

논문 2010-47CI-6-9

객체별 특징 벡터 기반 3D 콘텐츠 모델 해싱

(3D Content Model Hashing Based on Object Feature Vector)

이 석 환*, 권 기 룡**

(Suk-Hwan Lee and Ki-Ryong Kwon)

요 약

본 논문에서는 3D 콘텐츠 인증을 위한 객체별 특징 벡터 기반 강인한 3D 모델 해싱을 제안한다. 제안한 3D 모델 해싱에서는 다양한 객체들로 구성된 3D 모델에서 높은 면적을 가지는 특징 객체내의 꼭지점 거리들을 그룹화한다. 그리고 각 그룹들을 치환한 다음, 그룹 계수, 랜덤 변수 키와 이진화 과정에 의하여 최종 해쉬를 생성한다. 이 때 해쉬의 강인성은 객체 그룹별 꼭지점 거리 분포를 그룹 계수에 의하여 향상되고, 해쉬의 유일성은 그룹 계수를 치환 키 및 랜덤변수 키 기반의 이진화 과정에 의하여 향상된다. 실험 결과로부터 제안한 해싱이 다양한 메쉬 공격 및 기하학 공격에 대한 해쉬의 강인성과 유일성을 확인하였다.

Abstract

This paper presents a robust 3D model hashing based on object feature vector for 3D content authentication. The proposed 3D model hashing selects the feature objects with highest area in a 3D model with various objects and groups the distances of the normalized vertices in the feature objects. Then we permute groups in each objects by using a permutation key and generate the final binary hash through the binary process with the group coefficients and a random key. Therefore, the hash robustness can be improved by the group coefficient from the distance distribution of vertices in each object group and the hash uniqueness can be improved by the binary process with a permutation key and a random key. From experimental results, we verified that the proposed hashing has both the robustness against various mesh and geometric editing and the uniqueness.

Keywords : 3D 모델 해싱(3D model hashing), 객체특징벡터 (Object feature vector), 강인성(Robustness), 유일성(Uniqueness)

I. 서 론

최근 3D 기반 TV, 영화, 게임, 캐릭터 등의 기존 3D 분야 뿐만 아니라 의료, 교육, 설계 도면, GIS, 전자도서관 등 다양한 분야에서 3D 콘텐츠 시장이 활발히 확대

되고 있다. 3D 콘텐츠 시장의 확대와 더불어 3D 콘텐츠물의 저작권 보호, 복사 방지 및 3D 콘텐츠 인증과 같은 보호 기술이 필요하게 되었다. 이들 중 저작권 보호를 위한 3D 워터마킹 기술들이 많이 연구되어지고 있으나, 3D 콘텐츠물의 인증 및 복사 방지 등에서 필요한 3D 콘텐츠 해싱 기술은 3D 워터마킹 기술에 비하여 많이 연구되지 않고 있다.

MD5, SHA 계열 (SHA-1/-2) 등과 같은 암호화 해쉬 함수(Cryptographic hash function)는 데이터의 무결성 검증을 위한 대표적인 기술이다. 암호화 해쉬 함수에 의하여 생성된 해쉬는 입력의 모든 비트에 대하여 영향을 받으므로 멀티미디어 또는 콘텐츠 해쉬 함수(Content hash function)에는 적합하지 못하다. 즉, 콘텐

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

** 정회원, 부경대학교 IT융합응용공학과
(Department of IT Convergence and Application Engineering, Pukyong National University)

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

접수일자: 2010년6월4일, 수정완료일: 2010년10월25일

츠 해싱 (Content hashing)에서는 정확한 이진 정보 표현 방법보다 콘텐츠 변형에 대한 민감 여부가 더욱 중요하다^[1~10]. 예를 들어 영상 및 비디오와 같은 콘텐츠들은 신호 처리에 의하여 쉽게 변형될 수 있다. 그러나 원 영상 콘텐츠와 변형된 영상 콘텐츠들 간의 해쉬는 동일하여야 한다. 강인한(Robust) 또는 인지적(Perceptual) 해쉬 함수는 원 콘텐츠가 심각하게 변형되지 않는 한 동일한 해쉬를 생성하는 것으로 다양한 멀티미디어 응용 분야에서 콘텐츠 인증에 필요한 기술로 제기되었다. 많은 연구진들에 의하여 영상^[1~7] 또는 비디오^[8~10] 해싱에 대한 연구가 진행되어져 왔으나 3D 콘텐츠 해싱에 대한 연구는 영상 및 비디오 해싱에 비하여 활발히 진행되지 못하였다.

3D 모델 해싱에 대한 요구조건 및 프레임워크는 [11~12]에 처음으로 제기되었으며, 이 논문에서는 블록 표면 계수(Block shape coefficient)를 이용한 3D 메쉬 모델 해싱이 제안되었다. 이 기법에서는 3D 메쉬 모델 상에서 3D SSD(Shape spectrum descriptor) 및 표면 곡률(Curvedness) 기반의 평면계 블록 표면 계수로 구성된 특징벡터들을 획득한 후, 치환 키 및 랜덤 변수 키에 의하여 이진 해쉬를 생성한다. 블록 표면 계수의 특징 벡터들은 기하학 및 위상학 공격에 강인하나, 스케일링 및 삼각형 부분할 등에 연약성을 가지고 있다. 또한 이 기법은 단일 객체 모델로 구성된 3D 메쉬 모델에 대한 해싱으로 계층적인 객체 모델들로 구성된 3D 모델에 대하여 적용되지 못한다. A. Hamza 등은^[13~14] 서브 메쉬의 Laplace-Beltrami 행렬의 고유 분해와 스펙트럴 계수 및 Tsallis 엔트로피 예측을 통하여 해쉬값을 생성하였다. 그러나 이 기법은 3D 모델의 특징 해쉬 벡터를 추출하는 것으로 해쉬 보안성에 대하여 고려하지 않는다.

본 논문에서는 계층적인 객체 구조로 구성된 3D 모델에 대한 강인한 해싱 기법을 제안한다. 3D 모델들은 다양한 편집들에 의하여 쉽게 기하학 및 위상학 공격에 의하여 편집될 수 있다. 이 때, 공격에서는 일부 객체 또는 전체 모델에 대하여 공격이 수행될 수 있다. 따라서 본 논문에서는 이와 같은 객체별 또는 모델별 공격에 강인하며, 키 기반 특징 벡터에 의하여 유일한 해쉬를 생성하는 3D 모델 해싱을 제안하고자 한다. 이를 위하여 제안한 3D 모델 해싱에서는 먼저 3D 모델에서 면적 비율이 높은 특징 객체들을 선택한 다음, 이들 객체들의 면적이 기준 면적이 되도록 객체들의 꼭지점들을

정규화한다. 그리고 정규화된 객체별 꼭지점들의 거리들을 그룹화한 다음, 치환 키에 의하여 그룹들을 치환한다. 마지막으로 동일 인덱스를 가지는 객체별 치환 그룹 내의 평균 꼭지점 거리를 랜덤 변수 키와 이진화에 의하여 최종 해쉬를 생성한다. 3D 모델 인증 과정에서는 치환 키 및 랜덤 변수 키에 의하여 전송된 3D 모델에서 해쉬를 생성한 다음, 원 해쉬와의 해밍 거리차(Hamming distance)에 의하여 3D 모델을 인증한다. 실험 결과로부터 제안한 3D 모델 해싱이 다해상도 변환, 삼각 부분할, 꼭지점 집합 및 객체 삭제 등과 같은 메쉬 편집과 RST 변환, 구부림, 점감, 비틀림 및 잠음과 같은 기하학 편집에 강인하며, 키 기반의 해쉬가 유일함을 확인하였다.

