

논문 2010-47CI-1-1

키 기반 블록 표면 계수를 이용한 강인한 3D 모델 해싱 (Robust 3D Hashing Algorithm Using Key-dependent Block Surface Coefficient)

이 석 환*, 권 기 룡**

(Suk-Hwan Lee and Ki-Ryong Kwon)

요 약

3D 콘텐츠 산업 분야의 급격한 성장과 더불어, 3D 콘텐츠 인증 및 신뢰, 검색을 위한 콘텐츠 해싱 기술이 요구되어지고 있다. 그러나 영상 및 동영상과 같은 2D 콘텐츠 해싱에 비하여 3D 콘텐츠 해싱에 대한 연구가 아직까지 미비하다. 본 논문에서는 키 기반의 3D 표면 계수 분포를 이용한 강인한 3D 메쉬 모델 해싱 기법을 제안한다. 제안한 기법에서는 기본적인 Euclid 기하학 변환에 강인한 3D SSD와 표면 곡률의 평면계 기반의 블록 표면 계수를 특징 벡터로 사용하며, 이를 치환 키 및 랜덤 변수 키에 의하여 최종 이진 해시를 생성한다. 실험 결과로부터 제안한 해싱 기법은 다양한 기하학 및 위상학 공격에 강인하며, 모델 및 키별로 해시의 유일성을 확인하였다.

Abstract

With the rapid growth of 3D content industry fields, 3D content-based hashing (or hash function) has been required to apply to authentication, trust and retrieval of 3D content. A content hash can be a random variable for compact representation of content. But 3D content-based hashing has been not researched yet, compared with 2D content-based hashing such as image and video. This paper develops a robust 3D content-based hashing based on key-dependent 3D surface feature. The proposed hashing uses the block surface coefficient using shape coordinate of 3D SSD and curvedness for 3D surface feature and generates a binary hash by a permutation key and a random key. Experimental results verified that the proposed hashing has the robustness against geometry and topology attacks and has the uniqueness of hash in each model and key.

Keywords : 3D 모델 해싱(3D model hashing), 블록 표면 계수(Block surface coefficient), SSD(Shape spectrum descriptor), 표면 곡률(Curvedness)

I. 서 론

E.J. Delp는 22세기 콘텐츠 보안 (DRM) 방향에 대한 주요 사항으로 Pre-Pay 모델 또는 Auxiliary Pay 모델

에 기반한 새로운 패러다임의 콘텐츠 결제 시스템이 개발될 것이며, 이 때 콘텐츠의 저작권 보호 개념은 사라질 것으로 판단하였다.^[1] 따라서 그들은 저작권 보호 기술보다 콘텐츠 신뢰, 인증, 포렌식 및 새로운 서비스를 위한 정보은닉 기술이 차세대 멀티미디어 보안 기술의 방향으로 제시하였다.

* 정희원, 동명대학교 정보보호학과
(Dept. of Information security,
Tongmyong University)

** 정희원, 부경대학교 전자컴퓨터정보통신공학부
(Div. of Electnoics, Computer & Telecommunication,
Pukyong National University)

※ 이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임
(KRF-2009-0071269)

접수일자: 2009년12월16일, 수정완료일: 2010년1월11일

이와 같은 콘텐츠 보안 기술 중 하나인 콘텐츠 인증에서는 해시 함수 또는 워터마킹 기술이 사용된다. MD5, SHA-1 등 암호 기반의 해싱 함수들은 모든 메시지 비트가 오류없이 전송될 때 메시지의 무결성을 확인하는 것으로, 메시지 비트 변화에 매우 민감하다. 이와 같은 비트 변화 민감도는 텍스트 메시지 인증에서

중요하지 않으나, 다양한 편집, 압축, 포맷 변환 등이 가능한 디지털 콘텐츠 인증에서 매우 중요한 요소이다. 따라서 암호 기반의 비트 단위 인증 기법들은 콘텐츠 인증에 적합하지 못하다. 워터마킹에서는 인증 관련 정보를 워터마크로 사용하여 이를 콘텐츠 내에 삽입한다. 이 때 콘텐츠 내의 특정 계수들은 워터마크에 따라 변경되므로, 이에 대한 화질 열화가 발생되기도 한다. 워터마킹 기술과는 달리, 특징 벡터(feature vector, FV) 기반의 콘텐츠 해싱에 관한 연구가 많이 이루어지고 있다. 콘텐츠 인증과 함께 콘텐츠 검색 기술에서도 특징 벡터를 추출하여 이를 데이터베이스의 검색 키로 사용한다. 그러나 기존 검색 기법들은 콘텐츠 간의 비교 검색에 의하여 계산 측면에서 효율적이지 못하며, 다양한 편집 및 공격에 대한 강인성을 고려하지 않는다. 이와 같은 검색 기법들의 문제점들은 강인성 콘텐츠 해싱 기법에 의하여 해결될 수 있다.

최근 영상 및 동영상 콘텐츠들의 복사 검출 및 인증을 위한 콘텐츠 해싱 기법들에 대하여 많이 연구되어져 왔다.^[2~8] 콘텐츠 기반 해싱 기법들의 주요 개념으로는 콘텐츠의 특징 벡터를 추출하여 이를 양자화 및 압축 과정에 의하여 이진 해쉬를 만든 다음, 이를 인증 과정에서 사용된다. 여기서 해싱의 강인성은 콘텐츠의 특징 벡터에 의하여 결정되어진다. Swaminathan 등^[2]은 영상 RST 및 필터링에 강인한 Fourier-Mellin 변환 기반의 랜덤 키 해싱 기법과 미분 엔트로피(differential entropy) 기반의 영상 해싱 보안성 평가 방법을 제안하였다. Mao 등^[3]은 Shannon의 Unicity 거리 기반으로 영상 해싱의 보안성을 분석하였다. Monga 등은 비음수(non-negative) 행렬 인수분해(matrix factorization)^[4], FDoG(first derivative of Gaussian) 연산자와 Morlet 웨이블릿에 의한 End-stopped 웨이블릿 변환 기반의 특징 추출^[5], 랜덤 클러스터링^[6] 기반의 강인한 영상 해싱 기법을 제안하였다. Coskun 등^[7]은 3D-DCT와 3D-RBT(random bases transform) 기반의 공간 및 시간축 변환 계수를 이용한 동영상 해싱 기법을 제안하였다. Roover 등^[8]은 키 프레임 영상들의 RASH(radial hASHing) 벡터 기반의 동영상 해싱 기법을 제안하였다. 이상과 같이 최근 연구되어온 콘텐츠 기반 해싱 기법들은 모두 영상 및 비디오 콘텐츠들의 복사 검출, 인증 등을 위한 해싱 기법들이며, 영상 화소가 아닌 그래픽 데이터로 이루어진 3D 콘텐츠에 대하여 적용되지 못한다. 따라서 3D 콘텐츠의 복사 검출 방지 및 인증을

위한 강인한 해싱 기법이 필요하게 되었다.

3D 콘텐츠는 3D 다각형 모델, NURBS 모델, CAD 모델 등 다양한 형태의 모델로 표현되며, 이들 모델들은 많은 3D 산업 분야에서 활용되고 있다. 이들 모델들 중, 본 논문에서는 가장 일반적으로 많이 사용되고 있는 3D 다각형 또는 메쉬 모델에 대한 해싱 기법을 제안한다. 3D 콘텐츠 해싱에서는 영상 해싱과 마찬가지로 특징 벡터 추출, 양자화 및 압축 과정을 수행하여야 한다. 여기서 강인한 3D 해싱을 위한 주요 요구 조건으로는 다양한 기하학 및 위상학 공격에 강인한 3D 특징 벡터 추출이다. 3D 메쉬 모델의 특징 벡터는 3D 검색^[9~13], 분할^[14~15] 및 3D 워터마킹^[16~23] 기법에서도 매우 중요하며, 이를 추출하기 위한 많은 기법들이 제시되었다. 제안한 기법에서는 다양한 기하학 및 위상학적 공격에 대한 강인성과 전처리 과정(preprocessing)없이 랜덤 키에 의한 해쉬 추출을 위하여 여러 가지 3D 메쉬 모델 특징 벡터들 중, 3D SSD(shape spectrum descriptor)와 3D 표면 곡률(curvedness)을 이용한 블록 표면 계수를 특징 벡터로 사용한다. 우선, 제안한 기법에서는 꼭지점별 3D 표면 계수를 이용한 평면계를 블록별로 분할한 다음, 각 블록에 할당되는 꼭지점들의 3D 표면 계수를 구한다. 그리고 치환 키에 의하여 치환된 블록의 표면 계수와 랜덤변수에 의하여 3D 특징 벡터를 구한다. 이들 특징 벡터들은 이진화 과정에 의하여 최종 이진 해쉬로 변환된다. 본 실험에서는 제안한 해싱 기법의 성능 평가를 위하여 강인성 및 유일성을 평가하였다. 강인성 평가 결과로부터 해쉬가 구부림, 잡음 물결, 푸쉬, 신축, 회전, 이동 및 확대 등의 기하학 공격 및 다해상도 변환과 메쉬 부분할 등의 위상학 공격에 강인함을 확인하였다. 또한 생성된 해쉬가 키에 의하여 유일함을 확인하였다.

본 논문의 구성은 다음과 같다. 우선 II장에서는 3D 모델의 콘텐츠 해싱 구조에 대하여 살펴보고, III장에서는 표면 계수 기반 3D 메쉬 모델 해싱에 대하여 살펴보기로 한다. IV장에서는 해쉬의 강인성 및 유일성 평가 실험 결과에 대하여 논의하며, 마지막 장에서는 본 논문의 결론을 맺는다.

