

<http://dx.doi.org/10.7236/IIBC.2015.15.1.37>

IIBC 2015-1-5

웹 이미지 콘텐츠 저작권보호 방법에 관한 연구

A Study on Copyright Protection Method of Web Image Contents

이영훈*, 조만기*, 조성환**

Yeong-Hun Yi*, Man-Gi Cho*, Seong-Hwan Cho**

요약 웹에서 게시되는 이미지 콘텐츠에 대한 기술적 조치들은 화면캡처 방지와 같은 복제방지 방식과 워터마킹 삽입이나 특징점 정보를 통해 무단복제물을 검출할 수 있는 추적 기술들이 존재한다. 그러나 화면캡처 방지 기술은 이미지 소스 URL이 노출될 경우에는 무단복제를 막을 수 없고 추적 기술은 불법행위를 적발하기 위한 후처리방식이기 때문에 불법복제를 원천적으로 차단하지 못한다는 단점이 존재한다. 또한 저작권 정보 표시기술을 이용할 경우 저작권 정보가 저작권보호 대상의 콘텐츠로부터 간단히 제거될 수 있다는 단점이 있다. 본 논문에서는 웹 이미지 콘텐츠의 저작권정보를 쉽게 분리할 수 없게 하면서 허가된 사이트에서만 이미지 콘텐츠가 게시되어 열람될 수 있도록 하는 웹 이미지 콘텐츠 저작권 보호 시스템 모델을 제시한다.

Abstract Technical treatments of image contents on the web include the copy protection method such as the image capture protection technology and the traitor tracing method to detect unauthorized duplications through watermarking insertion or feature information technology. However, these two methods have their own weaknesses. The image capture protection method is unable to protect illegal captures when the URLs of image sources are exposed. The traitor tracing method is fundamentally unable to protect illegal captures due to its post-treatment method. Besides, the weakness of using the copyright information display technology involves easy removal of copyright information from copyrighted contents. This paper suggests a model of the web image contents protection system which makes it hard to separate copyright information from web image contents and allows image contents to be shown only in the authorized websites.

Key Words : Web image content, DRM, Copy protection

1. 서론

2013년 저작권보호연차보고서에 따르면 2012년 기준 국내 디지털콘텐츠 온라인 불법복제 시장규모는 850억 원 수준으로 보고되고 있다.^[1] 이는 비록 2011년에 비해 0.2% 정도의 감소세를 보이고는 있지만 출판 분야(97% 감소)를 제외한 음악, 영화, 방송, 게임 등 여타 콘텐츠에

대해서는 오히려 평균 20.6%가 증가하여 전반적인 불법 복제 시장규모는 크게 증가하고 있음이 확인되었다. 이처럼 디지털콘텐츠는 복제와 배포의 용이성으로 인하여 초고속 인터넷 매체를 통한 저작권침해 피해가 해마다 증가하고 있는 실정이다. 이에 따라 저작권자 또는 온라인 콘텐츠 서비스 제공자들은 음악이나 동영상과 같은 스트리밍기반의 서비스가 필요한 콘텐츠는 물론이고 텍

*정회원, (주)파수닷컴

**정회원, 금강대학교 교양학부(교신저자)

접수일자 : 2014년 12월 15일, 수정완료 : 2015년 1월 14일

게재확정일자 : 2015년 2월 13일

Received: 15 December, 2014 / Revised: 14 January, 2015

Accepted: 13 February, 2015

**Corresponding Author: shcho@ggu.ac.kr

School of Liberal Arts & Sciences, Geumgang University, Korea

스트나 이미지와 같은 일반적인 온라인 디지털콘텐츠에 대해서도 불법복제방지를 위한 보호 조치를 강화해 나아가고 있다.^[2]

이들 보호조치 중에 이미지 콘텐츠에 적용되고 있는 기술적 조치들은 화면캡처 방지와 같은 복제방지 기술이나 워터마킹/특징점 정보를 통해 무단복제물을 검출할 수 있는 추적 기술들이 존재한다. 그러나 화면캡처 방지 기술은 이미지 소스 URL이 노출될 경우에는 무단복제를 막을 수 없고 추적 기술은 불법행위가 적발이 된 이후의 후처리방식이기 때문에 불법복제를 원천적으로 차단하지 못한다는 단점이 존재한다. 또한 저작권 정보 표시 기술을 이용할 경우 저작권정보가 저작권보호 대상의 콘텐츠와 간단히 제거 될 수 있다는 단점이 있다.

