422	100	67.59	80.56	54.94	76.54	56.79	57.41	75.93	65.43	58.02	55.25
	LBFs	.030	.457	100	71.60	99.69	60.19	99.69	92.28	59.88	95.68	84.57	73.46	56.79
	MHBs	**.020**	**.167**	100	**99.69**	100	**74.07**	100	**87.96**	**62.65**	**91.67**	**81.79**	**75.31**	**51.23**
teddy	RBFs	.338	.616	100	65.12	75.00	55.86	73.15	68.83	62.35	73.15	63.27	62.35	52.78
	LBFs	.050	4.131	100	72.53	99.69	62.96	88.89	88.27	81.17	88.27	87.04	82.10	56.48
	MHBs	**.038**	**.238**	100	**99.69**	100	**65.74**	**84.57**	**89.20**	**78.74**	**90.74**	**90.74**	**89.20**	**71.60**
Chinese	RBFs	2.822	1.941	100	71.91	88.89	59.88	87.35	79.94	63.58	96.30	81.17	76.54	62.04
lion	LBFs	.014	.231	100	89.81	100	82.10	100	99.38	72.22	100	96.91	87.96	56.79
	MHBs	**.008**	**.025**	100	**95.99**	100	**86.73**	100	**98.77**	**74.38**	100	**96.60**	**89.81**	**57.72**
armad-	RBFs	.146	2.143	100	62.04	74.38	59.26	90.43	78.09	65.43	89.20	74.69	70.99	58.64
illo	LBFs	.012	.336	100	78.09	100	72.84	100	98.46	76.23	99.69	97.22	89.20	58.33
	MHBs	**.006**	**.074**	100	**95.06**	100	**94.14**	100	**99.69**	**80.56**	100	**98.15**	**93.21**	**58.64**
eros	RBFs	1.781	1.994	100	76.30	86.73	72.84	78.09	81.79	67.90	94.75	87.65	81.79	70.68
	LBFs	.008	.339	100	94.44	100	98.46	100	100	97.84	100	100	100	70.99
	MHBs	**.006**	**.021**	100	**98.15**	100	**96.30**	100	100	**92.90**	100	100	100	**92.28**
Asia	RBFs	.121	2.348	100	67.90	85.19	73.77	95.99	89.20	78.40	96.60	93.21	87.04	72.22
dragon	LBFs	.164	1.078	100	76.23	100	99.38	100	100	85.19	100	100	95.37	61.42
	MHBs	**.006**	**.293**	100	**99.38**	100	100	100	100	100	100	100	100	**99.07**

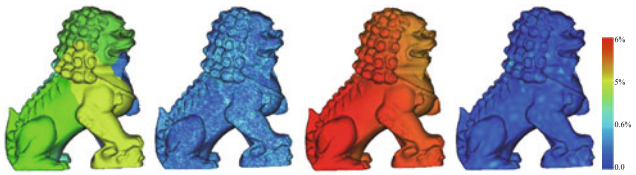


Fig. 5 Watermarked Chinese lion. (**a**) is the original segmented model with 153 k vertices and five patches. (**b**)–(**d**) are watermarked meshes using LBFs with $\alpha = 0.001$, RBFs with $\alpha = 0.01$ and MHBs with $\alpha = 0.001$ respectively. The $d_{2,50}$ for (**b**)–(**d**) are: 1.941285, 0.230947, 0.025299, respectively. The color maps in (**b**)–(**d**) are coded according to relative distances between original ones and watermarked ones

5.4 Robustness comparison

The proposed algorithm can achieve better robustness than LBFs and RBFs because the watermark signature bits generated by ECDSA are embedded into the low-frequency spectral coefficients of all patches repeatedly and extracted with regard to the corresponding variations of their coefficients. We compare the robustness of our algorithm with the two algorithms for different scale meshes under various attacks, such as similarity transformations, random noise, smoothing, loop subdivision, simplification, re-meshing, cropping, and their combinations.