본 논문의 구성은 다음과 같다. 먼저 II장에서는 제안한 객체 기반 3D 해싱에 대하여 자세히 살펴보면, III장에서는 강인성 및 유일성 실험에 대한 평가 결과에 대하여 살펴본다. 마지막으로 IV장에서는 본 논문의 결론을 맺는다.

II. 제안한 객체 기반 3D 해싱 기법

3D 콘텐츠 모델들은 객체별로 구성되어 있으며, 각 객체들은 꼭지점 좌표와 연결 데이터로 구성된 기하학 정보와 움직임 데이터인 타임 정보로 구성되어 있다. 본 논문에서는 3D 애니메이션 또는 정지 모델에 적용 가능한 객체 기반 3D 해싱 기법을 제안한다. 제안한 객체 기반 3D 해싱 기법은 그림 1에서와 같이 3D 모델의 특징 객체 정규화, 특징 객체별 특징 벡터 추출 및 해쉬

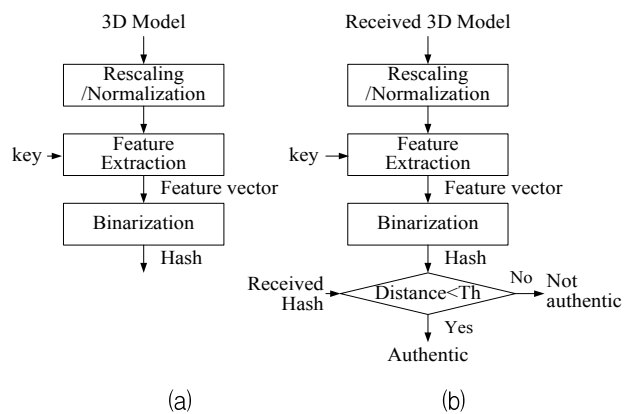


그림 1. 3D 모델의 (a) 해쉬 생성 및 (b) 해쉬 기반 인증 과정
Fig. 1. The process of (a) Hash generation and (b) hash authentication for 3D model.

생성 단계로 구성된다. 이 때 특징 벡터들은 치환 키 \mathbf{K}_P 및 랜덤 계수 키 \mathbf{K}_R 에 의하여 생성된다.

1. 특징 객체 정규화

3D 모델 $\mathbf{M} = \{\mathbf{O}_i | i \in [1, N_O]\}$ 은 N_O 개의 객체들로 구성되며, 각 객체 $\mathbf{O}_i = \{\mathbf{V}_i, \mathbf{M}_i, \mathbf{P}_i\}$ 는 꼭지점 데이터 $\mathbf{V}_i = \{\mathbf{v}_{ik} | k \in [1, N_{V_i}]\}$, 메쉬 데이터 $\mathbf{M}_i = \{\mathbf{m}_{ik} | k \in [1, N_{M_i}]\}$ 및 키타임별 위치, 방향 등의 보간기 데이터 \mathbf{P}_i 로 구성된다. 각 객체들은 그림 2 (a)에서와 같이 모델의 주요 또는 비주요 부분으로 나뉘어질 수 있다. 이 때 주요 객체들은 모델의 형상 또는 특징을 나타내므로, 주요 객체가 삭제시 원 모델의 형상을 유지할 수 없다.

제안한 방법에서는 면적 비율이 높은 객체들을 선택하여 이들을 3D 모델 내의 주요 객체인 특징 객체로 사용한다. 먼저 각 객체의 표면 면적 A_i 을 메쉬들의 면적 합에 의하여

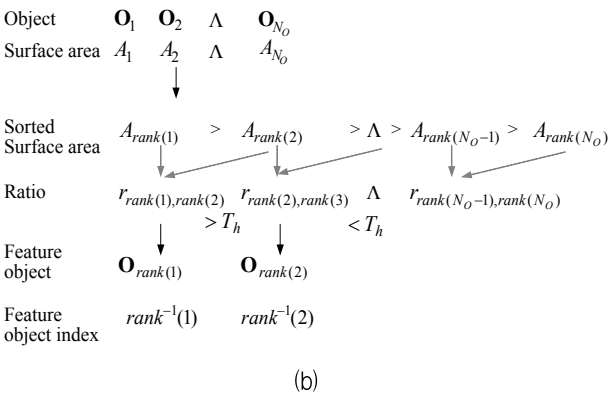
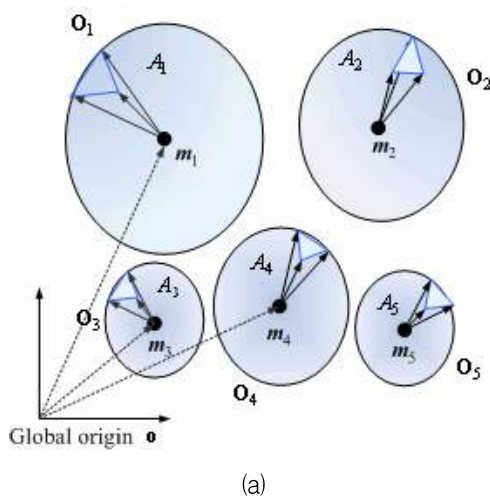


그림 2. (a) 객체별 표면 면적과 (b) 특징 객체 추출 과정
 Fig. 2. (a) Surface area in each object and (b) the process for extracting feature object.

$$A_i = \sum_{k=1}^{N_{M_i}} A_{ik}, \quad (1)$$

$$\text{where } A_{ik} = \frac{1}{2} \|\overrightarrow{\mathbf{v}_{ik,1}\mathbf{v}_{ik,2}}\| \|\overrightarrow{\mathbf{v}_{ik,1}\mathbf{v}_{ik,3}}\| \sin\theta_{ik}$$

$$= \frac{1}{2} \|\overrightarrow{\mathbf{v}_{ik,1}\mathbf{v}_{ik,2}}\| \|\overrightarrow{\mathbf{v}_{ik,1}\mathbf{v}_{ik,3}}\| \sqrt{1 - (\hat{\mathbf{u}}_{ik,1} \cdot \hat{\mathbf{u}}_{ik,2})^2}$$

와 같이 구한다. 여기서 A_{ik} 는 i 번째 객체 내의 k 번째 메쉬 \mathbf{m}_{ik} 의 면적이며, 메쉬 \mathbf{m}_{ik} 은 $\mathbf{v}_{ik,1}$, $\mathbf{v}_{ik,2}$, $\mathbf{v}_{ik,3}$ 의 삼각형 메쉬를 나타낸다. 그리고 $\hat{\mathbf{u}}_{ik,1}$ 및 $\hat{\mathbf{u}}_{ik,2}$ 는 각각 $\overrightarrow{\mathbf{v}_{ik,1}\mathbf{v}_{ik,2}}$ 와 $\overrightarrow{\mathbf{v}_{ik,1}\mathbf{v}_{ik,3}}$ 의 단위벡터들이다. 따라서 3D 모델 \mathbf{M} 의 전체 표면 면적 $A(\mathbf{M})$ 은 각 객체 면적들의 합이며, $A(\mathbf{M})$ 는 특징 객체와 비특징 객체들의 면적으로 구분되어진다.

$$A(\mathbf{M}) = \sum_{i=1}^{N_O} A_i = \sum A_{i,feature} + \sum A_{i,non-feature} \quad (2)$$

객체 면적을 이용하여 특징 및 비특징 객체를 구분하기 위하여 제안한 방법에서는 각 객체의 면적들을 내림차순으로 순위 정렬한다.

$$\{A_1, A_2, \dots, A_{N_O}\} \rightarrow \{A_{rank(1)}, A_{rank(2)}, \dots, A_{rank(N_O)}\}$$