II. 콘텐츠 해싱

본 장에서는 Swaminathan^[2] 및 Monga^[4~6] 등이 제시한 영상 해싱 프레임워크를 기반으로 3D 모델 해싱

의 요구 사항 및 일반적인 개념에 대하여 간략히 살펴 보기로 한다. 본 논문에서는 D 를 유한한 3D 모델의 집합, K 를 키의 집합이라 할 때, 임의의 콘텐츠 $D \in D$ 와 키 $k \in K$ 에 의한 해쉬 함수를 $H(D, k)$ 라 하고, 이 함수에 의하여 생성된 해쉬를 $h_{D,k}$ 라 한다. 그리고 키는 완전 랜덤(perfect randomization) 변수라 가정한다.

1. 해싱 요구 사항

대표적인 영상 콘텐츠 해싱 기법에서는 해싱 함수에 대한 세 가지 요구 사항들을 제시하고 있다. 3D 모델에 견주어 이를 요약하면 다음과 같다.

가. 보안성 (Security)

보안성은 해쉬의 예측불가능성(unpredictability)으로, 키를 알지 못할 때 해쉬는 쉽게 예측되지 않아야 한다. Monga 등이 제시한 해쉬의 예측불가능성은 $\Pr(h_{D,k} = v) \approx 1/2^q, \forall v \in \{0,1\}^q$ 와 같이 어떠한 키를 사용하더라도 출력되는 q 비트의 해쉬는 모두 정규화 분포를 가져야 한다는 것이다. Swaminathan 등은 해쉬 보안성은 해쉬 생성 시 사용되는 비밀키에 의하여 제기되며, 단일 방향(one-way)과 충돌 회피(collision-free) 성질들을 해쉬에 적용하였다. 단일 방향성은 해쉬 $h_{D,k}$ 와 해쉬 함수 $H(\cdot)$ 이 주어졌을 때, 키 없이 $h_{D,k} = H(D)$ 를 만족하는 모델 D 를 찾는 것이 계산적으로 어려워야 한다. 그리고 충돌 회피성은 모델 D 와 해쉬 함수 $H(\cdot)$ 가 주어졌을 때, $H(D) = H(\hat{D})$ 를 만족하는 모델 \hat{D} 를 찾는 것이 계산적으로 어려워야 한다. 이를 위하여 그들은 키 기반 랜덤 방식에 의하여 강인성과 보안성을 가지는 영상 해싱 기법을 제안하였으며, 또한 미분 엔트로피에 의하여 해쉬의 랜덤한 양을 측정함으로써 해쉬의 보안성을 평가하였다.

기존 영상 해싱의 보안성과 유사하게 3D 모델 해싱에서도 예측불가능성, 단일 방향성 및 충돌 회피성 등의 보안성을 유지하여야 한다. 이는 특징 추출, 양자화 또는 압축 과정에서 키 기반 랜덤 방식을 적용함으로써 보안성을 유지할 수 있다.

나. 강인성 (Perceptual Robust)

강인성은 해쉬 함수에서 동일한 키 k 가 사용되었을 때 시각적으로 유사한 모델들은 동일한 해쉬를 생성하여야 한다. Monga 등이 제시한 강인성 조건으로는 원

모델 D 와 이와 시각적으로 유사한 모델 \hat{D} 에 생성된 해쉬 $h_{D,k}$ 및 $h_{\hat{D},k}$ 의 차이가 $\Pr(h_{D,k} - h_{\hat{D},k}) \geq 1 - T_1$ ($0 < T_1 < 1$)와 같이 확률적으로 주어진 문턱치 $1 - T_1$ 보다 커야 한다. 예를 들어, 악의적인 사용자가 원 모델 D 를 편집하여도 동일한 해쉬가 생성되어야 한다.

3D 모델들은 2D 영상과는 달리 다양한 기하학적 및 위상학적 형태의 공격에 의하여 시각적으로 유사한 모델들로 변환이 가능하다. 여기서 기하학적 공격으로는 꼭지점 좌표를 변경하는 것으로 구부림, 잠음, 푸쉬, 완화, 리플, 몽롱화, 신축, 점감, 비트림, 꼭지점 제거 및 추가, 회전, 이동 등이 있으며, 위상학적 공격으로는 꼭지점 좌표와 연결 정보를 변경하는 것으로 메쉬 간단화 및 삼각화, 리메쉬, 인덱스 재배열 등이 있다. 이들 공격들은 세기에 따라 원 모델과 매우 유사한 모델들을 생성할 수 있다. 따라서 강인성은 이와 같은 공격에 의하여 변형된 모델에 대해서도 동일한 해쉬를 유지하여야 한다.

다. 유일성 (Uniqueness)

유일성은 다른 모델들 간에 생성된 해쉬들은 확률적으로 독립이어야 한다. 예를 들어, 임의의 두 모델 D_1 및 D_2 에 의하여 생성된 해쉬들이 다를 확률이 $\Pr(h_{D_1,k} \neq h_{D_2,k}) \geq 1 - T_2$ ($0 < T_2 < 1$)와 같이 매우 높아야 한다.

일반적으로 해쉬의 강인성 및 유일성은 정규화된 해밍(hamming) 거리에 의하여 평가된다. 즉, 두 이진 해쉬 h_1 와 h_2 의 정규화 된 해밍 거리 $d(h_1, h_2)$ 는 $d(h_1, h_2) = \sum_{i=1}^N |h_{1,i} - h_{2,i}| / N$ 와 같다. 또한 ROC(received operating characteristics)에 의하여 해쉬의 강인성을 평가할 수 있다.

이상과 같이 해싱 기법들은 보안성, 강인성 및 유일성을 가져야 하나, 이들 성질들은 서로 상호 보완적인 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. 이에 대한 설명은 다음 절에 자세히 언급하기로 한다.

2. 3D 모델 해싱 구조

영상 및 비디오와 유사하게 3D 모델 해싱의 일반적인 구조는 그림 1에서와 같이 3D 모델의 유일한 해쉬 특징 벡터를 추출하여 이를 양자화, 압축 과정을 통하여 이진 해쉬를 생성한 다음, 이를 인증에 사용한다. 여기서 특징 추출 과정은 해쉬의 강인성이 결정되는 것으로 해싱 구조에서 가장 중요하다. 또한 키 기반 랜덤함수를 이용한 특징 추출에 의하여 강인성과 보안성이 같이 고려될 수 있다.

3D 모델의 특징 추출은 3D 검색과 분할 및 3D 워터마킹 등의 분야에서 많이 제시되었다. Bustos 등^[9~10]은 기존 3D 검색 기법들에서 제시된 특징 벡터들을 통계적(statistics) 기반, 구 하모닉스(spherical harmonics) 서술자, 볼륨(volume) 기반, 표면 기하학(shape geometric) 특징 기반 기반의 3D 서술자(3D descriptors)로 분류하였다. 통계적 기반 서술자로는 바운딩 볼륨, 객체 방향, 객체 볼륨 등의 가장 기본적인 서술자, PCA 기반의 매개 변수화된 통계적(parameterized statistics) 서술자, 기하학 3D 모멘트 및 표면 분포의 히스토그램 등이 있다. 구 하모닉스 서술자로는 이들 표현의 광선 기반 표본화(ray-based sampling)와 SFFT(fast fourier transform on sphere) 등이 있다. 볼륨 기반 서술자로는 셀, 섹터 형태의 표면 히스토그램, 점군(point cloud) 서술자, 복셀(voxel) 볼륨 등이 있다. 표면 기하학 기반 서술자로는 표면 곡률, EGI(extended gaussian image) 등이 있다. 특히 표면 곡률은 3D 메쉬 분할에서 영역 확대를 위한 특징 벡터^[14], 3D 삼각화의 최적화에 사용되었다.^[15] MPEG-7에서

는 3D SSD를 3D 표면 기술자로 사용하고 있다.^[11~13] 3D 워터마킹에서는 위상(topology) 정보를 이용한 메쉬 분광 영역 계수^[16], 폴리곤 모델의 다해상도 분해^[17~18], 메쉬 방향 히스토그램 분포^[19~20], 꼭지점 길이 분포^[21~22], 클러스터링 기반의 벡터 분포^[23] 등의 다양한 기하학 및 위상학 특징들을 사용하고 있다.

이상과 같이 3D 검색, 분할 및 워터마킹 분야에서 3D 모델의 표면 특징에 대한 연구가 활발히 진행되어 왔다. 그러나 3D 검색과 분할 분야에서 제시되는 모델 특징들은 3D 모델 해싱에 필요한 다양한 공격에 대한 강인성을 만족하지는 못한다. 그리고 3D 워터마킹 분야에서 제시되는 모델 특징들은 워터마크에 의하여 변형되는 특징들로 다양한 공격에 강인성을 가지나, 모델의 표면 특징들에 대한 표현이 부족하며, 보안성 및 유일성을 만족하지는 못한다. 따라서 3D 모델 해싱에서는 이와 같은 특징 추출 기법들을 이용하여 강인성, 보안성 및 유일성을 모두 만족하도록 설계되어야 한다. 본 논문에서는 이동, 회전 및 스케일링에 독립적인 표면 스펙트럼 기술자 3D SSD^[11~13]와 표면 곡률^[14~15] 기반으로 다양한 공격에 강인한 키 기반 3D 표면 계수 분포를 해쉬 특징 벡터로 사용한다.

