

3D Mesh Model Watermarking Based on Projection

Suk-Hwan Lee[†], Ki-Ryong Kwon^{**}

ABSTRACT

The common requirements for watermarking are usually invisibility, robustness, and capacity. We proposed the watermarking for 3D mesh model based on projection onto convex sets for invisibility and robustness among requirements. As such, a 3D mesh model is projected alternatively onto two convex sets until it converge a point. The robustness convex set is designed to be able to embed watermark into the distance distribution of vertices. The invisibility convex set is designed for the watermark to be invisible based on the limit range of vertex movement. The watermark can be extracted using the decision values and index that the watermark was embedded with. Experimental results verify that the watermarked mesh model has both robustness against mesh simplification, cropping, affine transformations, and vertex randomization and invisibility.

Keywords: 3D Mesh Model, Watermarking, Projection

1. INTRODUCTION

There has been a recent increased interest in Web 3D techniques that realize 3D graphics. Among such techniques, the international standards organization, ISO/IEC, has confirmed the Virtual Reality Modeling Language (VRML) as the standard for representing 3D graphics on the Web, which has made sources of VRML available to the general public[1]. Thus, 3D watermarking has recently been a focus of research to protect the copyright of VRML[2-8]. 3D graphic model in VRML are usually represented as a mesh defined by vertex coordinates and connectivity of vertices. However, this mesh can be easily edited by a geometrical and topological attack, and represented by many descriptors. Geometrical attack removes or

changes the coordinate of vertices, such as affine transformation, vertex noise addition, and cropping. Topological attack removes or changes the connectivity of vertices, such as remeshing or mesh simplification. 3D watermarking must consider geometrical and topological operator to be robust.

The watermarking algorithms developed by Ohbuchi et al. are based on geometrical or topological modifications[2]. TSQ (Triangle Similarity Quadruple) watermarking modifies vertices coordinates of four adjacent meshes to encode the watermark, by properly setting the value of ratios between edges length of the meshes group. TVR (Tetrahedral Volume Ratio) watermarking codes the hidden information by varying the ratio of tetrahedral volume. MDP (Mesh Density Pattern) watermarking uses topological modifications to embed the visible watermark. These algorithms are not robust to remeshing or mesh simplification. Benedens proposed a watermarking method that modifies the model's normal distribution to store information solely in the geometry of the model[3]. As such, this algorithm is robust to randomization of the vertices, re-meshing, and mesh simplification. Yet, if the watermarked model is attacked by partial resection, such as cropping, the watermark em-

※ Corresponding Author :Suk-Hwan Lee, Address : (608-711) Yong-Dong Dong 535 Nam-Gu, Busan Korea
TEL : +82-51-610-8752, FAX : +82-51-610-8846
E-mail : skylee@tit.ac.kr

Receipt date : Jan. 3, 2005, Approval date : June. 8, 2005

[†] Tongmyong University of Information Technology, Department of Information Security

^{**} Pusan University of Foreign Studies, Division of Digital and Information Engineering
(E-mail : krkwon@pufs.ac.kr)

※ This Work was supported by Tongmyong University of Information Technology Research Fund of 2005.

bedded in that section will disappear, whereas for an affine transformation, this algorithm needs to be realigned by using the normal distributions of the original model.

There are the robustness and the invisibility in the requirements for watermarking system. The conventional watermarking embeds the watermark into the location with both robustness and invisibility, or embeds the watermark into the location with robustness to be invisible using HVS (Human visual system). However to satisfy two requirements at once in this paper, we design the robust constraint set and the invisible constraint set independently, then project 3D-mesh model alternatively into two sets until the convergence condition is satisfied. Finally the watermarked model is the element common to two sets. Experimental results verify that the proposed algorithm is both robust to affine transformations, mesh simplification, cropping, and vertex randomization and imperceptible.

