논문 2011-2-26

멀티미디어 콘텐츠 보호를 위한 스마트 홈 환경

Smart Home Environment for the Protection of Multimedia Digital Contents

최기현*, 장경수**, 신호진***

Kee-Hyun Choi, Kyung-Soo Jang, Ho-Jin Shin

요 약 디지털 콘텐츠는 IT 산업의 핵심적인 콘텐츠로 인터넷의 발전과 더불어 다양한 분야에서 개발되고 있다. 사용자의 멀티미디어 장비가 다양해지고 성능이 향상되어 감에 따라 디지털 콘텐츠 보호는 더욱 복잡해지고 다양한 보호 시스템 개발을 요구한다. DRM(Digital Rghts Management)은 대표적인 콘텐츠 보호 시스템이며 이 기술 기반으로 다양한 콘텐츠 보호 기법이 등장하고 있다. 그러나 콘텐츠와 배포형태에 따른 다수의 기술을 적용해야하는 문제점과 “analog hole” 문제 및 키 분배 방식의 비효율성으로 인해 안전하게 보호하기 어렵다. 본 논문에서는 이러한 문제점을 해결하기 위해서 RFID(Radio Frequency Identification) 기술을 이용한 콘텐츠의 인증 및 보호 시스템 제안하고 스마트 홈 환경에서 자유로운 콘텐츠의 복제 및 효율적인 콘텐츠관리가 가능함을 보인다.

Abstract As internet is getting advanced day by day, digital contents have been developed in various areas as killer content in the IT industry. It needs to develop lots of complicated digital content protect systems due to the enhancement and variety of user's multimedia devices. Although there are lots of protect systems based on DRM(Digital Rights Management) technology, it is difficult to provide secure protection because of the problems resulting from analog hole problem, inefficiency of key sharing and various independent protect technologies. Thus, in this paper, we propose a novel authentication and protect system based on RFID(Radio Frequency Identification) technology to solve the problems and show possibility of free content duplication and efficient contents management in smart home environments.

Key Words : DRM, RFID, Digital Contents, Key sharing, Smart home environments

Ⅰ. 서 론

정보기술(IT)산업과 인터넷기술의 성장에 힘입어 멀티미디어 디지털 콘텐츠는 킬러 콘텐츠로써 기업의 전통적인 이윤 창출 역할을 하였다. 최근 유비쿼터스 환경에 맞추어 핸드헬드 디바이스를 비롯한 다양한 가전제품이 스마트화 되어 멀티미디어 디지털 콘텐츠의 배포 방식도 다양해지고 있으며 그 중요성은 더 커지고 있다. 따라서 콘텐츠 산업의 보호는 해당 산업뿐만 아니라 이와 연관된 산업의 발전에 기여하는 바가 크다. 그러나 불법적인 콘텐츠의 복제로부터 권리자의 저작권 보호는 제대로 이루어지고 있지 않다. 이러한 문제점을 해결하기 위해서 디지털 콘텐츠 보호를 위한 노력은 국내외에서 폭넓게 연구되어 왔으며 DRM(Digital Rights Management) 기술을 포함한 다양한 디지털 콘텐츠 보호기술이 등장하고 있다. 콘텐츠 보호기술의 개발에도 불구하고 불법적인 콘텐츠로부터 권리자의 저작권 보호가 제대로 이루어지지 않은 이유는 콘텐츠 보호기술 자체의 문제가 아니라

*정회원, 성균관대학교 정보통신기술연구소
**정회원, 경인여자대학 영상방송 정보과
***정회원 한신대학교 정보통신학과
접수일자: 2011.2.23, 수정일자: 2011.3.25
게재확정일자: 2011.4.15

시스템 외적인 문제를 해결하지 못하였기 때문이다. 기존의 보호기술은 주로 디지털 콘텐츠가 실행되기 전에 암호화 기법을 통해서 해당 콘텐츠를 보호하지만 실행 후에는 자유롭게 복제가 가능하다. 일부 보호기술은 실행 후의 콘텐츠 보호에 대한 기술(HDCP[4], DTCP[5])을 포함하고 있으나 다음의 문제점을 해결하지 못하였다. 첫째, 아날로그 복제로부터 자유로워 질수가 없다. 즉, 순수 "analog hole" 문제를 해결한 시스템이 현재까지 존재하지 않다. 둘째, 원본 콘텐츠에서 다양한 형태의 포맷으로의 복제를 막기 어렵다. 셋째, 실행하는 콘텐츠가 합법적인 미디어 매체(CD, DVD)에 저장되었는지 확인할 수 있는 방법이 없다. 본 논문에서는 이러한 문제점을 해결하기 위해서 RFID 기술을 이용한 스마트 홈 콘텐츠 보호 시스템을 제안하여 콘텐츠 인증방식을 개선하고 "analog hole" 문제를 해결하였다.

