Journal of Korea Multimedia Society Vol. 14, No. 6, June 2011(pp. 742-751)

형상 특징자 기반 강인성 3D 모델 해싱 기법

이석환[†], 권성근[††], 권기룡[†††]

요 약

본 논문에서는 형상 특징자인 열 커널 인증 (Heat Kernel Signature, HKS)를 기반으로 강인한 3D 모델 해싱을 제안한다. 키와 매개변수에 의존한 형상 특징자 기반 3D 모델 해싱을 제안한다. 제안한 방법에서는 Mesh Laplace 연산자의 고유치와 고유벡터에 의하여 각 꼭지점에 대한 전역 및 국부 타임 HKS 계수를 구한 다음, 이 계수들을 정방형 2D 셀로 군집화한다. 그리고 각 셀에 할당된 HKS 계수 쌍의 거리 가중치 기반으로 정의된 특징계수와 랜덤 계수 키와의 조합에 의하여 중간 해쉬 계수를 생성한 다음, 이진화 과정에 의하여 최종 이진 해쉬를 생성한다. 본 실험에서는 3D 범용 툴을 이용한 다양한 기하학적 공격과 위상학적 공격을 통하여 강인성을 평가하였고, 모델과 키 조합에 대한 해쉬의 유일성을 평가하였다. 또한 인증 범위를 만족하는 공격 세기를 측정함으로써 모델 공간성을 평가하였다. 실험결과로부터 제안한 3D 모델 해싱이 기존 해싱에 비하여 강인성, 모델 공간성 및 유일성이 우수함을 확인하였다.

Robust 3D Model Hashing Scheme Based on Shape Feature Descriptor

Suk-Hwan Lee[†], Seong-Geun Kwon[††], Ki-Ryong Kwon[†††]

ABSTRACT

This paper presents a robust 3D model hashing dependent on key and parameter by using heat kernel signature (HKS), which is special shape feature descriptor. In the proposed hashing, we calculate HKS coefficients of local and global time scales from eigenvalue and eigenvector of Mesh Laplace operator and cluster pairs of HKS coefficients to 2D square cells and calculate feature coefficients by the distance weights of pairs of HKS coefficients on each cell. Then we generate the binary hash through binarizing the intermediate hash that is the combination of the feature coefficients and the random coefficients. In our experiment, we evaluated the robustness against geometrical and topological attacks and the uniqueness of key and model and also evaluated the model space by estimating the attack intensity that can authenticate 3D model. Experimental results verified that the proposed scheme has more the improved performance than the conventional hashing on the robustness, uniqueness, model space.

Key words: 3D Model(3D 모델), Content Hashing(콘텐츠 해싱), Shape Feature Descriptor(형상 특징자)

※ 교신저자(Corresponding Author) : 권기룡, 주소 : 부산광역시 남구 대연3동 599-1(608-737), 전화 : 051)629- 6257, FAX : 051)629-6210, E-mail : krkwon@pknu.ac.kr
접수일 : 2011년 3월 14일, 수정일 : 2011년 5월 24일
완료일 : 2011년 6월 9일
[†] 종신회원, 동명대학교 정보보호과 부교수
(E-mail : skylee@tu.ac.kr)
[††] 정회원, 경일대학교 전자공학과 조교수
(E-mail : sgkwon@kiu.ac.kr)
[†††] 종신회원, 부경대학교 IT융합응용공학과 부교수
(E-mail : krkwon@pknu.ac.kr)
※ 본 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (KRF-2010-0016835, KRF-2010-0016684)

1. 서 론

정보통신 기술 발달과 더불어 디지털 콘텐츠의 급진적인 전환에 따라 이에 대한 보호 기술이 많이 발전되어 왔다. 향후 콘텐츠 거래 시스템은 새로운 패러다임의 Pre-pay 모델 또는 Auxiliary pay 모델 방향으로 제시될 경우 포렌식 및 정보 은닉 기반의 콘텐츠 인증 기술이 21세기 멀티미디어 보호의 주요한 이슈로 인식되었다[1]. 이와 별개로 비트 변화에 민감한 암호화 기반 해싱보다 압축, 전송 등의 비트 변화 및 편집에 강인한 영상 기반 해싱 기법들이 많이 연구되어져 왔다[2-4].

최근에는 3D 콘텐츠에 대한 관심이 고조되면서, 3D 모델에 대한 워터마킹[5,6]뿐만 아니라 3D 모델의 인증 및 검색을 위한 해싱 기법들이 제안되어지고 있다[7-10]. 3D 모델 해싱은 기존 영상 해싱에서와 같이 강인성, 유일성, 공간성, 및 보안성 조건을 만족하여야 한다. 강인성은 해쉬 함수에서 동일한 키가 사용되었을 때 시각적으로 유사한 모델들에서 동일한 해쉬를 생성하여야 한다. 3D 모델들은 2D 영상과는 달리 다양한 기하학적 및 위상학적 형태의 공격에 의하여 지각적으로 유사한 모델들로 변환이 가능하다. 유일성은 다른 모델들 간에 생성된 해쉬들은 확률적으로 독립이어야 한다. 예를 들어, 임의의 두 모델에 의하여 생성된 해쉬들이 다를 확률이 매우 높아야 한다. 공간성은 동일한 해쉬가 생성되는 원 모델과 공격받은 모델들의 집합을 나타내며, 이는 동일한 해쉬가 생성될 때까지의 공격 세기로 측정된다. 보안성은 해쉬의 예측불가능성(unpredictability)으로, 키를 알지 못할 때 해쉬를 쉽게 예측할 수 없어야 한다. 이는 특징 추출, 양자화 또는 압축 과정에서 키 기반 랜덤 방식을 적용함으로써 보안성을 유지할 수 있다. 이상과 같이 성질들은 서로 상호 보완적인(trade-off) 관계이다.

기존 콘텐츠인 영상 및 비디오 해싱과 3D 모델 해싱의 차이점은 강인성을 고려한 특징 추출이다. 즉, 영상 및 비디오 해싱에서는 화소 또는 DCT/DWT 등의 변환계수 기반 특징 추출이나, 3D 모델 해싱에서는 벡터 기반의 꼭지점 좌표 기반 특징 추출을 수행하여야 한다. 기존 3D 모델 해싱 기법들은 3D SSD와 표면곡률 기반 블록 표면 계수[8,9], 객체별 거리 분포 계수[10]을 이용한 특징 계수를 추출한 후, 이를 최종 이진 해쉬로 생성하였으며, 미분 엔트로피 기반의 해쉬 보안성을 평가하였다. 그러나 기존 기법들은 메쉬 간단화(mesh simplification) 및 부분할(subdivision)와 같은 메쉬 위상 공격에 강인하지 못한 단점을 가진다.

