3D 모델 해싱의 미분 엔트로피 기반 보안성 분석

정회원 이 석 환*, 권 기 룡**°

Security Analysis based on Differential Entropy in 3D Model Hashing

Suk-Hwan Lee*, Ki-Ryong Kwon**° *Regular Members*

요 약

영상, 동영상 및 3D 모델의 인증 및 복사방지를 위한 콘텐츠 기반 해쉬 함수는 강인성 및 보안성의 성질을 만족하여야 한다. 이들 중 해쉬의 보안성을 분석하기 위한 방법으로 미분 엔트로피 방법이 제시되었으나, 이는 영상 해쉬 추출에서만 적용되었다. 따라서 본 논문에서는 미분 엔트로피 기반의 3D 모델 해쉬 특징 추출의 보안성을 분석하기 위한 모델링을 제안한다. 제안한 보안성 분석 모델링에서는 3D 모델 해싱 기법 중 가장 일반적인 두 가지 형태의 특징 추출 방법을 제시한 다음, 이들 방법들을 미분 엔트로피 기반으로 보안성을 분석하였다. 이들 결과로부터 해쉬 추출 방법에 대한 보안성을 분석하고 보안성과 강인성과의 상호보완관계에 대하여 논하였다.

Key Words : 3D model hashing, Security analysis, Differential entropy, 3D feature value, 3D model authentication

ABSTRACT

The content-based hashing for authentication and copy protection of image, video and 3D model has to satisfy the robustness and the security. For the security analysis of the hash value, the modelling method based on differential entropy had been presented. But this modelling can be only applied to the image hashing. This paper presents the modelling for the security analysis of the hash feature value in 3D model hashing based on differential entropy. The proposed security analysis modeling design the feature extracting methods of two types and then analyze the security of two feature values by using differential entropy modelling. In our experiment, we evaluated the security of feature extracting methods of two types and discussed about the trade-off relation of the security and the robustness of hash value.

Ⅰ. 서 론

멀티미디어 또는 콘텐츠 기술의 급격한 발전과 더불어 콘텐츠 복사 방지, 인증 및 저작권 보호와 같은 콘텐츠 보호 기술들이 많이 제안되어져 왔다. 최근 3D 영상물에 대한 관심이 고조되면서 3D 워터마킹[1-7] 및 3D 해싱[8-10]과 같은 콘텐츠 보호 기술에 대한 연구가 필요하게 되었다. 3D 워터마킹은 3D 모델 내의 기하학 또는 위상학적 구조를 이용하여 저작권 정보에 대한 워터마크를 삽입하는 기술로서, 워터마크 삽입시 구조 변화가 나타나게 된다. 이와 반대로 3D 해싱은 3D 모델의 특징 벡터를 추출하여 이를 특정 정보와 결합하여 사용자에게 유일한 해쉬를 생성하는 것으로 원 모델의 변화가 전혀 없는 것이다.

※ 본 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(KRF-2009-0071269)
* 동명대학교 정보보호학과 (skylee@tu.ac.kr),
** 부경대학교 IT융합응용공학과 (krkwon@pknu.ac.kr) (° : 교신저자)
논문번호 : KICS2010-08-390, 접수일자 : 2010년 8월 9일, 최종논문접수일자 : 2010년 11월 30일

콘텐츠 해싱은 일반적으로 전처리, 특징 벡터 추출, 이진화 과정 및 해쉬 생성의 단계로 이루어진다. 그리고 콘텐츠 해싱의 가장 주요한 조건으로는 보안성과 강인성이 있다. 이는 특징 벡터 추출 방법에 의하여 대부분 만족할 수 있다. 여기서 강인성은 다양한 공격에서도 해쉬가 보존되어야 하는 것이다. 공격 형태로는 영상에서는 압축, RST, 영상처리 등이 있고, 3D 모델에서는 기하학적 변형 및 위상학적 변형이 있다. 보안성은 해쉬의 예측불가능성, 단일 방향성 및 충돌 회피성 등을 만족하여야 하는 것이다. 그러나 콘텐츠 해싱 연구에서 정량적으로 보안성을 평가하기가 어려워, 많은 논문에서는 이를 제시하지 못하였다. 이러한 문제점을 해결하기 위하여 Swaminathan 등[11,12]은 영상 해싱에서 특징 추출의 보안성을 평가하기 위하여 미분 엔트로피 기반으로 특징 벡터의 랜덤 양을 측정하였다. 그러나 이들은 영상 해싱에서만 적용되는 것으로 3D 모델 해싱에서는 아직까지 적용되지 못하였다.

본 논문에서는 Swaminathan 등[11,12]이 제시한 미분 엔트로피 기반으로 3D 모델 해싱의 특징 벡터의 보안성을 평가하고자 한다. 제안한 방법에서는 3D 모델에서 여러 개의 객체들 중 주요 객체를 선택한 후, 주요 객체의 그룹별 꼭지점 거리 분포를 생성한다. 그리고 모든 객체의 거리 분포들을 치환 조합하여 그룹 계수를 추출한다. 이 때 그룹 계수는 가우시안 랜덤 키 계수와 합과 곱의 형태로 나누어 해쉬 생성에 필요한 특징 계수가 생성된다. 제안한 방법에서는 랜덤 키 기반 합과 곱의 형태의 특징 계수들을 미분 엔트로피에 의하여 보안성을 평가한다. 모델에 따라 특징 계수가 다르므로 해쉬의 보안성은 랜덤 키와 특징 계수 및 객체 수에 의하여 결정된다. 실험 결과로부터 합의 형태보다 곱의 형태가 보안성이 우수함을 확인하였다.