여기서 $rank(i)$ 는 i 번째 객체의 순위를 나타내는 것으로, $j = rank(i)$ 로 두면 순위 j 의 객체 인덱스는 $i = rank^{-1}(j)$ 가 된다. 그런 다음, 현재 순위 면적 A_j 과 다음 순위 면적 A_{j+1} 간의 면적 비율 $r_{j,j+1} = A_{j+1}/A_j$ 을 차례로 문턱치 T_h 와 비교하여, T_h 보다 작은 면적 비율이 나오면 현재 순위까지의 모든 객체 인덱스를 특징 객체의 인덱스로 저장한다. 즉, 특징 객체 \mathbf{FO} 는

$$\mathbf{FO} = \{\mathbf{O}_i | i \in [1, N_{FO}], rank(i) > rank(i+1)\} \quad (3)$$

$$\text{where } r_{rank(i),rank(i+1)} > T_h, \forall i \in [1, N_{FO}-1],$$

$$\text{and } r_{rank(N_{FO}),rank(N_{FO}+1)} < T_h$$

와 같으며, 특징 객체 인덱스 $I(\mathbf{FO})$ 는 해쉬 추출을 위하여 저장된다. 이와 같이 특징 객체 추출 과정은 그림 2 (b)에서와 같다.

임의의 비율로 스케일링된 모델에서는 표면 면적이 스케일링 비율에 따라 가변된다. 따라서 제안한 방법에서는 특징 객체 $\mathbf{FO} = \{\mathbf{O}_i | i \in [1, N_{FO}]\}$ 들의 표면 면적 A_i 이 기준 면적 A^* 의 값이 되도록 특징 객체들을 정규화한다. 즉, 객체별로 기준 면적이 되도록 정규화한다.

특징 객체 \mathbf{O}_i 의 표면 면적 A_i 이 기준 면적 A^* 이 되

기 위하여 O_i 내의 모든 메쉬 $\mathbf{m}_{ik} (\forall k \in [1, N_M])$ 들의 면적 A_{ik} 들을 변경하여야 하며, 이는 꼭지점 좌표 변경에 의하여 수행되어진다. 예를 들어, 메쉬 \mathbf{m}_{ik} 의 면적이 A_{ik} 라 할 때, \mathbf{m}_{ik} 를 구성하는 꼭지점 좌표 $\mathbf{v}_{ik,1}, \mathbf{v}_{ik,2}, \mathbf{v}_{ik,3}$ 를 임의의 인자 α 에 $\mathbf{v}'_{ik,j} = \alpha \mathbf{v}_{ik,j}, j \in [1,3]$ 와 같이 변경될 수 있다. 이 때 변경된 좌표 $\mathbf{v}'_{ik,j}$ 에 의한 메쉬 \mathbf{m}_{ik} 의 면적 A'_{ik} 은 수식 (1)에 의하여

$$A'_{ik} = \alpha^2 A_{ik} \quad (4)$$

와 같이 된다. 이를 기반으로 정규화된 특징 객체의 면적 A'_i 를

$$A'_i = \gamma A_i = \sum_{k=1}^{N_M} \gamma A_{ik}, \quad \gamma = A^*/A_i \quad (5)$$

이라 할 때, A'_i 는 정규화된 꼭지점 좌표 \mathbf{v}'_{ik}

$$\mathbf{v}'_{ik} = \sqrt{\gamma} \mathbf{v}_{ik}, \quad (\forall k \in [1, N_V]) \quad (6)$$

에 의하여 구하여진다. 위 식에 의하여 특징 객체 내의 모든 꼭지점 좌표들은 정규화된다.

2. 특징 벡터

제안한 방법에서는 특징 객체 O_i 내의 중점 \mathbf{m}_i 과 모든 정규화된 꼭지점 \mathbf{v}'_{ik} 과 거리 d_{ik} 를

$$D_i = \{d_{ik} = \|\overrightarrow{\mathbf{m}_i \mathbf{v}'_{ik}}\| | k \in [1, N_V]\} \quad (7)$$

와 같이 구한 다음, 그룹 간격 $\Delta s = d_{\max}/N_H$ 으로 해쉬 비트수 N_H 만큼 거리 d_{ik} 를 그룹화한다.

이 때 모든 객체의 거리를 동일한 간격으로 그룹화하기 위하여, 그룹 간격 Δs 는 최대 거리 $d_{\max} = \max\{d_{ik} | i \in [1, N_{FO}], k \in [1, N_V]\}$ 에 의하여 결정된다. 따라서 특징 객체 O_i 내에 거리를 이용한 꼭지점 거리 그룹 G_i 은

$$G_i = \{G_{ij} | j \in [1, N_H]\}, \quad (8)$$

$$G_{ij} = \{d_{i,j,k} | (j-1)\Delta s \leq d_{i,j,k} < j\Delta s, k \in [1, N_{G_j}]\}$$

와 같다. 여기서 N_{G_j} 는 그룹 G_{ij} 에 할당된 거리의 개수이다.

제안한 방법에서는 그림 3에서와 같이 해쉬 보안성을 향상시키기 위하여, 특징 객체들의 그룹 치환 키 \mathbf{K}_P 를

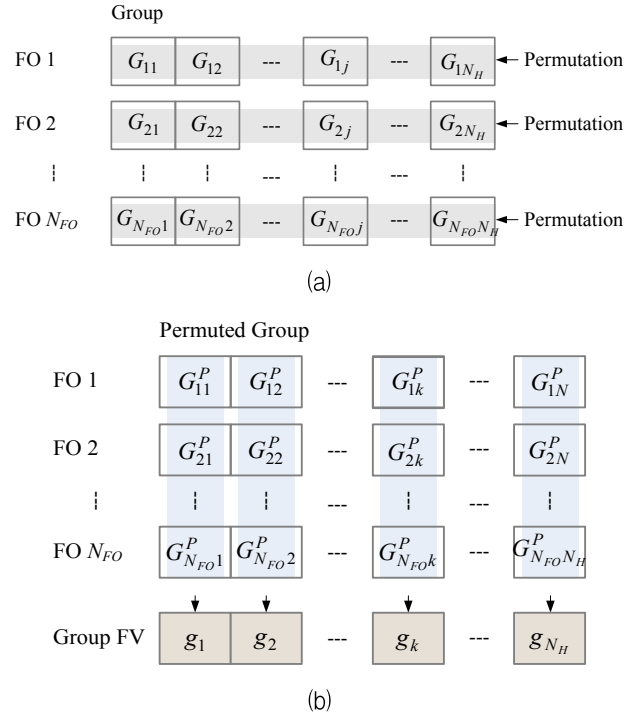


그림 3. (a) 특징 객체별 그룹 및
(b) 치환 그룹 상의 특징 벡터 생성
Fig. 3. (a) Groups in each feature object and
(b) feature vectors in the permuted groups.

$$\mathbf{K}_P = \{p_i | i \in [1, N_{FO}]\}, \quad (9)$$

$$p_i = \{p_i(j) | p_i(j) \neq p_i(j'), j \neq j', j, j' \in [1, N_H]\}$$

와 같이 생성한 다음, 특징 객체의 각 그룹들을 치환하여 치환된 그룹 G^P_i ($i \in [1, N_{FO}]$) 들을 각각 구한다.

$$G^P_i = \{G^P_{ip_i(j)} | j, p_i(j) \in [1, N_H]\} \quad (10)$$

$$G^P_{ip_i(j)} = \{\hat{d}_{ip_i(j),n} = d_{ip_i(j),n} - (j-1)\Delta s |$$

$$0 \leq \hat{d}_{ip_i(j),n} < \Delta s, n \in [1, N_{G_{ip_i(j)}}]\}$$

이 때 각 그룹의 계수를 구하기 위하여 제안한 방법에서는 치환된 그룹 내의 거리 값들을 동일한 크기 범위 $[0, \Delta s]$ 내에 있도록 변환한 후, 이들 평균 거리를 치환 그룹 계수 g_i 로 사용한다.

$$g_i = \{g_{ip_i(j)} | p_i(j) \in [1, N_H]\}, \quad g_{ip_i(j)} = \sum_{n=1}^{N_{G_{ip_i(j)}}} \hat{d}_{ip_i(j),n} / N_{G_{ip_i(j)}} \quad (11)$$

그림 4는 특징 객체별 그룹과 치환된 그룹 내의 특징 벡터 생성에 대하여 각각 보여주고 있다.