본 논문에서는 웹 이미지 콘텐츠의 저작권정보를 쉽게 분리할 수 없게 하면서 허가된 사이트에서만 이미지 콘텐츠가 게시될 수 있도록 하는 웹 이미지 콘텐츠 저작권 보호 시스템 모델을 제시하고 이에 대한 Chrome 웹 브라우저 상에서의 구현 결과를 보여준다.

II. 웹 콘텐츠 저작권 보호 기술 분석

웹에 게시되는 콘텐츠에 대한 저작권 보호기술은 콘텐츠 복제방지 기술, 추적기술, 저작권 정보표시 기술 형태로 구분될 수 있다.

1. 콘텐츠 복제방지 기술

콘텐츠 복제방지 기술은 콘텐츠에 대한 복제를 원천적으로 차단하는 기술로서 암호화, 화면캡처 방지, 소스보기 방지 방식의 기술들이 존재한다.

가. 암호화 방식

암호화 방식의 보호기술은 웹에 게시되는 음악이나 동영상 콘텐츠를 암호화하여 웹 브라우저에 전달해 주는 기술로 주로 스트리밍 서비스에 사용된다. 이 방식은 사용자가 HTML 페이지로부터 암호화된 동영상의 URL을 획득하고 이를 다운로드 받는다 하더라도 해당 콘텐츠가 암호화 되어 있기 때문에 클라이언트에서 단독으로 재생될 수 없게 만드는 기술이다. 웹에 게시된 암호화된 콘텐츠는 링크 형태로 존재하며 실 데이터는 콘텐츠 배포 서버를 통해 스트리밍 형태로 제공된다. 이때 브라우저는 콘텐츠 복호화를 키를 포함한 라이선스를 콘텐츠를 게시

한 웹 사이트에 요청하고 해당 웹 사이트는 사용자 인증을 거친 후에 라이선스 발급 서버를 통해 라이선스를 전달한다. 브라우저는 다운받은 스트리밍 콘텐츠와 라이선스를 복호화 모듈에 전달해 주고, 복호화 모듈을 통해 복호화된 콘텐츠는 렌더링 된 이후에 브라우저에게 전달되어 최종적으로 사용자에게 열람된다. 현재 상용화 되어 있는 표준 웹 콘텐츠 암호화 기술로는 W3C Encrypted Media Extension(EME)^[3]이 있다. 그림 1은 W3C EME의 구동 개요를 보여준다.

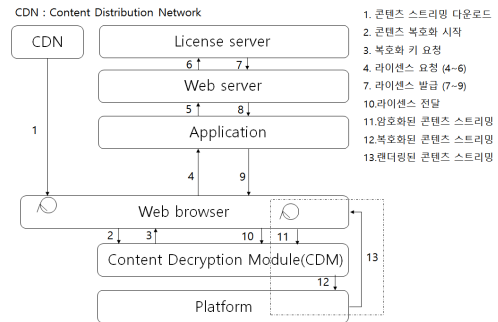


그림 1. Encrypted Media Extension 구동 개념도
Fig. 1. Overview of the Encrypted Media Extension

나. 화면캡처 방지 방식

화면캡처 방지 보호기술은 웹에 게시되는 텍스트나 이미지 콘텐츠가 웹 브라우저에서 열람되는 동안에 사용자가 화면캡처 기능을 이용하여 내용물을 복제하는 것을 방지해 주는 기술이다. 이 기술은 화면캡처 키보드 제어, 클립보드 제어, 그래픽관련 시스템 API제어, 캡처프로그램 제어 등 다양한 방식으로 구현될 수 있다. 이 방식은 기술의 보안적 특성상 현재까지 표준화된 기술은 조사되지 않고 있다.