2. PROPOSED 3D MESH WATERMARKING

2.1 Scheme of watermark embedding

In this paper, we consider a 3D-mesh model M with $N \times 1$ vectors (N vertices) in \mathbb{H} . The watermark embedding process can be described by the following steps:

1) Take the original model M as the initial model M_0 .

- 2) Compute $M_n = P_v P_r M_{n-1}$ for each iteration $n = 1, 2, \dots$. P_r and P_v are the projection onto the sets C_r and C_v as shown in Fig. 1.
- 3) Iterate 2) step continuously until the convergence condition is satisfied, which is in detail described in the next subsection.

The watermarked model is the convergence point M^* , common to C_r and C_v , that obtained through the above process. C_r is designed according to the scheme of watermark embedding and C_v is designed according to the limit movement of vertex.

Given a 3D-mesh model M with N vertices $v_{j \in \{1, N\}} \in \mathbb{R}^3$, all vertices are converted into spherical coordinate $\{r, \theta, \phi\}$ to the mass center $m = \sum_{j=1}^N v_j / N$ instead of the origin, since the origin can be different in some attacks. All components of r_j ($j = 1, 2, \dots, N$) are sampled into bin Q_i with the spherical volume $V_i = \alpha_i V_1$. The interval of sample bin Q_i is $[r_{\min} - \Delta r_{i-1}, r_{\min} + \Delta r_{i-1}]$, where Δr_i is $\sqrt[3]{\frac{3\alpha_i}{4\pi} V_1 + (r_{\min} + \Delta r_{i-1})^3 - r_{\min}^3}$ ($i \geq 2$). K is determined to consider the bit number for binary watermark. r_{\min} and r_{\max} are the max and min value among the r components, respectively. α_i is the ratio of the volume that is randomly determined. Thus, when r_j is within $[r_{\min} - \Delta r_{i-1}, r_{\min} + \Delta r_{i-1}]$, the sample bin of r_j is Q_i . The sample means $E_i = \sum_{j=1}^{N_i} r_j / N_i$, $r_j \in [r_{\min} - \Delta r_{i-1}, r_{\min} + \Delta r_{i-1}]$ of r

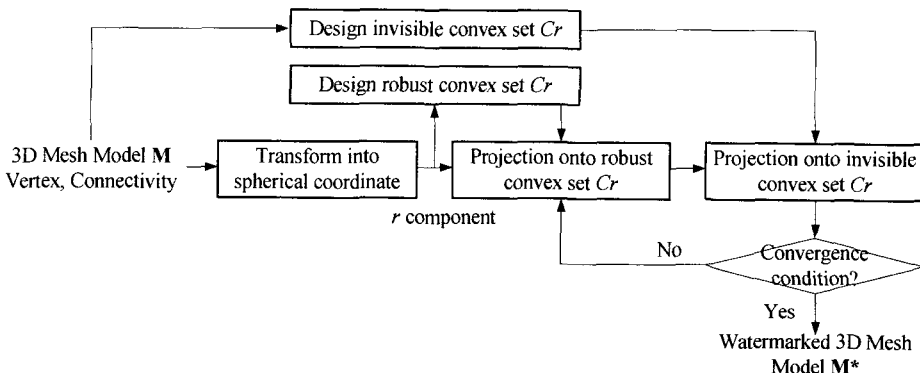


Fig. 1. The process for 3D mesh watermarking based on POCS.

components that are sampled into each bin Q_i are calculated and they are ranked in a descending order according to the density $D_i = N_i/V_i$ of each bin Q_i . N_i is the number of r components that are sampled into Q_i and V_i is volume of Q_i .

