Journal of Korea Multimedia Society Vol. 12, No. 7, July 2009(pp. 953-961)

개인간 콘텐츠 양도기능을 제공하는 온라인 디지털 콘텐츠 유통 모델 및 시스템 설계

이혜주[†], 남제호[††]

요 약

DRM 기술이 적용된 콘텐츠를 이용하는 것은 사용자의 편의성을 감소시키기 때문에 사용자는 이러한 콘텐츠를 사용하는 것을 기피하게 된다. 따라서 본 논문에서는 DRM 기술이 적용된 디지털 콘텐츠를 구입하는 사용자들이 서로 간에 디지털 콘텐츠를 자유롭게 매매하도록 하는 새로운 유통 모델을 제안한다. 이는 사용자를 유통 객체에 포함시켜 건전하게 콘텐츠를 유통시키도록 유도한다. 이를 위하여 본 논문에서는 기존의 디지털 티켓이나 쿠폰에 적용되는 방식을 기반으로 패키징된 콘텐츠와 사용권한을 양도하는 방식을 제안하고 이중양도(double transfer), 사용권한의 위조 및 변조(forgery and modification) 가능성, 사용권한 및 콘텐츠의 재생성(reproduction)에 관한 안전성을 논의한다.

Online Digital Content Distribution Model and System Design for Interindividual Content Transferability

Hyejoo Lee[†], Jeho Nam[††]

ABSTRACT

The usage of DRM-applied digital contents reduces user's convenience, thus it leads the many users to avoid using DRM-applied digital contents. In this paper, therefore, we propose the new distribution model in which the users, who purchase the DRM-applied digital contents, can resale freely those contents to the other users. As a result, the proposed model induces the users to distribute contents soundly by including them in one of distribution objects. For the purpose of this, in this paper, we propose that a packaged content and usage rights are transferred to another user by using a method which based on some existing digital ticket or coupon. In addition, the security of the proposed system is discussed for the double transfer, the forgery and the modification of usage rights, and the reproduction of contents and usage rights.

Key words: digital rights management(디지털저작권관리), content protection and distribution(콘텐츠 보호 및 유통), digital tickets(디지털 티켓)

1. 서 론

디지털 콘텐츠의 이용 증가와 함께 디지털 콘텐츠의 불법 복제는 콘텐츠 저작권자의 저작권 침해 및 금전적 손실을 초래하고 있다. 이러한 금전적 손실로 인한 콘텐츠 산업의 피해는 고품질의 콘텐츠 제작을

※ 교신저자(Corresponding Author) : 이혜주, 주소 : 부산시 남구 대연3동 599-1(608-737), 전화 : 051)629-6249, FAX : 051)620-6249 E-mail : iamhj@paran.com
접수일 : 2008년 8월 8일, 완료일 : 2009년 5월 26일
[†] 준회원, 부경대학교 시간강사
[††] 정회원, 한국전자통신연구원 방통융합미디어연구부 선임연구원
(E-mail : namjeho@etri.re.kr)
※ 본 연구는 지식경제부 및 한국산업기술평가관리원의 IT 신성장동력핵심기술개발사업의 일환으로 수행하였음. [2007-S-003-03, 지상파DTV 방송프로그램 보호 기술개발]

감소시켜 고품질의 디지털 콘텐츠를 선호하는 사용자들의 불만으로 이어지게 된다. 이에 저작권자의 권리를 보호하기 위한 법적 시도와 기술적 시도가 이루어지고 있다[1-9]. 기술적 시도의 하나인 DRM(digital rights management) 기술은 디지털 콘텐츠에 암호 기술을 적용하여 정당하게 콘텐츠를 획득한 사용자만이 사용 가능하게 하는 방식이다.

DRM 기술의 제약은 기술 간의 상호호환성(interoperability)이 제공되지 않는 것으로 DRM 기술이 적용된 디지털 콘텐츠를 구매하였을 경우 서로 다른 DRM 기술이 적용된 장치에서는 콘텐츠를 이용하기 어렵다는 것이다. 이것은 사용자의 편의성을 감소시켜 사용자들의 콘텐츠 사용 욕구를 감소시킨다. 따라서 DRM 기술이 적용된 콘텐츠를 정당하게 구매하는 콘텐츠 사용자에게 인센티브를 제공하여 콘텐츠의 사용에 대한 반감을 감소시킬 필요가 있다. 또한 음성적으로 이루어지고 있는 디지털 콘텐츠의 유통을 양성화하여 저작권자의 권리를 보호하고 콘텐츠 사용자의 사용 권리를 동시에 보호할 수 있는 방법을 고려해야 한다. 이를 목적으로 본 논문에서는 정당하게 구매한 콘텐츠를 사용자들이 자유롭게 양도할 수 있는 콘텐츠 유통 모델을 고려하고 이를 위한 온라인 디지털 콘텐츠 매매 중개를 위한 시스템을 설계한다. 먼저 2장에서는 콘텐츠의 양도를 고려한 콘텐츠 유통 모델을 소개하고 3장에서는 양도 기능이 있는 온라인 디지털 콘텐츠 매매 중개를 위한 시스템에 대해 기술한다. 그리고 4장에서는 해당 시스템의 문제점, 안정성 등에 대해 분석하고, 5장에서는 결론으로써 앞으로의 향후 과제에 대해 논의하고자 한다.

