

국가연구개발 보고서원문 성과물 전담기관인 한국과학기술정보연구원에서 가공·서비스 하는
연구보고서는 동의 없이 상업적 용도로 사용할 수 없습니다.

2016-CCP-9500

클라우드 기반 콘텐츠 저작권 보호기술 개발
(Developments of Contents Copyright Protection based on
Cloud)

경일대학교 산학협력단

문화체육관광부

국가연구개발 보고서원문 성과물 전담기관인 한국과학기술정보연구원에서 가공·서비스 하는
연구보고서는 동의 없이 상업적 용도로 사용할 수 없습니다.

제 출 문

문화체육관광부 장관 귀하

이 보고서를 “ 클라우드 기반 콘텐츠 저작권 보호기술 개발 ” 과제의 최종보고서
로 제출합니다.

2017년 2월 28일

주관연구기관명 : 경일대학교 산학협력단

주관연구책임자 : 윤은준

연 구 원 : 김대수

연 구 원 : 김평한

연 구 원 : 로즈마리 코이카라

연 구 원 : 정광열

연 구 원 : 김영주

연 구 원 : 서경윤

참여연구기관명 : (주)우경정보기술

대 표 자 : 박윤하

보고서 요약서

과제번호	2016-CCP-9500	지원분야	자유공모	기술분야	저작권 보호 기술개발
과제명	클라우드 기반 콘텐츠 저작권 보호기술 개발				
연구기간	2016년 7월 1일 ~ 2017년 2월 28일		당해연도 협약기간	2016년 7월 1일~2017년 2월 28일	
연구책임자	윤은준	참여연구원수	전체 : 6 명 내부 : 6 명 외부 : 0 명	연구개발비	정부: 344.000 천원 기업: 114,667 천원 합계: 458,667 천원
주관연구기관명 (소속부서명)	경일대학교 산학협력단		참여연구기관명 (대표자)	(주)우경정보기술 (박윤하)	
위탁연구기관명 (소속부서명)			연구책임자		
요약(연구결과를 중심으로 개조식 500자 이내)				보고서면수	40 page
<p>현재 국내에서는 웹툰과 같은 클라우드 기반 이미지 및 콘텐츠들을 서비스하는 사업이 활발해짐에 따라, 서비스 사업의 신뢰성 및 안전성 제공이 절대적으로 우선시되어야 한다. 또한 클라우드 환경에서 콘텐츠 보호와 동시에 속도저하를 유발시키지 않는 메커니즘에 대한 시급한 시장 수요 예측에 따른 선도성 기술개발이 필요한 시점이다.</p> <p>기존 저작권 기술은 저작자의 권리를 효율적으로 보호하고 저작물의 공정한 이용을 도모하기 위한 기술 및 서비스를 말하지만 저작권 보호를 위한 기술들은 비용 지불에 민감한 개인사용자나 영세·중소기업의 경우 이러한 저작권기술에 접근하기 어려운 실정이다. 본 과제의 최종목표는 클라우드 환경에서 저작권보호 서비스(CaaS: Copyright protection <i>as a Service</i>)를 통한 콘텐츠 보호 및 개인 및 영세·중소기업을 대상으로 하는 효율적이고 접근성이 높은 저작권보호 서비스를 제공하는 것이다. 이를 위한 개발 목표는 다음과 같다.</p> <ul style="list-style-type: none"> (1) 경량 암호 기반 콘텐츠 인증 기술: 클라우드 환경에서 콘텐츠 보호를 위해 고속의 경량암호 모듈인 LEA(Lightweight Encryption Algorithm)를 이용한 ① 경량 암호 기반 콘텐츠 인증 기술을 개발하여 인증을 통한 콘텐츠에 대한 접근제한을 제공하여준다. (2) 특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술: 또한 특징점(DNA) 기반 필터링 기술에 제로정보은닉 기반의 스테가노그레피 기법을 접목하여 ② 특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술을 개발하여 고품질의 콘텐츠를 제공하여 준다. (3) 클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS) 개발: ①의 기술개발 내용과 ②의 내용을 기반으로 하여 ③ 클라우드 기반의 웹툰/이미지 저작권 보호 시스템 개발을 통해 클라우드환경에서 정지영상에 대한 특징점(DNA) DB를 제공할 뿐만 아니라 저작권보호 및 안전한 콘텐츠 서비스를 제공을 하는 클라우드 저작권 보호 서비스(CaaS: Copyright protection <i>as a Service</i>)를 개발한다. <p>클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS)의 사업화를 위하여 최종결과물을 이용하여 솔루션 개발을 통해 저작권 보호서비스 형태로 클라우드 업체에 콘텐츠 보안 솔루션으로 제공할것이며, 클라우드 서버 구축후 자체 서비스를 개시하여 개인이나 중소기업의 콘텐츠를 대상으로 시범사업을 진행하여 국내 클라우드 저작권 시장 개척을 할 것이다. 향후 저작권 위원회와 연계하여 콘텐츠 저작권보호 서비스를 저작권위원회에 제공하여 현 시스템에서 보다 효율적인 저작권보호 시스템을 구축하고, 향후 국내 뿐만 아니라 국외 클라우드 업체 및 포털사이트를 연계하여 저작권 시장을 선도해 나갈 것이다.</p>					
색인어 (각 5개 이상)	한글	클라우드, 저작권보호, 제로정보은닉, 경량암호, 특징점			
	영어	Cloud, Copyright, Zero-data hiding, lightweight cryptography, Feature point			

요약문

I. 제목

클라우드 기반 콘텐츠 저작권 보호기술 개발

II. 기술개발의 목적 및 필요성

현재 국내에서는 웹툰과 같은 클라우드 기반 이미지 및 콘텐츠들을 서비스하는 사업이 활발해짐에 따라, 서비스 사업의 신뢰성 및 안전성 제공이 절대적으로 우선시되어야 한다. 또한 클라우드 환경에서 콘텐츠 보호와 동시에 속도 저하를 유발시키지 않는 메커니즘에 대한 시급한 시장 수요예측에 따른 선도성 기술개발이 필요한 시점이다.

기존 저작권 기술은 저작자의 권리를 효율적으로 보호하고 저작물의 공정한 이용을 도모하기 위한 기술 및 서비스를 말하지만 저작권 보호를 위한 기술들은 비용 지불에 민감한 개인사용자나 영세·중소기업의 경우 이러한 저작권기술에 접근하기 어려운 실정이다. 따라서 본 과제에서는 저렴한 비용으로 개인 사용자나 영세기업들이 부담없이 접근할 수 있는 클라우드 기반의 저작권보호 서비스(CaaS: Copyright protection as a Service)와 기존 공용특징정보 사업에서 사용하는 DNA 필터링기반 콘텐츠 검증 기술에 제안하는 제로정보온닉 기술을 접목하여 저작물인식조치, 검색제한조치, 송신제한조치 및 경고문구 발송 등 기술적 조치와 함께 저작권 보호 정보를 은닉함으로 콘텐츠의 불법 유포자와 배포 경로를 추적하는 저작권 보호를 제공해줄 수 있는 하이브리드 저작권보호기술을 제안 및 개발한다.

III. 기술개발의 내용 및 방법

(1) 경량 암호 기반 콘텐츠 인증 기술 개발

- o LEA 경량 암호알고리즘 기반의 안전하고 효율적인 저작권 보호 컨텐츠 암복호화 및 보안인증 기술

○ 클라우드 기반 경량 암호 콘텐츠 인증 서비스 구현

- (2) 특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술 개발
 - 제로정보은닉 기반 위변조 방지 및 저작권 정보 삽입 프로그램
 - 제로정보은닉 기반 위변조 방지 및 저작권 정보 추출 프로그램
- (3) 클라우드 기반의 웹툰/이미지 저작권보호서비스 개발

IV. 기술개발결과

- (1) 경량 암호 기반 콘텐츠 인증 기술 개발
- (2) 클라우드 기반 경량 암호 콘텐츠 인증 서비스 구현
- (3) 특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술 개발
- (4) 클라우드 기반 저작권 보호기술 서비스 구현
- (5) 클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS) 개발

V. 기술개발결과의 활용계획

클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS)의 사업화를 위하여 최종결과물을 이용하여 솔루션 개발을 통해 저작권 보호서비스 형태로 클라우드 업체에 콘텐츠 보안 솔루션으로 제공할 것이며, 클라우드 서버 구축후 자체 서비스를 개시하여 개인이나 중소기업의 콘텐츠를 대상으로 시범사업을 진행하여 국내 클라우드 저작권 시장 개척을 할 것이다. 향후 저작권 위원회와 연계하여 콘텐츠 저작권보호 서비스를 저작권위원회에 제공하여 현 시스템에서 보다 효율적인 저작권보호 시스템을 구축하고, 향후 국내 뿐만 아니라 국외 클라우드 업체 및 포털사이트를 연계하여 저작권 시장을 선도해 나갈 것이다.

S U M M A R Y

I . Title

Developments of Contents Copyright Protection based on Cloud

II . Purpose and necessity of technology development

As the business of providing cloud-based images and contents such as webtoons becomes active in Korea, providing reliability and security of service business should be given priority. In addition, it is time to develop the leading technology based on the anticipated market demand for the mechanism that does not slow down the content while protecting the contents in the cloud environment.

Existing copyright technologies are technologies and services that efficiently protect the rights of authors and promote the fair use of copyrighted materials. However, technologies for copyright protection are not accessible to individual users who are paying for expenses, or to small and medium-sized enterprises It is true. In this project, we propose a cloud-based copyright protection service (CaaS) that can be easily accessed by individual users or small businesses at a low cost and a content verification technology based on DNA filtering used in the existing public feature information business Zero information concealment technology can be applied to provide copyright protection that tracks illegal dissemination of content and distribution path by hiding copyright protection information along with technical measures such as recognition of copyrighted works, restriction of search, transmission restriction and warning statement. Propose and develop hybrid copyright protection technology.

III . Contents and method of technology development

- (1) Development of contents encryption technology based on lightweight encryption
 - o Secure and efficient copyright protection contents encryption and security authentication technology based on LEA lightweight encryption algorithm

- o Implement cloud-based lightweight cryptographic content authentication service
- (2) Development of content copyright protection technology based on zero information hiding applying feature-based filtering
 - o Prevention of forgery and alteration based on zero information hiding and copyright information insertion program
 - o Prevention of forgery and falsification based on zero information hiding and copyright information extraction program
- (3) Cloud-based webtoon/image copyright protection service development

IV. Technology development result

- (1) Development of contents authentication technology based on lightweight encryption
- (2) Implement cloud-based lightweight password content authentication service
- (3) Development of content copyright protection technology based on zero information hiding applying feature-based filtering
- (4) Implement cloud-based copyright protection technology service
- (5) Cloud-based webtoon/image copyright protection service(CaaS) development

V. Plan to utilize technology development results

In order to commercialize cloud-based webtoons/image copyright protection service(CaaS), we will provide cloud protection service as content protection solution through solution development using final product, launch self service after building cloud server We will pilot the domestic cloud copyright market by conducting a pilot project for the contents of individuals or small and medium enterprises. In the future, we will provide a copyright protection service to the copyright committee in cooperation with the copyright commission, and we will build a more effective copyright protection system in the current system, and lead the copyright market by linking overseas cloud companies and portal sites in the future.