N_w bits of watermark are embedded into the sample means of high ranked bin as shown in Fig. 2. In this figure, $\text{rank}(D_i)$ is the rank of D_i that is the density of bin Q_i . If $\text{rank}(D_i)$ is k , $\text{rank}^{-1}(k)$ is the subscript i of bin Q_i . k th watermark $w_k \in W$ is embedded into the sample mean $E_{\text{rank}^{-1}(k)}$ of k th ranked bin $Q_{\text{rank}^{-1}(k)}$ as follows;

$$E'_{\text{rank}^{-1}(k)} = (1 + \alpha R_k) \times E_{\text{rank}^{-1}(k)} \quad (1)$$

$$R_k = \begin{cases} -1 & \text{if } w_k = 0 \\ 1 & \text{else } w_k = 1 \end{cases} \quad (2)$$

where α is the embedding strength. Since $E_{\text{rank}^{-1}(k)}$ is sample mean of the original model \mathbf{M} considered as the initial model \mathbf{M}_0 in the above subsection, it is written by $E_{\text{rank}^{-1}(k),0}$ in this paper.

2.2 Constraint sets and projectors

For the above watermark embedding scheme, two geometric constraint sets are constructed plus their

projectors, such as a robustness constraint set C_r and invisibility constraint set C_v . The former can be a global constraint set, while the latter can be a local constraint set.

2.2.1 Robustness constraint set

The sample mean $E_{\text{rank}^{-1}(k)}$ where the embedded watermark falls in Eq. (1) must be robust. If $w_k = 1$, then

$$E_{\text{rank}^{-1}(k),0} \leq E'_{\text{rank}^{-1}(k)} \leq (E_{\text{rank}^{-1}(k),0} + E_{\text{rank}^{-1}(k+1),0})/2$$

and otherwise $w_k = 0$, then

$$(E_{\text{rank}^{-1}(k-1),0} + E_{\text{rank}^{-1}(k),0})/2 \leq E'_{\text{rank}^{-1}(k)} \leq E_{\text{rank}^{-1}(k),0}$$

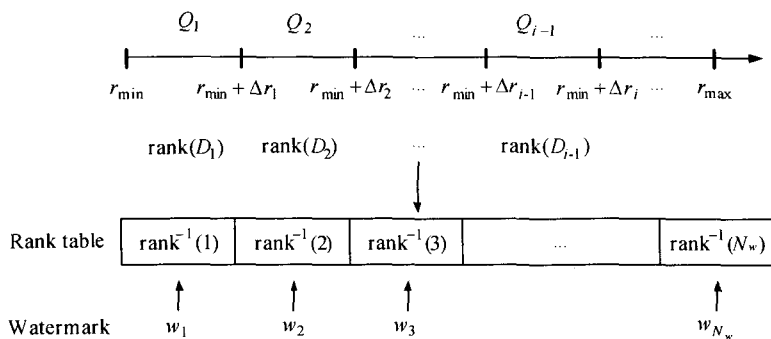
as shown in Fig. 3. Therefore, since $E'_{\text{rank}^{-1}(k)}$ has to be near to the center point of the interval, the closed convex set for the robustness constraint can be defined as

$$C_r = \{ \mathbf{M}^T \mid |E_{\text{rank}^{-1}(k)}[r] - E^*_{w_k}| \leq \epsilon, k = 1, 2, \dots, N_w \} \quad (3)$$

where

$$E^*_{w_k} = \begin{cases} (3E_{\text{rank}^{-1}(k),0} + E_{\text{rank}^{-1}(k)+1,0})/4, & \text{if } w_k = 1 \\ (3E_{\text{rank}^{-1}(k),0} + E_{\text{rank}^{-1}(k)-1,0})/4, & \text{else } w_k = 0 \end{cases}$$

It can be easily shown that this set is closed and convex. C_r is the set of 3D models whose sample means into which the watermark of N_w bit is embedded be within $[E^*_{w_k} - \epsilon, E^*_{w_k} + \epsilon]$.



D_i : Density of bin Q_i
 $\text{rank}(D_i)$: Rank of D_i
 $\text{rank}^{-1}(k)$: Subscript of bin with k th rank

Fig. 2. Watermark bits are embedded into sample bins with high density.

