Buyer-Seller 워터마킹 프로토콜 기반의 모바일 3D 콘텐츠 워터마킹 기법

정회원 권 성 근*, 이 석 환**, 배 성 호***, 박 재 범****, 권 기 룡*****

Mobile 3D Contents Watermarking Technique Based on Buyer-Seller Watermarking Protocol

Seong-Geun Kwon*, Suk-Hwan Lee**, Sung-Ho Bae***, Jae Bum Park****,
Ki-Ryong Kwon***** ***Regular Members***

요 약

본 논문에서는 모바일 상에서 서비스되는 3D 콘텐츠들의 저작권 보호 및 불법 복제 방지를 위한 워터마킹 기법을 제안한다. 제안한 방법에서는 Buyer-Seller 워터마킹 프로토콜 기반으로 모바일 애니메이션 데이터 내에 저작권 정보 및 사용자의 폰번호를 공간 영역 및 암호화 영역 상에서 각각 삽입한다. 또한 인가된 사용자만 모바일 폰 상에서 3D 애니메이션 게임을 실행하기 위하여 실행키를 실행코드 내에 삽입한다. 본 실험에서는 모바일 애니메이션 저작툴인 G3-SDK 상에서 제안한 방법을 구현하였다. 실험 결과로부터 제안한 방법이 모바일 3D 애니메이션의 저작권 보호 및 불법 복제 방지가 가능함을 확인하였으며, 잡음첨가, 데이터 정밀도 가변, 확대, 축소 등의 공격에 대하여 워터마크가 검출됨을 확인하였다.

Key Words : Mobile 3D Contents, Digital Watermarking, Buyer-Seller Watermarking Protocol

ABSTRACT

This paper presents a watermarking method for copyright protection and illegal copy prevention of mobile 3D contents. The proposed method embeds copyright information and user's phone number into spatial domain and encryption domain of mobile animation data based on Buyer-Seller watermarking protocol. Furthermore, we insert user's operation key so that only authorized user can play 3D animation game in mobile device. We implemented the proposed method by using mobile animation tool, G3-SDK. From experimental results, we verified that the proposed method is capable of copyright protection and illegal copy prevention since the watermark can be well extracted against geometrical attacks, such as noise addition, data accuracy variableness and data up/down scaling.

Ⅰ. 서 론

최근 모바일 기술의 급진적인 발전과 더불어 모바일 상에서 실행되는 3D 게임 기술이 발달되고 있다. 그러나 모바일 3D 게임의 섬세한 그래픽이나 치밀한 스토리 구조에 의하여 게임의 용량이 증가

※ 본 연구는 2006년도 SK Telecom 재원으로 설립된 동명대학교 SKTU차세대통신기술 연구소 학술연구비 지원에 의하여 이루어진 것임(SKTU-06-003).

* 삼성전자 무선사업부 (SeongGeunKwon@hanmail.net), ** 동명대학교 정보보호학과 (skylee@tu.ac.kr)
*** 동명대학교 멀티미디어공학과 (baesh@tu.ac.kr), **** SKT (trigun@sktelecom.com)
***** 부경대학교 전자컴퓨터정보통신공학부 (krkwon@pknu.ac.kr)

논문번호 : KICS2007-02-076, 접수일자 : 2007년 2월 20일, 최종논문접수일자 : 2007년 8월 1일

되고 있다. 모바일 게임의 용량이 커져 가면서 데이터 통신비에 대한 사용자의 부담을 덜고자 'PC 싱크'를 통한 다운로드 방법이 대안으로 제시되는 가운데 불법 복제 우려에 대한 관심이 높아지고 있다. 현재 불법복제방지와 관련하여 인증 모듈들이 상용 서버에 적용되고 있으나, 콘텐츠 자체에 대한 DRM 저작권법 또는 워터마킹 기술이 매우 절실하다. 일반적으로 사용자는 브라우저를 통하여 모바일 3D 게임 콘텐츠를 해당 모바일 기기로 다운로드하여 아무런 제한없이 사용할 수 있다. 그러나 악의적인 사용자에 의해 3D 게임 콘텐츠를 PC로 다운로드하거나 모바일기기 간 콘텐츠 전송을 통해 다른 사용자에게 유포할 수 있다.

3D 컨텐츠 산업의 발달과 더불어 3D 컨텐츠들의 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[3]-[6]. 3D CAD 도면 모델 워터마킹 기법에서는 3D CAD의 기본 성분인 Line, Arc, Circle 및 3DFACE의 기하학적 성질을 이용하여 워터마크를 삽입한다[7]. 그러나 이들 방법들은 정지된 그래픽 모델에 적용된 워터마킹 기법이며, 또한 각 모델의 정보들은 고정된 실수 값들로 모바일 상에서 서비스되는 3D 게임 콘텐츠에는 적용되지 못한다.

최근 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[8],[9]. Memon 등[8]은 판매자 (seller)가 워터마크된 콘텐츠들에 대한 직접적인 접근을 방지함으로써 고객 권리 문제 (customer right problem)를 다루는 Buyer-Seller 워터마킹 프로토콜을 제안하였다. 이 프로토콜 상에서는 판매자는 구매자의 워터마크를 포함하는 콘텐츠를 복제할 수 없으며, 만약 판매자가 허가되지 않은 콘텐츠 발견시 이 콘텐츠로부터 구매자를 확인하여 제3의 인증기관에 통하여 이 사실을 증명한다. 이는 허가되지 않은 콘텐츠의 복제 여부가 판매자에 의하여 이루어질 수 있다는 것을 구매자가 주장하지 못하도록 하는 것이다.

본 논문에서는 모바일 3D 콘텐츠의 저작권 보호 및 불법 복제 방지를 위하여 Buyer-Seller 워터마킹 프로토콜 상에서 공간 영역 및 암호화 영역 상에서 다중 워터마크를 삽입하는 방법을 제안한다. 제안한 방법에서는 모바일 3D 콘텐츠를 구성하는 캐릭터 모델의 오브젝트 또는 애니메이터 데이터 내에 다중 워터마크를 공간 영역 및 암호화 영역 상에서 삽입한다. 워터마크 삽입 방법에서는 판매자가 저작권 정보 및 구매 번호로 구성된 1차 워터마크를 캐릭터 모델의 오브젝트 또는 애니메이션 데이터들 중 임의로 선택된 데이터 값에 삽입한다. 1차 워터마크가 삽입된 데이터를 암호화한 후, 인증기관이 치환 및 암호화한 구매자의 모바일폰 번호를 암호화 영역 내에 선형 결합하여 2차 워터마크 및 암호화된 콘텐츠를 구매자에게 전달한다. 구매자는 이를 복호화하여 다중 워터마크된 콘텐츠를 얻은 후, 실행키에 의하여 모바일 3D 콘텐츠를 실행한다. 불법 복제된 다중 워터마크된 콘텐츠 발견시, 판매자는 콘텐츠 내에 1차 워터마크를 추출하여 저작권 정보 및 구매 번호를 확인한 다음, 치환된 2차 워터마크를 추출하여 이를 인증기관에 전달한다. 인증기관은 이를 역치환하여 구매자의 모바일폰 번호 및 구매 번호의 정보를 확인함으로써 불법 배포한 최초 구매자를 추적한다. 본 실험에서는 모바일 3D 게임용 개발 도구인 G3-SDK[11]를 이용하여 제안한 방법의 알고리즘을 구현하였다. 실험 결과로부터 모바일 3D 애니메이션 캐릭터의 저작권 보호와 불법 복제 방지가 가능함을 확인하였으며, 다중 워터마크된 콘텐츠들의 PSNR이 39.8dB-42.1dB이고, 잡음첨가, 데이터 정밀도 가변, 확대 및 축소 등에 대하여 견고함을 확인하였다.