CONTENTS

Chapter 1. Outline of technical development task	10
Section 1. Necessity of Technology Development.....	10
Section 2. Purpose of technology development.....	20
Section 3. Differentiation of this technology.....	21
Chapter 2. Status of domestic and overseas technology development	22
Section 1. Status and prospects of domestic and overseas industry	22
Section 2. Status of domestic and overseas technology development	22
Section 3. Differentiation of technology.....	34
Chapter 3. Contents, methods and results of technology development	38
Section 1. Development contents of lightweight cryptographic content au- thentication technology	22
Section 2. Development contents of contents copyright protection based on zero data hiding applying feature based filtering	34
Section 3. Development contents of cloud based webtoons/image copyright protection service	38
Section 4. Technology development method	41
Section 5. Results	44
Chapter 4. Achievement of goal and contribution to related field	92
Section 1. Goal achievement	92
Section 2. Performance goals and indicators o technology development	93
Section 3. Contribution to related fields	94
Chapter 5. Plan to utilize technology development results	99
Chapter 6. Overseas science and technology information collected during the technology development process	101
Section 1. Lightweight cryptography	101
Section 2. Data hiding technology	101
Chapter 7. References	102

목 차

제1장 기술개발과제의 개요	10
제1절 기술개발의 필요성	10
제2절 기술개발의 목적	14
제2장 국내외 기술개발 현황	16
제1절 국내외 산업 현황 및 전망	16
제2절 국내외 기술개발 현황	20
제3절 본 기술의 차별성	21
제3장 기술개발 내용, 방법 및 결과	22
제1절 경량 암호 기반 콘텐츠 인증 기술 개발 내용	22
제2절 특징 기반 필터링을 응용한 제로정보온닉 기반 콘텐츠 저작권 보호기술 개발 내용	34
제3절 클라우드 기반의 웹툰/이미지 저작권보호서비스 개발 내용	38
제4절 기술개발 방법	41
제5절 연구결과 성과물	44
제4장 목표달성도 및 관련분야에의 기여도	92
제1절 목표달성도	92
제2절 기술개발의 성과목표 및 지표	93
제3절 관련분야에의 기여도	94
제5장 기술개발결과의 활용계획	99
제6장 기술개발과정에서 수집한 해외과학기술정보	101
제1절 경량암호 기술	101
제2절 정보온닉 기술	101
제7장 참고문헌	102

제1장 기술개발과제의 개요

제1절 기술개발의 필요성

저작권 보호를 위한 기술에는 배타적 사전 접근 통제기술, 이용자 친환경 기술, 불법 콘텐츠를 막아주는 필터링 기술, 저작물 자유이용 활성화 돋는 ‘자유 이용 활성화 기술’이 있다. 배타적 사전 접근 통제 기술은 종래 디지털 저작권 보호기술은 DRM으로 통칭되는데 이는 디지털 콘텐츠를 불법복제로부터 보호하고, 요금을 부가하여 저작권자에게 발생하는 이익을 관리하는 기술 또는 서비스의 의미로 사용되고 있다. 이용자 친환경 기술은 사후이용실적 추적으로 콘텐츠에 대한 접근을 사전에 통제하는 DRM을 보완하기 위한 기술이 워터마킹/포렌식마크 기반의 저작권 기술을 말한다. 불법 콘텐츠를 막아주는 필터링 기술은 온라인상의 콘텐츠 불법 유통 균열을 위해 저작권법은 특수한 유형의 OSP에 대하여 기술적 보호조치 의무를 부과한다. 이에 따라 OSP는 불법전송을 차단하는 기술적 보호조치로 제목필터링, 문자열비교방식, 특정유형파일 필터링, 해시값 비교 필터링, 오디오·비디오 인식 필터링 등을 적용한다. 자유 이용 활성화란 CCL(조건부 자유이용허락) 등 저작물 이용에 관한 정보를 쉽게 확인·관리할 수 있는 이용자 친화적인 기술이다. 이러한 기술들은 현재 상호 보완적으로 각기 다른 기능을 제공하여 저작권 보호를 하고 있다. 하지만 저작권 보호를 원하는 개인이나 기업의 입장에서는 각기 다른 기술과 기능을 적용하는데 있어 절차적인 문제로 번거롭게 여길 수 있다. 따라서 본 과제에서는 각 기술의 장단점을 취합하여 각각의 저작권 보호 서비스 기능을 제공해 줄 수 있는 통합 저작권 보호 솔루션을 개발하는데 있다.



그림 1 공용특징정보사업의 인터페이스 환경

공용특징정보 사업은 온라인상에서 유통되는 저작물 보호를 위해 신뢰성 있는 필터링기술 사업자와 온라인 서비스 사업자에게 특징점 DB를 제공하는 사업이다. 공용특징정보 사업에서 사용되는 DNA 기법은 특정 영상을 정보의 화면이나 음원 트랙의 특징적인 패턴을 시간적인 배열의 관계 속에서 찾아 내는 기법으로 원본의 내용에 대한 마스터 DNA가 정확할 경우 상당히 높은 수준으로 그 영상을 판별해 낼 수 있기 때문에 수동작업에 머물러 있는 그간의 영상을

필터링의 대안으로 사용된다. 하지만 이러한 DNA 필터링 기술로는 저작권 보호를 위한 안전한 장치가 명확하게 제공되지 않고 콘텐츠에 대한 소유권 증명에 제한이 있다. 본 사업에서는 기존 공용특징정보사업에서 사용하는 DNA 필터링기반 콘텐츠 검증 기술에 제안하는 제로정보은닉 기술을 접목하여 저작물인식조치, 검색제한조치, 송신제한조치 및 경고문구 발송 등 기술적 조치와 함께 저작권 보호 정보를 은닉함으로 콘텐츠의 불법 유포자와 배포 경로를 추적하는 저작권 보호를 제공해줄 수 있는 하이브리드 저작권보호기술을 개발한다.

표 1 특징 기반 필터링의 메타파일 예

```
<?xml version="1.0" encoding="UTF-8" ?>
<METADATA>
    <TITLE><![CDATA[꾸러기 탐구생활 47회]]></TITLE>
    <RELEASE>20100729165811</RELEASE>
    <PLAYTIME>02537</PLAYTIME>
    <RIGHTOWNERNAME>SBS</RIGHTOWNERNAME>
    <RIGHTOWNERID>cu0409f0004700</RIGHTOWNERID>
    <RIGHTEXPIREDATE>NONE</RIGHTEXPIREDATE>
    <RIGHTPOLICY />
    <RIGHTPAYMENT />
    <SEARCHTYPE />
    <GENRE>교양</GENRE>
    <GRADE>00</GRADE>
    <DIRECTOR />
    <ACTOR><![CDATA[]]></ACTOR>
    <COUNTRY_FLAG>1</COUNTRY_FLAG>
</METADATA>
```

또한, 기존 저작권 기술은 저작자의 권리를 효율적으로 보호하고 저작물의 공정한 이용을 도모하기 위한 기술 및 서비스를 말하지만 저작권 보호를 위한 기술들은 비용 지불에 민감한 개인 사용자나 영세·중소기업의 경우 이러한 저작권기술에 접근하기 어려운 실정이다. 따라서 본 과제에서는 저렴한 비용으로 개인 사용자나 영세기업들이 부담없이 접근할수 있는 클라우드 기반의 저작권보호 서비스(CaaS: Copyright protection as a Service)를 제안한다.

클라우드는 각 PC 단말에서 개별적으로 프로그램을 설치해 데이터를 저장하던 기존 방식에서 벗어나, 인터넷 네트워크상에 모든 IT자원(소프트웨어, 스토리지, 서버, 네트워크 등)을 저장하여 개별 컴퓨터에 할당하는 개념으로 제공 업체들이 고객들의 필요에 따라 소프트웨어, 플랫폼, 인프라로 이루어진 IT 서비스를 사용한 만큼 가격을 책정하여 사설 또는 공용 네트워크 기반으로 서비스를 제공하는 것을 의미한다. 클라우드는 신속한 서비스 제공 및 탄력성(Rapid Elasticity), 수요에 따라 자동화되어 제공되는 서비스, 광범위한 네트워크 접속 기능, 컴퓨팅 자원들의 공유 집합화, 계량화된 서비스를 핵심 특징으로 가지고 있다. [1-4]

클라우드를 제공하는 서비스는 IT자원에 따라 인프라서비스(Infrastructure as a Service: IaaS), 플랫폼서비스(Platform as a Service: PaaS) 및 소프트웨어서비스(Software as a Service: SaaS)

로 구분할 수 있다.

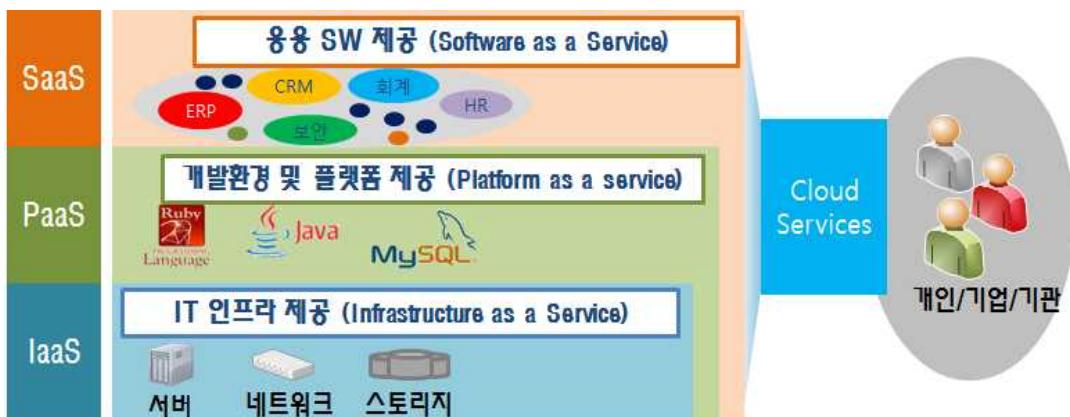


그림 2 클라우드 서비스 모델

국외기업에는 아마존, 구글, 마이크로소프트, VMware, SAP, Salesforce.com의 사업자가 있으며, 국내기업에는 KT, SKT, LG-CNS, 더존비즈온, 한글과컴퓨터, 파수닷컴, 다우기술 등의 사업자들이 서비스를 해주고 있다.

클라우드를 이용하는 경우, 온라인서비스와 마찬가지로 클라우드 서비스 중에는 그 성질상 클라우드 서버에 데이터를 저장하거나 인터넷을 통하여 그 데이터에 접속을 가능케 하는 서비스가 존재한다. 클라우드의 속성 중의 하나는 이용자들이 희망하는 콘텐츠를 언제 어디서나 이용 할 수 있도록 하기 위한 것이고 이를 위해서는 콘텐츠가 다운로드 형태뿐만 아니라 스트리밍 형태 등으로 제공되고, 후자의 과정에서 소프트웨어와 같은 콘텐츠는 클라우드 이용자의 컴퓨터 RAM에 일시적으로 복제된다. 나아가 클라우드 서비스 제공자도 현행 저작권법이 정의하고 있는 온라인서비스제공자(online service provider: OSP)가 될 수 있고 저작권 침해책임을 부담 할 수 있다. **클라우드 서비스 과정에서 제3자의 저작물이 포함된 콘텐츠가 취급되는 경우에 서비스 이용과정에서 저작물의 복제와 공중송신 행위가 발생하면 저작권법상의 문제가 발생할 수 있다. [5-7]**

법적으로 제정한 클라우드 서비스 제공자의 책임은 아래의 표와 같다.

표 2 클라우드 서비스 제공자의 저작물에 대한 책임

제 102 조 온라인서비스제공자의 책임 제한 온라인서비스제공자는 다음 각 호의 행위와 관련하여 저작권 그 밖에 이 법에 따라 보호되는 권리가 침해되더라도 그 호의 분류에 따라 각 목의 요건을 모두 갖춘 경우에는 그 침해에 대하여 책임을 지지 아니한다.

1. 내용의 수정 없이 저작물등을 송신하거나 경로를 지정하거나 연결을 제공하는 행위 또는 그 과정에서 저작물등을 그 송신을 위하여 합리적 으로 필요한 기간 내에서 자동적 중개적 일시 적으로 저장하는 행위
2. 서비스이용자의 요청에 따라 송신된 저작물등을 후속 이용자들이 효율적으로 접근하거나 수신 할 수 있게 할 목적으로 그 저작물등을 자동적 중개적 일시적으로 저장하는 행위
3. 복제 전송자의 요청에 따라 저작물등을 온라인서비스제공자의 컴퓨터에 저장하는 행위
4. 정보검색도구를 통하여 이용자에게 정보통신망상 저작물등의 위치를 알 수 있게 하거나 연결하는 행위

저작권법 제102조는 인터넷 접속서비스, 캐싱서비스, 호스팅서비스 및 정보검색서비스로 구분하여 온라인서비스제공자의 일정한 면책사유를 정하고 있다. 이 유형들은 이용자의 관점에서 이용자의 관여가능성에 따라, 이용자의 행위와 서비스가 직접 연관성이 있는 것이 호스팅서비스와 정보검색서비스이고, 직접관여를 필요로 하지 않는 것이 접속서비스와 캐싱서비스에 해당한다. 현재 N드라이브, 다음클라우드, U클라우드와 같이 국내에서 서비스 되고 있는 대부분의 클라우드 서비스는 서버에 일정한 저장공간을 부여하고, 그 공간에 저장된 다양한 포맷(동영상, 음악, 문서 등)의 파일을 유무선 통신을 이용, 이동형 단말기를 통해서 이용할 수 있도록 서비스를 제공하고 있다. 이러한 클라우드 서비스는 유무선 통신과 컴퓨터 및 이동형 단말기를 이용하여 일정한 저장공간에 파일을 업로드하고, 언제 어디서나 자신의 정보를 이용할 수 있는 서비스를 제공 중이며, 이를 서비스는 SaaS라는 서비스 유형에 해당하고, 이러한 서비스는 복제·전송자의 요청에 따라 저작물 등을 온라인서비스제공자의 컴퓨터에 저장하는 행위를 하는 호스팅 서비스에 해당될 것이다. 따라서 현재 N드라이브, 다음클라우드, U클라우드 등 다양한 클라우드 서비스는 저작권법 제102조의 호스팅서비스에 대한 책임제한 규정이 적용될 수 있을 것이다. 따라서 클라우드 서비스를 제공하는 기존 업체들은 콘텐츠에 대한 저작권보호와 필터링기능을 제공 할 수 있는 저작권보호 서비스(CaaS: Copyright protection as a Service) 제공이 필요한 실정이다.

