제2회 정보통신표준화 우수논문집

01 | 우수상 / 일반부문

DRM 시스템과 이미지 핑거프린팅 시스템의 통합 프레임워크

Integrating Framework of DRM System and Image Fingerprinting System

이준석, 정혜원 / 한국전자통신연구원, 디지털콘텐츠연구단

Jun-Suk Lee, Hye-Won Jung / Digital Contents Research Division, ETRI

DRM 시스템과 이미지 핑거프린팅 시스템의 통합 프레임워크

Integrating Framework of DRM System and Image Fingerprinting System

이준석, 정혜원 / 한국전자통신연구원, 디지털콘텐츠연구단
Jun-Suk Lee, Hye-Won Jung / Digital Contents Research Division, ETRI

요 약

DRM (Digital Rights Management) 기술은 디지털 콘텐츠의 저작권 보호를 위한 기술적인 한계와 표준화의 어려움으로 실용화에 난항을 겪고 있다. 이에 따라 콘텐츠 불법 유통 방지 및 저작권 보호를 위해 불법 배포자 추적이 가능한 핑거프린팅(Fingerprinting) 기술과의 접목이 요구되고 있다. 따라서 본 논문에서는 불법 콘텐츠의 최초 배포자를 추적할 수 있는 핑거프린팅 시스템 아키텍처를 설계하고 기존의 다양한 DRM 시스템들과 제안한 핑거프린팅 시스템이 상호 연동되는 통합 프레임워크를 제안한다. 제안한 통합 프레임워크를 근간으로 DRM 시스템들과 핑거프린팅 시스템이 상호 호환성을 보장할 수 있는 표준 인터페이스를 정의하였으며 또한 핑거프린트 코드의 안전한 전달을 보장하는 암호화 메커니즘을 제안한다.

Ⅰ. 서론

인터넷 환경이 급속도로 발전함에 따라 멀티미디어 콘텐츠의 범람과 사용자들의 유료 콘텐츠 사용에 대한 인식 부족이 디지털 콘텐츠 저작권 침해의 심각한 문제로 대두되고 있다. 이는 디지털 콘텐츠가 아날로그 콘텐츠와는 달리 질적 저하 없이, 원본과 동일한 형태로 무한 복제되고, 대용량 매체와 보안 위협에 쉽게 노출되어 있는 인터넷이 범용화 되면서 신속 배포 및 대량 배포가 가능하기 때문이다. 이렇게 불법 콘텐츠들의 무분별한 공유와 유통은 저작권 침해와 비정상적인 유통문제를 야기하여, 디지털 콘텐츠 산업 발전을 크게 저해하고 있다.

국내 음반시장의 경우 시장 규모가 과거 4000억원 (2000년도 기준)에서 근래 1000억원으로 75% 줄었으며, 영상산업의 경우에도 1조 2000억원(1990년)에서 7000억원(2004년)으로 54%가 감소되었다[1]. 이러한 콘텐츠 산업의 시장 축소와 침체의 가장 큰 원인은 음반 및 영상 콘텐츠의 무분별한 불법복제 및 유통이라 볼 수 있다.

2005년도에 들어 이러한 심각성을 알고 불법복제를 방지하기 위한 저작권법 개정과 저작권 협회들의 단속활동을 강화하고 있다. 그러나 보다 근본적인 해결책은 콘텐츠 사용자의 의식변

화와 함께 이들 콘텐츠가 인터넷 상에서 불법으로 유통되는 것을 근본적으로 차단할 수 있는 새로운 DRM[1] 기술의 개발이라 하겠다.

이와 같은 문제점을 해결하기 위한 기술적인 솔루션으로서 DRM, 디지털 워터마킹[2], 핑거프린팅[3] 기술들이 산업적인 요구에 의해 증가되고 있다. 그러나 기존의 암호화 기반의 DRM 콘텐츠 유통 시스템은 콘텐츠를 인터넷을 통하여 사용자에게 안전하게 전달하는 역할에 주력해 왔다[2] [3] [4].

DRM 시스템을 통해 전달된 콘텐츠는 사용자가 콘텐츠를 실행할 때 원본 이미지나 영상이 화면에 디스플레이 되거나 스피커의 소리를 통해서 사용자에게 전달된다. 이 단계에서 불법복제 행위를 원하는 사용자는 범용 어플리케이션을 이용하여 영상이나 이미지를 캡처하거나 사운드를 녹음하여 질적 저하 없는 원본과 동일한 복제물을 재생산할 수 있다. 또한 이렇게 불법 복제된 콘텐츠를 웹 블로그, P2P, 웹하드, 카페나 동호회 등에 공유할 경우 불특정 다수에게 순식간에 퍼져 나가, 불법 콘텐츠의 대량 유통도 가능해진다[5].

이렇듯 기존의 DRM 기술만으로는 불법 복제 방지 및 콘텐츠 저작권 보호에 한계가 있기 때문에 최근 불법 복제 억제 및 방지의 핵심 기술로 핑거프린팅 기술이 대두되고 있다. 기존 DRM 시스템에 핑거프린팅 기술이 접목될 때 콘텐츠를 불법 유통한 최초의 배포자를 추적할 수 있으며, 이를 통해 불법 복제 콘텐츠의 유통 방지 및 억제 효과를 기대할 수 있다[6].

본 논문에서는 인터넷 상에서 불법콘텐츠를 추적하기 위한 핑거프린팅 시스템에 대한 정의와 시스템 아키텍처를 설계한다. 그리고 콘텐츠 유통 시스템과 핑거프린팅 시스템간의 통합시스템 프레임워크의 표준을 제안하고 전체적인 시스템 흐름과 인터페이스를 정의하고자 한다. 통합시스템에서 콘텐츠의 신뢰성 확보와 보안을 위해 필요한 암호화 메커니즘에 대해서도 정의한다. 단, 핸드폰, PDA 등 모바일 플랫폼과 DVD 등 셋톱박스 환경은 고려하지 않으며 인터넷을 사용하는 PC 플랫폼으로 실행 환경을 제한하며 콘텐츠의 타입은 이미지로 한정한다.

본 논문의 II 장에서는 최근 국내외 표준 기구들의 표준화 내용을 기술하고, III 장에서는 일반적인 DRM 시스템의 구성 및 기능들을 서술한다. IV 장에서는 핑거프린팅 시스템의 정의

1) DRM(Digital Rights Management): 디지털콘텐츠의 불법 유통과 복제를 방지하고 적법한 사용자만이 콘텐츠를 사용하게 하며, 과금 서비스 등을 통하여 디지털콘텐츠 저작권을 관리하는 기술이다.

2) 디지털 워터마킹(Digital Watermarking): 사진 이미지나 음악 파일 같은 멀티미디어 콘텐츠에 인간의 시각이나 청각으로 식별이 어렵도록 저작권 정보를 삽입하여 배포하고 저작권 분쟁이 발생하였을 경우 이를 추적하여 저작권을 보호하는 방법이다.

3) 핑거프린팅(Fingerprinting): 모든 콘텐츠에 동일한 저작권 정보를 삽입하는 워터마킹 기법과는 달리 콘텐트마다 각기 다른 구매자 정보를 삽입함으로써 불법복제 및 유통행위가 발견되었을 때 불법 배포자를 추적하고자 하는 기술이다. 저작권 정보만을 이용하는 워터마킹보다는 적극적인 의미의 보호 기법이라 할 수 있다.

와 아키텍처를 제안하고, V 장에서는 핑거프린팅 시스템과 DRM 시스템의 통합 프레임워크를 제안한다. VI 장에서는 통합 프레임워크에서 핑거프린트 코드의 안전한 사용을 위한 암호화 메커니즘을 정의하고, VII 장에서는 통합 프레임워크의 각 시스템 간 상호 인터페이스를 정의했다.

Ⅱ. 표준화 현황

디지털 콘텐츠의 저작권 보호와 관련된 국내 · 외 표준화는 DRM 기술에 국한되어 진행되고 있다.

디지털 콘텐츠의 불법복제 방지 및 저작권 보호를 위해 다양한 DRM 기술 및 제품들이 출시되고 있으나, DRM 벤더별 독자적인 기술규격 사용으로 디지털 콘텐츠 및 디지털 기기의 상호호환성이 보장되지 않고 있다.