본 논문에서는 위상 공격뿐만 아니라 기하학 공격에 강인하며, 공간성 및 유일성을 가지는 3D 모델 해싱 기법을 제안한다. 해쉬의 강인성을 위하여 3D 모델의 형상 특징 추출이 매우 중요하다. 3D 모델의 형상 특징 추출은 특징 기반 3D 형상 검색 (Feature-based shape retrieval), 3D 워터마킹 등의 분야에서 많은 연구들이 이루어져 왔다. 대표적인 특징자로는 HKS(Heat kernel-based signatures), 3D Harris features, Salient points, 3D SSD, 가우시안 곡률(Gaussian curvature) 등이 있다. 제안한 방법에서는 곡률의 다층 스케일 개념을 제공하고, 다양한 변형에 강인한 HKS를 이용하여 해쉬 특징 벡터들을 추출한다. 제안한 방법에서는 곡률의 다층 스케일 개념을 제공하고, 다양한 변형에 강인한 HKS(Heat kernel signature)[11,12]를 이용하여 해쉬 특징 계수를 추출한다. 먼저, 제안한 방법에서는 3D 모델의 각 꼭지점에 대한 국부 및 전역 타임 스케일에 대한 HKS 계수 쌍을 구한 다음, 이들 계수 쌍을 2D 정방형 셀로 그룹화한다. 그리고 HKS 계수 쌍의 n차 Butterworth 함수 기반 거리 가중치에 의하여 각 셀의 특징 계수를 구한 다음, 랜덤 계수와의 조합에 의하여 중간 해쉬 계수를 생성한다. 마지막으로 최종 해쉬는 중간 해쉬 계수의 이진화 과정에 의하여 생성된다. 실험 결과로부터 제안한 방법이 기존 방법에 비하여 강인성, 유일성이 보다 우수함을 확인하였다.

본 논문의 구성을 살펴보면 다음과 같다. 먼저 2장에서는 제안한 HKS 기반 해싱 기법에 대하여 상세히 살펴보며, 3장에서는 강인성, 유일성 및 모델 공간성에 대한 기존 방법과의 평가 비교를 살펴보고 마지막으로 4장에서는 본 논문의 결론을 맺는다.

2. 3D 모델 해싱

본 논문에서는 제안한 3D 모델 해쉬 생성 과정 및 해쉬 기반 인증 과정은 그림 1에서와 같다. 그림에서 살펴보는 바와 같이, 제안한 해쉬 생성 과정에서는 3D 표면 특징 추출, 매개변수 설정, 중간 해쉬 생

성 및 이진화 과정으로 구성된다. 이 때 매개변수 설정 및 중간 해쉬 생성은 강인성, 유일성 및 공간성 조건을 만족하는 목표치에 도달하도록 반복적으로 수행된다. 해쉬 기반 인증 과정은 해쉬 생성 과정과 동일하며, 전송된 3D 모델과 매개변수와 저장된 키에 의하여 생성된 해쉬와 원 모델의 해쉬와의 해밍 거리차에 의하여 인증을 수행한다.

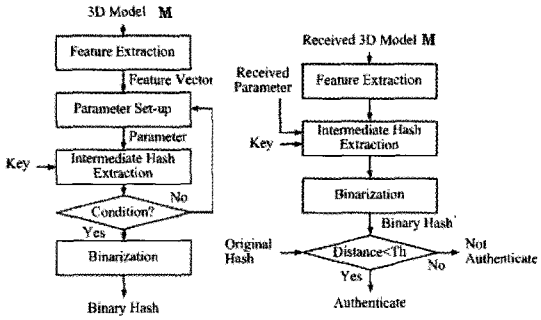


그림 1. (a) 3D 모델의 해쉬 생성 과정 및 (b) 해쉬 기반 3D 모델 인증 과정

2.1 HKS 추출

임의의 꼭지점 $v_i \in V$에서의 HKS는 $k_t(v_i, v_i) = \sum_{j=1}^{n} e^{-\lambda_j t}\phi_j^2(v_i)$와 같이 Laplace-Beltrami 연산자의 고유치 λ와 고유벡터 ϕ에 의하여 구하여진다. 제안한 방법에서는 3D 모델의 표면면적이 100이 되도록 각 꼭지점들을 스케일링한 후, J. Sun의 방법[11]과 동일하게 Belkin[13]이 제시한 메쉬 표면 상의 Discrete Laplace 연산자 $L_K^h f(v)$에 대한 고유치와 고유벡터들을 구한다. 여기서 $L_K^h f(v)$

$$L_K^h f(v) = \frac{1}{4\pi h^2}\sum_{M_v}\frac{S(M_v)}{N_{M_v}} A_{M_v} \quad (1)$$

$$\text{where } A_{M_v} = \sum_{k=1}^{N_M} \exp\left(-\frac{\|v - v_k\|}{4h}\right)(f(v) - f(v_k))$$

와 같이 정의되며, M_v는 v에 연결된 메쉬를 나타내고, N_{M_v}는 M_v 내의 꼭지점 개수를 나타낸다. 위 식을 행렬 형태로 나타내면

$$L_K^h f = A^{-1} W f \quad (2)$$

where $A = diag(4\pi h_i^2)$, $W = diag(w_i) - w_{ij}$

와 같다. 여기서 W의 원소들은

$$w_{ii} = \begin{cases} \frac{1}{2}\sum_{j=1}^{N_{v_i}} (A_{ij,1} + A_{ij,2}) e^{-\frac{\|v_i - v_j\|}{4h_{v_i}}}, & \text{if } i = j \\ -\frac{1}{2}(A_{ij,1} + A_{ij,2}) e^{-\frac{\|v_i - v_j\|}{4h_{v_i}}}, & \text{if } i \neq j \end{cases} \quad (3)$$

와 같이 구하여진다. 여기서 h_i는 v_i에 연결된 메쉬들의 크기에 부합하는 양의 값이다. 본 논문에서는 $n = 300$개의 고유치와 이에 대한 고유벡터들을 구하고 로그 스케일의 타임 구간 $[\ln(t_{\min}), \ln(t_{\max})]$, $(t_{\min} = e^{\ln 10},\ t_{\max} = e^{100 \ln 10})$를 150 타임의 등간격 $\Delta t = (\ln(t_{\max}) - \ln(t_{\min}))/150$으로 나눈 후, 각 타임 $t_i = t_{\min} + (i-1)e^{\Delta t}$ $(i \in [1, 150])$에 대하여 모든 꼭지점들의 HKS를 구한다. 제안한 방법에서는 해쉬 강인성과 HKS의 stable을 높이기 위하여 타임 스케일을 국부 스케일 $(\log(t_{\min}) \leq \log t \leq \log(t_{\min} + 75e^{\Delta t}))$과 전역 스케일 $(\log(t_{\min} + 75e^{\Delta t}) < \log t \leq \log(t_{\max}))$로 나눈 후, 두 스케일 상의 평균 HKS을 꼭지점의 두 계수 벡터 $v_i \rightarrow hks(v_i) = (x_i, y_i)(i \in [1, N_V])$로 사용한다.