미국 노동부의 IPI(2007a)는 'The True Cost of Copyright Industry Piracy to the U.S. Economy' 보고서를 통해 373,375명의 미취업 미국인들이 불법복제된 영화, 비디오 게임, 음반을 소유·배포하고 있으며, 이로 인해 그들 스스로의 취업 기회를 빼앗기는 것은 물론 미국 경제에 무려 163억 달러의 경제적 손실을 입히고 있다고 분석하였다. 위 연구에서는 저작권 산업을 영화, 음반, 소프트웨어, 비디오게임으로 분류하고 이를 산업에서의 불법복제로 인한 미국 경제 전반에 걸친 경제적 손실을 추정하고 있다. 만약 불법복제물이 사라진다면 미국 경제에 373,375개의 새로운 일자리가 추가될 것이며, 그 중 123,814개의 일자리가 저작권 관련 산업에서 창출될 수 있을 것이라고 분석했다. 그리고 다른 산업 분야에서도 249,561개의 일자리가 새롭게 추가될 수 있을 것으로 예상했다.

표 3 불법복제물로 인한 세수 손실 규모

구 분	손실된 금액	비 고
생산액 손실	63조 8000억 원(580억 달러)	-
일자리 손실	373,375개	저작권관련 산업에서 123,814개 일자리 손실 / 미국의 다른 산업에서 249,561개 일자리 손실
근로 소득의 손실	17조 9,300억 원(163억 달러)	저작권관련 산업 종사자로부터 72억 달러 소득 손실 / 기타 산업분야 종사자로부터 91억 달러 소득 손실
세수 손실	2조 8,600억 원(26억 달러)	이중 18억 달러는 개인 소득세 형태, 8억 달러는 법인세 형태의 세수 손실임

나아가 저작권 관련 산업에서 추가된 인력은 72억 달러의 수익을 얻을 수 있는 규모이며, 기타 산업 분야에서 추가된 인력으로 91억 달러의 수익이 발생할 것으로 예상했다. 불법복제물로 인한 세수 손실 규모는 총 26억 달러이며 이중 18억 달러는 개인 소득세 형태로 나머지 8억 달러는 기업 대상의 법인세 형태의 세수손실로 추정했다.

이와 같이 불법복제물로 인해 저작권의 소유자와 저작물의 제작자뿐만 아니라 미국의 소비자, 노동자 그리고 납세자 등 미국 모든 국민에게 피해가 돌아간다고 결론지었다. 또한 미국이 국제시장에서 지속적이 경쟁력을 유지하려면 정책 입안자들이 수많은 의제 중 저작권 침해 문제를 우선순위에 두어야 할 것이라고 지적했다. 본 과제의 목표인 개인 및 영세·중소기업을 대상으로 한 효율적이고 접근성이 높은 클라우드 기반 저작권보호 서비스 제공으로 생산액손실과 일자리 손실, 근로소득의 손실 및 세수의 손실을 줄일 수 있을 것으로 보이며, 이는 국가 경제 차원에서 손실을 줄일 수 있을 것을 보인다.

현재 제공 중인 공용특징정보 사업의 문제점과 클라우드 환경에서 콘텐츠 저작권 문제를 고려하여 저작권 보호 조치를 제대로 제공받지 못하는 개인 및 영세·중소기업을 대상으로 한 본 과제의 최종 목표는 클라우드 환경에서 저작권보호 서비스(CaaS: Copyright protection as a Service)를 통한 콘텐츠 보호 및 개인 및 영세·중소기업을 대상으로 한 효율적이고 접근성이 높은 저작권보호 서비스 제공하는 것이다.

제2절 기술개발의 목적

본 과제의 최종목표는 클라우드 환경에서 저작권보호 서비스(CaaS: Copyright protection as a Service)를 통한 콘텐츠 보호 및 개인 및 영세·중소기업을 대상으로 하는 효율적이고 접근성이 높은 저작권보호 서비스를 제공하는 것이다.



그림 3 기술개발의 최종 목표

이를 달성하기 위한 개별목표는 다음과 같다.

- (1) 경량 암호 기반 콘텐츠 인증 기술: 클라우드 환경에서 콘텐츠 보호를 위해 고속의 경량암호 모듈인 LEA(Lightweight Encryption Algorithm)를 이용한 ① 경량 암호 기반 콘텐츠 인증 기술을 개발하여 인증을 통한 콘텐츠에 대한 접근제한을 제공하여준다.
- (2) 특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술: 또한 특징점(DNA) 기반 필터링 기술에 제로정보은닉 기반의 스테가노그래피 기법을 접목하여 ② 특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술을 개발하여 고품질의 콘텐츠를 제공하여 준다.
- (3) 클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS) 개발: ①의 기술개발 내용과 ②의 내용을 기반으로 하여 ③ 클라우드 기반의 웹툰/이미지 저작권 보호 시스템 개발을 통해 클라우드환경에서 정지영상에 대한 특징점(DNA) DB를 제공할 뿐만 아니라 저작권보호 및 안전한 콘텐츠 서비스를 제공을 하는 클라우드 저작권 보호 서비스(CaaS: Copyright protection as a Service)를 개발한다.

클라우드 환경에서 저작권보호 서비스(CaaS: Copyright protection as a Service)를 통한 콘텐츠 보호 및 개인 및 영세·중소기업을 대상으로 한 효율적이고 접근성이 높은 저작권보호 서비스 제공하는 것

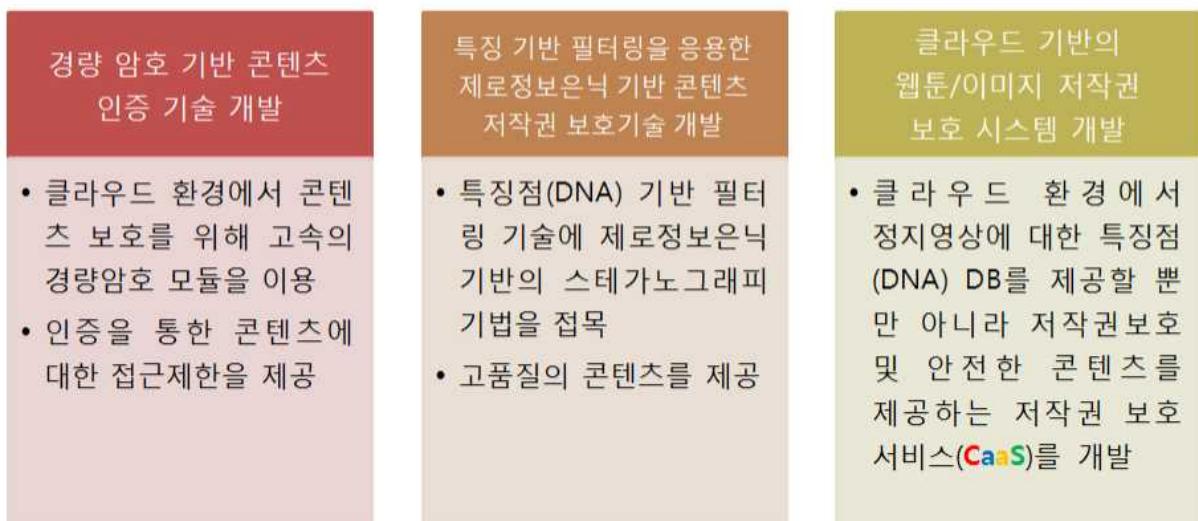


그림 4 기술개발의 최종 목표

본 기술개발결과의 활용방안 및 기대성과로서 본 과제의 최종결과물인 클라우드 기반의 웹툰/이미지 저작권 보호 시스템 개발을 통해 생산한 콘텐츠에 대한 저작권을 보호받지 못하는 개인 또는 영세·중소기업 콘텐츠에 대한 저작권 보호와 특징점(DNA) DB를 제공과 콘텐츠에 대한 저작권 보호를 제공함에 따라 저작권에 대한 인식을 확대할 수 있어 저작권 침해문제로 발생되는 금전적인 손실을 줄일 수 있을 것이다. 또한 본 과제의 연구내용은 기존에 구축되어있는 클라우드 관련 기술들이 가지는 다양한 저작권 문제점을 해결하며 클라우드 기반 저작권 기술에 관한 최근 연구를 보다 발전시켜 안전성 및 효율성 보장은 물론 실용성을 가지는 강력한 웹툰/이미지 저작권 보호 서비스(CaaS) 제공으로 차세대 클라우드 시스템 개발 및 구축을 목표로 함으로 해당 기술 개발 및 기술 확보는 클라우드 산업뿐만 아니라 저작권 산업 발전을 위해 실용적으로 활용될 수 있다.

제2장 국내외 기술개발 현황

제1절 국내외 산업 현황 및 전망

1. 시장 현황 및 전망

가. 국내외 시장규모

▣ 국내시장

- (국내시장) ‘13년 3,932억원 → ’14년 5,238억원으로 33.22% 성장(‘14년 NIPA)하여 연평균 30%이상 고성장 예상



그림 5 국내 클라우드 시장규모 및 전망,
‘14년 부산시 클라우드 산업육성 계획

- 국내 클라우드 시장은 통신사와 포털을 중심으로 초기 시장이 형성되었으나 최근 글로벌 ICT 기업들이 국내 시장에 적극적으로 참여
- 국내 서비스로는 KT의 U클라우드 비즈가 6,000여 기업 고객을 보유한 국내 1위 기업형 클라우드 서비스로 대표적이고 네이버와 다음도 개인고객과 중소기업을 중심으로 클라우드 시장에서 선전
- ‘클라우드 산업 육성 계획’을 확정하였는데, 특히 2017년까지 공공기관의 15%이상에 민간 클라우드를 활용할 수 있도록 유도하려함
- 클라우드 기술 및 표준화, 생태계 기반 조성 등을 통해 국내 클라우드 시장규모를 2012년 5천억원 규모에서 2017년 2조 5천억원으로 확대하고자 함
- 미래부 산하 4개 공공기관과 5개 클라우드 사업자들이 사업에 참여하고 있으며, 공공 기관의 민간 클라우드 이용 확산을 위한 가능성 탐진 및 사례 구축 추진을 목적으로 하고 있어 공공기관의 민간 클라우드 본격 도입과 서비스 확산에 기여할 전망임

■ 국외시장

- '13년 368억불 → '18년 1,275억불(연23%) 성장('14년 IDC)
- 中 국가판권국, 클라우드에서의 저작권 보호성과 거듭: 2015년 12월 3일 국가판권국의 보도에 따르면, 2015년 10월 20일 《인터넷 클라우드 서비스 저작권 질서 규범에 관한 통지(关于规范网盘服务版权秩序的通知)》의 공포에 따라, 클라우드 서비스 제공자들은 자율적으로 불법저작물을 삭제하였음. 또한 규범적인 인터넷 클라우드 환경을 구축하기 위하여 서비스제공자들은 저작물의 저작권정보, 업로드자의 연락처, 저작물의 심사 기준 등을 명확히 기재하여 통지 및 삭제(Notice and Takedown)제도를 적극적으로 활용함으로써 저작권자의 권리보호를 강화함

(단위: 백만 달러)



	2013	2014	2015	2016	2017
퍼블릭	47,396	59,487	73,541	89,411	107,217
프라이빗	9,050	9,830	10,750	11,850	13,154

그림 6 글로벌 클라우드 시장규모 및 전망,
‘14년 부산시 클라우드 산업육성 계획

- 국외의 경우 미국, 영국 등을 중심으로 공공기관 민간 클라우드 도입이 적극적으로 추진되었으며 이를 통한 비용절감, 효율성 개선의 효과가 현실화되었음
- 미국은 2010년부터 ‘Cloud First Policy’ 정책을 발표해 클라우드 우선적인 정책을 시행하고 있으며, 영국은 공공분야 클라우드에 대한 전략으로 ‘G-Cloud’를 발표하고 민간 기업이 참여하는 ‘Cloud Store’를 운영
- Amazon, IBM 등 ICT 기업들은 B2G 클라우드 시장에서 수익창출을 가시화 하고있음