이에 국제 표준 단체인 MPEG-21, OMA (Open Mobile Alliance), CORAL, DMP(Digital Media Project) 등에서는 DRM의 상호호환성 보장을 위해 DRM 표준화를 위해 노력하고 있다[7] [8].

국내 DRM 표준화는 2001년부터 DRM 포럼, MPEG Korea 포럼, 한국디지털케이블 포럼 등을 중심으로 관련 기술의 보급과 산업 활성화에 노력하고 있다[1]. 그러나 이미 업체들이 제품 개발이 완료된 상태에서 표준화가 진행되고 있어 현실적으로 표준화하기에 어려움이 있다. 제품이 출시된 후의 표준화 작업은 업체들 간의 손익이 걸려 있어 민감한 사항이기 때문이다. 그래서 기존의 DRM 시스템에서 사용되는 패키지된 콘텐츠를 상호 교환 할 수 있는 EXIM (EXport /IMport)을 통한 표준화 방향으로 진행되고 있다. 이와 같이 사용자들은 업체들간 상호호환 되지 않는 DRM 서비스를 제공받고 있기 때문에 구매한 콘텐츠의 사용에 많은 제약을 가지고 있고, 이러한 것들이 DRM 시스템의 활성화에 장애요소로 작용하고 있다.

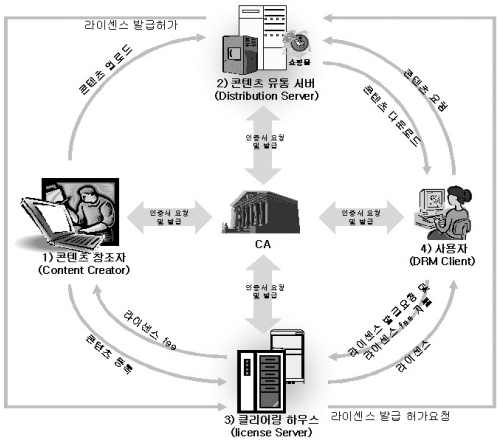
현재까지 국내 · 외에서 불법 콘텐츠 추적을 위한 핑거프린팅 시스템에 대한 표준화 활동은 없었으며 또한 DRM 시스템과 핑거프린팅 시스템의 통합 시스템에 대한 표준화는 전무한 상태이다.

따라서 본 논문에서 핑거프린팅 시스템의 아키텍처를 정의하고 기존의 DRM 시스템과 통합을 위한 인터페이스를 정의함으로써, 불법복제 콘텐츠의 유통 및 저작권 보호를 위한 기술 표준화를 주도하고자 한다.

III. 콘텐츠 유통 시스템

콘텐츠 유통 시스템은 디지털 콘텐츠의 불법 유통을 억제하고 방지함으로써 디지털콘텐츠에 연관된 콘텐츠 제작자 또는 저작권자의 권리를 보호하기 위한 시스템이다[2] [4]. 전체 구조는 서비스 형태에 따라 다를 수 있으나, 일반적으로 기본 구조 및 기능은 유사하다. 아래에 콘텐츠 유통 시스템의 기본 구조 및 기능에 대해서 알아본다.

1. 콘텐츠 유통 시스템의 구조



(그림 1) 콘텐츠 유통 시스템의 기본 구조도

(그림 1)에서와 같이 콘텐츠 유통 시스템은 콘텐츠를 최초로 창조하는 콘텐츠 창조자, 콘텐츠의 배포를 담당하는 콘텐츠 유통 서버, 콘텐츠에 대한 권한 설정 및 과금을 담당하는 클리어링 하우스(또는 라이선스 서버), 콘텐츠를 이용하는 사용자 그리고 객체 상호간을 인증을 담당하는 인증기관으로 구성된다. 각 객체의 기능을 살펴보면 다음과 같다.

- **콘텐츠 창조자**
  - 콘텐츠를 제작하는 객체로서 창작된 콘텐츠를 콘텐츠 유통 서버에 전달한다.
- **콘텐츠 유통 시스템**
  - 콘텐츠 등록 및 관리, 콘텐츠 유통 관리 등을 수행한다.
  - 콘텐츠 암호화 및 메타데이터 관리를 통한 패키징 기능을 담당한다.
  - 암호화 키 및 암호화된 콘텐츠의 발급 및 관리를 수행 한다.
- **클리어링 하우스(또는 라이선스 서버)**
  - 라이선스 발급 및 결제를 통한 사용자 권한 설정 및 리포팅 기능을 제공한다.
- **DRM 클라이언트**
  - 암호화된 콘텐츠를 복호화 한다.
  - 콘텐츠에 대한 라이선스를 관리한다.
- **인증기관(CA : Certificate Authority)**
  - 사용자 인증, 메시지 인증 및 전자 서명 등의 기능을 수행한다.

2. 콘텐츠 공급자와 DRM 솔루션 업체와 관계

콘텐츠 유통 시스템은 시스템적인 관점에서 콘텐츠를 서비스하는 콘텐츠 공급자와 DRM 솔루션을 제공하는 DRM 솔루션 제공자와의 관계에 따라 독립적인 구조와 종속적인 구조로 나눌 수 있다. 이렇게 구분하는 이유는 핑거프린팅 시스템과의 통합시 콘텐츠 유통 시스템의 구조가 핑거프린트 구조에 영향을 미치기 때문이다.

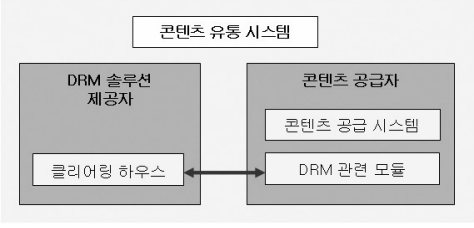
2.1 독립적 구조

콘텐츠 공급 시스템이 DRM 솔루션을 제공받아 자체적으로 클리어링 하우스를 운영하는 콘텐츠 유통 시스템을 의미한다. 즉 콘텐츠 공급 시스템이 DRM 시스템에 관련된 제반 사항을 관리하고 운영하는 경우로서 (그림 2)와 같다.

(그림 2) 독립적 구조

2.2 종속적 구조

콘텐츠 공급 시스템이 DRM 시스템이 제공하는 클리어링 하우스를 포함하고 있지 않으며 클리어링 하우스 서비스는 DRM 솔루션 제공자를 통해서 서비스를 제공받는 형태이다. 즉 콘텐츠 공급 시스템은 콘텐츠를 패키징하여 사용자에게 제공하는 기능을 수행하고 DRM 솔루션 업체가 제공하는 클리어링 하우스는 라이선스 기능을 수행하는 형태로 (그림 3)과 같다.

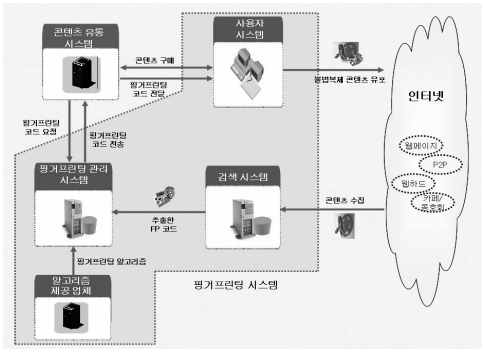


(그림 3) 종속적 구조

IV. 핑거프린팅 시스템

본 논문에서 제안하고 있는 핑거프린팅 시스템의 구조 및 기능들에 대해서 설명한다.

핑거프린팅 시스템이란 핑거프린트 기술을 활용하여 콘텐츠를 불법 배포한 부정자를 추적, 그 증거자료를 확보하여 불법 복제에 대한 법적 책임을 물음으로써, 디지털 콘텐츠의 저작권을 보호할 수 있는 시스템을 말한다. 핑거프린팅 시스템은 (그림 4)와 같이 핑거프린팅 관리 시스템, 사용자 시스템, 검색 시스템, 그리고 알고리즘 제공 시스템으로 나눌 수 있으며 각 시스템의 주요 기능 및 역할은 다음과 같다.



