A ROBUST 3D MESH WATERMARKING SCHEME AGAINST CROPPING

Seung-Min Mun, Han-Ul Jang, Do-Gon Kim, Sunghee Choi, Heung-Kyu Lee †

School of Computing
Korea Advanced Institute of Science and Technology
Republic of Korea

ABSTRACT

Various watermarking schemes achieved the robustness against the usual operations such as simplification, remeshing and noise addition. However, the techniques were not robust against cropping, nevertheless the cropping attack is commonly performed by general editing. In this paper, we propose a robust 3D mesh watermarking method against cropping. We achieve the blind watermarking scheme involving consistent segmentation and the scheme improves the robustness against cropping. The experimental results show that the proposed method achieves higher performance than the previous 3D mesh watermarking methods.

Index Terms— Blind watermarking, 3D mesh, cropping, vertex norm, segmentation.

1. INTRODUCTION

Watermarking is used to identify protect ownership of the copyright of media contents by embedding invisible data into original contents. Watermarking is considered as the only way to protect the copyright of media data instead of digital rights management (DRM) because DRM can be erased and a number of digital contents are freely shared without DRM today on the Internet. Therefore, watermarking becomes the ultimate prevention measure from illegal redistribution on the Internet.

Recently, prevalence of 3D printer boosted an increase of 3D model applications. As a result, new watermarking scheme combining with 3D meshes becomes important. A 3D mesh watermarking scheme should be robust against attacks that modifies the shape of models directly or changes the representation of the mesh data without any shape distortions. The former is called distortion attack and the latter is called distortion-less attack. Existing non-blind schemes which utilize side information depending on the given mesh have a certain level of robustness against these attacks [1][3]. However, these non-blind schemes are not appropriate for practical use in real world because the techniques require additional data for every mesh. Hence, in this paper, we propose a blind watermarking scheme focused on cropping attack which is appropriate for utilization in real world.

Cropping is generally to remove a certain part from the original content. Cropping on 3D meshes is commonly performed by general editing, however, it strongly breaks the synchronization of watermarks. For example, a user can crop out the head from a 3D figure A and replace it with the model of his/her own head B. Then the user can assert that the combined 3D figure is his/her own creation because the watermarks of the 3D figure A cannot be extracted. This attack significantly violates the integrity of watermarks. However, only few papers have focused on this issue because it is too difficult to solve with blind schemes [14-16].

The 3D mesh watermarking method based on volume moments [4] computes the center of mass from m_{000}, m_{100}, m_{010} and m_{001}, but the set of patches are gained incorrectly when a small part of model is cropped. The scheme based on surface parameterization [5] endures against cropping only when the cropping performed on a tiny part since cropping attack affects the whole spectral domain. The scheme with double watermarking was proposed [6]. The paper focuses on the cropping but built on the assumption that consistent segmentation are achieved after cropping. Besides, the method requires additional watermarking scheme for robustness while our proposed scheme is more robust against cropping without any second watermark.

In this paper, we present a new blind mesh watermarking which is robust against cropping and other general attacks. The scheme includes consistent segmentation and watermarking procedure for each segment. The watermark sequence is embedded for all the segments repeatedly in 3D model.

The outline of the paper is as following: Section 2 describes the consistent segmentation algorithm used in this paper. Section 3.1 demonstrates an overview of the proposed method with the block diagrams for embedding and extraction. Section 3.2 and 3.3 explains the detailed embedding and extraction procedure, respectively. Section 4 discusses the results obtained from the proposed scheme with cropping and other attacks. Finally, Section 5 concludes the paper.

†: Corresponding Author:hklee@mmc.kaist.ac.kr

978-1-5090-1265-7/15/$31.00 ©2015 IEEE

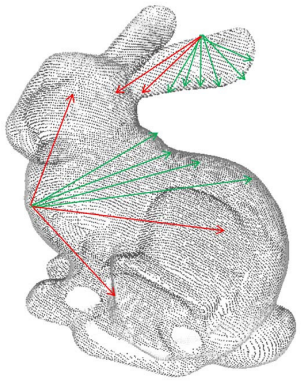


Fig. 1. An example of the SDF calculation in mesh model "bunny". For each surface point, the length of cone-shaped rays bring the SDF value where green rays mean the acceptable length.