다. 소스보기 방지 방식

소스보기 방식의 보호기술은 웹에 게시되는 텍스트가 웹 브라우저에서 열람되는 동안에 사용자가 클립보드 기능을 이용하여 게시물을 복제하는 것을 방지해 주는 기술이다. 이 기술은 자바스크립트를 이용하여 마우스의 특정 이벤트를 제어 하거나 소스의 내용을 난독화 또는 스크램블링하여 사용자가 소스를 확보한다고 하더라도 쉽게 내용을 확인할 수 없도록 하는 방법이 사용되고 있다. 이 방식은 기술의 보안적 특성상 현재까지 표준화된 기술은 조사되지 않고 있다.

2. 콘텐츠 추적 기술

콘텐츠 추적 기술은 콘텐츠의 무단 사용을 검출하기 위한 기술로서 워터마킹 삽입이나 특징점 정보를 이용하는 기술들이 존재한다.

가. 워터마킹 삽입 방식

워터마킹 기술은 보호하고자 하는 이미지, 음악, 동영상 콘텐츠 내부에 저작권에 관련된 정보를 삽입하여 향후 무단 사용에 대한 검출을 용이하게 하는 기술로서, 보이는(visible) 정보 삽입방법과 보이지 않는(invisible) 정보 삽입방법이 존재한다. 이 기술은 사용자가 콘텐츠에 대한 열람시 복호화 모듈과 같은 별도의 클라이언트가 존재하지 않아도 된다는 장점이 있는 반면 원본콘텐츠 내부에 제거가 쉽지 않은 데이터를 삽입하고자 할 경우 원본작품에 대한 시각적 또는 청각적 훼손의 가능성이 존재한다.

나. 특징점 정보 방식

특징점 정보 기술은 보호하고자 하는 이미지, 음악, 동영상 콘텐츠의 특징점 정보를 추출하여 DB로 구축한 이후, 향후 인터넷상에 게시되는 콘텐츠를 다운로드하여 특징점을 추출한 후 구축된 DB와 비교하여 무단 사용을 검출하는 기술이다. 이 기술은 암호화 방식을 사용하지 않는다는 특징을 가지고 있어 워터마킹 기술과 동일한 장점이 있고, 또한 원본 이미지에 데이터를 삽입하지 않기 때문에 원본 이미지에 대한 손상도 없다. 그러나 검출 대상이 되는 콘텐츠에 대한 특징점 DB를 별도로 유지해야 하는 부담이 존재한다. 특징점 정보를 이용하여 유사한 콘텐츠를 검색해 주는 방식으로 가장 일반적인 서비스는 구글의 이미지 검색 기능을 예로 들 수 있다.

3. 저작권 정보표시

저작권정보 표시 방법은 게시되는 콘텐츠에 저작권 정보를 함께 표기함으로써, 인터넷 사용자에게 위법 행위에 대한 경각심을 심어주는 효과를 이용한 저작권 보호 방법이다. 가장 일반적으로 사용되는 방법은 ‘All rights reserved’와 같은 포괄적 저작권 표시 방식이 있을 수 있고, CCL(Creative Common License)^[4]과 같이 정해진 범위 안에서 이용허락 라이선스가 이미 발급된 형태의 개방형 저작권 표시 방식이 존재한다. 그러나 저작권정보 표시 방식은 원본콘텐츠 내부에 워터마킹 형태

로 삽입되지 않는 경우 콘텐츠로부터 저작권정보를 쉽게 분리될 수 있다는 단점이 있다. 이 방식의 표준 기술은 현재 표준이 진행 중에 있는 W3C HTML5 Image Description Extension^[5]이 존재한다.

4. 각 기술별 장단점 분석

표 1은 웹 콘텐츠 저작권 보호 기술 각각에 대한 장단점을 보여준다.