본 논문의 구성을 살펴보면, 2장에서는 간단한 3D 모델 해싱 특징 계수 추출 기법에 대하여 제안하며, 3장에서는 두 가지 형태에 대한 미분 엔트로피 모델링에 대하여 설명한다. 그리고 4장에서는 보안성 평가에 대한 결과 및 분석에 대하여 살펴보며 마지막 5장에서 본 논문의 결론을 맺는다.

Ⅱ. 3D 모델 해싱

3D 그래픽스, 3D 캐릭터, 3D 영화 등에서 사용되는 3D 모델은 일반적으로 여러 개의 객체들로 구성되어 있으며, 이들 객체들은 꼭지점과 연결정보로 구성된 기하학 정보와 킷 타임별로 움직이는 정보인 보간기 정보로 구성된다. 따라서 본 논문에서는 3D 객체 모델에 적용할 수 있는 간단한 해싱 기법[10]과 이에 대한 보안성을 평가한다.

제안한 3D 해싱의 전체 과정에서 그림 1에서와 같으며 이를 간단히 요약하면 다음과 같다.

1) 3D 객체 모델 M 내의 객체들 중 면적 비율이 높은 객체들을 선택하여 이를 특징 객체 $O_1, O_2, \cdots O_n$로 선택한다. 이 때 n은 선택된 특징 객체의 수를 나타낸다.
2) 특징 객체 O_i들 내의 모든 꼭지점들의 거리를 구한 다음, 이를 B개의 거리 간격으로 나누어진 그룹으로 할당한다. 그룹 개수 B는 해쉬 비트수를 결정한다. 그리고 각 그룹 내의 모든 거리들을 동일한 범위 $[0\,\Delta s]$ 내에 있도록 정규화한 다음, 이들의 평균 거리를 그룹 계수 $g_{ik} = \sum_{j=1}^{N_{ik}} d_{ik,j} / N_{ik}$로 사용한다. 여기서 i,k는 특징 객체 인덱스와 그룹 인덱스를 각각 나타내며, N_{ik}는 i,k번째 그룹 내에 할당된 거리의 개수이다. 그리고 $d_{ik,j}$는 정규화된 꼭지점 거리를 나타낸다.
3) 치환된 그룹 내의 동일 인덱스를 가지는 그룹 계수들의 합 $\sum_{i=1}^{n} g_{ij}$을 구한다.
4) 가우시안 랜덤 계수 r_k를 생성한 다음, 그룹 계수의 합을 이용하여 두 가지 타입의 특징 계수 f_k를 구한다. 첫 번째 특징 계수는

$$f_k^{(1)} = r_k \Delta s/2 + \sum_{i=1}^{n} g_{ik}/2n \tag{1}$$

와 같이 랜덤 계수와 그룹 계수와의 합의 형태를 가지고 있다. 두 번째 특징 계수는

$$f_k^{(2)} = r_k \left(\sum_{i=1}^{n} (g_{ik} - \Delta s/2)/n\right) \tag{2}$$

와 같이 랜덤 계수와 그룹 계수와의 곱의 형태를 가지

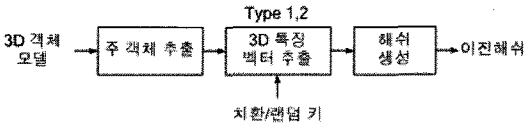


그림 1. 3D 객체 모델 상에서 해쉬 생성 과정

고 있다.

5) 위에서 구한 특징 계수를 이진화 과정에 의하여 최종 해쉬 $h_k(k \in [1,B])$를 생성한다.

제안한 방법에서는 해쉬의 보안성을 높이기 위하여 랜덤 계수의 길이를 증가하면 되나, 동일한 랜덤 계수 길이에 대하여 두 가지 형태의 랜덤 양을 평가하고자 한다.

Ⅲ. 보안성 평가 모델링

제안한 방법에서는 Swaminathan 등[11,12]이 제시한 미분 엔트로피 기법을 이용하여 두 가지 형태의 특징 계수를 모델링하여 보안성을 평가한다. 랜덤 변수 X가 받침 영역 $\boldsymbol{X}$ 내에 확률밀도함수 $p(x)$를 가질 때 X의 미분 엔트로피 $h(X)$는

$$h(X) = -\int_{-\boldsymbol{X}} p(x)\log_2 p(x)dx \tag{3}$$

와 같이 정의된다[12]. 이는 해쉬 값의 랜덤 양을 측정하는 척도로 사용되며, $h(X)$가 클수록 랜덤 양이 크며 해쉬 값을 변조하기 위하여 많은 시도($\alpha^{h(X)}$, $\alpha > 1$)가 필요하다. 앞 절에서 구한 두 가지 특징 계수에 대한 미분 엔트로피 모델링은 다음과 같다.