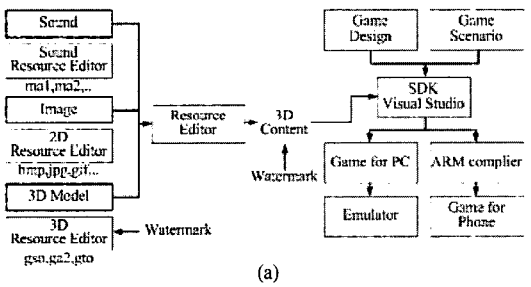
본 논문의 구성은 다음과 같다. 우선 Ⅱ장 기존 연구에서는 모바일 3D 엔진 및 Buyer-Seller 워터마킹 프로토콜에 대하여 간략히 살펴본 후, Ⅲ장에서는 Buyer-Seller 워터마킹 프로토콜 상에서 모바일 3D 콘텐츠 내에 다중 워터마크를 삽입하는 방법에 대하여 살펴본다. 그리고 Ⅳ장에서는 구현 실험 결과를 보며, 마지막 Ⅴ장에서는 본 논문의 결론을 맺는다.

Ⅱ. 기존 연구

2.1 모바일 3D 엔진

모바일용 콘텐츠들은 위피(WIPI) 및 브루(Brew)

의 무선 인테넷 플랫폼 기반으로 SK-VM, GNEX (GVM), 브루(Brew) 등의 모바일 콘텐츠 개발 도구를 이용하여 제작되고 있으며, 최근 급속적인 모바일 기술의 발전과 더불어 많은 개발 콘텐츠 개발 도구들도 발전되고 있다. 대표적인 모바일 3D 엔진으로는 고미드의 G3 엔진[11], 가바플러스의 NF3D 엔진[12], 리코시스의 M3D 엔진[13] 등이 있다. 본 장에서는 대표적인 모바일 3D 엔진인 G3-SDK[11]에 대하여 간략히 설명한다. 기본적으로 3D 콘텐츠를 제작하기 위한 3D 엔진과 3D 아바타 시스템, 3D 월드 뷰어, 3D 저작도구로 구성되어 있다. 엔진의 크기는 50KB의 저용량으로 엔진을 활용하여 응용 프로그램을 제작할 경우 응용 프로그램의 크기는 약 500KB 정도이다. 엔진의 성능은 500 폴리곤 정도의 환경에 대해 초당 20장의 이미지를 그릴 수 있다. 탑재된 3D 엔진은 OpenGL ES 1.0과 호환되며, 추가적으로 모델 및 애니메이션 데이터 로딩 및 본(Bone) 애니메이션 등과 같이 진보된 형태의 기능을 제공한다.



(a)

```
unsigned char center_gso[65243] = {
0x00, 0x00, 0x00, 0x08, 0x01, 0x63, 0x65, 0x6E, 0x74, 0x65, 0x72, 0x2E,
0x08, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x63, 0x65, 0x6E, 0x74, 0x65, 0x72, 0x00, 0x00, 0x00,
```

```
unsigned char center_ga2[93968] = {
0x67, 0x61, 0x02, 0x01, 0x02, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x02, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x01, 0xC7, 0xFD,
0xFF, 0xFD, 0x93, 0x00, 0x00, 0x48, 0x20, 0x78, 0x00, 0x03, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x02, 0x01, 0x6A, 0xFF, 0xFF, 0x87, 0x6E,
```

(b)

그림 1. (a) 모바일 3D 게임 개발 구조 및 (b) GSO 및 GA 데이터 구조

G3 SDK에서 제공하는 개발 툴에는 그림 1 (a)에서와 같이 2D, 3D, 사운드와 관련된 리소스를 편집, 관리, 변환하는 기능을 갖는 리소스 툴이 있다. 이 툴에는 프로젝트 단위로 리소스들을 일괄 관리하는 것이 특징이며, 리소스 타입은 기본적으로 2D 이미지, 3D 모델링 오브젝트, 사운드 관련 리소스로 분류되고, 이외의 리소스 타입은 사용자 타입으로 지정하여 관리한다. 여기서 2D로는 BMP, JPG, GIF, PCX, PNG 이미지 파일 형식을 리소스로 등록할 수 있으며, 3D로는 GSO, GA, GTO 파일을, 사운드는 SMAF (Synthetic music Mobile Aplication Format) 파일을 등록할 수 있다. 이외의 형식을 가진 리소스는 사용자 타입으로 분류가 되어 관리된다. 3D 모델링 오브젝트와 관련된 파일인 GSO는 VRML 데이터의 메쉬 정보와 유사하는 것으로 3차원 직각 좌표계의 (x,y,z) 좌표값 및 스킨 정보들로 구성되어 있다. GA는 본의 구조 및 애니메이션 정보를 나타내는 것으로 VRML 데이터의 움직임 정보를 나타내는 위치, 방향, 색상의 보간기 정보와 유사하다. 메쉬 및 보간기에 대한 설명은 VRML[14] 및 MPEG4-BIFS[15]의 3D 애니메이션 부분에 자세히 언급되어 있다. 본 논문에서는 그림 1 (b)에서와 같이 Hexa 데이터로 이루어진 GSO 및 GA 데이터들 중 임의로 선택된 데이터들의 비트에 워터마크를 삽입한다.

2.2 Buyer-Seller 워터마킹 프로토콜

Memon 등[8]이 제안한 Buyer-Seller 워터마킹 프로토콜에서는 그림 2에서와 같이 '구매자(buyer)'와 '판매자(seller)', 그리고 '워터마크 인증기관(watermark certification authority, WCA)'의 3자로 구성된다. 계약과정에서 각 구성원 간에 일어나는 일련의 절차들 중 워터마크 생성 프로토콜과 워터마크 삽입 프로토콜에 대하여 살펴보면 다음과 같다.

먼저 판매자의 보유 콘텐츠에 대한 구매 의사를 가진 구매자는 공개키(pk_B)와 비밀키(sk_B)의 쌍을 생성한 후, 구매자의 신원 I_B와 공개키 pk_B를 인증기관에 전달하여 워터마크의 생성을 요구한다(I). 인증기관(WCA)은 생성한 워터마크 $\mathbf{W}=\{w_1,w_2,\cdots,w_n\}$를 pk_B를 이용하여 암호화한 후, 암호화된 워터마크 $E_{pk_B}(\mathbf{W})$와 $E_{pk_B}(\mathbf{W})$의 유효성을 입증하는 서명 $Sign_{WCA}(E_{pk_B}(\mathbf{W}))$을 구매자에게 제공한다(II). 이 때 암호화된 워터마크 $E_{pk_B}(\mathbf{W})$는

$$E_{pk_B}(\mathbf{W})=\{E_{pk_B}(w_1),E_{pk_B}(w_2),\cdots,E_{pk_B}(w_n)\} \quad (1)$$

와 같이 워터마크의 각 성분들이 같은 키 pk_B로 암호화된 것이다. 구매자는 전달받은 $E_{pk_B}(\mathbf{W})$와 $Sign_{WCA}(E_{pk_B}(\mathbf{W}))$ 및 pk_B를 구매리스트와 함께 판매자에게 전송한다(III). 판매자는 우선 $Sign_{WCA}(E_{pk_B}(\mathbf{W}))$를 통해 $E_{pk_B}(\mathbf{W})$의 유효함을 확인

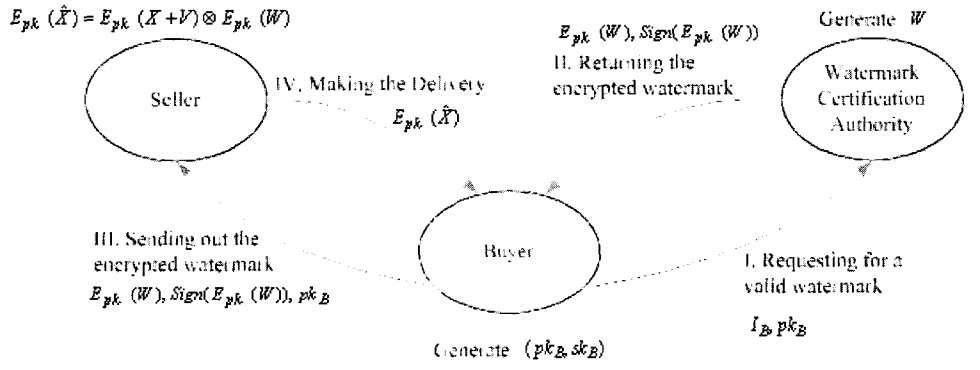


그림 2. Buyer-Seller 워터마킹 프로토콜 상에서의 구매절차

한 후, 일반 워터마킹 기법에 의하여 콘텐츠 X 내에 1차 워터마크인 구매자 정보 V를 삽입한다(X′). 그리고 암호화된 워터마크 $E_{pk_B}(\mathbf{W})$의 각 성분들을 랜덤 치환 $\sigma(E_{pk_B}(\mathbf{W})) = E_{pk_B}(\sigma(\mathbf{W}))$하여 이를 2차 워터마크로 사용한다. $E_{pk_B}(\sigma(\mathbf{W}))$를 1차 워터마크된 콘텐츠 X′ 내에 pk_B를 이용하여 암호화 영역 내에

$$E_{pk_B}(\hat{\mathbf{X}}) = E_{pk_B}(\mathbf{X}') \otimes E_{pk_B}(\sigma(\mathbf{W})) = E_{pk_B}(\mathbf{X}' \otimes \sigma(\mathbf{W})) \quad (2)$$