3D 모델 특징 추출 과정에서 획득된 해쉬 특징 벡터들은 양자화 및 압축의 이진화 과정에 의하여 최종 이진 해쉬로 변환된다. 이진화 과정은 영상 및 비디오 해싱에서 제시한 기법들을 동일하게 적용할 수 있다. 영상 및 비디오 해싱에 제시된 이진화 과정을 간략히 살펴보면 다음과 같다. Swaminathan 등^[2]은 특징벡터를 양자화 및 그레이 부호화에 의하여 이진 해쉬열을 생성한 다음, 3차 Reed-Muller 복호기를 통하여 압축하였다. 이들은 해쉬의 보안성을 향상시키기 위하여 양자화 단계에서 키 기반 랜덤 양자화기를 사용하거나, 압축 단계에서 양자화된 해쉬 벡터들로부터 해쉬값을 랜덤하게 선택하거나 또는 Reed-Muller 복호기의 차수를 랜덤하게 선택하기도 한다. 또한 키에 의하여 생성된 치환 테이블에 따라 압축 해쉬 비트열을 랜덤하게 치환한다. Monga 등^[5]은 특징 벡터의 정규화된 히스토그램 분포 기반의 양자화기를 이용하여 해쉬의 이진화를 수행하였다. 정규화된 히스토그램은 화질이 유지되는 공격에 대하여 매우 견고하며, 랜덤화된 양자화 출력이 가능하다. Coskun 등^[7]은 공간-시간축에 대한 3D-RBT에 의하여 생성된 변환 계수들을 순위 차(rank-ordered)로 나열된 계수들의 중간값을 기준으로 이진화를 수행하였

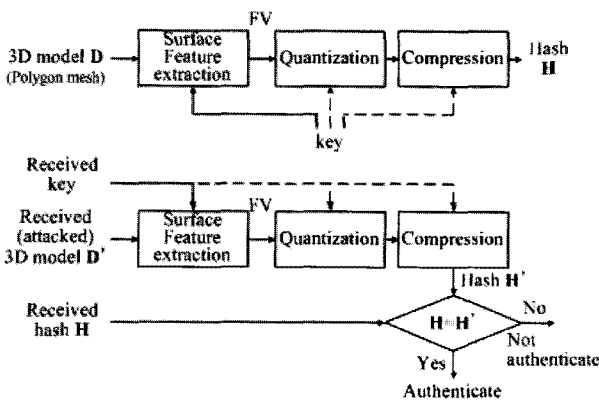


그림 1. 해쉬 생성 과정과 해쉬 기반 인증 과정
 Fig. 1. The process for generating hash and the process for content authentication based on hash.

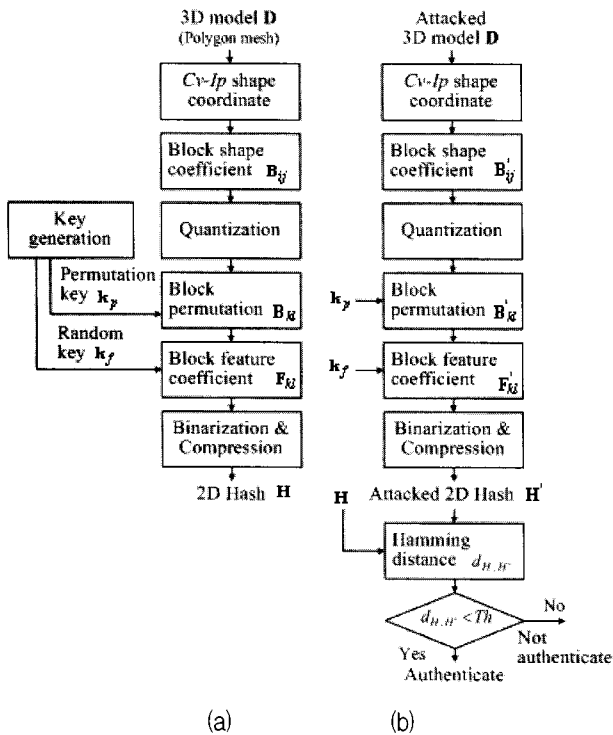


그림 2. 제안한 3D 메쉬 모델 (a) 해쉬 생성 과정 및 (b) 해쉬 기반 인증 과정
 Fig. 2. The proposed process (a) for generating a 3D mesh model-based hash and (b) for authenticating based a hash.

다. 본 논문에서는 이상의 이진화 과정을 기반으로 3D 모델의 특징 벡터 계수들을 이진화하여 최종 해쉬를 생성한다.

III. 제안한 3D 모델 해싱

콘텐츠 기반 3D 모델 해싱을 위하여 본 논문에서는 두 가지 조건을 만족하고자 한다. 첫 번째 조건으로는 다양한 3D 기하학 및 위상학 공격에 강인하면서, 보안성과 유일성을 만족하여야 한다. 두 번째 조건으로는 3D 해쉬 추출 과정에서 어떠한 전처리 과정이 없어야 한다. 즉, 이동, 회전, 스케일링 또는 메쉬 간단화 등에 의하여 변형된 3D 모델들을 이전 모델로 변환하는 과정 없이 바로 추출이 가능하여야 한다. 이를 위하여 제안한 방법에서는 우선 공격에 강인한 특징점 추출에 초점을 맞추며, 랜덤 키 기반의 해쉬 계수 생성에 의하여 보안성과 유일성을 만족하고자 한다. 이 때 제안한 방법에서는 이동, 회전, 스케일링에 강인하며, 전처리 과정이 필요없는 3D 표면 계수 분포를 모델 특징 계수로 사용한다.

제안한 3D 모델 해쉬 생성 과정 및 해쉬 기반 인증 과정은 그림 2에서와 같다. 그림에서 살펴보는 바와 같이, 제안한 해쉬 생성 과정은 3D 표면 계수 평면계의 블록 분할, 각 블록의 표면 계수 양자화 및 블록 치환을 통한 특징 계수 추출, 이진화 및 압축을 통한 해쉬 H 생성으로 구성된다. 이 때 블록 치환 및 블록 특징 계수는 치환 키 k_p 및 랜덤계수 키 k_f 에 의하여 구하여진다. 해쉬 기반 인증 과정은 해쉬 생성 과정과 동일하며, k_p 및 k_f 에 의하여 생성된 해쉬 h' 와 원 모델의 해쉬 h 와의 해밍 거리 차에 의하여 인증을 수행한다.

1. 해쉬 생성

가. 표면 계수의 평면계

제안한 방법에서는 공격에 강인한 3D 메쉬 모델 해싱을 위하여 표면 곡률 $C(v)$ 와 SSD 표면 인덱스 $I(v)$ 의 크기 분포를 3D 표면 특징으로 사용한다. 표면 곡률 $C(v)$ 와 표면 인덱스 $I(v)$ 는 스케일링과 Euclidean 변환에 대하여 변하지 않는다. 임의 객체의 기하학적 형상은 구부림 에너지로 알려진 표면 곡률에 의하여 정의될 수 있다. 임의의 꼭지점 v 에서 표면 곡률 $C(v)$ 는 주 곡률 벡터 $k_1(v)$ 와 $k_2(v)$ 에 의하여

$$C(v) = \sqrt{(k_1^2(v) + k_2^2(v))/2} \quad (1)$$

와 같이 정의되는 곡률 세기이다. 여기서 주곡률 벡터 $k_1(v)$ 와 $k_2(v)$ 는 평균 곡률 $H(v)$ (mean curvature)와 가우시안 곡률 $K(v)$ (Gaussian curvature)에 의하여

$$k_1(v) = H(v) + \sqrt{H^2(v) - K(v)}, \quad (2)$$

$$k_2(v) = H(v) - \sqrt{H^2(v) - K(v)}$$

와 같이 정의된다. 여기서 $H(v)$ 및 $K(v)$ 는 각각

$$H(v) = \frac{\sum \|e_i\|^2 \beta_i / 4}{A/3}, \quad K(v) = \frac{2\pi - \sum \alpha_i}{A/3} \quad (3)$$

와 같다. 여기서 e_i 는 v 와 이에 연결된 꼭지점 v_i 과의 거리 $\|\overrightarrow{vv_i}\|$ 이고, β_i 는 v 와 v_i 를 잇는 선을 포함하는 두 메쉬 간의 2면각을 나타낸다. 그리고 A 는 v 에 연결된 메쉬 M_i ($i \in [1, N_M]$) 면적들의 합이며, θ_i 는 v 에 연결된 메쉬 M_i 상의 각도를 나타낸다. MPEG-7에서는 3D 메쉬 모델의 고유한 표면 기술자로 SSD를 사용하며, 이는 두 개의 주 곡률 (principal curvature)에 의하여 정

의된 표면 인덱스이다. 임의의 꼭지점 v 에서 두 주 곡률이 $k_1(v)$ 와 $k_2(v)$ 라 할 때, v 의 표면 인덱스 $I(v)$ 는

$$I(v) = \frac{1}{2} - \frac{1}{\pi} \tan^{-1} \frac{k_1(v) + k_2(v)}{k_1(v) - k_2(v)}, k_1(v) \geq k_2(v) \quad (4)$$

와 같이 주 곡률 벡터의 극 좌표계에서 위상축(angular coordinate)으로 정의된다. 여기서 $k_1(v) = k_2(v)$ 일 경우 또는 평면(planar surface) 상에서는 표면 인덱스 $I(v)$ 가 정의되지 못하므로, 이 경우 제안한 방법에서는 $I(v)$ 를 0으로 놓는다. 여기서 두 주 곡률 벡터 $k_1(v)$ 와 $k_2(v)$ 는 일반적으로 Weingarten map(W)의 고유값으로 정의되나, 본 논문에서는 표면 곡률에서 계산되어지는 평균 곡률과 가우시안 곡률에 의하여 얻어진 주 곡률을 사용한다.

제안한 방법에서는 꼭지점과 연결정보로 구성된 3D 메쉬 모델 $D = \{V, M\}$ 의 각 꼭지점 $v_n \in V$ 들을 표면 곡률 $C(v_n)$ 과 표면 인덱스 $I(v_n)$ 의 쌍 $(C(v_n), I(v_n))$ 로 표현한다.