2. SEGMENTATION BASED ON SDF

To endure attacks with distortion or watermark embedding, the segmentation should be maintaining consistency, otherwise the synchronization could be failed. In this paper, surface diameter function (SDF) – segmentation [9] is used because the computation of SDF is faster and more precise than the traditional indicator called medial axis transform (MAT) while both function values are used inside the segmentation process.

SDF can be calculated by shooting the wide cone-shaped rays inward to gain weighted average of the lengths. And this value is determined for each face of 3D mesh. The segmentation is mainly dependent on this mapping while some additional information like connectivity or normal is exploited. First, the distribution of the surface diameter (SD) values gets fitting with Gaussian mixture model (GMM) by performing EM algorithm [10]. Secondly, thresholding and k-way graph-cut algorithm decide the final segmentation. We can adjust the parameters about smoothing factor and the number of component of GMM so that the size of partition can be controlled. Coarser partitioning is more helpful for watermarking because it tends to be noise-tolerant.

3. PROPOSED METHOD

3.1. The overview of the proposed method

For the embedding, SDF based segmentation is performed to gain (face, segment) pair, then a watermark bit is inserted into each bin of the histogram of vertex-norm distribution. The detail of bit insertion is following in Section 3.2. Similarly, for each segment are used to extract the watermark sequence and throw the final decision based on the set of sequences by using majority voting system (MVS) [11]. Again, the cropping-robustness is achieved with consistent segmentation and the modification of the method

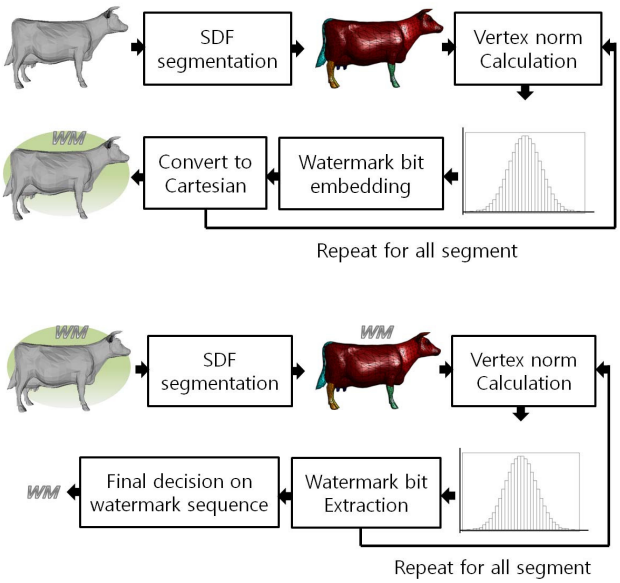


Fig 2. Block diagram for embedding (top) and extracting (bottom) procedure.

of Cho et al. [2].

3.2. Watermark embedding

The embedding procedure is as following:

Step 1. Get (face, segmentation) paring by performing SDF-segmentation to the model.

Step 2. Divide the vertex set into N disjoint sub vertex set V_n using the pairs in Step 1.

Step 3. Normalize each V_n by subtracting center of mass.

Step 4. Convert to spherical coordinate system.

Step 5. Get a vertex norm histogram.

Step 6. Insert a bit into each bin. Bit "1" insertion is performed as following loop:

$$\begin{aligned} &while(mean[V_{n,i}] < 1+\alpha): \\ &k = k - \triangle k \\ &V_{n,i} = \{v^k \mid v \in V_{n,i}\} \\ &endwhile \end{aligned} \tag{1}$$

And bit "0" insertion is performed as following:

$$\begin{aligned} &while(mean[V_{n,i}] > 1-\alpha): \\ &k = k + \triangle k \\ &V_{n,i} = \{v^k \mid v \in V_{n,i}\} \\ &endwhile \end{aligned} \tag{2}$$

where $V_{n,i}$ is the set of the vertex norms in the i-th bin normalized to [0,1].