(그림 4) 핑거프린팅 시스템의 구성도

- **알고리즘 제공 시스템**
  - 핑거프린팅 알고리즘을 개발하는 업체의 시스템들이다.
  - 각 시스템은 콘텐츠 타입, 공모공격 대응, 강인성 등의 요구사항에 따라 핑거프린팅 알고리즘을 개발한다.
  - 개발된 알고리즘에 대하여 핑거프린팅 관리 시스템에 서비스를 요청한다.
- **핑거프린팅 관리 시스템**
  - 사용자가 요청한 핑거프린트 코드를 생성하고 관리한다.

– 콘텐츠별 지원 가능한 포맷, 사이즈, 핑거프린팅 삽입 방식에 따른 다양한 핑거프린팅 프로그램을 보유하고 버전 및 프로그램을 관리한다.
– 검색 시스템으로부터 전송받은 추적 정보를 관리한다.

• **사용자 시스템**
– 콘텐츠 유통 시스템으로부터 적법하게 콘텐츠를 구매하고 실행하는 시스템으로 간주한다.
– 미리 설치된 핑거프린트 삽입 프로그램을 통해 콘텐츠가 실행될 때 핑거프린트 코드가 동적으로 삽입된다.

• **검색 시스템**
– 인터넷 환경에서 콘텐츠를 검색하고 다운로드한다.
– 수집한 콘텐츠에 대해 핑거프린트 추출 프로그램을 이용하여 핑거프린트 코드의 유 · 무를 확인한다.
– 핑거프린트 코드가 존재하면 불법 콘텐츠로 간주하고, 해당 수집 정보와 핑거프린트 코드를 핑거프린팅 관리 시스템에 전달한다.

V. 통합 프레임워크

본 장에서는 콘텐츠 유통 시스템과 핑거프린팅 시스템과의 통합을 위한 동작 시나리오 및 필요한 기술적인 절차들에 대해서 설명한다.

통합 프레임워크는 콘텐츠 유통 시스템, 사용자 시스템, 핑거프린팅 관리 시스템, 검색 시스템, 알고리즘 제공 시스템이 상호 연동되어 유기적으로 동작하는 시스템이다. 독립적으로 운영되는 각 시스템들이 어떻게 상호 연동되어 운영되는지를 설명한다.

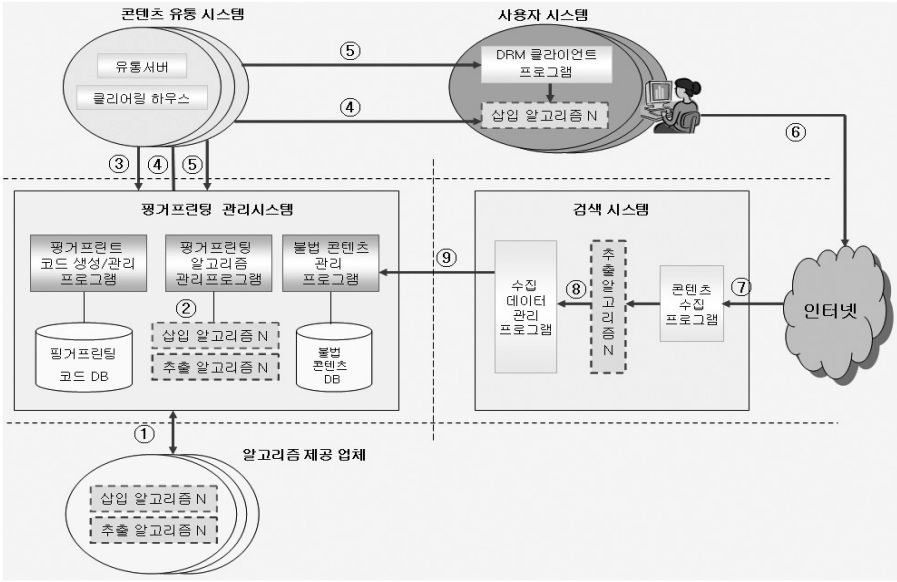
1. 동작 시나리오

(그림 5)에서는 통합 프레임워크가 동작하는 시나리오를 보여주고 있으며 화살표에 표시된 번호 순서대로 설명하면 다음과 같다.

① 알고리즘 제공 시스템들은 요구사항에 따라 핑거프린팅 알고리즘을 개발하고 이것을 핑거프린팅 관리시스템에게 제공한다.
핑거프린팅 관리 시스템은 공개키, 비밀키 생성알고리즘을 제공한다.
알고리즘 제공 시스템들은 핑거프린팅 알고리즘에 대응하는 비밀키와 공개키를 생성하고 비밀키를 핑거프린팅 추출 알고리즘에 하드 코딩된 핑거프린팅 삽입/추출 알고리즘을 제공한다.

② 핑거프린팅 관리 시스템은 핑거프린팅 알고리즘에 불법적인 해킹코드가 있는지 검사하고 문제가 없다고 판단하면 한 개의 서비스 알고리즘으로 핑거프린팅 알고리즘 관리 프로그램에 등록한다.

③ 콘텐츠 유통 시스템들은 핑거프린팅 관리 시스템이 제공하는 다양한 핑거프린팅 알고리즘을 검토하고 각 유통 환경 및 요구사항을 만족하는 알고리즘을 선택한다.



(그림 5) 통합시스템 동작 시나리오

다양한 콘텐츠 유통 시스템이 핑거프린팅 관리시스템과 연동될 수 있으며, 하나의 콘텐츠 유통 시스템은 핑거프린팅 관리시스템에서 제공되는 여러 개의 알고리즘을 서비스 받을 수도 있다.

④ 콘텐츠 유통 시스템이 서비스 받을 알고리즘을 선택하면 핑거프린팅 관리 시스템은 핑거프린팅 삽입 알고리즘을 콘텐츠 유통 시스템에 제공하고 콘텐츠 유통 시스템은 이 알고리즘을 콘텐츠 사용자 시스템에 설치한다.

⑤ 콘텐츠 유통 시스템은 사용자의 콘텐츠 구매 요청이 들어오면 핑거프린팅 관리 시스템에게 구매자의 고유정보를 전송하고 핑거프린트 코드를 요청한다.

핑거프린트 코드 생성/관리 프로그램은 구매자의 고유정보와 대응하는 핑거프린트 코드를 생성하여 콘텐츠 유통 시스템에게 전달한다.

콘텐츠 유통 시스템은 사용자 시스템에 이미 설치된 DRM 클라이언트 프로그램에게 핑거프린트 코드를 안전하게 전달한다. 사용자는 DRM 클라이언트 프로그램을 통하여 콘텐츠를 복호화하고 콘텐츠가 실행되기 직전에 핑거프린팅 삽입 프로그램이 동작하여 핑거프린트 코드를 삽입하게 된다.

⑥ 사용자가 불법적으로 콘텐츠를 인터넷 – 웹사이트, P2P, 웹하드 등–에 콘텐츠를 배포한다.

⑦ 검색 시스템에서는 인터넷 상에서 공유되고 있는 콘텐츠들을 수집하여 핑거프린팅 추출 알고리즘에 전달한다.

⑧ 추출 알고리즘은 수집된 콘텐츠에 핑거프린트 정보가 있는지 검사하고 핑거프린트 코드가 있을 경우 해당 콘텐츠를 수집 데이타 관

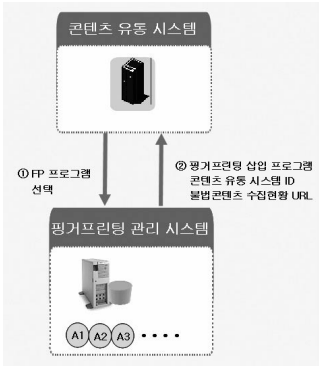
리 프로그램에 전달한다.

⑨ 수집 데이터 관리 프로그램은 추적한 정보를 핑거프린팅 관리 시스템에 전달한다.

⑩ 불법 콘텐츠 관리 프로그램은 수집된 불법 콘텐츠에 대하여 정보를 콘텐츠 유통 시스템에게 제공한다.