나. 블록 표면 계수

제안한 방법에서는 그림 3 (a)에서와 같이 2차원 평면계 $C(v) - I(v)$ 를 $V \times H$ 크기의 블록으로 분할한 다음, 각 꼭지점들을 $(C(v_n), I(v_n))$ 에 따라 각 블록으로 할당한다. 표면 곡률 $C(v)$ 및 표면 인덱스 $I(v)$ 는 각각 $C(v) \geq 0$ 및 $0 \leq I(v) \leq 1$ 이므로, 평면계 $C(v) - I(v)$ 는 정방형이 아니다. 따라서 $C(v)$ 및 $I(v)$ 축들은 각각 일정한 크기 $V = C(v)_{\max}/N_V$ 및 $H = 1/N_H$ 으로 분할될 수 있다. 여기서 블록 크기 $H \times V$ 는 해쉬 길이에 영향을 주며, 또한 강인성과 보안성 및 유일성에도 영향을 준다. 즉, 블록 크기가 클수록 강인성은 증가하나 보안성 및 유일성이 감소된다. 이와 반대일 경우 강인성은 감소되나 보안성 및 유일성은 증가된다. 본 논문에서는 실험적으로 평면계의 블록 개수가 $N_V \times N_H = 40 \times 20$ 이 되도록 블록의 크기를 결정하였다.

각 꼭지점들 $v_n \in V$ 은 $(C(v_i), I(v_i))$ 에 따라 각 블록 $B_{ij} (i \in [1, N_V], j \in [1, N_H])$ 으로 할당된다. 이 때 각 블록 B_{ij} 의 중점은 $(\frac{2i+1}{2}V, \frac{2j+1}{2}H)$ 이고, 블록 B_{ij} 로 할당된 꼭지점들의 집합 B_{ij} 은

$$B_{ij} = \{v_n \mid iV \leq C(v_n) < (i+1)V \text{ and } jH \leq I(v_n) < (j+1)H\} \quad (5)$$

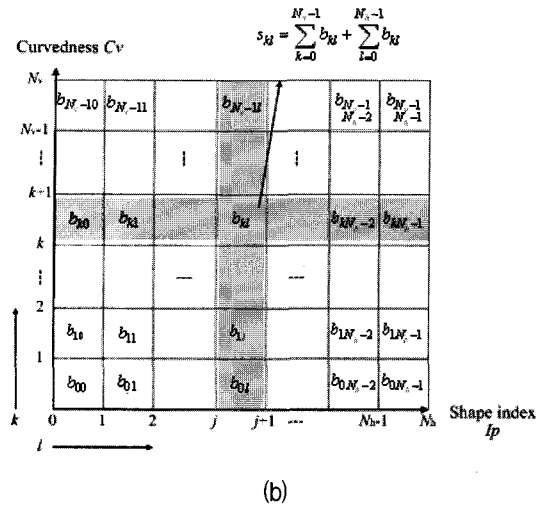
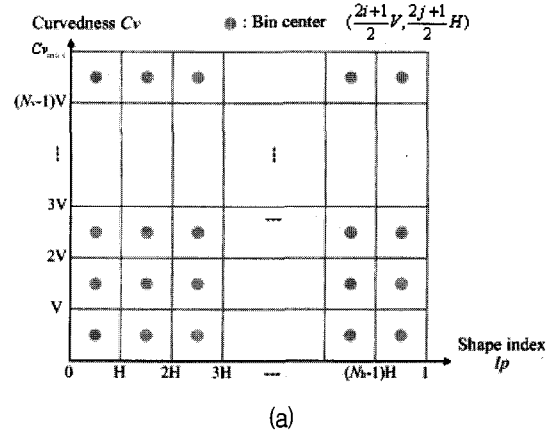


그림 3. (a) $V \times H$ 크기의 블록으로 분할된 2차원 평면계 $C(v) - I(v)$ (b) 랜덤 치환된 블록의 특징 계수

Fig. 3. (a) $C(v) - I(v)$ 2D shape coordinate that is segmented to $V \times H$ blocks. and (b) block feature coefficient with random permutation.

이다. 이 때 꼭지점의 표면 계수 $d(v_n)$ 는

$$d(v_n) = \sqrt{(C(v_n)^2 + I(v_n)^2)/2} \quad (6)$$

와 같이 $(C(v_i), I(v_i))$ 의 크기 계수로 정의된다. 제안한 방법에서는 블록 집합 B_{ij} 내 꼭지점들의 표면 계수 $d(v_n)$ 합을 구한 다음, 이를 블록 표면 계수 $b_{ij} = \sum_{v_n \in B_{ij}} d(v_n)$ 로 사용한다.

각 블록들은 표면 곡률-인덱스 쌍 $(C(v_i), I(v_i))$ 에 따라 분할되므로, 꼭지점 표면 계수는 블록마다 크기가 다르다. 예를 들어, 블록의 인덱스가 $i < i', j < j'$ 이고, 블록 B_{ij} 와 $B_{i'j'}$ 으로 할당된 두 꼭지점의 표면 계수가 각각 $d(v_n)$ 과 $d(v_{n'})$ 일 때, 항상 $d(v_n) < d(v_{n'})$ 이다. 즉

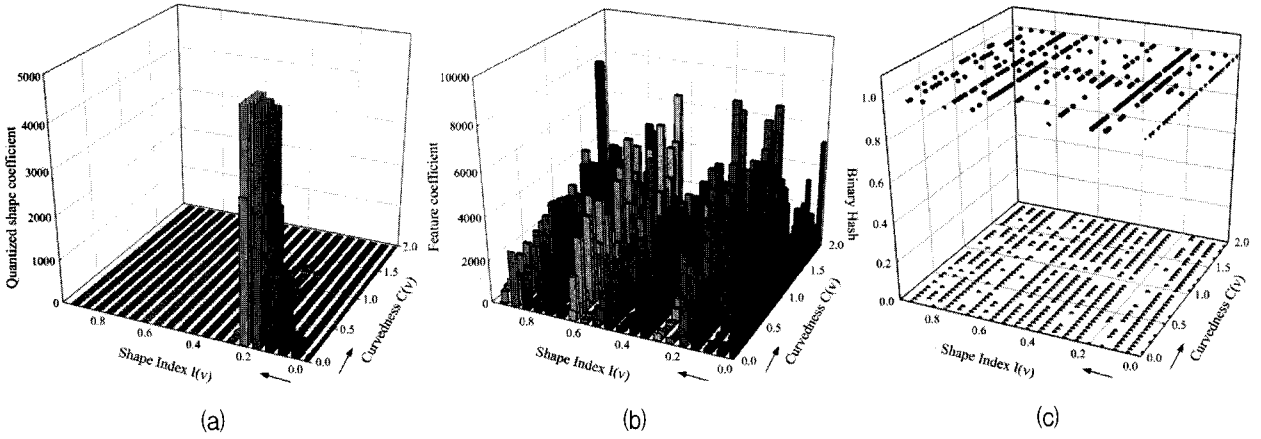


그림 4. Bunny 모델의 (a) 양자화된 블록 표면 계수, (b) 랜덤 키 기반의 블록 특징 계수 및 (c) 최종 이진 해쉬
 Fig. 4. (a) Quantized block shape coefficient, (b) block feature coefficient dependent on random key and (c) a final binary hash of Bunny model.

블록 B_{ij} 와 $B_{i'j'}$ 내에 할당된 꼭지점 개수가 동일할 경우, 두 블록의 표면 계수는 항상 $d_{ij} < d_{i'j'}$ 이다. 따라서 제안한 방법에서는 각 블록 표면 계수 b_{ij} 를 동일한 양으로 정규화하기 위하여 각 블록의 중점 표면 계수 g_{ij} 로 b_{ij} 를 양자화한다.

$$\hat{b}_{ij} = \sum_{v_n \in B_{ij}} d_{ij} / g_{ij}, \quad (7)$$

$$g_{ij} = \sqrt{\left(\left(\frac{2i+1}{2}V\right)^2 + \left(\frac{2j+1}{2}H\right)^2\right) / 2}$$

이 때 보안성을 향상시키기 위하여 랜덤 양자화기를 이용하거나, 랜덤 계수 r_{ij} 를 이용하여 $\hat{b}_{ij} = \sum_{v_n \in B_{ij}} d_{ij} / r_{ij} g_{ij}$ 와 같이 양자화할 수 있다.

다. 블록 특징 계수

각 블록 B_{ij} 의 위치 (i, j) 는 $(N_V \times N_H)$ 크기의 치환 키 k_p 에 의하여 랜덤 치환된다. 즉, 블록 B_{ij} 는 임의의 위치 (k, l) 로 치환된다. 랜덤 치환된 블록 B_{kl} 의 특징 계수 f_{kl} 는 그림 3 (b)에서와 같이 k 번째 행의 블록 표면 계수 합과 l 번째 열의 블록 표면 계수 합 $f_{k,l} = \sum_{k=1}^{N_V} b_{kl} + \sum_{l=1}^{N_H} b_{kl}$ 이다. 이 때 제안한 방법에서는 $[0, 1]$ 의 균등 분포(uniformly distribution)를 가지는 $(N_V \times N_H)$ 크기의 랜덤 계수 키 $k_f = \{\gamma_{k,l} | k \in [1, N_V], l \in [1, N_H]\}$ 에 의하여 랜덤 키 기반의 특징 계수 벡터 F 를

$$F = \{f_{kl} | k \in [1, N_V], l \in [1, N_H]\}, \quad (8)$$

$$f_{k,l} = \gamma_{k,l} \left(\sum_{k=1}^{N_v} b_{kl} + \sum_{j=1}^{N_h} b_{kl} \right)$$

와 같이 얻는다. 이 때 보안성을 향상시키기 위하여 특징 계수 f_{kl} 은 행과 열에 대하여 각각 랜덤 계수를 곱함으로써 $f_{k,l} = \gamma_k \sum_{k=1}^{N_V} b_{kl} + \gamma_l \sum_{l=1}^{N_H} b_{kl}$ 와 같이 얻을 수 있다.