와 같이 삽입하여 암호화된 콘텐츠 $E_{pk_B}(\hat{\mathbf{X}})$를 구매자에게 전달한다(IV). 이 때 공개키 암호화 시스템은 워터마크 삽입 연산자 ⊗에 대하여 "privacy homomorphism"의 성질을 가진다. 구매자는 비밀키 sk_B를 이용하여 $E_{pk_B}(\hat{\mathbf{X}})$를 복호하여 워터마크된 콘텐츠 $\hat{\mathbf{X}}$를

$$\hat{\mathbf{X}} = D_{pk_B}(E_{pk_B}(\hat{\mathbf{X}})) = \mathbf{X}' \otimes \sigma(\mathbf{W}) \quad (3)$$

획득하게 한다. Memon 등[8]은 'privacy homorphism' 성질을 가지는 RSA 암호화 시스템 내에 Cox 등이 제안한 대역 확산 워터마킹 기법을 이용하여 암호화 영역 내에서 워터마크를 삽입하였다. 구매자에게 제공된 워터마크된 콘텐츠 $\hat{X}$에 대한 저작권 침해 및 분쟁 해결 프로토콜은 Memon 등의 논문[8]에 자세히 언급되어 있다. 이상과 같이 Memon 등[8]이 제안한 프로토콜을 구현하기 위하여 효과적인 암호화 알고리즘과 'privacy homorphism'에 따른 워터마크 삽입 연산자의 설계가 필요하다. 이들은 일반 정지영상에 대하여 워터마크 추출시 원본이 필요한 Cox 등의 기법을 사용하였다. 본 논문에서는 Memon 등[8]이 제안한 Buyer-Seller 워터마크 프로토콜 상에서 모바일 3D 애니메이션의 저작권 보호를 위한 워터마크 삽입 알고리즘을 제안한다.

Ⅲ. 제안한 모바일 3D 애니메이션 워터마킹

제안한 모바일 3D 애니메이션 워터마킹 시스템에서는 그림 3의 Buyer-Seller 워터마킹 프로토콜을 기반으로 다중 워터마크를 암호화 영역 및 공간 영역에 각각 삽입한다. 우선 모바일 3D 애니메이션에 대한 워터마킹 프로토콜에 대하여 살펴본 후, 이 프로토콜 상에서의 워터마크 삽입 기법에 대하여 살펴보기로 한다.

3.1 모바일 3D 애니메이션에 대한 워터마킹 프로토콜

제안한 워터마킹 시스템에서 사용되는 정보로는 표 1에서와 같이 구매자의 구매 번호 n_o, 실행키 k_B 및 모바일폰/시리얼 번호 n_B, 판매자의 저작권 정보 V이다.

표 1. 제안한 워터마킹 시스템에서의 워터마크 정보

워터마크 정보	구매 번호 n_o	저작권 정보 V	모바일폰/시리얼번호 n_B	실행키 k_B
생성자	판매자, WCA	판매자	WCA	구매자
워터마크	1차 워터마크	1차 워터마크	2차 워터마크	-
삽입영역	공간영역	공간영역	암호화영역	실행코드

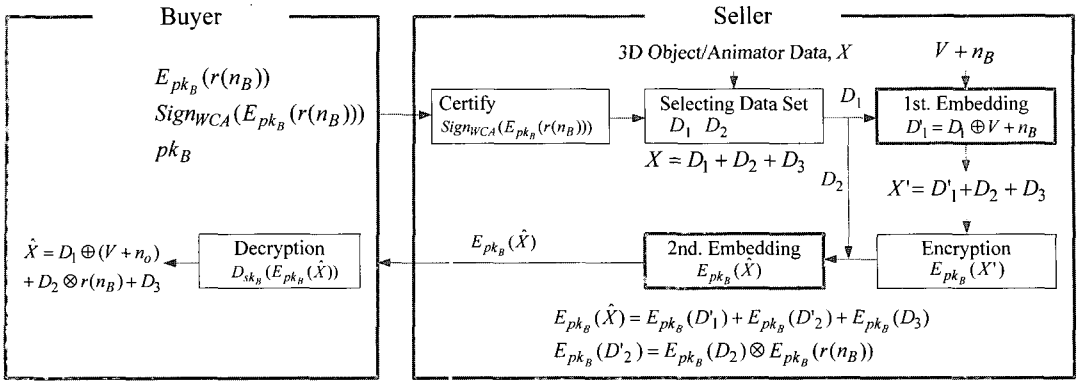


그림 3. 판매자와 구매자 사이에서의 워터마킹 프로토콜

제안한 시스템에서는 우선 구매자는 키 (pk_B, sk_B)를 생성한 후, WCA에 구매자의 신원 I_B, 공개키 pk_B 및 모바일폰/시리얼 번호 n_B를 전달한다. WCA는 I_B를 확인한 후, 구매자의 모바일폰/시리얼 번호 $\boldsymbol{n_B}$를 랜덤 함수 $r_{WCA}()$에 의하여 치환 $r_{WCA}(\boldsymbol{n_B})$한 다음, 이를 암호화하여 $E_{pk_B}(r_{WCA}(\boldsymbol{n_B}))$ 및 $Sign_{WCA}(E_{pk_B}(r_{WCA}(\boldsymbol{n_B})))$를 구매자에게 전달한다. 구매자는 판매자에게 pk_B, $E_{pk_B}(r_{WCA}(\boldsymbol{n_B}))$, $Sign_{WCA}(E_{pk_B}(r_{WCA}(\boldsymbol{n_B})))$ 및 구매자의 실행키 k_B를 전달하면, 판매자는 워터마크의 유효성 $Sign_{WCA}(E_{pk_B}(r_{WCA}(\boldsymbol{n_B})))$을 확인한다. 그리고 3D 애니메이션 콘텐츠 X의 데이터들 중 임의의 데이터 집합 $\mathbf{D}_1$ 및 $\mathbf{D}_2$를 선택하여, 데이터 집합 $\mathbf{D}_1$ 내에 저작권 정보 ($\boldsymbol{V}$) 및 구매자의 구매번호 ($\boldsymbol{n_o}$)의 1차 워터마크 $\boldsymbol{W_1} = \boldsymbol{V} + \boldsymbol{n_o}$를 공간 영역 내에 삽입하여 1차 워터마크된 콘텐츠 $\boldsymbol{X'} = \mathbf{D}'_1 + \mathbf{D}_2 + \mathbf{D}_3$, $\mathbf{D}'_1 = \mathbf{D}_1 \odot \mathbf{W}_1$를 얻는다. 그런 다음 $\boldsymbol{X'}$를 pk_B에 의하여 암호화한 후

$E_{pk_B}(\boldsymbol{X'}) = E_{pk_B}(\mathbf{D}'_1) + E_{pk_B}(\mathbf{D}_2) + \mathrm{E}_{\mathrm{pk_B}}(\mathbf{D}_3)$,

