A ROBUST BLIND WATERMARKING FOR 3D MESHES USING DISTRIBUTION OF SCALE COEFFICIENTS IN IRREGULAR WAVELET ANALYSIS

Min-Su Kim[1,2], Jae-Won Cho[1,2], Ho-Youl Jung[2] and Rémy Prost[1]

[1]CREATIS, INSA-Lyon, CNRS UMR 5515, INSERM U630, 69100, Villeurbanne, France*
[2]MSP Lab., Yeungnam Univ., 214-1 Dae-dong, Gyeongsan-si, 712-749, Gyeongsangbuk-do, Korea†

ABSTRACT

We propose a new method for watermarking of 3D surface mesh. After *irregular wavelet analysis*, the watermark is embedded in the *scale coefficients*. We modify the mean of the distribution of the vertex norm of the approximation mesh in order to obtain *blind scheme* which does not require the original mesh for detection. Experimental results show the effectiveness of the proposed algorithm both in terms of invisibility and robustness against simplification and progressive lossy compression.

1. INTRODUCTION

In these last years digital watermarking has allowed great possibility as a DRM (Digital Right Management) technique. Unlike traditional data protection techniques such as encryption, digital watermarking does not restrict access to the host data, but ensures the hidden data to remain inviolate and recoverable. Watermarking provides a mechanism for copyright protection by embedding information, so-called watermark, into host data [1].

In general, there are two different classes according to the application. Fragile and semi-fragile watermarking is used for checking content authenticity or integrity and highlight the region that have been tampered with. In copyright protection, the watermark should be perceptually invisible and robust against various copyright attacks. Robust watermarking has been investigated for this [2–5]. The watermarking system also can be classified into informed detection and blind detection according to detection procedure. It has been known that blind detection schemes are less robust than informed schemes but they are more useful for most applications as they do not require the host signal for their detection procedure [1].

Kanai *et al.* [2] proposed non-blind watermarking by modifying the wavelet coefficients from semi-regular wavelet analysis. Uccheddu *et al.* [3] extended [2] to blind watermarking. The downside of two methods is that only a semi-regular mesh could be available because of the limitation of the 4:1 subdivision connectivity in Lounsbery's scheme [6]. They can embed the watermark into an irregular mesh by using remeshing that converts an irregular mesh into a semi-regular one. However, the remeshed model can not be seen as the original, as it corresponds to a different sampling of the underlying 3D surface: the mesh connectivity is different from the original.

In our prior work [4], we proposed spread-spectrum approach [1] for both semi-regular and irregular meshes by using wavelet transform. We used the irregular wavelet multiresolution analysis [7] to solve the subdivision connectivity problem in [2, 3]. Although irregular wavelet analysis has a good performance for both semi-regular and irregular meshes, there still exists an open question for the watermarking, so-called, global synchronization of the mesh. Unlike discrete wavelet transform of 2D images, the wavelet coefficients of 3D meshes depend on the seed-triangle group merged during connectivity graph simplification. This artifact results from both irregular sampling and unusual scanning of the 3D surface. In addition, although the lossless reconstruction of integer coordinates meshes is possible and the reconstructed mesh is exact in terms of geometry, the original vertex indices are lost when processing with the irregular wavelet analysis [7]. Even regular wavelet analysis can not avoid the global synchronization after reconstruction. This is not a problem for the application of visualization, but it is critical for the applications such as copyright protection or content authentication. We solved the problem by using the reordering algorithm before and after the wavelet transform, and we could obtain the exact index order of the vertices and faces. The method does not use the original mesh during extraction and can embed over than 315 bits into wavelet coefficients norms on Stanford Bunny model. It was robust against various geometrical attacks such as additive noise, smoothing, affine transform, and distortion-less topological attacks such as random reordering.

Previous works [2–4] which are based on wavelet transform have a weakness against topological attacks. It is caused by the limitation of subdivision connectivity of semi-

*{kim, cho, prost}@creatis.insa-lyon.fr
†This work was supported by the Ministry of Information & Communications, Korea, under the Information Technology Research Center (ITRC) Program (204-B-000-215). hoyoul@yu.ac.kr

regular wavelet analysis or by the synchronization of wavelet coefficients.

In this paper, we extend our previous method [4] to be robust against topological attacks. In sharp contrast with our previous paper, we do not embed the watermark into the wavelets coefficients but into the scale coefficients (e.g. the approximated mesh) which is less sensitive to topological attacks. We modify the mean of the distribution of vertex norms of the approximation mesh. Our method adjusts the distribution by given threshold according to binary watermark in order to obtain a blind scheme which does not require the original mesh for detection.