라. 해쉬 생성

블록 특징 계수 f_{kl} 들은 이진화 과정에 의하여 최종적인 이진 해쉬로 변환된다. 제안한 방법에서는 간단한 임계화(thresholding)를 이용하여 블록 특징 계수를 최종 이진 해쉬를 변환한다.

$$h = \{h_{kl} | k \in [1, N_v], l \in [1, N_h]\} \quad (9)$$

$$h_{kl} = \begin{cases} 1, & f_{kl} > T \\ 0, & f_{kl} \leq T \end{cases} \text{ where } T = E[f_{kl}]$$

여기서 임계화에 사용된 문턱치 T 는 모든 블록의 평균 특징 계수이다.

그림 4에서는 Bunny 모델의 양자화 된 블록 표면 계수 \hat{b}_{ij} , 치환 및 랜덤 키 기반의 블록 특징 계수 $f_{k,l}$ 및 최종 이진 해쉬 $h_{k,l}$ 를 보여준다. 여기서 $i \in [1, 40]$, $j \in [1, 20]$ 이고, 블록 크기 $V \times H$ 는 0.05×0.05 이다. 우선 그림 4 (a)의 양자화 된 블록 표면 계수 \hat{b}_{ij} 를 살펴보면, 표면 인덱스 $I(v)$ 가 $[0.05, 0.25]$, 표면 곡률 $C(v)$ 가 $[0.05, 0.5]$ 일 때, 많이 분포되어 있음을 볼 수 있다. 이는 $[0.05, 0.5]$ 사이의 표면 곡률을 가지는 오목한 구형 컵 (Concave spherical cup) 형태와 홈(rut) 형태의 표면이

많이 분포되어 있음을 보여준다. 블록 표면 계수는 각 모델의 주요 형태에 따라 다르게 나타나지만, 그림 4 (a)에서와 같이 특정 영역에 많이 분포되어 있으므로 모델의 블록 표면 계수 분포는 쉽게 유추될 수 있다. 따라서 제안한 방법에서는 이를 치환키에 의하여 블록 치환을 수행한 다음, 랜덤변수 키에 의하여 블록 특징 계수를 구함으로써 보안성을 향상시킨다. 그림 4 (b)의 랜덤 키 기반의 블록 특징 계수 $f_{k,l}$ 를 살펴보면, $f_{k,l}$ 가 랜덤하면서, 다양하게 분포되어 있음을 볼 수 있다. 그림 4 (c)는 랜덤 키 기반의 블록 특징 계수 $f_{k,l}$ 를 평균 특징 계수에 의한 임계화에 따라 생성된 최종 이진 해쉬를 보여준다.

2. 해쉬 인증

사용자에게 전송 또는 공격된 3D 모델 D' 의 해쉬 인증 과정에서는 그림 1 (b)에서와 같이 저장된 치환 키 k_p 와 랜덤변수 키 k_f 를 이용하여 $C(v) - I(v)$ 평면계의 블록 특징 계수 F' 및 이진화에 의하여 해쉬 h' 를 추출한다. 이 때 해쉬 인증 과정에서는 원 모델의 위치, 방향, 스케일링 등으로 변환하는 전처리 과정 없이 해쉬 추출이 가능하다.

제안한 방법에서는 추출된 해쉬 h' 와 원 해쉬 h 와의 정규화된 해밍 거리차 $d(h, h')$ 를 이용하여

$$\begin{aligned} & \text{A if } d(h, h') < Th_R \\ & \text{NA if } d(h, h') > Th_R \end{aligned} \quad (10)$$

$$\text{where } d(h, h') = \frac{1}{N_V \times N_H} \sum_{i=1}^{N_V} \sum_{j=1}^{N_H} |h_{i,j} - h'_{i,j}|$$

와 같이 3D 모델 D' 를 인증(A) 또는 비인증(NA)을 판별한다. $d(h, h')$ 가 0.5에 가까울수록 D' 와 D 는 서로 별개의 모델이고, 0에 가까울수록 D' 와 D 는 동일 모델로 판별된다. 또한 해쉬의 유일성 평가를 위하여 제안한 방법에서는 모델 D 과 이와 다른 모든 모델 $D_k (\in DB)$ 에서 추출된 해쉬 h 및 h_k 와의 정규화된 해밍 거리차 $d(h, h')$ 가

$$\text{Unique, if } d(h, h_k) > Th_U \quad \forall D, D_k \in DB \quad (11)$$

와 같이 Th_U 보다 작으면, 해쉬의 유일성을 판별한다. 본 논문에서는 해쉬의 강인성 문턱치 $Th_R=0.15$ 와 유일성 문턱치 $Th_U=0.35$ 으로 설정하였다.

IV. 실험결과

본 실험에서는 기존 워터마킹에서 많이 사용되어진 Bunny, Venus, Knots 모델을 포함한 100개 3D 메쉬 모델들을 이용하여 제안한 방법의 강인성, 유일성 및 보안성 평가를 수행하였다. 이 때 3D 메쉬 모델들은 다양한 꼭지점 개수 및 메쉬 개수를 가지며, 동일한 파일 포맷을 위하여 VRML 데이터로 변환된다. 실험에 사용된 평면계의 블록 개수는 40×20 이므로 압축 및 정정 부호를 사용하지 않을 경우, 최종 이진 해쉬는 800 비트이다. 기존 방법들은 영상 및 비디오에 대한 해싱 기법들로 제안한 3D 메쉬 모델 해싱과는 비교 평가 대상이 아니므로, 본 실험에서는 제안한 방법에 대한 평가를 수행하였다.

1. 강인성 평가

강인성 평가 실험에서는 3D 범용 편집툴인 3DS-MAX에서 제공하는 구부림(Bending), 잡음(Noising), 푸쉬(Pushing), 신축(Stretching), 다해상도(Multi-resolution) 및 부분할(Tessellate)과 이동(Translation), 회전(Rotation) 및 스케일링(Scaling)을 공격으로 수행하였다. 이 때 3D 메쉬 모델의 형상을 유지하는 공격(Content-Preserved Attack)이 되도록 세기를 조정하였다. 실험 결과로는 그림 5에서와 같이 모든 테스트 3D 메쉬 모델들을 동일한 세기의 공격을 수행한 후 추출된 해쉬와 원 해쉬와의 정규화된 해밍 거리차들의 평균으로 나타내었다. 여기서 제안한 블록 표면 계수의 특징 벡터는 이동, 회전 및 스케일링에 전혀 변형이 없다. 따라서 이들 공격에는 해쉬의 오류가 전혀 없음을 확인하였다.

가. 다해상도 변형 (메쉬 간단화)

다해상도 변형 또는 메쉬 간단화(Mesh Simplification)는 모델을 렌더링하기 위해 필요한 메모리의 오버헤드를 줄이기 위하여 꼭지점 및 메쉬의 개수를 줄이는 것이다. 원 모델의 형상을 유지하면서 꼭지점 및 메쉬를 줄이는 3D 모델의 다해상도 변형 기법들은 QEM(Quadratic Error Metric) 기반, 점진적 메쉬(Progressive mesh) 등 다양하게 제안되어져 왔다.

본 실험에서는 꼭지점 개수 비율을 50~90%으로 가변하면서, 3D 메쉬 모델들을 간단화하였다. 그림 5는 원 모델인 100%와 70% 및 50%으로 간단화된 Bunny 모

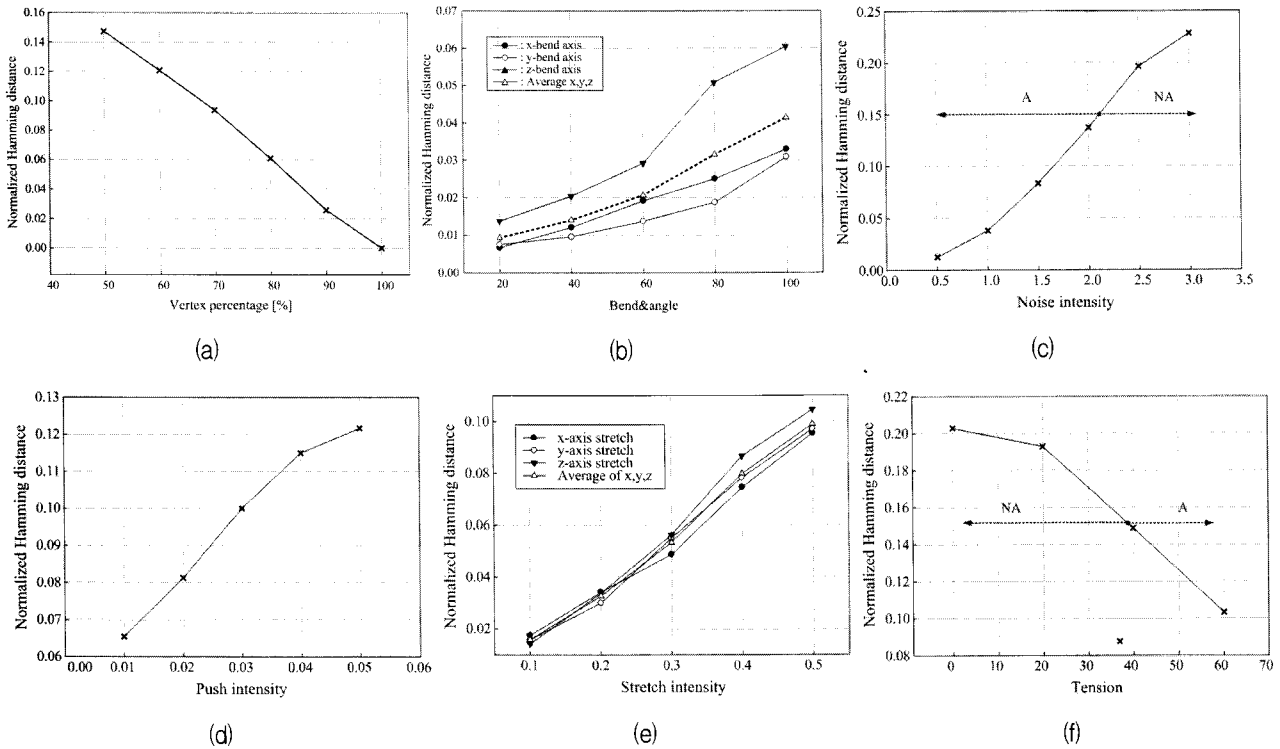


그림 5. (a) 다해상도 변형, (b) 구부림, (c) 잡음, (d) 푸쉬, (e) 신축 및 (f) 부분할에 대한 평균 정규화된 해밍 거리차
 Fig. 5. Normalized Hamming distance in (a) multires, (b) bending, (c) noising, (d) pushing, (e) stretching and (f) tessellating attacks.