$E_{pk_B}(r_{WCA}(\boldsymbol{n_B}))$를 암호화된 데이터 집합 $E_{pk_B}(\mathbf{D}_2)$ 내에 선형 결합, 2차 워터마크 및 암호화된 콘텐츠 $E_{pk_B}(\hat{\mathbf{X}})$을 $E_{pk_B}(\mathbf{D}'_2) = E_{pk_B}(\mathbf{D}_2) \oplus \mathrm{E}_{\mathrm{pk_B}}(\mathrm{r}_{\mathrm{WCA}}(\mathbf{n_B}))$으로 선형 결합하여 2차 워터마크 및 암호화된 콘텐츠 $E_{pk_B}(\hat{\mathbf{X}})$을

$$\begin{aligned} E_{pk_B}(\hat{\boldsymbol{X}}) &= E_{pk_B}(\mathbf{D}'_1) + E_{pk_B}(\mathbf{D}'_2) + E_{pk_B}(\mathbf{D}_3) \\ &= E_{pk_B}(\mathbf{D}_1 \odot (\mathrm{V} + \mathrm{n}_o) + \mathbf{D}_2 \oplus r_{WCA}(n_B) + \mathbf{D}_3) \end{aligned} \quad (4)$$

와 같이 얻는다. 따라서 판매자는 $E_{pk_B}(\hat{\boldsymbol{X}})$와 구매자의 실행키 k_B를 콘텐츠 실행 코드 내에 탑재하여 구매자에게 최종 전달한다. 구매자는 sk_B에 의하여 복호화 $D_{sk_B}(E_{pk_B}(\hat{\boldsymbol{X}}))$하여 다중 워터마크된 애니메이션 $\hat{\boldsymbol{X}} = (\boldsymbol{X} \odot (\boldsymbol{V} + \boldsymbol{n_o})) \oplus r_{WCA}(\boldsymbol{n_B})$를 얻은 후, 실행키 k_B에 의하여 $\hat{\boldsymbol{X}}$를 실행한다. 여기서 $\odot$ 및 $\oplus$는 공간 영역 내에 삽입 연산자 및 암호화 영역 내에 삽입 연산자이다. 암호화 영역 내에 삽입 연산자 $\oplus$는 워터마킹 기법에 따라 'privacy homomorphism'을 만족하는 더하기, 곱하기, 빼기 등이 될 수 있다. 이상과 같이 판매자와 구매자 사이에서의 워터마킹 프로토콜은 그림 3에서와 같다. 판매자의 공간영역 상에서의 1차 워터마크 삽입 및 암호화 영역 상에서의 2차 워터마크 삽입 과정은 다음 절에 자세히 설명된다.

본 시스템에서는 WCA가 믿을만한 거래처라 가정하였을 때, 판매자는 구매자의 정보를 알지 못하므로 구매자의 익명성을 보장할 수 있다. 그리고 구매자는 다중 워터마크된 애니메이션의 삽입 유무 및 위치를 알지 못하므로 워터마크 정보 ($\boldsymbol{n_o}$, $\boldsymbol{V}$, $\boldsymbol{n_B}$)를 추출할 수 없다. 다중 워터마크된 애니메이션 $\hat{\boldsymbol{X}}$에 대하여 저작권 분쟁이 발생하였을 경우, 판매자는 $\hat{\boldsymbol{X}}$ 내에 있는 1차 워터마크를 공간 영역 상에서 추출하여 저작권 정보 $\boldsymbol{V}$와 구매 번호 $\boldsymbol{n_o}$를 확인한다. 그런 다음 암호화 영역 내 삽입 연산자에 해당되는 추출 방법에 의하여 2차 워터마크 $r_{WCA}(\boldsymbol{n_B})$를 추출한다. 판매자는 추출된 구매 번호 $\boldsymbol{n_o}$ 및 $r_{WCA}(\boldsymbol{n_B})$를 WCA에 전달하면, WCA는 랜덤 함수 $r_{WCA}()$에 의하여 모바일폰/시리얼 번호 $\boldsymbol{n_B}$를 추출하여 구매 번호 $\boldsymbol{n_o}$의 정보와 일치하는지 확인함으로써 불법 배포한 구매자를 추적한다.

3.2 공간 영역 상에서의 워터마크 삽입

본 절에서는 그림 3에서 나타나듯이 판매자에서 저작권 정보 (V) 및 구매자의 구매번호 (n_o)의 1차 워터마크를 삽입하는 방법에 대하여 살펴보기로 한다. 제안한 방법은 평균치 기반의 워터마크 삽입 방법[16]을 기반으로 한다. 우선 두 정보 $V+n_0$를 아스키 코드 $A(V+n_0)$로 변환한 후 비트열 $\mathbf{B}=\{b_i|i\in[1,N_1]\}$로 생성한다. 생성된 비트열을 랜덤 치환 $r_S(\mathbf{B})$하여 이를 1차 워터마크 $W_1=r_S(\mathbf{B})=\{w_i|i\in[1,N_1]\}$로 사용한다. 그런 다음 그림 1에서와 같은 3D 객체 데이터 (GSO) 또는 3D 움직임 데이터 (GA)들 중 $2n\times N_1$개 데이터들의 집합 D_k을 m개 선택하여 이들 데이터 집합들 $\mathbf{D}_1=\{\mathrm{D}_{1k}|\mathrm{k}\in[1,\mathrm{m}]\}$에 1차 워터마크를 삽입한다. 즉, N_1비트의 1차 워터마크 W_1는 m개의 데이터 집합 $\mathbf{D}_1=\{\mathrm{D}_{1k}|\mathrm{k}\in[1,\mathrm{m}]\}$에 m번 반복하여 삽입된다. 이 때 데이터 집합 $\mathbf{D}_1$의 시작 주소를 가지는 인덱스 $\mathrm{I}_1=\{\mathrm{I}_{1k}|\mathrm{k}\in[1,\mathrm{m}]\}$은 워터마크 추출하기 위하여 저장된다. 임의의 데이터 집합 $D_{1k\in[1,m]}=\{d_i|i\in[I_{1k},I_{1k}+2n\times N_1]\}$ 내에 워터마크 비트를 삽입하기 위한 방법에 대하여 살펴보기로 한다. 제안한 방법에서는 하나의 워터마크 비트 $w_{i\in[1,N_1]}$를 $2n$개의 데이터 분포에 각각 삽입한다. 즉, 좌우 n개 데이터들의 평균값 m_{i1} 및 m_{i2}를

$$m_{i1}=\sum_{x=I_k+i*2n}^{I_k+i*2n+n}\frac{d_x}{n},\quad m_{i2}=\sum_{x=I_k+i*2n+n+1}^{I_k+i*2n+2n}\frac{d_x}{n} \tag{5}$$

와 같이 구한 후, 워터마크 비트 $w_{i\in[1,N_1]}$가 1이면 두 평균값이 $m_{i1}>m_{i2}$이 되도록 하고, 워터마크 비트 $w_{i\in[1,N_1]}$가 0이면 두 평균값이 $m_{i1}<m_{i2}$이 되도록 한다. 워터마크 비트에 따라 두 평균값을 변경하기 위하여 각 데이터들의 값을 다음과 같이 변경한다.

IF $w_{i\in[1,N_1]}$=1 and $m_{i1}<m_{i2}$, Then

$$m'_{i1}=m_{i1}+\alpha\cdot e=\sum_{x=I_k+i*2n}^{I_k+i*2n+n}\frac{d_x+\alpha\cdot e}{n} \tag{6}$$

$$m'_{i2}=m_{i2}-\alpha\cdot e=\sum_{x=I_k+i*2n+n+1}^{I_k+i*2n+2n}\frac{d_x-\alpha\cdot e}{n} \tag{7}$$

IF $w_{i\in[1,N_1]}$=0 and $m_{i1}>m_{i2}$, Then

$$m'_{i1}=m_{i1}-\alpha\cdot e=\sum_{x=I_k+i*2n}^{I_k+i*2n+n}\frac{d_x-\alpha\cdot e}{n} \tag{8}$$

$$m'_{i2}=m_{i2}+\alpha\cdot e=\sum_{x=I_k+i*2n+n+1}^{I_k+i*2n+2n}\frac{d_x+\alpha\cdot e}{n} \tag{9}$$

여기서 α는 삽입 강도를 나타낸 것으로, 워터마크 삽입 조건을 만족하기 위하여 $\alpha>1/2$이어야 한다. 하나의 워터마크 비트를 삽입하기 위하여 $2n$개의 데이터가 위의 방법에 따라 변경되어지므로, 워터마크의 비가시성이 문제가 될 수 있다. 따라서 제안한 방법에서는 삽입강도를 결정하기 위하여 $\alpha>1/2$이며, PSNR이 40dB 이상이 되도록 실험적으로 α를 0.7로 결정하였다. 이상과 같은 방법으로 워터마크 비트 $w_{i\in[1,N]}$를 m개의 데이터 집합 $\mathbf{D}_1=\{\mathrm{D}_k|\mathrm{k}\in[1,\mathrm{m}]\}$에 각각 삽입한다.

