한국 CAD/CAM 학회 논문집
제 12권 제 2호 2007년 4월 pp. 95-100

기술논문

VR 환경에서 공동 소유권 증명을 위한 다중 워터마킹 프레임워크

조미성*, 손유승**

Multiple Digital Watermarking Framework for Joint-Creatorship Verification in VR Environment

Misung Cho* and Yuseung Sohn**

ABSTRACT

Virtual Reality(VR) data in VR environments like Manufacturing industries are often created jointly by many creators. It is then necessary to provide protection of the joint-creatorship and the creatorship of each participating creator. This paper proposes Multiple Digital Watermarking Framework(MDWF) to solve the problem of joint-creatorship. The proposed framework, MDWF, makes use of 3D private watermarking technology and a novel key sharing protocol for joint-creatorship verification. MDWF embeds 3D private multiple watermarks for the creatorship of each participating creators in a non-overlapping manner during the creation process. After key agreement of all private keys, MDWF embeds an additional 3D private watermark for the joint-creatorship. Therefore MDWF successfully handles the creatorship dispute among creators. That is, each participating creator can prove his/her partial creatorship as well as joint-creatorship by MDWF. In addition, MDWF can solve the collusion problems because shared secret key(SSK) can be made by every users.

Key words : Multiple Watermark, Joint-Creatorship, Secret Sharing Protocol

1. 서 론

디지털 컨텐츠의 제작 및 배포 기술과 통신 기술의 발달에 따라 많은 디지털 저작물들의 생성 및 유통이 증가하고 있으며 또한 분산환경에서의 협업 역시 증가하고 있는 상태이다. 그러나 이러한 디지털 저작물의 생성 및 유통 기술의 발달은 디지털 정보의 불법 복제 및 유출을 가능하게 하여 가치있는 자산으로 평가 받는 기업 정보와 같은 디지털 컨텐츠에 대한 정보 보호 기술 역시 발달하고 있다[1].

특히, 제조 기업 환경에서 사용되는 3D 데이터들은 보통 대용량이고 제작하는데 다양한 전문 기술을 포함하고 있으므로 종종 많은 사람들의 협업 및 분업에 의해서 제작된다. 협업으로 3D 데이터를 제작하는 경우 협업에 참여한 제작자들의 저작물에 대한 소유권 관련 문제가 중요한 이슈가 되고 있다. 첫째, 협업에 참여한 모든 제작자들은 자신이 제작한 데이터에 대한 소유권을 인정받길 원한다. 둘째, 협업에 참여한 모든 제작자들은 최종 결과물에 대한 공동의 소유권을 인정받길 원한다. 셋째, 협업에 참여한 일부 제작자들이 다른 제작자들의 소유권을 무시하고 전체 저작물의 소유권을 주장하여 판매하는 등의 행위를 방지하기를 원한다.

최근까지 공동 소유권 증명을 위한 워터마킹 방법[2,3]에 대한 연구는 아주 미미하다.

Guo와 Georganas는 공동 소유권 증명을 위한 이미지 워터마킹 방법을 소개하였다. 이 방법은 신뢰할 수 있는 분배자(Trusted Dealer)가 없는 상황에서 비밀키 공유를 통해 이미지 워터마크를 삽입/추출하는 것으로, 이미지에 특성화된 워터마킹 방법이다. 각 소유권자들의 워터마크와 비밀키 공유를 통해 생성된 공동 워터마크를 결합하여 삽입함으로써 전체 및 부분적인 소유권 주장이 가능하다. 그러나 이 방법은 몇 명의 소유권자들이 공모하여 전체 저작물에 대한 소유권을 주장할 수 있는 문제를 야기할 수 있다[4].