나. 국내외 시장의 특성

■ 국내시장

- 2015년 3월 3일 클라우드 컴퓨팅 발전법이 국회 본회의를 통과하여 2015년 9월 28일부터 시행되고 있음
- 법안의 주 목적은 공공부문 클라우드 도입확대, 클라우드 산업 투자 활성화, 그리고 클라우드의 안전한 이용환경 조성, 산업 전반의 경비절감, 생산성 증가 등에 있음
- 클라우드 확산의 가장 큰 벽인 ‘보안’ 부분의 개선을 위해서 다양한 규정을 제정

■ 국외시장

- 중국: 클라우드 컴퓨팅 산업 육성정책 발표로 관련 산업 50% 이상 성장, 중국은 클라우드 산업을 육성하기 위한 정책을 지속적으로 시행하고 있으며, 2014년 공공 클라우드 서비스 기업들의 매출은 약 70억 위안(약 1조 2,300억원)으로 2013년에 비해 47%증가, ‘클라우드 컴퓨팅 산업의 창의적인 발전 촉진 및 정보산업 신규 경영 모델 육성 관련 의견’을 발표하며 향후 클라우드 컴퓨팅 산업에 대한 지원 방안을 제시
- 일본: 가스미가세키 프로젝트, 클라우드 이용률 급증, 일본은 일찍이 2009년부터 클라우드 컴퓨팅 산업 육성 정책을 실시, ‘가스미가세키’ 프로젝트가 대표적으로 ‘13개 중앙부처 서버 통합 및 자체 클라우드 도입’, ‘2020년까지 데이터센터 서버수 400 만대로 확대’, ‘미국 등 전 세계 글로벌 IT 기업의 데이터센터를 일본에 유치’ 등이 있음, 이를 통해 2010년 1~2% 수준에 불과했던 기업들의 클라우드컴퓨팅 이용률이 한 자릿수 후반까지 상승하는 추세를 보이고 있음
- 미국: Cloud First 정책을 통해 공공기관 클라우드 적극 도입, 클라우드 도입이 가장 활발한 미국의 경우 2010년 12월 클라우드 퍼스트 정책을 통해 공공기관에 클라우드 컴퓨팅을 적극적으로 도입, 당시 CIO였던 비벡 쿤드라는 각 정부기관들에 대해 기존에 사용하고 있는 솔루션 가운데 세가지를 택해 1개를 12개월 이내에, 나머지 두 가지는 18개월 이내에 이전을 완료하도록 강제조항(mandate)으로 만들어 활성화 시킴, 2012년, 국토안보부를 포함한 미국의 7개 기관 기준 21개에 불과했던 클라우드 서비스 도입 프로젝트의 수는 2014년 101개까지 5배 가까이 증가했으며, 클라우드 관련 투자 비용도 약 3억불에서 5.3억불까지 72% 상승, 특히 CIA에서 아마존과 10년간 6억불 규모의 계약을 맺고 클라우드 서비스를 도입

다. 국내외 시장의 경쟁현황

- (IaaS) 아마존(28% 점유), MS(10% 점유) 등이 시장을 주도 중이며, 최근 알리바바·텐센트 등 중국기업이 IaaS에 적극 투자 중
※알리윤(中)은 미국에 클라우드 데이터센터 개설을 위해 약 10억불 투자 발표(' 15.7월)
- 국내는 KT·네이버 등 통신사(B2B) 및 인터넷(B2C) 기업을 중심으로 IaaS를 제공(KT는 공공 기관 전용 클라우드 출시, ' 15.8월)
- (PaaS) IaaS 주도권을 확대하고 다양한 SaaS를 유입하여 자사만의 생태계를 확보하기 위해 아마존, MS 등 글로벌 기업이 경쟁 중
※세계 PaaS 순위(IDC, '15년) : (1위) MS, (2위) 세일즈포스닷컴, (3위) 아마존
- (SaaS) 세일즈포스닷컴·구글·MS 등 미국 기업이 주도하는 가운데, SAP·오라클·어도비 등 전통적인 SW 기업들도 시장 진입 중
- 국내는 더존비즈온·한글과컴퓨터 등이 ERP, 오피스 SaaS를 글로벌 시장에 진출 추진 중
※더존비즈온은 ERP를 SaaS로 전환 후 매출 급증(' 13년 53억원 → ' 14년 280억원)
※세계 SaaS순위(IDC, '15년) : (1위) 세일즈포스닷컴, (2위) 인튜이트, (3위) SAP

2. 생산 현황 및 전망

가. 국내외 생산규모

- ‘Private’ 과 ‘Public’ 이 결합된 형태의 ‘Hybrid’ 클라우드 확산이 주요 키워드로 이

어질 것으로 전망되며, 오픈스택(OpenStack)에 대한 관심 또한 지속될 전망임

- 클라우드 플랫폼이 기능적인 면에서 성숙 단계로 진입하면서, ‘Private’과 ‘Public’을 병행하는 ‘Hybrid’ 클라우드의 수요가 증대될 것으로 기대됨
- 혁신에 대한 대응 역량, 개방형 기술, 비용절감효과, 종속 방지 등의 강점으로 오픈스택을 도입하려는 기업들의 수요는 더욱 증가할 것으로 전망됨

구분		'13년	'14년	'15년	'16년	'17년	'18년	'19년	CAGR '14-'19
세계	SW	1,231,526	1,280,242	1,335,907	1,397,643	1,465,001	1,538,697	1,619,653	4.8%
	클라우드	70,914	83,610	96,927	115,278	135,533	158,370	182,211	16.9%
	클라우드비중	5.8%	6.5%	7.3%	8.2%	9.3%	10.3%	11.2%	
국내	SW	20,821	22,209	21,936	22,760	23,576	24,459	25,387	2.7%
	클라우드	419.6	537.7	630.4	751.9	886.2	1,045.9	1,216.2	17.7%
	클라우드비중	2.0%	2.4%	2.9%	3.3%	3.8%	4.3%	4.8%	

그림 7 국내 및 국외 소프트웨어 시장과 클라우드 시장 비교, ‘15년 Gartner

나. 국내외 생산업체 및 제품생산 현황

■ 국내시장

- 산업재산권 보유현황은 243개이며, 출원진행현황은 105개로 나타남
- 산업재산권 보유현황은 SaaS가 117개, Cloud SW가 56개, IaaS가 32개, Paas가 25개, Cloud HW가 13개의 순으로 많이 보유하고 있음
- 산업재산권 출원진행현황은 Paas가 34개, SaaS가 31개, Cloud SW가 27개, IaaS가 12개, Cloud HW가 1개의 순으로 많이 진행되고 있음
- 2012년 클라우드 근로자는 전체 상시 근로자 대비 약 3.14%이며, 2013년 클라우드 근로자는 전체 상시 근로자 대비 약 5.22%로 매년 클라우드 근로자 비중이 증가하는 것으로 나타남

■ 국외시장

- 중국: 중국의 클라우드 서비스 제공 사업자는 China Telecom, China Mobile, China Unicom 등 통신 사업자와 Baidu, Tencent, Qihoo 360 등 현지 대기업들이 주력을 이루고 있음, China Telecom은 자체 클라우드 컴퓨팅 서비스인 e-Surfing을 2012년에 상용화했으며, 3위 통신사업자로서 클라우드 컴퓨팅 분야 투자를 통해 순위 역전을 노리고 있음, China Mobile은 2012년 8월에 Mccloud 서비스를 개시해 사용자들에게 16GB 용량의 데이터 서비스를 무료로 제공 중이며, 2013년 12월부터 20억 위안을 들여 33만 3,000제곱미터 크기의 클라우드 컴퓨팅 센터를 건설 중, China Unicom은 2012년 5월부터 기업을 대상으로 하는 기업용 클라우드 서비스를 제공 중이며, 2013년 12월에는 퍼블릭 클라우드 서비스 ‘Wo Cloud’도 출시, 한편, Baidu, Tencent, Qihoo360 등 주요 인터넷 기업들도 자사의 고객들을 대상으로 대용량의 클라우드 서비스를 제공하고 있으며, 해당 서비스는 Android, iOS, Windows 등을 기본으로 지원, Kanbox, 115网盘, Weibo, Kuaipan, Huawei 등도 개인용 클라우드 스토리지 서비스 상품을 제공하고 있음

제2절 국내외 기술개발 현황

1. 배타적 사전 접근통제 기술

- 가. 종래 디지털 저작권 보호기술은 DRM으로 통칭되는데 이는 디지털 콘텐츠를 불법복제로부터 보호하고, 요금을 부가하여 저작권자에게 발생하는 이익을 관리하는 기술 또는 서비스의 의미로 사용되고 있음
- 나. DRM기술은 온라인상의 디지털 콘텐츠 보호를 위해 적용되고 있으며, 최근 디지털방송 및 IPTV, 스마트폰 등 신서비스의 등장으로 그 수요는 다양한 분야로 확산되고 있음
- 다. 그러나 DRM은 기술간 호환성이 결여된 폐쇄성을 특성으로 하고 있어 일부 사업자는 DRM 기술을 독점시장 구축 수단으로 활용하여 공정시비 논란이 제기됨
- 라. 또한 호환성 부재로 인해 소비자가 가정 등에서 편리하게 복제할 수 있는 권리가 제한되는 등 이용자 불편이 증가함에 따라 사용자 친화형 저작권 기술의 필요성이 대두
- 마. DRM 상호연동 기술은 DRM 기술의 호환성 부족에 대한 반성으로 등장
- 바. 이는 다양한 서비스 환경 및 상이한 DRM 시스템 간 호환성을 제고함으로써 디지털 콘텐츠의 안전한 이용을 보장하는 기술
- 사. DRM의 호환성을 제고하기 위한 가장 손쉽고 확실한 방법은 단일 기술규격으로 DRM 기술을 표준화하는 것이나 이미 많은 DRM 기술이 존재하고 있어 쉽지 않은 상황임

2. 이용자 친환경 기술

- 가. 콘텐츠에 대한 접근을 사전에 통제하는 DRM을 보완하기 위한 기술이 워터마킹/포렌식마크 기반의 저작권 기술
- 나. 워터마크는 콘텐츠에 사람이 인지할 수 없는 저작권 정보를 삽입하고 검출기를 통해 삽입 정보를 식별하는 기술이며, 이러한 워터마크 기술에 구매자 정보나 유통경로 및 사용자 정보를 삽입하여 유포자와 배포경로를 추적할 수 있는 기술이 포렌식마크
- 다. 현재 UMG(Universal Music Group)는 워터마크를 삽입하여 음악 트랙을 제공한 판매자 정보를 관리하고 있는데, 2009년 8월 국내 전문업체 마크애니는 UMG에 향후 3년간 매년 70만 달러에 달하는 워터마크 기술 공급계약을 체결한 바 있음
- 라. 또한 IPTV, 지상파 방송국 등에서 포렌식마크 기술을 이용한 불법 콘텐츠 추적과 모니터링 시스템 구축을 준비하는 등 워터마크/포렌식마크 기술수요가 점차 증대되고 있는 상황

3. 불법 콘텐츠를 막아주는 필터링 기술

- 가. 온라인상의 콘텐츠 불법 유통 근절을 위해 저작권법은 특수한 유형의 OSP에 대하여 기술적 보호조치 의무를 부과
- 나. 이에 따라 OSP는 불법전송을 차단하는 기술적 보호조치로 제목필터링, 문자열비교방식, 특정유형파일 필터링, 해시값 비교 필터링, 오디오·비디오 인식 필터링 등을 적용
- 다. 오디오·비디오 인식 필터링 기술은 음원 또는 영상파일의 고유한 특징인 주파수나 화면 전환 정보, 위치정보, 컬러정보 등 특징점(음원DNA, 영상DNA라고 부르기도 함) DB를 구축하여 복제물과 비교하는 방식으로서 현재로서는 최적의 필터링 기술로 평가되고 있으며 P2P, 웹하드, UCC 등의 저작권 보호 외에 콘텐츠 검색 분야에 활용할 경우 개인의 콘텐츠

활용도 및 이용활성화에 기여할 수 있는 기술로 평가되고 있음

4. 저작물 자유이용 활성화 돋는 ‘자유 이용 활성화 기술’

- 가. 자유 이용 활성화란 CCL(조건부 자유이용허락) 등 저작물 이용에 관한 정보를 쉽게 확인 · 관리할 수 있는 이용자 친화적인 기술입니다. 국내의 경우 CC Korea(사단법인 크리에이티브 커먼즈 코리아)를 통해 저작물의 자유이용을 촉진하고 있으며, 국내의 주요 블로그 및 카페, 사진 공유 서비스와 포털의 게시판에서도 이에 동참
- 나. 또한 CC Korea에서는 CCL 적용사이트의 콘텐츠를 통합해 검색할 수 있는 CC Search 서비스를 제공하고 있습니다. 2009년 미국도서관협회는 저작물의 공정한 사용을 평가하는 정보를 수집 및 보관할 수 있는 툴 ‘FairUse Evaluator’를 발표하여 일반에 제공
- 다. 우리나라의 경우 문화체육관광부에서 2007년부터 자유이용저작물 사이트를 개설하여 저작권이 만료된 저작물과 기증저작물을 일반인들이 편리하게 이용할 수 있도록 제공하고 있으며, 최근에는 새롭게 대두되고 있는 창조경제 패러다임에 부응하기 위하여 정부부처 등과 공공정보 민간활용촉진에 대해 정책공조를 하는 한편, 자유이용 공유저작물-만료저작물, 기증저작물, CCL부착 저작물, 공공기관이 무료로 개방하는 저작물 등의 사회적 확산 정책을 적극 추진중

제3절 본 기술의 차별성

기존 국내외 개발되어 상용화되는 기술은 배타적 사전 접근통제 기술, 이용자 친환경 기술, 필터링 기술, 자유 이용 활성화 기술로 구분된다. 하지만 이러한 기술은 콘텐츠에 대해 따로 제공이 되어 지기 때문에 사용자에게 있어 혼란을 가중하고 절차적인 복잡성이 문제된다. 따라서 본 과제에서 제안하는 클라우드 기반 콘텐츠 저작권 보호기술은 클라우드의 특성을 이용한 접근통제와 이용자 친환경을 위한 제로정보온너, 불법 콘텐츠를 막기위한 필터링기술, 사용자가 쉽게 접근할 수 있는 자유이용 활성화기술의 장점들을 모은 하나의 콘텐츠 저작권 보호 서비스(CaaS)를 제공할 수 있다.