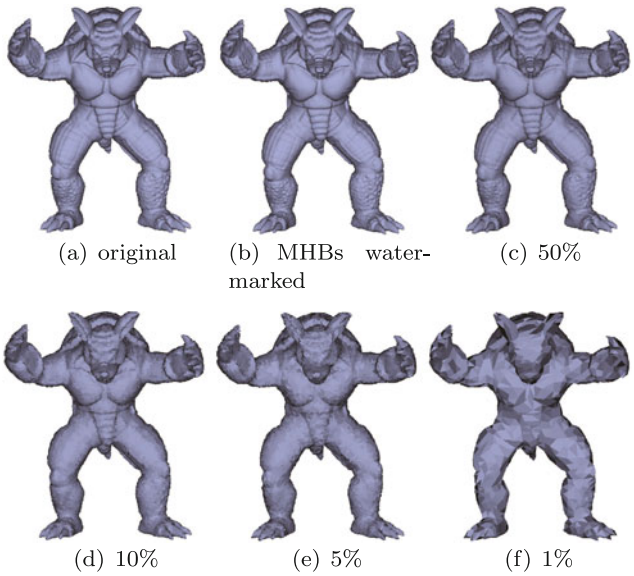
In our implementations, mesh simplification attacks are performed using the quadric error metrics approach [41]. The Laplacian smoothing, Taubin smoothing, Loop subdivision, and mesh cropping operations are performed using MeshLab [42]. The re-meshing operation is performed by RapidForm 2006 [43].

From Table 4, our algorithm is more robust under various attacks than the LBFs and RBFs in general. Occasionally, our algorithm is not as robust as the LBFs under the smoothing, re-meshing, Loop subdivision, and simplification attacks. However, their ERs are so similar that we can claim the mesh ownership.

Figure 6 shows the watermarked armadillo meshes attacked by different level simplifications. Figure 7 shows the partial watermarked Asia dragon meshes attacked by random noises. Figure 8 shows the re-meshed watermarked teddy meshes. Figure 9 shows the watermarked bunny meshes attacked by the Taubin and Laplacian smoothing operations. All of the ERs in these figures can be found in Table 4.

Table 5 is the statistics of robustness of three algorithms under the combination attacks. Figure 10 shows some attacked examples by cropping or combination operations. Thanks to the mesh segmentation, the watermarked mesh

Author's personal copy



(a) original (b) MHBs watermarked (c) 50%

(d) 10% (e) 5% (f) 1%

Fig. 6 The watermarked armadillo mesh (173 k vertices) is attacked by mesh simplification with different levels. The ERs of (**c**)–(**f**) are 100%, 98.15%, 93.21%, and 58.64%, respectively

(a) MHBs watermarked (b) 0.1% (c) 0.5%

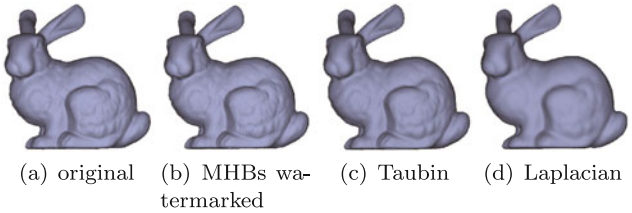
Fig. 7 Partial watermarked Asia dragon mesh (1 M vertices) attacked by random noises. The ERs of (**b**) and (**c**) are 100% and 99.38%, respectively

(a) original (b) MHBs watermarked (c) re-meshed

Fig. 8 Watermarked teddy (46 k vertices) attacked by re-meshing. The ER of (**c**) is 89.20%