3. 해쉬 생성

특징 객체별 치환 블록 계수 \mathbf{g}_k 들은 모두 $[0, \Delta s]$ 범위 내에 있다. 제안한 방법에서는 해쉬 비트수 만큼 $[0, 1]$ 사이의 균일 분포를 가지는 랜덤 계수 키 \mathbf{K}_R 를

$$\mathbf{K}_R = \{r_k | k \in [1, N_H]\}, r_k \in [0, 1] \quad (12)$$

와 같이 생성한 다음, 동일한 위치 상에 있는 특징 객체별 치환 블록 계수들의 평균과 랜덤 계수를 이용하여 특징 벡터 \mathbf{FV} 를

$$\mathbf{FV} = \{f_k | k \in [1, N_H]\}, f_k = (r_k + \sum_{i=1}^{N_{FO}} g_{i_p(j)} / N_{FO}) / 2 \quad (13)$$

와 같이 구한다. 여기서 특징 벡터 계수 f_k 는 치환 블록 계수와 같이 모두 $[0, \Delta s]$ 의 범위 내에 있으므로, 제안한 방법에서는 특징 벡터 계수 f_k 를 중간 범위값 $\Delta s / 2$ 과 비교함으로써 해쉬 비트 \mathbf{H} 를

$$\mathbf{H} = \{h_i | i \in [1, N_H]\} \quad (14)$$

$$h_i = \begin{cases} 0, & \text{if } f_k \leq \Delta s / 2 \\ 1, & \text{if } f_k > \Delta s / 2 \end{cases}$$

와 같이 생성한다.

그림 4는 Armchair 모델 상에서 특징 객체 거리 분포 및 치환된 그룹별 거리 분포, 특징 벡터 및 최종 생성된 이진 해쉬를 보여준다. Armchair 모델은 2개의 객체로 구성되며, 이들 면적 비율이 유사하여 2개 모두 특징 객체 (FO1, FO2)로 선택되어진다. 여기서 FO1은 5-31번째 그룹 사이 골고루 분포되어 있으나, FO2는 13-19번째 그룹에 거리들이 집중되어 있음을 그림 4 (a)에서 볼 수 있다. 그리고 FO1과 FO2의 치환된 그룹별 거리 분포는 그림 4 (b)에서와 같이 많은 그룹으로 치환됨을 볼 수 있다. Armchair 모델에서 최대 거리 d_{max} 는 32.20으로, 해쉬 길이가 50bit 일 경우 그룹 간격 Δs 는 0.644이다. 각 치환된 그룹 계수 \mathbf{g}_k 및 랜덤계수 키에 의한 특징 벡터 \mathbf{FV} 는 그림 4 (c)에서와 같이 $[0, 1]$ 사이에 골고루 분포되어 있다. 특징 벡터 \mathbf{FV} 에 의하여 최종 생성된 이진 해쉬 \mathbf{H} 는 그림 4 (d)에서와 같다.

4. 해쉬 기반 인증

해쉬 기반 3D 모델 인증 과정에서는 그림 1 (b)에서와 같이 전송된 3D 모델 \mathbf{D}' 상에서 치환 키 \mathbf{K}_p 및 랜덤계수 키 \mathbf{K}_R 를 이용하여 해쉬 \mathbf{H} 를 생성한다. 그리고

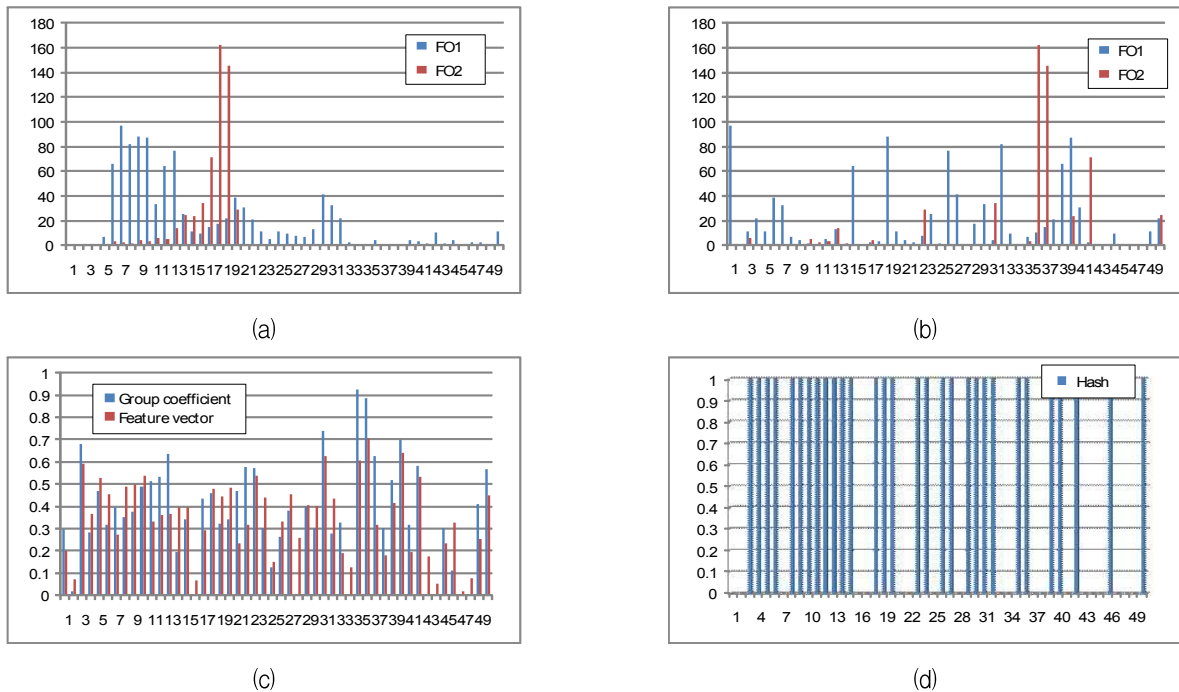


그림 4. Armchair 모델에서 (a) 특징 객체들의 그룹별 거리 분포 및 (b) 치환된 그룹별 거리 분포, (c) 그룹계수 및 랜덤계수에 의한 특징벡터와 (d) 최종 생성된 이진 해쉬

Fig. 4. (a) The distance distribution of each groups in feature objects, (b) the distance distribution of permuted groups, (c) feature vectors of group coefficients and (d) final binary hash in an Armchair model.