2. 등록 절차

최초에 콘텐츠 유통 시스템이 핑거프린팅 서비스를 제공하기 위해서는 핑거프린팅 관리 시스템에 등록 절차를 거쳐야 한다. (그림 6)에 등록 과정을 도식화하여 보여주고 있으며 화살표에 표시된 번호 순서대로 서술하면 다음과 같다.



(그림 6) 등록 과정

2.1 핑거프린팅 관리 시스템은 콘텐츠 유통 시스템의 서비스 목적, 요구사항– 콘텐츠 유형, 허용 왜곡 범위, 공모공격 허용 여부 등 –에 따라 다양한 핑거프린팅 알고리즘들을 보유하고 있다고 가정한다.

우선 콘텐츠 유통 시스템은 이러한 다양한 핑거프린팅 알고리즘들의 기능을 분석하고 가장 적당한 핑거프린팅 프로그램을 선택한다.

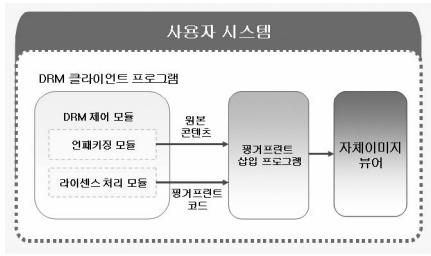
2.2 핑거프린팅 관리 시스템은 콘텐츠 유통 시스템이 핑거프린팅 서비스를 제공받을 수 있도록 핑거프린팅 삽입 프로그램, 콘텐츠 유통 시스템 ID를 전달하고 불법콘텐츠 추적현황을 열람할 수 있는 URL을 전송한다.

3. 사용자 시스템

사용자 시스템은 DRM 클라이언트 프로그램, 핑거프린트 삽입 프로그램, 그리고 자체 이미지 뷰어로 구성되어 있다. (그림 7)에서는 사용자 시스템의 구성도를 보여주고 있으며 각 구성 요소들의 기능들은 다음과 같다.

3.1 DRM 클라이언트 프로그램

- 사용자가 콘텐츠를 구매하면 DRM 시스템으로부터 패키징된 콘텐츠(암호화된 콘텐츠)와 라이선스를 전송받는다.
- 암호화 라이브러리 및 메타데이터 해석기로 구성된 언패키징 모듈은 암호화된 콘텐츠를 언패키징(복호화)을 수행한다.



(그림 7) 사용자 시스템 구성도

- 라이선스 처리 모듈은 라이선스를 인증하고 라이선스에 명시된 메타데이타를 근간으로 사용 권한을 통제한다.
- 복호화된 콘텐츠와 라이선스에 포함된 핑거프린트 코드를 가지고 핑거프린트 삽입 프로그램을 호출한다.

3.2 핑거프린팅 삽입 프로그램

- 원본 콘텐츠에 핑거프린트 코드를 삽입한다.

3.3 자체 이미지 뷰어

- 핑거프린트 코드가 삽입된 이미지를 화면에 디스플레이 한다.

본 논문에서는 범용 뷰어 예를 들어, 알씨(ALSee), ACDSee, 포토데스크, 다바 등은 고려하지 않는데, 그 이유는 다음과 같다.

첫째, 핑거프린트 삽입은 압축된 콘텐츠를 디코드(decode)한 후에 수행해야 한다. 즉 범용 뷰어가 콘텐츠를 디코드한 후에 핑거프린팅 삽입 프로그램을 호출해야 하는데, 현실적으로는 어렵다. 물론 핑거프린팅 삽입 프로그램이 강제적으로 시스템 제어를 후킹하여 핑거프린트 코드를 삽입하도록 강요하는 방법이 있을 수 있다. 그러나 이 방법도 다양한 범용 뷰어를 모두 지원할 수는 없을 것이다.

둘째, 범용 뷰어와 핑거프린팅 삽입 프로그램이 상호 통신을 한다고 가정해도 이와 같은 환경에서는 보안상의 문제가 존재하여 원본 데이터의 해킹을 용이하게 하는 원인을 제공할 수 있다.

셋째, 이미지 콘텐츠에 대한 DRM 시스템 서비스는 대부분 자체 뷰어로 이루어지고 있다.

따라서 이러한 이유로 이미지의 경우 범용 뷰어를 대상으로 핑거프린트 코드를 삽입하는 것은 현실적으로 어렵다. 그러나 오디오나 비디오 콘텐츠인 경우에는 시스템 제어의 후킹을 통한 강제적인 핑거프린트 코드 삽입이 가능하기 때문에 범용 플레이어의 사용을 고려해야 한다.

VI. 암호화 메커니즘

DRM 시스템에서는 안전한 콘텐츠 전달을 위해 암호화 메커니즘에 대한 연구가 진행되고 있다[9] [10] [11].

DRM 시스템과 핑거프린팅 시스템의 통합에 있어서 중요한 정보는 핑거프린트 코드와 삽입 및 추출 시에 사용될 생성키이며, 신뢰성 있는 통합 시스템을 위해서는 사용자 시스템과 검색 시스템에 이것들이 안전하게 제공되어져야 한다. 이 정보가 누출될 경우, 핑거프린팅 서비스의 근본 기능인 부정자 추적 수행에 문제가 발생하기 때문이다. 이에 본 장에서는 핑거프린트 코드와 생성키의 안전한 전달을 위한 암호화 메커니즘을 제안하고자 한다.

1. 통합 프레임워크의 요구 조건

다음은 암호화 메커니즘 설계시 통합 프레임워크가 만족해야 할 사항이다.

- **핑거프린팅 알고리즘의 기밀성**
  핑거프린팅 알고리즘 소스는 알고리즘 제공 시스템만 알고 있어야 한다.

- **핑거프린트 코드의 기밀성**
  콘텐츠에 삽입될 사용자의 정보 즉 핑거프린트 코드는 핑거프린팅 관리 시스템만 알고 있어야 한다.
- **핑거프린트 코드와 생성키의 무결성**
  사용자 시스템에 설치된 핑거프린팅 삽입 프로그램은 핑거프린팅 관리 시스템이 발급한 핑거프린트 코드와 생성키에 대한 무결성을 보장해야 한다.
- **핑거프린트 코드와 생성키의 위조 불가**
  핑거프린팅 관리 시스템 이외의 다른 시스템에서는 정확한 핑거프린트 코드와 생성키를 생성할 수 없어야 한다.
- **핑거프린팅 알고리즘과 핑거프린트 코드의 적합성**
  핑거프린팅 관리 시스템이 생성한 핑거프린트 코드는 반드시 대응하는 핑거프린트 삽입 프로그램에 의해 삽입됨을 보장해야 한다.

2. 제안 시스템

[매개변수 및 시스템 설정]

pg_{emb}, pg_{dec} : 핑거프린팅 삽입 및 추출 알고리즘
F_{code} : 핑거프린트 코드
$gk_{F_{code}}$: F_{code} 삽입, 추출에 사용될 생성키
$E_k(\cdot)$, $D_k(\cdot)$: 키 k를 이용한 암호 및 복호 알고리즘
$Sign_k(\cdot)$: 키 k를 이용한 전자서명 생성 알고리즘
$Ver_{k'}(\cdot)$: 키 k'을 이용한 전자서명 검증 알고리즘
$h(\cdot)$: 해쉬 알고리즘
$Alg[k]$: k가 하드코딩[4]된 알고리즘 Alg
sk_{pg}, pk_{pg} : 핑거프린팅 삽입 · 추출 알고리즘의 비밀키 및 이에 대응되는 공개키
sk_{FPMS}, pk_{FPMS} : 핑거프린팅 관리 시스템의 비밀키 및 이에 대응되는 공개키

(그림 8)은 제안 암호화 메커니즘의 구성도이며, 시스템은 아래의 절차로 수행된다.

Step 1 : 알고리즘 제공 시스템 → 핑거프린팅 관리 시스템 : $pg_{emb}[pk_{FPMS}, sk_{pg}]$, $pg_{dec}[sk_{pg}]$

- 알고리즘 제공 시스템은 핑거프린팅 관리 시스템에 핑거프린팅 삽입 및 추출 알고리즘을 제공한다.
- 이때 전달되는 핑거프린팅 삽입 알고리즘, pg_{emb}에는 pk_{FPMS}와 sk_{pg}가 하드 코딩되어 있으며,
- 핑거프린팅 추출 알고리즘, pg_{dec}에도 sk_{pg}가 하드 코딩되어 있다.