[5]에서 Zhang과 Emmanuel은 공동 소유권 주장을

*교신저자, (주)알티캐스트 δ-Project TFT
**(재)그래픽스연구원 정보보증팀
- 논문투고일: 2006. 03. 27
- 심사완료일: 2007. 01. 17

위한 워터마킹 프레임워크를 제안하였는데 이 방법은 작업에 참여한 저작권자가 자신이 만든 저작물에 각각 워터마킹을 삽입한 후 전자서명을 하는데 최종 결과물이 나올 때까지 데이터 수정의 각 단계마다 위의 과정을 반복하게 된다. 그러나 이 방법도 전체 저작물에 대한 단합의 문제가 발생할 수 있으며, 수정되는 각 단계에서 복잡한 연산을 필요로 하는 전자서명 프로토콜을 사용하기 때문에 연산에 대한 부하가 클 수 있다.

본 논문에서 제안하는 다중 워터마킹 프레임워크(Multiple Digital Watermarking Framework : MDWF)은 협업작업을 통해 3D 데이터를 생성하는 제작자들의 소유권 분쟁을 없애고 신뢰할 수 있는 관계를 제공하기 위한 것으로 협업을 통해 만들어진 전체 데이터의 생성에 자신이 기여한 부분에 대한 소유권을 증명할 수 있으면서 동시에 전체 저작물에 대한 공동의 소유권을 증명할 수 있도록 한다. 더욱이 전체 저작물에 대한 소유권 증명은 제작에 참여한 모든 사람들에 의해서만 이루어지므로 제작에 참여한 사람들의 단합을 방지할 수 있다. MDWF는 3D 데이터 생성 과정에 적용되며 3D 비밀 워터마킹(Private Watermarking) 기술과 비밀키 공유를 위한 키 공유(Key Sharing) 암호 프로토콜을 활용한다.

2. 3D 워터마킹

2.1 3D 워터마킹

워터마킹 기술은 적용되는 미디어 매체의 종류에 따라 분류되며 현재 이미지, 오디오, 비디오 워터마킹 기술이 주류를 이루고 있다. 그러나 최근 CAD 기반의 3D 데이터의 사용이 급증하고 가상공간에서 이러한 데이터를 활용한 제품의 판매 등이 증가하면서 이러한 데이터를 소유한 회사나 소유권자들의 소유권 관련 문제들이 발생하고 있다. 3D 기반 데이터의 불법 복제 및 배포 등의 문제 등은 3D 데이터에 저작권 소유자에 대한 신분증명 등의 정보를 삽입함으로써 방지할 수 있으며 이러한 소유권 증명을 위해 삽입되는 정보를 워터마크(Watermark)라고 한다. 또한 이러한 정보를 이용하여 소유권자는 불법적으로 데이터를 배포시킨 출처를 확인할 수 있게 된다.

워터마크 삽입이 가능한 VRML(Virtual Reality Modeling Language) 모델의 미디어 타입은 크게 오디오 샘플, 질감과 배경 이미지, 3D 기하학적 기반 데이터로 나눌 수 있다. 그러나 오디오 샘플과 질감, 배경이미지는 전체 VRML 데이터의 가치의 큰 손상없이 쉽게 제거할 수 있기 때문에 대부분의 3D 워터마킹 기술들에서 워터마크 삽입을 위해 3D 기하 기반 모델 데이터를 사용하고 있다.

일반적으로 워터마크는 비밀 워터마크(Private Watermark)와 공개 워터마크(Public Watermark)로 크게 나눌 수 있다. 비밀 워터마크는 분쟁 시 소유권을 증명하기 위해 소유권자의 신분 증명 등의 정보를 포함하며 이러한 비밀 워터마크 추출을 위해서는 오직 워터마크를 삽입한 사람만이 알 수 있는 비밀키를 알아야만 한다. 따라서 비밀 워터마킹 알고리즘에는 강인성(Robustness)이 요구된다. 반면 공개 워터마크는 보통 데이터를 수신하는 사람들에 의해 추출되므로 추출을 위해서 데이터에 의해 결정되는 특징키를 제외한 별도의 정보가 필요하지 않는다. 3D 모델 데이터에서 공개 워터마크는 형상 파일의 헤더나 섹션에 존재하게 된다. 따라서 공개 워터마킹 알고리즘에서는 강인성보다는 높은 수용력(Capacity)이 요구된다.