The geometric projection P_r onto C_r can be defined as follows;

$$E'_{rank^{-1}(k)} = \alpha(E_{w_k=1}^* + \epsilon) + (1-\alpha)E_{rank^{-1}(k)} \text{ if } w_k = 1$$

$$\alpha(E_{w_k=0}^* - \epsilon) + (1-\alpha)E_{rank^{-1}(k)} \text{ else } w_k = 0$$

(4)

where

$$(E_{v_i=1}^* - \epsilon) \leq \alpha(E_{v_i=1}^* + \epsilon) + (1-\alpha)E_{rank^{-1}(k)} \leq (E_{v_i=1}^* + \epsilon) \text{ if } w_k = 1$$

$$(E_{v_i=0}^* - \epsilon) \leq \alpha(E_{v_i=0}^* + \epsilon) + (1-\alpha)E_{rank^{-1}(k)} \leq (E_{v_i=0}^* + \epsilon) \text{ if } w_k = 0$$

Thus, $\frac{(E_{w_k=1}^* - \epsilon) - E_{rank^{-1}(k)}}{(E_{w_k=1}^* + \epsilon) - E_{rank^{-1}(k)}} \leq \alpha \leq 1$ if $w_k = 1$

and $\frac{E_{rank^{-1}(k)} - (E_{w_k=0}^* + \epsilon)}{E_{rank^{-1}(k)} - (E_{w_k=0}^* - \epsilon)} \leq \alpha \leq 1$ if $w_k = 0$. α is determined as the intermediate value of each interval.

2.2.2 Invisibility constraint set

Since the set C_r only considers an equal embed-

ding strength of r components in the sample mean as the watermark embedding scheme, this set can not satisfy invisibility. Thus, the invisibility constraint set C_v is the set of 3D mesh models whose r components of vertices are within the limit bounds as follows

$$C_v = \{M^T | T_L \leq r_i \leq T_H, i=1,2,\dots,N\}$$

(5)

where T_L, T_H are respectively the lower and upper bounds for the r_i component of the i th vertex v_i . It can be easily shown that this set is also closed and convex.

A vertex $v_i = (x_i, y_i, z_i)$ must be changed within the range that is below each Cartesian coordinate value of the valence vertices $v_{ia} = (x_{ia}, y_{ia}, z_{ia})$ connected to it as shown in Fig. 4. The available ranges for each coordinate value in a vertex are $x_i - \Delta x \leq x_i \leq x_i + \Delta x$, $y_i - \Delta y \leq y_i \leq y_i + \Delta y$, and $z_i - \Delta z \leq z_i \leq z_i + \Delta z$. Δx ,

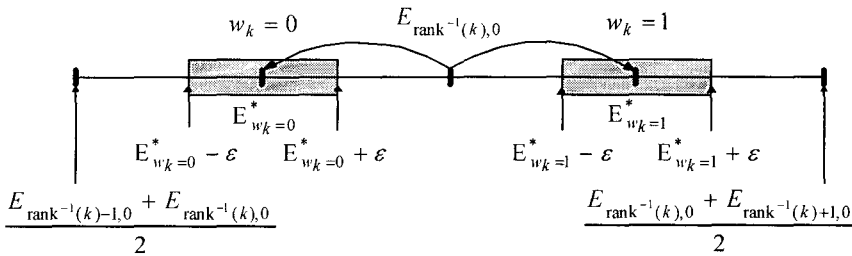


Fig. 3. Move the sample mean $E_{rank^{-1}(k),0}$ of bin $Q_{rank^{-1}(k)}$ according to the watermark bit w_k .

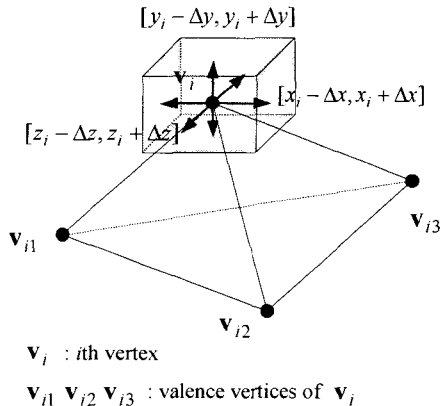


Fig. 4. The limit movement of a vertex $v_i = (x_i, y_i, z_i)$.