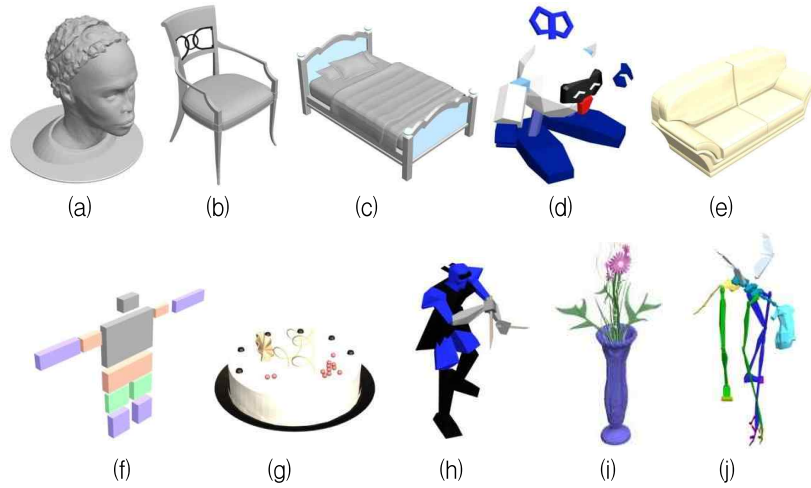


그림 5. 실험에 사용된 대표적 3D 모델인 (a) Africanas bust, (b) Armchair, (c) Bed, (d) Bomb, (e) Sofa, (f) Boxbody, (g) Cake, (h) Ninja, (i) Vase flower 및 (j) Walier 모델들

Fig. 5. (a) Africanas bust, (b) Armchair, (c) Bed, (d) Bomb, (e) Sofa, (f) Boxbody, (g) Cake, (h) Ninja, (i) Vase flower and (j) Walier models that are typical 3D models used in our experimentation.

원 해쉬 \mathbf{H} 와 추출된 해쉬 \mathbf{H}' 와의 정규화 해밍 거리 (Normalized Hamming distance) $e(\mathbf{H}, \mathbf{H}')$

$$e(\mathbf{H}, \mathbf{H}') = \sum_{i=1}^{N_H} |h_i - h'_i| / N_H \quad (15)$$

를 문턱치와 비교함으로써

IF $e(\mathbf{H}, \mathbf{H}') < Th$, Then $\mathbf{D}' = A$

Else $\mathbf{D}' = NA$

와 같이 3D 모델 \mathbf{D}' 를 인증한다. 여기서 A (Authenticate) 와 NA (Not authenticate)는 각각 인증 및 비인증을 나타낸다. 정규화된 해밍 거리가 0에 가까울수록 두 해쉬 간의 유사성이 높으나, 0.5에 가까울수록 두 해쉬간의 유사성이 거의 없음을 나타낸다. 본 논문에서는 인증을 위한 문턱치 Th 를 0.15로 결정하였으며, 해쉬의 유일성 평가를 위한 문턱치를 0.35로 결정하였다.

III. 실험 결과

본 실험에서는 다양한 3D 기하학 공격에 대한 강인성 및 랜덤 키 기반 해쉬의 유일성에 대하여 제안한 해싱의 성능을 평가하였다.

1. 실험 환경

본 실험에 사용된 3D 모델들은 archibase.net^[15]에서

표 1. 대표적인 3D 모델의 객체 수, 특징객체 수 및 면적, 면적비율

Table 1. The number of total objects and feature objects and surface area and area ratio in typical 3D models.

모델명	객체수	특징 객체수	면적비율 [%]	그룹간격 Δ_s
Africanas bust	5	4	94.70	0.165
Armchair	2	2	100.00	0.644
Bed	21	3	86.11	1.005
Bomb	17	3	53.05	6.832
Sofa	4	1	76.42	0.704
Boxbody	11	2	48.61	0.903
Cake	25	1	65.15	0.248
Ninja	19	19	100.00	4.508
Vase flower	154	1	31.20	0.255
Walier	59	4	71.80	0.175

제공하는 모델 중 60개 모델을 선택한 것이며, 각 모델들은 다양한 객체 수를 가지며, 또한 객체별로 꼭지점 및 메쉬의 개수가 다양하다. 본 실험의 대표적인 테스트 모델의 객체 수, 특징 객체 수 및 면적 비율은 표 1에서와 같으며, 각 모델은 그림 5에서와 같다. 이 표를 살펴보면, Africanas bust, Armchair 및 Ninja 모델들은 객체들 간의 면적 차이가 거의 없으므로, 대부분 객체들이 특징객체로 선택되며, 선택된 특징객체의 면적비율이 거의 90% 이상을 차지한다. 이와는 반대로 Bed, Bomb, Boxbody, Cake 및 Vase flower 모델들은 객체수에 비하여 일부 객체가 대부분의 면적을 차지함으로

선택된 특징 객체수가 상당히 작다. 그러나 Boxbody 및 Vase flower 모델을 제외하고 대부분 특징 객체들의 면적 비율이 전체 모델 면적에 비하여 약 50% 이상을 차지함을 볼 수 있다.

본 실험에서는 모든 모델에서 $N_H=50$ 비트의 해쉬를 생성하였으며, 각 모델의 꼭지점 거리들은 그룹 간격 $\Delta s = d_{max}/50$ 에 의하여 50개 그룹으로 나뉘어진다. 이때 각 모델에 대한 그룹 간격 Δs 는 표 1에서와 같다. 각 모델들의 특징 객체들이 면적에 따라 정규화 되었지만, 꼭지점 분포가 모두 다르므로 표 1에서와 같이 그룹 간격이 모두 다르게 나타난다. 특히 Bomb과 Ninja 모델들은 객체별 꼭지점 개수가 매우 작으며, 분포가 매우 넓게 나타나며, 다른 모델에 비하여 그룹 간격이 매우 높게 나타남을 표에서 볼 수 있다. 그러나 대부분 모델의 그룹 간격은 1이하이며, 이는 해쉬 비트수에 따라 결정된다.

2. 유일성 평가

본 실험에서는 동일한 모델에 대한 서로 다른 두 개의 키에 대한 해쉬의 유일성과 서로 다른 두 모델에 대한 해쉬의 유일성을 각각 평가하였다.

키에 대한 해쉬의 유일성 실험에서는 각 모델에 대하여 임의의 키에 의하여 생성된 해쉬 H_0 와 1,000개 키에 의하여 생성된 해쉬 $H_i (i \in [1, 1000])$ 들 간의 정규화 해밍 거리 $e(H_0, H_i)$ 를 측정하였다. 그림 6 (a)는 Armchair 모델에서 1,000개 키에 대한 정규화 해밍 거리를 보여주고 있다. 이 그림으로부터 이 모델의 정규화 해밍거리가 [0.28 0.70] 사이에 있음을 볼 수 있다. 그림 6 (b)에서와

같이 키에 대한 정규화 해밍 거리의 확률 분포 $\Pr(e(H_0, H_i))$ 를 살펴보면, 평균 m 이 0.484, 분산 σ 이 0.004692인 가우시안 분포를 가지고, 유일성 문턱치 $Th = 0.35$ 보다 클 확률이 $\Pr(e(H_0, H_i) > 0.35) = 0.98$ 이고, $\Pr(0.15 < e(H_0, H_i) < 0.35) = 0.02$ 이다. 다른 모델에 대한 실험에서도 위와 같은 유사한 결과가 나타남을 확인하였다. 이 결과로부터 임의의 키에 대하여 생성된 해쉬는 98% 정도의 유일성을 가짐을 확인하였다.

3. 강인성 평가

제안한 해싱의 강인성을 평가를 위하여 기존의 3D-SSD 기법^[11~12]과 Entropic 기법^[13~14]을 동일한 실험 조건에 대하여 공격을 수행한 후, 정규화 해밍 거리의 평균치 $\bar{e}(H, H')$ 가 인증 문턱치 1.5 보다 작을 때까지 공격 세기를 비교 평가하였다. 실험 결과인 그림 7은 모든 실험 모델에 대한 각 공격의 정규화된 해밍 거리 $e(H, H')$ 의 평균 $\bar{e}(H, H')$ 을 나타내고 있다.