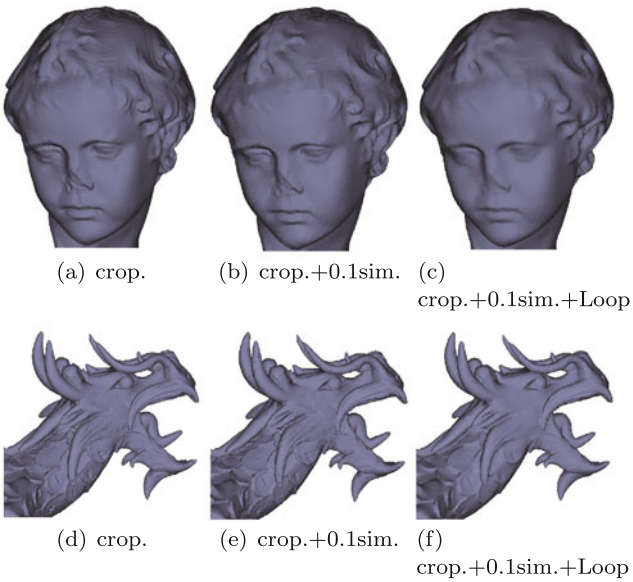
can resist the cropping attacks well provided there is one patch not cropped.

In summary, our algorithm exhibits good robustness under various attacks. However, it can not resist global mesh deformation attacks because the mesh alignment and resampling do not work in that case. This issue will be the focus in future research.



(a) original (b) MHBs watermarked (c) Taubin (d) Laplacian

Fig. 9 The watermarked bunny (35 k vertices) attacked by Taubin and Laplacian smoothing operations for five steps. The ERs of (**c**) and (**d**) are 100% and 74.07%, respectively



(a) crop. (b) crop.+0.1sim. (c) crop.+0.1sim.+Loop

(d) crop. (e) crop.+0.1sim. (f) crop.+0.1sim.+Loop

Fig. 10 Combination attacks for watermarked eros (476 k vertices) and watermarked Asia dragon (1 M vertices) made by MHBs. (**a**) 255 k vertices, (**d**) 371 k vertices. The ERs of (**a**)–(**f**) are 100%, 100%, 63.58%, 100%, 100%, and 63.27%

5.5 ROC curve

The false positive rate is acceptable because we adopt the original unwatermarked mesh, not the watermarked mesh which is adopted in RBFs for the mesh alignment and resampling operations in watermark extraction. A false positive occurs when a watermark extractor indicates the presence of a watermark in an unwatermarked mesh. To assess the fidelity and determine the appropriate threshold of the proposed algorithm (i.e., MHBs), we have shown our experimental results by distributions histogram and Receiver Operating Characteristic (ROC) curve in Fig. 11. An ROC curve is a parametric curve that plots the false positive rate (the x-axis) against the false negative rate (the y-axis) of extraction rate as a function of the threshold [4]. To plot distributions of extraction rates and draw the ROC curve, the extractor of MHBs was applied to 74 watermarked meshes and 74 unwatermarked meshes to undertake the attacks in Table 4 and Table 5, respectively. From Fig. 11(a), we can see that there is a very small overlap of distributions and the