Δy , and Δz are

$$\Delta x_i = \min |mx_i - x_{ia}|/2, \quad \Delta y_i = \min |my_i - y_{ia}|/2, \quad (6)$$

$$\Delta z_i = \min |mz_i - z_{ia}|/2$$

where $mx_i = \sum_{a=1}^{n_i} x_{ia}/n_i$, $my_i = \sum_{a=1}^{n_i} y_{ia}/n_i$,

and $mz_i = \sum_{a=1}^{n_i} z_{ia}/n_i$.

n_i is the number of valence vertices. The projection P_v onto the set C_v , which takes the limitation of each $r_{i \in [1, N]}$ components, considering the environment of its vertex v_i , is followed by

$$r'_i = \begin{cases} T_H, & \text{if } r_i > T_H \\ T_L, & \text{else if } r_i < T_L \\ r_i, & \text{else} \end{cases} \quad (7)$$

where $T_L = r_{i,avg} - \sqrt{\Delta x^2 + \Delta y^2 + \Delta z^2}$,

$T_H = r_{i,avg} + \sqrt{\Delta x^2 + \Delta y^2 + \Delta z^2}$, and

$r_{i,avg} = \sqrt{mx_i^2 + my_i^2 + mz_i^2}$.

2.3 Watermark extracting

The watermark in attacked model is extracted by using the rank table for the density of the sample bins, and the initial sample means $E_{rank^{-1}(k),0}$ ($1 \leq k \leq N_w$) of bins into which the watermark has been embedded. The rank table is need both to inform the position into which the watermark is embedded and to obtain the exactly mass center in the attacked model. $E_{rank^{-1}(k),0}$ is the decision value for extracting the watermark.

The origin of the attacked model can be different with the origin of the original model. If the origin of the watermarked model is translated to unknown position, anyone doesn't know the previous origin in the translated model. However, since the mass center m can be constant in case of translation, rotation, and scaling, we use the mass center m as the origin of the model in the embedding process since the mass center is identical. But it

can be changed by means of cropping, mesh simplification, vertex randomization, and translation with other attacks. Since the vertex densities of bins in these attacked models and original model are different, the watermark can't be extracted. Therefore, the mass center of the original model in these attacked models has to be detected before the watermark extracting.

When the mass center is falsely detected, there are a number of the bit errors in the extracted watermark. Fig. 5 shows the number of the bit error in the extracted watermark while varying the origin of the watermarked Stanford bunny model as $m' = m + e$. The bit error is not produced until e is below 8×10^{-4} . Thus, the effective range of m^* is $|m^* - m| < 8 \times 10^{-4}$. Actually since m is unknown without having the original model, we don't know whether the detected mass center is within the effective range. We detect in detail the mass center of the original model using the rank table.

First, the densities of sample bins in the attacked model are calculated using the mass center m' of the attacked model. Then the rank k of the density of bin $Q_{rank^{-1}(k)}$ ($1 \leq k \leq N_w$) in the rank table of the original model is compared with the rank $rank'(Q_{rank^{-1}(k)})$ of the density $D'_{rank^{-1}(k)}$ of bin

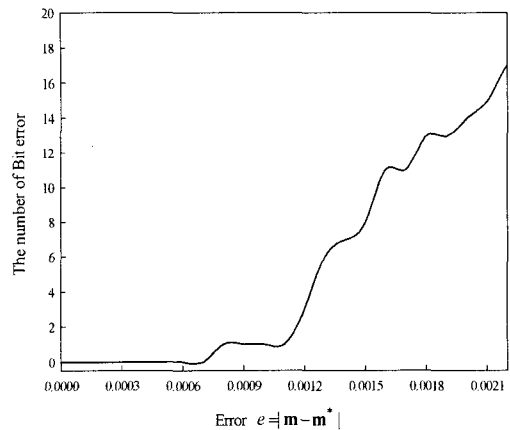


Fig. 5. The number of bit error in the extracted watermark while varying the origin of the watermarked Stanford bunny model as $m' = m + e$.