본 논문의 구성은 다음과 같다. 2장은 기존 콘텐츠 보호 시스템에 대해서 소개하고, 3장은 본 논문에서 제안한 RFID 기술을 이용한 인증 시스템을 통해서 기존 시스템의 문제점을 해결하기위한 방법을 논의하고 콘텐츠의 배포방식에 따른 인증 기법 및 보호 방법을 제안한다. 4장에서는 제안한 시스템을 이용한 시뮬레이션 결과를 보인다. 5장은 본 논문의 결론이다.

Ⅱ. 관련 연구

본 장에서는 기존 시스템의 소개와 문제점에 대해서 논의 한다. 디지털 콘텐츠 보호기술중에서 DRM 기술, CAS(Conditional Access System)기술, 복제방지 기술 등을 소개한다.

1. DRM 기술

DRM 기술은 콘텐츠의 생성에서 소멸에 이르는 전 과정에 걸쳐 콘텐츠의 저작권을 보호하기 위해서 사용된다[1][7][8]. 일반적으로 인터넷을 통한 콘텐츠의 배포에 사용되고 있으며 실시간 처리를 필요로 하는 콘텐츠의 보호에는 취약하고, DRM 상호연동 및 사용자의 다양한 기기로의 배포가 쉽지 않다. 최근 음반 산업의 4대 기업 (EMI group, Sony BMG, Universal Music Group, Warner Music group) 에서 DRM기술을 통한 콘텐츠의 배포를 포기한 이유는 DRM 기술로 보호된 콘텐츠가 쉽게 훼손될 수 있고 캡처 프로그램을 이용해서 다른 형태의 포맷으로 재생성이 가능하기 때문이다.

2. CAS 기술

디지털 방송 콘텐츠의 보호를 위한 기술로, 방송망을 통하여 전송되는 콘텐츠에 대해서 인가된 사용자에게만 수신 권한을 부여하는 기술이다. 일반적으로 CAS기술은 사용자의 접근을 제한하는 기술로 아날로그 방송에서는 스크램블(scramble) 방식을 의미하며[1][6], 최근 IPTV에서도 콘텐츠의 보호를 위해서 사용자의 수신제안 기법으로 연구되고 있다. CAS기술 또한 정상적인 사용자의 불법적인 콘텐츠 복제에 대해서 제어할 수 있는 방법이 없다. 정상적인 사용자의 PC를 통하여 수신된 신호는 소프트웨어/하드웨어를 통해서 캡처될 수 있기 때문이다.

3. 복제방지 기술

기기간의 전송 또는 기록 장치로 저장할 때 콘텐츠 불법복제 방지를 위한 기술이다. 대부분의 경우 암호화 알고리듬을 이용하여 기기간의 복제를 방지하는 목적으로 사용된다[4][5]. 최근 유비쿼터스 환경에서는 다양한 사용자의 기기가 존재하기 때문에 효율적인 기기간의 콘텐츠의 공유가 제공되어야 한다. 기기간의 전송에서 문제점은 암호화에 쓰인 키의 공유이며 일반적으로 그룹 키 또는 도메인권한 관리기술을 이용한다. 이러한 기술의 단점은 해당 기기의 성능과 무관하게 복잡한 암호화 시스템을 제공해야 한다는 것과 특정 케이블을 사용해야 하고 각기 다른 표준을 사용해야 한다는 것이다.

디지털 콘텐츠 보호기술은 콘텐츠 배포방식에 따라서 다양하게 연구 되고 있다. 스트리밍형태로 콘텐츠를 배포해야 하는 경우, 저장 매체(CD, DVD)를 통해서 배포하는 경우, 인터넷을 통해서 파일 형태로 배포하는 경우 등으로 나뉠 수 있다. 스트리밍 형태의 배포 방식에서는 제공될 콘텐츠를 준비하는 과정(mastering)을 통해 콘텐츠를 암호화 하고 사용자에게 키를 제공하는 방식을 사용한다. 이와 같이 다양한 형태의 보호기술이 존재하기 때문에 상이한 구조의 보호체계 상호간의 연동이 필요하며 사용자가 보유한 기기에서 자유로운 실행이 보장되어야 한다.

Ⅲ. 디지털 콘텐츠 보호를 위한 스마트 홈 환경

기존 디지털 콘텐츠 보호 시스템은 Ⅱ장에서 설명했던 바와 같이 DRM 기술의 상호 연동 및 다수의 실행기기를 허용해야하기 때문에 구조가 복잡하고 각각의 독립된 DRM기술을 중복해서 사용해야한다. 또한 기존 보호 시스템은 “analog hole” 문제를 효과적으로 해결하지 못하였으며 합법적으로 구매한 콘텐츠의 복제는 사실상 불가능 하였다. 디지털 콘텐츠가 보호받지 못하는 이유는 DRM 기술 기반의 보호 시스템 자체의 문제가 아니라 불법복제가 행해지는 근본적인 원인을 해결하기 위한 접근 방식이 잘못 되었기 때문이다. 본 논문에서는 콘텐츠 보호를 위해서 RFID 기술 기반 인증방식을 통해 기존 시스템에서 고려하지 못한 문제점인 불법복제 및 “analog hole” 문제를 해결하였다. 다음은 기존 시스템으로 해결하기 어렵거나 불가능한 문제점이다.