2.2 정방형 셀 계수

제안한 방법에서는 국부 및 전역 HKS 계수 X, Y에 대한 2D 정방형 셀을 가지는 히스토그램을 구한다. 이를 위하여 먼저 X, Y를 2D 좌표축으로 정의한 다음, 각 축을 기준으로 독립적으로 중점값을 결정한 후 2D로 확장함으로써 2D 좌표축을 정방형의 셀을 결정한다. 즉, $X \times Y$ 좌표축의 셀 크기는 각 축에 대한 bin 중점값에 의하여 결정되며, bin 크기에 따라 최종 해쉬 비트 길이가 결정된다. L2 risk 함수 [1] 기반의 최소 bin 크기는

$$\text{argmin}_{\Delta} \frac{2\overline{m} - \sigma^2}{\Delta^2}, \quad (4)$$

$$\text{where } \overline{m} = \sum_{i=1}^{k} m_i/k \text{ and } \sigma^2 = \sum_{i=1}^{k} (m_i - \overline{m})^2/k$$

와 같이 $\overline{m}$ and 분산 σ of 히스토그램 크기 h에 의하여 구하여진다. 제안한 방법에서는 모든 꼭지점들의 국부 HKS 계수 X와 전역 HKS 계수 Y에 대하여 최소 bin 크기 Δx_1, Δx_2를 각각 구한 다음, 동일한 bin의 개수가 되도록

$$N=a\min(\lfloor\frac{\max(x)-\min(x)}{\Delta x}\rfloor,\ \lfloor\frac{\max(y)-\min(y)}{\Delta y}\rfloor)+b \tag{5}$$

와 같이 구한다. 따라서 $X\times Y$ 축의 2D 셀의 개수는 $N\times N$으로 이는 해쉬 비트수와 동일하다. 그리고 셀의 개수는 3D 모델에 따라 다르므로, 해쉬 인증시 유일성이 증가된다. 여기서 2D 셀의 개수에 따라 해쉬 비트수 및 셀의 분포가 달라지며, 특히 해쉬의 강인성에 영향을 준다. 따라서 본 논문에서는 변수 a,b를 각각 $a=1/10$, $b=10$으로 놓음으로써 각 축의 bin의 개수가 [10 19]에 있도록 하였으며, 이는 2D 셀의 개수 및 해쉬 비트수의 범위가 [100 361] 된다.

제안한 방법에서는 각 축에 대한 셀 중심값 $\mu=(\mu_x,\mu_y)$들을 이용하여 $X-Y$ 2D 셀 $B=\{B_{ij}=\Delta x_i\times\Delta y_j|i,j\in[1,N]\}$로 확장한다. 이 때, 각 셀에 포함되는 $X-Y$ 쌍 벡터들의 집합은

$$G=\{\boldsymbol{G}_{ij}|i,j\in[1,N]\}, \tag{6}$$

where $\boldsymbol{G}_{ij}=\{hks(\boldsymbol{v}_k)=(x_k,y_k)\in B_{ij}|\ k\in[1,N_{ij}]\}$

와 같으며, 임의의 셀 B_{ij}에 포함될 확률은 $p_{ij}=N_{ij}/N_V$이다. 그림 2 (a)은 $X-Y$ 2D 셀을 보여주고 있다.

2.3 해쉬 생성

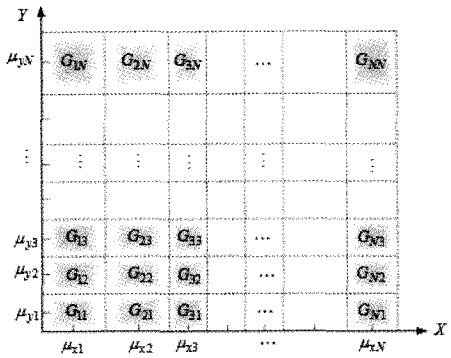
제안한 방법에서는 2D 정방형 셀 상의 계수들을 랜덤 키 패턴으로 투영한 다음, 이들 투영 계수들이 강인성을 가지는 목표치가 되도록 중간 해쉬 벡터들을 생성한 후 이를 이진화에 의하여 최종 이진 해쉬를 획득한다.

먼저 제안한 방법에서는 셀의 중심값 $\mu_{ij}=(\mu_{xi},\mu_{yj})$과 국부 및 전역 HKS 계수 $hks(\boldsymbol{v}_k)=(x_k,y_k)$와의 거리차 $d_k=\|hks(\boldsymbol{v}_k)-\mu_{ij}\|$를 이용한 n차 Butterworth 함수 기반의 가중치 HKS 계수 크기로 셀 계수 b_{ij}를

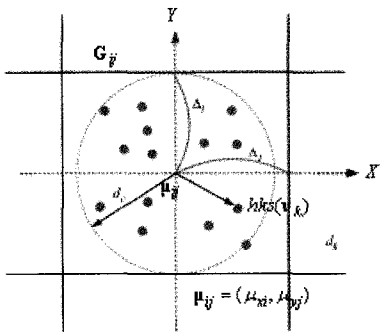
$$b_{ij}=\sum_{k=1}^{N_V}\frac{a_{ij}^2}{1+(d_k/dc_{ij})^n}\times\frac{|hks(\boldsymbol{v}_k)|}{|\mu_{ij}|}, \tag{7}$$

where $|hks(\boldsymbol{v}_k)|=\sqrt{x_k^2+y_k^2}$, $|\mu_{ij}|=\sqrt{\mu_{xi}^2+\mu_{yj}^2}$

와 같이 구한다. 여기서 dc_{ij}는 3dB 주파수 거리로 $dc_{ij}=\min(\|\Delta_i\|,\|\Delta_j\|)$, $\|\Delta_i\|=\|(\mu_{i+1j}-\mu_{ij})/2\|$, $\|\Delta_j\|=\|(\mu_{ij+1}-\mu_{ij})/2\|$와 같이 셀의 좌우 거리 중 최



(a)



(b)

그림 2. (a) $X-Y$ 상에서 2D 정방형 셀 및 (b) 임의의 그룹 G_{ij} 상의 중심값과 거리값 기반의 가중치 히스토그램

소 거리를 나타내며, a_{ij}는 Butterworth 함수의 크기로 강인성 목표치 계수가 되기 위한 해싱 매개 변수로 이용된다. n차 Butterworth 가중치는 그림 2 (b)에서와 같이 셀 중점값 기준으로 차단 주파수 (cutoff frequency) 영역 내의 HKS 계수와 그 이외 영역 외의 HKS 계수들의 가중치를 다르게 주기 위함이다.

