

익명 Buyer-Seller 워터마킹 프로토콜 기반 모바일 3D 콘텐츠의 기하학적 다중 워터마킹 기법

이석환^{*}, 권성근^{**}, 권기룡^{***}

요 약

본 논문에서는 모바일 3D 콘텐츠들의 저작권 보호 및 불법복제 방지를 위한 다중 워터마킹 기법을 제안한다. 제안한 방법에서는 익명 Buyer-Seller 워터마킹 프로토콜 기반으로 모바일 3D 콘텐츠의 공간 영역 및 암호화 영역 상에서 단일 워터마크 및 WCA 워터마크를 삽입한다. 우선, 판매자는 단일 워터마크를 생성하여, 이를 3D 콘텐츠 객체의 꼭지점 데이터 본포 상에 삽입한다. 그리고 WCA에서 전달받은 암호화된 워터마크를 암호화된 꼭지점 데이터에 준동형 특성을 이용한 연산자에 의하여 삽입한다. 본 실험에서는 모바일 콘텐츠 개발툴인 PowerVR MBX 상에서 제안한 방법을 구현하였다. 실험 결과로부터 제안한 방법이 모바일 3D 콘텐츠의 저작권 보호 및 불법 복제 방지가 가능함을 확인하였으며, 잡음첨가, 데이터 정밀도 가변, 확대, 축소 등의 공격에 대하여 워터마크가 검출됨을 확인하였다.

Geometric Multiple Watermarking Scheme for Mobile 3D Content Based on Anonymous Buyer-Seller Watermarking Protocol

Suk-Hwan Lee^{*}, Seong-Geun Kwon^{**}, Ki-Ryong Kwon^{***}

ABSTRACT

This paper presents multiple watermarking method for the copyright protection and the prevention of illegal copying of mobile 3D contents. The proposed method embeds an unique watermark and a WCA watermark into the spatial and encryption domains of mobile 3D content based on anonymous Buyer-Seller watermarking protocol. The seller generates an unique watermark and embeds it into the distribution of vertex data of 3D content object. After receiving the encrypted watermark from WCA, the seller embeds it into the encrypted vertex data by using operator that satisfies the privacy homomorphic property. The proposed method was implemented using a mobile content tool, PowerVR MBX and experimental results verified that the proposed method was capable of copyright protection and preventing illegal copying, as the watermarks were also accurately extracted in the case of geometrical attacks, such as noise addition, data accuracy variation, and data up/down scaling.

Key words: Mobile 3D Contents(모바일 3D 콘텐츠), Digital Watermarking(디지털 워터마킹), Anonymous Buyer-Seller watermarking protocol(익명 Buyer-Seller 워터마킹 프로토콜)

* 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: 2008년 6월 30일, 완료일: 2008년 11월 24일

^{*} 정회원, 동명대학교 정보보호학과 조교수
(E-mail: skyllee@tu.ac.kr)

^{**} 정회원, 삼성전자 무선사업부
(E-mail: seonggeunkwon@hanmail.net)

^{***} 종신회원, 부경대학교 전자컴퓨터정보통신공학부 교수
※ 본 논문은 2007년 정부(교육인적자원부)의 재원으로 한국과학기술진흥재단의 지원을 받아 수행된 연구임(KRF-2007-331-D00320)

1. 서 론

최근 국내의 이동통신사들은 새로운 킬러 콘텐츠로 주목받고 있는 모바일 3D 게임을 제작 및 서비스하고 있으며, 이를 위하여 일반 모바일 폰보다 게임 및 그래픽스 성능이 향상된 폰을 출시하고 있다. 모바일 3D 게임은 크게 임베디드 방식, WAP (Wireless application protocol) 방식, 다운로드형 및 네트워크형 VM (Virtual Machine) 방식으로 나누어지며, 다양한 모바일 플랫폼 기반으로 많이 제작되어지고 있다[1-6]. 특히 모바일 3D 게임의 용량이 증가할수록 데이터 통신비에 대한 사용자 부담을 줄이기 위하여 PC 다운로드 S/W를 통한 다운로드 방법이 제공되면서 불법 복제 우려에 대한 관심이 높아지고 있다. 현재 불법 복제 방지와 관련하여 GVM/GNEX 인증 모듈이 적용되고 있으나[6], 모바일 3D 콘텐츠에 대한 저작권 보호 기술 및 워터마킹 기술을 적용함으로써 보안 수준을 높일 수 있다. 3D 콘텐츠 산업의 발달과 더불어 3D 콘텐츠들의 저작권 보호 및 불법 복제 추적을 위한 3D 워터마킹 기술이 필요함에 따라 3D 그래픽 모델, 3D CAD 데이터 및 3D 애니메이션 데이터에 대한 워터마킹 기술이 제안되어지고 있다. 3D 그래픽 모델에 대한 워터마킹 기법에서는 다각형 형태의 메쉬(mesh) 모델을 구성하는 꼭지점 좌표 및 꼭지점들의 연결정보에 워터마크를 삽입한다[7-11]. 그러나 이들 방법들은 정지된 그래픽 모델에 적용된 워터마킹 기법이며, 또한 각 모델의 정보들은 고정된 실수값들로 모바일 상에서 서비스되는 3D 게임 콘텐츠에는 적용되지 못한다.

현재 디지털 워터마킹 기법과 함께 전자상거래 상에서 구매자와 판매자 모두가 신뢰할 수 있는 계약절차를 제공하는 암호학적 프로토콜도 함께 연구되었는데 그중의 하나가 바로 워터마킹 프로토콜이다. 워터마킹 프로토콜은 암호학적 시스템과 워터마킹 기법을 결합하여 불법적으로 유통되는 디지털 콘텐츠의 적발시, 부정자 추적을 통해 불법 배포의 책임소재를 가려내는 것이다[12,13]. Kwon 등은 Memon [12]이 제시한 프로토콜 상에서의 모바일 3D 게임 콘텐츠 워터마킹 기법을 제안하였다[14,15]. 그러나 이 프로토콜은 구매자의 익명성이 보장되지 않으며, 비결합 문제를 가지고 있다. 또한 이 기법에서는 특정 개발물 상의 3D 객체 데이터 및 움직임 데이터

정보 내에 워터마크를 삽입하므로, 3D 객체의 원형 정보인 꼭지점 좌표의 기하학적 특성을 고려하지 않는다. 그리고 데이터 순서가 변하는 공격 및 데이터 삭제 등에 대하여 견고하지 못하며, 워터마크 추출시 워터마크 삽입 대상체의 인덱스 정보가 필요한 단점이 있다. Lei 등은 고객 권리 문제 (customer's right problem)와 비결합 문제 (unbinding problem)를 해결하기 위하여 PKI (Public-Key Infrastructure) 기반의 익명 Buyer-Seller 워터마킹 프로토콜을 제안하였다[13]. 고객 권리 문제는 악의적인 판매자가 임의의 구매자를 포함하기 위하여 저작권 침해를 위조하는 것이다. 비결합 문제는 선택된 하나의 워터마크가 특정 거래 또는 콘텐츠와 결합되지 못하는 것이다. 즉, 판매자가 저작권 침해를 위조하기 위하여 복제된 콘텐츠에 삽입되어 있는 워터마크를 다른 콘텐츠에 삽입이 가능하다는 것이다.

본 논문에서는 모바일 3D 콘텐츠의 저작권 보호 및 불법 복제 방지를 위하여 Lei등이 제안한 익명 Buyer-Seller 워터마킹 프로토콜 상에서 공간 영역 및 암호화 영역 상에서 다중 워터마크를 삽입하는 방법을 제안한다. 제안한 방법에서는 모바일 3D 콘텐츠를 구성하는 메쉬 객체들의 꼭지점 데이터 내에 다중 워터마크를 공간 영역 및 암호화 영역 상에서 삽입한다. 워터마크 삽입 방법에서는 판매자가 저작권 정보를 나타내는 단일 워터마크를 임의로 선택된 객체 내의 꼭지점 데이터 분포에 삽입한다. 단일 워터마크가 삽입된 객체들을 암호화한 후, 인증기관이 암호화한 워터마크를 암호화 영역 내에 선행 결합하여 다중 워터마크 및 암호화된 콘텐츠를 구매자에게 전달한다. 구매자는 이를 복호화하여 다중 워터마크된 콘텐츠를 얻은 후, 모바일 3D 콘텐츠를 실행한다. 본 실험에서는 모바일 3D 콘텐츠 도구인 PowerVR MBX[16]를 이용하여 제안한 방법의 알고리즘을 구현하였다. 실험 결과로부터 모바일 3D 콘텐츠의 저작권 보호와 불법 복제 방지가 가능함을 확인하였으며, 다중 워터마크된 콘텐츠의 SNR비가 각각 36.37-40.76dB 및 68.86-73.75dB이고, 잡음첨가, 데이터 정밀도 가변, 확대 및 축소 등에 대하여 견고함을 확인하였다.