가. 메쉬 공격

다해상도 변환은 웹 기반 3D 응용 분야에서 계층적 렌더링에 많이 사용되는 것으로, 렌더링에 필요한 메모리 오버헤드를 줄이기 위하여 각 모델의 꼭지점 및 메쉬 개수를 줄이는 것이다. 본 실험에서는 각 모델의 특징 객체들의 꼭지점 개수를 원 객체에 비하여 약 80~10%로 줄였다. 그림 8 (a) 및 (b)는 Armchair 모델의 특징 객체 와이어프레임과 60%로 변환된 모델의 와이어프레임을 보여주고 있다. 전체 모델에 대한 정규화된 해밍 거리 평균 $\bar{e}(H, H')$ 은 그림 7 (a)에서와 같

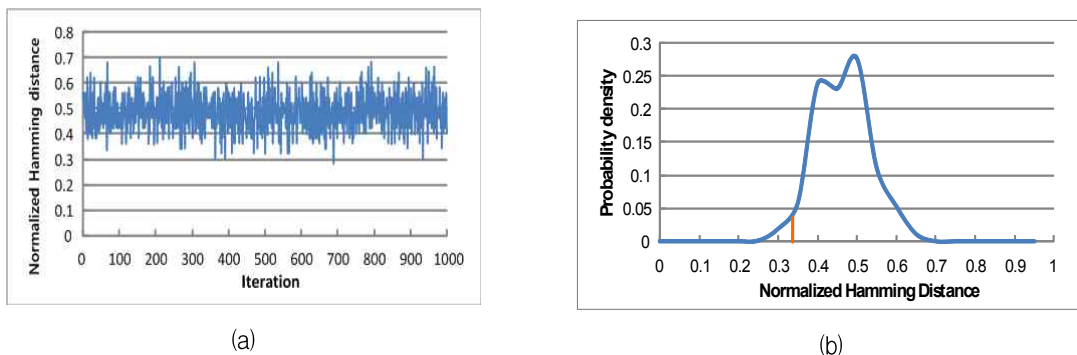


그림 6. Armchair 모델에 대한 키 기반 해쉬 유일성 실험 결과;
 (a) 1,000개 키에 대한 정규화 해밍 거리 및 (b) 확률 분포 ($m=0.484, \sigma=0.004692$)
 Fig. 6. Experimental results of key based hash uniqueness in an Armchair model;
 (a) the normalized Hamming distance in 1,000 keys and (b) probability density.

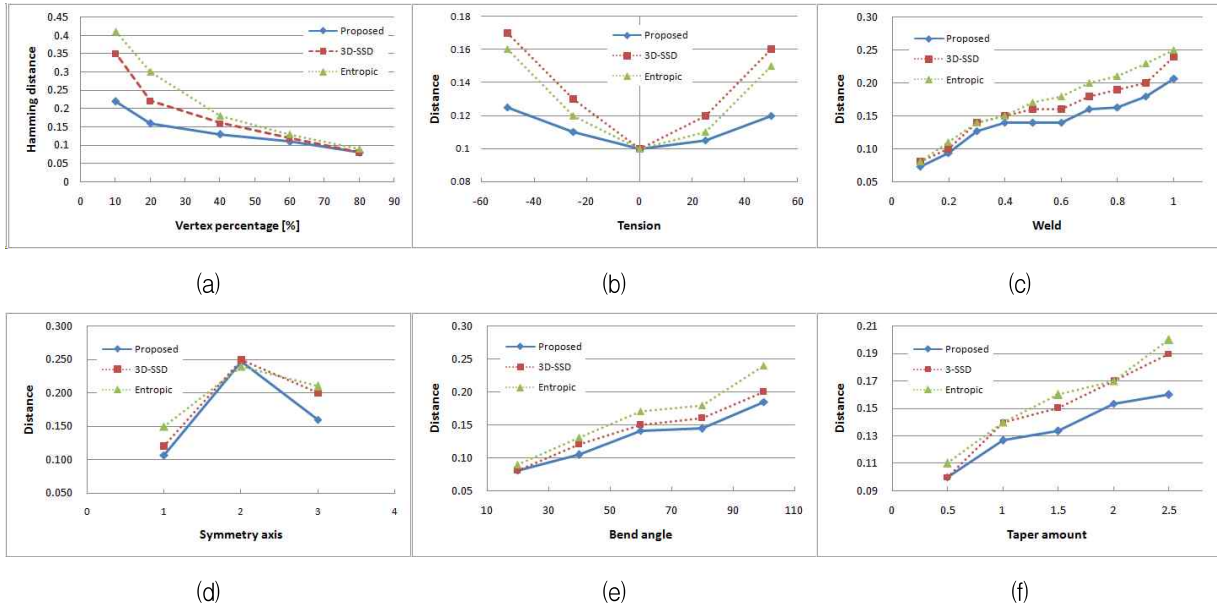


그림 7. 각 공격에 대한 정규화된 해밍 거리의 평균치; (a) 다해상도 변화, (b) 삼각 부분할, (c) 꼭지점 접합, (d) 대칭, (e) 구부림, (f) 점감

Fig. 7. The average of normalized Hamming distances in each attack; (a) multi-resolution transformation, (b) tessellation, (c) vertex weld, (d) symmetry, (e) bending and (f) tapering.

이 80-40% 변환에서는 0.08-0.13이고 20-10% 변환에서는 0.16-0.22이다. 즉, 제안한 해싱은 다해상도 변환에서 약 28% 변환까지 강인함을 알 수 있었다. 기존 3D-SSD 기법과 Entropic 기법은 약 40%와 약 50% 변환까지 강인하게 나타났다. 따라서 다해상도 변환 공격에 대하여 제안한 해싱이 기존 방법에 비하여 보다 강인함을 확인하였다.

삼각 부분할은 삼각형 메쉬를 4개의 부 메쉬로 분할하는 것으로 모델의 곡면을 부드럽게 또는 세밀하게 변형한다. 본 실험에서는 텐션(Tension) 크기를 조정하면서 모든 객체들의 메쉬들을 1회 부분할하였다. 부분할 수행 횟수에 따라 메쉬의 개수가 4배로 증가되면서 모델의 곡면이 더욱 부드럽게 된다. 텐션은 부분할 후 새로 생성되는 메쉬들을 평면, 오목, 볼록하게 하는 것이다. 즉, 양의 텐션값은 꼭지점들을 면의 바깥쪽으로 푸쉬하면서 면들을 볼록하게 하고, 이와 반대로 음의 텐션값은 꼭지점들을 면의 안쪽으로 끌면서 면들을 오목하게 한다. 그림 8 (c) 및 (d)는 Africanas bust 모델의 와이어프레임과 0 텐션으로 부분할된 모델의 와이어프레임을 각각 보여주고 있다. 삼각 부분할에 대한 실험 결과인 그림 7 (b)를 살펴보면, 텐션값이 0일 때 $\bar{e}(\mathbf{H}, \mathbf{H}')$ 은 0.1이하이며, 텐션값이 ± 25 , ± 50 일 때

0.105-0.125이다. 즉, 제안한 해싱은 텐션값이 [-50 +50] 일 때 모두 강인함을 알 수 있었다. 기존 3D-SSD 기법과 Entropic 기법 결과를 살펴보면, 텐션값이 각각 ± 50 및 ± 45 일 때까지 강인하게 나타났다. 따라서 삼각 부분할에서 제안한 해싱은 기존 방법에 비하여 보다 강인함을 확인하였다.