표 1. 웹 콘텐츠 저작권 보호 기술 장단점
 Table 1. Merits and Demerits on the Copyright Protection Technologies for Web Contents

분류		장점	단점
복제 방지 기술	암호화	강력한 복제방지	복호화 클라이언트 모듈 필요
	화면캡처 방지	이미지, 텍스트 복제방지에 용이	근본적인 복제 방지 안 됨
	소스보기 방지	텍스트 복제방지에 용이	근본적인 복제 방지 안 됨
추적 기술	워터마킹 삽입	DB 구축 부담 없음	원본 콘텐츠 훼손
	특징점 정보	원본 콘텐츠 훼손 없음	DB 구축 부담
저작권 정보표시		적용비용 최소화방법	저작권 정보 제거 용이

5. 웹 이미지 콘텐츠 저작권 보호를 위한 기존 기술의 문제점

상기에서 설명된 웹 콘텐츠 저작권 보호 기술에 의하면 현재 웹 이미지 콘텐츠 저작권 보호 방법으로는 화면 캡처, 추적기술, 그리고 저작권 정보표시 기술이 사용되고 있음을 알 수 있다. 그러나 표 1의 장단점 분석에 의하면 웹 이미지 콘텐츠 저작권 보호를 위하여 이러한 3가지의 방식이 병행되어 사용된다 하더라도, URL 노출에 따른 이미지 콘텐츠의 근본적인 저작권 보호가 어렵고, 복제되어 타 사이트에서 게시되는 경우 연계된 저작권표시 정보에 대한 무결성을 보장 받을 수 없다. 또한 추적기술을 활용한다 하더라도 사후처리라는 단점으로 인해 원천적인 복제 방지가 되지 않을뿐더러, 원본 훼손에 대한 부담이 존재한다.

III. 웹 이미지 콘텐츠 저작권 보호 방법 제안 모델

본 연구는 웹에서 게시되는 이미지 콘텐츠에 대하여,

URL이 노출이 되더라도 복제가 불가능하고, 아울러 무단 링크를 통해 타 웹 페이지에서 게시되는 경우에 열람이 불가능하며, 연계된 저작권표시 정보에 대한 무결성까지 보장 받을 수 있는 원천적인 저작권보호 모델을 제시한다. 이 방식은 이미지 콘텐츠를 암호화하고, 게시되는 사이트 도메인 정보를 기반으로 암호화된 콘텐츠 복호화 키 및 저작권 정보를 포함하고 있는 라이선스의 위치를 태그^[6]의 속성으로 제공하는 모델이다. 웹 이미지 콘텐츠 저작권보호 방법 제안 모델에 대한 개념도는 그림 2와 같다.

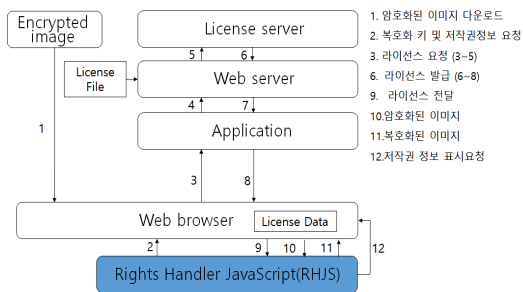


그림 2. 웹 이미지 콘텐츠 저작권보호 방법 모델
Fig. 2. Model of the Copyright Protection for Web Image Contents

1. 웹 이미지 저작권 보호 구동 메커니즘

사용자가 저작권 보호가 되어 있는 웹 이미지를 포함한 페이지에 접속하게 되면 브라우저는 외부 링크로 연결된 암호화된 이미지를 다운받고, 브라우저와 연계되어 있는 RHJS(Rights Handler JavaScript)는 복호화 키와 저작권정보가 포함된 라이선스를 획득한다. 라이선스 내부에는 게시되는 저작물에 대한 저작권정보와 암호화된 이미지를 복호화 할 수 있는 키 정보가 포함되어 있다. RHJS는 라이선스로부터 이미지가 게시된 사이트의 도메인 정보를 기반으로 암호화되어 있는 키 정보를 복호화하고 이 키를 이용하여 암호화된 이미지를 복호화 하여 화면에 보여준다.