본 논문의 구성은 다음과 같다. 우선 2장 및 3장에서는 모바일 3D 엔진 및 Buyer-Seller 워터마킹 프로토콜에 대하여 간략히 살펴본 후, 4장에서는 익명

Buyer-Seller 워터마킹 프로토콜 상에서 모바일 3D 콘텐츠 내에 다중 워터마크를 삽입하는 방법에 대하여 살펴본다. 그리고 5장에서는 구현 실험 결과를 보며, 마지막 6장에서는 본 논문의 결론을 맺는다.

2. 모바일 3D 콘텐츠

모바일 3D 게임 콘텐츠 워터마킹에서는 모바일 게임 엔진 내에 콘텐츠 데이터 구조 및 게임 로직에 따라 다양하게 제안되어질 수 있다. 따라서 본 장에서는 모바일 3D 게임 엔진 구조 및 3D 콘텐츠의 구조에 대하여 간략히 살펴본 다음, 모바일 콘텐츠의 워터마킹 기술에 대하여 언급한다.

2.1 모바일 3D 게임 엔진

모바일 3D 게임 엔진은 모바일폰과 같은 저사양 기기에서 3D 콘텐츠를 렌더링 및 애니메이션 할 수 있도록 해주는 것으로 국내외적으로 많이 개발되어지고 있다[1-6]. 일반적인 모바일 3D 게임 엔진 구조는 그림 1에서와 같다. 우선 모바일 3D 게임의 1D, 2D 및 3D 콘텐츠들은 범용 편집 툴에 의하여 콘텐츠 설계자의 기호에 따라 생성된다. 이들 콘텐츠 데이터들은 리소스 편집기에 의하여 모바일 환경에 맞게 데이터 변환이 된다. 예를 들어, 2D 영상에서는 RGB 16비트 표현 (565 또는 444)으로 변환되고, 3D 모델에서는 부동소수점이 고정소수점 표현으로 변환된

다. 대부분의 모바일 기기의 CPU는 소수점 연산을 위하여 비교적 연산량이 적은 고정소수점 연산을 사용한다. 모바일 게임 설계자들은 변환된 콘텐츠 데이터들을 로딩하여 게임 로직에 맞게 설계 및 프로그래밍하여 최종 타겟인 모바일 기기에 탑재하게 된다.

이상과 같은 모바일 3D 게임 엔진 상에서 워터마크는 세 가지 경우의 콘텐츠 데이터에 삽입이 될 수 있다. 첫 번째로는 범용 편집 툴에서 생성된 1D, 2D 및 3D 콘텐츠 데이터 내에 워터마크를 삽입하는 것으로 최근까지 연구되어진 오디오, 영상, 비디오, 3D 모델 워터마킹 기술들은 대부분 여기에 속한다. 그러나 모바일 리소스 편집기의 데이터 변환에 의하여 워터마크 손실이 많이 발생한다. 그리고 대부분 엔진 개발툴(SDK)에서는 변환된 데이터들을 범용 편집 툴 포맷으로의 역변환 기능을 제공하지 않으므로 워터마크 추출이 어렵다. 두 번째로는 모바일 리소스 편집기에 의하여 변환된 모바일 콘텐츠 데이터 내에 워터마크를 삽입하는 것이다. 이 경우에서는 모바일 리소스 편집기 내에 워터마크 삽입이 이루어지며, 워터마크된 콘텐츠 데이터들을 이용하여 여러 가지 모바일 게임을 제작할 수 있다. 세 번째로는 게임 설계 시 모바일 콘텐츠 데이터 로딩시 워터마크를 삽입하는 것으로, 이는 모바일 게임 DRM 기술과 연계하여 제안되어질 수 있다. 두 번째와 세 번째 경우에는 고정소수점 형태의 모바일 데이터 포맷을 고려하여야 하며, 오디오, 영상, 비디오 및 3D 모델 데이터 내에 워터마크를 삽입할 수 있다. 본 논문에서는 특정 모바일 게임의 저작권 보호를 위하여 게임 설계시 로딩된 모바일 3D 콘텐츠 데이터 내에 워터마크를 삽입하는 알고리즘을 제안한다.

2.2 모바일 3D 콘텐츠

일반적인 모바일 3D 콘텐츠 데이터의 구조를 그림 2에서와 같이 살펴보면, 각 오브젝트 단위의 3D Scene으로 구성되어 있다. 여기서 Scene 노드를 여러 개로 묶은 것을 Group이라 하며, 전체 Scene을 포함하고 있는 Super Group을 World라 한다. 즉, World는 3D 오브젝트 계층구조의 최상위 그룹으로 활성화된 카메라와 배경정보를 저장하고 있다. Mesh는 기본적인 형상 오브젝트로 꼭지점 버퍼(vertex buffer), 인덱스 버퍼(index buffer) 및 형상 정보(appearance)를 가진다. 꼭지점 버퍼에는 꼭지

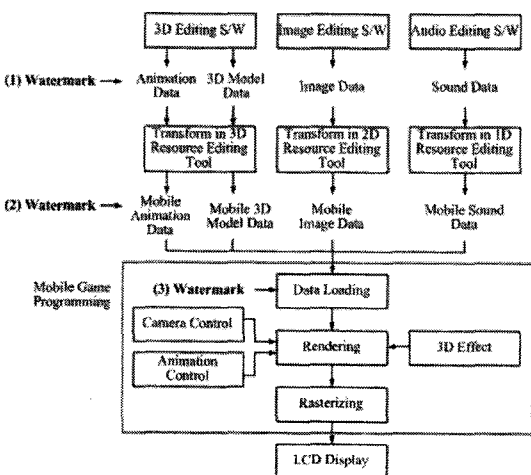


그림 1. 일반적인 모바일 3D 게임 엔진 구조 및 워터마크 삽입 가능 대상체

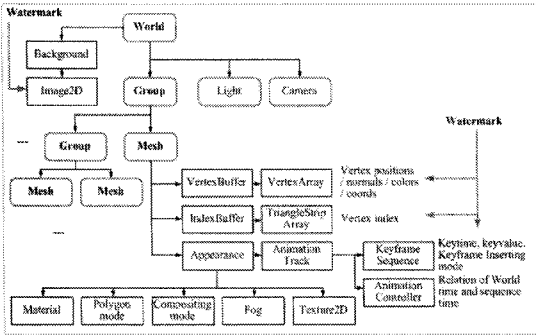


그림 2. 일반적인 모바일 3D 콘텐츠 데이터 구조 (3)

점의 좌표, 법선 및 색상에 대한 배열 정보가 있으며, 인덱스 버퍼에는 삼각형 스트립 (triangle strip)을 나타내기 위한 꼭지점들의 인덱스 정보가 있다. 그리고 형상 정보에는 키프레임 시퀀스 및 애니메이션 조정기로 구성된 애니메이션 트랙과 표면정보를 나타내는 재질 (material) 정보, 폴리곤 모드, 텍스처 등이 있다. 워터마크 삽입 대상체로는 꼭지점 버퍼 내의 꼭지점 좌표값, 인덱스 버퍼 내의 삼각형 스트립 배열, 애니메이션 트랙의 키프레임 시퀀스 내에 키타임과 키값들로 선택될 수 있다. 또한 3D 오브젝트 렌더링 시에 정의되는 배경 이미지 (Background image)도 삽입 대상체로 선택될 수 있다. 그 이외의 형상 정보 (Appearance) 내의 값들은 외부 환경 요소에 따라 쉽게 변하므로 워터마크 삽입 대상체로 적절하

지 못하다. 제안한 방법에서는 공간 영역 및 암호화 영역 상에서 다중 워터마크를 꼭지점 좌표값 및 삼각형 스트립 배열 내에 삽입한다.

3. 익명 Buyer-Seller 워터마킹 프로토콜

Lei의 익명 Buyer-Seller 워터마킹 프로토콜은 등록 프로토콜(registration protocol), 워터마크 삽입 프로토콜, 식별 및 중재 프로토콜(identification and arbitration protocol)로 구성된다[13]. 본 논문에서는 모바일 3D 콘텐츠의 저작권 보호를 위하여 Lei 등이 제안한 익명 Buyer-Seller 워터마킹 프로토콜 기반의 다중 워터마크 삽입 방법을 제안한다. 본 장에서는 익명 Buyer-Seller 워터마킹 프로토콜 및 이 프로토콜 기반에서 모바일 3D 콘텐츠의 다중 워터마크 삽입 방법에 대하여 간략히 살펴보기로 한다.