3.3 암호화 영역 상에서의 워터마크 삽입

제안한 방법에서는 1차 워터마크된 X'를 암호화 $E_{pk_B}(X')$하여, $E_{pk_B}(X')$ 내에 암호화된 2차 워터마크 $E_{pk_B}(r_{WCA}(n_B))$를 삽입한다. 이 때, 암호화 영역 내에서 워터마크를 삽입하기 위하여 식 (2)에서 같은 'privacy homomorphism' 성질을 만족하여야 하며, 또한 워터마크 추출시 원 데이터가 필요없어야 한다. Memon 등은 2D 영상의 암호화 영역에서 워터마크를 삽입하기 위하여 Cox 등이 제안한 DCT 기반의 대역확산기법을 이용하였다. 그러나 이 방법은 워터마크 추출시 원 데이터가 필요한 단점이 있다. 기존의 3D 모델에 대한 워터마킹 기법들이 많이 제안되어지고 있으나, 이들 모두 'privacy homomorphism'를 만족하지 못한다. 따라서 제안한 방법에서는 위의 두 조건을 만족하기 위하여 더하기, 곱하기 연산에 대한 'privacy homomorphism'를 만족하는 RSA 기반으로 임의의 데이터 내의 특정 비트에 워터마크를 삽입한다. 이 때 삽입 방법은 비트 치환 기법[17]에 기반한다.

$r_{WCA}(n_B)$는 WCA에서 구매자의 모바일폰/시리얼 번호 n_B를 ASCII 코드로 변환한 후, 랜덤함수 $r_{WCA}()$에 의하여 치환된 비트열 $r_{WCA}(n_B)=\{r_i|i\in[1,N_2]\}$이다. 우선, 1차 워터마크된 X' 내에 N_2개의 데이터 원소를 가지는 데이터 $D_{2k}=\{d_i|i\in[1,N_2]\}$들을 m개 선택하여 2차 워터마크의 삽입 대상 데이터 집합 $\mathbf{D}_2=\{\mathrm{D}_{2k}|\mathrm{k}\in[1,\mathrm{m}]\}$를 선택한다. 이 때, 데이터 집합 $\mathbf{D}_2$의 시작 주소 $\mathrm{I}_2=\{I_{2k}|k\in[1,m]\}$는 워터마크 추출시 필요한 정보이다. 임의의 데이터 집합 $D_{2k}=\{d_i|i\in[I_{2k},I_{2k}+N_2]\}$ 내에 모든 원소들의 t번째 비트들을 모두 0으로 놓

은 후, D_{2k}를 암호화한다.

암호화된 2차 워터마크 $E_{pk_B}(r_{WCA}(\boldsymbol{n_B}))=\{E_{pk_B}(r_i)|i\in[1,N_2]\}$는 각 원소 $E_{pk_B}(r_i)$에 $E_{pk_B}(2^t)$를 곱한 후, 암호화된 집합 $E_{pk_B}(D_{2k})=\{E_{pk_B}(d_i)|i\in[I_{2k},I_{2k}+N_2]\}$의 각 원소 $E_{pk_B}(d_i)$에

$$E_{pk_B}(d'_i)=E_{pk_B}(d_i)+E_{pk_B}(2^t)\cdot E_{pk_B}(r_i) \quad (10)$$
$$=E_{pk_B}(d_i+2^t\cdot r_i)$$

와 같이 더하여진다. $E_{pk_B}(r_{WCA}(\boldsymbol{n_B}))$를 위 식에 따라 $\mathbf{D}_2=\{\mathrm{D}_{2k}|\mathrm{k}\in[1,\mathrm{m}]\}$에 m번 반복하여 삽입하여 2차 워터마크가 삽입된 $E_{pk_B}(\mathbf{D'}_2)=\{E_{pk_B}(D'_{2k})|k\in[1,m]\}$를 얻는다. 판매자는 최종 워터마크된

$$E_{pk_B}(\hat{\boldsymbol{X}})=E_{pk_B}(\mathbf{D'}_1)+E_{pk_B}(\mathbf{D'}_2)+E_{pk_B}(\mathbf{D}_3)$$
$$=E_{pk_B}(\mathbf{D'}_1+\mathbf{D'}_2+\mathbf{D}_3) \quad (11)$$

를 구매자에게 전달한다. 위의 방법을 공간 영역 상에서 살펴보면, $r_{WCA}(\boldsymbol{n_B})$의 각 비트 r_i를 2^t배하여 데이터 집합의 각 원소 d_i에 더함으로써 워터마크가 삽입된 데이터 집합

$$D'_{2k,k\in[1,m]}=\{d'_i=d_i+2^t\cdot r_i|i\in[1,N_2]\} \quad (12)$$

을 구하는 것으로 각 데이터의 t번째 비트에 r_i를 삽입하는 것과 같다. 구매자는 판매자에게 전달받은 $E_{pk_B}(\hat{\boldsymbol{X}})$를 복호키 sk_B를 이용하여 복호하여 다중 워터마크된 $\hat{\boldsymbol{X}}$를 얻는다.

3.4 워터마크 추출

모바일 3D 애니메이션에 대한 저작권 분쟁이 발생시, 우선 판매자는 의심되는 컨텐츠 $\hat{\boldsymbol{X}}^*=\mathbf{D}_1^*+\mathbf{D}_2^*+\mathbf{D}_3^*$ 내에 인덱스 $\mathrm{I}_1=\{\mathrm{I}_{1k}|\mathrm{k}\in[1,\mathrm{m}]\}$을 이용하여 저작권 정보 $\boldsymbol{V}$ 및 구매 번호 $\boldsymbol{n_o}$의 1차 워터마크가 삽입된 데이터 집합 $\mathbf{D}_1^*=\{\mathrm{D}_{1k}^*|\mathrm{k}\in[1,\mathrm{m}]\}$를 획득한다. 그리고 각 데이터 집합 $D^*_{k\in[1,m]}=\{d_i|i\in[I_{1k},I_{1k}+2n\times N_1]\}$ 내에 워터마크 비트 $W_k^*=\{w_{ki}^*|i\in[1,N_1]\}$를 추출한다. 즉, i번째 워터마크 비트 w_{ki}^*는 $2n$개의 데이터 원소들 $\{d_x|x\in\{I_k+i\times 2n,I_k+i\times(2n+1)\}\}$중, 좌우 n개 데이터들의 평균값 m_{i1} 및 m_{i2}를 구한 후, $m_{i1}>m_{i2}$이면 w_{ki}^*=1이고, $m_{i1}<m_{i2}$이면 w_{ki}^*=0이다. m개의 데이터 집합 내에 m개의 워터마크 비트들을 모두 추출한다. 최종 추출된 워터마크 비트 $\hat{W}=\{\hat{w}_i|i\in[1,N_1]\}$는 $\hat{w}_i=\mathrm{INT}(\sum_{k=1}^{m}w_{ki}^*/m+0.5)$이다. 판매자는 추출된 워터마크를 역치환 $r^{-1}(\hat{\boldsymbol{W}})=\boldsymbol{B}$하여, 아스키 코드에 해당되는 저작권 정보 $\boldsymbol{V}$ 및 구매 번호 $\boldsymbol{n_o}$를 확인한다.