3.1 특징 계수 - 타입 1

특징 계수에서 r_k는 평균 m_r과 분산 σ_r^2인 가우시안 분포 함수 $p_r(x) = \frac{1}{\sqrt{2\pi}\sigma_r} exp(-\frac{(x-m_r)^2}{2\sigma_r^2})$이다. 그리고 그룹 계수는 그룹 내에 꼭지점 개수가 전혀 없으면 0, 있으면 가우시안 분포를 가진다. 즉 그룹 계수는 g_{ik}는

$$g_{ik} = b_{ik} w_{ik} \tag{4}$$

와 같이 Bernoulli 분포를 가지는 계수 b_{ik} ($P[b_{ik}=0] = 1/2$ $P[b_{ik}=1] = 1/2$)와 평균 $m_w = \triangle s/2$와 분산 σ_w를 가지는 가우시안 분포 $p_w(x) = \frac{1}{\sqrt{2\pi}\sigma} exp(-\frac{(x-m_w)^2}{2\sigma_w^2})$를 계수 w_{ik}의 곱으로 정의될 수 있다. 이 때 분산은 모델마다 다르게 나타난다. 3D 테스트 모델 중 Armchair 모델과 Africanas bust 모델에 대한 그룹 계수 분포는 그림 2 (a)와 (b)에서와 같다. 이들 분포로부터 그룹 계수의 분포가 Bernoulli 분포와 가우시안 분포의 곱으로 모델링될 수 있음을 볼 수 있다. 제안한 방법에서는 모든 모델의 동일한 분포 모델링을 위하여 최대 그룹 계수 범위 $\triangle s$를 1이 되도록 정규화한다. 이 때 정규화된 그룹 계수의 평균은 0.5에 근접한다.

수식 (1)의 특징 계수 1의 미분 엔트로피를 구하기 위하여 특징 계수 $f_k^{(1)}$의 확률밀도함수 $p_{f^{(2)}}(x)$를 구하여야 한다. 제안한 방법에서는 수식 (1)를

$$\begin{aligned} f_k^{(1)} &= R_k + G_k \\ \text{where } R_k &= r_k \triangle s/2, \\ G_k &= \sum_{i=1}^{n} g_{ki}/2n = \sum_{i=1}^{n} b_{ki} w_{ki}/2n \end{aligned} \tag{5}$$

와 같이 두 변수 R_k, G_k에 의하여 정의한다. 여기서 R_k는 평균 m_R 및 분산 σ_R^2이 각각

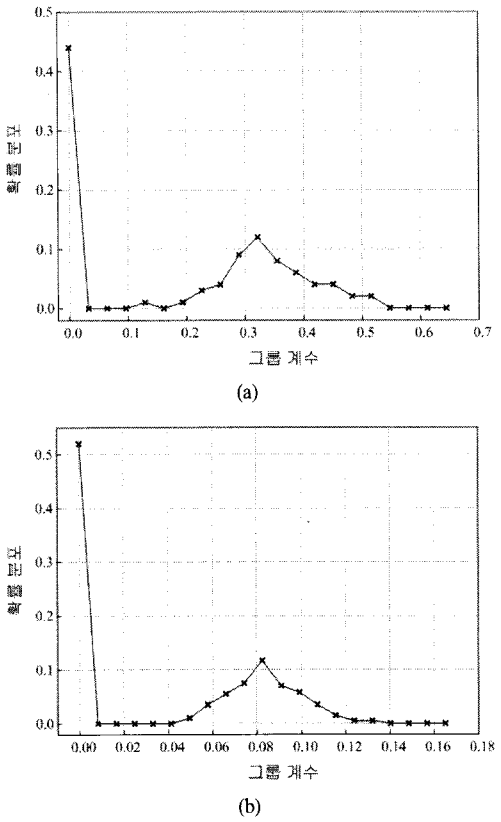


그림 2. (a) Armchair 모델 ($\triangle s$=0.644002)과 (b) Africanas bust 모델 ($\triangle s$=0.165053), 의 그룹 계수의 분포

$$m_R = (\Delta s/2)m_r,\ \sigma_R^2 = (\Delta s/2)\sigma_r^2 \quad (6)$$

와 같은 가우시안 분포를 가진다. 그리고 G_k는 b_{ki}와 $w_{ki}/2n$ 계수 곱의 합으로 정의된다. 즉, R_k와 G_k의 합으로 이루어져있으므로, 제안한 방법에서는 특성 함수(Characteristic function)를 이용하여 확률밀도함수 $p_{f^{(1)}}(x)$를 구한다. 우선 R_k의 특성 함수 $\Phi_R(\omega)$는

$$\Phi_R(\omega) = \exp(j\omega m_R - \omega^2\sigma_R^2/2) \quad (7)$$

이다. G_k에서 $b_{ki}w_{ki}/2n$ $(i \in [1,n])$은 iid(independent and identically distributed) 랜덤 변수이므로 G_k의 특성 함수 $\Phi_G(\omega)$은 $b_{ki}w_{ki}/2n$의 특성 함수 $\Phi_{G_{ki}}(\omega)$ $= \frac{1}{2}(1+\exp(j\omega m_G - \omega^2\sigma_G^2/2))$의 곱으로

$$\begin{aligned}\Phi_G(\omega) &= \{\Phi_{G_k}(\omega)\}^n \\ &= \frac{1}{2^n}(1+\exp(j\omega m_G - \omega^2\sigma_G^2/2))^n \\ &= \frac{1}{2^n}\sum_{i=0}^{n}\binom{n}{i}\exp(j\omega i m_G - \omega^2\sigma_G^2 i/2) \\ &\binom{n}{i} = \frac{n!}{i!(n-i)!}\end{aligned} \quad (8)$$