2. 개인 간 콘텐츠 양도기능을 갖는 콘텐츠 유통 모델

2.1 개념

시장에서 유통되는 모든 상품은 적정 가격으로 발행된 후 그 가치에 따라 가격이 할인되거나 혹은 프리미엄이 부가되어 유통되는 것이 일반적인 형태이다. 본 논문에서는 디지털 콘텐츠 유통 시에도 이러한 특성을 갖는 유통 모델을 제안하고 이를 '온라인 디지털 콘텐츠 매매 중개 유통 모델'(이하 중개 유통 모델)이라 한다. '중개 유통 모델'은 그림 1과 같이

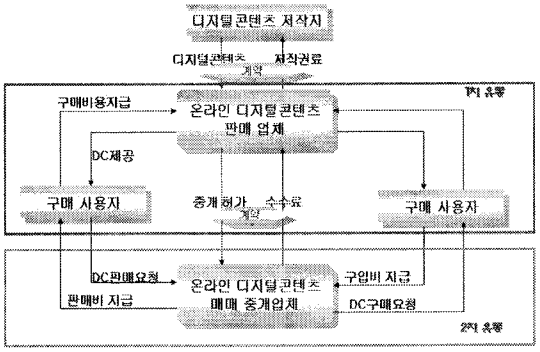

그림 1. 사용자간 사용권한 양도기능을 갖는 콘텐츠 유통 모델

디지털 콘텐츠의 유통을 1차와 2차 유통으로 분류한다. 1차 유통이란, 콘텐츠 사용자가 온라인 디지털 콘텐츠 판매자로부터 직접 콘텐츠를 구매하는 것으로 사용자는 콘텐츠의 1차 구매자가 된다. 2차 유통은 1차 구매자가 구매한 콘텐츠를 매매 중개 시스템을 이용하여 사용권한이 남아있는 콘텐츠를 다른 사용자에게 저렴한 가격으로 판매하는 경우를 의미한다. 그림 1에 나타난 바와 같이 '중개 유통 모델'에서의 참여자는 디지털콘텐츠 저작자, 온라인 디지털 콘텐츠 판매업체(이하 판매업체), 온라인 디지털 콘텐츠매매 중개 업체(이하 중개 업체), 그리고 1차 구매자와 2차 구매자로 구성된다. 디지털 콘텐츠 저작자와 판매업체는 디지털 콘텐츠 제공과 저작권료 지급에 관한 계약을 체결하고, 판매업체는 계약에 따라 콘텐츠를 온라인으로 판매한다. 이때 디지털 콘텐츠는 DRM과 같은 기술적 보호조치에 의해 보호되어진다. 1차 구매자인 콘텐츠 사용자는 자신이 원하는 사용권한(라이센스)과 디지털 콘텐츠를 구매하여 판매업체에게 비용을 지불하고 사용권한에 따라 디지털 콘텐츠를 사용하게 된다. 이때 1차 구매자가 콘텐츠를 일정기간 혹은 횟수를 사용한 후에, 사용권한이 만료되지 않았지만 더 이상 콘텐츠의 사용을 원하지 않는 경우 이를 재판매할 수 있도록 한다. 1차 구매자는 중개업체의 시스템에 접속하여 판매하고자 하는 콘텐츠와 사용권한을 중개업체에 등록시킨다. 이때 디지털 콘텐츠의 판매가격은 실제 판매업체로부터 판매되는 가격보다 저가의 가격으로 책정하게 된다. 따라서 판매업체보다 저가이면서 축소된 사용권한이 있는 콘텐츠를 사고자 하는 사용자는 중개업체로부터 자신이 원하는 콘텐츠를 사용권한과 함께 구매할 수 있다.

2.2 기존 유통 모델과의 비교

OMA, DMP 등 콘텐츠 서비스를 위한 연구나 기존의 유통 모델들을 살펴보면 일반적인 유통 모델[6-8]은 콘텐츠 제작(콘텐츠 제작자 혹은 저작권자)→유통(서비스 제공자)→소비(소비자)의 형태로 구성된다. 즉, 기존의 유통 모델에 있어서 사용자는 서비스 제공자로부터 제공되는 콘텐츠를 구매하여 소비하는 소비 객체로, 대부분 최종 사용자(end user)이다. 그림 2는 기존의 유통 모델과 제안하는 유통 모델을 표시한 것으로 점선으로 표시된 부분이 일반적인 기존의 유통 모델을 나타내고 있다.

그림 2와 같이 단순하게 사용자를 소비의 주체만으로 고려한 기존의 모델과 달리 제안하는 유통 모델은 사용자를 유통 객체로 참여시킴으로써 콘텐츠의 건전한 유통을 장려하여 DRM 기술이 적용된 콘텐츠에 대한 사용자들의 거부감을 감소시키는 것을 목적으로 한다.

2.3 수익 구조

이러한 유통 모델에 의해 중개업체는 1차 구매자와 2차 구매자간의 시스템 사용에 대한 수수료를 수익으로 하거나, 혹은 1차 구매자로부터 디지털 콘텐츠를 직접 구입하여 2차 구매자에게 판매하여 그 매매차익을 직접 수익으로 할 수 있다. 판매 업체는 중개업체로부터의 수수료와 1차 유통에서 발생되는 콘텐츠 판매비가 수익이 되며, 디지털 콘텐츠 저작권자는 판매업체로부터 저작권료를 받음으로서 수익을 얻을 수 있다. 또한 1차 구매자는 사용권한은 있지만 더 이상 사용하지 않을 콘텐츠를 판매함으로써 약간의 콘텐츠 구매 비용을 보전할 수 있음에 따라 합법적인 유통 시스템의 사용을 권장할 수 있게 될 것이다.