꼭지점 접합은 문턱치 Tr 내에 존재하는 모든 꼭지점들을 접합하는 것으로 단혀진 또는 중복되는 꼭지점들을 가지는 메쉬들을 제거하는 데 사용된다. 여기서 문턱치 Tr 은 접합 과정 전 꼭지점들이 얼마만큼 가까운 거리에 있는지를 나타내는 것으로, Tr 이 높을수록 접합되는 꼭지점들이 많아지며 더욱 작은 메쉬들을 제거됨으로써 메쉬 형상이 변형된다. 본 실험에서는 문턱치 Tr 을 [0.1 1.0]으로 가변하면서 모든 모델의 객체들에 대하여 꼭지점 접합을 수행하였다. 그림 8 (e)는 0.6의 문턱치 Tr 로 접합된 Bed 모델을 보여주고 있다. 실험 결과인 그림 7 (c)를 살펴보면, Tr 이 0.1-0.6일 때 $\bar{e}(\mathbf{H}, \mathbf{H}')$ 은 0.073-0.14이며, Tr 이 0.7-1.0일 때 $\bar{e}(\mathbf{H}, \mathbf{H}')$ 은 0.16-0.20이다. 즉, 제안한 해싱은 꼭지점 접합에 대하여 Tr 이 약 0.65일 때까지는 강인함을 알 수 있었다. 기존 3D-SSD 기법과 Entropic 기법의 결과를 살펴보면, Tr 이 약 0.40일 때까지 강인하게 나타났으므로, 제

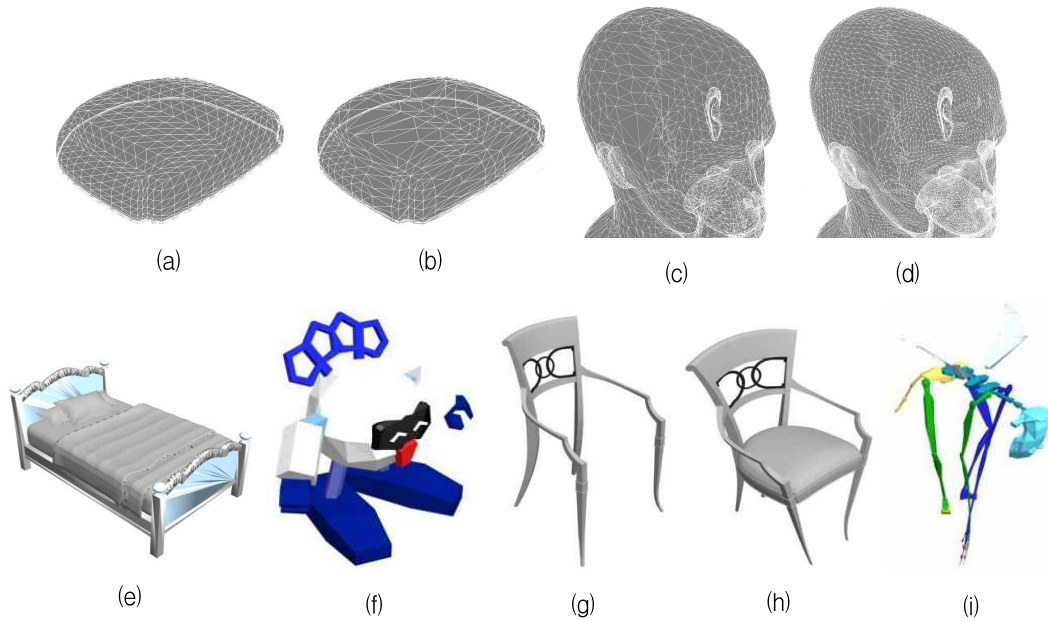


그림 8. (a) Armchair 모델의 특징 객체 와이어프레임모델과 (b) 60%로 다해상도 변환된 모델, (c) Africanas bust 모델의 와이어프레임모델과 (d) 0 텐션값으로 부분화된 모델, (e) 0.6의 Tr로 꼭지점 접합된 Bed 모델, (f) x축으로 대칭된 Bomb 모델, (g) 일부 특징 객체가 삭제된 Armchair 모델, (h) x축으로 40도 구부러진 Armchair 모델, (i) 1.0의 세기로 점감된 Waller 모델

Fig. 8. (a) A wireframe model of feature object in Armchair model and (b) a model transformed to 60% resolution of (a), (c) a wireframe model of Africanas bust model and (d) a model tessellated to 0 tension value, (e) Bed model welded to 0.6 threshold, (f) Bomb model symmetric to x axis, (g) Armchair model with cropped feature object, (h) Armcahir model bended to 40degree on the x axis, and (i) Waller model tapered with 1.0 intensity.

안한 해싱이 기존 방법에 비하여 보다 강인함을 확인할 수 있다.

모델 대칭은 캐릭터 모델링, 건물 또는 항공기 설계 등에 매우 유용한 기능으로 선택된 객체들을 x, y, 또는 z 평면에 대칭되도록 반사하는 것으로 필요시 객체 일부분을 자르기도 한다. 그리고 모델 대칭에서 꼭지점들은 공통 이음면에 따라 접합된다. 본 실험에서는 모든 모델의 객체들을 x, y, 및 z 평면 기준으로 대칭되도록 변형하였다. 그림 8 (f)는 x축으로 평면 대칭된 Bomb 모델을 보여주고 있다. 모델 대칭의 실험 결과인 그림 7 (d)를 살펴보면, x축 평면 대칭에서는 $\bar{e}(\mathbf{H}, \mathbf{H}')$ 가 0.107로 낮으나 y축 및 z축 평면 대칭에서는 $\bar{e}(\mathbf{H}, \mathbf{H}')$ 가 각각 0.247 및 0.160으로 높게 나타남을 볼 수 있다. 즉, 제안한 해싱은 x축 평면 대칭에서는 강인하나, y축 및 z축 평면 대칭에서는 약함을 알 수 있었다. 기존 3D-SSD 기법과 Entropic 기법들은 모든 축에 대한 평면 대칭에서 약하게 나타났다. 따라서 모델 대칭에 대하여 제안한 해싱이 기존 방법에 비하여 일부 강인함을 확인하였다.

3D 모델의 주요 객체들은 삭제되어 다른 곳에 사용되거나 혹은 주요하지 않은 객체들이 삭제되어 주요 객체들만 남겨질 수 있다. 제안한 해싱에서는 주요 객체인 특징 객체를 해쉬 대상으로 하고 있으므로, 비특징 객체 삭제와는 무관하다. 따라서 본 실험에서는 하나 이상의 특징 객체를 가지는 모델에 대하여 임의의 특징 객체들을 삭제하였다. 그림 8 (g)는 일부 특징 객체가 삭제된 Armchair 모델을 보여주고 있다. 실험 결과로 1개의 특징 객체 삭제에서는 $\bar{e}(\mathbf{H}, \mathbf{H}')$ 가 0.14이나 2개 이상의 특징 객체 삭제에서는 $\bar{e}(\mathbf{H}, \mathbf{H}')$ 가 0.25으로 높게 나타났다. 즉, 제안한 해싱에서는 1개의 특징 객체 삭제에 대하여 강인함을 확인하였다. 기존 3D-SSD 기법은 단일 객체 모델에 대하여 적용된 것으로 객체 삭제에 대하여 약하게 나타났다. 그러나 Entropic 기법은 부메쉬 분할에 의하여 일부 객체가 삭제되더라도 나머지 부메쉬에 의하여 해쉬 추출이 가능하다.

나. 기하학 편집

3D 모델들은 임의의 위치 및 방향으로 이동 및 회전

될 수 있으며, 임의의 스케일로 확대 및 축소될 수 있다. 이와 같은 RST 공격은 3D 모델의 가장 일반적인 공격으로 형상 변환없이 모든 꼭지점 좌표가 변경된다. 제안한 해싱은 특징 객체별 꼭지점 거리 분포를 이용하므로 회전 및 이동 공격에는 전혀 영향이 없다. 또한 특징 객체의 면적 기반 정규화 과정이 수행되므로 스케일링 공격에도 영향을 받지 않는다. 따라서 RST 실험 결과에서 $\bar{e}(\mathbf{H}, \mathbf{H}')$ 는 모두 0으로 오류없이 추출됨을 확인하였다. 표 3에서와 같이 기존 방법은 이동 및 회전에 대하여 강인하나, 확대 및 축소에 대하여 매우 약하게 나타났다.