Author's personal copy

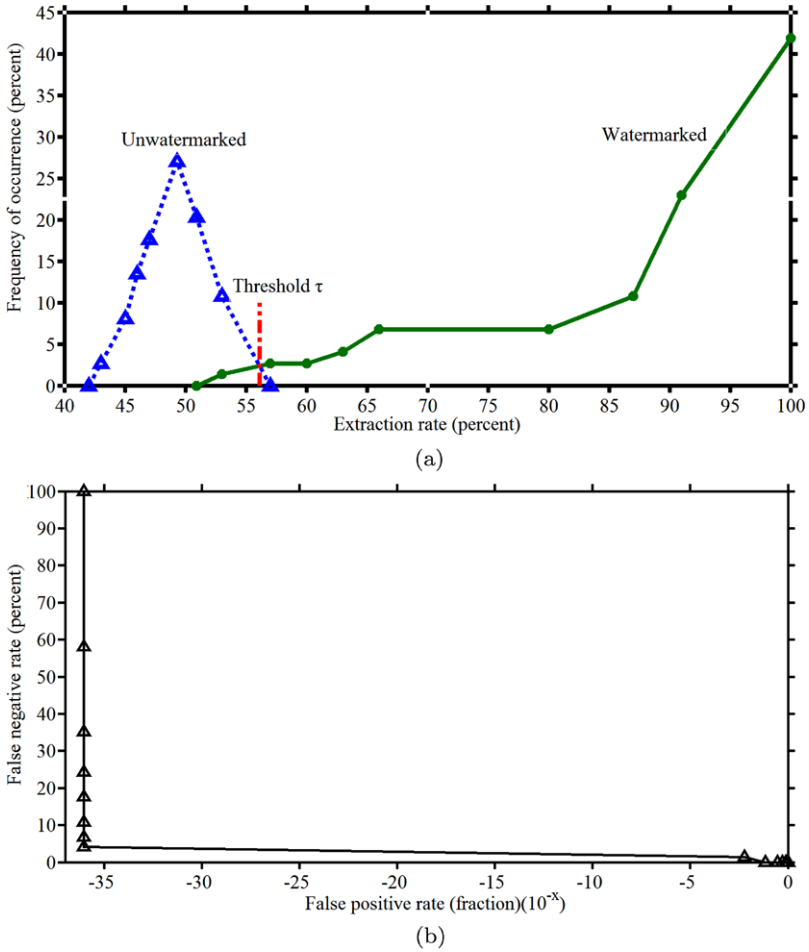


Fig. 11 Distributions histogram and ROC curve. (**a**) shows the distributions of extraction rates for the unwatermarked meshes (*dashed blue line*) and MHBs watermarked meshes (*solid green line*). (**b**) shows the ROC curve in which the x-axis is plotted in logarithmic scale

Table 5 Robustness comparisons, i.e., ER (%) under combination attacks, where "crop." means mesh cropping, "0.1 sim." and "0.3 sim." mean 10% and 30% mesh simplification, respectively, "LS" means Laplacian smoothing for three steps, and "Loop" means Loop subdivision. Note that original mesh is used for the mesh alignment and re-sampling steps in LBFs and MHBs while watermarked mesh is used in RBFs

Models	Types	crop. +0.1 sim.	0.3 sim. +Loop	crop. +0.1 sim. +Loop	0.3 sim. +Loop +LS
eros	RBFs	53.09	66.67	54.32	63.58
	LBFs	99.69	84.88	52.78	62.65
	MHBs	100	**87.35**	**63.58**	**65.74**
Asia	RBFs	51.85	62.35	53.09	57.72
dra.	LBFs	92.59	66.98	57.41	59.57
	MHBs	100	**95.99**	**63.27**	**80.56**

appropriate threshold can be chosen as 56.1%. Figure 11(b) shows the ROC curve in which the x-axis is plotted in logarithmic scale. Therefore, Fig. 11 shows that the proposed algorithm has a good performance.

6 Conclusions and future work

In this paper,we proposed a robust non-blind confirmable spectral watermarking algorithm of two-manifold mesh by combining manifold harmonics basis and elliptic curve digital signature algorithm. Meanwhile, because only a minimal number of MHB functions for watermark embedding is computed, our algorithm can watermark a large-scale 3D mesh with millions of vertices. To compensate for the shape distortion introduced by the truncation of frequency spectrum, the reconstruction difference is added to the watermarked mesh. To improve the robustness, the signature bits are embedded into all segmented patches in an absolute embedding manner and extracted according to the corresponding variations of their coefficients. Through detailed comparisons among LBFs, RBFs, and the proposed algorithm for different scale meshes, the proposed algorithm is shown to have better visual quality and robustness. The LBFs and RBFs algorithms can also be improved by fully adopting our framework.

In the future, we will investigate how to resist global mesh deformation attacks in our watermarking framework. It is also interesting to extend our work to the watermark-

Author's personal copy

ing algorithm for CAD models and the blind watermarking algorithm for 3D meshes.

Acknowledgements This work is supported by the National Natural Science Foundation of China under Grant Nos. 60933007 and 60736019, the 973 program of China under Grant No. 2009CB320801, the Program for New Century Excellent Talents in University under Grant No. NCET-10-0728, and the Natural Science Foundation of Zhejiang Province under Grant No. Y1100837. We wish to thank Sivan Toledo for providing us the latest TAUCS package. The 3D models are courtesy of the Aim@Shape Shape repository and the Stanford 3D scanning repository.