델의 와이어프레임 일부분을 보여주고 있다. 그림을 살펴보면, 꼭지점 및 메쉬의 비율이 작아지더라도 원 모델의 형상이 유지됨을 볼 수 있다. 또한 다해상도 변형에서는 꼭지점의 좌표 및 메쉬의 연결성이 변경되며, 또한 꼭지점 정렬 인덱스가 변경된다. 따라서 다해상도 변형에서는 꼭지점 및 메쉬의 기하학 및 위상 정보가 모두 변경되며, 또한 이들 개수가 줄어지면서 꼭지점 정렬 인덱스가 변경된다. 3D 해상에서는 이와 같은 기하학 및 위상 정보와 꼭지점 정렬 인덱스가 모두 변경이 되더라도 해쉬를 추출할 수 있어야 한다. 제안한 블록 특징 계수는 별도의 전처리 과정없이 다해상도 변형된 모델에 대하여 추출이 가능하다.

모든 테스트 모델에 대한 정규화된 해밍 거리차 $d(h, h')$ 는 그림 5 (a)에서와 같이 꼭지점 비율이 [50% 90%]일 때 [0.1475 0.0258]이다. 낮은 꼭지점 비율로 간단화된 모델에서는 각 꼭지점별 인접한 메쉬들의 개수, 면적, 거리 및 연결 정보 등이 모두 변경되므로, 표면 인덱스와 표면 곡률의 변경량이 크다. 그러나 원 모델의 형상을 유지하면서 꼭지점 비율이 낮아지므로, 블록 표면 계수 분포의 변경은 크지 않다. 즉, 꼭지점 비율이

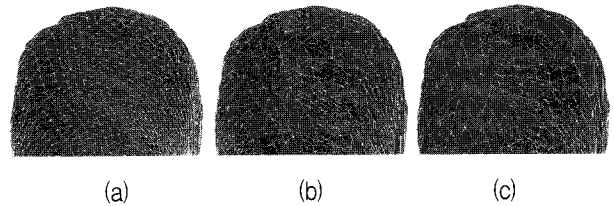


그림 6. (a) 100%, (b) 70% 및 (c) 50%으로 간단화된 Bunny 모델의 부분 와이어프레임
 Fig. 6. Part of wireframe Bunny model simplified to (a) 100%, (b) 70%, and (c) 50%.

50%배로 줄이더라도 $d(h, h')$ 는 0.1475로 입증됨을 알 수 있으며, 이는 추출된 해쉬 h' 의 약 85%이상이 오류가 없음을 보여준다. 따라서 제안한 해싱 기법에서는 약 0-1/2배까지 간단화된 모델에 대하여 강인함을 확인할 수 있다.

나. 구부림

객체 구부림은 임의의 축을 기준으로 방향과 각도에 따라 모델의 객체를 균일하게 구부린다. 여기서 각도는 수직 평면으로부터 구부러지는 각도이고, 방향은 수평 평면에 대응하는 구부림의 방향을 나타낸다. 구부림에

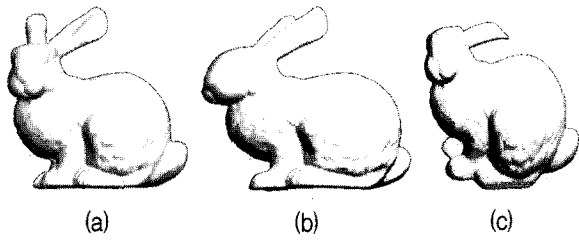


그림 7. (a) 원 Bunny 모델과 (b) x축, (c) y축 방향으로 100° 구부러진 Bunny 모델
 Fig. 7. (a) Original Bunny model and models bended to (b) x-axis and (c) y-axis with 100°.

의하여 꼭지점의 좌표는 변경되나, 꼭지점 배열 인덱스 및 메쉬 연결성은 변경되지 않는다. 구부림 실험에서는 각 모델들을 x,y,z 축을 기준으로 방향 및 각도를 동일한 값인 (20° 20°)에서 (100° 100°)으로 구부렸다. x,y 축을 기준으로 (100° 100°)의 방향 및 각도로 구부러진 Bunny 모델은 그림 7에서와 같다. 그림을 살펴보면, 각 축에 대하여 모델 형상이 구부러져도 원 모델과 같이 인증되어야 함을 볼 수 있다.

각 축에 대하여 구부러진 모델의 해쉬에 대한 정규화된 해밍 거리차 $d(h,h')$ 는 그림 5 (b)에서와 같다. x,y 축에 대하여 $d(h,h')$ 는 약 7.5×10^{-3} - 3.29×10^{-2} 으로 매우 낮으며, z축에 대하여 $d(h,h')$ 는 1.3×10^{-2} - 6.0×10^{-2} 으로 x,y축에 비하여 조금 높다. 그러나 이 값들은 인증 문턱치인 T_h 보다 매우 작은 값이다. 이는 모델의 꼭지점별 표면 인덱스 및 표면 곡률의 변경량은 모델 전체 형상 구부림에 대하여 크지 않으므로, 추출된 해쉬 h' 의 오류가 거의 없음을 보여준다. 따라서 제안한 해상 기법이 구부림 공격에 대하여 매우 강인함을 확인할 수 있다.

다. 잡음 물결

잡음 변형은 x,y,z 축의 각 세기에 따라 모델의 꼭지점 위치들을 랜덤하게 변조하는 것이다. 이 때 프랙탈 (Fractal)을 적용함으로써 랜덤한 물결 패턴으로 변조된다. 잡음 변형은 전체적인 물결 패턴에 따라 모든 꼭지점들의 위치가 랜덤하게 변경이 된다. 그러나 구부림에서와 같이 꼭지점 배열 인덱스와 메쉬 연결정보는 변경되지 않는다. 잡음 변형 실험에서는 프랙탈의 거침 정도([0 1])를 1로 설정하고, x,y,z 축의 잡음 세기를 모두 동일하게 (0.5,0.5,0.5)-(3.0,3.0,3.0)으로 변형하였다. 잡음 세기가 1.0과 2.0으로 변형된 Bunny 모델은 그림 8에서와 같다. 이 그림을 살펴보면, 각 축의 세기에 대한 큰

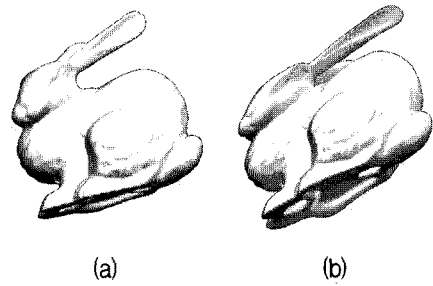


그림 8. 프랙탈 거침정도가 1이고 각 축에 대한 세기가 (a) 1.0과 (b) 2.0으로 잡음 물결된 Bunny 모델
 Fig. 8. Bunny model rippled with fractal roughness 1 and (a) 1.0 and (b) 2.0 noise intensity on each axis.

물결 패턴에 따라 모든 꼭지점들이 변조되어 있음을 볼 수 있다.

각 잡음 세기에 대한 정규화된 해밍 거리차 $d(h,h')$ 는 그림 5 (c)에서와 같이 잡음 세기가 0.5-1.5일 때 약 1.25×10^{-2} - 8.33×10^{-2} 으로 낮으나, 잡음 세기가 2.5부터 1.96×10^{-1} 이상이다. 즉, 잡음 세기가 2.0일 때까지 변형된 모델들은 인증으로 판별된다. 잡음 세기가 2.5이상일 경우, 프랙탈에 의한 큰 랜덤 물결 패턴에 따라 전체 꼭지점의 위치가 크게 변조됨으로 꼭지점별 표면 인덱스 및 표면 곡률 변형에 영향을 준다. 즉, 잡음 세기가 클 경우 꼭지점의 표면 계수 변경으로 다른 블록으로 할당됨에 따라 블록 표면 계수가 변경이 된다. 따라서 제안한 해상 기법은 잡음 세기가 2.0일 때까지 해쉬의 강인성을 확인하였다.