The rest of this paper is organized as follows. In Section 2, we describe briefly irregular wavelet transform. Watermarking embedding and extraction are presented in Section 3. Simulation results show the effectiveness of our proposal in Section 4. Finally, we draw a conclusion.

2. BACKGROUND

Irregular wavelet analysis scheme [7] simplifies the original mesh by reversing an irregular subdivision scheme. The simplification is repeated until the resulting mesh cannot be simplified anymore. For meshes homeomorphic to a sphere, the simplest mesh is a tetrahedron. We obtain a hierarchy of meshes from the simplest one M^0, called base mesh, to the original mesh M^J. Following [7], the wavelet decomposition can be applied to the geometry of the different meshes which are linked by the following matrix relations:

$$C^{j-1} = A^j C^j \tag{1}$$

$$D^{j-1} = B^j C^j \tag{2}$$

$$C^j = P^j C^{j-1} + Q^j D^{j-1} \tag{3}$$

where C^j is the $v^j \times 3$ matrix representing the coordinates of the scale coefficients at the resolution level j, v^j is the number of vertices for each mesh M^j. D^{j-1} is the $(v^j - v^{j-1}) \times 3$ matrix of the wavelet coefficients at level j. A^j and B^j are the analysis filters, P^j and Q^j are the synthesis filters. Valette's scheme [7] attempt to inverse the connectivity simplification to 1:4 subdivision as much as possible. This is for semi-regular regions in the irregular input meshes. If 4:1 simplification is not possible, it will be merged in groups of three or two faces, or leave some faces unchanged. Edge flips are performed when needed. In addition, starting from the Lazy wavelet filter-bank (Eq. (1) - (3)) following [6] we build new filters A^j, Q^j by the Lifting scheme in order to make the wavelet functions more orthogonal to the scaling functions in the 1-ring.

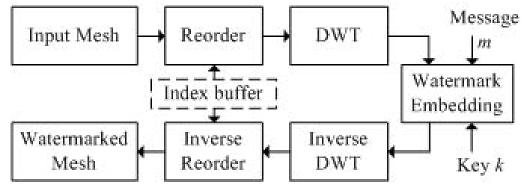


Fig. 1. Watermark embedding

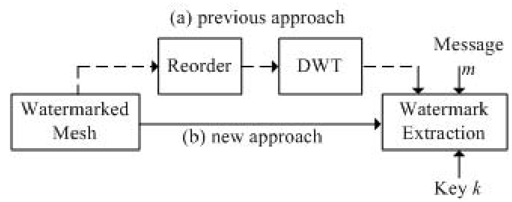


Fig. 2. Watermark extraction for (a) previous approach [4] (b) new approach

3. PROPOSED WATERMARKING METHOD

3.1. Watermark Embedding

After we compute forward wavelet transform of the mesh, we obtain the scale coefficient vector C^{j-1} from Eq. (1) as follows,

$$C^{j-1} = [\, c_0,\ c_1, \dots\ ,\ c_{I-1}\,]^t \tag{4}$$

where, $c_i = [x_i\ y_i\ z_i]^t$ and I is the number of scale coefficients. In the following we omit the resolution level $j-1$ for the sake of notational simplicity.

We convert the Cartesian coordinates of c_i to spherical coordinates $[\rho_i\ \theta_i\ \phi_i]$, where ρ_i denotes vertex norm of c_i. Then, the probability distribution is divided into N distinct bins with equal range, according to their magnitude. Each bin is used independently to hide one bit of watermark. The maximum ρ_{max} and the minimum ρ_{min} are calculated prior to build N bins from the vertex norms. After, vertex norms belonging to the n-th bin are mapped into the normalized range of $[0, 1]$. The attached random variable is now noted x_n.

The next step of the proposed watermark embedding is to shift the mean value of each bin via transforming vertex norms by the histogram mapping function ($y_n = x_n^{k_n}$ for $0 < k_n < \infty$ and $k_n \in \mathbb{R}$). We use a binary bit sequence as the watermark ($\omega_n \in \pm 1$). The distribution moves to the left ($\omega_n = -1$) or to the right($\omega_n = +1$) by given threshold. The threshold is determined as the mean of the uniform distribution in the range of [0,1]. Then the mean of each bin, $\widetilde{\mu}'_n$, is changed by