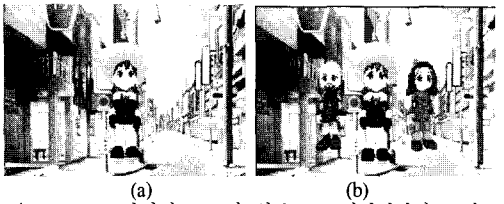
또한 2차 워터마크 $r_{WCA}(\boldsymbol{n_B})=\{r_i|i\in[1,N_2]\}$를 추출하기 위하여 인덱스 $\mathrm{I}_2=\{\mathrm{I}_{2k}|\mathrm{k}\in[1,\mathrm{m}]\}$를 이용하여 두 번째 데이터 집합 $\mathbf{D}_2^*=\{\mathrm{D}_{2k}^*|\mathrm{k}\in[1,\mathrm{m}]\}$를 획득한다. 그리고 각 데이터 집합 $D^*_{k\in[1,m]}=\{d_i^*|i\in[I_{2k},I_{2k}+N_2]\}$ 내에 각 원소 d_i^*의 t번째 비트가 r_{ki}^*이다. 즉, $r_{ki}^*=(d_i^*\,\&\,2^t)\gg t-1$이다. 여기서 &는 비트곱이고, >>는 우측 비트쉬프트 연산이다. m개의 데이터 집합 내에 m개의 비트들을 모두 추출하여, 최종 추출된 2차 워터마크 $r^*_{WCA}(\boldsymbol{n_B})=\{r_i^*|i\in[1,N_2]\}$, $r_i^*=\sum_{k=1}^{m}r_{ki}^*/m$를 얻는다. 판매자는 추출된 $r^*_{WCA}(\boldsymbol{n_B})$를 WCA에 전달하며, WCA는 역치환 $r_{WCA}^{-1}(\cdot)$하여 구매자의 모바일폰/시리얼 번호 $\boldsymbol{n_B}$를 확인한다.

Ⅳ. 실험 결과

본 장에서는 Buyer-Seller 워터마킹 프로토콜 상에서 제안한 다중 워터마크 삽입 구현 및 실험 결과에 대하여 살펴보기로 한다. 본 실험에서는 제안한 방법의 구현을 위하여 G3 SDK에서 제공하는 Pino,

표 1. GSO/GA 데이터의 개수 및 삽입된 워터마크 비트수

모델명		Pino	Vincent	Brianna
GSO 데이터 개수		65,243	57,196	73,912
GA 데이터 개수		93,968	140,408	140,408
1차 워터마크 $\boldsymbol{V}+\boldsymbol{n_o}$	비트수 N_1	160bit	184bit	184bit
	삽입 데이터 개수 $\mathbf{D}_1$	2,880	3,312	3,312
2차 워터마크 $\boldsymbol{n_B}$	비트수 N_1	88bit	88bit	88bit
	삽입 데이터 개수 $\mathbf{D}_2$	264	264	264



(a) (b)

그림 4. LCD 화면에 로드된 원본 3D 애니메이션 모델 (a) Pino 및 (b) Pino, Brianna와 Vincent

Vincent, Brianna의 테스트 모델을 이용하였다. 실험에 사용된 저작권 정보 V는 "TUTest0603"의 10자리 문자와 3D 캐릭터명이고, 사용자의 구매번호 n_o 및 폰번호 n_B는 임의의 6자리 및 11자리 숫자이다. 화면에 로드된 Pino, Vincent, Brianna의 모델들은 그림 4에서와 같다. 본 실험에서는 이들을 각각 ASCII 코드(8bit)로 변환하여 생성된 비트열을 워터마크로 사용하였다. 각 테스트 모델에 대한 3D 오브젝트 데이터 (GSO) 및 애니메이터 데이터 (GA)의 개수와 삽입되는 워터마크 비트수 및 삽입 대상 데이터 개수는 표 1에서와 같다. 본 실험에서는 1차 워터마크 삽입 대상 집합 D_1으로 $2n \times N_1$ ($n=3$)개의 원소를 가지는 데이터 집합을 3개 선택하였고, 2차 워터마크 삽입 대상 집합 D_2으로 N_2개의 원소를 가지는 데이터 집합을 3개 선택하였다. 그리고 각각의 워터마크를 각 모델의 3D 오브젝트 데이터 (GSO) 및 애니메이터 데이터 (GA) 내에 각각 삽입하였다.

4.1 워터마크된 모바일 애니메이션 게임 구현

판매자 측에서 G3 SDK 기반의 모바일 3D 애니메이션 게임 설계 시 다중 워터마크를 삽입하기 위한 과정은 그림 5에서와 같이 공간 상에서의 1차 워터마크 삽입, 애니메이션 게임 로드, 및 암호화 영역 상에서의 2차 워터마크 삽입 단계로 나누어진다. 첫 번째 단계인 1차 워터마크 삽입 과정에서 화면 세트 (Surface Set)는 모바일 LCD 화면의 크기에 대응되는 가상 프레임 버퍼를 생성하여 이 버퍼를 LCD 화면에 설정한다. 본 실험에서는 176×240 크기의 가상 프레임 버퍼를 설정하여 이 버퍼 상에 3D 오브젝트, 텍스쳐, 애니메이터 데이터 등이 나타나도록 하였다. 화면 세트 후 WCA에서 전달받은 암호화된 2차 워터마크 $Sign_{WCA}(E_{pk_B}(r_{WCA}(n_B)))$의 유효성을 확인한 다음 3D 애니메이션 모델 데이터 X 내에 1차 워터마크 $V+n_o$를 삽입한다.

두 번째 단계인 애니메이션 게임 로드에서는 3D 작업을 위한 영역 생성, 뷰포트 설정, OpenGL 수행을 위한 초기화 등의 게임 초기화 (Init Game)를 먼저 수행한뒤 SynchFrame에 의하여 3D 그래픽스가 그려지는 총 프레임 비율을 조정한다. 그리고 구

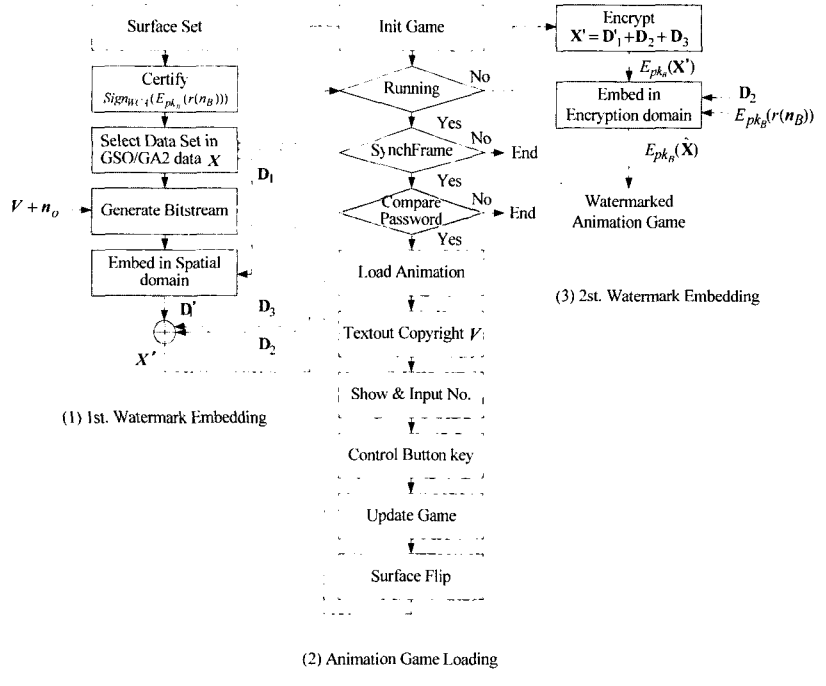
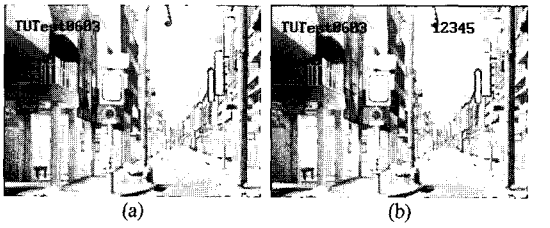