4) 프로그램 소스 자체에 어떤 data값을 직접 적어두는 방식

Step 2 : 핑거프린팅 관리 시스템 → 검색 시스템: $E_{pk_{pg}}(gk_{F_{code}}),\ pg_{dec}[sk_{pg}]$

– 핑거프린팅 관리 시스템은 검색 시스템에 생성키, $gk_{F_{code}}$와 $pg_{dec}[sk_{pg}]$를 제공한다.

– 이 때, $gk_{F_{code}}$는 pk_{pg}로 암호화되어 전달된다.

Step 3 : 사용자 시스템

– 사용자 시스템은 DRM 클라이언트 프로그램과 핑거프린팅 삽입 프로그램을 설치하고, 콘텐츠 유통 시스템에 콘텐츠 구매를 요청한다.

Step 4 : 콘텐츠 유통 시스템

– 콘텐츠 유통 시스템은 DRM에 관련된 기능을 수행하고, 핑거프린팅 관리 시스템에 구매자에 대응하는 핑거프린트 코드를 요청한다.

Step 5 : 핑거프린팅 관리 시스템 → 콘텐츠 유통 시스템: $E_{pk_{pg}}(F_{code}), Sign_{sk_{FPMS}}(h(F_{code}))$, $E_{pk_{pg}}(gk_{F_{code}}), Sign_{sk_{FPMS}}(h(gk_{F_{code}}))$

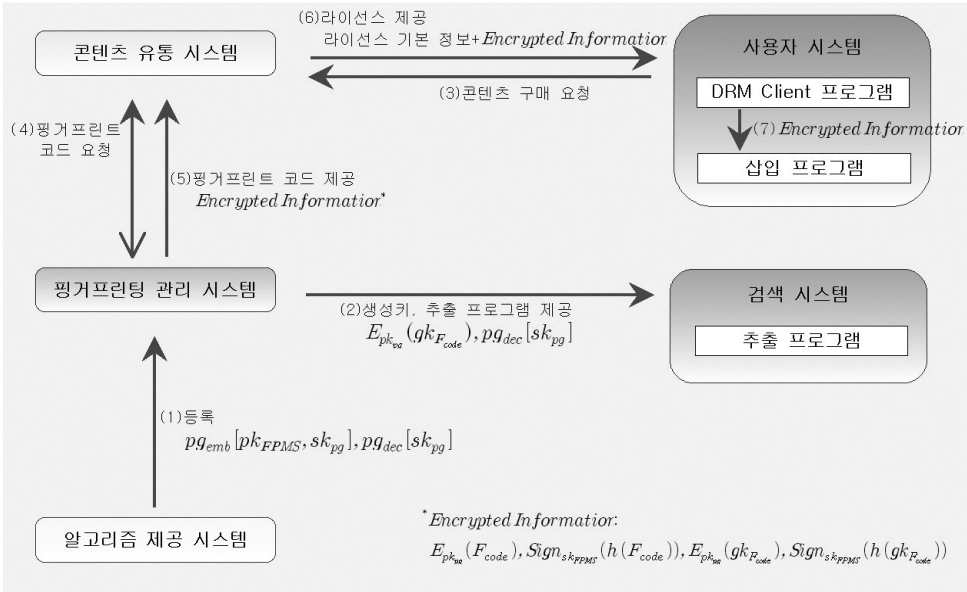
– 핑거프린팅 관리 시스템은 F_{code}와 $gk_{F_{code}}$를 아래와 같이 처리한 후, 콘텐츠 유통 시스템에 제공한다.

① $E_{pk_{pg}}(F_{code})$: 핑거프린트 관리 시스템은 해당 핑거프린팅 알고리즘의 공개키 pk_{pg}로 F_{code}를 암호화한다.

② $Sign_{sk_{FPMS}}(h(F_{code}))$: 해쉬 알고리즘을 이용하여 F_{code}를 해쉬한 후, 그 값을 핑거프린팅 관리 시스템의 비밀키, sk_{FPMS}를 이용하여 전자서명한다.

③ $E_{pk_{pg}}(gk_{F_{code}})$: pk_{pg}로 생성키, $gk_{F_{code}}$를 암호화한다.

④ $Sign_{sk_{FPMS}}(h(gk_{F_{code}}))$: $gk_{F_{code}}$에 대한



(그림 8) 암호화 메커니즘 구성도

해쉬값을 구한 후, 이 값에 대해 sk_{FPMS}으로 전자서명한다.

Step 6 : 콘텐츠 유통 시스템 → 사용자 시스템: 라이선스

- 콘텐츠 유통 시스템은 Step 5에서 받은 암호화된 정보를 라이선스 내부에 삽입하여 사용자 시스템의 DRM 클라이언트 프로그램에 전달한다.

Step 7 : 사용자 시스템

- 사용자 시스템 내 DRM 클라이언트 프로그램은 Step 6에서 제공받은 정보를 같은 시스템내의 삽입 프로그램에 전달한다.
- 삽입 프로그램은 전달받은 정보를 아래의 절차에 따라 복호하고, 검증한 후, 검증에 성공하면 해당 콘텐츠에 핑거프린트 코드, F_{code}를 삽입한다.
  ① $D_{sk_{pg}}(E_{pk_{pg}}(F_{code}))$: pg_{emb}에 하드 코딩되어 있는 sk_{pg}로 $E_{pk_{pg}}(F_{code})$를 복호하여 F_{code}를 얻는다.
  ② $Ver_{pk_{FPMS}}(Sign_{sk_{FPMS}}(h(F_{code})))$: 먼저 핑거프린팅 관리 시스템의 공개키 pk_{FPMS}를 이용하여, $h(F_{code})$를 얻는다. ①에서 얻은 F_{code}를 해쉬 알고리즘을 이용하여 해쉬한 후, 그 값과 위에서 얻은 $h(F_{code})$가 같은 지 확인한다. 이는 F_{code}의 무결성과 위조 여부 확인을 위한 절차이므로, 두 값이 같지 않으면 작업을 중지하고, 그렇지 않으면 다음 단계를 수행한다.
  ③ $D_{sk_{pg}}(E_{pk_{pg}}(gk_{F_{code}}))$: sk_{pg}로 $E_{pk_{pg}}(gk_{F_{code}})$를 복호하여 생성키, $gk_{F_{code}}$를 얻는다.
  ④ $Ver_{pk_{FPMS}}(Sign_{sk_{FPMS}}(h(gk_{F_{code}})))$: pk_{FPMS}를 이용하여, $h(gk_{F_{code}})$를 얻고, ③에서 얻은 $gk_{F_{code}}$를 해쉬 알고리즘을 이용하여 해쉬한 후, 그 값과 위에서 얻은 $h(gk_{F_{code}})$를 비교한다. 이 역시, $gk_{F_{code}}$의 무결성과 위조 여부 확인을 위한 절차이므로, 두 값이 동일한 경우에만 콘텐츠를 실행할 수 있도록 한다.

Step 8 : 검색 시스템

- 검색 시스템은 인터넷에 유포된 콘텐츠를 수집하고 이 콘텐츠들에서 핑거프린트 코드 추출을 시도한다.
- 이 때, 검색 시스템은 $E_{pk_{pg}}(gk_{F_{code}})$과 수집된 콘텐츠로 핑거프린팅 추출 프로그램 $pg_{dec}[sk_{pg}]$을 호출한다. 핑거프린팅 추출 프로그램의 내부에 하드 코딩된 sk_{pg}을 이용 $D_{sk_{pg}}(E_{pk_{pg}}(gk_{F_{code}}))$를 수행하여 생성키, $gk_{F_{code}}$를 얻는다.
- 위에서 얻은 $gk_{F_{code}}$로, 수집된 콘텐츠에서 핑거프린트 코드를 추출한다.

3. 제안 시스템의 분석

본 장에서는 제안 시스템의 안전성 및 특성을 앞에서 제시한 요구 조건에 따라 분석한다.