$Q_{rank^{-1}(k)}$ in the attacked model. If rank tables in the original model and the attacked model are not equal, m^* that minimizes the difference of two rank tables is searched for varying m' in \mathbb{R}^3 .

$$m^* = \operatorname{argmin}_{m' \in \mathbb{R}^3} \left\{ \sum_{k=1}^{N_k} |k - \operatorname{rank}'(D'_{rank^{-1}(k)})| \right\} \quad (8)$$

Next, the sample means in the attacked model are calculated and then the sample mean $E'_{rank^{-1}(k)}$ into which the watermark has been embedded is compared to $E_{rank^{-1}(k)}$. If $E_{rank^{-1}(k)}[r] - \tilde{E}_{rank^{-1}(k)}[r] < 0$, then $w_k = 1$. Otherwise, $w_k = 0$.

3. EXPERIMENTAL RESULTS

To evaluate the performance of the proposed algorithm, computer simulations were performed using VRML data for the Stanford Bunny and Knots that are downloaded in the Web[10]. Table 1 shows the number of vertices and meshes in these models. The binary watermark was a 50 length Gaussian random sequence converted to 1bit. In this experiment, we make 100 sample bins while varying the ratio of volume and embed the watermark into the

50 bins with the high vertex density.

Iteration number of each models for projecting alternatively into the robust and the invisible constraint sets is about 7-8 and takes about 7-10 second in Pentium III 800MHz. Iteration number and embedding time have an effect on the number of vertices of models.

The models that are watermarked by using the proposed algorithm are shown in Fig. 3. In this figure, a subjective evaluation was used to verify that the watermark was imperceptible. No objective evaluation for visibility has yet been adopted for 3D graphics. So, we used VSNR (vertex SNR), $10 \log_{10}(\operatorname{var}(\|v - v_M\|) / \operatorname{var}(\|v - v'\|))$, such as the PSNR in image processing. v and v' are the vertex coordinate of the original model and the watermarked model and v_M is the center mass of the original mesh. VSNRs of the watermarked Stanford bunny and Knots are 42.69 and 40.77 dB. These values show the good quality.

We experimented the robustness performance against mesh simplification, vertex randomization and cropping attacks with or without translation. The strength of the attacks was also adjusted, such as the % in the mesh simplification and α in the

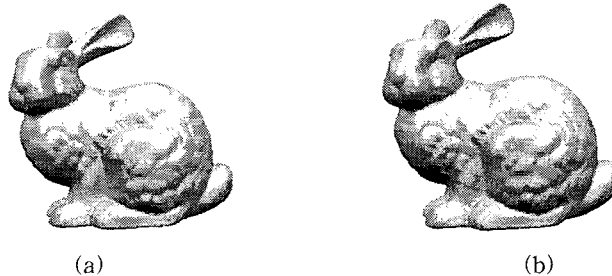


Fig. 6. (a) Original Stanford bunny and (b) watermarked Stanford bunny.

Table 1. Models used in the experiment and embedding times, iteration numbers, and VSNRs of the watermarked models.

Model	Number of vertices	Number of meshes	File size [kB]	Embedding time [s]	Iteration number	VSNR [dB]
Stanford Bunny	35,947	69,451	3,626	10.23	8	42.65
Knots	23,232	46,464	2,364	6.84	7	40.78