오디오, 비디오와 이미지 데이터와는 달리 3D 모델의 워터마킹 기술은 다음과 같은 요소들을 고려해야 한다.

- 3D 모델 데이터에 비해 상대적으로 작은 데이터 양
- 다양한 기하 또는 위상 연산
- 다양한 모델의 표현(Representation) 방법

2.2 3D 워터마킹 시스템의 요구사항

수용력(Capacity)과 강인성(Robustness) 이외에 3D 워터마킹 시스템 구현 시 요구되는 성질들은 다음과 같다.

- 백그라운드 처리와 처리속도 최소화
- 다중 워터마크(Multiple Watermark) 삽입 가능
- 사전 지식의 최소화
- 처리 부하의 최소화

2.3 3D 비밀 워터마킹 시스템

3D 모델에 워터마크를 삽입하는 방법에는 메쉬 변경방법, 위상 변경방법, 가시 패턴 삽입 방법 등 여러 방법들이 있다.

본 논문에서 제안하는 MDWF에서는 [6]에서 제안된 bin을 이용한 3D 비밀 워터마킹 시스템을 사용한다. 이 방법은 메쉬 표현에 독립성을 보장하기 위해 법선(normal) 분포를 변경하는 방식을 사용한다. MDWF의 기반이 되는 bin을 이용한 3D 워터마킹 시스템의 워터마크 삽입 및 추출 절차는 다음과 같다.

2.3.1 3D 비밀 워터마크 삽입 절차

3D 모델 데이터의 삼각형 패치(Triangle patch)로 구성된 메쉬 표현을 입력으로 받아 메쉬 표면의 법선 분포를 변경시킴으로써 워터마크를 삽입한다. 특히 워터마크 1비트를 입력하기 위해 곡면 패치들의 집합인 "bin"을 사용하게 되며 비밀키에 따라 "bin"을 선택한다. 이 방법을 이용한 워터마크의 삽입 절차는 다음과 같다.

E1. 표면 패치 법선들을 계산
E2. bin을 생성하기 위해 모델의 법선들을 샘플링
E3. 핵심 워터마크 삽입 알고리즘을 적용
- 샘플링한 법선들의 2D 정사영(P_j)을 계산
- 2D 정사영들로부터 형상 중심(center of mess : *com*)을 계산(NSN : 샘플링한 법선의 개수)

$$com = \frac{1}{NSN}\sum p_j \tag{1}$$

- 1 비트의 정보를 삽입하기 위해서, bin의 형상 중심을 특정한 방향으로 이동
(그림 1에서와 같이 0 삽입을 위해서는 왼쪽으로, 1 삽입을 위해서는 오른쪽을 이동)

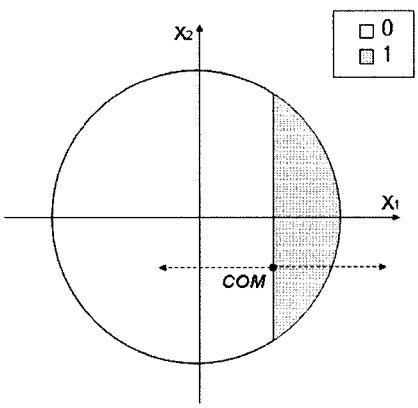

Fig. 1. 워터마크 선택과정.

2.3.2 3D 비밀 워터마크 추출 절차

워터마크를 추출하기 위해서는 다음의 정보가 필요하다.

- bin의 개수 N_B
- bin 중심 법선들 $BC_i(i = 1, \cdots, N_B)$과 각도 R_i
- 워터마크 삽입 전 모델의 형상 중심값 com

워터마크 추출 방법은 대부분 형상 변경 과정 전까지 삽입 방법과 동일하다.