문제점 1: 디지털 콘텐츠가 배포될 당시의 매체(CD, DVD)에 저장되었는지 확인할 수 있는 방법이 없다. 즉, 물리적인 저장매체가 합법적으로 구매한 것인지 사용자가 임의로 복제한 콘텐츠를 저장하고 있는지 확인할 수 없다.

문제점 2: “analog hole” 문제는 단순하게 오디오나 비디오를 하드웨어를 통해서 복제하는 방식과 사용자의 개인용 PC를 통해서 실행되는 신호를 캡처하는 방식으로 나눌 수 있다. 캠코더나 녹음기와 같은 하드웨어를 통한 캡처가 전자에 포함 되며 순수 “analog hole” 문제라고 할 수 있다, 일반적으로 가장 문제시 되는 것이 PC를 통한 불법적인 복제이며 최근에는 출력 장비로 전송되는 시그널 자체가 디지털화되기 때문에 “digital hole” 문제라고 볼 수도 있다.

문제점 3: 사용자가 보유한 다양한 기기로의 복제가 자유롭지 않다. 합법적으로 구입한 콘텐츠는 자유로운 공유가 가능해야 하며, 불법적인 복제는 차단하는 기능이 필요하다. 문제점 1을 해결하기 위해서는 해당하는 기기에서만 유일하게 실행되도록 해야 하지만 DRM을 반대하는 가장 큰 이유인 합법적 콘텐츠의 자유로운 복제를 위해서는 댁내에 있는 사용자의 모든 기기에서 사용가능해야 하기 때문에 반드시 해결돼야 하는 문제다.

기존의 보호시스템에서는 콘텐츠가 어떤 매체에 저장되었더라도 해당 기기를 통해서 자유롭게 실행이 가능하다. 불법복제 콘텐츠가 저장되었는지 아닌지 물리적으로 확인하는 방법이 없다. 콘텐츠 인증과정에서 문제점 1을 해결하기 위해서는 물리적으로 객체의 식별을 할 수 있는 기술이 필요하다.

불법적인 콘텐츠 복제는 “analog hole”문제에서 발생하며 일반적으로 캠코더나 녹음기를 통한 복제는 품질이 낮기 때문에 대부분 PC를 통해서 불법 복제를 한다. 문제점 2를 해결하기 위해서는 실행되는 기기와 출력장치 또는 다른 멀티미디어 기기와의 암호화된 전송이 필요하다.

DRM 기술을 반대하는 이유 중에 하나가 바로 자유로운 콘텐츠의 공유이다. 문제점 3을 해결하기 위해서는 실행 장치중심의 콘텐츠 복제방지가 아니라 출력 장치에 따른 복제방지 기법이 필요하다. 또한 특정 케이블을 이용한 보호가 아니라 장치 독립적으로 사용할 수 있어야 한다.

1. 멀티미디어 디지털 콘텐츠 보호 시스템 구조

최근 유비쿼터스 환경에서 가전제품들이 점점 스마트화 되어가고 있다. 따라서 본 논문에서 최근 동향에 맞추어 상기 제시된 문제점들을 해결하기 위해서 스마트 홈 환경 상에서 모든 멀티미디어 기기는 RFID 태그가 부착되고 태그내의 정보를 통해서 암호화된 전송이 가능함을 가정하였다. 이를 위해서 댁내에는 RFID 리더기가 인증서버에 존재하거나 RFID 리더기가 탑재된 핸드헬드 장비를 통해서 수신이 가능해야한다. 디지털 콘텐츠를 보호하기 위해서는 사용자가 구입한 콘텐츠의 형태와 실행되는 기기에 따라서 처리해야하기 때문에 문제점 1, 2를 해결하기 위해서 인증과 복제방지 기술은 시나리오별로 다른 구조를 갖는다. 문제점 1을 만족하면서 문제점 3을 해결하기 위해서 댁내에서는 콘텐츠의 자유로운 복제가 가능하지만 다른 곳에서는 실행이 불가능하도록 해야 하기 때문에 각 출력 장치에 따라 원본 시그널을 처리해야 한다.

가. 스트리밍 형태의 콘텐츠

스트리밍 형태의 콘텐츠는 일반적으로 구입 시 마스

터링과정을 통해서 암호화되고 수신기에서 복호화 하는 형태를 취한다. 수신된 콘텐츠는 해당 기기에서만 실행이 가능하며 라이선싱을 통해서 다른 기기로의 전송이 가능하다. 이런 형태의 콘텐츠를 보호하기 위한 DRM기술은 다양하게 개발되고 있기 때문에 표준화된 방식으로 해당 멀티미디어 기기에서 지원 가능해야 한다.