Appendix: Proof of Theorem 1

Proof For $0 \le k \le m_1 - 1$, the corresponding eigenvalues are equal in $\boldsymbol{MHB^{(m_1)}}$ and $\boldsymbol{MHB^{(m_2)}}$, and then

$$\bar{\boldsymbol{H}}^{\boldsymbol{k,m_1}} = \bar{\boldsymbol{H}}^{\boldsymbol{k,m_2}}. \tag{25}$$

Take $\tilde{\boldsymbol{x}}$ component in spectral space as the example, and let $\tilde{x}_k^{(m_1)}$ and $\tilde{x}_k^{(m_2)}$ be the spectral coefficients of the mesh transformed by $\boldsymbol{MHB^{(m_1)}}$ and $\boldsymbol{MHB^{(m_2)}}$, respectively. Then

$$\begin{aligned}\Delta x_i^{(m_1)} &= \sum_{k=0}^{\infty} \tilde{x}_k^{(m_1)} \bar{H}_i^{k,m_1} - \sum_{k=0}^{m_1-1} \tilde{x}_k^{(m_1)} \bar{H}_i^{k,m_1} \\ &= \sum_{k=m_1}^{\infty} \tilde{x}_k^{(m_1)} \bar{H}_i^{k,m_1} \\ \Delta x_i^{(m_2)} &= \sum_{k=0}^{\infty} \tilde{x}_k^{(m_2)} \bar{H}_i^{k,m_2} - \sum_{k=0}^{m_2-1} \tilde{x}_k^{(m_2)} \bar{H}_i^{k,m_2} \\ &= \sum_{k=m_2}^{\infty} \tilde{x}_k^{(m_2)} \bar{H}_i^{k,m_2}.\end{aligned}$$

After the embedding process using (12) and (13), we have

$$\begin{aligned}x_i^{(m_1)} &= \tilde{x}_0^{(m_1)} \bar{H}_i^{0,m_1} + \sum_{k=1}^{m_1-1} (\tilde{x}_k^{(m_1)} + \alpha s''_{3(k-1)} \varphi_x) \bar{H}_i^{k,m_1} \\ &\quad + \Delta x_i^{(m_1)}.\end{aligned}$$

By induction,

$$x_i^{(m_1)} = x_i + \alpha \varphi_x \sum_{k=1}^{m_1-1} s''_{3(k-1)} \bar{H}_i^{k,m_1}. \tag{26}$$

For the same reason, then,

$$x_i^{(m_2)} = x_i + \alpha \varphi_x \sum_{k=1}^{m_1-1} s''_{3(k-1)} \bar{H}_i^{k,m_2}. \tag{27}$$

According to (25), we have $x_i^{(m_1)} = x_i^{(m_2)} (0 \le i \le n-1)$. It is the same for the $\boldsymbol{y}$ and $\boldsymbol{z}$ coordinate vectors. Thus, $M_S^{(m_1)} = M_S^{(m_2)}$. □