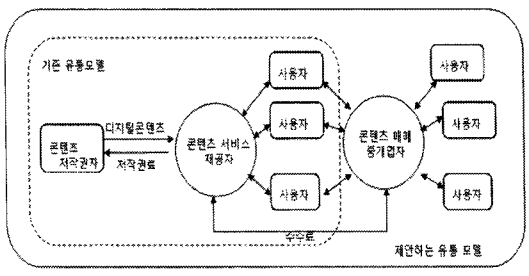

그림 2. 기존의 유통모델과 제안하는 유통 모델의 비교

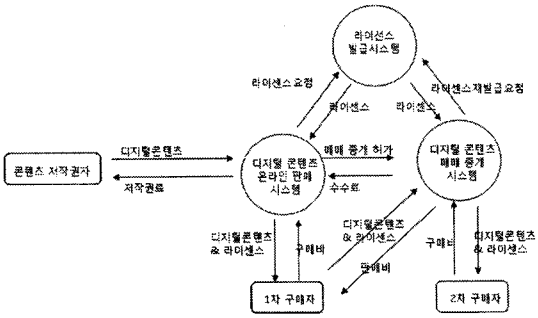

그림 3. 사용자간 콘텐츠 양도기능을 갖는 콘텐츠 유통 모델 프레임워크

2.4 서비스 프레임워크

앞에서 기술한 콘텐츠 유통 모델을 지원하기 위한 온라인 디지털 콘텐츠 매매 중개 서비스 프레임워크(이하 서비스 프레임워크)는 그림 3과 같이 구성된다.

제안하고자 하는 서비스 프레임워크의 참여자 및 서비스 단계는 각각 다음과 같다.

2.4.1 참여자

- 온라인 디지털콘텐츠 온라인 판매시스템(이하 판매 시스템)
  저작권자로부터 디지털 콘텐츠의 판매를 허가받고 디지털 콘텐츠를 판매하는 업체의 판매시스템
- 온라인 디지털 콘텐츠 매매 중개 시스템(이하 중개 시스템)
  디지털 콘텐츠 판매업체의 허가를 받고 디지털 콘텐츠의 매매를 중개하는 업체의 시스템
- 라이센스 발급 시스템(이하 발급 시스템)
  디지털 콘텐츠에 대한 사용권한인 라이센스를 발급하는 시스템으로 판매시스템과 매매 시스템으로부터 요청을 받아서 구매자의 라이센스를 발급
- 1차 구매자
  판매시스템을 이용하여 원가의 디지털 콘텐츠를 구매한 사용자
- 2차 구매자
  중개 시스템을 이용하여 1차 구매자로부터 할인된 가격으로 디지털 콘텐츠를 구매한 사용자

2.4.2 서비스 단계

- 콘텐츠 판매 단계

콘텐츠 저작권자로부터 계약에 의해 콘텐츠를 제

공받은 판매업체는 1차 구매자 디지털 콘텐츠 구매 요청에 따라 콘텐츠 패키징 및 라이센스 발급하여 콘텐츠를 판매한다. 이때 안전한 콘텐츠 유통을 위한 DRM과 같은 기술적인 보호 조치를 이용하여 콘텐츠를 배포한다.

• 콘텐츠 위임 단계

1차 구매자가 일정 기간동안 콘텐츠를 사용하고 사용권한이 만료되기 전에 재판매를 원한다면 중개 시스템에 접속하여 디지털 콘텐츠의 매매를 요청하고 디지털 콘텐츠와 자신이 가지고 있는 라이센스를 전송하여 위임시킨다. 이때 1차 구매자에 의한 콘텐츠 이중 양도(double transfer, 하나의 콘텐츠를 2회 이상 양도하는 것)를 방지하기 위해 콘텐츠 양도에 대한 부인방지, 그리고 불법적 행위의 추적을 위한 기능 등이 요구된다.

• 콘텐츠 양도 단계

매매 중개 시스템에 의해 등록된 1차 구매자의 디지털 콘텐츠와 라이센스에 대하여 2차 구매자가 디지털 콘텐츠의 구매를 요청하면, 중개 시스템은 라이센스 재발급을 수행하고 디지털 콘텐츠와 재발급된 라이센스를 2차 구매자에게 전송하게 된다. 이때 콘텐츠의 이중 양도, 콘텐츠의 양도 및 매매의 부인 방지, 추적 기능이 요구된다.

3. 개인 간 콘텐츠 양도기능을 갖는 콘텐츠 유통 시스템 설계

3.1 양도기능을 갖는 디지털 쿠폰

온라인 디지털 콘텐츠 매매 중개 시스템의 중요한 기능은 1차구매자가 소유한 콘텐츠와 콘텐츠 사용권한을 2차 구매자에게 양도하는 것이다. 양도성(transferability)을 제공하는 대표적인 기술로 전자화폐(digital cash)를 들 수 있다. 일반적으로 전자화폐는 양도성, 분할가능성(divisibility), 추적 불가능성(untraceability) 등의 특성을 갖는데 이를 기반하여 디지털 티켓이나 디지털 쿠폰 등에 전자화폐 기법을 적용한 방식이 제안되기도 하였다[9-12]. 디지털 티켓(쿠폰)이란 일반적인 종이 티켓(쿠폰)의 개념을 온라인에 사용하기 위해 적용한 것으로 제공되는 서비스에 대한 사용 권한이 포함된다. 본 논문에서는 디지털 티켓이나 쿠폰의 양도성을 제공하기 위해 전자화폐의 양도성 기법을 적용한 M. Terada 등이 제안한 'FlexToken'[12]을 기반으로 한다.