2. 이미지 패키징 및 게시

보호할 이미지에 대한 패키징은 암호화 및 라이선스 정보 생성과정을 통해 이루어지고, 해당 저작물에 대한 게시는 암호화된 이미지와 라이선스 위치정보를 게시되는 페이지의 태그에 기술함으로써 완료된다.

가. 암호화

이미지는 하나의 랜덤 키를 이용하여 암호화 되고 암호화된 이미지 콘텐츠의 URL은 웹페이지 의 src 속성에 기술된다. 암호화에 사용된 알고리즘과 암호화 키는 라이선스에 저장된다.

나. 라이선스 정보 생성 및 전달방식

라이선스는 저작권정보와 이미지 복호화키를 담고 있는데, 이미지 복호화에 사용되는 키는 이미지가 게시될 도메인 정보를 이용하여 암호화 한다. 라이선스 정보는 게시되는 도메인별로 별도로 존재하며 게시되는 페이지에 포함되어 있거나 파일형태 또는 실시간 생성되어 전달된다. 라이선스는 표 2와 같은 형태의 XML 스키마를 가진다.

표 2. 라이선스 정보를 위한 스키마
Table 2. Schema for License Information

엘리먼트	출현횟수	설명
copyrights	1	저작권 정보
agreement	1	라이선스 내용
party	1	저작권자
rights Holder	1..n	저작권자 정보.(uid, role, name, contactInfo)
asset	1	저작물 정보 (uid, host, url, filesize, description, hash)
encryption	0..1	암호화 정보 (algorithm, key)
hmac	1	저작권 정보 파일의 hmac 값

다. 저작물 게시

암호화된 이미지 저작물에 대한 게시는 기존 HTML5에서 사용되고 있는 태그를 사용하고 저작권정보를 추가하기 위한 copyright 속성이 추가한다. 표 3은 보호된 이미지 저작물 게시를 위한 태그의 스키마를 보여준다.

표 3. 보호된 이미지 저작물 게시 스키마
Table 3. Schema for Posting Protected Image Contents

엘리먼트	출현 횟수	설명
img	1	이미지 콘텐츠
@src	1	이미지 소스 위치
@copyright	1	저작권 정보 획득 위치

3. RHJS 기능

RHJS는 암호화 이미지에 대한 라이선스 요청 및 다운로드, 키 복호화를 통한 불법링크 방지, 이미지 복호화, 무결성 검증을 통한 저작권정보 위변조 방지, 마우스 이벤트 처리기를 통한 저작권 정보표시 기능들을 제공하며 Javascript로 작성되어 웹 브라우저와 연동된다. 그림 3은 RHJS 모듈의 세부구조와 웹 브라우저와의 관계를 설명한다.

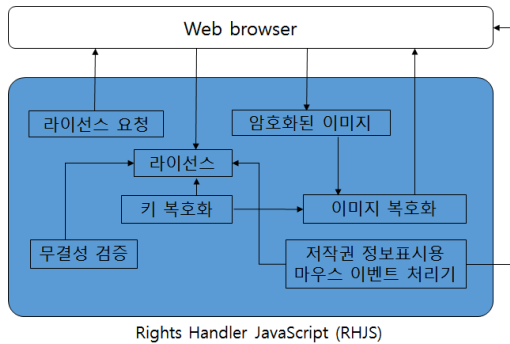


그림 3. RHJS 세부 구조
 Fig. 3. Structure of the RHJS

IV. 구현 및 테스트

웹 이미지 콘텐츠 저작권보호 제안 모델에 대한 구현은 윈도우즈 패키지와 Chrome extension^[7]을 이용한 크롬 브라우저의 확장을 통해 구현되었다. 라이선스 전달 방식은 라이선스 서버를 별도로 두지 않고 패키지를 통해 생성된 라이선스 파일을 웹 서버에 게시하는 형태로 구현 하였다. 구현을 위해 사용된 개발 환경은 표 4와 같다.