Step 7. For each V_n, reconstruct the original coordinate and complete the watermarked model.

Table 1 Baseline evaluations of the proposed scheme.

Model		elephant	bunny	horse	Man
Time(s)	Segmentation	22.51	21.77	12.7	24.15
	Embedding	1.088	1.141	0.922	1.464
Time(s)	Segmentation	22.72	25.55	12.5	24.35
	Extracting	0.314	0.260	0.194	0.205
MRMS		0.172	0.020	0.181	24.62

Table 2 Robustness against uniform quantization attacks for each vertex coordinate

Model	Bit	BER	Corr
bunny	7	0.0625	0.8704
	8	0.0625	0.8704
	9	0	1
elephant	7	0.25	0.4667
	8	0.0625	0.8783
	9	0	1
horse	7	0	1
	8	0	1
	9	0	1
armadillo	7	0.0625	0.8704
	8	0	1
	9	0	1

3.3. Watermark extraction

The extraction procedure is as following:
Step 1-5. The same as embedding.
Step 4. Determine the watermark bit from the each bin by computing the mean.
Step 5. Make a three different candidate for watermark sequence.
Step 6. By applying MVS to each bit, throw the final decision. The MVS procedure is as following:

$$\begin{aligned} e_1 &= sign(\sum w_n) \\ e_2 &= \underset{w_j}{\operatorname{argmin}}\{\mathrm{BER}(e_1, w_j)\} \\ e_3 &= \underset{w_j}{\operatorname{argmin}}\{\sum BER(w_n, w_j)\} \\ e_4 &= sign(e_1 + e_2 + e_3) \end{aligned} \quad (3)$$

where w_n is the extracted watermark sequence from the n-th segment and e_4 is the final decision.

4. EXPERIMENTAL RESULTS

4.1. Experimental setup

Consistent segmentation procedure used CGAL 4.6 to produced paired .txt file for given .off mesh. For SDF, parameter set with k=4 and smoothing factor=0.7 was used for coarser segmentation. The length of watermark sequence

Table 3 Robustness against Laplacian smoothing (λ =0.03)

Model	Iteration	BER	Corr
bunny	10	0	1
	30	0.0625	0.8704
	50	0.3125	0.4229
elephant	10	0	1
	30	0.0625	0.8783
	50	0.3125	0.3578
horse	10	0	1
	30	0	1
	50	0.125	0.7333
armadillo	10	0	1
	30	0.3125	0.3578
	50	0.25	0.4667

Table 4 Robustness against surface simplification

Model	Reduction ratio (%)	BER	Corr
bunny	25	0.25	0.4667
	50	0.4375	0.0976
	(Uniform)70	0.375	0.2582
	(Uniform)90	0.4375	0.0976
	(Uniform)95	0.4375	0.0976
elephant	25%	0.5625	-0.0976
	50%	0.1875	0.5919
	(Uniform)70	0.4375	0.0976
	(Uniform)90	0.5	-0.0667
	(Uniform)95	0.5625	-0.1627
horse	25	0.1875	0.6180
	50	0.4375	0.1627
	(Uniform)70	0.5625	-0.24371
	(Uniform)90	0.4375	0.1627
	(Uniform)95	0.375	0.3333
armadillo	25	0.375	0.2582
	50%	0.5	0.0667
	(Uniform)70%	0.25	0.5164
	(Uniform)90%	0.5625	0.0898
	(Uniform)95%	0.5625	-0.1627