• 핑거프린팅 알고리즘의 기밀성

제안 시스템에서 알고리즘 제공 시스템은

핑거프린팅 삽입 · 추출 알고리즘을 핑거프린팅 관리 시스템에 전달한다. 이 때, 알고리즘은 소스 그 자체가 아니라, 컴파일된 실행 파일 형태로 전달된다. 따라서 알고리즘을 개발한 알고리즘 제공 시스템 이외의 다른 시스템은 핑거프린팅 알고리즘을 알 수 없다. 따라서 제안 시스템은 핑거프린팅 알고리즘의 기밀성을 제공한다.

- **핑거프린트 코드의 기밀성**

  제안 시스템에서 핑거프린트 코드는 해당 핑거프린팅 알고리즘의 공개키로 암호화되어 전송된다. 제안 시스템에서는 수학적으로 안전하다고 증명된 암호 알고리즘을 사용하므로, 사용된 암호 알고리즘이 안전한 이상, 핑거프린트 코드를 직접 생성한 시스템 이외의 다른 개체는 생성된 핑거프린트 코드를 알 수가 없다. 본 시스템에서는 핑거프린트 관리 시스템만 핑거프린트 코드를 알고 있으므로, 핑거프린트 코드의 기밀성을 제공한다고 볼 수 있다.

- **핑거프린트 코드와 생성키의 무결성**

  제안 시스템에서는 사용자 시스템의 삽입 프로그램이 콘텐츠에 핑거프린트 코드를 삽입하기 전에 생성키와 핑거프린트 코드의 변조 유 · 무를 확인한다. 2장의 Step 7에 설명된 것처럼, 핑거프린트 코드와 생성키는 해당 핑거프린팅 알고리즘의 공개키로 암호화되었을 뿐만 아니라, 해쉬된 상태로도 전송되기 때문에, 중간에 그 값이 변경되었다면, Step 7의 무결성 확인 단계를 통과할 수 없다. 왜냐하면 핑거프린트 코드의 해쉬값이 또 다시 핑거프린팅 관리 시스템의 비밀키로 이중 암호화되었기 때문에, 검증 절차를 통과하기 위해서는 핑거프린팅 관리 시스템의 비밀키를 알고 있어야 하기 때문이다. 핑거프린팅 관리 시스템의 비밀키가 노출되지 않는 이상, 제안 시스템은 핑거프린트 코드와 생성키의 무결성을 제공한다.

- **핑거프린트 코드와 생성키의 위조 불가**

  제안 시스템에서 핑거프린트 코드와 생성키는 핑거프린팅 관리 시스템의 비밀키로 암호화되어 전송되고, 이의 검증 시 비밀키에 대응되는 공개키가 요구된다. 따라서 다른 시스템이 핑거프린트 코드와 생성키를 위조하기 위해서는 반드시 핑거프린팅 관리 시스템의 비밀키를 알아야 한다. 제안 시스템에서는 핑거프린팅 관리 시스템만이 자신의 비밀키를 알고 있으므로, 핑거프린팅 관리 시스템 이외의 다른 시스템은 정확한 생성키와 핑거프린트 코드를 생성할 수 없다.

- **핑거프린팅 알고리즘과 핑거프린트 코드의 적합성**

  제안 시스템에서 핑거프린트 코드 삽입 및 추출에 사용되는 생성키는 해당 알고리즘의 공개키로 암호화되어 삽입 프로그램에 전달된다. 또한 이의 복호에 이용될 비밀키도 해당 알고리즘에 하드 코딩되어 전달된다. 따라서 생성키가 적합하지 않은 다른 알고리

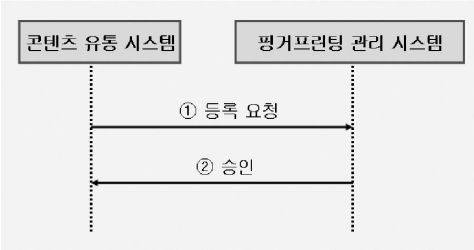
즘의 공개키로 암호화된다면, 생성키 추출 및 핑거프린트 코드 삽입은 제대로 실행될 수 없다. 따라서 제안 시스템은 핑거프린팅 알고리즘과 핑거프린트 코드, 생성키의 적합성을 보장한다.

VII. 통합 프레임워크 상호 인터페이스

V 장에서는 콘텐츠 유통 시스템과 핑거프린팅 시스템과의 통합 프레임워크에 대해서 설명하였다. 본 장에서는 통합 프레임워크를 구성하고 있는 각 시스템간 인터페이스, 핑거프린트 구조, 그리고 라이선스에 대하여 서술한다.

1. 등록 인터페이스

콘텐츠 유통 시스템과 핑거프린팅 관리 시스템과의 통신을 위해 초기 설정 인터페이스가 필요하다. 콘텐츠 유통 시스템은 서비스하고자 하는 서비스 형태 및 요구사항 스펙에 따라 원하는 핑거프린팅 프로그램을 선택하여야 한다. 등록절차 인터페이스는 (그림 9)에서 보여주고 있다.



(그림 9) 등록 인터페이스

1.1 등록 요청

콘텐츠 유통 시스템은 핑거프린팅 서비스를 받기 위해 핑거프린팅 시스템에 등록요청을 해야 한다. 이 때 서비스 받고자 하는 핑거프린팅 프로그램을 선택하고 다음과 같은 정보를 제공한다.

- IP Address: 핑거프린팅 관리 시스템과 통신할 콘텐츠 유통 시스템의 IP 주소
- 일련번호: 콘텐츠 유통 시스템이 등록 요청한 순번을 의미한다. 예를 들어 III 장에서 종속적인 구조를 가진 경우에는 콘텐츠 공급자에 따라 여러번 등록 요청을 할 수 있다.

1.2 승인

핑거프린팅 관리 시스템은 콘텐츠 유통 시스템의 서비스 요청에 대한 승인 프로세스를 수행하고 다음과 같은 정보를 전달한다.

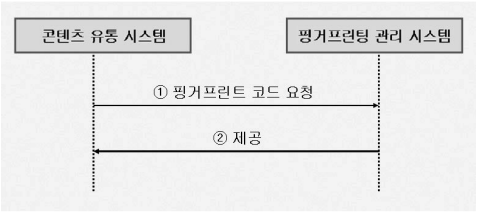
- 핑거프린팅 삽입 프로그램: 서비스 받고자 하는 핑거프린팅 삽입 프로그램
- 핑거프린팅 삽입 프로그램 고유번호: 핑거프린팅 프로그램 고유 번호
- 핑거프린팅 삽입 프로그램 버전: 제공한 삽입 프로그램의 버전
- 콘텐츠 유통 시스템 고유번호: 핑거프린팅 관리 시스템이 서비스 요청시 콘텐츠 공급 시스템을 인식하기 위한 고유 번호
- URL: 불법콘텐츠 추적현황을 열람할 수 있는 URL 정보

위의 내용을 ASN.1 형태로 표시하면 다음과 같다.

```
ApproveRequest ::= SEQUENCE {
  fpInsertProg  FPInsertProgID,
  DitributionSystemNum        SEQUNCE        OF
DitributionSystemID
}
FPInsertProg ::= SEQUENCE {
  fpInsertProgData FPInsertProgData
  fpInsertProgID    FPInsertProgID,
  fpInsertProgVer   [0] EXPLICIT
}
FPInsertProgData ::= BIT
FPInsertProgID ::= INTEGER
FPInsertProgVer ::= INTEGER { v1(0) }.
CPServiceSystemID ::= INTEGER
URL ::= STRING
```

2. 핑거프린트 코드 요청 · 제공 인터페이스

사용자가 콘텐츠 구매를 요청할 때 콘텐츠 유통 시스템은 구매자와 관련된 정보를 수집하고 이 정보와 대응되는 구매자의 일련번호를 생성한 후, 핑거프린팅 관리 시스템에 핑거프린트 코드를 요청한다. 핑거프린팅 관리 시스템은 일련번호와 대응되는 핑거프린트 코드를 생성하여 제공하면 콘텐츠 유통 시스템은 사용자에게 핑거프린트 코드가 포함된 라이선스를 발급한다. 핑거프린트 코드 요청 · 제공 인터페이스는 (그림 10)에서 보여주고 있다.