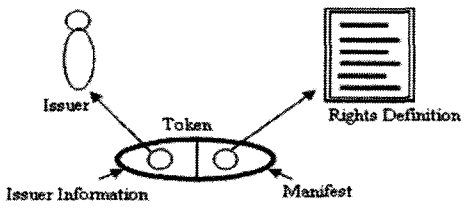

그림 4. FlexToken의 디지털 토큰

FlexToken 방식의 디지털 티켓이나 쿠폰은 그림 4와 같이 권리를 기술한 '권리 정의(rights definition)'와 토큰(token)으로 구성된다. 전자는 일반적인 저장 매체에, 토큰은 스마트카드에 저장된다. 토큰은 두 가지 정보인 '발급자 정보(issuer information)'와 '권한 정의(rights definition)에 대한 링크(Manifest)'로 구성된다. FlexToken 방식에서 디지털 권리의 양도는 스마트카드 내에 안전하게 저장된 토큰을 양도함으로써 이루어진다.

FlexToken 방식과 제안방식의 차이점은 FlexToken 방식은 디지털 티켓과 같은 권리만이 양도의 대상이고 본 논문에서는 권리를 포함한 콘텐츠가 양도의 대상이 된다. 따라서 제안방식에서는 콘텐츠를 보호하기 위한 기존 DRM 방식에 적용하는 콘텐츠 패키징 기술과 디지털 권리 양도를 위한 FlexToken 방식과의 혼합 방식을 적용하여 사용권한 및 콘텐츠를 양도하는 방식으로 그림 5와 같은 구조로 이루어진다.

'콘텐츠 토큰'에는 판매자와 구매자에 대한 '추적정보(trace information)' 와 DRM이 적용된 패키징된 콘텐츠에 대한 링크(manifest)가 저장된다. FlexToken 방식과 마찬가지로 '콘텐츠 토큰'은 스마트카드와 같은 안전한 저장소에, 패키징된 콘텐츠는 하드디스크와 같은 일반 저장장치에 저장된다.

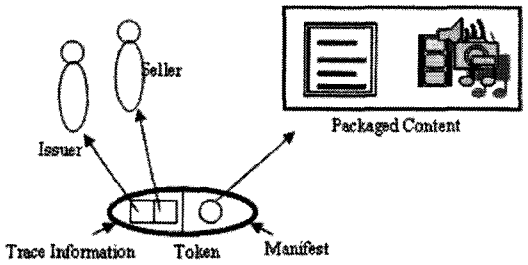

그림 5. 제안방식의 콘텐츠 토큰

표 1. FlexToken 방식과 제안방식의 비교

FlexToken		제안방식	
발급 단계	디지털 토큰을 생성하여 사용자에게 발급	발급 단계	콘텐츠 토큰을 생성하여 사용자에게 발급
양도 단계	발급된 디지털 토큰을 다른 사용자에게 양도	위임 단계	사용자는 사용권한 양도를 위해 콘텐츠 토큰과 콘텐츠를 중개업자에게 위임
회수 단계	디지털 토큰을 서비스 제공자에게 제시하여 서비스를 제공받고 서비스 제공자는 디지털 토큰을 회수	양도 단계	중개업자는 다른 사용자에게 위임받은 콘텐츠 토큰과 콘텐츠를 판매

FlexToken 방식의 단계는 발급단계(issue transaction), 양도단계(transfer transaction), 회수단계(redemption)로 나누어진다. 표 1은 FlexToken 방식과 본 논문에서 제안하는 방식과의 각 단계를 비교한 것이다. 표 1과 같이 제안방식에서는 FlexToken 방식의 회수 단계가 제외되고, FlexToken 방식의 양도단계와 제안방식의 위임단계는 '콘텐츠 토큰'과 콘텐츠의 패키징 과정을 제외하면 그 과정은 유사하다. 이와 같은 제안 방식의 각 단계별 세부 프로토콜을 다음에 기술한다.

3.2 서비스 단계별 프로토콜

각 단계에서 이루어지는 세부 과정을 기술하기에 앞서 논문의 각 기호는 다음과 같은 의미를 갖는다.

- $P \in \{I, U_i, A\}$, $i \in \{1,2\}$: 시스템의 참여자로 순서대로 판매업자, 구매자, 중개업자
- (SK_P, PK_P): 참여자 P의 개인키와 공개키 쌍
- $D_{list} = \{PK_{D_1}, PK_{D_2}, ..., PK_{D_n}\}$: 신뢰할 수 있는 도메인을 제공하기 위해 인증된 장치에서만 콘텐츠의 사용을 허용하기 위한 인증된 장치들의 리스트(공개키)
- $M_{\{1,2,A\}} = (L_i, m_i)$: 패키징된 콘텐츠로 사용권한 L_i과 $m_i = E_{CK}(C) \| E_{PK_{U_i}}(CK)$로 구성
- C_P: 각 단계에서 생성한 세션정보로 $C_P := (c_1, c_2) := (H(PK_P), s)$와 같이 참여자 P의 공개키 해쉬값(식별자), 그리고 세션 값으로 구성
- CT_i: 콘텐츠 토큰으로 판매업자 및 구매자들의 공개키 해쉬값(식별자)과 패키징된 콘텐츠의 해쉬 값(링크)로 구성
- $S_{SK_P}(x)$: 참여자 P의 개인키(private key) SK_P를 키로 하는 메시지 x에 대한 서명 함수
- $V_{PK_P}(x, y)$: 참여자 P의 공개키(public key)에 대한 서명 x의 검증 함수로

$$V_{PK_P}(x,y) := \begin{cases} true, & S^{-1}_{PK_P}(x) = y \\ fail, & S^{-1}_{PK_P}(x) \neq y \end{cases}$$