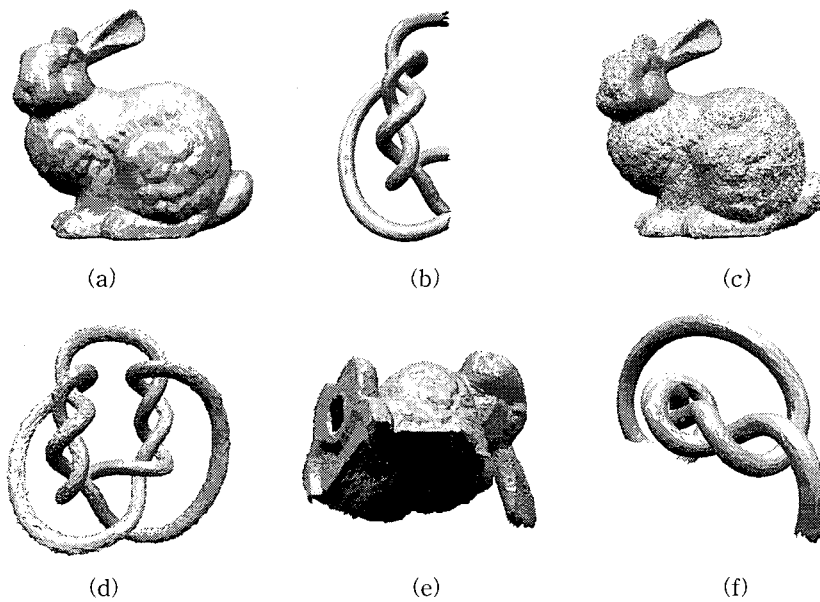


Fig. 7. (a) Stanford bunny simplified to 35.28 % by using mesh simplification, (b) partial cropped Knots, (c) Stanford bunny and (d) Knots added to random noise at all vertices, (e) (a) model with cropping and (45o, 45o, 45o) rotation and (f) Knots simplified to 56.5%, cropped, rotated to (90o, 45o, 25o).

Table 2. Results of mesh simplification experiment

Model	Percentage of vertex number [%]	Number of vertices	No translation		Translation	
			BER	Extracting time [s]	BER	Extracting time [s]
Stanford bunny	51.2	18,427	0.00	0.25	0.02	25m 12s
	21.0	7,582	0.10	0.19	0.16	18m 30s
Knots	56.5	13,136	0.04	0.23	0.05	22m 41s
	24.3	5,644	0.11	0.15	0.15	17m 23s
Venus	61.0	20,470	0.00	0.28	0.01	26m 07s
	27.0	9,144	0.07	0.21	0.13	19m 05s

Table 3. Results of vertex randomization and cropping experiment

Model	Attack	No translation		Translation	
		BER	Extracting time [s]	BER	Extracting time [s]
Stanford bunny	Vertex randomization	0.04	0.33	0.06	28m 02s
	Cropping (14,284 vertices)	0.01	0.24	0.08	37m 23s
	Simplify + Cropping (4,957 vertices)	0.12	0.12	0.23	34m 58s
Knots	Vertex randomization	0.09	0.29	0.12	26m 45s
	Cropping (10,455 vertices)	0.00	0.22	0.10	35m 08s
	Simplify + Cropping (6,050 vertices)	0.12	0.17	0.19	33m 26s
Venus	Vertex randomization	0.05	0.32	0.07	27m 44s
	Cropping (13,347 vertices)	0.01	0.22	0.13	36m 53s
	Simplify + Cropping (8,187 vertices)	0.08	0.18	0.20	35m 12s

vertex randomization, to produce bit error. The robustness against these attacks is shown in Table 2 and 3, which uses average bit error rate, BER of the extracted watermark in 10 times experiments. In case of translation, the extracting time is very long because of the realignment process; it takes about 18–25m in translation. However, the extracting time is about 0.2–0.3s without translation or uniform scaling. The average BER in translation or uniform scaling is above about 0.01–0.12 than the average BER in no translation or uniform scaling.