모델 구부림은 임의의 축 상에서 0-360도 방향으로 모델 형상을 균일하게 구부리는 것이다. 이 공격에서는 구부림 축 상에서의 구부림 각도 및 방향에 의하여 구부림 세기를 조절할 수 있다. 여기서 구부림 각도는 수직 평면 상에서 구부러지는 각도를 나타내고, 구부림 방향은 수평 방향에 대한 구부러지는 방향을 나타낸다. 본 실험에서는 x, y, z 축을 기준으로 20-100도의 각도로 모델을 구부렸다. 그림 8 (h)는 x축 기준으로 40도로 구부러진 Armchair 모델을 보여주고 있다. 실험 결과인 그림 7 (e)를 살펴보면, x축 상에서는 20-40도일 때 $\bar{e}(\mathbf{H}, \mathbf{H}')$ 는 0.1-0.133이고, y축 상에서는 20-60도일 때 $\bar{e}(\mathbf{H}, \mathbf{H}')$ 는 0.093-0.153이고, z축 상에서는 20-100도일 때 $\bar{e}(\mathbf{H}, \mathbf{H}')$ 는 0.05-0.140이다. 실험 결과로부터 제안한 해싱은 x축 상에서는 40도, y축 상에서는 60도 그리고 z축 상에서는 100도까지 강인함을 확인하였다. 즉, 제안한 해싱은 모든 축에 대한 평균 구부림 각도가 85도일 때까지 강인하게 나타났다. 기존 3D-SSD 기법과 Entropic 기법의 결과를 살펴보면, 각각 60도 및 50도일 때까지 강인하게 나타났다. 이 결과로부터 제안한 방법이 기존 방법에 비하여 구부림 공격에 다소 약함을 확인하였다.

점감은 모델의 한 쪽 끝을 확장하고 나머지 끝을 축소함으로써 모델의 윤곽을 점감시킨다. 이 변형은 점감의 주축과 효과축 상의 점감량 및 곡선량에 의하여 점감 크기를 조정한다. 여기서 점감량은 모델의 양 끝을 확대 또는 축소 크기를 나타내며, 곡선량은 점감된 모델의 측면을 바깥쪽 또는 안쪽 곡면이 되기 위한 곡면 크기를 나타낸다. 주축은 점감의 중심축을 나타내며, 효과축은 주축에 대한 점감의 방향을 나타낸다. 본 실험에서는 주축 및 효과축을 각각 z축 및 xy축으로 놓은 다음, [0.5 2.5]의 점감량을 가변하면서 모든 모델들을

점감하였다. 그림 8 (i)는 1.0의 점감세기로 점감된 Walier 모델을 보여주고 있다. 실험 결과인 그림 7 (f)를 살펴보면, 점감량이 [0.5 2.0]일 때 $\bar{e}(\mathbf{H}, \mathbf{H}')$ 는 0.1-0.1533이고, 점감량이 2.5일 때 $\bar{e}(\mathbf{H}, \mathbf{H}')$ 는 0.16이다. 즉, 제안한 해싱이 점감량이 약 1.8일 때까지는 강인함을 확인하였다. 기존 3D-SSD 기법과 Entropic 기법의 결과를 살펴보면, 점감량이 각각 1.5 및 1.2일 때까지 강인하게 나타났다.

이상의 강인성 실험 결과로부터 제안한 해싱은 기존 방법에 비하여 구부림 공격을 제외한 메쉬 및 기하학 편집에 대하여 보다 강인함을 확인하였다.

IV. 결 론

본 논문에서는 3D 콘텐츠 인증을 위하여 강인성과 유일성을 만족하는 특징 객체 기반 3D 모델 해싱을 제안하였다. 일반적으로 3D 모델은 다양한 객체들로 구성되며, 이들 객체들은 꼭지점 좌표와 연결정보를 가지는 기하학 정보와 프레임 간의 이동, 회전 및 스케일링 등의 운동 정보를 가지고 있다. 따라서 제안한 3D 모델 해싱에서는 3D 모델의 객체들 중, 높은 면적을 가지는 객체들을 특징 객체로 선택한 후, 이들 객체 내의 꼭지점 좌표들을 정규화한다. 그리고 객체별 꼭지점 거리를 그룹화한 다음, 각 그룹 계수들을 치환 키 및 랜덤 변수 키에 의하여 최종 이진 해쉬를 생성한다. 실험 결과로부터 제안한 3D 모델 해싱이 다양한 메쉬 편집 및 기하학 편집에 강인성을 가지며, 치환 키 및 랜덤 변수 키 기반 특징 객체별 그룹 계수를 통하여 생성된 해쉬의 유일성을 확인하였다. 제안한 3D 모델 해싱은 3D 모바일 게임, 3D CG 영화, 3D E-콘텐츠, 3D 의료 모델 및 3D 전자도서관 등 다양한 3D 콘텐츠 산업 분야에서 3D 콘텐츠 인증에 사용될 수 있을 것이다. 본 연구진에서는 향후 제안한 3D 모델 해싱의 보안성을 평가하고자 하며, 3D 콘텐츠 산업 분야에 적용이 가능한 3D 모델 해싱 프로토콜을 연구하고자 한다.

참 고 문 헌

- [1] 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.

- [2] 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.
- [3] V. Monga and M.K. Mhcaik, "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.
- [4] 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.
- [5] 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.
- [6] F. Khelifi and J. Jianmin, "Perceptual Image Hashing Based on Virtual Watermark Detection," *IEEE Transactions on Image Processing*, Vol. 19, Issue 4, pp. 981-994, 2010.
- [7] Z. Guopu, H. Jiwu, S. Kwong, Y. Jianquan, "Fragility Analysis of Adaptive Quantization-Based Image Hashing," *IEEE Transactions on Information Forensics and Security*, Vol. 5, Issue 1, pp. 133-147, 2010.
- [8] 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.
- [9] 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.
- [10] L. Sunil and C.D. Yoo, "Robust Video Fingerprinting for Content-Based Video Identification," *IEEE Trans. on Circuits and Systems for Video Technology*, Vol. 18, Issue 7, pp. 983-988, July 2008.
- [11] 이석환, 권기룡, "키 기반 블록 표면 계수를 이용한 강인한 3D 모델 해싱," *대한전자공학회논문지*, 제47권 CI편 제1호, 1쪽~14쪽, 2010년 1월.
- [12] S.-H. Lee, E.-J. Lee and K.-R. Kwon, "Robust 3D Mesh Hashing Based on Shape Features," *IEEE International Conference on Multimedia & Expo*, pp. 1040-1043, July 2010.
- [13] M. Ghaderpanah, A. Abbas, A. Hamza, "Entropic Hashing of 3D Objects Using Laplace-Beltrami Operator," *IEEE International Conference on Image Processing*, pp. 3104-3107, Oct. 2008.
- [14] K. Tarmissi and A. Hamza, "Information-Theoretic Hashing of 3D Objects Using Spectral Graph Theory," *Expert Systems with Applications*, Vol 36, pp. 9409-9414, 2009.
- [15] Archibase Net, <http://www.archibase.net>, Accessed to July 2010.

 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 신호처리>



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 컴퓨터전자
 공학부 부교수
 2006년~현재 부경대학교 전자컴퓨터정보통신
 공학부 교수
 <주관심분야 : 멀티미디어 정보보호, 멀티미디어
 통신 및 신호처리>