각 셀 간의 특징 계수는 인접한 셀 계수들을 이용하여

$$\begin{aligned}f_{ij}&=\sum_{i=1}^{N}b_{ij}+\sum_{j=1}^{N}b_{ij}\\&=\sum_{i=1}^{N}(\sum_{k=1}^{N_V}\frac{a_{ij}^2}{1+(d_k/d_c)^n}\times\frac{|hks(\boldsymbol{v}_k)|}{|\mu_{ij}|})+\\&\quad\sum_{j=1}^{N}(\sum_{k=1}^{N_V}\frac{a_{ij}^2}{1+(d_k/d_c)^n}\times\frac{|hks(\boldsymbol{v}_k)|}{|\mu_{ij}|})\end{aligned} \tag{8}$$

와 같이 구하여진다. 여기서 a_{ij}는 셀 계수의 크기값으로 중간 해쉬 계수 h_{ij}가 강인성 목표치가 되도록 예측되는 해쉬 매개 변수이다. 제안한 방법에서는 $a_{ij}=a_{ij}^{(0)}\alpha_{ij}$로 놓고, 초기치 $a_{ij}^{(0)}$를 [0 1] 범위의 균일

랜덤 계수 $U(0,1)$로 선택하며 a_{ij}를 임의로 1로 놓는다. 여기서 초기치 $a_{ij}^{(0)}$에 대한 특징 계수 f_{ij}를 재정리하면

$$f_{ij}=a_{ij}^{(0)}\Big(\sum_{i=1}^{N}\sum_{k=1}^{N_V}\frac{1}{1+(d_k/d_c)^n}\times\frac{|hks(v_k)|}{|\mu_{ij}|} + \sum_{j=1}^{N}\sum_{k=1}^{N_V}\frac{1}{1+(d_k/d_c)^n}\times\frac{|hks(v_k)|}{|\mu_{ij}|}\Big) = a_{ij}^{(0)}w_{ij} \quad (9)$$

와 같다. 이와 같은 초기 특징 계수 $F=\{f_{ij}|i,j\in[1,N]\}$들을 랜덤 계수 키 $R=\{r_{ij}|i,j\in[1,N]\}$으로 투영함으로써 중간 해쉬 벡터 H_I는

$$H_I=FR^T \quad (10)$$

와 같이 구하여진다. 여기서 R의 원소들은 서로 독립이고, 계수 크기가 특징 벡터와 동일하므로 $H_I=FR$와 같다.

H_I는 이진화 과정에 의하여 최종 이진 해쉬 H가 되므로 H_I에 따라 해쉬 H의 강인성이 결정된다. 따라서 제안한 방법에서는 H_I가 강인성을 가지는 목표치 T가 되도록 셀 계수 크기 $A=\{a_{ij}|i,j\in[1,N]\}$를 예측하며, 이를 원소에 대하여 나타내면

$$hi_{ij}=\sum_{k=1}^{N}\alpha_{ik}f_{ik}r_{kj}=\sum_{k=1}^{N}\alpha_{ik}a_{ik}^{(0)}w_{ik}r_{kj},\ a_{ij}=a_{ij}^{(0)}\alpha_{ij} = \sum_{k=1}^{N}a_{ik}w_{ik}r_{kj}\rightarrow t_{ij} \quad (11)$$

와 같다. 여기서 H_I의 이진화 과정을 위한 문턱치 Th는 H가 0 또는 1이 되는 확률이 $\Pr[H_I<Th]=\Pr[H_I>th]=1/2$와 같이 동일하도록 H_I의 중간값을 이용하여

$$Th=(H_I(rank(N^2/2))+H_I(rank(N^2/2+1))/2 \quad (12)$$

와 같이 설정한다. 이 때 $H_I(rank(i))$는 i번째 높은 값을 가지는 H_I의 계수를 나타낸다. 제안한 방법에서는 보안성 및 공간성을 향상시키기 위하여 $H_I=\{h_{I,ij}|i,j\in[1,N]\}$를 2D 치환 키 P에 의하여 랜덤하게 치환한 후, 이들 계수들을 문턱치 Th를 이용하여 최종 해쉬 벡터 $h_{M,K}$를

$$h_{ij}=\begin{cases}1, \text{if } h_{I,ij}>Th\\ 0, \text{else}\end{cases},\ \forall i,j\in[1,N] \quad (13)$$

와 같이 생성한다. 이와 같이 임의의 모델 M과 키 K=(R,P)가 주어졌을 때, 해쉬 매개 변수 $\Theta(M,K)=(\mu,A)$에 의하여 강인성, 유일성 및 공간성을 만족하는 최종 해쉬 벡터 $h_{M,K}$가 생성된다.

2.4 해쉬 인증

모델 DB HDB에서는 각 모델 M과 키 K별로 해쉬 생성 과정을 통하여 생성된 매개 변수 Θ와 해쉬 h들로 표 1에서와 같이 구성된다. 여기서 키 K는 사용자에 의하여 생성되는 것으로 모델 M과 결합하여 매개변수와 해쉬가 생성된다. 임의의 모델 M_n과 사용자 키 K_{nj}에 대한 인증은 M_n과 K_{nj}에 대한 매개변수 Θ_{nj}와 해쉬 $h_{n,j}$를 DB에서 찾은 다음, 매개변수 Θ_{nj}를 이용하여 해쉬 $h'_{n,j}=H(M_{nj},\Theta_{nj};K_{nj})$를 추출한다. 추출된 해쉬 $h'_{n,j}$와 원 해쉬 $h_{n,j}$와의 정규화된 해밍 거리 차이가 $D(h_{nj},h'_{nj})<0.2$이면 M_n과 K_{nj}를 인증한다.

표 1. 모델별 해쉬 DB 예시

모델	키	변수	해쉬
M_1	K_{11}	Θ_{11}	h_{11}
	K_{12}	Θ_{12}	h_{12}
	⋮	⋮	⋮
	K_{1m_1}	Θ_{1m_1}	h_{1m_1}
⋮	⋮	⋮	⋮
M_n	K_{n1}	Θ_{n1}	h_{n1}
	K_{n2}	Θ_{n2}	h_{n2}
	⋮	⋮	⋮
	K_{nm_n}	Θ_{nm_n}	h_{nm_n}

3. 실험 결과

본 실험에서는 Princeton Shape Benchmark[14]에서 제공하는 1,000개의 모델(.off)들을 VRML 데이터로 변환한 다음 동일한 바운딩 박스 크기가 되도록 재스케일링한 후 이를 제안한 방법의 강인성, 유일성, 공간성 및 보안성 평가를 위하여 사용하였다. 각 평가에 대한 결과는 다음과 같다.