와 같이 정의되어진다. 그러므로 $f_k^{(1)}$의 특성 함수 $\Phi_{f^{(1)}}(\omega)$는

$$\Phi_{f^{(1)}}(\omega) = \Phi_R(\omega)\Phi_G(\omega) \quad (9)$$

$$= \frac{1}{2^n}\sum_{i=0}^{n}\binom{n}{i}\exp(j\omega i m_G - \omega^2\sigma_G^2 i/2)\exp(j\omega m_R - \omega^2\sigma_R^2/2)$$

$$= \frac{1}{2^n}\sum_{i=0}^{n}\binom{n}{i}\exp(j\omega(i m_G + m_R) - (i\sigma_G^2 + \sigma_R^2)\omega^2/2)$$

이고, $p_{f^{(1)}}(x)$는 이의 역 특성 함수이므로

$$p_{f^{(1)}}(x) = \frac{1}{2^n}\sum_{i=0}^{n}\binom{n}{i}\frac{1}{\sqrt{2\pi}\,\sigma_i}exp(\frac{(x-m_i)^2}{2\sigma_i^2}) \quad (10)$$

$$\text{where } m_i = i m_G + m_R,\ \sigma_i^2 = i\sigma_G^2 + \sigma_R^2$$

와 같이 구하여진다. 위에서 구한 $p_{f^{(1)}}(x)$는 n+1개의 가우시안 밀도 함수의 합으로 구성됨으로 수식 (3)에서 정의된 미분 엔트로피 $h(f_k^{(1)})$를 수학적으로 모델링하기가 어렵다. 따라서 제안한 방법에서는 이산 구간에 대한 면적의 합에 의하여

$$h(f_k^{(1)}) \simeq -\sum_{j=0}^{N} f_k(x_j)\log_2(x_j)\Delta t \quad (11)$$

$$\text{where } x_j = j\Delta t$$

와 같이 $h(f_k^{(1)})$를 수치적으로 계산한다. 여기서 N은 $f_k^{(1)}$의 반침 영역 상의 샘플 개수이고, Δt는 거의 0에 가깝다.

$p_{f^{(1)}}(x)$에 따라 $h(f_k^{(1)})$는 3D 모델의 특징 객체 수 n와 평균 m_G, 분산 σ_G^2과 랜덤 계수 키의 평균 m_R 및 분산 σ_R^2에 의하여 결정된다. 여기서 m_G는 거의 0.5에 가까우므로, 제안한 방법에서는 그룹 계수와 랜덤 계수의 평균을 동일하게 m_R가 0.5로 놓았다. 이로부터 특징 계수 $f_k^{(1)}$의 보안성은 3D 모델과 랜덤 계수 키의 분산 및 객체 수에 의하여 결정된다.

3.2 특징 계수 - 타입 2

수식 (2)에서 타입 2의 특징 계수 $f_k^{(2)}$는 두 개의 랜덤변수 r_k와 y_k의 곱으로

$$f_k^{(2)} = r_k y_k \quad (12)$$

$$\text{where } y_k = \sum_{i}^{n}(g_{ki} - \Delta s/2)/n$$

와 같이 정의된다. 두 계수의 곱으로 이루어진 특징 계수의 확률밀도함수 $p_{f^{(2)}}(x)$를 구하는 것은 어렵다. 제안한 방법에서는 이를 간단하게 모델링하기 위하여 우선 랜덤 계수 r_k를 평균과 분산 각각 m_r=0, σ_r^2=0.2의 가우시안 분포를 가지도록 한다. 그리고 y_k에서 꼭지점 개수를 포함하지 않는 그룹은 제외하며, 그룹 계수 g_{ki}/n의 범위가 $[-\Delta s/2, \Delta s/2]$ 내에 있도록 g_{kl}를 $g_{ki} - \Delta s/2$에 의하여 $[-\Delta s/2, \Delta s/2]$ 범위로 이동한다. 즉, 수식 (5)의 Bernoulli 분포를 가지는 계수 b_{kl}이 제외되며, $(g_{ki} - \Delta s/2)/n$는 평균이 0이고, 분산이 σ_{ki}^2/n인 가우시안 분포를 가진다. 따라서 y_k의 확률밀도함수 $p_y(x)$는 $(0, \sigma_{ki}^2/n)$ 가우시안 분포 함수의 합으로 이루어지므로, $p_y(x)$는

$$f_y(x) = \frac{1}{\sqrt{2\pi(\sum_{i=1}^{n}\sigma_{ki}^2/n)}}exp(-\frac{x^2}{2\sum_{i=1}^{n}\sigma_{ki}^2/n}), \quad (13)$$

$$(m_y = 0,\ \sigma_y^2 = \sum_{i=1}^{n}\sigma_{ki}^2/n)$$

와 같다.

$f_k^{(2)}$는 두 개의 다른 가우시안 분포 함수의 곱의 형태를 가진다[13]. 따라서 $f_k^{(2)}$의 확률밀도함수 $p_{f^{(2)}}(x)$는

$$\begin{aligned} f_k^{(2)}(x) &= f_{ry}(x) \\ &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f_r(u) f_y(v)\delta(uv-x)dudv \quad (14) \\ &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} [\frac{1}{\sqrt{2\pi}\,\sigma_r} exp(-\frac{u^2}{2\sigma^2}) \times \\ &\quad \frac{1}{\sqrt{2\pi(\sum_{i=1}^{n}\sigma_{ki}^2/n)}} exp(-\frac{v^2}{2\sum_{i=1}^{n}\sigma_{ki}^2/n}), \\ &\quad \delta(uv-x)]dudv \\ &= \frac{1}{\pi\sigma_r\sigma_y} K_0(\frac{|x|}{\sigma_r\sigma_y}), \ \sigma_y = \sqrt{\sum_{i=1}^{n}\sigma_{ki}^2/n} \end{aligned}$$