R1. 표면 패치 법선들을 계산
R2. bin을 생성하기 위해 모델의 법선들을 샘플링
R3. 핵심 워터마크 추출 알고리즘을 적용
: E3에서와 같은 방법으로 com' = (cx', cy')을 계산한 후, 다음 식에 의해서 워터마크 1 비트를 추출

$$s' = \begin{cases} 1 & cx' > cx \\ 0 & cx' \le cx \end{cases} \tag{2}$$

2.3.3 3D 비밀 다중 워터마킹 시스템

위에서 설명한 3D 워터마킹 시스템은 워터마크 1 비트를 삽입하기 위해 표면 메쉬들로 구성된 1개의 bin이 필요하며 사용되는 bin들은 모두 중첩되지 않도록 선택된다. 따라서 bin의 선택 방법을 조절하면 다중 워터마크의 삽입 또한 가능해지며 모델의 표면 수와 bin의 선택 방법에 따라서 가능한 다중 워터마크 삽입 횟수가 결정된다. 이에 대한 실험은 향후 연구 과제로 진행할 것이다.

3. 다중 워터마킹 프레임워크

본 논문에서 제안하는 다중 워터마킹 프레임워크는 협업을 통해 제작된 VR 데이터의 공동 소유권을 증명하기 방법으로 3D 비밀 다중 워터마킹 기술과 비밀키 공유를 위한 암호 프로토콜을 사용한다. 2.3절에서 언급한 3D 비밀 워터마킹 기술은 메쉬 단순화(Mesh simplification) 같은 다양한 위상/기하 공격에 강인하며 워터마크 삽입을 위해 이용되는 bin의 선택에 의해 다중 워터마크 삽입이 가능하다. 따라서 3절에서는 공동 소유권 증명을 위한 비밀키 공유 방법을 소개하고 비밀 워터마킹과 비밀키 공유 방법을 기반으로 한 MDWF를 제안한다.

특히, [4]에서 소개한 비밀키 공유 프로토콜에서는 신뢰할 수 있는 분배자(Trusted Dealer)가 존재하지 않는 상황을 가정하나 제조 기업 환경에서 사용하는 VR 데이터는 보안 관리 등의 목적으로 VR 데이터 등록을 위한 서버 같은 신뢰할 수 있는 제 삼자(Trusted Third Party : TTP)의 존재를 가정하는 것이 일반적이다. 따라서 본 논문에서는 TTP의 존재를 가정하는 경우와 가정하지 않는 경우를 분리하여 비밀키 공유 프로토콜을 제안한다.

3.1 비밀키 공유 프로토콜

n명의 사용자 O_1, O_2, ⋯, O_n에게 각각 비밀키 Sk_1, Sk_2, ⋯, Sk_n이 주어진다. 다음의 비밀키 공유 프로토콜에서는 해쉬 함수 H를 사용한다.

3.1.1 Trusted Third Party(TTP)를 활용한 비밀키 공유 프로토콜

- 사용자 $O_i(i = 1, \cdots, n)$는 자신의 비밀키 Sk_i를 입력하여 TTP에게 전달
- TTP는 공동 소유권 증명을 위한 공유 비밀키 $SSk = H(Sk_1 \| Sk_2 \| \cdots \| Sk_n)$를 계산하여 출력

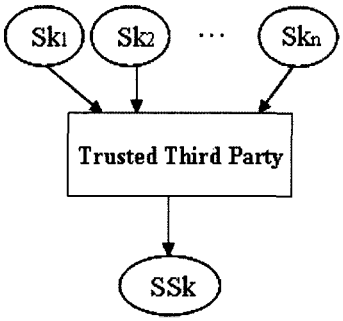

Fig. 2. TTP를 활용한 비밀키 공유 프로토콜.

3.1.2 Multi-party Computation를 활용한 비밀키 공유 프로토콜

TTP를 가정하지 않는 경우에는 사용되는 해쉬함수 H가 모든 입력 a와 b에 대해서 $H(a)H(b) = H(ab)$를 만족하는 Homomorphic Property를 갖는다고 가정하고 Key Sharing Server(KSS)가 Multi-party Computation에 참여한다.