스트리밍 형태의 콘텐츠는 LCD TV 또는 PDP TV와 같은 출력장치를 통해서 콘텐츠를 구입하는 경우와 PC 또는 핸드헬드 장비에서 구입하는 경우로 나누어 처리할 수 있다. 여기서 주목할 점은 출력 장치가 독립된 형태로 되어 있는 경우이다. 즉, TV처럼 일체형 장비가 아닌 PC처럼 출력 장치가 독립된 형태로 존재할 경우 출력장치별로 각기 다른 암호화키를 통해 전송이 가능해야 한다. 상기 제기된 문제점 2를 해결하기 위해서 반드시 고려돼야 하는 부분이다. 본 논문에서는 출력 장치로는 LCD 모니터/TV 그리고 일반 스피커, 이어폰만을 가정하였다. 출력장치에서 직접 콘텐츠를 받는 경우에는 해당 기기에 부착된 태그의 정보를 콘텐츠 제공업자로 전송하고, 이 정보는 마스터링 과정에서 이용된다. 전송되는 태그정보는 해당 기기 내부의 비밀키를 이용해서 복호가 가능한 공개키다.

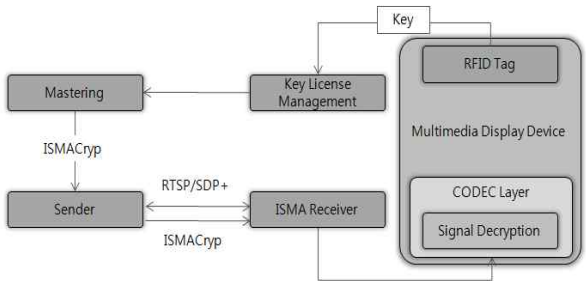

그림 1. RFID 기술 기반 ISMA DRM 아키텍처
Fig. 1. RFID-based ISMA DRM architecture

대표적인 스트리밍 형태의 콘텐츠 보호 기술은 ISMACryp가 있다[2][3]. 본 논문에서는 이 기술을 기본으로 ISMA DRM 구조를 수정하였다. 그림 1은 수정된 RFID 기술기반 ISMA DRM 구조를 보여준다. 기존 기술에서 키 전송 메커니즘을 수정하였다. 출력장치에 부착된 RFID Tag 내의 공개키는 송신측에 전송되고, 마스터링과정에서 콘텐츠를 암호화한다. 공개키는 출력장치에 유일한 키이기 때문에 이 키를 이용하여 암호화 할 경우 해당 출력 기기에서만 복호화가 가능하기 때문에 송신측에서 키를 생성/관리하는 과정이 필요 없다. 콘텐츠 암호화를 송신측의 대칭키로 할 경우 수신측의 공개키는 대칭키의 암호화에 사용될 수 있다.

나. 미디어 배포, 다운로드 형태의 콘텐츠

"Analog hole" 문제는 플레이어를 이용하여 재생된 아날로그/디지털 데이터가 쉽게 복제가 가능하기 때문에 발생한다. 콘텐츠를 멀티미디어 출력장치로 전송을 할 경우 아날로그 신호 또는 디지털 신호로 전송하게 되며 이 신호는 쉽게 복제가 가능하다. 이 문제를 해결하기 위해서 콘텐츠 배포 형태에 따라서 암호화/복호화 과정을 다르게 처리해야한다. 본 항에서는 미디어와 다운로드 형태의 콘텐츠 보호 방식을 설명한다.

(1) 미디어 배포를 통한 콘텐츠

CD/DVD와 같은 저장매체를 이용한 배포 형태에서 멀티미디어 콘텐츠의 암호화/복호화는 미디어에 부착된 태그와 출력 장치에 부착된 태그의 정보를 이용한다. 이기종 기기간의 상호호환성을 보장하기 위해서는 인증 서버에서 댁내에 존재하는 모든 기기의 태그 정보를 관리해야 한다.

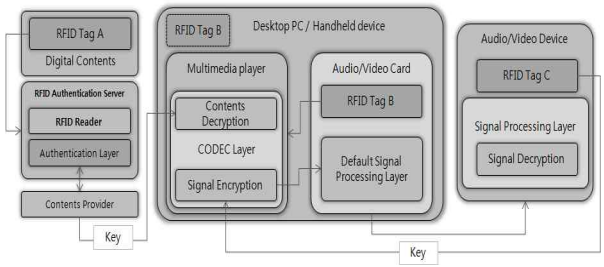

그림 2. 미디어 배포형 콘텐츠 보호
Fig. 2. Protection mechanism for contents in storable media

그림 2는 RFID 기술을 이용하여 디지털 콘텐츠를 복호화하고 댁내에 있는 출력 장치로 전송하는 과정을 도식화 한 것이다. RFID 인증 서버는 디지털 콘텐츠 및 출력 장비에 부착된 태그 정보(RFID Tag A, C)를 수신하여 인증과 복호화를 마친 후 미들웨어 상에 정보를 저장하고 이를 관리한다. RFID Tag B는 실행 장치에서 기본적으로 신호를 처리하거나 다운로드 형태의 콘텐츠를 처리할 경우 사용된다. 자세한 인증과정은 2절에서 논의한다.