Table 5 Robustness against uniform remeshing

Model	#Vertex (%)	BER	Corr
bunny	100	0	1
	50	0.5	0.0667
elephant	100	0	1
	50	0.5	0
horse	100	0.0625	0.87831
	50	0.5625	-0.1627
armadillo	100	0.125	0.7746
	50	0.5	0

Table 6 Robustness against additive noise

Model	Noise amplitude (%)	BER	Corr
bunny	0.1	0	1
	0.3	0	1
	0.5	0.4375	0.2437
elephant	0.1	0.0625	0.8783
	0.3	0.1875	0.6180
	0.5	0.0625	0.8783
horse	0.1	0	1
	0.3	0	1
	0.5	0	1
armadillo	0.1	0	1
	0.3	0.0625	0.8783
	0.5	0.0625	0.8783

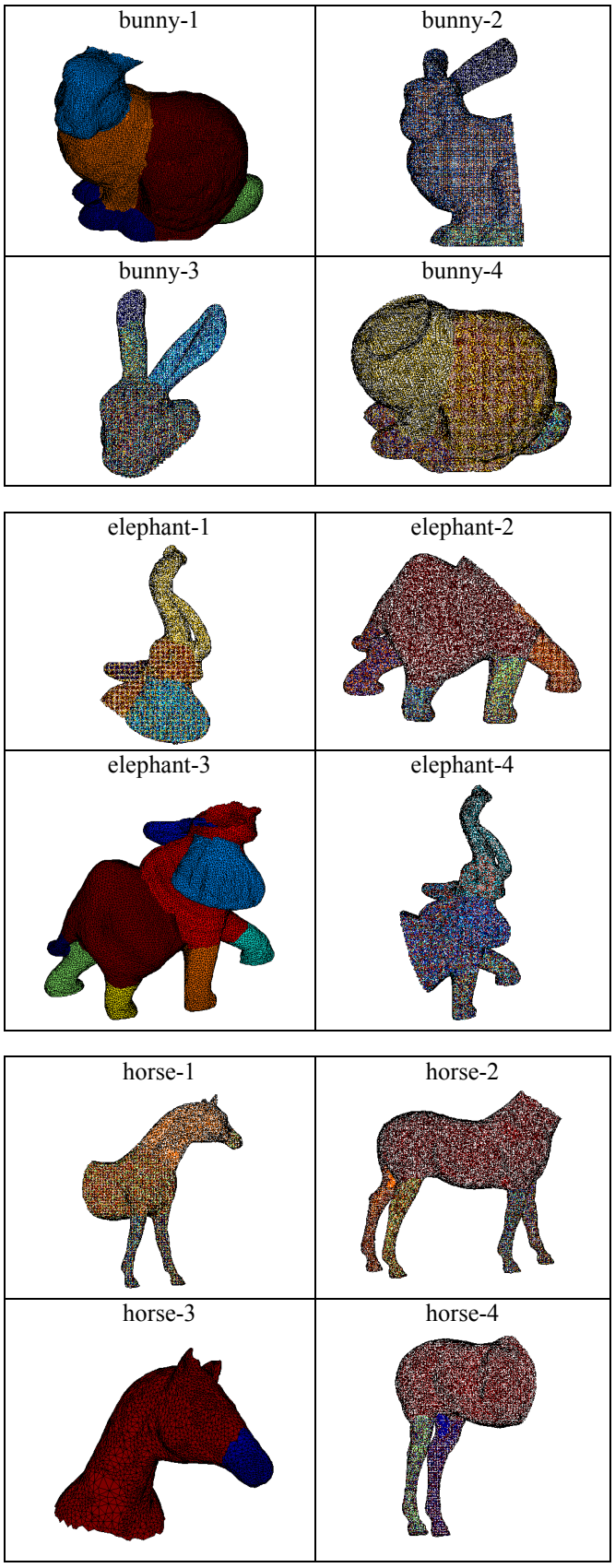
Table 7 Robustness against cropping

Model	Number (cropped ratio)	BER	Corr
bunny	1 (10%)	0	1
	2 (35%)	0	1
	3 (72%)	0.3125	0.4229
	4 (24%)	0	1
elephant	1 (52%)	0	1
	2 (50%)	0.25	0.5164
	3(20%)	0	1
	4(25%)	0	1
horse	1(42%)	0	1
	2 (19%)	0	1
	3 (78%)	0.3125	0.4229
	4(50%)	0	1
armadillo	1(37%)	0	1
	2 (49%)	0.4375	0.1627
	3 (14%)	0	1
	4(66%)	0.375	0.2582