3.1 강인성 평가

강인성 평가 실험에서는 각 테스트 모델별로 100개의 해쉬를 생성한 후, 3ds-max에서 제공하는 다양

한 기하학 공격과 위상학 공격에 대하여 추출된 해쉬의 정규화된 해밍 거리차 $D(\mathrm{h},\mathrm{h}')$, $\mathrm{h}=H(\mathrm{M},\Theta;\mathrm{K})$, $\mathrm{h}'=H(\mathrm{M}',\Theta;\mathrm{K})$를 측정한 다음, 강인성 인증에 대한 오류 확률

$$P_{fn}=1-\Pr[D(\mathrm{h},\mathrm{h}')<0.2] \tag{14}$$

를 분석하였다. 모든 공격에 대한 실험 결과인 그림 3에서는 각 공격의 세기에 따라 정규화된 해밍 거리차와 인증 오류 확률을 볼 수 있다. 정규화된 해밍 거리차는 간단히 해밍 거리차라 하기로 한다.

구부림 실험에서는 3D 모델들을 z축 기준으로 20도-200도까지 구부렸다. 원 모델과 z축을 기준으로 100도로 구부려진 모델은 그림 4 (a) 및 그림 4 (b)에서와 같다. 구부림 실험 결과인 그림 3 (a)의 해밍 거리차를 살펴보면, 매우 낮은 구부림 각도인 10-60도일 까지는 제안한 방법이 3D-SSD 방법에 비하여 4.06×10^{-4}-8.46×10^{-3}정도 높은 거리차 D를 가지나, 구부림 각도 80도부터 제안한 방법이 3D-SSD 방법에 비하여 1.55×10^{-2}-2.36×10^{-2} 정도 낮은 거리차를 나타났다. 또한 80도-200까지 인증 오류 확률 P_{fn} 결과를 살펴보면, 제안한 방법은 6.11×10^{-15}-2.46×10^{-2}으로 모두 98%이상 인증되나, 3D-SSD 방법은 3.88×10^{-8}-1.20×10^{-1}으로 180도까지는 98%이상 인증되나 200도일 때부터 88%로 인증률이 다소 감소된다.

잡음물결 실험에서는 잡음세기를 x,y,z 축 상에 동일하게 수행하여 불규칙한 물결 형태의 형상이 되도록 하였다. 잡음세기가 2.0으로 잡음물결된 모델은 그림 4 (c)에서와 같다. 잡음물결 실험결과인 그림 3 (b)를 살펴보면, 잡음세기가 1.6-2.0일 때 제안한 방법의 해밍 거리차 D는 6.61×10^{-2}-1.23×10^{-1}으로 3D-SSD에 비하여 0.07 정도 낮게 나타났다. 그리고 동일 세기에서 인증 오류 확률 P_{fn}에서는 제안한 방법이 1.05×10^{-10}-2.46×10^{-2}으로 약 97%의 인증률을 보이나, 3D-SSD은 6.82×10^{-2}-4.47×10^{-1}으로 인증률이 매우 낮게 나타났다.

푸쉬 실험에서는 모델의 평균 꼭지점 법선 벡터 방향을 기준으로 바깥쪽 방향으로 모든 꼭지점들을 푸쉬 세기에 따라 푸쉬하였다. 여기서 푸쉬 세기는 평균 꼭지점에 대하여 이동되는 꼭지점들의 거리를 나타낸다. 푸쉬세기가 0.6으로 푸쉬된 모델은 그림 4 (d)에서와 같다. 푸쉬 실험결과인 그림 3 (c)를 살펴보면, 제안한 방법의 해밍 거리차 D는 0.6-1.0 세기일 때 0.148-0.1818으로 3D-SSD에 비하여 6.98×10^{-3}-1.49×10^{-2}정도 다소 낮게 나타났다. 동일 세기에서 인증 오류 확률 P_{fn}를 살펴보면, 제안한 방법이 0.127-0.35 정도로 인증률이 낮게 나타났으나, 3D-SSD에 비하여 약 0.04-0.10정도 높게 나타났다. 즉, 제안한 방법은 푸쉬 세기가 0.4일 때까지 약 95% 이상의 인증률을 나타내나, 그 이상의 세기에서는 90% 미만의 인증률을 나타냈다.

3D 모델들은 메모리 오버헤드를 줄이기 위하여 다양한 메쉬 간단화에 의하여 모델의 형상이 유지되면서 꼭지점과 메쉬의 개수가 줄여진다. 본 실험에서는 3ds-max의 MultiRes 편집기를 이용하여 꼭지점의 개수를 원 개수의 90-20%으로 줄였다. 메쉬 간단화 실험결과는 그림 3 (d)에서와 같으며, 해밍 거리차를 살펴보면 간단화 비율이 60-20%일 때 제안한 방법이 3D-SSD에 비하여 0.016-0.076정도 낮게 나타났으며, 간단화 비율이 40%일 때까지 0.2보다 작음을 볼 수 있다. 인증 오류 확률 P_{fn}를 살펴보면, 제안한 방법이 3D-SSD에 비하여 0.08-0.28정도 낮게 나타났으며, 간단화 비율이 60%일 때 까지 인증률이 약 95% 이상이나, 간단화 비율이 40-20%일 때 인증률이 70%-50%으로 감소됨을 볼 수 있다.

3D 모델들은 메쉬 간단화와는 달리 렌더링시 유연한 곡면을 발생하기 위하여 메쉬 부분할 또는 메쉬 해상도가 증가될 수 있다. 본 실험에서는 3ds-max의 tessellate와 MultiRes 편집기를 이용하여 3D 모델의 꼭지점 개수를 ×1.5-×4.0배로 증가하였다. 메쉬 해상도 업에 대한 실험 결과는 그림 3 (e)에서와 같으며, 해밍 거리차를 살펴보면 제안한 방법은 ×3.0배 까지 0.087-0.165으로 0.2보다 작으나 ×3.5-×4.0배에서 0.20-0.25으로 0.2보다 크게 나타났다. 3D-SSD 방법에서도 ×3.0배 까지는 0.2보다 작으나 ×3.5-×4.0배에서 0.21-0.28으로 제안한 방법보다 더 크게 나타났다. 인증 오류 확률 P_{fn}를 살펴보면, ×2.5배 까지는 제안한 방법과 3D-SSD은 0.043미만으로 인증률이 95% 이상으로 나타났으나, ×3.5배 이상일 때 제안한 방법은 0.50-0.72으로 인증률이 50% 미만이며, 3D-SSD 방법은 0.56-0.79으로 인증률이 46% 미만으로 나타났다.