인증과 복호화를 마친 후 실행과정은 기존의 콘텐츠

의 실행과정과 동일하지만 최종단계에서 출력 장비에 부착된 공개키로 2차 암호화 하는 과정을 수행한다. 즉, 출력 장비로 신호를 전송할 때 아날로그/디지털 신호를 출력 장비에 부착된 태그내의 키로 2차 암호화한 후 전송하게 된다. 따라서 이 신호는 해당 장비이외에서는 복호화가 불가능하기 때문에 신호를 가로채어 콘텐츠를 재생성하더라도 다른 사용자에게 제공할 수 없게 된다. 만약 출력하고자하는 장비가 다수이고 그중에 선택해야 할 경우 미들웨어상의 사용자 지원 서비스를 통하여 사용자가 원하는 출력 장비를 선택할 수 있다.

(2) 다운로드 방식 콘텐츠

이 방식에서는 콘텐츠를 사용자에게 전송하기 전에 암호화가 이루어져야 한다. 일반적으로 사용자의 PC 또는 핸드헬드 장비를 통해서 콘텐츠를 다운로드 받기 때문에 콘텐츠 암호화에 필요한 키는 해당 장비에 부착된 태그의 정보를 통해서 이루어진다. 또한 해당 장비에 출력 장비가 독립된 형태로 연결 된 경우 출력 장비의 태그 정보를 이용하여 2차 암호화를 하는 과정을 거쳐야 한다.

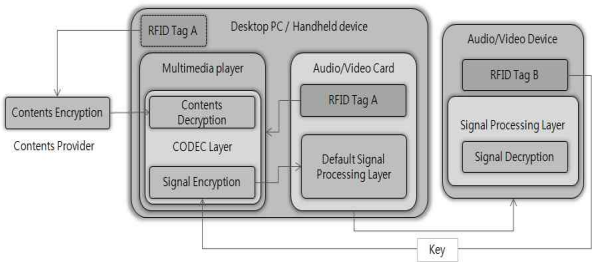

그림 3. 다운로드 방식을 사용하는 콘텐츠의 보호
Fig. 3. Protection mechanism for download-type contents

그림 3은 다운로드 방식의 콘텐츠의 복제방지를 위한 DRM 구조이다. 사용자의 장비에 부착된 RFID Tag A의 공개키를 이용하여 제공할 콘텐츠를 암호화 하고 사용자 장비 내부에 존재하는 비밀키를 이용하여 복호화 한다. 출력 장치에 전송되기 전에 사운드/비디오 카드에서 타깃 출력장치가 설정이 되어 있지 않을 경우 기본적인 신호처리(그림에서 Default Signal Processing Layer)를 거쳐 외부로 출력되기 때문에 이 신호를 캡처할 경우 해당 장비이외에서는 실행 될 수 없다. 타깃 장치가 설정된 경우에는 출력장치에 부착된 RFID Tag B의 정보를 이용하여 2차 암호화 하고 이 신호는 출력장치에서 복호화 된다.

다. 멀티미디어 장비를 이용한 콘텐츠의 복제 제어

디지털 콘텐츠의 생성 시에도 유사한 방법으로 처리할 수 있다. 디지털 콘텐츠를 생성할 경우 사용자는 댁내에 있는 멀티미디어 생성 장비(캠코더, 디지털 녹음기 등)의 비밀키로 암호화하고 부착된 태그의 정보를 이용하여 복호화 한다. 따라서 댁내에 생성 시에 사용하였던 장비가 존재하지 않을 경우 생성된 콘텐츠는 실행할 수 없다. 실행과정은 다운로드 형태의 콘텐츠와 유사하지만 암호화 과정에서 멀티미디어 생성 장비내의 비밀키가 사용되고 복호화에는 태그내의 키가 사용된다.

2. 콘텐츠 인증 과정

콘텐츠 인증 문제를 해결하기 위해서는 인증과정에서의 사용자의 개입을 제거하고 하드웨어를 통한 인증을 수행해야한다. 또한 콘텐츠 실행 프로그램 내에 인증에 관련된 코드가 없어야 하며 독립된 장비에서의 인증과정이 필요하다. 점점 복잡해지고 해독하기 어려운 기술을 이용한 인증 기법을 사용함에도 불구하고 제대로 된 보호 기술이 없었던 이유는 인증과정에서의 복호키의 노출이다. 암호화 기법은 가장 간단한 기법을 사용할지라도 복호키를 모른다면 해독이 거의 불가능하다. 본 논문에서는 이러한 문제점을 해결하기위해 인증과정의 자동화를 통한 멀티미디어 콘텐츠 인증 방법을 제안한다.