- 사용자 $O_i(i = 1, \cdots, n)$는 자신의 비밀키 Sk_i에 대한 해쉬값 $H(Sk_i)$를 계산하여 KSS에게 전달
- KSS는 공유 비밀키 $SSk = H(Sk_1 \cdot Sk_2 \cdot \cdots \cdot Sk_n) = H(Sk_1)H(Sk_2) \cdots H(Sk_n)$를 계산하여 출력

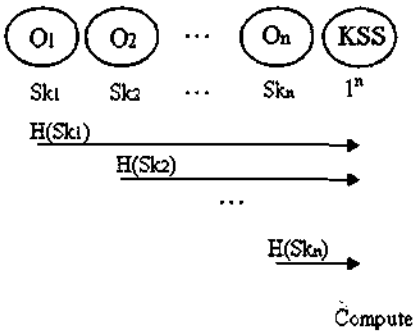

Fig. 3. MPC를 활용한 비밀키 공유 프로토콜.

3.2 다중 워터마크 삽입 방법

3D 데이터 $I_T = (I_1, I_2, \cdots, I_n)$는 n명의 공동 제작자 $O_1, O_2, \cdots, O_n$에 의해 생성되고 각 제작자 $O_i(i = 1, \cdots, n)$는 워터마크 W_i 삽입에 필요한 비밀키 Sk_i를 선택한다. 각 제작자 O_i의 저작물 I_i에 대한 소유권 증명과 동시에 전체 저작물 I_T에 대한 공동 소유권 증명을 위한 다중 워터마크 삽입 과정은 다음과 같다(Fig. 4 참조).

- 각 저작물 $I_i(i = 1, \cdots, n)$에 제작자 O_i의 비밀키 Sk_i를 입력 받아 2.3절에서 설명한 3D 비밀 워터마킹 삽입 알고리즘(Watermarking Embedding Algorithm : 3DEA)를 이용하여 워터마크 W_i 삽입
- Key Sharing Protocol(KSP)를 통해 모든 제작자들의 비밀키 $Sk_1, Sk_2, \cdots, Sk_n$을 공유하여 새로운 비밀키 SSk 생성
- 전체 저작물 I_T에 공동 소유권 증명을 위한 워터마크 W를 공유 비밀키 SSk를 이용하여 삽입

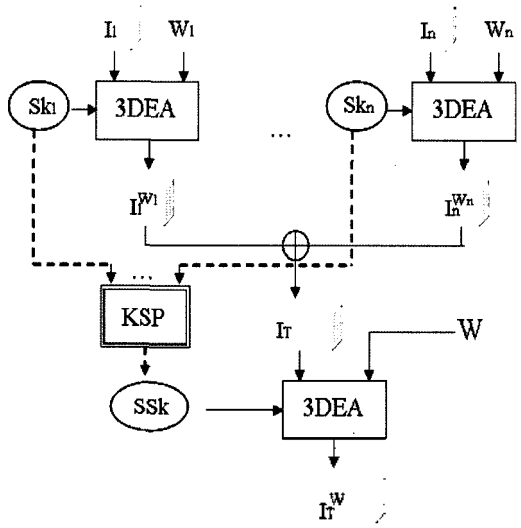

Fig. 4. 워터마크 삽입 블록도.

3.3 다중 워터마크 추출 방법

3D 데이터 $I_T = (I_1, I_2, \cdots, I_n)$의 공동 소유권을 증명하기 위해서 워터마크 W를 추출하는 방법은 3D 비밀 워터마크 추출 알고리즘을 사용하는 것을 제외하고 삽입의 방법과 유사하다.

- 모든 저작물 $I_i(i = 1, \cdots, n)$에 제작자 O_i의 비밀키 Sk_i를 입력받아 Key Sharing Protocol(KSP)를 통해 공유 비밀키 SSk 생성
- 공유 비밀키 SSk와 3D 비밀 워터마크 추출 알고리즘을 이용하여 전체 저작물 I_T에 공동 소유 증명을 위한 워터마크 W 추출

또한, 각 제작자 O_i가 자신의 저작물 I_i의 소유권을 주장하기 위해서는 전체 저작물 I_T에 자신의 비밀키 Sk_i와 3D 비밀 워터마크 추출 알고리즘을 이용하여 워터마크 W_i를 추출한다.