그림 5. 제안한 모바일 3D 애니메이션 게임 상에서의 워터마크 삽입 과정

매자가 등록한 실행키 k_B가 모바일폰의 버튼에 의하여 입력된 숫자 또는 글자와 일치하면 애니메이션 데이터를 로드한다. 이 때 사용자가 입력한 숫자 또는 글자는 화면에 나타나도록 하고, 또한 판매자의 저작권 정보 V를 화면 상단에 나타나도록 한다. 로드된 애니메이션 데이터들이 좌우상하 이동, 회전, 확대 및 축소, 정지, 플레이 등의 동작을 수행되도록 버튼키를 설정한다. 동작 버튼키에 의하여 수행된 애니메이션은 Update Game에 의하여 반영되며, Surface Flip에 의하여 화면에 출력된다. 애니메이션 게임이 로드된 후, 1차 워터마크된 애니메이션 데이터 X'를 암호화 $E_{pk_B}(X')$하여, $E_{pk_B}(X')$ 내에 암호화된 2차 워터마크 $E_{pk_B}(r_{WCA}(n_B))$를 삽입함으로써 최종 워터마크된 애니메이션 데이터 $E_{pk_B}(\hat{X})$를 생성한다. 판매자는 워터마크된 애니메이션 데이터가 탑재된 모바일 애니메이션 게임을 구매자에게 전달하게 된다. 모바일 단말기 환경에서 제안한 워터마킹을 구현하기 위하여 본 실험에서는 WCA에서 제공한 $r_{WCA}(n_B)$ 대신 임의의 11자리 모바일폰 번호 n_B를 암호화하여 2차 워터마크로 사용하였다.

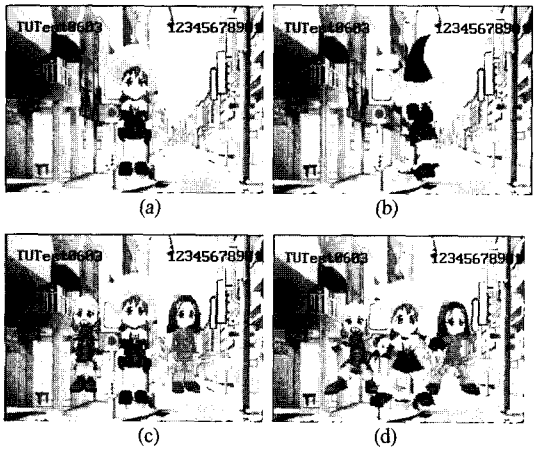
4.2 실행키에 의한 애니메이션 로드

제안한 방법에서는 모바일 3D 콘텐츠 보호를 위하여 초기 실행을 할 때 바로 애니메이션이 실행되는 것이 아니라 그림 5에서의 두 번째 단계에 의하여 구매자가 이미 등록한 실행키와 모바일폰의 버튼에 의하여 입력한 키가 동일할 경우에만 애니메이션이 로드된다. 제안한 방법에 의하여 워터마크가 삽입된 모바일 3D 애니메이션 게임의 초기 실행시 그림 6의 (a)에서 같이 가시적으로 저작권 정보 "TUTest0603" 삽입된 배경 화면이 나타난다. 다음으로 3D 애니메이션 모델을 로드하기 위하여 구매자가 등록키를 입력해야 하며, 이 때 그림 6의 (b)에서와 같이 LCD 화면에 입력한 키가 나타난다. 여기서 등록키 k_B는 임의의 11자리 숫자를 사용하였고 등록키 파일을 생성하여 프로그램 실행 시 읽어 들인다. 등록키가 동일하지 않을 경우에는 3D 애니메이션 모델이 로드되지 않으며 게임이 실행되지 않는다. 등록키 실행 후 구매자가 복호키 sk_B를 이용하여 $E_{pk_B}(\hat{X})$를 복호하면 그림 7의 (a)에서 같이 워터마크된 애니메이션 모델이 로드된다. 이 때 모델은 정지된 상태이며 지정된 버튼키에 따라 그림 7 (b)에서와 같이 모델이 동작된다.



(a) (b)

그림 6. (a) 프로그램 실행 시 LCD 초기 화면 및 (b) 실행키 입력시 LCD 화면



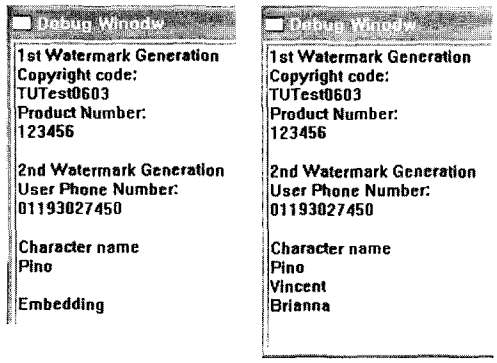
(a) (b) (c) (d)

그림 7. 구매자가 실행키 입력 및 복호과정 후 (a) 3D 애니메이션 로드 화면 및 (b) 동작 화면과 3D 애니메이션 모델이 하나 이상일 때의 (c) 로드 화면 및 (d) 동작 화면

4.3 워터마크 삽입/추출 화면

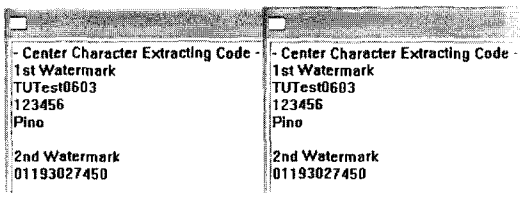
워터마크 삽입 및 추출 과정들은 G3 에뮬레이터의 디버깅 창에서 확인한다. 애니메이션 모델이 하나일 경우와 하나 이상일 경우에 각 모델에 대하여 1차 및 2차 워터마크 삽입 정보를 나타내는 디버깅 창은 그림 8의 (a) 및 (b)에서와 같다. 이 그림을 살펴보면, 우선 저작권 정보, 캐릭터명 및 구매 정보가 표시된 후 비트열로 변환되어 각 모델의 1차 데이터 집합 상에 각각 삽입된다. 그런 다음, 구매자가 등록한 실행키를 저장한 후, 각 캐릭터를 암호화하여 암호화 영역에서 2차 워터마크가 삽입된다.

워터마크 추출은 판매자 또는 개발자만이 알 수 있는 단말기 내에 일련의 버튼키 입력에 의하여 동작된다. 본 실험에서는 추출을 위한 일련의 버튼키를 프로그램 상에서 지정한 키를 사용하고 키보드 입력 또는 G3 에뮬레이터의 스킨을 적용하여, 디버깅 창에서 확인하도록 하였다. 3D 모델이 하나일 경우와 하나 이상일 경우에 워터마크 추출 화면에서는 그림 9에서와 같이 저작권 정보, 캐릭터명, 구매자의 휴대폰번호가 나타난다.



(a) (b)

그림 8. (a) 3D 모델이 하나일 때 워터마크 삽입 확인 정보 및 (b) 3D 모델이 하나 이상일 때 워터마크 삽입 확인 정보



(a) (b)

그림 9. (a) 3D 모델이 하나일 때 추출된 다중 워터마크 정보 및 3D 모델이 하나 이상일 때 (b) 중간 모델에서 추출된 워터마크 정보

4.4 비가시성 및 견고성 실험

본 실험에서는 워터마크의 비가시성을 확인하기 위하여 각 데이터 값들에 대한 PSNR= $10\log_{10}(MAX^2/\sum_{i=1}^{N}(d_i-d'_i)^2)$을 사용하였다. 여기서 MAX는 워터마크 삽입 대상 집합 내의 데이터 값 중 최대값이고, N은 각 모델의 데이터 개수를 나타낸다. 1차 및 2차 워터마크된 Pino, Vincent 및 Brianna 모델의 PSNR은 각각 39.8dB, 41.2dB 및 42.1dB이다. 그림 7의 다중 워터마크된 애니메이션 모델이 로드된 화면과 그림 6의 원 모델이 로드된 화면을 살펴보면 워터마크의 비가시성을 확인할 수 있다.