와 같이 정의

- $H(x)$: 입력 x에 대한 해시값으로, x가 참여자의 공개키 값인 경우 참여자의 식별자임
- $E_K(x)$: 키 K를 이용한 평문 x의 암호문
- R_P: 각 세션의 완료를 확인하기 위한 영수증으로 $R_P := (r_1, r_2) := (S_{SK_P}(C_P), PK_P)$와 같이 세션정보에 대한 참여자 P의 서명값, 공개키로 구성
- TDL(trusted device list) T: 콘텐츠 판매업자가 신뢰하는 장치 리스트로

$$T := \begin{cases} t_1 := H(PK_{D_1}), H(PK_{D_2}), ..., H(PK_{D_n}) \\ t_2 := S_{SK_I}(H(PK_{D_1})) \| ... \| S_{SK_I}(H(PK_{D_n})) \\ t_3 := PK_I \end{cases}$$

와 같이 각 장치의 공개키 해쉬값(장치 식별자), 서명값, 그리고 판매업자의 공개키로 구성

- SD_U: 세션 정보를 저장하는 세션 데이터베이스
- $SMF_{\{1,2,A\}}$: 콘텐츠 토큰 및 패키징된 콘텐츠를 전송하는 메시지 포맷으로 $SMF_{\{1,2,A\}} = (e_1, e_2, (e_3, e_4), e_5, e_6) \| M_{\{1,2,A\}}$로 구성된다. 이때, (e_1, e_2)는 콘텐츠 토큰으로 e_1은 패키징된 콘텐츠 $M_{\{1,2,A\}}$의 해쉬값(링크), e_2는 참여자 식별자, e_3, e_4는 세션정보, e_5는 서명값, e_6는 공개키 값으로 구성된다.
- CK: 콘텐츠 패키징 시 콘텐츠를 암호화하기 위해 사용된 암호 키

3.2.1 콘텐츠 판매 단계

구매과정에서 콘텐츠 구매자 U_1은 판매업자에게 특정 콘텐츠의 구매를 요청하면 아래와 같은 과정을 수행하게 된다.

(1) 판매업자 I는 안전한 도메인을 확립하기 위해

신뢰하는 장치의 공개키 리스트 D_{list}에 대해 TDL $T=\{t_1,t_2,t_3\}$를 사용자 U_1에게 전송한다.

(2) 사용자 U_1는 세션 정보 $C_{U_1}:=(c_1,c_2):=(H(PK_{U_1}),s)$와 공개키 PK_{U_1}를 판매업자 I에게 전송한다. 이때, s는 랜덤하게 생성된 수로 사용자 U_1은 세션 데이터베이스 SD_{U_1}에 s를 저장한다.

(3) 세션 정보와 공개키를 받은 판매업자 I는 콘텐츠 C, 사용권한 L_1에 대해 패키징된 콘텐츠 $M_1=(L_1,m_1)=(L_1,E_{CK}(C)\|E_{PK_{U_1}}(CK))$을 생성하고 $SMF_1=(e_1,e_2,e_3,e_4,e_5,e_6)\|M_1$을 전송한다. 이때, $(e_1,e_2,e_3,e_4,e_5,e_6)$은

$$\begin{cases} e_1:=H(M_1) \\ e_2:=H(PK_I) \\ (e_3,e_4):=(c_1,c_2) \\ e_5:=S_{SK_I}(e_1\|e_2\|e_3\|e_4) \\ e_6:=PK_I \end{cases}, \quad (1)$$

와 같이 정의된다.

(4) 사용자 U_1은 수신한 SMF_1으로부터 단계(2)에서의 세션정보와 서명을 검증하고 확인하는 과정을 수행한다. 즉,

$$\begin{cases} e_3=H(PK_{U_1}) \\ e_4\in SD_{U_1} \\ V_{e_5}(e_1\|e_2\|e_3\|e_4,e_5)=true \\ H(e_6)=e_2 \end{cases} \quad (2)$$

이 만족되는지를 검증한다.

(5) 위의 검증이 모두 성공하면 사용자 U_1은 콘텐츠 토큰 $CT_1=(e_1,e_2)=(H(M_1),H(PK_I))$과 M_1을 각각 저장한 뒤 세션을 완료하기 위해 $R_{U_1}:=(r_1,r_2):=(S_{SK_{U_1}}(C_{U_1}),PK_{U_1})$을 판매업자 I에게 전송한다.

(6) 판매자는 전송된 영수증 R_{U_1}에 대해 $V_{r_2}(C_{U_1},r_1)$, $H(r_2)$를 계산하여 검증이 성공되면 콘텐츠 판매 과정을 종료한다.

3.2.2 콘텐츠 위임 단계

사용자 U_1은 구매한 콘텐츠를 일정기간 사용한 후에 아직 사용권한이 만료되지 않았지만 콘텐츠를 더 이상 사용하지 않는 콘텐츠를 다시 팔기 위해 매매중개업자 A에게 콘텐츠 중개 매매를 요청하기 위한 다음 단계를 수행한다.