등록 프로토콜에서는 구매자에게 익명 인증서를 발행한다. 우선 구매자는 임의의 키 (pk_B, sk_B)을 선택하여, 공개키 pk_B 를 인증기관 CA(Certification Authority)에 전달한다. CA는 익명 인증서 ($Cert_{CA}(pk_B)$)를 생성하여, 이를 구매자에게 전달한다. 여기서 CA는 $Cert_{CA}(pk_B)$ 와 구매자의 정보를 결합(binding)하며, 중재인 ARB(Arbitrer)에 의하여 요구되지 않는 한, 이 결합 정보가 공개되지 않음을 보증한다. 워터마크 삽입 프로토콜은 그림 3에서와 같



그림 3. 익명 Buyer-Seller 워터마킹 프로토콜 상에서 구매자, 판매자 및 WCA와의 상호 관계

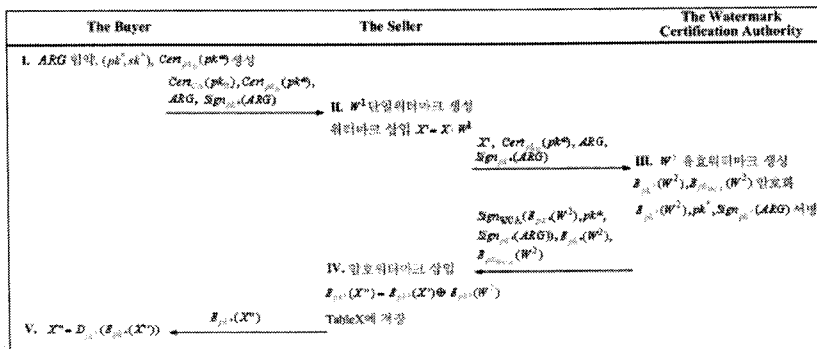


그림 4. 익명 Buyer-Seller 워터마킹 프로토콜 상에서의 워터마크 삽입 프로토콜의 세부 절차

이 구매자, 판매자 및 워터마크 인증기관 WCA (Watermark Certification Authority)간에 이루어진다. 세부적인 절차는 그림 4에서와 같다. 그림 4에서의 구매 테이블 Tablex는 각 거래 상에서 발생한 위의 정보들을 저장하고 있다. 이때 각 정보 상에서의 단일 워터마크 V 는 불법 복제된 콘텐츠 발생시 Tablex 내의 정보 위치를 탐색하기 위한 검색키로 사용되어진다.

식별 및 중재 프로토콜은 판매자, ARB 및 WCA로 구성된다. 불법 복제된 콘텐츠 Y 가 발생되었을 때, 판매자는 Y 내에 단일 워터마크 W^1 를 검출한 후, Tablex 내의 각 W_k^1 와 W^1 의 유사도를 계산하여 최대 유사도를 가지는 W_k^1 를 선택한다. 그런 다음, 판매자는 Y 와 W_k^1 에 연계된 정보 $Cert_{CA}(pk_B)$, $Cert_{pk_B}(pk^*)$, ARG , $Sign_{pk^*}(ARG)$, $E_{pk^*}(W^2)$, $E_{pk_{WCA}}(W^2)$, $Sign_{WCA}(E_{pk^*}(W_k^2), pk^*, Sign_{pk^*}(ARG_k))$ 를 ARB에 전달한다. ARB은 인증서 및 서명을 확인한 다음, WCA에게 $E_{pk_{WCA}}(W^2)$ 을 복호하도록 요청하여 W^2 를 얻는다. 그리고 공개키 pk^* 에 의해 W^2 를 암호화하여 판매자에게 전달받은 $E_{pk^*}(W^2)$ 와 정확도 비교를 확인한 후, Y 내에 워터마크 W^2 를 검출한다. 이를 통하여 ARB는 구매자의 불법 복제 유무를 판정한다. 이상의 이명 Buyer-Seller 워터마킹 프로토콜을 살펴보면, 판매자는 단일 워터마크 W^1 를 콘텐츠 X 내에 삽입하고, WCA에서 전달받은 암호화된 워터마크 $E_{pk_{WCA}}(W^2)$ 를 암호화 영역에서 삽입하여 이를 구매자에게 전달한다. 여기서 단일 워터마크 W^1 의 삽입 방법은 콘텐츠의 종류, 공격 유무 등에 따라 결정되고, 암호화 영역에서의 $E_{pk^*}(W^2)$ 삽입 방법은 암호 연산자 성질에 따라 결정된다.

4. 제안한 모바일 3D 콘텐츠 워터마킹

본 논문에서는 모바일 3D 콘텐츠의 저작권 보호를 위하여 3D 콘텐츠 내의 공간 영역 및 암호화 영역 상에서 다중 워터마크를 삽입하는 방법을 제안한다. III 장에서 설명하였듯이, 모바일 3D 콘텐츠 X 의 매쉬 객체 O 내에 꼭지점 좌표값 V 을 워터마크 삽입 대상체로 선택되어진다. 따라서 제안한 방법에서는 그림 5에서와 같이 판매자 측에서 랜덤 가우시안 비트열로 구성된 단일 워터마크 W^1 를 생성한 후, 각

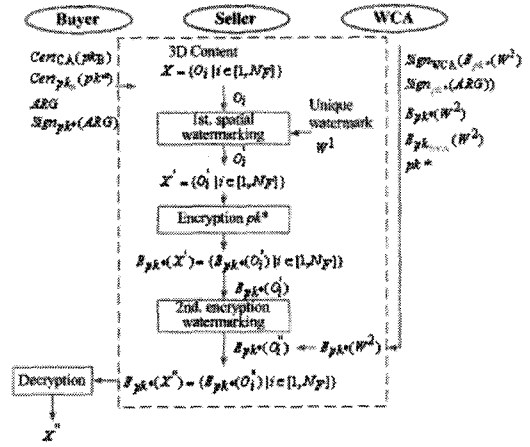


그림 5. 제안한 모바일 3D 콘텐츠 다중 워터마킹 알고리즘

오브젝트의 꼭지점 좌표에 삽입하여 1차 워터마크된 콘텐츠 X' 를 얻는다. 그리고 X' 를 암호화한 다음, 비공개 준동형 특성을 만족하는 연산자를 통하여 $E_{pk^*}(W^2)$ 을 암호화된 객체 $E_{pk^*}(O'_i)$ 내의 꼭지점 좌표 값에 삽입함으로써 최종 암호화된 워터마크 콘텐츠 $E_{pk^*}(X'')$ 을 얻는다. 구매자는 판매자로부터 $E_{pk^*}(X'')$ 을 전달받은 다음, pk^* 에 의하여 복호하여 다중 워터마크된 X'' 을 획득한다.

4.1 공간영역 상에서의 1차 워터마크 삽입

제안한 공간영역 상에서의 워터마킹에서는 기하학적 공격 및 연결정보 공격에 강인하게 워터마크를 객체에 삽입한다. 즉, 스케일링, 회전, 이동 및 연결성 정보 공격에 강인하기 위하여 그림 6 (a)에서와 같이 각 객체의 꼭지점 좌표를 정규화한 다음, 중점 벡터와 꼭지점 벡터와의 사이각 분포에 따라 워터마크 삽입 대상을 선택한다. 그리고 선택된 분포 내에 속하는 꼭지점 데이터의 거리에 워터마크를 삽입한다.

1) 꼭지점 좌표 정규화

임의의 객체 O_i 내의 꼭지점 데이터 $V_i = \{v_k | k \in [1, N_i]\}$ 좌표들은 객체 중점 좌표 c_i 과 각 꼭지점와의 평균 거리 $\bar{r}_i = \sum_{k=1}^{N_i} \|c_i v_k\| / N_i$ 가 1이 되도록

$$\bar{r}_i = \sum_{k=1}^{N_i} \|c_i \hat{v}_k\| / N_i = \sum_{k=1}^{N_i} \|c_i v_k\| / (\bar{r}_i N_i) = 1 \quad (1)$$

와 같이 정규화한다. 식 (1)를 만족하기 위하여 정규화된 꼭지점 좌표 \hat{v}_k 는

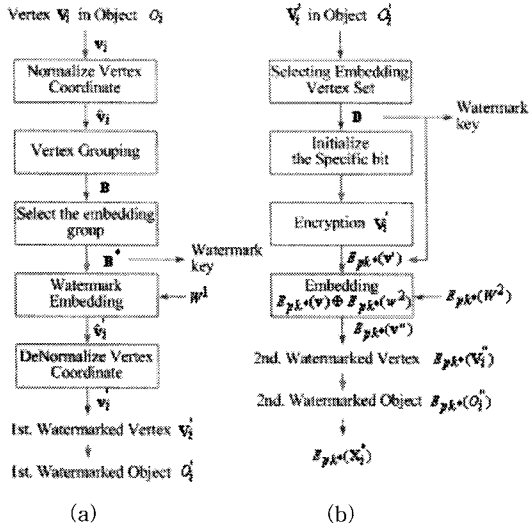


그림 6. 제안한 (a) 공간영역 및 (b) 암호화영역 상에서의 워터마크 삽입 방법

$$\|\vec{c}_i \hat{\mathbf{v}}_k\| = \|\vec{c}_i \mathbf{v}_k\| / \bar{r}_i \quad (2)$$

$$\begin{aligned} & (\hat{x}_k - cx_i)^2 + (\hat{y}_k - cy_i)^2 + (\hat{z}_k - cz_i)^2 \\ & = ((x_k - cx_i)^2 + (y_k - cy_i)^2 + (z_k - cz_i)^2) / \bar{r}_i^2 \end{aligned} \quad (3)$$