구매자는 모바일 단말기 상에서의 3D 애니메이션 게임 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 검출 유무를 판단하였다. 견고성 실험에서는 GSO 또는 GA 데이터에 랜덤 잡음, 데이터 정밀도 가변, 데이터 삭제, 확대, 축소 등을 수행하였다. 여기서 랜덤 잡음 실험에서는 모든 데이터 값들을 $d'=d\times(1+\alpha\times uniform())$로 변경하였다. 여기서 α는 변조도이며, uniform()는 [-0.5 0.5]의 범위를 가지는 균등한 랜덤 함수이다. 데이터 정밀도 가변 실험에서는 데이터 값들을 [-3, 3] 범위 내의 임의의 값을 더하였다. 즉, 데이터의 정밀도가 ±3이내이다. 데이터 삭제에서는 임의의 데이터만큼 삭제하였으며, 확대 및 축소는 데이터 값에 임의의 비율만큼 곱하였다. 실험 결과로는 표 2에서와 같으며, 추출된 데이터의 비트 오류가 없는 경우에서만 검출됨을 확인하였다. 랜덤 잡음 ($\alpha=0.5$) 및 데이터 정밀도 가변에서는 모든 워터마크가 오류없이 검출되었으나, 데이터 삭제에서는 1차 워터마크의 비트 오류가 발생되었다. 이는 1차 워터마크의 삽입 대상 집합이 2차 워터마크의 대상 집합보다 10배 이상 많으므로 데이터 삭제에 포함될 경우가 많기 때문이다. 그러나 두 워터마크의 대상 집합 내에 데이터가 삭제되면 워터마크 비트가 발생될 것이다. 이는 워터마크를 여러 위치에 동시에 삽입할 경우 데이터 삭제와 같은 공격에 대하여 강인할 수 있으나, 삽입 대상 집합의 데이터 개수가 증가될 것이다. 그리고 1차 워터마크 삽입 방법은 데이터 분포 상에 삽입되므로 확대 및 축소에는 강인하다. 그러나 2차 워터마크는 임의의 특정 비트에 삽입되므로 원 데이터에 비하여 확대 및 축소된 비율을 알지 못하면 검출되지 못함을 알 수 있다. 이는 원 데이터 비율로 스케일링 과정을 수행하면 확대 및 축소에서 비트 오류가 발생되지 않을 것이다.

표 2. 공격에 대한 워터마크 검출 여부

공격	Pino		Vincent		Brianna		비고
	1차 워터마크	2차 워터마크	1차 워터마크	2차 워터마크	1차 워터마크	2차 워터마크	
랜덤 잡음 ($\alpha=0.5$)	○	○	○	○	○	○	
데이터 정밀도 가변 (±3)	○	○	○	○	○	○	
데이터 삭제	×	○	×	○	×	○	애니메이션 로드 안됨
확대	○	×	○	×	○	×	
축소	○	×	○	×	○	×	

V. 결 론

본 논문에서는 모바일 상에서 서비스되는 3D 애니메이션에 대한 저작권 보호 기술을 위하여 Buyer-Seller 워터마킹 프로토콜 기반의 다중 워터마크 삽입 방법을 제안하였다. 제안한 방법에서는

판매자 측에서 오브젝트 또는 애니메이터 데이터들 중 임의의 두 데이터 집합을 선택한다. 그리고 저작권 정보와 구매 번호의 1차 워터마크를 비트열로 생성한 후, 첫 번째 데이터 집합 내에 데이터 값 분포 상에 1차 워터마크 비트열을 삽입한다. 그리고 구매자에게 전달받은 암호화된 모바일폰 번호를 암호화된 두 번째 데이터 집합 내의 데이터 값과 선형 결합을 통하여 암호화 영역 상에서 이들을 삽입한다. 또한 인가된 사용자만 3D 애니메이션을 실행할 수 있도록 사용자의 등록한 실행키를 실행코드 내에 삽입하여 이를 구매자에게 전달한다. 본 실험에서는 모바일 3D 게임용 개발 도구인 G3-SDK를 이용하여 제안한 방법의 알고리즘을 구현하였다. 실험 결과로부터 모바일 3D 애니메이션 캐릭터의 저작권 보호와 불법 복제 방지가 가능함을 확인하였고, 랜덤 잡음, 데이터 정밀도 가변, 확대 및 축소 등에 대하여 워터마크가 검출됨을 확인하였다.

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 privacy homomorphism를 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. 모바일 3D 콘텐츠들을 모바일 환경 하에서 구현되어져야 하므로 기존의 3DS-Max 또는 Maya 등에서 구현한 3D 애니메이션 모델과는 데이터 특성이 다르고, 아직까지 이들에 대한 워터마킹 기술이 매우 미흡하다. 향후에는 모바일 3D 콘텐츠에 대한 공격 형태 및 비가시성을 평가하기 위한 척도 등이 연구되어져야 할 것이다.

참 고 문 헌

[1] 정일홍, "모바일 3D 기술 현황과 3D 아바타," *한국멀티미디어학회지*, 제8권 1호, pp. 27-34, 2004.

[2] D. Lukashev and A. Puresev, "3D Applications for 3G Mobile Phones: Design, Development, Resource Utilization," *IEEE Tenth International Symposium on Consumer Electronics, ISCE '06*, pp. 1-4, June 2006.

[3] R. Ohbuchi, H. Masuda, and M. Aono, "Watermarking Three-Dimensional Polygonal Models," *Proceedings of the ACM Multimedia*, pp. 261-272, 1997.

[4] O. Benedens, "Geometry-Based Watermarking of 3D Models," *IEEE Computer Graphics and Applications*, pp. 46-55, 1999.

[5] 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, Feb. 2005.

[6] 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, May 2005.

[7] 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, Oct. 2006.

[8] N. Memon and P.W. Wong, "A Buyer-Seller Watermarking Protocol," *IEEE Trans. on Image Processing*, Vol. 10, No. 4, April 2001.

[9] C.L. Lei, P.L. Yu, P.L. Tsai and M.H Chan, "An Efficient and Anonymous Buyer-Seller Watermarking Protocol," *IEEE Trans. on Image Processing*, Vol. 13, No. 12, Dec. 2004.

[10] I.J. Cox, J. Kilian, T. Leighton and T. Shammon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Processing*, vol. 6, pp. 1673-1687, Dec. 1997.

[11] G3 SDK, http://www.gomid.com

[12] NF3D, http://www.nf3d.co.kr

[13] M3D, http://www.rekosys.co.kr

[14] ISO/IEC 14772-1, The virtual reality modeling language.

[15] ISO/IEC 14496-1, Coding of Audio-Visual Objects-Part 1: Systems, 2001.

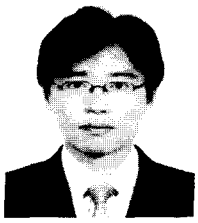
[16] Z. Guannan, W. Shuxun, and W. Quan, "An adaptive block-based blind watermarking algorithm," *International Conference on Signal Processing*, vol. 3, pp. 2294-2297, 2004.

[17] B. G. Mobasseri, "Exploring CDMA for Watermarking of Digital Video," *Proc. SPIE*, vol. 3657, pp. 96.102, Jan. 1999.

권 성 근 (Seong-Geun Kwon) 정회원

1996년 2월 : 경북대학교 전자공학과 공학사
1998년 2월 : 경북대학교 전자공학과 공학석사
2002년 2월 : 경북대학교 전자공학과 공학박사
2002년~현재 : 삼성전자 책임연구원
<관심분야> 영상신호처리, 영상통신, 정보보호

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

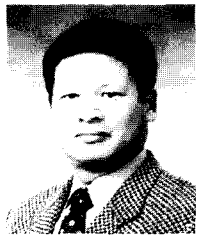
배 성 호 (Sung-Ho Bae) 정회원

1991년 2월 : 경북대학교 전자공학과 공학사
1993년 2월 : 경북대학교 전자공학과 공학석사
1997년 8월 : 경북대학교 전자공학과 공학박사
1998년 8월~1999년 8월 : 삼성전자 무선통신사업부 책임연구원
1999년 9월~현재 : 동명대학교 멀티미디어공학과 부교수
<관심분야> 워터마킹, 영상신호처리, 컴퓨터비젼

박 재 범 (Jae Bum Park) 정회원

1989년~1994년 : Bachelor of Science (Computer Science) University of Southern California
1994년~1995년 : Master of Science (Computer Graphics) University of Southern California
1996년~2000년 : LG 종합 기술원 연구원
2000년~2002년 : 데이콤 대리
2002년~2004년 : 삼성전자 책임연구원
2004년~현재 : SKT Manager
<관심분야> DRM, 정보보호, Home Network

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