(1) 사용자 U_1은 $G_{U_1}:=(g_1,g_2):=(S_{SK_D}(PK_{U_1}),PK_D)$과 TDL T를 중개업자 A에게 전송한다. 이때, $PK_D\in D_{list}$는 U_1의 장치에 저장된 장치의 공개키로써 이 정보는 사용자 U_1이 소유한 장치가 인증된 장치임을 검증하기 위함이다.

(2) 중개업자 A는 세션 정보 $C_A:=(c_1,c_2):=(H(PK_A),s)$를 생성하여 사용자 U_1에게 전송하고 세션 데이터베이스 SD_A에 추가한다.

(3) 사용자 U_1은 콘텐츠 암호화 키 CK를 s로 암호화하여 $m'_1=E_{CK}(C)\|E_s(CK)$를 계산하여 $M_2=(L_1,m'_1)=(L_1,E_{CK}(C)\|E_s(CK))$를 생성하고 중개업자 A에게 $SMF_A=(e_1,e_2,e_3,e_4,e_5,e_6)\|M_2$를 전송한다. 단,

$$\begin{cases} e_1:=H(M_2) \\ e_2:=H(PK_I)\|H(PK_{U_1})\|H(PK_A) \\ (e_3,e_4):=(c_1,c_2) \\ e_5:=S_{SK_{U_1}}(e_1\|e_2\|e_3\|e_4) \\ e_6:=PK_{U_1} \end{cases}, \quad (3)$$

으로 구성되고, SMF_A의 복사본을 저장한다.

(4) 중개업자 A는 사용자 U_1이 전송한 SMF_A에 대해 세션정보, 서명, 정당한 장치인지를 검증한다. 즉,

$$\begin{cases} e_3=H(PK_{U_1}) \\ e_4\in SD_{U_1} \\ V_{e_5}(e_1\|e_2\|e_3\|e_4,e_5)=true \\ H(e_6)\|H(a_3)\|H(PK_A)=e_2 \\ V_{g_2}(e_6,g1)=true \\ H(g_2)\in t_1 \\ V_{t_3}(t_1,t_2)=true \end{cases} \quad (4)$$

이 만족하는지를 확인한다.

(5) 식(4)의 검증이 성공하면 중개업자 A는 콘텐츠 암호키 CK를 키 K_A로 암호화하여 하여 $M_A=(L_1,E_{CK}(C)\|E_{K_A}(CK))$와 (e_1,e_2)를 데이터베이스에 저장한다. 또한 s를 세션 데이터베이스 SD_A에서 삭제하고, 사용자 U_1에게 세션완료를 위해 $R_A:=(r_1,r_2):=(S_{SK_A}(C_U),PK_A)$를 전송한다.

(6) 사용자 U_1은 R_A를 $V_{r_2}(C_U,r_1)$, $H(r_2)$을 검증하여 만족하면 저장된 SMF_A의 복사본을 삭제하고 위임단계를 종료한다.

여기서 중개업자 A는 콘텐츠 위임에 관한 정보들을 데이터베이스에 관리하여 사용자 U_1에 의한 콘텐츠 위임에 대한 부인이나 이중양도를 위한 위임들을 방지한다.

3.2.3 콘텐츠 양도 단계

콘텐츠 양도 단계는 중개업자 A가 사용자 U_2에게 콘텐츠를 양도하는 단계로 판매단계와 매우 유사한다.

(1) 중개업자 A는 안전한 도메인을 확립하기 위해 신뢰하는 장치의 공개키 리스트 D_{list}에 대해 TDL $T=\{t_1,t_2,t_3\}$를 사용자 U_2에게 전송한다.

(2) 사용자 U_2는 세션 정보 $C_{U_2} := (c_1, c_2) := (H(PK_{U_2}), s)$와 공개키 PK_{U_2}를 중개업자 A에게 전송한다. 이때, s는 랜덤하게 생성된 수로 사용자 U_2은 세션 데이터베이스 SD_{U_2}에 s를 저장한다.

(3) 세션 정보와 공개키를 받은 중개업자 A는 사용자 U_2의 공개키 PK_{U_2}를 이용하여 저장된 M_A로부터 새로운 $m_2 = (E_{CK}(C) \| E_{PK_{U_2}}(CK))$를 생성한다. 그리고 라이센스 발급 시스템에 기존의 라이센스 L_1에 대해 새로운 라이센스 L_2를 발급받아서 $M_2 = (L_2, m_2) = (L_2, E_{CK}(C) \| E_{PK_{U_2}}(CK))$을 생성하고 $SMF_2 = (e_1, e_2, e_3, e_4, e_5, e_6) \| M_2$를 전송한다. 이때, $(e_1, e_2, e_3, e_4, e_5, e_6)$는

$$\begin{cases} e_1 := H(M_3) \\ e_2 := H(PK_I) \| H(PK_{U_1}) \| H(PK_A) \| H(PK_{U_2}) \\ (e_3, e_4) := (c_1, c_2) \\ e_5 := S_{SK_A}(e_1 \| e_2 \| e_3 \| e_4) \\ e_6 := PK_A \end{cases}, \quad (5)$$

와 같이 정의된다.