절단 실험에서는 x축을 기준으로 꼭지점 개수를 10-50% 정도 삭제하였다. 절단 실험 결과인 그림 3 (f)의 해밍 거리차를 살펴보면, 제안한 방법은 3D-

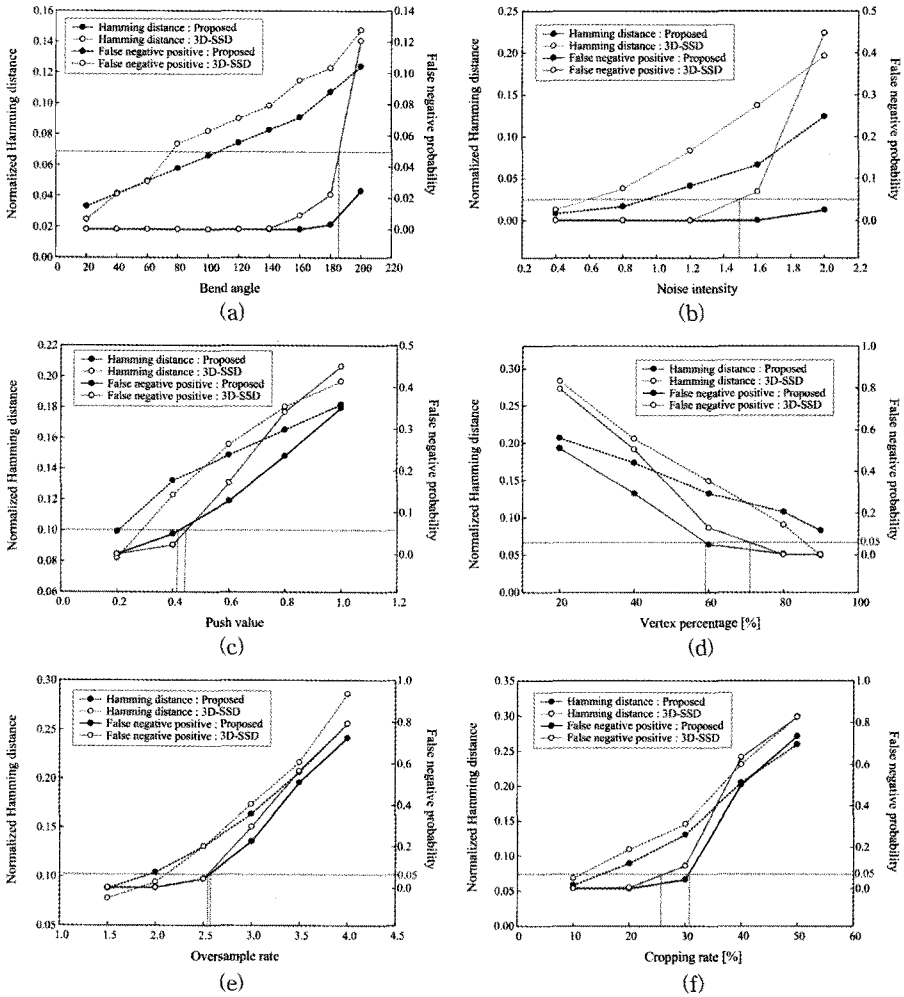


그림 3. (a) 구부림, (b) 잡음 물결, (c) 푸쉬, (d) 메쉬 간단화, (e) 메쉬 부분할, (f) 꼭지점 절단

그림 4. (a) 원 모델과 z축을 기준으로 (b) 100도로 구부려진 모델, (c) 잡음세기 2.0으로 잡음 물결된 모델, (d) 푸쉬세기 0.6으로 푸쉬된 모델

SSD 방법에 비하여 0.01-0.04정도 낮게 나타났으며, 절단량이 30%일 때까지는 0.130 이하나 40-50%일 때 0.204-0.259으로 0.2보다 높게 나타났다. 인증 오류 확률 P_{fn}를 살펴보면, 절단량이 30%일 때까지 제안한 방법은 0.043이하로 인증률이 약 95.7%이상이나 3D-SSD는 0.109으로 인증률이 약 89.1%이상으로 나타났다. 그러나 절단량이 40%이상일 때 제안한 방법은 0.499 이상으로 인증률이 50% 미만이고, 3D-SSD 방법은 0.632 이상으로 인증률이 약 46.8% 미만으로 나타났다.

이상의 결과로부터 제안한 방법이 3D-SSD 방법에 비하여 해쉬의 강인성이 보다 우수함을 확인하였다.

3.2 모델 공간성

모델 공간성 $\Psi(\mathrm{M})$을 평가하기 위하여 본 실험에서는 공격받은 모델 $\mathrm{M}'=attack(\mathrm{M},\alpha)$의 해쉬 $\mathrm{h}=H(\mathrm{M}',\Theta;\mathrm{K})$와 다른 모델 M_k의 해쉬 $\mathrm{h}_k=H(\mathrm{M}_k,\Theta_k;\mathrm{K}_k)$, $(\forall \mathrm{M}_k\neq \mathrm{M}\in \mathrm{HDB})$와의 유일 확률과 강인할 확률의 곱으로 이루어진 모델 공간 확률 P_s이

$$P_s=\Pr[D(\mathrm{h},\mathrm{h}')<0.2]\times\Pr[D(\mathrm{h}_k,\mathrm{h}')>0.3]>0.95 \quad (15)$$

를 만족하는 공격 세기 α를 측정하였다. $P_s>0.95$를 만족하는 모델 공간성 $\Psi(\mathrm{M})$의 공격 세기 α와 이 때 공간확률 P_s는 표 2에서와 같다. 일반적인 기하학 공격인 Bend, noise, push, relax를 살펴보면, 제안한 방법이 3D-SSD에 비하여 1.33-1.66배 정도 높은 공격 세기를 가지므로, 모델 공간성이 보다 넓음을 확인할 수 있다. 또한 메쉬 간단화 및 업-샘플링과 꼭지점 절단에서도 1.1-2배 정도 높은 공격 세기와 이 배율만큼 모델 공간성이 넓음을 확인할 수 있다.

표 2. 모델 공간 $\Psi(\mathrm{M})=\{\mathrm{M},\mathrm{M}'=attack(\mathrm{M},\alpha)\}$내의 공격 세기 α의 범위 및 공간확률 P_s

공 격	제안한 방법		3D-SSD	
	공격 세기	공간 확률	공격 세기	공간 확률
Bend	[0 200]	>0.950	[0 140]	>0.947
Noise	[0 2.0]	>0.947	[0 1.2]	>0.943
Push	[0 0.3]	>0.957	[0 0.2]	>0.948
Mesh down	[0 70%]	>0.957	[0 80%]	>0.953
Mesh up	[x1 x2.2]	>0.950	[x1 x2]	>0.956
Crop	[0 20%]	>0.993	[0 10%]	>0.955

3.3 유일성 평가

유일성에는 모델-키 유일성과 모델-동일 키 유일성으로 나눌 수 있다. 본 실험에서는 모델-키 유일성 평가를 위하여 1,000개 모델 상에서 서로 다른 키에 의하여 생성된 해쉬들간의 정규화된 해밍 거리차를 구한 다음, 유일성 확률 $\Pr[D(\mathrm{h},\mathrm{h}_k)>0.3]$, $\mathrm{h}=H(\mathrm{M},\Theta;\mathrm{K})$, $\mathrm{h}_k=H(\mathrm{M}_k,\Theta_k;\mathrm{K}_k)$, 미결정 확률 $\Pr[0.2<D(\mathrm{h},\mathrm{h}_k)\leq 0.3]$ 및 비유일 확률 $\Pr[D(\mathrm{h},\mathrm{h}_k)\leq 0.2]$으로 나누어 측정하였다. 모델-키 유일성 실험 결과는 표 3에서와 같으며, 제안한 방법의 유일 확률은 99.87%으로 매우 높으나 3D-SSD 방법의 유일 확률은 95.81%으로 제안한 방법에 비하여 약 4.06% 정도 낮음을 확인하였다.