라. 푸쉬

푸쉬 변형은 모델 꼭지점의 평균 법선 방향을 기준으로 각 꼭지점들을 안쪽 또는 바깥쪽으로 푸쉬하는 것으로 돌출 또는 팽창(inflation)과 수축(deflation) 효과를 나타낸다. 푸쉬 변형 정도를 나타내는 푸쉬값은 꼭지점들이 모델 중점에 따라 이동하는 실세계 단위 상의 거리를 나타낸다. 양수의 푸쉬값일 경우에는 꼭지점들이 평균 법선 방향의 바깥쪽으로 팽창되고, 음수의 푸쉬값일 경우에는 꼭지점들이 안쪽으로 수축된다. 푸쉬 변형에서는 구부림 변형과 마찬가지로, 모델의 전체 형상이 팽창 또는 수축되도록 꼭지점의 위치가 변경되며, 꼭지점 배열 인덱스 및 메쉬 연결정보는 변경되지 않는다. 푸쉬 변형 실험에서는 0.01-0.05 범위의 푸쉬값으로 임의의 꼭지점들을 팽창하였다. 0.02 및 0.05의 푸쉬값으로 팽창된 Bunny 모델은 그림 9에서와 같다. 이 그림을

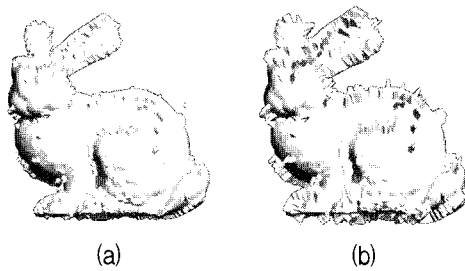


그림 9. 푸쉬값 (a) 0.02와 (b) 0.05으로 푸쉬된 Bunny 모델
 Fig. 9. Bunny model pushed to (a) 0.02 and (b) 0.05 push value.

살펴보면, 임의의 꼭지점들이 모델 중점을 기준으로 각각의 푸쉬값에 따라 바깥쪽으로 팽창 또는 돌출됨을 볼 수 있다.

각 푸쉬값에 대한 정규화된 해밍 거리차 $d(h, h')$ 는 그림 5 (d)에서와 같이 푸쉬값 0.02일 경우에는 8.13×10^{-2} 정도로 낮으며, 푸쉬값 0.05일 경우 1.22×10^{-1} 이다. 즉, 푸쉬값이 0.05일 때 까지 푸쉬된 모델들은 인증된다. 꼭지점의 표면 인덱스 및 표면 곡률들은 푸쉬값에 따라 증가되므로, 푸쉬된 꼭지점들은 블록 표면 계수 변경에 영향을 주며 추출된 해쉬의 비트 오류가 발생되어진다. 그러나 그림 9에서와 같이 원 모델의 형상을 인지할 수 있을 정도의 푸쉬값인 0.05이하일 경우 $d(h, h')$ 가 문턱치보다 작게 나타났다.

마. 신축

신축 변형은 x,y,z축 중 한 축에 대하여 임의의 비율로 스케일링하고 나머지 두 축에 따라 반대 비율로 스케일링한다. 신축되는 스케일링 비율은 모델의 중심에서 최대치이며, 바깥쪽으로 갈수록 비율은 감소된다. 또한 나머지 두 축에 대한 반대 스케일링 비율은 신축되는 축의 스케일링 효과 중심과의 거리에 따라 가변된다. 신축 변형은 신축세기에 의하여 조정되며, 이는 x,y,z 축의 기본 스케일링값 s를 결정한다. 예를 들어 신축세기가 1.5이면, 스케일링값은 $s=1.5+1=2.5$ 로 이는 250% 비율이다. 신축되는 축에 따라 250%로 스케일링되며, 나머지 두 축은 스케일링값의 역수 $1/2.5=0.4$ 즉, 40% 비율로 스케일링된다. 신축 변형 실험에서는 각 축에 대하여 0.1-0.5 범위의 신축세기로 3D 메쉬 모델들을 신축하였다. x,y,z 축에 대하여 0.5의 신축세기로 신축된 Bunny 모델은 그림 10에서와 같다.

x,y,z 축을 기준으로 각 신축세기에 따른 정규화된

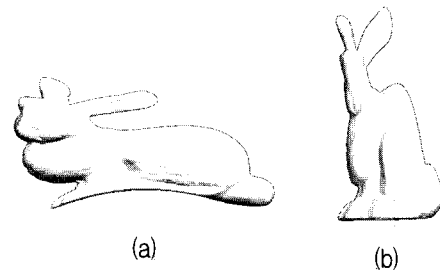


그림 10. (a) x축 및 (b) z축으로 신축세기 0.5로 신축된 Bunny 모델
 Fig. 10. Bunny model stretched to (a) x-axis and (b) z-axis with 0.5 stretching value.

해밍 거리차 $d(h, h')$ 는 그림 5 (e)에서와 같다. 이 결과를 살펴보면, 각 축에 대한 $d(h, h')$ 는 거의 유사하며, 신축세기가 0.1-0.4일 때 1.41×10^{-2} - 8.66×10^{-2} 정도이며, 신축세기가 0.5일 때 약 0.1이다. 따라서 신축되는 축에 상관없이 0.1-0.5 범위의 신축세기에 대하여 인증됨을 알 수 있다. 신축 변형은 구부림 변형에서와 같이 신축되는 축을 기준으로 신축세기에 따라 모든 꼭지점들이 균일하게 신축되므로 꼭지점별 표면 인덱스와 표면 곡률의 변경이 크지 않다. 따라서 제안한 해싱의 블록 표면 계수는 신축 변형에 강인함을 알 수 있다.

바. 부분할 (Tessellation)

부분할은 폴리곤 또는 삼각형 메쉬를 여러 개의 부메쉬들로 분할한다. 여기서 텐션(tension)에 따라 분할된 부 메쉬들은 평면, 볼록 또는 오목한 형태로 생성된다. 텐션값이 양수일 경우에는 꼭지점들을 바깥쪽 방향으로 푸쉬하면서 부 메쉬들을 볼록하게 라운딩한다. 텐션값이 음수일 경우에는 꼭지점들을 안쪽 방향으로 푸쉬하면서 부 메쉬들을 오목하게 라운딩한다. 그리고 텐션값이 0일 경우 부 메쉬들은 라운딩이 없는 평면이다. 본 실험에서는 텐션값을 0-60으로 변경하면서 메쉬들을 각 에지의 중점을 이으면서 4개의 부 메쉬들로 평면 및 볼록하게 분할하였다. 텐션값이 0인 평면 부분할 및 텐션값이 20인 볼록 부분할된 Bunny 모델은 그림 11에서와 같다. 이 그림을 살펴보면, 텐션값이 증가할수록 부분할된 모델의 라운딩이 부드러움을 볼 수 있다.

각 텐션값에 대한 정규화된 해밍 거리차 $d(h, h')$ 는 그림 5 (f)에서와 같다. 이 결과를 살펴보면, 텐션값이 40-60 정도 높은 볼록일 경우 $d(h, h')$ 는 0.148-0.103정도이며, 텐션값이 0-20 정도 낮은 볼록일 경우, $d(h, h')$ 가 0.202-0.192으로 높게 나타났다. 즉, 평면 부분할된

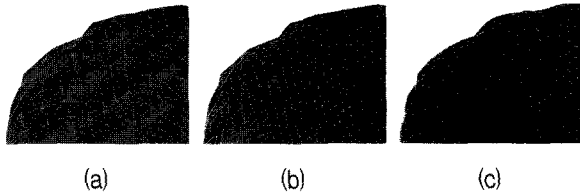


그림 11. (a) 원 Bunny 모델의 왼쪽 상단 부분 및 텐션 값이 (b) 0(평면), (c) 20(블록)으로 부분화된 (a) 모델의 와이어프레임

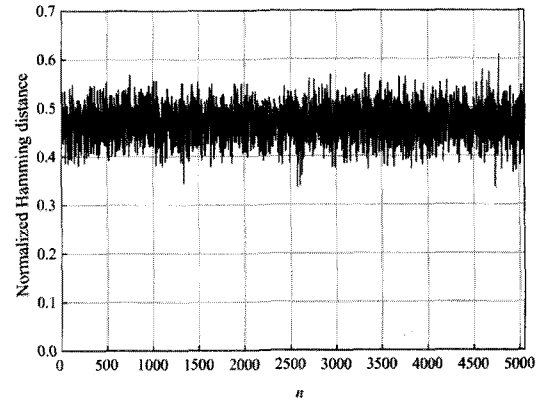
Fig. 11. Upper part wireframes of (a) Original Bunny model and Bunny model tessellated to (b) 0 and (c) 20 tension value.

모델보다 블록 부분화된 모델이 인증된다. 평면 부분화에 의하여 생성된 꼭지점들은 원 꼭지점들의 표면 계수와 차이가 크며, 인접한 꼭지점들의 표면 계수에도 영향을 준다. 그러나 블록 부분화에 의하여 생성된 꼭지점들은 평면 부분화에 비하여 원 꼭지점과의 표면 계수와의 차이가 크지 않으며 또한 인접한 꼭지점들의 표면 계수 영향이 크지 않다. 따라서 제안한 해싱 기법이 블록 부분화에 강인하나, 평면 또는 오목 부분화에 강인하지 못함을 확인하였다.

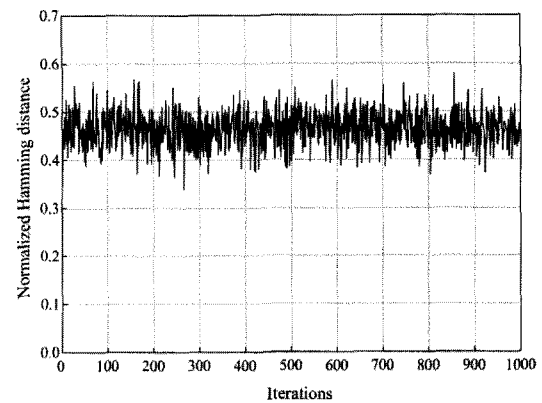
2. 유일성 평가

해쉬의 유일성 평가를 위하여 본 실험에서는 100개의 3D 메쉬 모델에 대하여 생성된 해쉬들 간의 정규화된 해밍 거리 $d(h_i, h_j)$, ($i, j \in [1, 100], i \neq j$)를 구하였다. 각 모델별 해쉬들 간의 $d(h_i, h_j)$ 는 그림 12 (a)에서와 같다. 이를 살펴보면, 평균 $d(h_i, h_j)$ 는 0.469 정도이고, [0.351 0.61] 범위를 가진다. 이 결과로부터 모든 테스트 모델별에 대하여 생성된 해쉬들 간의 유일성을 확인할 수 있다.