또한, 현재 상용화되어 서비스되고 있는 정보온너/워터마킹 기법은 원본 콘텐츠의 왜곡이 발생하기 때문에 고용량의 고품질 콘텐츠를 제공할 수 없는 문제가 있다. 하지만 본 과제에서 제안하는 제로 정보온너 기반의 콘텐츠 저작권 보호기술은 원본 콘텐츠의 수정이나 변경없이 원본을 그대로 사용할 수 있어 콘텐츠를 서비스 받는 사용자뿐만 아니라 콘텐츠를 제공하는 개인 또는 기업의 만족도를 향상 시킬 수 있다.

제3장 기술개발 내용, 방법 및 결과

제1절 경량 암호 기반 콘텐츠 인증 기술 개발 내용

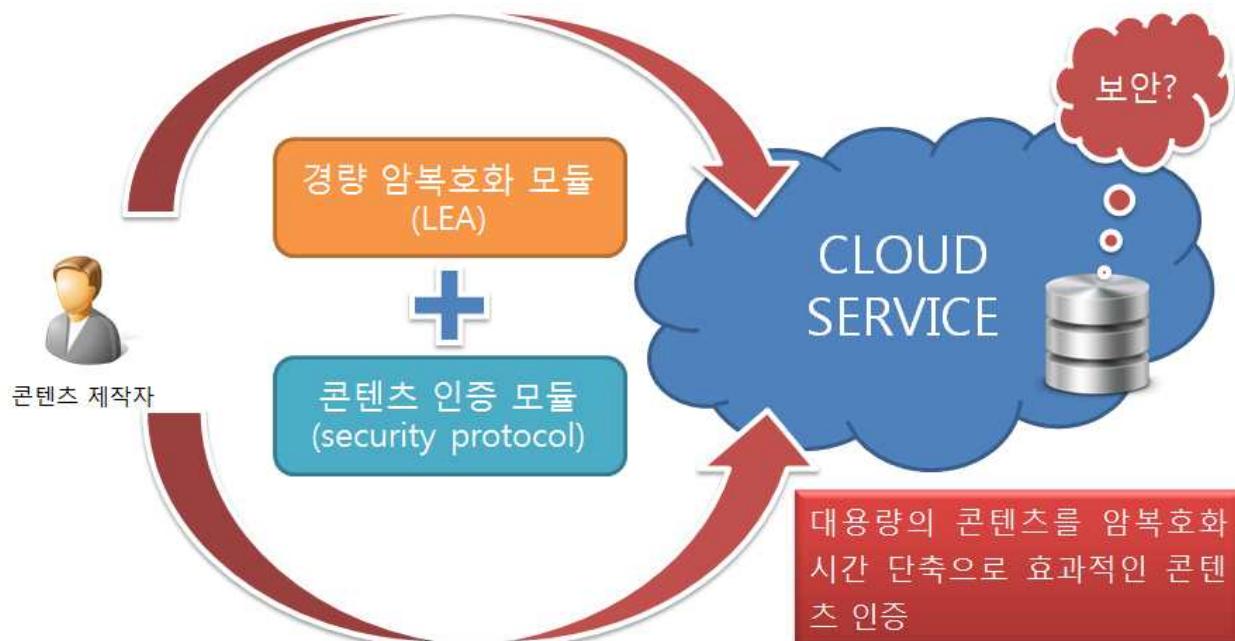


그림 8 경량 암호 기반 콘텐츠 인증 기술 개발 목표

[그림 8]은 제안하는 경량 암호 기반 콘텐츠 인증 기술 개발 목표를 보여준다. 스토리지를 제공하는 클라우드 환경에서 저장되어 있는 콘텐츠에 대한 보안을 적용하기 위해 가장 적합한 방법은 암호 모듈을 사용하는 것이다. 하지만 기존 암호모듈의 경우 대용량의 콘텐츠를 암·복호화하면 시간이 많이 소요되는 단점 때문에 실제 클라우드 환경에서 암호모듈이 잘 사용되지 않는다.

본 과제에서는 클라우드 환경에서 콘텐츠를 안전하게 보관하고 인증된 콘텐츠를 제공하기 위해 IoT 표준 암호모듈인 LEA 경량암호기반 콘텐츠 인증 기술을 개발한다. 본 기술의 가장 큰 장점은 클라우드 환경에 적합한 LEA 경량암호를 사용하여 대용량의 콘텐츠에 대한 암·복호화 시간의 단축으로 효율적인 콘텐츠 인증 기술을 제공한다.

1. 128비트 블록암호 LEA 소개

블록암호 LEA(Lightweight Encryption Algorithm)는 128비트 데이터 블록을 암호화하는 알고리즘으로 128, 192, 256비트 비밀키를 사용할 수 있으며 요구되는 안전성 기준에 따라 용도가 구분될 수 있다. LEA(Lightweight Encryption Algorithm)의 라운드 함수는 32비트 단위의 ARX(Addition, Rotation, XOR) 연산만으로 구성되어 있어, 이를 연산을 지원하는 범용 32비트 소프트웨어 플랫폼에서 고속으로 동작한다. 또한 라운드 함수내부의 ARX(Addition, Rotation, XOR) 연산 배치는 충분한 안전성을 보장하는 것과 동시에 S-box의 사용을 배제하여 경량 구현이 가능하도록 한다. [8-10]

LEA의 전체적인 동작 과정을 도시하면 아래 [그림 9]와 같다.



그림 9 LEA의 전체적인 동작 과정

암호화 과정: LEA의 암호화 함수 Encrypt는 k비트 키 K에 대해 키 스케줄 함수 $KeySchedule_k^{enc}$ 을 수행하여 생성된 Nr개의 192비트 라운드키와 128비트 평문 $P=(P[0], P[1], \dots, P[15])$ 를 입력받아 [그림 7]의 알고리즘을 수행하여 128비트 암호문 $C=(C[0], C[1], \dots, C[15])$ 를 출력한다.

$$RK_i^{enc} = (RK_i^{enc}[0], RK_i^{enc}[1], \dots, RK_i^{enc}[5]) \quad (0 \leq i \leq (Nr-1))$$

입력: 128비트 평문 P , Nr개의 192비트 라운드키 $RK_0^{enc}, RK_1^{enc}, \dots, RK_{Nr-1}^{enc}$

출력: 128비트 암호문 C

- 1: $X_0 \leftarrow P$
 - 2: **for** $i = 0$ to $(Nr - 1)$ **do**
 - 3: $X_{i+1} \leftarrow \text{Round}^{enc}(X_i, RK_i^{enc})$
 - 4: **end for**
 - 5: $C \leftarrow X_{Nr}$
-

그림 10 암호화 함수 알고리즘: $C \leftarrow \text{Encrypt}(P, RK_0^{enc}, RK_1^{enc}, \dots, RK_{Nr-1}^{enc})$

[그림 10]의 알고리즘의 $i(0 \leq i \leq (Nr-1))$ 번째 라운드의 라운드 함수 Round^{enc} 은 [그림 11]의

알고리즘과 같이 수행되며 [그림 12]는 암호화 과정의 i번째 라운드 함수를 도식화한 것이다.

입력:	128비트 내부상태 변수 X_i , 192비트 라운드키 RK_i^{enc}
출력:	128비트 내부상태 변수 X_{i+1}
1:	$X_{i+1}[0] \leftarrow ROL_9((X_i[0] \oplus RK_i^{enc}[0]) \oplus (X_i[1] \oplus RK_i^{enc}[1]))$
2:	$X_{i+1}[1] \leftarrow ROR_5((X_i[1] \oplus RK_i^{enc}[2]) \oplus (X_i[2] \oplus RK_i^{enc}[3]))$
3:	$X_{i+1}[2] \leftarrow ROR_3((X_i[2] \oplus RK_i^{enc}[4]) \oplus (X_i[3] \oplus RK_i^{enc}[5]))$
4:	$X_{i+1}[3] \leftarrow X_i[0]$

그림 11 암호화 과정의 i번째 라운드 함수 알고리즘: $X_{i+1} \leftarrow Round^{enc}(X_i, RK_i^{enc})$

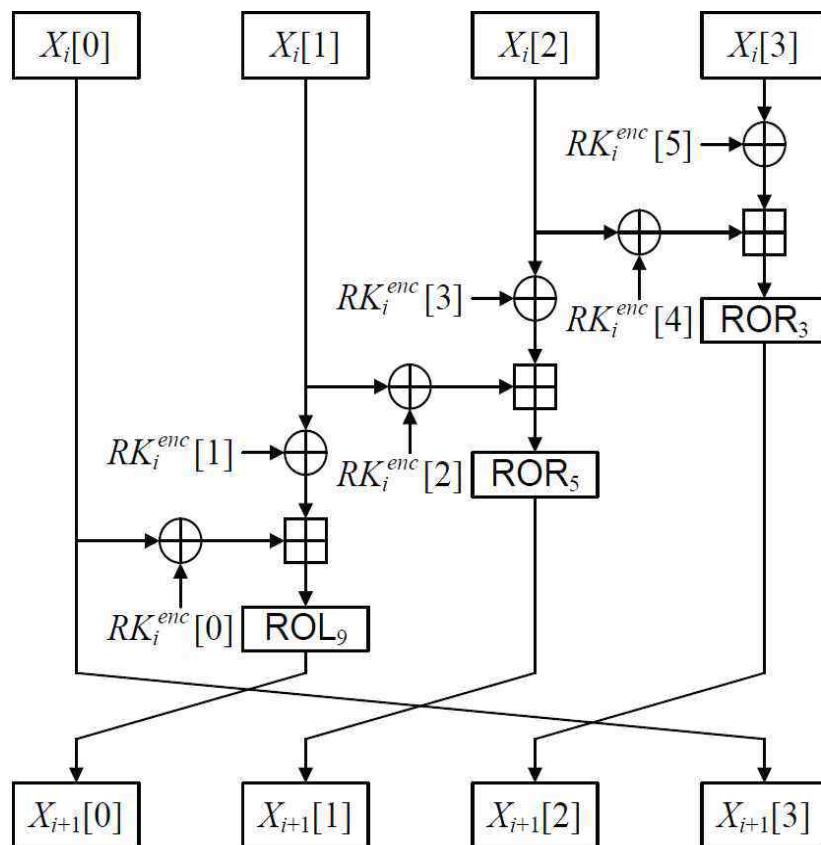


그림 12 암호화 과정의 i번째 라운드 함수($0 \leq i \leq (Nr-1)$)

복호화 과정: LEA의 복호화 함수 Decrypt는 k비트 키 K에 대해 키 스케줄 함수 $KeySchedule_k^{dec}$ 을 수행하여 생성된 Nr개의 192비트 라운드키와 128비트 암호문 $C=(C[0], C[1], \dots, C[15])$ 을 입력받아 [알고리즘 3]을 수행하여 128비트 평문 $P=(P[0], P[1], \dots, P[15])$ 을 출력한다.

$$RK_i^{dec} = (RK_i^{dec}[0], RK_i^{dec}[1], \dots, RK_i^{dec}[5]) \quad (0 \leq i \leq (Nr-1))$$

입력: 128비트 암호문 C, Nr개의 192비트 라운드키 $RK_0^{dec}, RK_1^{dec}, \dots, RK_{Nr-1}^{dec}$

출력: 128비트 평문 P

```

1:  $X_0 \leftarrow C$ 
2: for  $i = 0$  to  $(Nr - 1)$  do
3:    $X_{i+1} \leftarrow \text{Round}^{dec}(X_i, RK_i^{dec})$ 
4: end for
5:  $P \leftarrow X_{Nr}$ 

```

그림 13 복호화 함수 알고리즘 : $P \leftarrow \text{Decrypt}(C, RK_0^{dec}, RK_1^{dec}, \dots, RK_{Nr-1}^{dec})$

[그림 13]의 알고리즘에서 $i(0 \leq i \leq (Nr-1))$ 번째 라운드의 라운드 함수 Round^{dec} 는 [그림 14]의 알고리즘과 같이 수행되며 [그림 15]는 암호화 과정의 i 번째 라운드 함수를 도식화한 것이다.