임의의 키를 사용하여 다른 모델을 인증할 수 있다. 그러므로 임의의 키에 대한 다른 모델들의 인증 확률이 작아야 한다. 본 실험에서는 모델-동일 키에 대한 유일성 평가를 위하여 1,000개 모델 중 임의의 모델에 대한 해쉬 $\mathrm{h}=H(\mathrm{M},\Theta;\mathrm{K})$와 나머지 모델에서 동일 키 K를 사용한 해쉬 $\mathrm{h}_k=H(\mathrm{M}_k,\Theta_k;\mathrm{K})$와 동일 키 K 및 변수 Θ를 사용한 해쉬 $\mathrm{h}_k=H(\mathrm{M}_k,\Theta;\mathrm{K})$의 정규화된 해밍 거리차를 구한 다음, 유일 확률, 미결정 확률 및 비유일 확률을 측정하였다. 이에 대한 결과인 표 4를 살펴보면, 제안한 방법에서는 동일 키 K를 사용하더라도 매개변수 Θ에 의하여 유일 확률이 약 98% 이상을 보여준다. 그러나 동일 키 K와 매개변수 Θ에 의한 유일 확률은 약 88% 이상으로 작아지나, 3D-SSD 방법에 비하여 약 2.68%보다 높음을 확인하였다.

표 3. 모델-키 유일성 실험 결과

구 분	Proposed	3D-SSD
$\Pr[D(\mathrm{h},\mathrm{h}_k)>0.3]$	0.99875	0.95815
$\Pr[0.2<D(\mathrm{h},\mathrm{h}_k)\leq 0.3]$	0.00104	0.02298
$\Pr[D(\mathrm{h},\mathrm{h}_k)\leq 0.2]$	0.00021	0.01887

표 4. 모델-동일 키 유일성 실험 결과

구 분	Proposed		3D-SSD
	동일 키 K	동일 키 K와 변수 Θ	
$\Pr[D(\mathrm{h},\mathrm{h}_k)>0.3]$	0.98653	0.883073	0.856239
$\Pr[0.2<D(\mathrm{h},\mathrm{h}_k)\leq 0.3]$	0.01041	0.090909	0.107234
$\Pr[D(\mathrm{h},\mathrm{h}_k)\leq 0.2]$	0.00306	0.026018	0.036527

3.4 보안성 평가

본 논문에서는 해쉬의 보안성을 평가하기 위하여 랜덤 계수 키 기반의 중간 해쉬 계수의 미분 엔트로피 $H(h)$를 모델링한 후, 이를 측정하였다. 제안한 방법의 중간 해쉬 계수는 계수 $a_{ik}w_{ik}$와 랜덤 계수 r_{kj}와의 곱들의 합으로 이루어진다. 여기서 랜덤 계수 r_{kj}

는 정규분포 $N(m_r,\sigma_r^2)$이고, 셀 계수 a_{ik}는 정규분포 $N(m_A,\sigma_A^2)$로 예측되어지므로, 계수 $a_{ik}w_{ik}$는 $N(w_{ik}m_A,w_{ik}^2\sigma_A^2)$ 분포를 가진다. 그러므로 $(a_{ik}w_{ik})\times r_{kj}$는 정규 곱 분포와 같다. 두 계수 $a_{ik}w_{ik}$와 r_{kj}는 유사도가 0이고, 서로 독립이므로, $(a_{ik}w_{ik})\times r_{kj}$의 모멘트 함수 $M_y(x)$는

$$\exp((wm_A)m_r x+\frac{1}{2}((wm_A)^2\sigma_r^2+m_r^2(w\sigma_A)^2)x^2) \quad (16)$$

에 근접하게 되므로, $N(wm_Am_r,w^2\sigma_A^2m_r^2)$의 분포에 가깝게 된다. 따라서 중간 해쉬 계수의 확률밀도 p_{hi}는

$$p_{hi}(x)=N(m_rm_A\sum_{k=1}^{N}w_{ik},((m_A)^2\sigma_r^2+m_r^2\sigma_A^2)\sum_{k=1}^{N}w_{ik}^2) \quad (17)$$

이므로 미분엔트로피 $H(x)$는

$$H=\frac{1}{2}log(2\pi e\sigma^2) \quad (18)$$
$$=\frac{1}{2}log(2\pi e\times((m_A)^2\sigma_r^2+m_r^2\sigma_A^2)\sum_{k=1}^{N}w_{ik}^2)$$

이다. 제안한 방법에서 각 축에 대한 빈 숫자에 대한 미분 엔트로피와 3D-SSD[9]의 미분 엔트로피는 그림 5에서와 같다. 여기서 1,000개 모델 상에서 각 셀 또는 블록 상의 미분 엔트로피를 구한 후, 이 값의 최대, 평균 및 최소를 나타내었다. 제안한 방법의 미분 엔트로피를 살펴보면, 1D 셀의 개수가 10개일 때 H=[9.47 15.22]이나 개수가 증가할 때 H도 증가됨을 볼 수 있으며, 3D-SSD 방법의 미분 엔트로피는 H=[6.92 9.47]로 나타났다. 실험의 평균적인 미분 엔트로피를 살펴보면, 제안한 방법이 3D-SSD에 비하여 약 5.34-14.42정도 높음을 확인하였다.