를 만족하여야 한다. 이를 간단히 풀기 위하여 제안한 방법에서는 다음과 같이 결정하였다.

$$\hat{\mathbf{v}}_k - \mathbf{c}_i = (\mathbf{v}_k - \mathbf{c}_i) / \bar{r}_i \quad (4)$$

이를 풀면 정규화된 꼭지점 좌표는

$$\hat{\mathbf{v}}_k = \mathbf{v}_k / \bar{r}_i + (1 - 1/\bar{r}_i) \mathbf{c}_i \quad (5)$$

와 같으며 이는 그림 7 (a)에서와 같다. 워터마크 삽입 과정을 수행한 후, 다음과 같이 역 정규화가정을 수행함으로써

$$\mathbf{v}'_k = \bar{r}_i \hat{\mathbf{v}}_k - (\bar{r}_i - 1) \mathbf{c}_i \quad (6)$$

워터마크가 삽입된 객체를 얻는다.

2) 워터마크 비트 삽입 위치 결정

워터마크 삽입 대상체는 꼭지점 순서 정렬, 메쉬 연결성 정보 치환, 절단 등에 강인한 속성을 가져야 한다. 제안한 방법에서는 각 꼭지점과 객체 중점와의 사이각 분포를 이용하여 워터마크 삽입 위치 영역을 선택한 다음, 선택된 영역 내에 속하는 꼭지점들의 거리 분포에 워터마크를 삽입한다. 우선 그림 7 (a)에

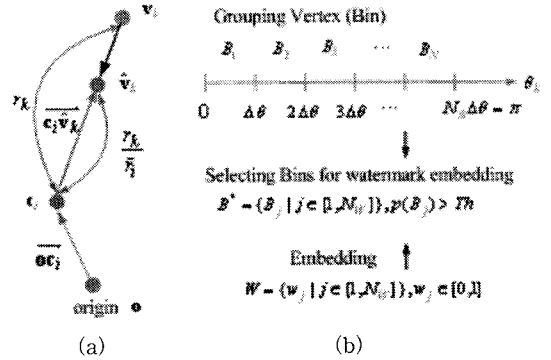


그림 7. (a) 꼭지점 좌표 \mathbf{v}_i 의 정규화 및 (b) 중점 좌표와 꼭지점 좌표와의 사이각 분포에 따른 워터마크 삽입 구간

서와 같이 기준 벡터 \vec{oc}_i 와 중점에 대한 정규화된 꼭지점 벡터 $\vec{c}_i \hat{\mathbf{v}}_k$ 와의 사이각 θ_k

$$\theta_k = \cos^{-1} \left(\frac{\vec{oc}_i \cdot \vec{c}_i \hat{\mathbf{v}}_k}{\|\vec{oc}_i\| \|\vec{c}_i \hat{\mathbf{v}}_k\|} \right), \quad 0 \leq \theta_k \leq \pi \quad (7)$$

를 구한 다음, θ_k 를 구간 $\Delta\theta = \pi/N_B$ 에 따라 N_B 개의 영역으로 구분한다. 그리고 각 꼭지점들 $\hat{\mathbf{v}}_{k \in [1, N]}$ 을 θ_k 가 속해 있는 영역별로 그룹화한다. 즉, N_B 개 그룹 B는

$$\begin{aligned} B &= \{B_l | l \in [1, N_B]\}, \\ B_l &= \{\hat{\mathbf{v}}_k | \theta_k \in [(l-1)\Delta\theta, l\Delta\theta], k \in [1, N_B]\} \end{aligned} \quad (8)$$

으로, 각 그룹 B_l 은 사이각이 $\theta_k \in [(l-1)\Delta\theta, l\Delta\theta]$ 을 만족하는 꼭지점들로 구성된다. 여기서 N_{B_l} 은 그룹 B_l 에 속한 꼭지점들의 개수이다. $\Delta\theta$ 는 영역을 구분하는 변수로 워터마크의 강인성 및 비가시성에 따라 몇 가지 고려하여 $\Delta\theta$ 를 결정하여야 한다. 첫 번째 사항으로는 비가시성을 고려하기 위하여 $\Delta\theta$ 는 워터마크에 의한 꼭지점 $\hat{\mathbf{v}}$ 의 허용 최대 변이보다 커야 한다. 두 번째 사항으로는 영역의 개수 N_B 가 워터마크 비트수 N_W 보다 커야 한다. 이는 워터마크 삽입 용량뿐만 아니라 꼭지점 개수가 많은 영역을 워터마크 삽입 위치를 선택하기 위한 것이다. 세 번째 사항으로는 객체의 꼭지점 개수를 고려하여야 한다. 모바일 3D 객체는 일반 3D 그래픽스 모델에 비하여 꼭지점 개수가 작으므로 많은 수의 워터마크를 삽입하지는 못한다. 제안한 방법에서는 세 가지 사항을 고려하여 $\Delta\theta$ 를 실험적으로 결정하였다.

위터마크 삽입 대상 영역은 영역 B_i 에 속하는 꼭지점들의 확률밀도 $p(B_i)$

$$p(B_i) = \frac{N_{B_i}}{N_i} > Th \quad (9)$$

가 문턱치 Th 보다 큰 영역 중 위터마크 삽입 비트 수만큼 선택된다.

3) 위터마크 비트 삽입

제안한 방법에서는 위터마크 $\mathbf{W}^i = \{w_j^i | j \in [1, N_{W^i}]\}$, $w_j^i \in [0, 1]$ 의 각 비트를 선택된 영역 $\mathbf{B}^i = \{B_j | p(B_j) > Th, j \in [1, N_{W^i}]\}$ 내에 순차적으로 삽입한다. 즉, 선택된 영역 $B_j = \{\hat{v}_{j,k} | \theta_{j,k} \in [(l-1)\Delta\theta, l\Delta\theta], k \in [1, N_{B_j}]\}$ 내에 속하는 모든 정규화된 꼭지점들의 객체 중점와의 거리 $\hat{r}_{j,k} = \|c_i \hat{v}_{j,k}\|$ 를 구한 후, 이를 임의의 인자 Δr 로 양자화된 거리값 $q_{j,k} = INT(\hat{r}_{j,k}/\Delta r + 0.5)$ 에 임의의 위터마크 비트 w_j^i 가 다음과 같이 삽입된다.

$$q'_{j,k} = \begin{cases} \lfloor q_{j,k} \rfloor + w_j^i, & \text{if } \lfloor q_{j,k} \rfloor \% 2 == 0 \\ \lfloor q_{j,k} \rfloor + 1 - w_j^i, & \text{if } \lfloor q_{j,k} \rfloor \% 2 == 1 \end{cases} \quad (10)$$

위 식을 살펴보면, 위터마크 비트 w_j^i 가 0이면 양자화된 거리값 $q_{j,k}$ 는 짝수로, w_j^i 가 1이면 $q_{j,k}$ 를 홀수로 변경된다. 따라서 삽입된 거리 $\hat{r}'_{j,k}$ 는 $\hat{r}'_{j,k} = q'_{j,k} \Delta r$ 이 되므로, 정규화된 꼭지점 좌표 $\hat{v}'_{j,k} = (\hat{x}'_{j,k}, \hat{y}'_{j,k}, \hat{z}'_{j,k})$ 는 $\hat{r}'_{j,k} = q'_{j,k} \Delta r$ 이 되도록 결정되어져 한다. 제안한 방법에서는 계산상의 용이를 위하여 아래와 같이 두고

$$\mathbf{X}'_{j,k} = \hat{v}'_{j,k} - c_i = \alpha_{j,k} \mathbf{X}_{j,k} = \alpha_{j,k} (\mathbf{v}_{j,k} - c_i) \quad (11)$$

$\hat{r}'_{j,k} = q'_{j,k} \Delta r$ 를 풀면 다음과 같다.