N=16, embedding factor α =0.05, Δk =0.001. The baseline evaluation results in Table 1 and the other results were obtained by the desktop equipped with a 3.5GHZ quad core processor and 16GB memory. The experiment on various attacks including cropping was carried while the performance measured by BER and correlation with common definition:

$$Corr = \frac{\sum (w'_n - \overline{w}')(w_n - \overline{w})}{\sqrt{\sum (w'_n - \overline{w}')^2 \bullet \sum (w_n - \overline{w})^2}}$$

where w_n indicates the original watermark sequence while $\overline{w}'$ indicates the extracted one. Each robustness evaluation was carried on four different models: bunny (34385 vertices and 69473 faces), elephant (24955 vertices and 49918 faces), horse (19851 vertices and 39698 faces) and armadillo (26002 vertices and 52000 faces). Quantization, smoothing, non-uniform simplification and additive noise attack were simulated by MATLAB. Uniform simplification and



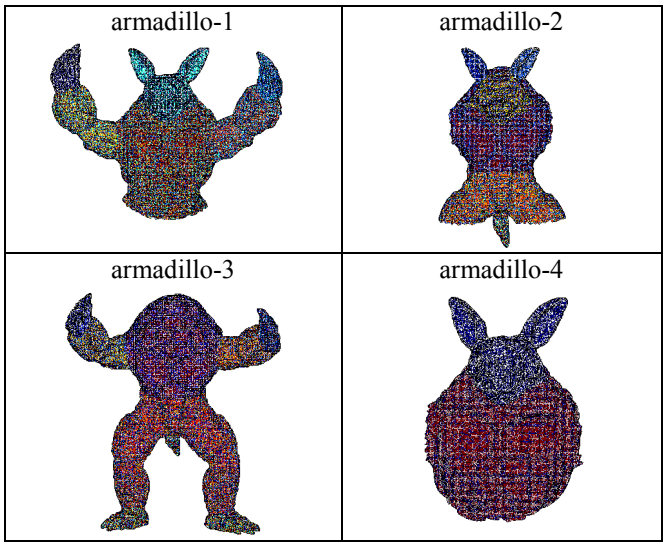


Fig 3. Cropped models where the watermark correlation of each model is presented in Table 7

remeshing were performed by the software ReMESH. Cropping attack was simulated by meshlab.

4.2. Experimental results against various attacks

Table 2 shows the extraction results after simulating quantization attacks. For all vertices, xyz coordinates were quantized respectively where quantization step is uniform over the interval between the minimum and maximum. Table 3 indicates the smoothing result. Laplacian smoothing tunes the vertices according to the average coordinates of its neighbor [12]. All watermarks extracted from the model were maintained perfectly until 10-th iteration with the factor 0.03. Table 4 indicates the results from simplification which uses the halfedge-collapse operation [13]. The percentage is calculated by the number of vertices. Table 5 represent the robustness against remeshing which is belongs to distortion-less attacks. Additive noise attack is indicated in Table 6 where the noise amplitude means the standard deviation of Gaussian. The percentage is calculated by the length of the average vertex norm. The result in Table 7 shows that our scheme is extremely robust against cropping attack. Especially, the high correlation was revealed in both body and head part of the models so that proposed watermark scheme could prevent the situation in scenarios we suggest.