4. MDWF의 안전성 분석

3절에서 제안한 MDWF를 구현할 때, 알고리즘 내부에서는 안전한 통신 채널을 사용한다. 따라서 MDWF의 안전성은 사용하는 키 공유 프로토콜과 3D 비밀 워터마킹 알고리즘의 안전성에 의존한다.

4.1 키 공유 프로토콜의 안전성

MDWF에서 제안하는 키 공유 알고리즘은 각 사용자가 다른 사용자의 비밀키에 대한 정보는 물론 공유되는 비밀키에 대한 어떠한 정보도 얻을 수 없다는 점에서 기존의 키 공유 프로토콜의 안전성 목표와는 상이하다[7]. TTP를 활용한 키 공유 프로토콜의 경우 TTP의 신뢰성이 보장되며 MPT를 활용한 키 공유 프로토콜의 경우 다중 사용자 연산의 안전성을 확보할 수 있다[8]. 따라서 MDWF의 키 공유 프로토콜은 다음의 안전성 목표를 달성해야 한다.

- 완벽성 : 공유 비밀키의 정보로부터 어떠한 사용자의 비밀키에 대한 정보도 얻을 수 없다.

키 공유 프로토콜의 완벽성은 공유 비밀키에 대한 정보 $H(Sk_i)$로부터 Sk_i에 대한 정보를 얻을 수 없어야 하는데 이는 해쉬함수의 원상 저항성(Preimage Resistance) 성질에 기반하게 된다.

4.2 3D 비밀 워터마킹 알고리즘의 안전성

본 논문에서 제안한 MDWF에서 사용하는 3D 워터마킹 알고리즘은 특히 메쉬 단순화 공격에 강인하다. [6]에 의하면 원래 face수의 최고 36% 정도의 메쉬 단순화에서도 강인함을 보이고 있다. Fig. 5와 Fig. 6은 메쉬 단순화 공격에 대한 예제로 Fig. 5의 왼쪽 그림은 10648개의 삼각형으로 구성된 메쉬 표현을 가진 예제 모델이고 오른쪽 그림은 그 예제 모델에 워터마크를 삽입한 모델이다(워터마크를 표시하기 위해 삽입된 부분을 푸른색으로 표시함). Fig. 6은 메쉬 단순화 공격을 실시한 이후의 모델 그림으로 왼쪽 그림은 50%의 메쉬 단순화를 실시하여 5262개의 삼각형으로 구성된 메쉬 표현을 가지며, 오른쪽 그림은 10%의 메쉬 단순화를 실시하여 9569개의 삼각형으로 구성된 메쉬 표현을 가지는 모델이다. 실험에 의하면 오른쪽 모델에서는 삽입된 워터마크가 추출 가능하나 왼쪽 모델에서는 삽입된 워터마크가 추출되지 않는다.

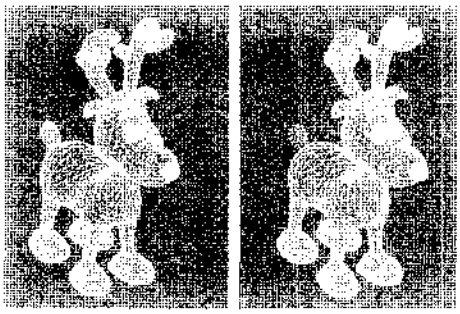

Fig. 5. 예제 모델(왼쪽)과 워터마크 삽입된 모델(오른쪽).

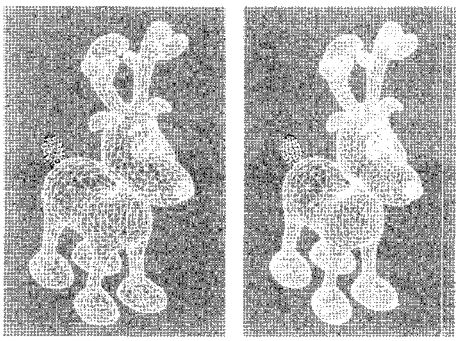

Fig. 6. 메쉬 단순화한 모델(왼쪽:50%, 오른쪽:10%).