$$\widetilde{\mu}'_n = \frac{1}{2} + \alpha\, \omega_n \tag{5}$$

, where α ($0 < \alpha < \frac{1}{2}$) is the strength factor that can control the robustness and the transparency of watermark. The exact parameter k_n can be found by computing the expectation of n-th bin and it results:

$$k_n = \frac{1 - 2\,\alpha\,\omega_n}{1 + 2\,\alpha\,\omega_n} \tag{6}$$

Note that k_n exists in the range of $]0, 1[$ when the watermark bit is $+1$, and k_n does in the range of $]1, \infty[$ when watermark bit is -1. In reality, the vertex norm distribution in each bin is not continuous nor uniform. Then the parameter k_n cannot be calculated by Eq. 6. To overcome this difficulty we use an iterative approach by decreasing k_n when the watermark bit is $+1$ or by increasing k_n when the watermark bit is -1. Note that the $y_n = x^{k_n}$ mapping prevent interference between bins. All transformed vertex norms in each bin are mapped onto the original range and after shifting the distribution.

Finally, the watermark embedding process is completed by combining all of the bins and converting the spherical coordinates to Cartesian coordinates.

3.2. Watermark Extraction

In our previous work [4], we extract the watermark after reordering and wavelet transform as shown in Fig. 2(a). We propose a new method to extract the watermark directly from the attacked mesh as in Fig. 2(b).

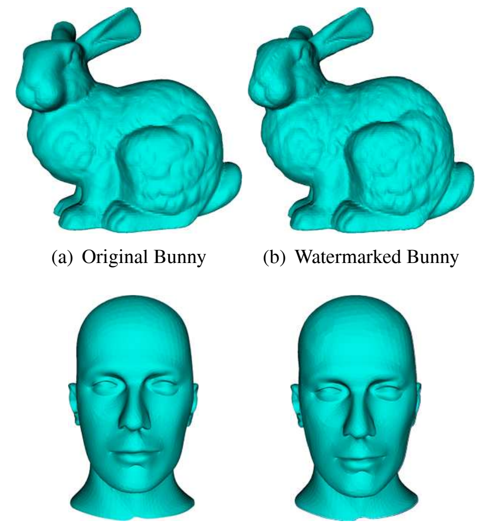
First Cartesian coordinates of the attacked mesh are converted to spherical coordinates. After finding the maximum and minimum vertex norms, the vertex norms are classified into N bins and mapped onto the normalized range of $[0, 1]$. Then, the mean of each bin, $\widetilde{\mu}''_n$ is calculated and compared to the threshold, $\frac{1}{2}$. The watermark hidden in the n-th bin, ω''_n, is extracted by means of

$$\omega''_n = \begin{cases} +1, & \text{if } \widetilde{\mu}''_n > \frac{1}{2} \\ -1, & \text{if } \widetilde{\mu}''_n < \frac{1}{2} \end{cases} \tag{7}$$

Note that the watermark detection process does not require the original meshes.

4. EXPERIMENTAL RESULTS

In this section, we demonstrate the experimental results to show the effectiveness of our proposal. We use Stanford Bunny (34,834 vertices and 69,451 faces) and Head (10,196 vertices, 20,261 faces). We embedded the watermark on C^{J-1}. A watermark of 64 bits is embedded into a Bunny model and a watermark of 32 bits is embedded into a Head model. These watermark lengths are no longer than our previous work [4], but note that we do not use the original mesh during extraction. The resulting models are presented in Fig. 3. The strength factors are 0.07 for Bunny and 0.055 for Head model. We could recover the exact message without an attack.



(a) Original Bunny (b) Watermarked Bunny

(c) Original Head (d) Watermarked Head

Fig. 3. Test models

Fig. 4 depicts the robustness results as linear correlation between the original message and the designated one. Note that, we only considered simplification and lossy compression in this paper. *WaveMesh* [8] was applied according to different quantization steps (bits/coordinate) for lossy compression in Fig. 4(a).

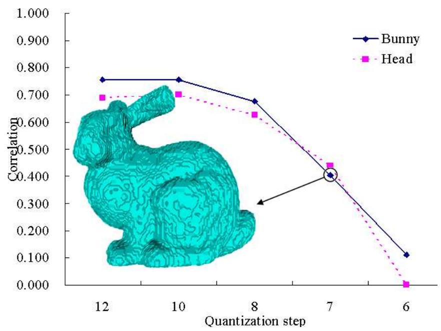
Simplification in Fig. 4(b) is done by using quadric error metrics [9]. Fig. 4(c) yields the result from combined attack of quantization and simplification (63% for Bunny, 75% for Head) by *WaveMesh* [8].