와 같이 구하여진다. 여기서 $K_n(x)$은 두 번째 타입의 수정된 Bessel 함수(modified Bessel function of the second kind)이며, 0차수 함수 $K_0(x)$는

$$\begin{aligned} K_0(x) &= \int_0^{\infty} \cos(x\sinh t)dt \\ &= \int_0^{\infty} \frac{\cos(xt)}{\sqrt{t^2+1}}dt \end{aligned} \quad (15)$$

와 같이 정의될 수 있다[14]. 위의 식을 이용하여 $p_{f^{(2)}}(x)$를 재정리하면,

$$\begin{aligned} f_{k^{(2)}}(x) &= \frac{1}{\pi\sigma_r\sigma_y} K_0(\frac{|x|}{\sigma_r\sigma_y}) \\ &= \frac{1}{\pi\sigma_r\sigma_y}\int_0^{\infty} \frac{\cos(xt)}{\sqrt{t^2+1}}dt \end{aligned} \quad (16)$$

와 같다. 따라서 $f_k^{(2)}$의 미분 엔트로피 $h(f_k^{(2)})$는 수식 (11)에서와 같이 수치적으로 계산하여 구하여진다.

특징 계수 $f_k^{(2)}$의 보안성은 $f_k^{(1)}$에서와 같이 3D 모델의 특징 객체 수 n 및 특징 객체별 분산 σ_{ki}^2과 랜덤 계수 키의 분산 σ_r^2에 의하여 결정된다.

Ⅳ. 실험결과

본 논문에서 제안한 3D 해싱 보안성 평가는 3D 모델과 랜덤 키에 의하여 결정되므로, 다양한 3D 모델에 대하여 보안성을 평가하였다. 본 실험에서는 그림 3에서와 같이 ARCHIBASE NET[16]에서 제공하는 모델들을 사용하였으며, 각 모델들의 객체 수 및 선택된 특징 객체 수와 σ_G, σ_y은 표 1에서와 같다. σ_G은 식 (10)에서와 같이 각 모델 그룹 계수의 꼭지점 거리 표준편차로 $h(f_k^{(1)})$를 결정하는 변수이고, σ_y은 각 모델의 그룹별 꼭지점 거리 표준편차의 제곱 합으로 식 (14)에서와 같이 $h(f_k^{(2)})$를 결정하는 변수이다.

특징 계수 1,2의 확률밀도함수를 살펴보기 위하여, 본 실험에서는 대표적인 Africanas bust 모델의 $p_{f^{(1)}}(x)$ 및 $p_{f^{(2)}}(x)$를 특징객체 수별로 그림 4에서와 같이 나타내었다. $p_{f^{(1)}}(x)$는 가우시안 분포를 가지며, 객체 수가 증가함에 따라 평균이 증가하고, 분산이 작아짐을 볼 수 있다. 그리고 $p_{f^{(2)}}(x)$는 2차 Bessel 분포를 가지며 마찬가지로 객체 수가 증가함에 따라 분포가 넓어짐을 볼 수 있다.

각 모델에 대한 객체수별 미분 엔트로피 $h(f_k^{(1)})$ 및 $h(f_k^{(2)})$는 그림 5에서와 같다. 이 그림을 살펴보면,

표 1. 대표적인 3D 모델의 객체 수, 특징객체 수 및 면적비율

모델명	객체 수	특징 객체 수	면적 비율 [%]	표준 편차σ_G	표준 편차σ_y
Africanas bust	5	4	94	0.1202	0.1487
Armchair	2	2	100	0.1707	0.1707
Bed	21	3	86	0.0864	0.1209
Cake	25	2	70	0.2273	0.2481
Sofa	4	2	82	0.1619	0.1730
평균	11	2.6	86.4	0.1533	0.1722

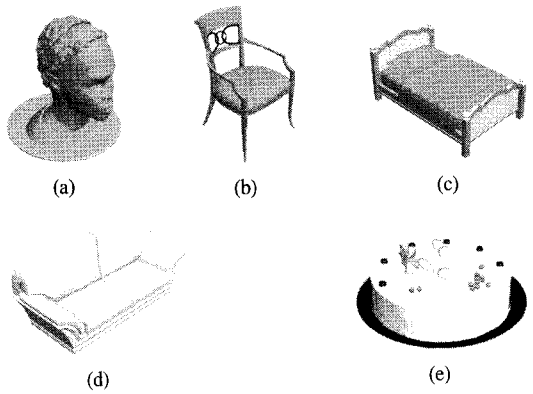
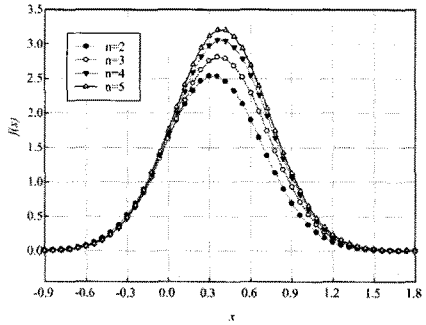
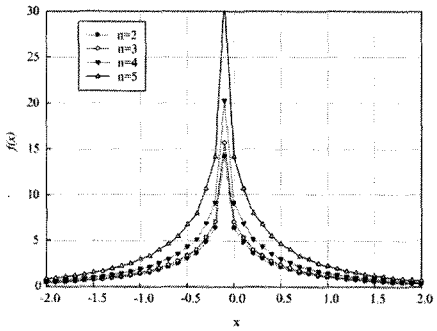


그림 3. 대표적인 3D 모델 (a) Africanas bust, (b) Armchair, (c) Bed, (d) Sofa 및 (f) Cake.