입력: 128비트 내부상태 변수 X_i , 192비트 라운드키 RK_i^{dec}

출력: 128비트 내부상태 변수 X_{i+1}

```

1:  $X_{i+1}[0] \leftarrow X_i[3]$ 
2:  $X_{i+1}[1] \leftarrow (ROR_9(X_i[0]) \boxminus (X_{i+1}[0] \oplus RK_i^{dec}[0])) \oplus RK_i^{dec}[1]$ 
3:  $X_{i+1}[2] \leftarrow (ROL_5(X_i[1]) \boxminus (X_{i+1}[1] \oplus RK_i^{dec}[2])) \oplus RK_i^{dec}[3]$ 
4:  $X_{i+1}[3] \leftarrow (ROL_3(X_i[2]) \boxminus (X_{i+1}[2] \oplus RK_i^{dec}[4])) \oplus RK_i^{dec}[5]$ 

```

그림 14 복호화 과정의 i 번째 라운드 함수 알고리즘: $X_{i+1} \leftarrow \text{Round}^{dec}(X_i, RK_i^{dec})$

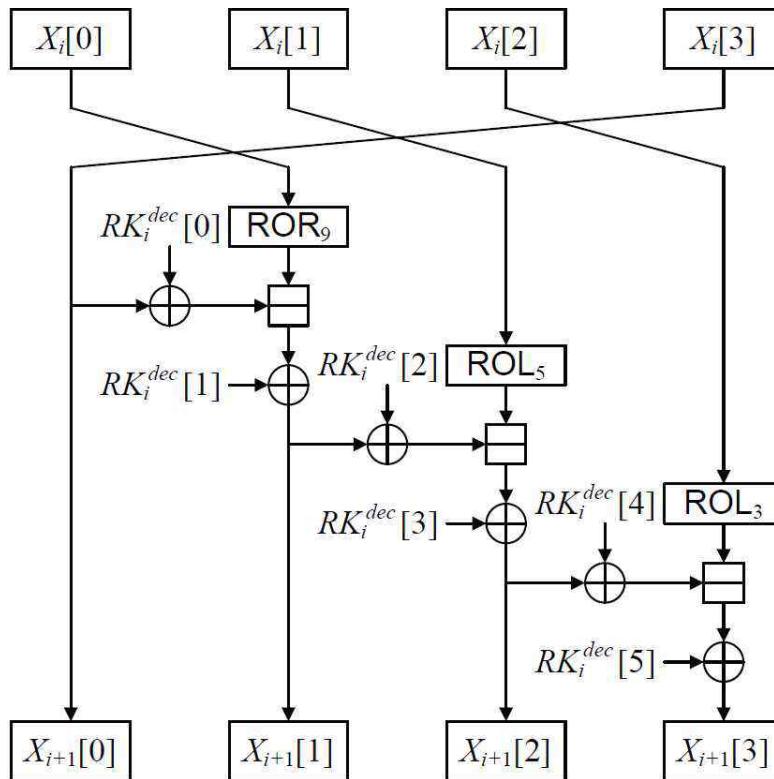


그림 15 복호화 과정의 i 번째 라운드 함수($0 \leq i \leq (Nr-1)$)

2. LEA 경량 암호알고리즘 기반의 안전하고 효율적인 저작권 보호 컨텐츠 암복호화 및 보안인증 기술

사물인터넷(IoT: Internet of Things) 환경에 적합한 경량고속블록암호모듈인 LEA(Lightweight Encryption Algorithm) 기반 경량 암호알고리즘 기반의 안전하고 효율적인 저작권 보호 컨텐츠 암복호화 및 보안인증 기술 개발은 (가) LEA 경량 암호알고리즘을 활용한 대칭키 기반의 저작권 보호 컨텐츠 암복호화 및 보안인증 프로토콜과 (나) LEA 경량 암호알고리즘을 활용한 ECC 비대칭키 기반의 저작권 보호 컨텐츠 암복호화 및 보안인증 프로토콜을 개발하여 활용한다. [11-14]

가. LEA 경량 암호알고리즘을 활용한 대칭키 기반의 저작권 보호 컨텐츠 암복호화 및 보안인증 프로토콜

- [그림 16]과 같이 안전한 전송 환경 구축을 위해 공유 비밀 키 기반으로 연산비용이 적은 LEA(Lightweight Encryption Algorithm) 알고리즘과 안전한 일방향 해쉬(Secure One-way Hash Algorithm) 알고리즘을 사용하여 다양한 보안 공격에 견딜 수 있는 경량 암복호화 및 보안인증 프로토콜을 기반으로 안전한 저작권 보호 컨텐츠 인증을 수행하도록 개발하였다.
- 프로토콜의 동작 과정

아래 [표 4]은 제안된 프로토콜에서 사용되는 시스템 파라미터들을 보여주며, [그림 16]은 제안된 LEA 경량 암호알고리즘을 활용한 대칭키 기반의 상호인증 프로토콜의 동작원리를 보여주고 있다.

표 4 시스템 파라미터

기호	정의
A, B	송신자와 수신자
P	타원곡선암호시스템 기반 베이스 포인트
k_{AB}	송신자 A 와 수신자 B 간에 공유된 비밀키
G	저작권 보호 컨텐츠
t	송신자 A 가 생성한 타임스탬프
$E(), D()$	LEA 경량 암복호화 알고리즘
$h()$	안전한 일방향 해쉬함수
$M_1 M_2$	데이터 M_1 과 M_2 의 연접
sk	공유 비밀 세션키(session key)
G	저작권 보호 컨텐츠 (일반/가역/제로스테가노그레피 등 정보은닉 기법이 적용된 컨텐츠)

(1) 저작권 보호 컨텐츠 암호화(Encryption) 과정

송신자 A 가 수신자 B 에게 저작권 보호 컨텐츠 G 를 안전하게 송신하기 원할 때 아래의 암호화 과정을 수행한다.

- ① 송신할 저작권 보호 컨텐츠 G 를 선택하여 가져온다.
- ② 재전송 공격 방어를 위해 타임스탬프 t 를 선택한다.
- ③ 공유 비밀키 k_{AB} 를 이용하여 세션키 $sk = h(t|k_{AB})$ 를 계산한다.
- ④ 저작권 보호 컨텐츠 G 를 sk 로 LEA 경량 암호알고리즘을 활용하여 암호화하여 암호화된 저작권 보호 컨텐츠 C 를 생성한다.

$$C = E_{sk}(G)$$

- ⑤ 무결성 검증을 위한 메시지 인증 코드(MAC) M 을 계산한다.

$$M = h(sk|G)$$

위 암호화 과정을 거친 후 송신자 A 는 암호화된 저작권 보호 컨텐츠 C 를 타임스탬프 t 및 MAC값 M 으로 구성된 암호문 $(C|M|t)$ 를 수신자 B 에게 전송한다.

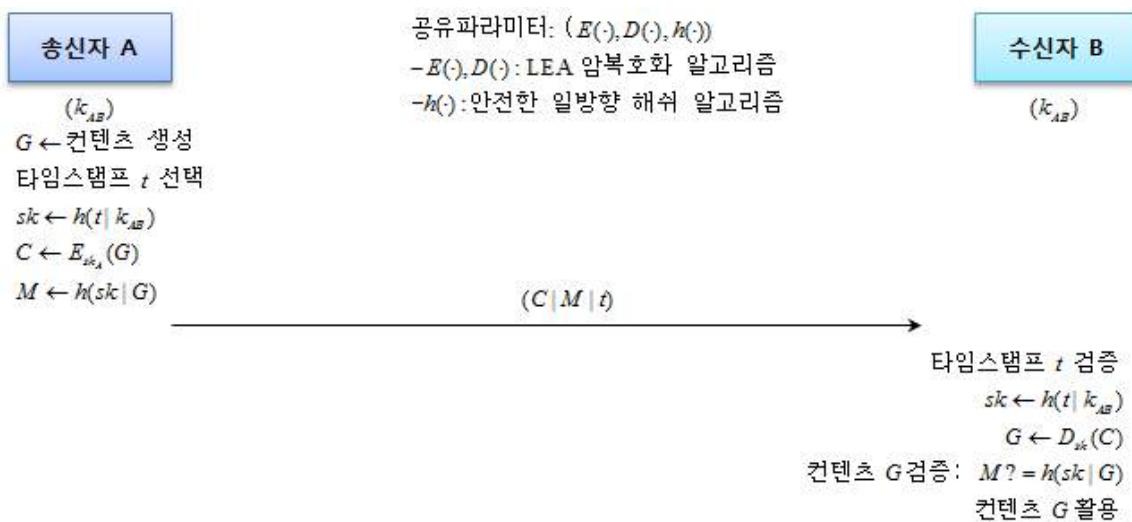


그림 16 제안된 LEA 경량 암호알고리즘을 활용한 대칭키 기반의 저작권 보호 컨텐츠 암복호화 및 보안인증 프로토콜

(2) 암호화된 저작권 보호 컨텐츠 복호화(Decryption) 과정

송신자 A 로부터 암호문 $(C|M|t)$ 를 수신한 수신자 B 는 원본 저작권 보호 컨텐츠 G 를 복원하기 위해 아래의 복호화 과정을 수행한다.

- ① 재전송 공격 방어를 위해 타임스탬프 t 의 유효성을 검증한다. 만약 유효하지 않은 t 인 경우 통신을 중단한다.
- ② 공유 비밀키 k_{AB} 를 이용하여 세션키 $sk = h(t|k_{AB})$ 를 계산한다.
- ③ 암호화된 저작권 보호 컨텐츠 C 를 sk 로 복호화하여 원본 저작권 보호 컨텐츠 G 를 복원한다.

$$G = D_{sk}(C)$$

- ④ 복원된 저작권 보호 컨텐츠 G 와 세션키 sk 를 이용하여 메시지 인증 코드(MAC) $h(sk|G)$ 를 계산한 후 수신한 M 과 동일한지를 검증한다. 만약 동일한 MAC으로 판별되면 수신자 B 는 송신자 A 가 보낸 저작권 보호 컨텐츠 G 을 인증하여 활용

하게 된다. 하지만 만약 두 MAC 값이 동일하지 않으면 수신자 B 는 해당 저작권 보호 컨텐츠가 위조 또는 조작 된 것으로 판단하여 활용하지 않는다.

[그림 17]는 제안된 LEA 경량 암호알고리즘을 활용한 대칭키 기반의 저작권 보호 컨텐츠 암복호화 및 보안인증 프로토콜을 적용한 저작권 보호 컨텐츠 암복호화 및 보안인증 기술 시뮬레이션 결과를 보여준다.