$$\begin{aligned} \hat{r}'_{j,k} &= q'_{j,k} \Delta r \\ &= \|\hat{v}'_{j,k} - c_i\| = \|\mathbf{X}'_{j,k}\| = \alpha_{j,k} \|\mathbf{X}_{j,k}\| = \alpha_{j,k} \hat{r}_{j,k} \end{aligned} \quad (12)$$

따라서 $\alpha_{j,k} = q'_{j,k} \Delta r / \hat{r}_{j,k}$ 이므로, 위터마크가 삽입된 정규화된 꼭지점 좌표는

$$\hat{v}'_{j,k} = \frac{q'_{j,k} \Delta r}{\hat{r}_{j,k}} \hat{v}_{j,k} + (1 - \frac{q'_{j,k} \Delta r}{\hat{r}_{j,k}}) c_i \quad (13)$$

와 같다. 최종 위터마크된 꼭지점 좌표 $\mathbf{v}'_{j,k} = (x'_{j,k}, y'_{j,k}, z'_{j,k})$ 는 역 정규화함으로써 다음과 같이 계산되어진다.

$$\begin{aligned} \mathbf{v}'_{j,k} &= \frac{q'_{j,k} \Delta r}{\hat{r}_{j,k}} r_i \hat{v}_{j,k} + (1 - \frac{q'_{j,k} \Delta r}{\hat{r}_{j,k}}) r_i c_i - (r_i - 1) c_i \\ &= \frac{q'_{j,k} \Delta r}{\hat{r}_{j,k}} r_i \hat{v}_{j,k} + (1 - \frac{q'_{j,k} \Delta r}{\hat{r}_{j,k}}) r_i c_i \end{aligned} \quad (14)$$

이상의 공간 영역 위터마크 삽입 방법에서는 1차 위터마크가 삽입된 객체 $\mathbf{O}'_i = \{\mathbf{V}'_i, \mathbf{U}_i, \mathbf{N}_i, \mathbf{F}_i\}$ 를 포함하는 모바일 3D 콘텐츠 $\mathbf{X}' = \{\mathbf{O}'_i, \mathbf{O}_k | i, k \in [1, N_F], i \neq k\}$ 를 얻는다.

4.2 암호화 영역 상에서의 위터마크 삽입

WCA에서 전달받은 암호화된 2차 위터마크 $E_{pk^*}(\mathbf{W}^2) = \{E_{pk^*}(w_j^2) | j \in [1, N_{W^2}]\}$ 는 암호화 영역 상에서 준동형 특성을 만족하는 연산자 \oplus 에 의하여 삽입되어야 한다. 암호화 영역 상에서 위터마크 삽입 연산자 \oplus 는 준동형 특성을 만족하여야 하며, 원본이 필요없는 블라인드 특성을 가져야 한다. 따라서 제안한 방법에서는 그림 6 (b)에서와 같이 암호화 영역 상에서 합과 곱으로 이루어진 비트 치환 방법에 의하여 2차 위터마크를 삽입한다.

먼저 2차 위터마크 삽입 대상인 꼭지점 데이터들을 임의의 객체 \mathbf{O}'_i 내에서 위터마크 길이 N_{w^2} 의 m 배 만큼 선택한다. 즉, 임의의 꼭지점 데이터 인덱스를 m 개 선택하여 이를 $I = \{I_k | k \in [1, m]\}$ 로 저장한다. 이때 각 인덱스간의 거리는 $|I_{k_1} - I_{k_2}| > N_{w^2}$ 이어야 한다. 2차 위터마크 삽입 대상 꼭지점 데이터 집합 \mathbf{D} 은

$$\begin{aligned} \mathbf{D} &= \{D_k | k \in [1, m]\}, \\ D_k &= \{\mathbf{v}'_j = (x'_j, y'_j, z'_j) | j \in [I_k, I_k + N_{w^2}]\} \end{aligned} \quad (15)$$

와 같이 선택된 인덱스 I_k 를 기준으로 N_{w^2} 개 만큼 꼭지점 데이터 원소들을 가지는 집합 D_k ($k \in [1, m]$)들로 구성된다. N_{w^2} 길이의 2차 위터마크는 m 번 반복하여 집합 \mathbf{D} 에 삽입된다. 여기서 꼭지점 데이터들은 32비트의 고정소수점들로 표현된다. 꼭지점 데이터 집합 D_k 내의 모든 데이터들은 소수점 영역의 임의의 t 번째를 0으로 초기화된다. 그런 다음 1차 위터마크가 삽입된 콘텐츠 $\mathbf{X}' = \{\mathbf{O}'_i, \mathbf{O}_k | i, k \in [1, N_F], i \neq k\}$ 를 pk^* 에 의하여 암호화된 콘텐츠 $E_{pk^*}(\mathbf{X}') = \{E_{pk^*}(\mathbf{O}'_i) | i \in [1, N_F]\}$ 가 생성된다.

제안한 방법에서는 암호화된 2차 위터마크 $E_{pk^*}(\mathbf{W}^2) = \{E_{pk^*}(w_j^2) | j \in [1, N_{W^2}]\}$ 를 암호화된 객체

$E_{pk^*}(\mathbf{O}_i)$ 의 데이터 집합 $E_{pk^*}(\mathbf{D})$

$$E_{pk^*}(\mathbf{D}) = \{E_{pk^*}(D_k) | k \in [1, m]\} \quad (16)$$

$$E_{pk^*}(D_k) = \left\{ E_{pk^*}(\mathbf{v}_j) = (E_{pk^*}(x_j), E_{pk^*}(y_j), E_{pk^*}(z_j)) \mid \right. \\ \left. j \in [I_k, I_k + N_w] \right\}$$

내에 연산자 \oplus 에 의하여 m 번 반복하여 삽입한다. 예를 들어, j 번째 워터마크 $E_{pk^*}(w_j^2)$ 는 임의의 데이터 집합 내의 j 번째 꼭지점 데이터 $E_{pk^*}(\mathbf{v}_j)$ 내에

$$E_{pk^*}(\mathbf{v}_j) = E_{pk^*}(\mathbf{v}_j) \oplus E_{pk^*}(w_j^2) \\ = E_{pk^*}(\mathbf{v}_j) + E_{pk^*}(2^t) \times E_{pk^*}(w_j^2) \quad (17)$$

와 같이 삽입된다. 연산자 \oplus 는 합과 곱에 대하여 준동형 특성을 만족하므로 위 식은 다음과 같다.

$$E_{pk^*}(\mathbf{v}_j) = E_{pk^*}(\mathbf{v}_j + 2^t \times w_j^2) \quad (18)$$

이를 공간영역 상에서 살펴보면, 워터마크 비트 w_j^2 를 2^t 배하여 데이터 집합의 각 원소 d_j 에 더함으로써 워터마크가 삽입된 데이터 집합

$$D_k = \{ \mathbf{v}_j = \mathbf{v}_j + 2^t \times w_j^2 \mid j \in [I_k, I_k + N_w] \} \quad (19)$$

을 구하는 것과 같다. 이와 같은 방법으로 판매자는 암호화된 객체 데이터 집합 내에 2차 워터마크를 삽입함으로써, 최종 워터마크된 암호 콘텐츠 $E_{pk^*}(\mathbf{X}'')$ 를 구매자에게 전달한다. 구매자는 비밀키 sk^* 에 의하여 $E_{pk^*}(\mathbf{X}'')$ 를 복호하여 다중 워터마크된 콘텐츠 \mathbf{X}'' 를 얻는다.

4.3 워터마크 추출

불법 복제된 콘텐츠 \mathbf{Y} 가 발생되었을 때에는 III절에서 설명하였듯이 식별 및 중재 프로토콜에 의하여 불법 복제 유무를 판정한다. 이 때 판매자 측에서는 \mathbf{Y} 내에 단일 워터마크 \mathbf{W}^1 를 ARB 측에서는 WCA 워터마크 \mathbf{W}^2 를 추출하며, 추출 방법은 삽입 방법과 유사하다. 단일 워터마크 \mathbf{W}^1 추출 방법에서는 \mathbf{Y} 객체 \mathbf{O}_i^* 내의 꼭지점 데이터 \mathbf{V}_i^* 을 그림 7 (b)에서와 같이 정규화 및 꼭지점 그룹화를 통하여 워터마크가 삽입된 꼭지점 그룹 $\mathbf{B}^* = \{B_j | p(B_j) > Th, j \in [1, N_w]\}$, $B_j = \{ \mathbf{v}_{j,k}^* | k \in [1, N_{B_j}] \}$ 을 얻는다. j 번째 워터마크 비트 w_j^* 는 j 번째 그룹 B_j 내의 꼭지점 좌표 $\mathbf{v}_{j,k}^*$ 들의 객체 중점과의 거리값 $\hat{r}_{j,k}^* = \frac{\|\mathbf{c}_{B_j} - \mathbf{v}_{j,k}^*\|}{N_{B_j}}$ 을 구한 다음, 이를 Δr 에