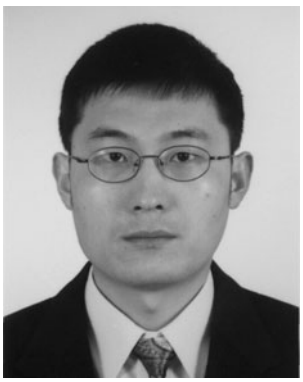
References

1. Schneier, B.: Applied Cryptography: Protocols, Algorithm, and Source Code in C, 2nd edn. Wiley, New York (1996)
2. Xie, L., Arce, G.R.: A class of authentication digital watermarks for secure multimedia communication. IEEE Trans. Image Process. **10**(11), 1754–1764 (2001)
3. Wang, K., Lavoue, G., Denis, F., Baskurt, A.: Three-dimensional meshes watermarking: review and attack-centric investigation. In: Information Hiding, pp. 50–64 (2007)
4. Cox, I.J., Miller, M.L., Bloom, J.A., Fridrich, J., Kalker, T.: Digital Watermarking and Steganography, 2nd edn. Morgan Kaufmann, San Francisco (2008)
5. Wang, K., Lavoue, G., Denis, F., Baskurt, A.: A fragile watermarking scheme for authentication of semi-regular meshes. In: Proc. of EUROGRAPHICS 2008, pp. 5–8 (2008)
6. Wang, Y.P., Hu, S.M.: A new watermarking method for 3D model based on integral invariant. IEEE Trans. Vis. Comput. Graph. **15**(2), 285–295 (2009)
7. Wang, Y.P., Hu, S.M.: Optimization approach for 3D model watermarking by linear binary programming. Comput. Aided Geom. Des. **27**(5), 395–404 (2010)
8. Wang, W.B., Zhang, G.Q., Yong, J.H., Gu, H.J.: A numerically stable fragile watermarking scheme for authenticating 3D models. Comput. Aided Des. **40**(5), 634–645 (2008)
9. Ohbuchi, R., Masuda, H., Aono, M.: Watermarking three-dimensional polygonal meshes. In: Proc. of ACM Multimedia 1997, pp. 261–272 (1997)
10. Harte, T., Bors, A.: Watermarking 3D models. In: Proc. of IEEE International Conference on Image Processing, pp. 661–664 (2002)
11. Ohbuchi, R., Masuda, H., Aono, M.: Watermarking three-dimensional polygonal models through geometric and topological modifications. IEEE J. Sel. Areas Commun. **16**(4), 551–559 (1998)
12. Benedens, O.: Two high capacity methods for embedding public watermarks into 3D polygonal models. In: Proc. of Multimedia and Security-workshop at ACM Multimedia, pp. 95–99 (1999)
13. Benedens, O.: Geometry-based watermarking of 3D models. IEEE Comput. Graph. Appl. **19**(1), 46–55 (1999)
14. Bors, A.G.: Watermarking mesh-based representations of 3D objects using local moments. IEEE Trans. Image Process. **15**(3), 687–701 (2006)
15. Kanai, S., Date, H., Kishinami, T.: Digital watermarking for 3D polygons using multiresolution wavelet decomposition. In: Proc. of the Sixth IFIP WG 5.2 International Workshop on Geometric Modeling, pp. 296–307 (1998)
16. Praun, E., Hoppe, H., Finkelstein, A.: Robust mesh watermarking. In: Proc. of SIGGRAPH 1999, pp. 69–76 (1999)
17. Yin, K., Pan, Z., Shi, J.: Robust mesh watermarking based on multiresolution processing. Comput. Graph. **25**(3), 409–420 (2001)
18. Levy, B., Zhang, H.: Spectral geometry processing. In: Proc. of ACM SIGGRAPH Asia (2009), Course Notes (2009)
19. Ohbuchi, R., Takahashi, S., Miyazawa, T., Mukaiyama, A.: Watermarking 3D polygonal meshes in the mesh spectral domain. In: Proc. of Graphics Interface 2001, pp. 9–17 (2001)
20. Ohbuchi, R., Mukaiyama, A., Takahashi, S.: A frequency domain approach to watermarking 3D shapes. Comput. Graph. Forum **21**(3), 373–382 (2002)