가. 미디어 배포형식의 콘텐츠 인증 및 키 교환

인증과정에서 중요한 문제는 태그 인증 및 판독기 인증이다. 태그 인증은 실제 물리적인 태그에 부착된 정상적인 태그인지 확인 하는 절차이며, 판독기 인증은 정상적인 제품상의 태그를 판독할 자격이 있는지 확인 하는 절차이다. 그림 4는 콘텐츠에 부착된 태그의 인증과정을 도식화 하였다. 판독기는 태그 인증을 위해서 태그 내에 저장된 키($E_k(A_{k\_pub} \| B_k)$)를 판독한다. 이 키는 판매업자가 보유하고 있는 키(A_{k_sec})로 복호화가 가능하기 때문에 태그의 인증을 거치지 않은 태그 정보는 의미가 없다. 판독기는 $E_k(A_{k_pub} \| B_k)$를 콘텐츠 제공자의 인증서버에 키 C_{k_pub}와 함께 전송하고 인증서버는 자신이 보유하고 있는 키 A_{k_sec}로 복호가 가능한지 확인한다. 인증서버에서 인증을 마친 후 사용자에게 콘텐츠 복호화에 필요한 키(B_k)를 암호화된 코드($E_k(C_{k\_pub} \| B_k)$)를 전송하고 판독기는 태그에 이 암호문을 저장한다. 따라서 해당 리더기 이외에 다른 판독기에서 정보의 수신은 가능하지만

복호화는 불가능하게 된다. 만약 인증서버에서 인증을 완료할 수 없는 경우 태그내의 정보가 훼손된 것으로 간주하고 사용자에게 인증 불가를 알림으로써 인증과정을 마친다.

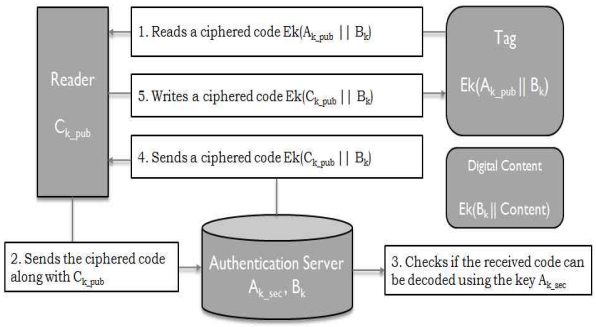

그림 4. 인증과정 및 키 교환 방식 1
Fig. 4. Procedure of authentication and key exchange 1

나. 다운로드 형식의 콘텐츠 인증 및 키 교환

그림 5는 다운로드 형식의 콘텐츠의 인증과정과 키 교환과정을 보여준다. 미디어 배포방식과 다른 점은 물리적인 태그를 사용할 수 없기 때문에 가상 태그를 사용한다. 우선 가상 태그의 더미 코드를 읽어 들인 후 판독기는 콘텐츠 제공자의 인증서버에 자신의 키 (C_{k_pub})와 함께 전송한다. 인증서버는 수신된 키를 이용해서 콘텐츠 복호화에 필요한 키 B_k를 암호화하여 사용에게 전송한다. 사용자는 가상 태그에 수신된 암호코드 $E_k(C_{k_pub} || B_k)$를 저장하고 콘텐츠 복호화에 사용한다.

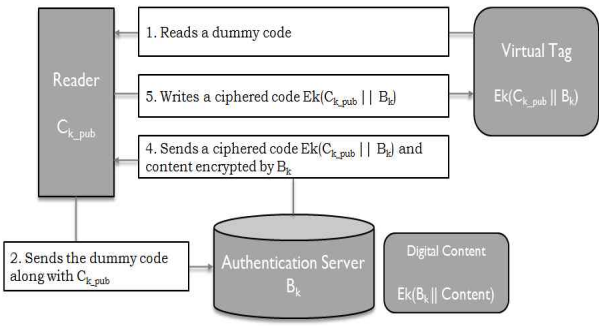

그림 5. 인증과정 및 키 교환 방식 2
Fig. 5. Procedure authentication and key exchange 2

다운로드 형식이나 미디어 배포형식에서 최초의 인증과정 이후에는 판매자의 서버에 접속할 필요가 없으며 판매자는 키 관리를 할 필요가 없다. 이후에 인증과정은 사용자의 RFID 인증 서버를 통해서 이루어지고 태그 내에는 단순히 키만 저장될 수 있는 것이 아니라 콘텐츠에 대한 사용권한 및 인증서버의 주소 등을 명시 할 수 있다.