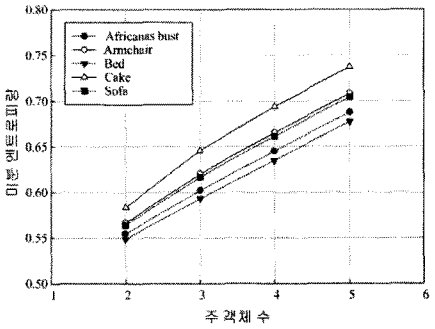


(a)

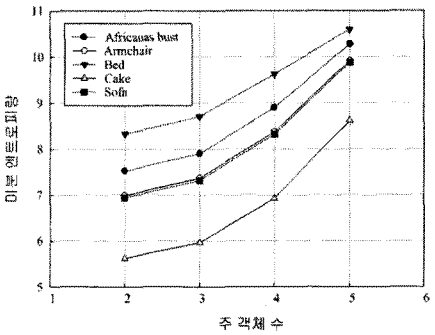


(b)

그림 4. Africanas bust 모델의 (a) $p_{f^{(1)}}(x)$ 및 (b) $p_{f^{(2)}}(x)$



(a)



(b)

그림 5. 각 모델의 객체 수에 대한 미분 엔트로피 값 (a) $h(f_k^{(1)})$ 및 (b) $h(f_k^{(2)})$

객체 수가 증가함에 따라 $h(f_k^{(1)})$, $h(f_k^{(2)})$ 모두 증가되므로, 보안성이 증가됨을 알 수 있다. 그리고 객체 수가 n=[2 5]일 때 평균적으로 $h(f_k^{(1)})$은 [0.56 0.70]이고, $h(f_k^{(2)})$은 [7.08 9.85]이다. $h(f_k^{(2)})$가 $h(f_k^{(1)})$보다 약 12-14배 정도 크게 나타났다. 따라서 곱의 특징계수 $f_k^{(2)}$가 합의 특징계수 $f_k^{(1)}$보다 보안성이 아주 우수함을 알 수 있었다.

그러나 객체 수가 증가할수록 공격에 대한 해쉬의 강인성이 약해진다. 각 모델들은 주요 객체의 비율이 비주요 객체에 비하여 많은 면적을 차지한다. 따라서 제안한 방법에서는 면적 비율이 높은 주요 객체들을 선택하여 이들 객체들에 대한 특징계수를 추출하여 해쉬를 생성한다. 표 1에 살펴보면, 특징객체가 전체 객체에 비하여 약 86% 정도의 면적을 차지하며, 거의 대부분의 모델에서 2-4개의 객체들이 선택됨을 볼 수 있다.

각 모델에 대한 미분 엔트로피량은 표 2에서와 같으며, 각 객체 수에 대한 특징계수 1의 미분 엔트로피 $h(f_k^{(1)})$는 0.5641-0.6449이고, 특징계수 2의 미분 엔트로피 $h(f_k^{(2)})$는 5.6222-8.8994이다. 즉, $h(f_k^{(2)})$가 $h(f_k^{(1)})$보다 평균적으로 12.5배 정도 높음을 볼 수 있다. 이 결과로부터, 해쉬의 특징 계수는 동일 길이를 가지는 랜덤 계수 키에서 합의 형태보다 곱의 형태가 보안성이 우수함을 알 수 있었다. 이는 3D 해싱 뿐만 아니라 3D 워터마킹, 3D 검색 등에서도 효과적으로 적용될 수 있을 것이라 판단된다.

제안한 3D 객체 모델 해싱의 보안성에 대한 비교 평가를 위하여 본 실험에서는 대표적인 영상 해싱 기법인 Swaminathan[10,11] 기법의 영상에 대한 미분 엔트로피양을 측정하여 이를 표 2에 나타내었다. Swaminathan 기법의 키 길이와 해쉬 길이가 다르므로, 본 실험에서는 동일한 키 길이와 해쉬 길이가 되도록 생성하였다. 표 2를 살펴보면, 영상 해싱의 미분 엔트로피양은 평균적으로 6.20-7.76으로 제안한 해싱의 특징계수 2보다 일부 모델을 제외하고 약 0.73-2.699보다 작음을 확인하였다.

마지막으로 본 실험에서는 보안성과 강인성의 상호 보완적인 관계를 살펴보기 위하여 객체 수를 가변하였을 때 일부 공격에 대한 강인성을 평가하였다. 강인성 평가에서는 기존 논문에서도 널리 사용되는 정규화된 Hamming 거리차 $D(h,h')$를