Author's personal copy

21. Wu, H.T., Kobbelt, L.: Efficient spectral watermarking of large meshes with orthogonal basis functions. Vis. Comput. **21**(8), 848–857 (2005)
22. Wang, J., Feng, J., Miao, Y., Pan, H.: A robust public-key non-blind watermarking algorithm for 3D mesh based on radial basis functions. J. Comput.-Aided Des. Comput. Graph. **23**(1), 21–31 (2011)
23. Liu, Y., Prabhakaran, B., Guo, X.: A robust spectral approach for blind watermarking of manifold surfaces. In: Proc. of ACM Multimedia and Security Workshop, pp. 43–52 (2008)
24. Wang, K., Luo, M., Bors, A.G., Denis, F.: Blind and robust mesh watermarking using manifold harmonics. In: Proc. of the IEEE International Conference on Image Processing, pp. 211–215 (2009)
25. Luo, M., Wang, K., Bors, A.G., Lavoue, G.: Local patch blind spectral watermarking method for 3D graphics. In: Proc. of the International Workshop on Digital Watermarking, pp. 211–226 (2009)
26. Vallet, B., Levy, B.: Spectral geometry processing with manifold harmonics. Technical Report, ALICE-2007-001 (2007)
27. Sorensen, D.C., Lehoucq, R.B., Yang, C., Maschhoff, K.: http://www.caam.rice.edu/software/ARPACK/ (2011)
28. Toledo, S., Chen, D., Rotkin, V.: http://www.tau.ac.il/~stoledo/taucs/ (2011)
29. Johnson, D., Menezes, A., Vanstone, S.: The elliptic curve digital signature algorithm (ECDSA). Int. J. Inf. Secur. **1**(1), 36–63 (2001)
30. Karypis, G., Kumar, V.: MeTiS: a software package for partitioning unstructured graphs, partitioning meshes, and computing fill-reducing orderings of sparse matrices version 4.0. University of Minnesota, Department of Computer Science (1998)
31. IEEE P1363-2000: IEEE Standard Specifications for Public-key Cryptography. IEEE Computer Society, Los Alamitos (2000)
32. FIPS 180-3: Secure hash standard. National Institute of Standards and Technology (2008)
33. ANSI/X9.62-2005: The elliptic curve digital signature algorithm (ECDSA). Public Key Cryptography for the Financial Services Industry (2005)
34. Besl, P., McKay, J.: A method for registration of 3D shapes. IEEE Trans. Pattern Anal. Mach. Intell. **14**(2), 239–255 (1992)
35. Aiger, D., Mitra, N.J., Cohen-Or, D.: 4-points congruent sets for robust pairwise surface registration. ACM Trans. Graph. **27**(3), 1–10 (2008)
36. Cignoni, P., Rocchini, C., Scopigno, R.: Metro: measuring error on simplified surfaces. Comput. Graph. Forum **17**(2), 167–174 (1998)
37. Aspert, N., Santa-Cruz, D., Ebrahimi, T.: Mesh: measuring error between surfaces using the hausdorff distance. In: Proc. of IEEE International Conference on Multimedia and Expo, pp. 705–708 (2002)
38. Corsini, M., Gelasca, E.D., Ebrahimi, T., Barni, M.: Watermarked 3D mesh quality assessment. IEEE Trans. Multimed. **9**(2), 247–256 (2007)
39. Lavoue, G., Gelasca, E.D., Dupont, F., Baskurt, A., Ebrahimi, T.: Perceptually driven 3D distance metrics with application to watermarking. In: Proc. of SPIE Applications of Digital Image Processing, pp. 6312, 63120L.1-63120L. 12 (2006)
40. Reuter, M., Wolter, F.-E., Peinecke, N.: Laplace-Beltrami spectra as "Shape-DNA" of surfaces and solids. Comput. Aided Des. **38**(4), 342–366 (2006)
41. Garland, M., Heckbert, P.S.: Surface simplification using quadric error metrics. In: Proc. of SIGGRAPH 1997, pp. 209–216 (1997)
42. http://meshlab.sourceforge.net/ (2011)
43. http://www.rapidform.com/ (2011)

Jinrong Wang is a Ph.D. candidate in the State Key Lab of CAD&CG, Zhejiang University, Peoples Republic of China. He received his M.Sc. in cryptography theory and practices from Hangzhou Dianzi University in 2004. His research interests include digital geometry processing, digital watermarking, and information security.



Jieqing Feng is a professor in the State Key Lab of CAD&CG, Zhejiang University, Peoples Republic of China. He received his B.Sc. in applied mathematics from the National University of Defense Technology in 1992 and his Ph.D. in computer graphics from Zhejiang University in 1997. His research interests include geometric modeling, real-time rendering, and computer animation.

Yongwei Miao is an associate professor in the College of Computer Science and Technology, Zhejiang University of Technology, P.R. China. He received his Ph.D. degree in computer graphics from the State Key Lab of CAD&CG, Zhejiang University. From February 2008 to February 2009, he was a visiting scholar at University of Zurich, Switzerland. His research interests include virtual reality, digital geometry processing and non-photo-realistic rendering.