Ⅳ. 모의실험 및 분석

본장에서는 Ⅲ장에서 제안한 RFID 기반 인증 플랫폼을 실험하기 위해서 가상 RFID 인증 서버, 가상 RFID 오디오 출력 장치, 일반 오디오 출력 장치, 가상 오디오 장치 컨트롤러, 가상 오디오 플레이어를 구현하여 제안 시스템의 타당성을 보이고 시그널 처리의 흐름을 통해서 콘텐츠가 보호되는 과정을 분석한다. 오디오 시그널은 wav 데이터(PCM 16bit, 16000Hz, mono)를 사용하고 스크램블 처리를 위해서 Matlab을 사용하였다. 그림 6은 가상 모듈을 실행하는 인스턴스 런처와 가상 장치/콘텐츠를 보여준다. 인스턴스 런처를 통해서 실행된 모듈은 인증서버에 등록되고 인증될 때 가상 태그내의 공개키를 볼 수 있다. 가상 오디오 콘텐츠를 인증한 후 가상 오디오 플레이어를 통해서 실행되고, 가상 오디오 컨트롤러를 거쳐 RFID 스피커에 출력되는 상황을 표현하였다. ①~③ 은 시그널의 흐름을 보여주고 [a]~[g]는 시그널이 각 모듈을 통과할 때 복호화와 암호화가 이루어지는 것을 나타낸다. 시그널 [a]는 사용자가 구입한 콘텐츠로서 제공자의 대칭키로 암호화 되어있다. 이 시그널은 가상 오디오 플레이어를 통해서 복호화([b])된 후 RFID 스피커가 인증서버에 등록이 되었을 경우에는 스피커에 부착된 태그를 이용하여 암호화 한다. 따라서 시그널 성~[f]는 같은 시그널이 된다. 보다 강력한 보호를 하기 위해서는 성를 컨트롤러의 키로 암호화 하고 컨트롤러에서는 등록된 스피커의 키로 암호화해서 전송한다. 이럴 경우에는 시그널 성와[d]가 같고, [e]와[f]가 같게 된다. [g]는 최종적으로 사용자가 가청 가능한 시그널이다. 댁내에 RFID가 가능한 스피커 장치가 없을 경우 성~[g]는 컨트롤러의 키로 암호화된 시그널이다. 그림7은 원본 시그널(a)과 스크램블된 시그널(b)을 보여준다. 그림 상으로 크게 변화되지 않았으나 실제 귀를 통해서 들을 경우 원음처럼 들을 수 없고, 그림 6에서 스크램블된 모든 시그널은 그림 7과 유사한 방식으로 스크램블된 것이다.

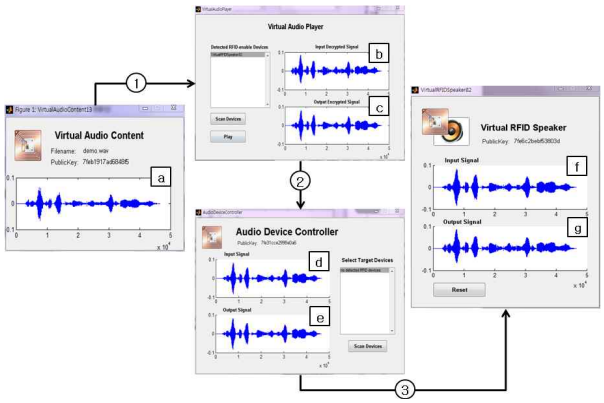

그림 6. RFID 기반 오디오 콘텐츠 보호 과정
Fig. 6. RFID-based protection procedure of audio contents

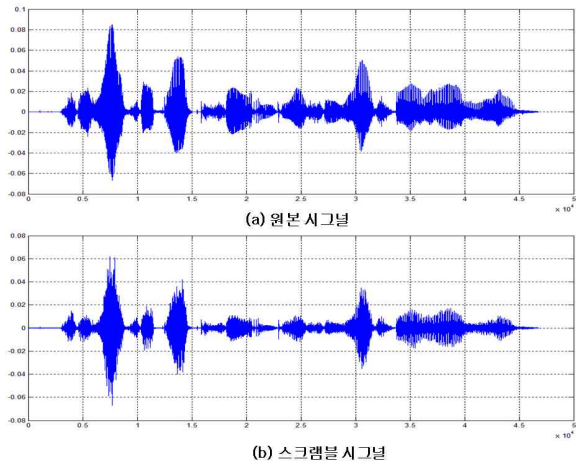

그림 7. 원본 시그널(a)와 스크램블 시그널(b)
Fig 7. Original signal(a) and scrambled signal(b)

시그널 b의 경우 오디오의 압축 방식과 배포 형식에 따라서 처리해야 한다. 일반적으로 다운로드 방식의 경우 mp3, flac이나 wav 형태의 파일 타입으로 제공되고 미디어를 통한 배포일 경우 wav 형태의 파일로 제공된다. 최근에 저장장치 가격의 하락과 용량의 증가, 처리속도의 증가로 인해서 원음에 가까운 파일을 제공하는 경우가 많아지고 있기 때문에 본 논문에서는 wav와 flac형태의 파일만을 고려하였다. wav나 flac의 경우 원음 자체에 암호화할 경우 미디어 플레이어에서는 암호화된 신호를 컨트롤러에 전송하고 컨트롤러는 출력장치에 따라 2차 암호화한다. 오디오 콘텐츠는 배포되기 전에 사용자의 공개키로 콘텐츠를 암호화하여 전송하고 사용자는 자신의 비밀키로 복호화하기 때문에 안전하게 보호될 수 있으며 콘텐츠 제공자가 비밀키를 관리할 필요가 없다. 미디어 배포 형태일 경우에는 제공자가 특정 사용자의 키를 알 수 없기 때문에 콘텐츠를 제공자의 대칭키로 암호화하여 배포하고 태그 내에는 제공자의 공개키를 이용해서 콘텐츠를 복호화 하는데 사용하는 대칭키를 암호화한 코드를 저장한다. 사용자는 최초 인증 시에 자신의 공개키와 태그내의 암호 코드를 제공자에 전달하고 제공자는 자신의 비밀키를 이용해서 대칭키를 복호화하고 사용자의 공개키로 암호화하여 사용자에게 전송한다. 이 코드는 태그 내에 다시 저장되기 때문에 태그복제에 의한 콘텐츠 공유를 방지할 수 있다.