(그림 10) 핑거프린트 코드 요청 · 제공 인터페이스

2.1 핑거프린트 코드 요청

- 콘텐츠 유통 시스템은 핑거프린팅 관리 시스템에 핑거프린트 코드 발급 요청을 위해 아래와 같은 정보들을 전송한다.
  - 콘텐츠 유통 시스템 고유 번호: 등록 과정에서 받은 콘텐츠 유통 시스템의 고유 번호
- 콘텐츠 타입: 이미지, 오디오, 비디오 등
  - 콘텐츠의 타입에 따라 핑거프린트 코드 길이가 달라질 수 있다.
- 핑거프린팅 삽입 프로그램 고유 번호: 서비스 받고자하는 핑거프린팅 삽입 프로그램 고유 번호
- 핑거프린팅 삽입 프로그램 버전: 제공한 핑거프린팅 삽입 프로그램의 버전
- 구매자 고유번호: 콘텐츠 유통 시스템은 사용자를 구별할 수 있는 사용자의 고유 번호
  - 사용자 고유 번호, 사용자 IP 주소, 사용자 하드 디스크 고유 번호 등과 같은 정보를 이용하여 고유번호를 생성할 수 있다.

위의 내용을 ASN.1 으로 표현하면 다음과 같다.

```
FPCodeRequset :: SEQUENCE {
 DistributionSystempID DistributionSystemID,
 contentTy  ContentType,
 fpInsertProgID FPInsertProgID,
 fpInsertProgVer [0] EXPLICIT FPInsertProgVer
                    DEFAULT v1,
 issueNum IssueNum,
}
IssueNum ::= INTEGER
```

2.2 제공

먼저 핑거프린팅 관리 시스템은 콘텐츠 타입

과 핑거프린팅 삽입 프로그램이 일치하는 지를 확인한다. 일치한다면 핑거프린팅 삽입 프로그램에서 사용하는 핑거프린트 코드 길이를 확인하고, 콘텐츠 유통 시스템이 제공하는 구매자 고유번호에 대응하는 핑거프린트 코드를 생성하게 된다. 핑거프린트 코드는 핑거프린팅 프로그램별로 유일한 값을 갖는다. 아래와 같은 정보를 콘텐츠 유통 시스템에 제공한다.

- 핑거프린트 코드를 핑거프린팅 프로그램의 공개키로 암호한 값
- 핑거프린트 코드의 해쉬 값을 핑거프린팅 관리 시스템의 비밀키로 전자서명한 값
- 생성키를 핑거프린팅 프로그램의 공개키로 암호화한 값
- 생성키를 해쉬한 값을 핑거프린팅 관리시스템의 비밀키로 전자서명한 값
- 해쉬 함수
- 핑거프린팅 관리시스템의 공개키

위의 내용을 ASN.1 형태로 표시하면 다음과 같다.

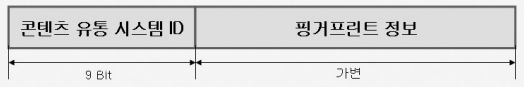
```
MakeFPCode ::= SEQUENCE {
 EInsertModulePublicKey[fingerprintCode]
EncryFingerprintCode,
 EFPmanagementserverPrivateKey[Hashing[fingerprintCode]]

EncryHashingFingerprintCode
 EInsertModulePublicKey[fingerprintKey] EncryFingerprintKey
 EFPmanagementserverPrivateKey[Hashing[fingerprintKey]]
                          EncryHashingFingerprintKey
 hashFunc HashFunc
 FPmanagementserverPublicKey BIT STRING
}
```

```
EncryFingerprintCode ::= SEQUENCE {
    Length       INTEGER
    EncryCode  BIT STRING
}
EncryHashingFingerprintCode ::= BIT STRING
EncryHashingFingerprintKey ::= BIT STRING
EncryFingerprintKey ::= BIT STRING
HashAlgorithm ::=SHA1
EncryptionAlgorithm::= RSA
SignatureAlgorithm ::= RSA
```

3. 핑거프린트 코드의 구조

핑거프린팅 관리 시스템에서 생성되는 핑거프린트 코드는 (그림 11)과 같이 콘텐츠 유통 시스템 고유 번호와 알고리즘에 의해 생성되는 콘텐츠 핑거프린트 정보로 구성된다.



(그림 11) 핑거프린트 코드의 구조

콘텐츠 유통 시스템 고유 번호는 핑거프린트 서비스를 받기 위해 등록할 때 발급 받는 고유번호를 의미하고 길이는 9bit이다. 콘텐츠 타입에 따라 다를 수 있지만 콘텐츠의 질적 저하를 막기 위해서는 삽입되는 정보의 양이 적으면 적을수록 좋다. 콘텐츠 유통 시스템 고유번호를 핑거프린트 코드에 추가한 이유는 검색 시스템이 핑거프린트 코드를 추출할 경우 이 콘텐츠가 어떤 콘텐츠 유통 시스템에서 서비스 되었는지 알 수 있고, 이를 통해 알면 해당 핑거프린팅 삽입 프로그램도 알 수 있기 때문이다. 콘텐츠 핑거프

린트 정보의 길이는 삽입 핑거프린팅 프로그램에 따라 가변적이다.

4. 라이선스 구조

콘텐츠 유통 시스템은 핑거프린트 코드 정보를 받아 사용자에게 제공하는 라이선스에 암호화된 핑거프린트 코드를 삽입하여 사용자의 DRM 클라이언트 프로그램에 전송할 수 있다. 핑거프린팅 시스템과의 연동을 위해 사용되는 라이선스의 구조는 핑거프린트 코드를 덧붙이기 위한 영역을 설정하는 것 외에는 기존의 클리어링 하우스의 라이선스 구조와 같다. 이와 같이 핑거프린트 코드를 라이선스에 부가하는 방법은 시스템에 따라 선택적으로 사용될 수 있다. 다른 방법으로는 라이선스 구조는 기존의 라이선스 구조대로 하고 핑거프린팅 시스템으로부터 받은 핑거프린트 코드를 라이선스와 함께 전송해 주는 방법도 가능하다.

5. 핑거프린팅 삽입 프로그램 인터페이스

핑거프린팅 삽입 프로그램이 DRM 클라이언트 프로그램에서 원활하게 동작할 수 있어야 한다. 그러기 위해서 (그림 12)와 같이 DRM 클라이언트 모듈과 핑거프린팅 삽입 프로그램과의 입력 및 출력 인터페이스의 정의가 필요하다.

(그림 12) 핑거프린팅 삽입프로그램 인터페이스

5.1 핑거프린팅 삽입 프로그램 호출

DRM 클라이언트 프로그램이 핑거프린팅 삽입 프로그램을 호출할 때의 각 파라메타는 아래와 같다.

- 이미지 데이터
  - 핑거프린트 코드를 삽입하고자 하는 이미지 데이터로 압축이 풀린 Raw 데이터
- 이미지 크기
  - 이미지의 높이와 폭에 대한 정보
- 핑거프린트 코드를 핑거프린팅 프로그램의 공개키로 암호한 값
- 핑거프린트 코드를 해쉬한 값을 핑거프린팅 관리시스템의 비밀키로 전자서명한 값
- 생성키를 핑거프린팅 프로그램의 공개키로 암호화한 값
- 생성키를 해쉬한 값을 핑거프린팅 관리시스템의 비밀키로 전자서명한 값
- 해쉬 함수

위의 내용을 ASN.1 형태로 표시하면 다음과 같다.

```
CallFPInsertProg ::= SEQUENCE {
 imageData  ImageData
 imageSize  ImageSize
 EInsertModulePublicKey[fingerprintCode] EncryFingerprintCode
 EFPmanagementserverPrivateKey[Hashing[fingerprintCode]]
                          EncryHashingFingerprintCode
 EInsertModulePrivateKey[Hashing[fingerprintKey]]
                          EncryHashingFingerprintKey
 EInsertModulePublicKey[fingerprintKey]  EncryFingerprintKey
 hashFunc HashFunc
}
ImageData ::= BIT STRING
```

```
ImageSize ::= SEQUENCE {
   imageHeight unsigned INTEGER,
   imageWidth  unsigned INTEGER,
}
```

5.2 핑거프린팅 삽입 프로그램의 출력

암호화된 핑거프린트 코드와 키 값을 복호화하고 전자서명을 이용하여 진위여부를 검증한다. 오류가 발생하지 않았을 경우 핑거프린팅 삽입 프로그램은 생성 키를 가지고 이미지에 핑거프린트 코드를 삽입하게 된다. 생성 키는 핑거프린트 코드의 랜덤 노이즈를 생성할 때 사용되어진다.