(4) 사용자 U_2은 수신한 SMF_2으로부터 단계(2)에서의 세션정보, 서명을 확인한다. 즉,

$$\begin{cases} e_3 = H(PK_{U_2}) \\ e_4 \in SD_{U_2} \\ V_{e_6}(e_1 \| e_2 \| e_3 \| e_4, e_5) = true \end{cases} \quad (6)$$

이 만족되는지를 검증한다.

(5) 위의 검증이 모두 성공하면 사용자 U_2은 콘텐츠 토큰

$$CT_2 = (e_1, e_2) = (H(M_1), H(PK_I) \| H(PK_{U_1}) \| H(PK_A) \| H(PK_{U_2}))$$

과 M_2을 저장한 뒤 세션을 완료하기 위해 $R_{U_2} := (r_1, r_2) := (S_{SK_{U_2}}(C_{U_2}), PK_{U_2})$을 중개업자 A에게 전송한다.

(6) 중개업자 A는 $V_{r_2}(C_U, r_1)$, $H(r_2)$를 계산하여 검증이 성공되면 콘텐츠 양도 과정을 종료한다.

3.2.4 거래의 중단

모든 단계에서 거래의 중단은 세션 정보가 일치하지 않는 경우, SMF 내의 서명 값이 다른 경우, 그리고 콘텐츠 구매에 대한 영수증 $R_P = (r_1, r_2)$의 값이 다른 경우에 각각 발생된다. 예로 판매단계에서의 거래의 중단은 다음과 같이 발생된다. 먼저, 세션 정보에 대한 거래의 중단은 다음과 같다. 사용자 U_1이 단계의 초기에 세션 정보 (c_1, c_2)를 생성하고 판매업자에게 전송된다. 이 세션 정보는 판매업자가 메시지 포맷 SMF_1내의 (e_3, e_4)로 다시 사용자 U_1에게 보낸다. 따라서 사용자 U_1은 수신한 (e_3, e_4)이 자신이 생성한 세션 정보와 일치하는지를 확인하고 일치하지 않으면 세션을 종료하고 거래를 중단한다. 두 번째로 서명 값에 대한 거래의 중단인 경우, 판매업자는 (e_1, e_2, e_3, e_4)를 자신의 개인키로 서명하여 SMF_1에 포함시켜 전송한다. 이때 사용자 U_1은 SMF_1 내의 (e_1, e_2, e_3, e_4)와 서명 값이 일치하는지를 확인하고 일치하지 않으면 세션을 종료하고 거래를 중단한다. 마지막으로 세션정보에 대한 사용자 U_1의 서명이 포함된 $R_{U_1} = (r_1, r_2)$을 받은 판매업자가 서명 값을 검증하고 검증이 실패한 경우에 세션을 종료하고 거래를 중단하게 된다.

4. 논 의

4.1 안전성

콘텐츠 사용권한 및 콘텐츠의 양도 가능한 콘텐츠 유통 시스템의 안전성은 콘텐츠 사용권한 및 콘텐츠의 이중양도(double transfer), 사용권한의 위조 및 변조(forgery and modification) 가능성, 사용권한 및 콘텐츠의 재생성(reproduction)에 의존한다. 따라서 안전한 콘텐츠 양도를 위해서는 이중양도의 방지, 사용권한의 위조 및 변조 방지 기능이 제공되어야 한다.

4.1.1 이중양도 방지

이중양도란 사용자 U_1이 하나의 콘텐츠에 대해 2번 이상 양도를 수행하는 것으로 본 시스템에서는 신뢰되는 중개자를 거쳐서 양도되어지기 때문에 중개자가 양도되는 콘텐츠에 대한 정보를 관리하는 경우 사용자 U_1은 이중으로 양도할 수 없다. 본 시스템에서는 콘텐츠 위임 단계에서 중개업자 A의 시스템에 (e_1, e_2)를 데이터베이스에 저장하여 사용자 U_1이 한번 이상 양도할 수 없도록 방지한다. 그러나, 사용자와 중개자가 서로 공모하여 이중양도를 하는 경우를 방지하기 위해서는 신뢰되는 제3자가 개입할 필요가 있다.

4.1.2 위변조 방지

본 시스템에서는 사용권한 L에 대한 $H(L)$의 값을 각 단계마다 e_1으로 전송하여 사용권한 L이 변조 혹은 위조 되었는지의 여부를 확인함으로써 위변조에

대한 방지가 가능하다.

4.1.3 재생성 방지

각 단계마다 발생되는 정보를 재저장하거나 또는 사용자 U_1이 양도할 콘텐츠와 사용권한을 삭제하지 않는 경우에 발생되는 문제이다. 단말 내에 위조방지(tamper-proof) 기능이 제공되면 각 단계는 안전하게 수행 가능하다.

4.2 사용권한의 형태

위에서 기술한 양도 메커니즘에 있어서 고려해야 할 문제는 사용권한의 종류이다. 양도 자체가 허용되지 않는 콘텐츠의 경우에는 제안하는 유통 모델에 이용될 수 없다. 사용권한이 '기간(period)'에 의한 형태인 경우에는 추가나 변경 없이 양도 메커니즘을 적용할 수 있으며, 반면에 기간제한이 아닌 횟수(time)에 의한 형태인 경우, 예를 들면 최초 구매자가 10번의 사용 권한을 구매하고, 2번을 사용한 다음에 남은 여덟 번의 사용권한 중에 네 번의 사용권한을 재판매하고자 하는 경우에는 위의 양도 메커니즘에 분할성(divisibility)을 적용한 부분이 추가되어야 한다. 이러한 기능은 복잡한 양도 절차가 수반되어지기 때문에 신중하게 고려되어야 한다.