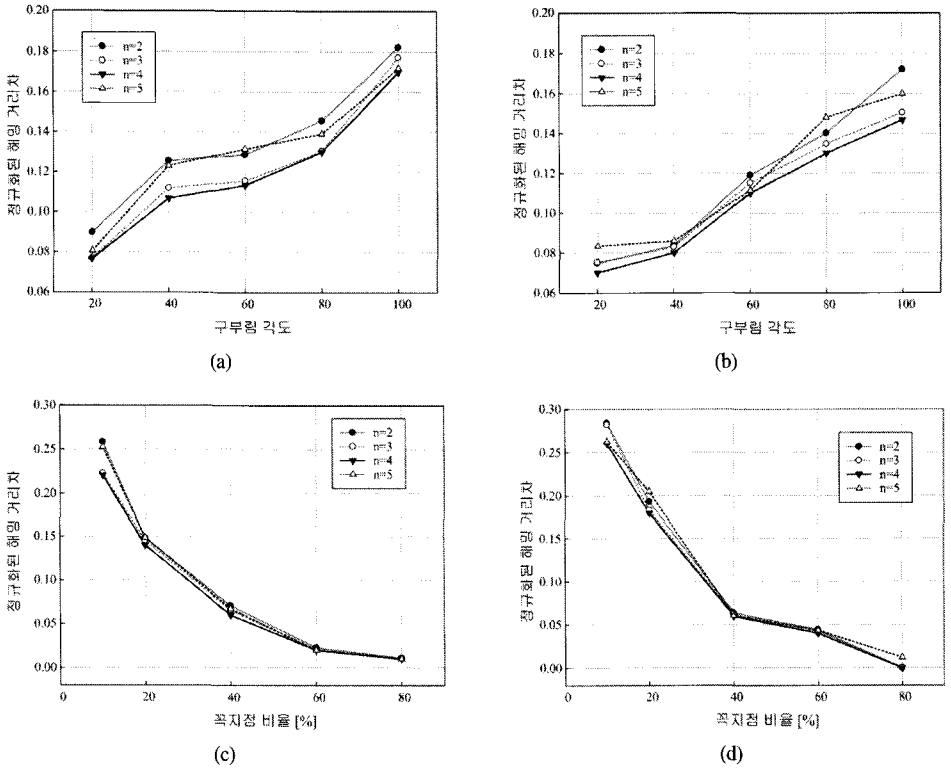


그림 6. Africanas bust 모델의 구부림 공격에 대한 (a) 특징계수 1, (b) 특징계수 2 및 메쉬 간단화에 대한 (c) 특징계수 1, (d) 특징계수 2의 정규화 Hamming 거리

$$D(h,h') = \frac{1}{N}\sum_{i=1}^{N}|h_i - h_i'| \qquad (17)$$

이용하였다. 여기서 $h=\{h_i|i\in[1,N]\}$는 원 모델 상의 해쉬를 나타내고, $h'=\{h_i'|i\in[1,N]\}$는 공격받은 모델 상의 해쉬를 나타낸다. 그리고 N은 해쉬 길이이다. 강인성 평가를 위한 공격에서는 가장 일반적인 3D 모델 편집인 메쉬 간단화와 구부림을 Africanas bust 모델에 대하여 수행하였다. 구부림은 전체 모델의 형상을 구부림 각도에 따라 구부리는 것으로 본 실험에서는 Africanas bust 모델을 x,y,z 축을 기준으로 20°-100°으로 구부렸다. 특징 계수 1,2에 대한 구부림 실험 결과는 그림 6 (a), (b)에서와 같으며, 이 그림으로부터 객체 수가 2,3,5일 때보다 4일 때 가장 강인함을 알 수 있었다. 그리고 특징 계수 2가 특징 계수 1보다 정규화된 Hamming 거리가 약 0.00517-0.0181 정도 낮게 나타났다. 즉, 특징 계수 2에 의하여 생성된 해쉬가 보다 강인함을 확인하였다. 메쉬 간단화는 모델의 꼭지점 개수 또는 메수 개수를 줄이는 것으로, 본 실험에서는 전체 꼭지점 개수의 80%-10%으로 줄였다. 특징 계수 1,2에 대한 메쉬 간단화 실험 결과는 그림 6 (c), (d)에서와 같으며, 이 그림으로부터 객체 수가 4일 때 가장 강인함을 알 수 있었다. 그리고 특징 계수 2가 특징 계수 1보다 정규화된 Hamming 거리가 약 0.0045-0.0336 정도 낮게 나타났으며, 이는 특징 계수 2에 의하여 생성된 해쉬가 보다 강인함을 보여준다. 다른 모델과 다른 공격에 대한 실험에서도 동일한 결과를 얻었다.

표 2. 미분 엔트로피량

모델명	제안한 방법		Swaminathan [10,11]
	타입1: $h(f_k^{(1)})$	타입2: $h(f_k^{(2)})$	
Africanas bust	0.6449	8.8994	6.20 (Lena, Peppers)
Armchair	0.5664	6.9896	
Bed	0.5931	8.7021	
Cake	0.5837	5.6222	
Sofa	0.5641	6.9384	
평균	0.5904	7.4303	

이상의 결과로부터 객체 수가 증가할수록 보안성은 향상되나 이와 반대로 강인성은 어느 객체 수까지는 증가되나 그 이상에서는 낮아짐을 확인하였다. 또한

특징 계수 1보다 특징 계수 2에 의하여 생성된 해쉬가 보안성 및 강인성이 보다 우수함을 확인하였다.