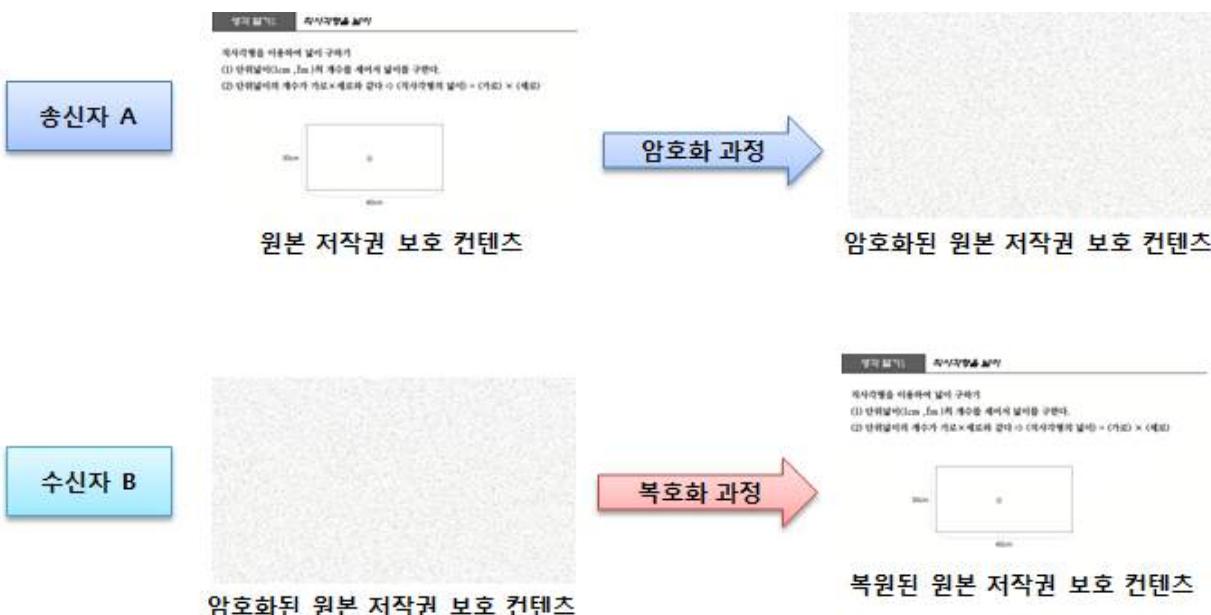


그림 17 제안된 LEA 경량 암호알고리즘을 활용한 대칭키 기반의 저작권 보호 컨텐츠 암복호화 및 보안인증 프로토콜을 적용한 저작권 보호 컨텐츠 암복호화 및 보안인증 기술 시뮬레이션 결과

나. LEA 경량 암호알고리즘을 활용한 ECC 비대칭키 기반의 저작권 보호 컨텐츠 암복호화 및 보안인증 프로토콜

- 타원곡선 암호시스템(Elliptic Curve Cryptography: ECC)은 RSA 암호시스템과 비교하여 적은 키 사이즈로 동일한 보안성을 제공할 수 있다. [그림 18]와 같이 안전한 전송 환경 구축을 위해 타원곡선암호시스템(ECC)을 활용한 비대칭키 기반으로 연산비용이 적은 LEA(Lightweight Encryption Algorithm) 알고리즘과 안전한 일방향 해쉬(Secure One-way Hash Algorithm) 알고리즘을 사용하여 다양한 보안 공격에 견딜 수 있는 경량 암복호화 및 보안인증 프로토콜을 기반으로 안전한 저작권 보호 컨텐츠 인증을 수행하도록 개발하였다. 제안한 기법에서 송신자와 수신자는 ECC 기반의 세션키(session key)를 생성하여 안전하고 효율적으로 저작권 보호 컨텐츠를 암호화 및 복호화 그리고 인증(authentication)을 수행하며, 타임스탬프(timestamp) 기술을 적용하여 재전송 공격(replay attack)을 방지하도록 설계하였다. 결론적으로 제안된 프로토콜은 실시간으로 빠른 저작권 보호 컨텐츠 암호화 및 복호화가 가능함으로 사물인

터넷 환경에서 실용적으로 사용되어 질 수 있다.

- 프로토콜의 동작 과정

제안한 프로토콜을 수행하기 전에 시스템 초기화 단계에서 키 생성 센터(key generation center)는 먼저 ECC기반 베이스 포인트(base point)인 P 를 선택한 후 각 통신 참가자 i 를 위한 개인키 및 공개키 쌍인 x_i 와 $P_i = x_i P$ 를 계산하여 발급해 준다. 아래 표 5는 제안된 프로토콜에서 사용되는 시스템 파라미터들을 보여주며, [그림 18]는 제안된 LEA 경량 암호알고리즘을 활용한 ECC 비대칭키 기반의 상호인증 프로토콜의 동작원리를 보여주고 있다.

표 5 시스템 파라미터

기호	정의
A, B	송신자와 수신자
P	타원곡선암호시스템 기반 베이스 포인트
x_A, P_A	송신자 A 의 개인키와 공개키($P_A = x_A P$)
x_B, P_B	수신자 B 의 개인키와 공개키($P_B = x_B P$)
G	저작권 보호 컨텐츠
t	송신자 A 가 생성한 타임스탬프
$E(), D()$	LEA 경량 암복호화 알고리즘
$h()$	안전한 일방향 해쉬 함수
$M_1 M_2$	데이터 M_1 과 M_2 의 연접
sk	공유 비밀 세션키(session key)
G	저작권 보호 컨텐츠 (일반/가역/제로스테가노그래피 등 정보온닉 기법이 적용된 컨텐츠)

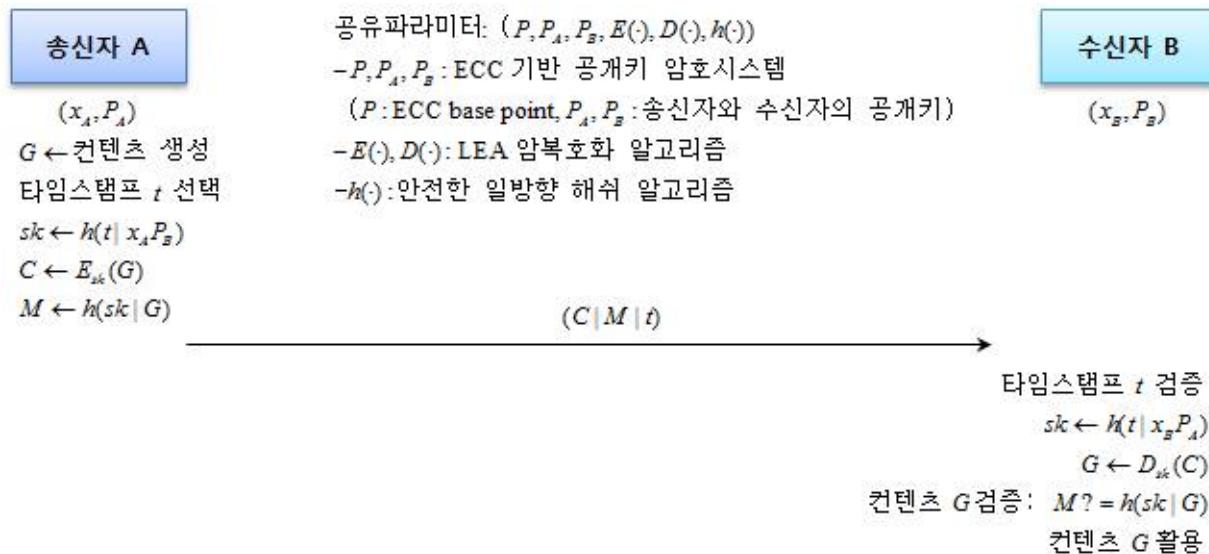


그림 18 제안된 LEA 경량 암호알고리즘을 활용한 ECC 비대칭키 기반의 저작권 보호 컨텐츠 암복호화 및 보안인증 프로토콜

(1) 저작권 보호 컨텐츠 암호화(Encryption) 과정

송신자 A 가 수신자 B 에게 저작권 보호 컨텐츠 G 를 안전하게 송신하기 원할 때 아래의 암호화 과정을 수행한다.

- ① 송신할 저작권 보호 컨텐츠 G 를 선택하여 가져온다.
- ② 재전송 공격 방어를 위해 타임스탬프 t 를 선택한다.
- ③ 수신자 B 의 공개키 P_B 와 자신의 비밀키 x_A 를 이용하여 세션키 $sk = h(t|x_A P_B)$ 를 계산한다.
- ④ 저작권 보호 컨텐츠 G 를 sk 로 LEA 경량 암호알고리즘을 활용하여 암호화하여 암호화된 저작권 보호 컨텐츠 C 를 생성한다.

$$C = E_{sk}(G)$$

- ⑤ 무결성 검증을 위한 메시지 인증 코드(MAC) M 을 계산한다.

$$M = h(sk|G)$$

위 암호화 과정을 거친 후 송신자 A 는 암호화된 저작권 보호 컨텐츠 C 를 타임스탬프 t 및 MAC값 M 으로 구성된 암호문 ($C|M|t$)를 수신자 B 에게 전송한다.

(2) 암호화된 저작권 보호 컨텐츠 복호화(Decryption) 과정

송신자 A 로부터 암호문 ($C|M|t$)를 수신한 수신자 B 는 원본 저작권 보호 컨텐츠 G 를 복원하기 위해 아래의 복호화 과정을 수행한다.

- ① 재전송 공격 방어를 위해 타임스탬프 t 의 유효성을 검증한다. 만약 유효하지 않은 t 인 경우 통신을 중단한다.
- ② 수신자 A 의 공개키 P_A 와 자신의 비밀키 x_B 를 이용하여 세션키 $sk = h(t|x_B P_A)$ 를 계산한다.
- ③ 암호화된 저작권 보호 컨텐츠 C 를 sk 로 복호화하여 원본 저작권 보호 컨텐츠 G 를 복원한다.

$$G = D_{sk}(C)$$

- ④ 복원된 저작권 보호 컨텐츠 G 와 세션키 sk 를 이용하여 메시지 인증 코드(MAC) $h(sk|G)$ 를 계산한 후 수신한 M 과 동일한지를 검증한다. 만약 동일한 MAC으로 판별되면 수신자 B 는 송신자 A 가 보낸 저작권 보호 컨텐츠 G 를 인증하여 활용하게 된다. 하지만 만약 두 MAC 값이 동일하지 않으면 수신자 B 는 해당 저작권 보호 컨텐츠가 위조 또는 조작 된 것으로 판단하여 활용하지 않는다.

- 안전성과 효율성 분석: 제안한 프로토콜에서 공격자가 송신자 A 로 위장하기 위해서는 합법적인 송신 메시지 ($C|M|t$)를 생성할 수 있어야 한다. 하지만 송신자 또는 수신자의 비밀키 x_A 또는 x_B 를 알지 못하는 공격자는 세션키 $sk = h(t|x_A x_B P)$ 를 구할 수 없음으로 합법적인 송신 메시지 ($C|M|t$)를 생성할 수 없다. 결론적으로 제안한 프로토콜은 위장, 위조, 중간자 공격 등에 안전하다. 제안한 프로토콜에서 송신자 A 는 재전송 공격 방어를 위해 타임스탬프 t 를 생성하여 전송할 뿐만 아니라 세션키 생성에도 활용한다. 수신자 B 는 복호화 과정을 수행하기 전에 먼저 타임스탬프 t 의 유효

성 검증을 수행하여 재전송 공격 여부를 판단한다. 결론적으로 제안한 프로토콜은 재전송 공격에 안전하다. 제안한 프로토콜에서 송신자 A와 수신자 B는 각각 1번의 ECC 곱셈 연산과 2번의 해쉬 연산을 수행한다. ECC의 연산 효율성을 기반으로 제안한 프로토콜은 안전성과 효율성 모두 제공할 수 있음을 알 수 있다.

- [그림 19]은 제안된 LEA 경량 암호알고리즘을 활용한 ECC 비대칭키 기반의 저작권 보호 컨텐츠 암복호화 및 보안인증 프로토콜을 적용한 저작권 보호 컨텐츠 암복호화 및 보안인증 기술 시뮬레이션 결과를 보여준다.