5. 결 론

본 논문은 협업작업을 통해 3D 데이터를 생성하는 제작자들에게 전체 데이터의 생성에 자신이 기여한 부분에 대한 소유권을 증명할 수 있으면서 동시에 전체 저작물에 대한 공동의 소유권을 증명할 수 있도록 하고 제작에 참여한 일부 사람들의 단합을 방지할 수 있는 프레임워크 제안을 목표로 하고 있다. 이를 위해 MDWF는 [6]에서 제안한 3D 비밀 워터마킹 기술을 활용하며 이 워터마킹 기술이 다중 워터마크 삽입이 가능한 성질을 이용한다. 특히 MDWF에서는 제작자들의 비밀키를 공유함에 있어 공유에 참여한 제작자들이 다른 제작자들의 비밀키는 물론 공유되는 비밀키에 대한 정보도 얻을 수 없게 하는 새로운 형태의 키 공유 프로토콜을 제안함으로써 제작에 참여한 사람들의 단합을 방지할 수 있게 된다. 또한 MDWF의 안전성은 키 공유 프로토콜과 3D 워터마킹 알고리즘의 안전성에 기반하며 이는 안전성이 보장된 해쉬함

수와 강인성이 보장된 3D 워터마킹의 선택에 의해 보장된다.

감사의 글

본 논문은 정보통신 선도기반기술개발사업(정보통신연구진흥원 A1100-0601-0061) [iCOD 멀티미디어 플랫폼 기술개발] 과제와 [실감형 가상공학 기술개발] 과제의 일환으로 수행되었음.

참고문헌

1. 장항배, 이호신, "설계정보 유출 방지를 위한 정보보안시스템 설계 및 구현", 한국CAD/CAM 학회 논문집, 제11권, 제5호, pp. 327-334, 2006.
2. Cox, I. J., Miller, M. L. and Bloom, J. A., "Digital Watermarking", Academic Press, ISBN:1-55860-714-5, 2002.
3. Arnold, M., Schmucker, M. and Wolthusen, S. D., "Digital Watermarking and Content Protection", Artech House, ISBN:1-58053-111-3, 2003.
4. Guo, H. and Georganas, N. D., "Digital Image Watermarking for Ownership Verification Without a Trusted Dealer", in Proceedings of ACM Multimedia 2002, Dec. 2002.
5. Zhang, Y. Q. and Emmanuel, S., "A Novel Watermarking Framework for Joint-Creatorship Protection", Proceedings of Cyberworlds 2005, Singapore, pp. 109-116, Nov. 2005.
6. O. Benedens, "Geomery-Based Watermarking of 3D models," IEEE Computer Graphics and Applications", Special Issue on Image Security (January/February 1999), pp. 46-55.
7. Menezes, A. J., Oorschot, P. C. and Vanstone, S. A., "Handbook of Applied Cryptography", CRC Press LLC, 1997.
8. O. Goldreich, "Secure Multi-Party Computation", Manuscript, 2002, (Version 1.4).

조 미 성

1991년 이화여자대학교 수학과 학사
1993년 이화여자대학교 대학원 수학과 석사
1998년 이화여자대학교 대학원 수학과 박사
2005년~2006년 (재)그래픽스연구원 정보보안팀 책임연구원
2006년~현재 (주)알디캐스트 δ-Project TFT 책임연구원
관심분야: 접근제어기술 및 저작권 보호 기술, 사용자 인증 프로토콜, 가상현실 보안

손 유 승

1996년 계명대학교 산업공학과 학사
2004년 포항공과대학교 정보통신학과 석사
2005년~현재 (재)그래픽스연구원 정보보안팀 선임연구원
관심분야: 가상현실 보안, 사용자 인증 프로토콜, 정보보호 관리체계