V. 결 론

본 논문에서는 미분 엔트로피 기반으로 3D 해싱에서 특징 계수의 보안성을 평가하는 모델링을 제안하였다. 제안한 방법에서는 Swaminathan 등이 제시한 영상 해싱의 미분 엔트로피 보안성 평가 모델링을 기반으로 3D 객체 모델 해싱에서 합과 곱의 형태를 지니는 해쉬 특징 계수들을 모델링하였다. 제안한 합과 곱 형태의 해쉬 특징 계수는 3D 객체 모델의 특징 객체 수 및 객체별 거리 분산과 랜덤 계수 키의 분산에 의하여 결정되며, 또한 두 형태의 확률밀도함수도 이들에 의하여 결정된다. 실험 결과로부터 합 형태의 특징 계수보다 곱 형태의 특징 계수에 의하여 생성된 해쉬의 보안성이 우수함을 확인하였다. 또한 선택된 객체 수가 증가할수록 보안성은 우수하나 이와 반대로 강인성은 만족하지 못함을 확인하였다. 따라서 3D 해싱에서는 모델의 특성에 따라 객체들을 선택한 후, 곱 형태의 특징 계수를 설계하여 이를 이진 해쉬로 생성하는 것이 보안성 및 강인성에서 우수한 결과를 가짐을 확인하였다.

참 고 문 헌

〔1〕 R. Ohbuchi, H. Masuda, and M. Aono, "Watermarking three-dimensional polygonal models through geometric and topological modification," *IEEE Journal on Selected Areas in Communications*, Vol.16, Issue4, pp.551-560, May 1998.

〔2〕 S.-H. Lee and K.-R. Kwon, "A watermarking for 3D-mesh using the patch CEGIs," *Digital Signal Processing*, Vol.17, Issue2, pp.396-413, March 2007.

〔3〕 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, 2008.

〔4〕 J.M. Konstantinides, A. Mademlis, P. Daras, P.A. Mitkas and M.G. Strintzis, "Blind robust 3-D mesh watermarking based on oblate spheroidal harmonics," *IEEE Transactions on Multimedia*, Vol.11, Issue1, pp.23-38, January 2009.

〔5〕 권성근, 이석환, 배성호, 박재범, 권기룡, "Buyer-Seller 워터마킹 프로토콜 기반의 모바일 3D 콘텐츠 워터마킹 기법," *한국통신학회논문지*, 제32권, 제8호, pp.788-799, 2007년 8월.

〔6〕 최기철, "RP 시스템 적용을 위한 3차원 메쉬 모델의 블라인드 워터마킹," *한국통신학회논문지*, 제32권 제12호, pp.1194-1202, 2007년 12월.

〔7〕 이석환, 권기룡, "헬스케어 정보 관리 시스템의 3D 의료영상 데이터 다중 워터마킹 기법, *한국통신학회논문지*, 제34권, 제11호, pp.870-881, 2009년 11월.

〔8〕 이석환, 권기룡, "키 기반 블록 표면 계수를 이용한 강인한 3D 모델 해싱," *대한전자공학회논문지*, 제47권 CI편 제1호, pp. 1-14, 2010년 1월.

〔9〕 S.-H. Lee, E.-J. Lee and K.-R. Kwon, "Robust 3D Mesh Hashing Based on Shape Features," *IEEE International Conference on Multimedia & Expo*, July 2010.

〔10〕 이석환, 권기룡, "객체별 특징 벡터 기반 3D 콘텐츠 모델 해싱," *대한전자공학회논문지*, 제47권 CI편 제6호, 2010년 11월.

〔11〕 A. Swaminathan, Y. Mao, and M. Wu, "Robust and secure image hashing," *IEEE Trans. on Information Forensics and Security*, Vol.1, Issue2, pp.215-230, June 2006.

〔12〕 A. Swaminathan, Y. Mao, and M. Wu, "Security of feature extraction in image hashing," *IEEE International Conference on Acoustic, Speech and Signal Processing*, Vol.2, pp.1041-1044, March 2005.

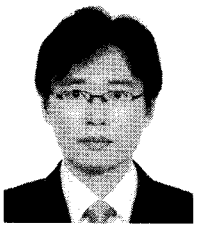
〔13〕 A. papoulis and S.U.Pillai, Probability, *Random Variables and Stochastic Processes*, New York:McGraw-Hill, 2002.

〔14〕 Normal Product Distribution, http://mathworld.wolfram.com/NormalProductDistribution.html

〔15〕 Modified Bessel Function of the Second Kind, http://mathworld.wolfram.com/ModifiedBesselFunctionoftheSecondKind.html

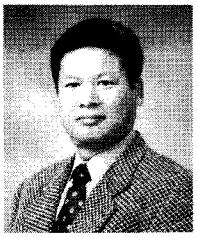
〔16〕 ARCHIBASE NET, http://www.archibase.net

이 석 환 (Suk-Hwan Lee) 정회원



1999년 2월 경북대학교 전자공학과 공학사
2001년 2월 경북대학교 전자공학과 공학석사
2004년 8월 경북대학교 전자공학과 공학박사
2005년 3월~현재 동명대학교 정보보호학과 조교수
<관심분야> 워터마킹, DRM, 영상신호처리

권 기 룡 (Ki-Ryong Kwon) 정회원



1986년 2월 경북대학교 전자공학과 공학사
1990년 2월 경북대학교 전자공학과 공학석사
1994년 8월 경북대학교 전자공학과 공학박사
2000년 7월~2001년 8월 Univ. of Minnesota, Post-Doc.
1996년 3월~2006년 2월 부산외국어대학교 컴퓨터전자공학부 부교수
2006년 3월~현재 부경대학교 전자컴퓨터정보통신공학부 교수
<관심분야> 멀티미디어 정보보호, 멀티미디어 통신 및 신호처리