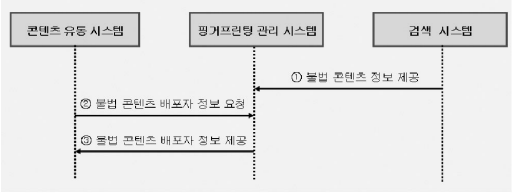
- 핑거프린트 코드가 삽입된 이미지 데이터
  – 이미지 뷰어에 전송하여 디스플레이 할 수 데이터 포맷이다.

5.3 오류 메시지

입력된 데이터 등에 오류가 발생 했을 경우에 오류 메시지를 제공한다.

6. 불법 콘텐츠 배포자 제공 인터페이스

핑거프린팅 관리 시스템이 불법 콘텐츠를 추적하였을 경우 관련 배포자 정보를 콘텐츠 유통 시스템에 제공하여야 하며 (그림 13)에서는 이러한 인터페이스를 보여주고 있다.



(그림 13) 불법 콘텐츠 배포자 제공 인터페이스

6.1 불법 콘텐츠 정보 제공

검색 시스템이 인터넷 상에 공유되고 있는 불법 이미지를 검색 및 수집하여 핑거프린트 코드를 추출한다. 핑거프린트 코드가 존재할 경우 불법 콘텐츠로 간주하고 아래와 같은 정보를 핑거프린팅 관리 시스템에 제공한다.

- 수집 정보: 검색 위치, 검색 시간
- 콘텐츠 정보: 사이즈, 포맷, 콘텐츠 명, 링크 정보 등
- 사용자 정보: 불법 공유한 사용자 ID, IP 주소 등

6.2 불법 콘텐츠 배포자 정보 요청

콘텐츠 유통 시스템이 등록 절차시 전송받은 URL을 통해서 불법콘텐츠 추적 현황 열람을 요청할 수 있다.

6.3 불법 콘텐츠 배포자 정보 제공

핑거프린팅 관리 시스템은 콘텐츠 유통 시스템의 요청이 들어 올 때 URL을 통하여 아래와 같은 정보를 보여준다.

- 일련번호 : 추출된 핑거프린트코드와 일치하는 구매자의 고유번호
- 수집 정보 : 검색 위치, 검색 시간
- 콘텐츠 정보 : 사이즈, 포맷, 콘텐츠 명, 불법 콘텐츠 링크 정보 등
- 사용자 정보 : 불법 공유한 사용자 ID, IP 주소 등

위의 내용을 ASN.1 형태로 표시하면 다음과 같다.

```
FPillegalInfo :: SEQUENCE {
  imageSaveUrl ImageSaveUrl
  searchTime SearchTime
  searchUrl SearchUrl
  fileType  FileType
  conentLength ContentLength
  linkWord  LinkWord
  }
  imageSaveUrl ::= STRING
  searchTime ::= STRING
  searchUrl ::= STRING
  fileType ::= INTEGER
  conentLength ::= INTEGER
  linkWord ::= STRING
```

VIII. 결론

국내 · 외에서 DRM 기술에 대한 표준화를 추진하고 있지만 이미 제품으로 출시되어 서비스되고 있는 상황에서 업체간 손익 등 많은 장애요소를 안고 있어 표준화 진행이 쉽지 않다. 국내의 경우도 마찬가지이며, 이러한 DRM 시스템이 오히려 유료 디지털 콘텐츠의 활성화를 저해하고 있다.

또한 DRM 기술만으로는 디지털 콘텐츠의 저작권 보호에 있어서 기술적인 한계가 있으며, 이를 극복하기 위해 핑거프린팅 기술이 요구되고 있다.

현재까지 이러한 핑거프린팅 시스템과 DRM 시스템과의 통합에 관한 표준화 추진은 없는 상태이다. 따라서 본 논문에서는 인터넷 상에서 불법복제 콘텐츠를 자동으로 다운로드하여 최초 배포자를 추적할 수 있는 핑거프린팅 시스템을 정의하고 설계하였다. 그리고 DRM 시스템과의 핑거프린팅 시스템과의 통합 프레임워크와 인터페이스, 그리고 암호화 메커니즘을 제안하였다.

본 논문에서 제안하고 있는 통합 프레임워크를 표준화함으로써 디지털 콘텐츠의 불법유통을 방지와 저작권 보호를 위한 투명한 디지털 콘텐츠 유통 질서를 확립할 수 있을 것으로 기대된다. 또한 콘텐츠 생산자 및 저작권자를 불법복제로 인한 경제적 손실로부터 보호하여 다양한 고품질의 콘텐츠 생산을 유도할 수 있고 그로인해 디지털 콘텐츠 산업의 활성화를 촉진할 수 있을 것이다.

>> 참고문헌

[1] 오원근, "DRM 표준화 및 평가기술", 전자통신동향분석 통권 94호 제20권 제4호 2005. 8

[2] Jun-seok Lee, "A DRM Framework for Distributing Digital Contents through the Internet", ETRI Journal vol 25. num 6, 2003

[3] Bill Rosenblat, Bill Trippe, and Stephen Mooney, "Digital Rights Management, Business and Technology", M&T Book, pp.79-102, 2002

[4] E.V.Faber, R.Hammelrath, and F.P.Heider, "The Secure Distribution of Digital Contents", Proc. Computer Security Application Conf., 13th Ann., pp.16-22, Dec. 1997

[5] 정혜원, 이준석 "불법콘텐츠 추적기술 연구동향", 전자통신동향분석 통권 94호 제20권 제4호 2005.8

[6] Sarah Jung, Jongwon Seok, and Jinwoo Hong, "An Improved Detection Technique for Spread Spectrum Audio Watermarking with a Spectral Envelop Filter", ETRI J., vol.25, pp.52-54, Feb. 2003

[7] Mpeg-21, http://mpeg.nist.gov/
[8] OMA, Open Mobile Allianve,ttp://www.openmobilealliance.org/
[9] H. Sakamoto, M. Yamada, T. Nakamura, T. Nakanishi, " Additional Content-Related Service/Product Offering System Based on New Standards: MPEG-21 and Content ID/DOI", proc. IEEE Multimedia and Expo'02, Int'l Conf., 2002.
[10] A.O. Waller, G. Jones, T. Whitley, J.Edward, D. Kaleshi, A. Munro, B. MacFarlane, and A. Wood, "Securing the Delivery of Digital Content over the Internet", Electronics & Comm. Eng.J., vol.14, pp.239-248, Oct. 2002
[11] U. Kohl, "Secure Container Technology as a Basis for Cryptographically Secured Multimedia Communication", proc. multimedia and security Workshop at ACM Multimedia'98, Sept. 1998.

>> 저자 소개

이 준 석 (Junseok Lee)
· Email: leejs@etri.re.kr
· Tel: +82-42-860-1036
· Fax: +82-42-860-1051

- 1986.3 아주대학교 전산학 학사
- 1989.8 동국대학교 전산학 석사
- 2004.3 충남대학교 전산학 박사
- 1991.4 ~ 현재 : 한국전자통신연구원 책임연구원
- 주관심분야 : 저작권 보호 기술, e-러닝

정 혜 원 (HyeWon Jung)
· Email:leonid92@etri.re.kr
· Tel: +82-42-860-1277
· Fax: +82-42-860-1051

- 1999.2 : 경원대학교 전자계산학 학사
- 2001.8 : 연세대학교 컴퓨터과학과 석사
- 2002.7~현재 : 한국전자통신연구원 연구원
- 주관심분야 : 핑거프린팅, 콘텐츠 추적