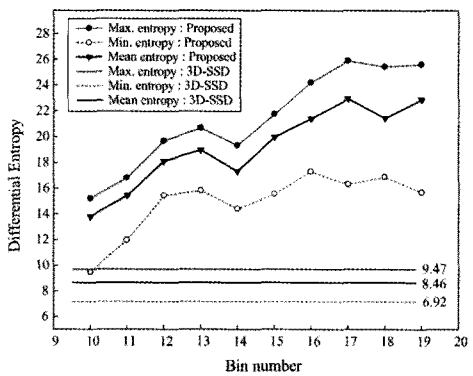


그림 5. 제안한 방법과 3D-SSD의 미분 엔트로피

4. 결 론

본 논문에서는 3D 모델의 인증을 위한 HKS 기반 키-변수에 의존적인 3D 모델 해싱 기법을 제안하였다. 2D 영상 해싱과 동일하게 3D 모델 해싱은 일부 속성들이 상호 보완적인 관계라 할지라도 해쉬의 강인성, 유일성, 보안성 뿐만 아니라 모델 공간성을 만족하여야 한다. 본 논문에서는 이와 같은 요구 조건들을 모두 만족하기 위하여 기존의 키 기반 해쉬 함수보다 키-매개변수 기반 해쉬 함수를 설계하였다. 여기서 해싱 단계 중의 특징 계수 추출은 강인성에 매우 주요한 단계로 제안한 해싱에서는 메쉬 Laplace 연산자의 고유치 및 고유벡터에 의한 HKS 계수들 중 국부 타임 및 전역 타임 스케일 상의 계수들을 정방형 셀로 클러스터링한 후, 각 셀의 HKS 계수들의 거리 가중치를 이용함으로써 특징 계수를 추출하였으며, 이를 렌덤 계수로 투영함으로써 중간 해쉬를 생성하였다. 여기서 매개변수는 각 셀의 크기와 셀 중점값들로 사용된다. 셀의 크기 및 개수는 모델마다 다르게 설정되므로 해쉬의 길이는 모델마다 다르며, 동일 모델 내에서도 다른 매개변수가 설정된다. 그리고 동일 모델 또는 다른 모델 간의 공간성 및 유일성을 높이기 위하여 매개변수 재설정단계가 수행된다. 또한 셀 중점값은 중간 해쉬가 요구되는 강인성 목표치에 도달하도록 설정되므로, 원하는 강인성의 공격 세기에 따라 셀 중점값을 설정할 수 있다. 실험 결과로부터 제안한 해싱이 기존 해싱에 비하여 기하학 공격 및 위상학 공격에 대하여 높은 강인성 및 넓은 모델 공간성을 가지며, 해쉬의 유일 확률이 보다 높으며, 보안성을 위한 미분 엔트로피가 약 5.34-14.42 정도 높음을 확인하였다.

참 고 문 헌

[1] E. J. Delp, "Multimedia Security: the 22nd century approach," *Multimedia Systems*, Vol.11, No.2. pp. 95-97, 2005.

[2] A. Swaminathan, Y. Mao, and M. Wu, "Robust and Secure Image Hashing," *IEEE Trans. on Information Forensics and Security*, Vol.1, No.2, pp. 215-230, 2006.

[3] Y. Mao and M. Wu, "Unicity Distance of

Robust Image Hashing," *IEEE Trans. on Information Forensics and Security*, Vol.2, No.3, part 1, pp. 462-467, 2007.

[4] V. Monga and M.K. Mhcak, "Robust and Secure Image Hashing via Non-Negative Matrix Factorizations," *IEEE Trans. on Information Forensics and Security*, Vol.2, No.3, part 1, pp. 376-390, 2007.

[5] 이석환, 권성근, 권기룡, "익명 Buyer-Seller 워터마킹 프로토콜 기반 모바일 3D 콘텐츠의 기하학적 다중 워터마킹 기법," 한국멀티미디어학회논문지, Vol.12, No.2, pp.244-256, 2009.

[6] 이석환, 권성근, 권기룡, "3D 애니메이션 콘텐츠의 강인성 및 연약성 인증을 위한 동시성 워터마킹 기법," 한국멀티미디어학회논문지, Vol.12, No.4, pp.559-571, 2009.

[7] K. Tarmissia and A. B. Hamza, "Information-Theoretic Hashing of 3D Objects using Spectral Graph Theory," *Expert Systems with Applications*, Vol.36, No.5, pp. 9409-9414, 2009.

[8] S.-H. Lee, E.-J. Lee, and K.-R. Kwon, "Robust 3D mesh hashing based on shape features," IEEE International Conference on Multimedia and Expo, pp. 1040-1043, 2010.

[9] 이석환, 권기룡, "키 기반 블록 표면 계수를 이용한 강인한 3D 모델 해싱," 전자공학회논문지-CI, 제47권, CI편, 제1호, pp. 1-14, 2010.

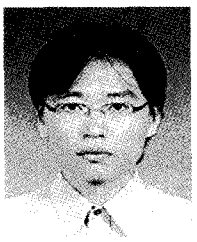
[10] 이석환, 권기룡, "객체별 특징 벡터 기반 3D 콘텐츠 모델 해싱," 전자공학회논문지-CI, 제47권 CI편, 제6호, pp. 75-85, 2010.

[11] J. Sun, M. Ovsjanikov, and L. Guibas, "A Concise and Provably Informative Multi-Scale Signature Based on Heat Diffusion," *Eurographics Symposium on Geometry Processing*, Vol.28, No.5, 2009.

[12] A.M. Bronstein, M.M. Bronstein, B. Bustos, U. Castellani, M. Crisani, B. Falcidieno, L.J. Guibas, I. Kokkinos, V. Murino, M. Ovsjanikov, G. Patane, I. Sipiran, M. Spagnuolo and J. Sun, "SHREC 2010: Robust Feature Detection and Description Benchmark," Eurographics Workshop on 3D Object Retrieval, 2010.

[13] M. Belkin, J. Sun, and J. Wang, "Discrete Laplace Operator on Meshed Surfaces," Proceedings of SOCG, pp. 278-287, 2008.

[14] Princeton Shape Benchmark, http://shape.cs.princeton.edu/benchmark/, Accessed to Dec. 2010.



이 석 환

1999년 경북대학교 전자공학과 졸업(공학사)
2001년 경북대학교 전자공학과 졸업(공학석사)
2004년 경북대학교 전자공학과 졸업(공학박사)
2005년~현재 동명대학교 정보보호학과 부교수
관심분야 : 워터마킹, DRM, 영상신호처리

권 성 근

1996년 경북대학교 전자공학과 졸업 (공학사)
1998년 경북대학교 전자공학과 졸업 (공학석사)
2002년 경북대학교 전자공학과 졸업 (공학박사)
2002년~현재 삼성전자 무선통신사업부 연구원
관심분야 : 영상처리, 영상통신, 정보보호

권 기 룡

1986년 경북대학교 전자공학과 학사 졸업(공학사)
1990년 경북대학교 전자공학과 석사 졸업(공학석사)
1994년 경북대학교 전자공학과 박사 졸업(공학박사)
2000년~2001년 Univ. of Minnesota, Post-Doc.
1996년~2005년 부산외국어대학교 디지털정보공학부 부교수
2006년~현재 부경대학교 전자컴퓨터정보통신공학부 교수
2008년~현재 한국멀티미디어학회 국제담당부회장
관심분야 : 멀티미디어 정보보호, 영상처리, 웨이브릿 변환