5. CONCLUSION

In this paper we proposed blind 3D mesh watermarking scheme which is robust against cropping attack. Robustness against cropping is the very crucial since cropping is common editing process and it causes watermarks to break. Consistent partitioning for 3D mesh watermarking was gained by SDF based segmentation and the watermark sequence s were extracted properly. The experimental results also demonstrate the proposed method achieves robustness against general mesh operation such as smoothing, simplification, noise addition.

ACKNOWLEDGEMENT

This work was supported by the Institute for Information & communications Technology Promotion(IITP) grant funded by the Korean government(MSIP)(No.R0126-15-1024, Managerial Technology Development and Digital Contents Security of 3D Printing based on Micro Licensing Technology)

7. REFERENCES

[1] Li, L., Zhang, D., Pan, Z., Shi, J., Zhou, K., & Ye, K. Watermarking 3D mesh by spherical parameterization. Computers & Graphics, 28(6), 981-989. 2004.

[2] Cho, J. W., Prost, R., & Jung, H. Y. An oblivious watermarking for 3-D polygonal meshes using distribution of vertex norms. Signal Processing, IEEE Transactions on, 55(1), 142-155. 2007.

[3] Wu, J., & Kobbelt, L. Efficient spectral watermarking of large meshes with orthogonal basis functions. The Visual Computer, 21(8-10), 848-857. 2005.

[4] Wang, K., Lavoué, G., Denis, F., & Baskurt, A. Robust and blind mesh watermarking based on volume moments. Computers & Graphics, 35(1), 1-19. 2011.

[5] Liu, Y., Prabhakaran, B., & Guo, X. Spectral watermarking for parameterized surfaces. Information Forensics and Security, IEEE Transactions on, 7(5), 1459-1471. 2012.

[6] Feng, X., Zhang, W., & Liu, Y. Double watermarks of 3D mesh model based on feature segmentation and redundancy information. Multimedia tools and applications, 68(3), 497-515. 2014.

[7] Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. Secure spread spectrum watermarking for multimedia. Image Processing, IEEE Transactions on, 6(12), 1673-1687. 1997.

[8] Swanson, M. D., Zhu, B., & Tewfik, A. H. Transparent robust image watermarking. In Image Processing, 1996. Proceedings., International Conference on (Vol. 3, pp. 211-214). IEEE. 1996.

[9] Shapira, L., Shamir, A., & Cohen-Or, D. Consistent mesh partitioning and skeletonisation using the shape diameter function. The Visual Computer, 24(4), 249-259. 2008.

[10] Bilmes, J. A. A gentle tutorial of the EM algorithm and its application to parameter estimation for Gaussian mixture and hidden Markov models. International Computer Science Institute, 4(510), 126. 1998.

[11] Lam, L., & Suen, C. Y. Application of majority voting to pattern recognition: an analysis of its behavior and performance. Systems, Man and Cybernetics, Part A:

Systems and Humans, IEEE Transactions on, 27(5), 553-568. 1997.

[12] Field, D. A. Laplacian smoothing and Delaunay triangulations. Communications in applied numerical methods, 4(6), 709-712. 1988.

[13] Heckbert, P. S., & Garland, M. Survey of polygonal surface simplification algorithms. CARNEGIE-MELLON UNIV PITTSBURGH PA SCHOOL OF COMPUTER SCIENCE. 1997.

[14] Zafeiriou, S., Tefas, A., & Pitas, I. Blind robust watermarking schemes for copyright protection of 3D mesh objects. Visualization and Computer Graphics, IEEE Transactions on, 11(5), 596-607. 2005.

[15] Alface, P. R., Macq, B., & Cayre, F. Blind and robust watermarking of 3D models: How to withstand the cropping attack?. In Image Processing, 2007. ICIP 2007. IEEE International Conference on (Vol. 5, pp. V-465). IEEE. 2007.

[16] Uccheddu, F., Corsini, M., & Barni, M. Wavelet-based blind watermarking of 3D models. In Proceedings of the 2004 workshop on Multimedia and security (pp. 143-154). ACM. 2004.