표 4. 구현 시스템의 개발 환경
 Table 4. Environment of the Implemented System

항목	사용 기술/환경
구동 시스템	Google Chrome v39.0.2171.71 m
개발툴	Eclipse Kepler, Visual studio 2008, Google Chrome
라이선스 전달방식	라이선스 파일
키 암호화방식	AES-128-CBC
개발 OS	Windows 7

1. 보호된 웹 이미지 게시 결과

그림 4는 보호된 웹 이미지가 게시된 HTML5 페이지의 모습을 보여준다.

```
<!DOCTYPE HTML>
<html>
...
  
...
</html>
```

그림 4. 보호된 웹 이미지 저작물 게시
 Fig. 4. Posting on the Protected Web Image Contents

2. 라이선스 생성 결과

그림 5는 XML 형태의 발급된 라이선스를 보여준다.

```
<?xml version="1.0" encoding="UTF-8"?>
<copyrights>
  <agreement>
    <party>
      <rightsHolder>
        <uid>IP-00-13-0000-0001</uid>
        <role><![CDATA[작사가]]</role>
        <name><![CDATA[홍길동]]</name>
      </rightsHolder>
    </party>
    <asset>
      <url>http://www.fasoo.com/hong-gd.png</url>
      <host>www.fasoo.com</host>
      <uid>PI-00-13-0000-0001</uid>
      <fileSize>2907907</fileSize>
      <title><![CDATA[홍길동 자화상]]</title>
      <hash>f0414b...</hash>
    </asset>
    <encryption>
      <algorithm>aes-128-cbc</algorithm>
      <key>Tmpto...</key>
    </encryption>
  </agreement>
  <hmac>hWBqPBHUIG6Hf5fnM98i7xtgIYI=</hmac>
</copyrights>
```

그림 5. 라이선스 정보
 Fig. 5. License Information

3. 보호된 웹 이미지 열람 결과

그림 6은 보호된 이미지 콘텐츠가 포함된 웹 페이지 열람 시 저작권이용 허락을 받은 도메인을 통한 정상적인 이미지 열람과 무단 사용된 도메인에서의 비정상적인 이미지 열람 결과를 보여준다.

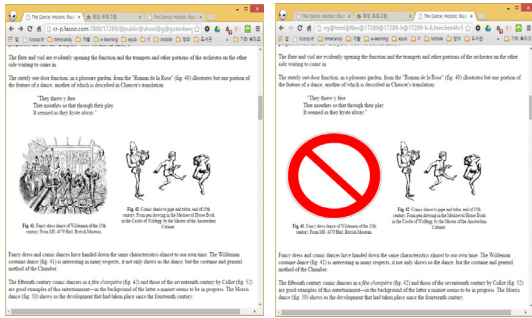


그림 6. 구현 결과 화면
Fig. 6. Implementation Result

그림 7은 허가된 도메인과 허가되지 않은 도메인으로부터 열람되는 보호된 웹 이미지에 대한 저작권 정보를 표시한 결과이다.

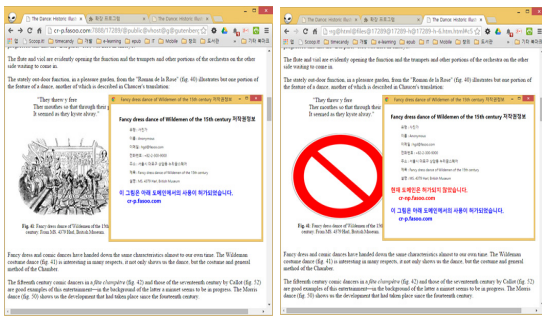


그림 7. 저작권 표시 화면
Fig. 7. Copyright Display

V. 결론 및 향후 과제

본 논문은 한국저작권위원회의 저작권기술 개발 사업으로 수행중인 “소셜 저작물의 저작권 보호 및 콘텐츠 메시업 도구 요소기술 개발” 과제의 2차년도 개발결과와 하나로, 웹 이미지 콘텐츠 저작권보호 방법 구현 모델을 제시하였다. 연구결과는 제시된 모델의 구현을 통해 크롬 브라우저상에서 저작권 보호된 이미지가 저작권이용을 받은 사이트에서는 정상적으로 열람이 되지만 무단 사용된 사이트를 통해서 열람이 되지 않음을 보여주었다.