각 모델별 해쉬 H는 생성된 치환 키 k_p 및 랜덤변수 키 k_f 에 따라 다르게 생성된다. 여기서 동일 모델 상에서 서로 다른 키에 의하여 생성된 해쉬는 유일하여야 한다. 즉, 두 개의 키에 따라 생성된 해쉬 h_{k1}, h_{k2} ($k1(k_{1p}, k_{1f}) \neq k2(k_{2p}, k_{2f})$)들 간에는 정규화된 해밍 거리 $d(h_{k1}, h_{k2})$ 도 유일성 문턱치를 넘어야 한다. 본 실험에서는 Bunny 모델에 대하여 임의의 키 (k_p, k_f)에 의한 해쉬 h 와 서로 다른 1,000개의 키 (k_{kp}, k_{kf}) ($k \in [1, 1000]$)에 의한 해쉬 h_k 와의 정규화된 해밍 거리 $d(h, h_k)$ 를 계산하였다. 각 키에 대한 $d(h, h_k)$ 는 그림 12 (b)에서 같다. 이를 살펴보면, 평균 $d(h, h_k)$ 는 0.463 정도로, [0.363 0.578] 범위를 가진다. 즉, 동일 모델에



(a)



(b)

그림 12. (a) 모델별 해쉬 간의 $d(h_i, h_j)$ 및 (a) 키별 해쉬 간의 $d(h_{k1}, h_{k2})$

Fig. 12. (a) $d(h_i, h_j)$ between each of models and (b) $d(h_{k1}, h_{k2})$ between each of keys.

대하여 서로 다른 키에 의하여 생성된 해쉬가 유일함을 확인할 수 있었다.

V. 결론

본 논문에서는 블록 표면 계수를 이용한 키 기반 3D 메쉬 모델 해싱 기법을 제안하였다. 기존 2D 영상 해싱과 같이 3D 모델 해싱에서도 강인성, 유일성 및 보안성을 만족하여야 한다. 그러나 영상 화소로 구성된 2D 영상과는 달리 벡터 데이터로 구성된 3D 모델은 원 형상을 유지하면서 다양한 기하학 및 위상학적 편집이 용이하다. 이와 같은 편집 공격에 강인하면서, 원 모델의 위치, 방향 및 스케일링으로 변환하는 전처리 과정없이 해쉬를 추출하기 위하여 제안한 기법에서는 3D SSD와 표면 곡률 기반의 블록 표면 계수를 특징 벡터로 사용한다. 이 때 보안성 및 유일성을 향상시키기 위하여 치

환 키 및 랜덤변수 키 기반의 블록 표면 계수를 얻은 다음, 이를 이진화 과정에 의하여 이진 해쉬를 생성한다. 실험결과로부터 제안한 해싱 기법이 강인성과 유일성을 만족함을 확인하였다. 제안한 기법에서는 치환 키와 랜덤변수 키 기반의 특징 벡터를 생성하였으나, 이진화 과정시 또는 표면 계수 양자화에서 랜덤 키 기반으로 수행시 보안성이 더욱 향상될 수 있다. 향후 연구방향으로는 기존의 미분 엔트로피 등의 보안성 평가를 이용하여 제안한 기법의 보안성을 분석하고자 한다.

참 고 문 헌

- [1] E. J. Delp, "Multimedia security: the 22nd century approach," *Multimedia Systems*, vol. 11, no. 2, pp. 95-97, Oct. 2005.
- [2] A. Swaminathan, Y. Mao, and M. Wu, "Robust and secure image hashing," *IEEE Trans. on Information Forensics and Security*, vol. 1, issue 2, pp. 215-230, June 2006.
- [3] Y. Mao and M. Wu, "Unicity Distance of Robust Image Hashing," *IEEE Trans. on Information Forensics and Security*, vol. 2, issue 3, part 1, pp. 462-467, Sept. 2007.
- [4] V. Monga and M.K. Mhca, "Robust and Secure Image Hashing via Non-Negative Matrix Factorizations," *IEEE Trans. on Information Forensics and Security*, vol. 2, issue 3, part 1, pp. 376-390, Sept. 2007.
- [5] V. Monga and B.L. Evans, "Perceptual Image Hashing Via Feature Points: Performance Evaluation and Tradeoffs," *IEEE Trans. on Image Processing*, vol. 15, issue 11, pp. 3452-3465, Nov. 2006.
- [6] V. Monga, A. Banerjee, and B.L. Evans, "A clustering based approach to perceptual image hashing," *IEEE Trans. on Information Forensics and Security*, vol. 1, issue 1, pp. 68-79, March 2006.
- [7] B. Coskun, B. Sankur, and N. Memon, "Spatio - Temporal Transform Based Video Hashing," *IEEE Trans. on Multimedia*, vol. 8, issue 6, pp. 1190-1208, Dec. 2006.
- [8] C. De Roover, C. De Vleeschouwer, F. Lefebvre, B. Macq, "Robust video hashing based on radial projections of key frames," *IEEE Trans. on Signal Processing*, vol. 53, issue 10, part 2, pp. 4020-4037, Oct. 2005.
- [9] B. Bustos, D. A. Keim, D. Saupe and T. Schreck, "Content-Based 3D Object Retrieval," *IEEE Computer Graphics and Applications*, vol. 27, issue 4, pp. 22-27, July-Aug. 2007.
- [10] B. Bustos, D. A. Keim, D. Saupe, T. Schreck, and D. V. Vranic, "Feature-based similarity search in 3D object databases," *ACM Computing Surveys (CSUR)*, vol. 37, issue 4, pp. 345-387, Dec. 2005.
- [11] T. Zaharia and F. Preteux, "3D-shape-based retrieval within the MPEG-7 framework," *Proc. SPIE on Nonlinear Image Processing and Pattern Analysis XII*, San Jose, CA, vol. 4304, pp. 133-145, Jan. 2001.
- [12] M. Bober, "MPEG-7 Visual Shape Descriptors," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 11, no. 4, pp. 716-719, June 2001.
- [13] C. Grana, M. Davolio and R. Cucchiara, "Similarity-Based Retrieval with MPEG-7 3D Descriptors: Performance Evaluation on the Princeton Shape Benchmark," *Lecture Notes in Computer Science*, vol. 4877, pp. 308-317, 2007.
- [14] A. Jagannathan and E. L. Miller, "Three-Dimensional Surface Mesh Segmentation Using Curvedness-Based Region Growing Approach," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 29, no. 12, pp. 2195-2204, Dec. 2007.
- [15] N. Dyn, K. Hormann, S.J. Kim and D. Levin, "Optimizing 3D Triangulations Using Discrete Curvature Analysis," *Math. Methods for Curves and Surfaces*, pp. 135-146, 2000.
- [16] R. Ohbuchi, S. Takahashi, T. Miyazawa, and A. Mukaiyama, "Watermarking 3D polygonal meshes in the mesh spectral domain," *Proc. of Graphics Interface*, pp. 9-17, 2001.
- [17] S. Kanai, H. Date, and T. Kishinami, "Digital watermarking for 3D polygons using multiresolution wavelet decomposition," *Proc. of Sixth IFIP WG 5.2 GEO-6*, pp. 296-307, Dec. 1998.
- [18] E. Praun, H. Hoppe, and A. Finkelstein, "Robust mesh watermarking," *Proc. of ACM SIGGRAPH*, pp. 49-56, Aug. 1999.
- [19] O. Benedens, "Geometry-based watermarking of 3D models," *IEEE Computer Graphics and Applications*, vol. 19, issue 1, pp. 46-55, Jan./Feb. 1999.
- [20] S.H. Lee and K.R. Kwon, "A Watermarking for 3D-Mesh Using the Patch CEGIs," *Digital Signal Processing*, vol. 17, issue 2, pp. 396-413, March 2007.
- [21] S.H. Lee and K.R. Kwon, "Mesh watermarking

based projection onto two convex sets,"
Multimedia Systems, vol. 13, no. 5-6, pp.
323-330, Feb. 2008.

- [22] 이석환, 권성근, 권기룡, "블록 집합 투영 기법을
이용한 3D 메쉬 워터마킹," 대한전자공학회논문지,
제43권 CI편 제2호, pp. 81-92, 2006년 3월.
[23] 이석환, 권기룡, "k-means++ 기반의 설계도면 워
터마킹 기법," 대한전자공학회논문지, 제46권 CI편
제5호, pp. 57-70, 2009년 9월.

저 자 소 개



이 석 환(정회원)
1999년 경북대학교 전자공학과
학사 졸업.
2001년 경북대학교 전자공학과
석사 졸업.
2004년 경북대학교 전자공학과
박사 졸업.

2005년~현재 동명대학교 정보보호학과 교수
<주관심분야 : 워터마킹, DRM, 영상신호처리,
3D 그래픽스>



권 기 룡(정회원)-교신저자
1986년 경북대학교 전자공학과
학사 졸업.
1990년 경북대학교 전자공학과
석사 졸업.
1994년 경북대학교 전자공학과
박사 졸업.

2000년~2001년 Univ. of Minnesota, Post-Doc.
1996년~2006년 부산외국어대학교
컴퓨터전자공학부 부교수
2006년~현재 부경대학교 전자컴퓨터정보통신
공학부 교수
<주관심분야 : 멀티미디어 정보보호, 멀티미디어
통신 및 신호처리>