In Fig. 5, Our method was analyzed by ROC (Receiver Operating Characteristic) curve that represents the relation between probability of false rejections P_{fr} and probability of false alarms P_{fa} varying the decision threshold to declare the watermark present. The probability density functions for P_{fr} and P_{fa} were measured experimentally with 100 correct and 100 wrong keys, and approximated to Gaussian distribution. We used the Bunny model as used in Fig. 4(c). EER(Equal Error Rate) is also indicated in this figure.

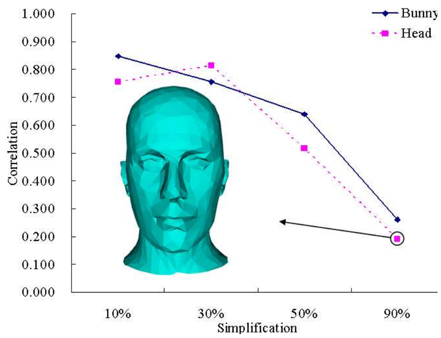
Since the contour of the probability distribution is not altered a lot after uniform quantization and simplification, we can fairly extract the watermark.

5. CONCLUSION

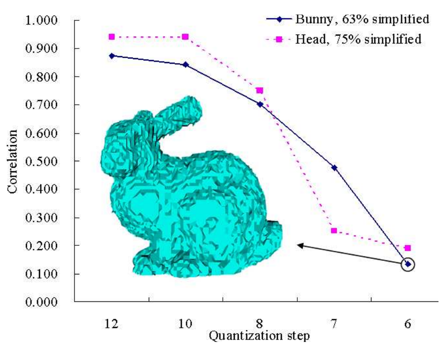
A robust blind watermarking method has been proposed in this paper. We embed the watermark into the scale coefficients from the approximated mesh by the irregular wavelet analysis. We modify the mean of the distribution of the



(a) Quantization



(b) Simplification



(c) Quantization + Simplification

Fig. 4. Robustness against attacks

approximation mesh in order to diminish sensitivity from topological attacks. All the vertex norms in each bin are modified by a histogram mapping function to prevent interference between the modified bins. Experimental results indicate the pertinence of the proposed algorithm in copyright protection of 3D models.

6. REFERENCES

[1] I. Cox, M. L. Miller, and J. A. Bloom, *Digital watermarking*, Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2002.

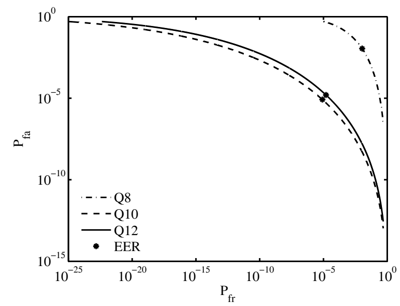


Fig. 5. ROC curves of Bunny model for 63% simplification and quantizations

[2] S. Kanai, D. Date, and T. Kishinami, "Digital watermarking for 3d polygon using multiresolution wavelet decomposition," in *Proc. Sixth IFIP WG 5.2 GEO-6*, Tokyo, Japan, December 1998, pp. 296–307.

[3] F. Uccheddu, M. Corsini, and M. Barni, "Wavelet-based blind watermarking of 3d models," in *Proceedings of the 2004 multimedia and security workshop on Multimedia and security*. 2004, pp. 143–154, ACM Press.

[4] M. S. Kim, S. Valette, H. Y. Jung, and R. Prost, "Watermarking of 3d irregular meshes based on wavelet multiresolution analysis," *Lecture Notes in Computer Science*, vol. 3710, pp. 313–324, September 2005.

[5] J. W. Cho, M. S. Kim, R. Prost, H. Y. Chung, and H. Y. Jung, "Robust watermarking on polygonal meshes using distribution of vertex norms," *Lecture Notes in Computer Science*, vol. 3304, pp. 283–293, March 2005.

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

[7] S. Valette and R. Prost, "Multiresolution analysis of irregular surface meshes," *IEEE Trans. Visual. Comput. Graphics*, vol. 10, no. 2, pp. 113–122, Mar-Apr 2004.

[8] S. Valette, A. Gouaillard, and R. Prost, "Compression of 3d triangular meshes with progressive precision," *Computer & Graphics, Special Issue on Compression*, vol. 28, no. 1, pp. 35–42, February 2004.

[9] M. Garland and P. S. Heckbert, "Surface simplification using quadric error metrics," in *SIGGRAPH '97*, New York, NY, USA, 1997, pp. 209–216, ACM Press/Addison-Wesley Publishing Co.