V. 결 론

디지털 콘텐츠는 최근 방송 융합을 통해 보다 다양한 방식으로 제공되고 있다. 기존의 인터넷과 유통망을 통한 콘텐츠의 배포에서 방송을 통한 스트리밍형 서비스로 진화하고 있으며 콘텐츠 제공자는 기존의 서비스뿐만 아니라 새로운 형태의 배포 형태에서도 일관된 보호 방식이 필요하다. 본 논문에서 제안한 RFID 기반 콘텐츠 보호 시스템은 배포형태나 콘텐츠의 타입에 관계없이 일관된 보호가 가능하고 기존 시스템에서 보호할 수 없었던 멀티미디어 기기를 통한 순수 아날로그 복제 또한 방지할 수 있다.

비디오 타입의 콘텐츠는 출력장치에 따라서 처리해야 한다. TV와 같은 경우에는 콘텐츠가 화면을 완전히 점유하게 되어 오디오 콘텐츠와 유사한 방식으로 보호가 가능지만 모니터의 경우 전부 또는 일정부분을 점유하기 때문에 지속적인 연구가 필요하다.

본 논문에서 제안한 시스템은 eBook과 이미지 콘텐츠의 보호뿐만 아니라 소프트웨어의 불법 복제의 방지[9]에도 적용가능하기 때문에 댁내에서 사용하는 모든 콘텐츠는 본 논문에서 제안한 RFID기반 콘텐츠 보호 시스템을 사용할 경우 안전하게 보호 될 것이다.

참 고 문 헌

[1] 박지현, 정연정, 윤기송, “DRM 기술 동향”, ETRI 전자통신 동향분석, 제22권 제4호, 118-132쪽, 2007년 8월

[2] ISMA, “Internet Streaming Media Alliance Implementation Specification Version 2.0”, 2007. 11.
[3] ISMA, “Internet Streaming Media Alliance Encryption and Authentication Version 1.1”, 2006. 9.
[4] Michael Ripley, C. Brendan S. Traw, Steve Balogh, Michael Reed “Content Protection in the Digital Home”, Intel Tech. Journal 6(4), pp. 49-56, 2002.
[5] Digital Content Protection LLC, “High-bandwidth Digital Content Protection System Revision 1.3”, 2006.12.
[6] EBU Project Group B/CA., “Functional model of a conditional access system”, EBU Technical Review, pp. 64-77, 1995.
[7] CEN, “Digital Rights Management”, final report, 2003.9
[8] Renato Ianella, “Digital Rights Management (DRM) Architectures,″ D-Lib Magazine, Vol. 7, No. 6, 2001.6.
[9] Kee-Hyun Choi, Dong-ryeol Shin, Ho-jin Shin, Kyung-soo Jang, “Content Self-Protection for Digital Products Using RFID-Enable Agent Platform″. IDC 2009, pp. 1783-1788, 2009.8.

※ 이 논문은 2009년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임. [NRF-2009-353-D00047]

저자 소개

최 기 현(정회원)

- 2000년 성균관대학교 전기전자 및 컴퓨터 공학과(공학사)
- 2002년 성균관대학교 전기전자 및 컴퓨터 공학과(공학석사)
- 2006년 성균관대학교 전기전자 및 컴퓨터 공학과(공학박사)
- 2006~2007년 성균관대학교 Post Doc.
- 2007년~2009년 성균관대학교 연구교수
- 2009년~현 재 성균관대학교 정보통신기술연구소 학술연구교수
- E-Mail: gyunee@ece.skku.ac.kr

<주관심분야 : WLAN, P2P, RFID/USN 기술, 이동무선통신>

장 경 수(정회원)

- 1994년 성균관대학교 전기 공학과 (공학사)
- 1998년 성균관대학교 전기 전자 및 컴퓨터 공학과 (공학석사)
- 2005년 성균관대학교 전기 전자 및 컴퓨터 공학과 (공학박사)
- 2001년~현 재: 경인여자대학 영상방송 정보과 교수
- E-Mail: ksjang@kic.ac.kr

<주관심분야 : 통신네트워크, 유비쿼터스 컴퓨팅, 센서네트워크>

신 호 진(정회원)

- 1994년 성균관대학교 전기 공학과(공학사)
- 1999년 성균관대학교 전기 공학과(공학석사)
- 2006년 성균관대학교 전기 전자 및 컴퓨터공학과(공학박사)
- 1994~1995년 삼성중공업(주)
- 2007~2008년 성균관대학교 Post Doc.
- 2009년~현 재 한신대학교 정보통신학과 조교수
- E-Mail: hjshin@hs.ac.kr

<주관심분야 : WLAN, RFID/USN 기술, 이동무선통신>