의하여 양자화하여 $q_{j,k}^* = \text{INT}(\hat{r}_{j,k}^* / \Delta r + 0.5)$

$$\begin{cases} w_{j,k}^* = 0, & \text{if } q_{j,k}^* \% 2 = 0 \\ w_{j,k}^* = 1, & \text{if } q_{j,k}^* \% 2 = 1 \end{cases} \quad (20)$$

$$w_j^* = \text{INT}(\sum_{k=1}^{N_{B_j}} w_{j,k}^* / N_{B_j} + 0.5) \quad (21)$$

와 같이 추출된다. 이상의 방법으로 모든 꼭지점 그룹 \mathbf{B}^* 에 대하여 워터마크 $\mathbf{W}^* = \{w_j^* | j \in [1, N_w]\}$ 를 추출한다. WCA 워터마크 \mathbf{W}^2 는 준동형 특성에 의하여 공간 영역 상에서 추출이 가능하다. WCA 워터마크 추출 방법에서는 우선 \mathbf{Y} 객체 \mathbf{O}_i^* 내의 워터마크 삽입 대상 꼭지점 집합 $\mathbf{D} = \{D_k | k \in [1, m]\}$ 를 획득한다. 그런 다음, 각 데이터 집합 $D_k = \{ \mathbf{v}_{kj}^* | j \in [I_k, I_k + N_w] \}$ 내의 꼭지점 좌표 원소 $\mathbf{v}_{kj}^* = (x_{kj}^*, y_{kj}^*, z_{kj}^*)$ 의 t 번째 비트가 w_{kj}^* 이다. 즉, $w_{kj}^* = (\mathbf{v}_{kj}^* \& 2^t) \gg t - 1$ 이다. 여기서 $\&$ 는 비트곱이고, \gg 는 우측 비트쉬프트 연산이다. m 개의 데이터 집합 내에 m 개의 비트들을 모두 추출하여, 최종 추출된 WCA 워터마크 $\mathbf{W}^{2*} = \{w_j^* | j \in [1, N_w]\}$, $w_j^* = \text{INT}(\sum_{k=1}^m w_{kj}^* / m + 0.5)$ 를 얻는다.

5. 실험 결과

본 장에서는 익명 Buyer-Seller 워터마킹 프로토콜 상에서 모바일 3D 콘텐츠에 대한 다중 워터마크 삽입 구현 및 실험 결과에 대하여 살펴보기로 한다.

5.1 모바일 3D 콘텐츠 내에 다중워터마킹 기법 구현

본 실험에서는 PowerVR SDK 상의 메인 메시지 루프 및 렌더 루프 내에 제안한 모바일 3D 콘텐츠 다중 워터마킹 방법을 그림 7에서와 같이 구현하였다. 이 그림을 살펴보면, InitApp, InitInstance, Render, ReleaseView, QuitApp, Exit 등의 상태(State)에 따라 각각 정의된 함수가 호출된다. InitApp 상태에서는 InitApplication 함수가 호출되며, 이 함수는 메인함수에서 초기에 한번 호출되는 것으로 렌더 API가 초기화되기 전 디바이스 환경 설정에 필요한 값들을 변경한다. InitInstance 상태에서는 OsInitOS, OsDofnitAPI, InitView 함수가 호출된다. OsInitOS 함수에서는 전역변수 상에 인스턴스 핸들을 저장하고 메인 프로그램 창을 생성하여 출력

한다. OsDoInitAPI 함수에서는 GL 초기화 실행하여 윈도우 창을 가져오게 한다. InitView 함수는 렌더링 텍스트 상의 변화가 있을 때 호출되는 것으로, 텍스처, 꼭지점 버퍼 등과 같은 값들을 초기화한다. Render 상태에서는 RenderScene, ApiRenderComplete, OsRenderComplete 함수가 호출된다. RenderScene 함수는 프로그램의 메인 렌더링 루프 함수로써 매 프레임마다 호출되며, 뷰 포트, 실제적인 렌더, 텍스트 출력 등을 실행한다. 렌더링이 수행된 다음, ApiRenderComplete, OsRenderComplete 함수에서 API 및 OS 렌더 완료가 선언된다. ReleaseVies 상태에서는 렌더 API가 종료되기 전 ReleaseView 함수가 호출된다. 이 함수에서는 InitView 함수에서 얻어진 메모리 및 리소스를 해제한다. QuitApp 상태에서는 프로그램 종료 전 QuitApplication 함수가 호출되며, 이 함수에서는 InitApplication 함수에서 얻어진 메모리 및 리소를 해제한다. 마지막으로 Exit 상태에서는 윈도우창을 해제하고 프로그램이 종료되는 OsExit 함수가 호출된다. 본 실험에서는 그림 8에서와 같이 모바일 3D 콘텐츠의 메시지 루프 및 렌더 루프 상의 InitApplication 함수 내에 3D 콘텐츠 객체를 로딩한 후, 각 객체에 제한한 다중 워터마크를 삽입하여 암호화된 콘텐츠 $E_{pk}(X)$ 를 얻는다. 그리고 암호화된 콘텐츠 $E_{pk}(X)$ 는 InitView 함수에서 복호키에 의하여 다중 워터마크된 X'' 로 복호된 다음,

RenderScene 함수에서 윈도우 창에 출력된다. 이상과 같은 본 실험에서는 PowerVR OpenGL ES SDK [16] 기반의 EvilSkull, Mouse, PolybumpHead, Vase 모델에 대하여 워터마킹 기법을 적용하였다. 각 모델의 객체, 폴리곤수, 꼭지점수 및 워터마크 비트수는 표 1에서와 같으며, 표 1를 살펴보면 PolybumpHead를 제외한 나머지 모델에서는 다중 워터마크를 각기 다른 객체에 삽입됨을 볼 수 있다. 본 실험에서는 랜덤 가우시안 분포를 가지는 이진 워터마크를 100비트 생성하여 이를 WCA 워터마크로 사용하였고, 각 모델 객체의 꼭지점 사이각 분포에 따라 워터마크 비트수를 결정하여, 이를 단일 워터마크로 사용하였다. 모바일 3D 콘텐츠 모델 및 워터마크된 모델들은 그림 9에서와 같다.

5.2 비가시성 평가 실험

일반적인 2D 영상신호처리에서는 영상 화질 척도로 각 화소값에 대한 PSNR(Peak signal-to-noise ratio)를 적용하고 있는 반면, 3D 꼭지점 좌표로 구성되는 모델에 대해서는 이와 같은 객관적인 화질 척도의 적용이 어렵다. 따라서 본 실험에서는 워터마크의 비가시성을 확인하기 위하여 꼭지점 좌표 거리에 대

표 1. 본 실험에 사용된 모델의 객체, 폴리곤수, 꼭지점수 및 삽입된 워터마크 비트수

모델명	객체	폴리곤수	꼭지점수	단일워터마크비트수	WCA워터마크비트수	꼭지점 SNR비 [dB]
EvilSkull	Skull	838	583	66	-	40.50
	Jaw	346	175	-	100	68.86
	계	838	583	66	0	
Mouse	Head	1078	605	62	-	38.42
	Hand Left	362	210	-	100	71.04
	Hand Right	362	212	-	100	72.19
	Body	332	189	-	100	73.75
	Object	760	410	39	-	26.37
	계	2,972	1,799	128	300	
Polybump Head	Head Low	276	153	17	100	33.80
Vase	Glass	480	287	-	100	69.03
	Silver	2352	1335	90	-	40.76
	계	756	440	17	200	

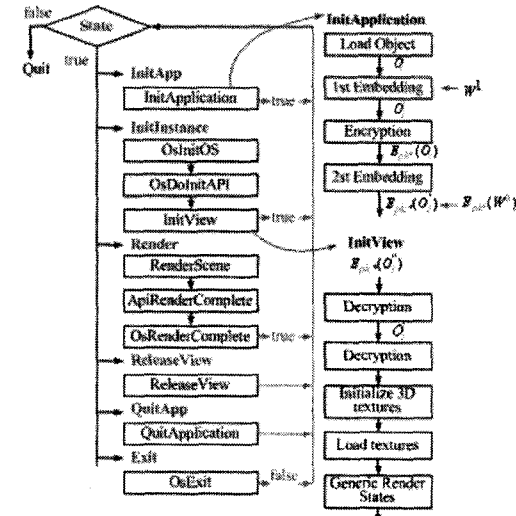


그림 8. PowerVR SDK 상의 제한한 모바일 3D 콘텐츠 다중 워터마크 삽입 과정

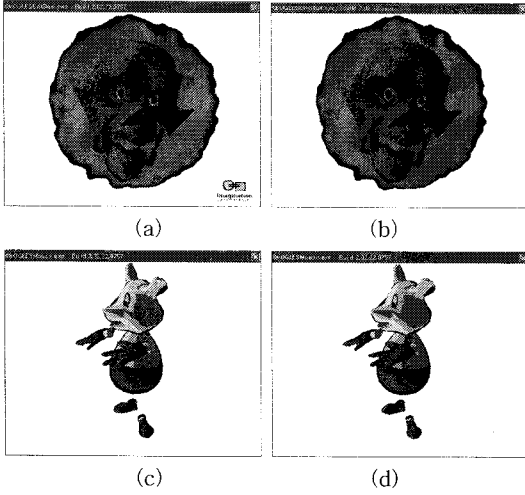


그림 9. 모바일 콘텐츠 및 워터마크된 콘텐츠의 첫 번째 프레임: (a) EvilSkull과 (b) 워터마크된 EvilSkull, (c) Mouse와 (d) 워터마크된 Mouse