“소셜 저작물의 저작권 보호 및 콘텐츠 메시업 도구 요소기술 개발” 연구는 2013년 6월부터 2016년 2월까지 3년간에 걸쳐 진행되고 있으며, 1차년도에서는 부분저작

물 저작권 보호 기초기술 개발을 목표로 협업저작물 DRM 기초 기술, 도서 특징점 추출 기술에 대한 개발이 진행되었다. 2차년도는 1차년도의 연구 결과를 기반으로 협업저작물 유통 플랫폼 기반 기술 개발을 위하여 저작권 침해 점검 도구, 협업 DRM, 구글드라이브 오픈 API 연계, HTML5 상의 저작권보호 기술에 대한 개발이 진행되고 있다. 3차년도 과제에서는 협업저작물 유통 플랫폼에 대한 개발 완료와 시범서비스가 예정되어 있다.

3개년간의 연구와 개발 작업이 마무리되면 개인 창작자들의 1차, 2차 저작권에 대한 기술적 보호조치가 가능한 협업 환경이 제공됨에 따라 소셜 협업을 통한 콘텐츠 창작 활성화와 소셜 콘텐츠 시장의 성장이 기대된다.

References

- [1] Annual Report on Copyright Protection”, Korea Federation of Copyright Organizations, 2013
- [2] H. Kang and S. Cho, “A Study on the Interoperable Rights Control Information between Heterogeneous Broadcasting DRM Schemes in Digital Home Domain,” The Journal of The Institute of Internet, Broadcasting and Communication, vol.8 no.5, pp.81–92, 2008.
- [3] D. Dorwin, J. Smith, M. Watson and A. Bateman, “Encrypted Media Extensions” – W3C Working Draft, World Wide Web Consortium (W3C), 2014
- [4] C. Nevile, Я. Yandex, and M Sadeck, “HTML5 Image Description Extension” – W3C Proposed Recommendation, World Wide Web Consortium (W3C), 2014
- [5] CCL, Creative Common License, Available: <http://creativecommons.org/>
- [6] I. Hickson, R. Berjon, et al, “A vocabulary and associated APIs for HTML and XHTML” – W3C Editor’s Draft, World Wide Web Consortium (W3C), 2014
- [7] Wikipedia, Google Chrome Extensions, 2014

※ 본 논문은 문화체육관광부의 저작권기술개발사업에 의거 한국저작권위원회의 정부지원금을 받아 연구되었습니다.

(This research project was supported by Government Fund from Korea Copyright Commission.)

저자 소개

이 영 훈(정회원)



- 1995년 : 세종대학교 전산학과 졸업(학사)
- 2002년 ~ 현재 : ㈜파수닷컴
<주관심분야: 저작권보호기술(DRM), 정보보호기술, 전자책>

조 만 기(정회원)



- 2010년 : 한국항공대학교 컴퓨터공학과 졸업(학사)
- 2013년 : 한국항공대학교 대학원 컴퓨터공학과(공학석사)
- 2013년 ~ 현재 : ㈜파수닷컴
<주관심분야: 저작권보호기술(DRM), 전자책>

조 성 환(정회원)



- 1980년 : 성균관대학교 전자공학과(학사)
- 1982년 : 성균관대학교 대학원 전자공학과(공학석사)
- 1991년 : 성균관대학교 대학원 전자공학과(공학박사)
- 1982년 ~ 1985년 : 해군사관학교 전기 및 전자공학과 전임강사
- 1997년 : 미국 Columbia 대학 CATT Visiting Scholar
- 1985년 ~ 2002년 : 동서울대학 컴퓨터공학과 부교수
- 2002년 ~ 현재 금강대학교 교수
<주관심분야 : 영상통신, 무선네트워크, 저작권보호기술(DRM)>