5. 결 론

디지털 콘텐츠 저작권 보호에 대한 사용자들의 인식 부족은 디지털 콘텐츠 보호를 위한 DRM 기술을 탄생시켰으나, 사용자의 편의성을 저하시키는 문제가 발생하였다. 본 논문에서는 DRM과 같은 콘텐츠 보호 기술이 적용된 디지털 콘텐츠를 구입하는 선의의 사용자들에게 인센티브를 제공하여 콘텐츠 사용권리를 보호하고 콘텐츠 유통을 양성화시켜 바람직한 콘텐츠 유통 환경을 제공하는 것을 목적으로 하였다. 지금까지의 콘텐츠 유통 시스템은 인터넷 포털과 같은 콘텐츠 서비스 업자가 콘텐츠 제공자로부터 제공받은 콘텐츠를 판매하는 형식이지만, 제안방식은 콘텐츠 유통을 1차 유통과 2차 유통으로 분리하여 2차 유통에서는 사용자들이 자유롭게 디지털 콘텐츠를 매매할 수 있는 서비스를 제공한다. 기술적으로 콘텐츠 사용권한과 콘텐츠를 양도하기 위하여 디지털 티켓이나 디지털 쿠폰에서 이용되는 양도성, DRM과 같은 콘텐츠 보호 기술을 기반하고 있다. 본 논문에서 제안한 비즈니스 모델이 현재의 저작권법에의 적법성 여부는 고려하지 않았으며 단지 제안한 비즈니스 모델의 기술적 요구사항만을 고려하였다. 따라서 향후에는 제안한 비즈니스 모델의 저작권법에 대한 적법성 여부에 대한 고찰과 서비스 안전성에 대한 논의, 하나 이상의 매매 시스템이 존재하는 경우 사용자의 이중 등록을 방지하기 위하여 매매 시스템간 연결, 다양한 콘텐츠 사용정책의 적용에 대한 연구 등이 필요하다.

참 고 문 헌

[1] 온라인 디지털콘텐츠산업 발전법, 법률 제8852호, 2008.2.29(일부개정), http://www.klaw.go.kr/DRF/MDRFLawService.jsp?OC=kipa&ID=009280.

[2] W. Zeng, H. Yu, and C-Y Lin, Multimedia Security Technologies of Digital Rights Management, ACADEMIC PRESS, USA, 2006.

[3] A. Uhl and A. Pommer, Image and Video Encryption From Digital Rights Management to Secured Personal Communication, Springer, Germany, 005.

[4] H. T. Sencar, M. Ramkumar, and A. N. Akansu, Data Hiding Fundamentals and Applications: Content Security in Digital Multimedia, Elsevier, Netherland, 2004.

[5] I. Cox, M. Miller, and J. Bloom, Digital Watermarking: Principles & Practice, MOGAN KAUFMANN Press, USA, 2001.

[6] OMA(open mobile alliance), http://www.openmobilealliance.org/Technical/DRM.aspx.

[7] DMP(digital media project), http://www.dmpf.org/.

[8] DRM인사이드, 디지털콘텐츠 유통경로에 따른 합리적 수익배분 조사, 한국소프트웨어진흥원, pp. 29-59, 2006.

[9] 이덕규, 오형근, 이임영, "전자화폐 시스템을 적용한 DRM 모델에 관한 연구," 멀티미디어학회 논문지 제7권 제8호, pp. 1107-1119, 2004.

[10] K. Fujimura and Y. Nakajima, "General-purpose Digital Ticket Framework," 3rd USENIX Workshop on Electronics Commerce, August 1998, pp. 177-186,

[11] K. Matuyama an K. Fujimura, "Distributed Digital-Ticket Management for Rights Trading System," E-Commerce 99, pp. 110-118, 1999.

[12] M. Terada, H. Kuno, M. Handate, and K. Fujimura., "Copy Prevention Scheme For Rights Trading Infrastructures," Proceedings of the fourth working conference on smart card research and advanced applications on Smart card research and advanced applications, pp. 51-70, 2001.

이 혜 주

1994년 부경대학교 전자계산학과 (이학사)
1997년 부경대학교 대학원 전자계산학과(이학석사)
2000년 부경대학교 대학원 전자계산학과(이학박사)
2000년~2001년 한국정보통신대학교 박사후 연구과정생
2001년~2005년 한국전자통신연구원 디지털방송연구단 선임연구원
2005년~2006년 경성대학교 멀티미디어대학 컴퓨터정보학부 초빙교수
2006년~2008년 모빌리존 개발팀장, 한국전자통신연구원 전파방송연구단 방송미디어연구그룹 방통융합콘텐츠보호연구팀 초빙연구원
2009년~현재 부경대학교 시간강사
관심분야 : 디지털 콘텐츠 보호 및 관리, DRM, 디지털 워터마킹, 멀티미디어 처리 기술

남 제 호

1994년 홍익대학교 전기제어공학과(학사)
1997년 University of Minnesota, Dept. of Electrical Eng. (석사)
2000년 University of Minnesota, Dept. of Electrical Eng. (박사)
2001년~현재 한국전자통신연구원(ETRI) 방송통신융합연구부문 방통융합미디어연구부 선임연구원
2007년~현재 과학기술연합대학원대학교(UST) 이동통신 및 디지털방송공학 겸임 부교수
관심분야 : 멀티미디어 신호처리, 디지털방송기술, MPEG, 콘텐츠 보호관리