한 SNR(Signal-to-noise ratio)를 사용하였다. 즉, 모델 객체 O_i 의 꼭지점 $V_i = \{v_k | k \in [1, N_i]\}$ 에 대한 SNR_i 는

$$SNR_i = 10 \log_{10} \left(\frac{R_{signal}^2}{R_{noise}^2} \right) = 20 \log_{10} \left(\frac{R_{signal}}{R_{noise}} \right) \quad (22)$$

$$= 20 \log_{10} \left(\frac{\sqrt{\frac{1}{N_i} \sum_{k=1}^{N_i} |v_k - M_i|^2}}{\sqrt{\frac{1}{N_i} \sum_{k=1}^{N_i} |v_k - v'_k|^2}} \right)$$

where $|v_k - M_i| = \sqrt{(x_k - \bar{x}_i)^2 + (y_k - \bar{y}_i)^2 + (z_k - \bar{z}_i)^2}$,
 $|v_k - v'_k| = \sqrt{(x_k - x'_k)^2 + (y_k - y'_k)^2 + (z_k - z'_k)^2}$

와 같이 각 꼭지점 $v_k = (x_k, y_k, z_k)$ 와 객체 O_i 의 중심 $M_i = (\bar{x}_i, \bar{y}_i, \bar{z}_i)$ 와의 거리차 $|v_k - M_i|$ 에 대한 RMS (Root mean square)인 R_{signal} 와 꼭지점 v_k 와 워터마크된 꼭지점 $v'_k = (x'_k, y'_k, z'_k)$ 와의 거리차 $|v_k - v'_k|$ 에 대한 RMS인 R_{noise} 의 비율이다.

각 모델 객체에 대한 꼭지점 SNR비는 표 1에서와 같다. 표 1를 살펴보면, 단일 워터마크가 삽입된 객체의 꼭지점 SNR비는 36.37-40.76dB 정도이며, WCA 워터마크가 삽입된 객체의 꼭지점 SNR비는 68.86-73.75dB 정도이다. 제안한 방법에서는 단일 워터마크 비트수가 WCA 워터마크 비트수에 비하여 작으나, 단일 워터마크를 꼭지점 분포에 삽입하므로, 삽

입 대상 꼭지점 수가 WCA 워터마크 삽입 방법에 비하여 2-3배 정도 많다. 따라서 단일 워터마크의 꼭지점 SNR비가 WCA 워터마크의 꼭지점 SNR비에 비하여 상대적으로 작게 나타남을 알 수 있다. PolybumpHead 모델은 하나의 객체로만 구성되므로, 이 모델에서는 단일 워터마크 및 WCA 워터마크가 동시에 삽입되었다. 이 모델의 꼭지점 SNR비는 33.80dB이다. 그림 9에서는 모바일 3D 콘텐츠 및 워터마크된 콘텐츠들의 렌더링된 첫 번째 프레임을 보여주고 있다. 이 그림을 살펴보면, 워터마크의 비가시성을 확인할 수 있다.

5.3 견고성 평가 실험

구매자는 모바일 단말기 상에서의 3D 콘텐츠 실행 파일 (.exe, .bin)을 제공받으므로, 불법 복제는 가능하나 편집은 할 수가 없을 것이다. 그러나 본 실험에서는 간단한 몇 가지 공격에 대하여 견고성을 평가하였으며, 워터마크의 비트 에러율 (bit error rate, BER)에 따라 검출 여부를 판단하였다. 견고성 실험에서는 각 객체의 꼭지점 데이터에 랜덤 잡음, 데이터 정밀도 가변, 데이터 삭제, 확대, 축소 등을 수행하였다.

랜덤 잡음 실험에서는 모든 꼭지점 좌표값들을 $v' = v \times (1 + \alpha \times \text{uniform}())$ 로 변경하였다. 여기서 α 는 잡음 크기를 나타내는 변조도이며, $\text{uniform}()$ 는 $[-0.5, 0.5]$ 의 범위를 가지는 균등한 랜덤 함수이다. 변조도 α 에 대한 실험 결과는 그림 10 (a)에서와 같다. 이 그림을 살펴보면, α 가 0.6일 경우에서는 워터마크가 모두 검출되었으며, α 가 0.8일 때까지는 워터마크의 80% 이상이 검출됨을 알 수 있다. 데이터 정밀도 가변 실험에서는 꼭지점 좌표값들의 소수점 자리수를 1에서 6까지 가변하였다. 즉, 꼭지점 좌표값들은 6자리수의 실수형이므로, 본 실험에서는 이를 5에서 1까지 자리수를 줄였다. 실험 결과로는 그림 10 (b)에서와 같이 검출된 워터마크의 BER이 0에서 0.024이므로, 거의 모든 워터마크가 검출됨을 알 수 있다. 데이터 삭제 실험에서는 각 객체의 꼭지점들 중 10%에서 60%의 꼭지점들을 임의로 삭제하였으며, 이에 대한 실험 결과는 그림 10 (c)에서와 같다. 이 그림을 살펴보면, 30% 정도 꼭지점 데이터를 삭제하여도 80% 이상의 워터마크가 검출됨을 알 수 있다. 즉, 제안한 방법에서는 1차 및 2차 워터마크

비트를 객체의 꼭지점 개수에 따라 반복 삽입하므로, 일정 부분의 꼭지점 데이터가 삭제되더라도 워터마크를 검출한다. 그러나 워터마크가 여러 위치에 동시에 삽입될 경우 데이터 삭제와 같은 공격에 대하여 강인할 수 있으나, 삽입 대상 집합의 데이터 개수가 증가될 것이다. 기하학적인 공격에 대한 실험에서는 회전, 이동 및 스케일링을 수행하였다. 우선 회전 공격 실험에서는 $[-50^\circ, +50^\circ]$ 범위 내의 각으로 모든 꼭지점들을 회전한 다음 워터마크를 검출하였다. 그리고 이동 공격 실험에서는 모든 꼭지점들을 $[-30, 30]$ 범위의 임의의 위치로 이동한 후, 이동된 모델에 대하여 워터마크를 검출하였다. 마지막으로 스케일링 공격 실험에서는 모든 꼭지점들을 $[0.5, 5.0]$ 범위 내의 임의의 비율로 확대 및 축소한 다음 워터마크를 검출하였다. 회전, 이동 및 스케일링 공격에 대한 실험 결과는 그림 10 (d)-(f)에서와 같다. 이 그림들을 살펴보면, 1차 워터마크 W^1 는 회전, 이동 및 스케일링 모든 공격에 대하여 모든 검출됨을 볼 수 있다. 제안한 방법에서는 공간 영역 상에서 꼭지점 좌표 정규화를 수행한 다음, 꼭지점 데이터들의 거리 분포에 W^1 가 삽입한다. 즉, 꼭지점 좌표 정규화 과정은 회전, 이동 및 스케일링

등의 기하학적 공격에서도 동일한 정규화가 되므로 W^1 는 이와 같은 공격에 대하여 강인성을 가진다. 그러나 암호화된 2차 워터마크 W^2 는 암호화 영역 상에서 꼭지점 데이터의 임의의 비트에 삽입되므로 회전, 이동 및 스케일링 공격에 대하여 약 60-50% 정도의 워터마크가 검출되었다. 암호화된 워터마크는 준동형 특성을 만족하면서 블라인드 특성을 가지는 삽입 연산자에 의하여 삽입되어야 한다. 그러므로 제안한 방법에서는 암호화 영역 상에서 암호화된 꼭지점 데이터의 특정 비트에 삽입하며, 추출시 복호화된 데이터 상에서 추출한다. 그러므로 회전, 이동 및 스케일링 공격에서는 꼭지점 데이터의 비트열이 바뀌게 되므로 추출시 워터마크 비트 오류가 발생된다. 이를 해결하기 위한 방법으로는 워터마크 삽입시 원래의 위치, 회전각, 스케일링 등으로 꼭지점들을 재배열하는 과정을 수행한 후, 워터마크를 검출 과정을 수행하면 비트 오류없이 검출될 것이다. 이와 같이 본 연구에서는 암호화 영역 상에서 준동형 특성을 만족하면서 기하학적 공격에 강인한 워터마크 삽입 기법과 회전, 이동 및 스케일링 등에 강인한 재배열 방법에 대하여 향후 진행하고자 한다.