The watermarked models were simplified by using *MeshToSS*[10]. The % in the table represents the percentage of the vertex number of the simplified model to the vertex number of the original model. No bit error occurred until the simplification reached 40–50%, and over 90% of the watermark remained until the model was simplified to 21%. When the vertex randomization was performed, all the vertices v were added to uniform random noise, $v' = (1 + \alpha \times \text{uniform}()) \times v$. The modulation factor α was 0.02, which was also varied to create a bit error, while the was a uniformly random function of $[-0.5 \ 0.5]$. In table 1, 90% of the watermark remained. For the cropping attacks, all vertices with x coordinate value over $\max_x/8$ were cropped, where \max_x was the maximum x coordinate value. All the watermarks could be extracted with no error. The rotation attack also had no affect on the proposed model. The models attacked by simplification, random noise, rotation, and cropping are shown in Figs. 7 (e), (f).

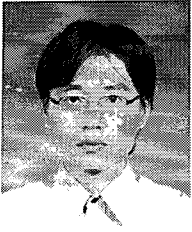
4. CONCLUSIONS

The robustness and the invisibility is trade-off in watermarking system. To achieve their necessary conditions, we proposed the 3D mesh watermarking based on POCS. As such, a binary watermark is embedded by modifying the sample means of r components, which is performed by alternately projecting the model onto a robust constraint con-

vex set and invisible constraint set. Experiments verified that the watermarked mesh was both robust to various attacks and invisible.

5. REFERENCES

- [1] ISO/IEC 14772-1, "The virtual reality modeling language."
- [2] R. Ohbuchi, H. Masuda, and M. Aono, "Watermarking Three-Dimensional Polygonal Models Through Geometric and Topological Modification," *IEEE JSAC*, Vol. 16, No. 4, pp. 551–560, May 1998.
- [3] O. Benedens, "Geometry-Based Watermarking of 3D Models," *IEEE CG&A*, pp. 46–55, Jan./Feb. 1999.
- [4] S. Kanai, H. Date, and T. Kishinami, "Digital Watermarking for 3D Polygons using Multiresolution Wavelet Decomposition," *Proc. Sixth IFIP WG 5.2 GEO-6*, pp. 296–307, Dec. 1998.
- [5] E. Praun, H. Hoppe, and A. Finkelstein, "Robust Mesh Watermarking," *Proc. SIGGRAPH 99*, pp. 49–56, 1999.
- [6] B.-L. Yeo and M. M. Yeung, "Watermarking 3D Objects for Verification," *IEEE CG&G*, pp. 36–45, Jan./Feb. 1999.
- [7] K.-R. Kwon, S.-G. Kwon, S.-H. Lee, T.-S. Kim, and K.-I. Lee, "Watermarking for 3D Polygonal Meshes Using Normal Vector Distributions of Each Patch," *IEEE International Conference on Image Processing*, Vol. 3, pp. 499–502, Sept. 2003.
- [8] S.-H. Lee and K.-R. Kwon, "Watermarking for 3D Mesh Model Using Patch CEGIs," *Lecture Notes in Computer Science*, Vol. 3481, pp. 557–566, April 2005.
- [9] Y. Yang and N. P. Galatsanos, "Projection-Based Spatially Adaptive Reconstruction of Block-Transform Compressed Images," *IEEE Trans. on Image Processing*, Vol. 4, No. 7, July 1995.
- [10] T. Kanai, MeshToSS Version 1.0.1, <http://graphics.sfc.keio.ac.jp/MeshToSS/indexE.html>.



Suk-Hwan Lee

He received a B.S., a M.S., and a Ph. D. degree in Kyungpook National University, Korea in 1999, 2001, and 2004 respectively. His research field has been in Multimedia Security, digital image processing, computer graphics.

He is currently a full-time instructor in department of Information Security at Tongmyong University of Information Technology.



Ki-Ryong Kwon

1986 Electronic Engineering, Kyuonpook National University (B.S.)

1990 Electronic Engineering, Kyuonpook National University (M.S.)

1994 Electronic Engineering, Kyuonpook National Uni-

versity (Ph. D.)

2000~2002 Visiting Professor, University of Minnesota

1996~Present Associate Professor, Pusan University of Foreign Studies

2005~Present Editorial Board Chairman of Korea Multimedia Society

Research Interests : Multimedia Security, Wavelet Transform, Digital Image Processing, 3D Recognition System