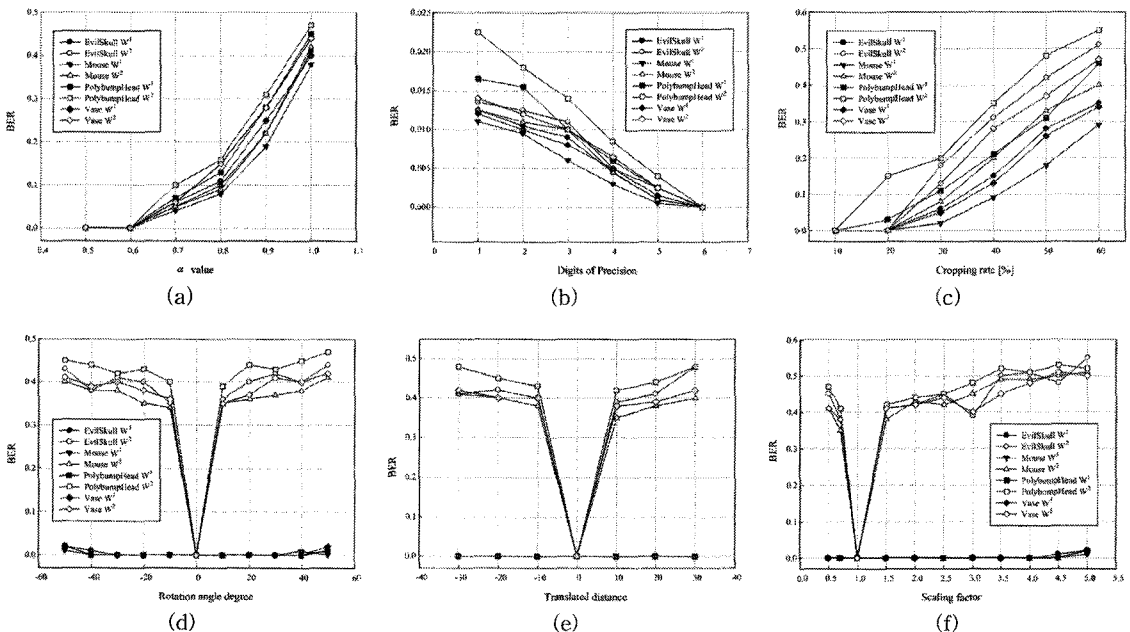


그림 10. (a) 잠입 첨가, (b) 데이터 정밀도 가변, (c) 꼭지점 데이터 삭제, (d) 회전, (e) 이동 및 (f) 스케일링 공격들에 대한 워터마크 BER

6. 결 론

본 논문에서는 모바일 3D 콘텐츠에 대한 저작권 보호 기술을 위하여 익명 Buyer-Seller 워터마킹 프로토콜 기반의 다중 워터마크 삽입 방법을 제안하였다. 제안한 방법에서는 판매자 측에서 모바일 콘텐츠를 구성하는 객체들 중 임의로 선택한 다음, 판매자의 단일 워터마크를 생성한다. 그리고 선택된 객체 내에 꼭지점 데이터들의 사이각 분포를 이용하여 워터마크 삽입 대상 집합을 결정한다. 이 집합에 속하는 꼭지점 데이터들에 단일 워터마크를 삽입한다. 단일 워터마크된 객체들을 암호화한 다음, WCA에게 전달받은 암호화된 워터마크를 암호화된 꼭지점 데이터 값과 선형 결합을 통하여 암호화 영역 상에서 이들을 삽입한다. 본 실험에서는 모바일 3D 콘텐츠 도구인 PowerVR MBX를 이용하여 제안한 방법의 알고리즘을 구현하였다. 실험 결과로부터 모바일 3D 콘텐츠의 저작권 보호와 불법 복제 방지가 가능함을 확인하였고, 랜덤 잡음, 데이터 정밀도 가변, 확대 및 축소 등에 대하여 워터마크가 검출됨을 확인하였다. 제안한 방법에서는 Lei 등이 제시한 익명 Buyer-Seller 워터마킹 프로토콜 기반으로 꼭지점 데이터의 기하학적 특성에 따른 워터마크 삽입 방법을 제시함으로써 기존 논문[14,15]의 문제점인 사용자의 익명성 보장 및 비결합 문제 해결과 기하학적 공격에 대한 워터마크의 견고성을 향상시키고자 하였다.

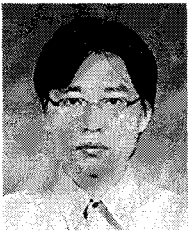
본 논문에서는 콘텐츠 내의 데이터들을 RSA 기반으로 각 데이터들을 1024 비트로 암호화하여 구현하였으나, 암호화된 데이터량이 각 데이터 개수에 1024배 만큼 증가된다. 그리고 암호화 영역 내에 워터마크를 삽입하기 위하여 더하기, 빼기, 곱하기 등의 선형 연산자에 대하여 준동형 특성을 만족하는 암호 기법 기반에 워터마크 삽입 연산을 설계하여야 한다. 제안한 방법에서는 더하기 연산에 기반하는 워터마크 삽입 연산자를 사용하였으나 암호화 영역 내에서 보다 많은 워터마킹 기법이 연구되어야 할 것이다.

참 고 문 헌

- [1] X-Forge Engine, Fathammer, <http://www.fathammer.com>
- [2] Mascot Capsule Engine, HI CORP., <http://www.hicorp.co.jp>
- [3] Swerve Engine, SINJISOFT, <http://www.sinjisoft.co.kr>
- [4] NF3D Engine, GAVAPLUS, <http://www.gavaplus.co.kr>
- [5] M3D, REAKOSYS, <http://www.reakosys.com>
- [6] GNEX SDK, Gnexclub, <http://www.gnexclub.com>
- [7] R. Ohbuchi, H. Masuda, and M. Aono, "Watermarking Three-Dimensional Polygonal Models," *Proceedings of the ACM Multimedia*, pp. 261-272, 1997.
- [8] O. Benedens, "Geometry-Based Watermarking of 3D Models," *IEEE Computer Graphics and Applications*, pp. 46-55, 1999.
- [9] K.R. Kwon, S.G. Kwon, and S.H. Lee, "3D Watermarking Shape Recognition System Using Normal Vector Distribution Modelling," *Lecture Notes in Computer Science*, vol. 3397-9743, pp. 481-490, 2005.
- [10] S.H. Lee and K.R. Kwon, "Watermarking for 3D Mesh Model Using Patch CEGIs," *Lecture Notes in Computer Science*, Vol.3481, pp. 557-566, 2005.
- [11] K.R. Kwon, H.J. Chang, G.S. Jung, K.S. Moon, and S.H. Lee, "3D CAD Drawing Watermarking Based on Three Components," *IEEE International Conference on Image Processing*, pp. 1385-1388, 2006.
- [12] N. Memon and P.W. Wong, "A Buyer-Seller Watermarking Protocol," *IEEE Transactions on Image Processing*, Vol.10, No.4, pp. 643-649, 2001.
- [13] C.L. Lei, P.L. Yu, P.L. Tasi, and M.W. Chan, "An Efficient and Anonymous Buyer-Seller Watermarking Protocol," *IEEE Transactions on Image Processing*, Vol.13, No.12, pp. 1618-1626, 2004.
- [14] 권성근, 이석환, 배성호, 박재범, 권기룡, "Buyer-Seller 워터마킹 프로토콜 기반의 모바일 3D 콘텐츠 워터마킹 기법," 한국통신학회논문지 제

32권 제8호, pp. 788-799, 2007.

- [15] S.G. Kwon, S.H. Lee, K.R. Kwon, E.J. Lee, S.Y. Ok and S.H. Bae, "Mobile 3D Game Contents Watermarking Based on Buyer-Seller Watermarking Protocol," *IEICE Transaction on Information and System*, Vol.E91-D, No.7, pp. 2018-2026, 2008.
- [16] PowerVR MBX OpenGL ES 1.x, Imagination Technology, <http://www.imgtec.com/>.



이 석 환

1999년 경북대학교 전자공학과 졸업(공학사)
 2001년 경북대학교 전자공학과 졸업(공학석사)
 2004년 경북대학교 전자공학과 졸업(공학박사)
 2005년~현재 동명대학교 정보보호학과 조교수

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