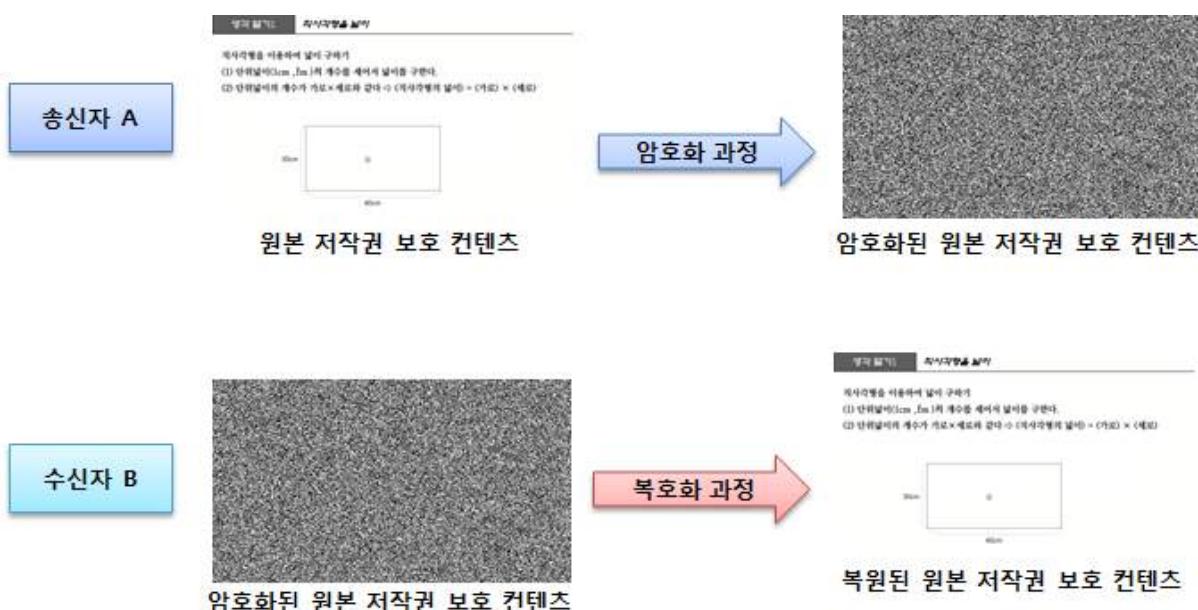


그림 19 제안된 LEA 경량 암호알고리즘을 활용한 ECC 비대칭키 기반의 저작권 보호 컨텐츠 암복호화 및 보안인증 프로토콜을 적용한 저작권 보호 컨텐츠 암복호화 및 보안인증 기술 시뮬레이션 결과

3. LEA 경량암호 기반 콘텐츠 암복호화 프로그램

국가보안기술연구소에서 개발한 128비트의 블록 암호화 알고리즘 LEA는 국제표준알고리즘인 AES 대비 1.5~2배의 속도 향상이 있으면서 AES를 개발한 벨기에 루汶대학 COSIC 연구소로부터 안전성검증을 받은 뛰어난 암호 알고리즘으로 기존 암호 알고리즘 대비 동일 레벨의 보안을 제공하면서 알고리즘을 단순화 함으로 대용량의 클라우드 환경에 적합한 암호화 기법이다.

가. LEA 경량암호 기반 콘텐츠 암호화 프로그램

- 구현된 [그림 20]의 LEA 경량암호 기반 콘텐츠 암호화 프로그램은 LEA 경량암호를 기반으로 이미지를 불러와 이미지의 이름, 크기, 해상도, 채널의 정보와 함께 이미지를 보여준다. 암호화된 파일이 저장되어질 폴더를 선택한 후 16진수의 8자리 키를 입력한 후 암호화 버튼을 클릭하면 이미지에 대한 LEA 암호화가 진행되어 암호화된 이미지 파일을 얻을 수 있다.

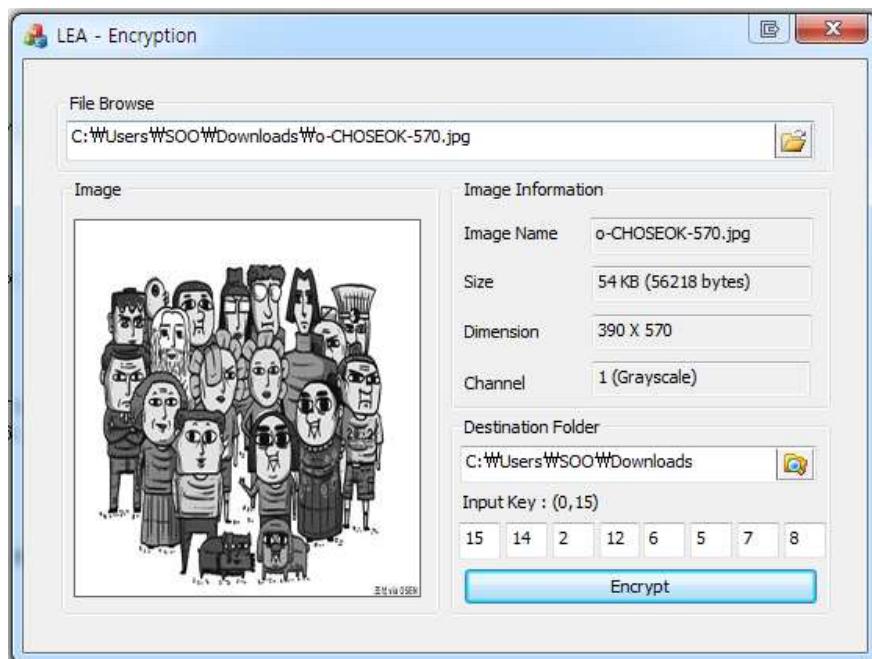


그림 20 LEA 경량암호 기반 콘텐츠 암호화 프로그램

나. LEA 경량암호 기반 콘텐츠 복호화 프로그램

- 구현된 [그림 21]의 LEA 경량암호 기반 콘텐츠 복호화 프로그램은 LEA 경량암호를 기반으로 암호화된 이미지를 불러오고 복호화된 이미지가 저장될 경로를 지정한 후, 암호화키와 동일한 키를 복호화 키로 16진수의 8자리를 입력한 후 복호화 버튼을 클릭하면 LEA 복호화가 진행되어 복호화된 이미지 파일을 얻을 수 있다. 또한, 해당 이미지의 이미지의 이름, 크기, 해상도, 채널의 정보와 함께 복호화된 이미지를 보여준다.

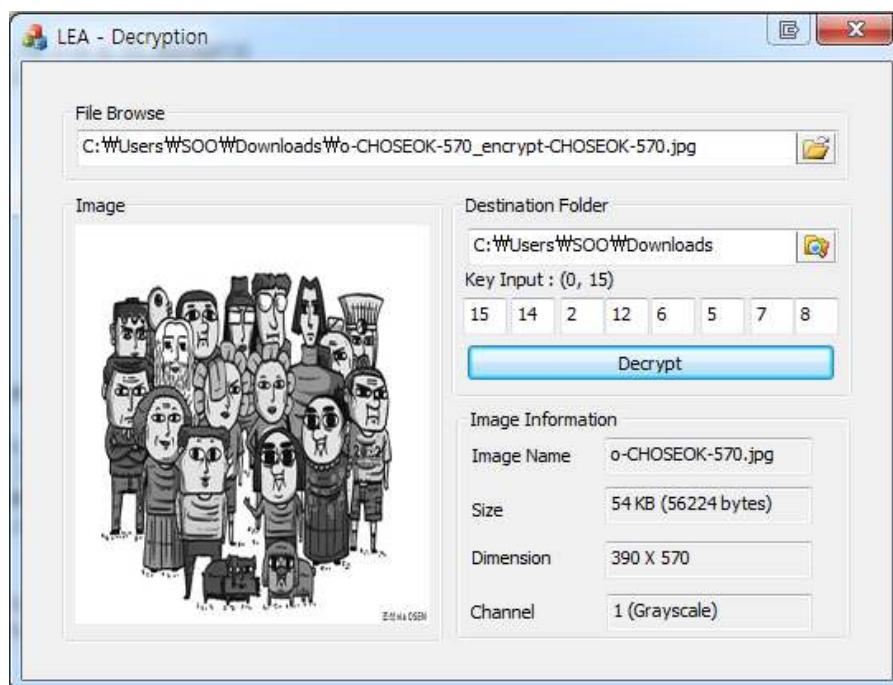


그림 21 LEA 경량암호 기반 콘텐츠 복호화 프로그램

4. 클라우드 기반 경량 암호 콘텐츠 인증 서비스 구현

[그림 22]는 클라우드 기반 경량암호 콘텐츠 인증서비스의 개요이다. 다수의 사용자들이 대용량의 콘텐츠를 사용하는 클라우드 환경에서 효율적인 콘텐츠 인증을 위한 내용을 보여준다. 클라우드 환경에서는 개인콘텐츠 제작자 뿐만 아니라 기관에서 다수의 대용량 콘텐츠를 한번에 또는 분할적으로 업로드 및 다운로드를 하게 된다. 이러한 환경에서 효율적으로 콘텐츠를 인증하기 위해서는 기존 암호알고리즘 대비 1.5~2배의 속도향상된 경량암호를 이용하여 효율적인 콘텐츠 인증을 해야한다.



그림 22 클라우드 기반 효율적인 콘텐츠를 인증을 위한 서비스 개요

다음의 [그림23]은 다수의 사용자와 대량의 콘텐츠를 사용하는 클라우드 환경에서 콘텐츠에 대한 보안을 제공하기 위한 저작권 보호 프로그램의 동작 내용을 나타낸다. 클라우드 환경에서 콘텐츠가 저장되어지는 스토리지 서버에서 콘텐츠가 업로드 되는 것이 동작되면 저작권 보호 클라우드 서버에서 이를 감지하고 저작권 보호 모듈이 동작된다. LEA 경량암호 모듈과 고속의 병렬 처리 모듈이 동작되어 다수의 고용량 콘텐츠에 효율적으로 보안이 제공된다.



그림 23 LEA 경량암호 모듈과 병렬처리 모듈로 구성된 저작권 보호 프로그램

제2절 특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술 개발 내용

[그림 24]는 기존 공용특징정보사업에서 사용하는 특징 기반 DNA 필터링 기법을 응용하여 제로정보은닉 기반 콘텐츠 저작권 보호기술 개발 목표를 보여준다. 기존 기술적 조치를 위한 필터링 기법과 저작권 보호를 위한 불법콘텐츠 유포와 배포경로를 추적하는 워터마크와 포렌식 마크 기술을 별개로 취급하여 절차적으로 복잡성을 가지게 된다. 또한 워터마크를 콘텐츠에 적용하는데 있어 콘텐츠 원본이 훼손되는 문제점이 발생하게 된다.

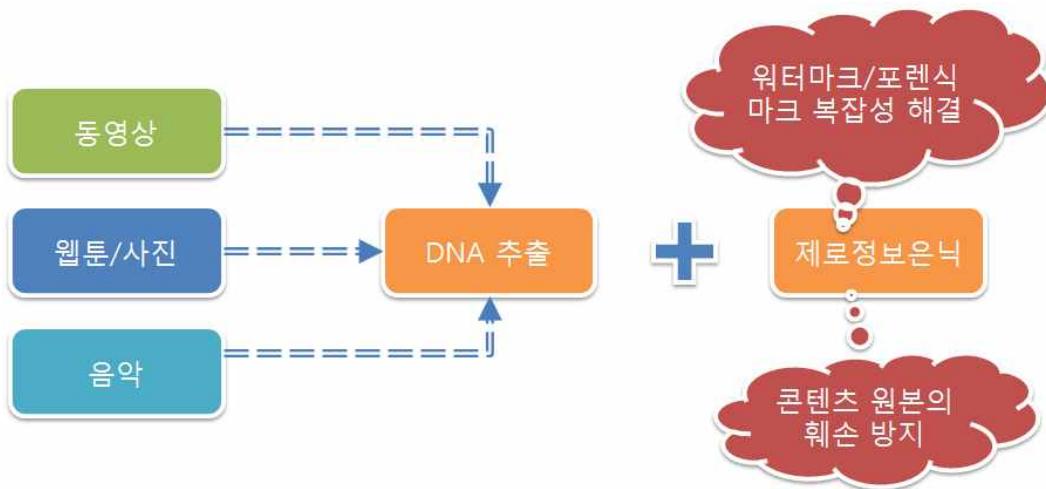


그림 24 특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권
보호기술 개발 목표

이러한 문제점을 해결하기 위해 본 과제에서는 콘텐츠 원본이 훼손되지 않으면서 저작권 보호 정보를 은닉할 수 있는 제로정보은닉 기반의 스테가노그래피 기법과 DNA 필터링 기법을 응용한 저작권 보호 기법을 개발하고 있다. 특징기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술로 저작물인식조치, 검색제한조치, 송신제한조치 및 경고문구 발송 등의 기술적 조치와 함께 저작권 보호 정보를 은닉함으로 콘텐츠의 불법 유포자와 배포 경로를 추적할 수 있는 저작권 보호를 제공해줄 수 있는 기술을 개발하고 있다.

1. 제로정보은닉 기반 위변조 방지 및 저작권 정보 삽입 프로그램

[그림 25]는 본 과제에서 사용하는 카오스 기반의 제로스테가노그래피 기법의 키 생성 절차이다. 이미지 I 로부터 특징점 \bar{I} 를 추출하고, 아래의 수식을 이용하여 키 K 를 생성한다.

$$K_i = P_i \oplus \bar{I}_i \oplus C_i$$

여기서 C 는 카오스 기반의 Logistic map을 이용하여 생성되는 시퀀스이다. 키 K 는 XOR 연산을 이용하여 생성하기 때문에 고속의 연산이 가능함으로 고속 저작권 정보 삽입이 가능

하다. 본 과제에서 제안하는 제로정보은닉 기반의 콘텐츠저작권 보호기술에서는 동영상, 웹툰/사진, 음악파일에서 특징점을 추출하고 이를 통해서 저작권 보호 키를 생성하여 콘텐츠의 훼손 없이 저작권 정보를 삽입할 수 있다.

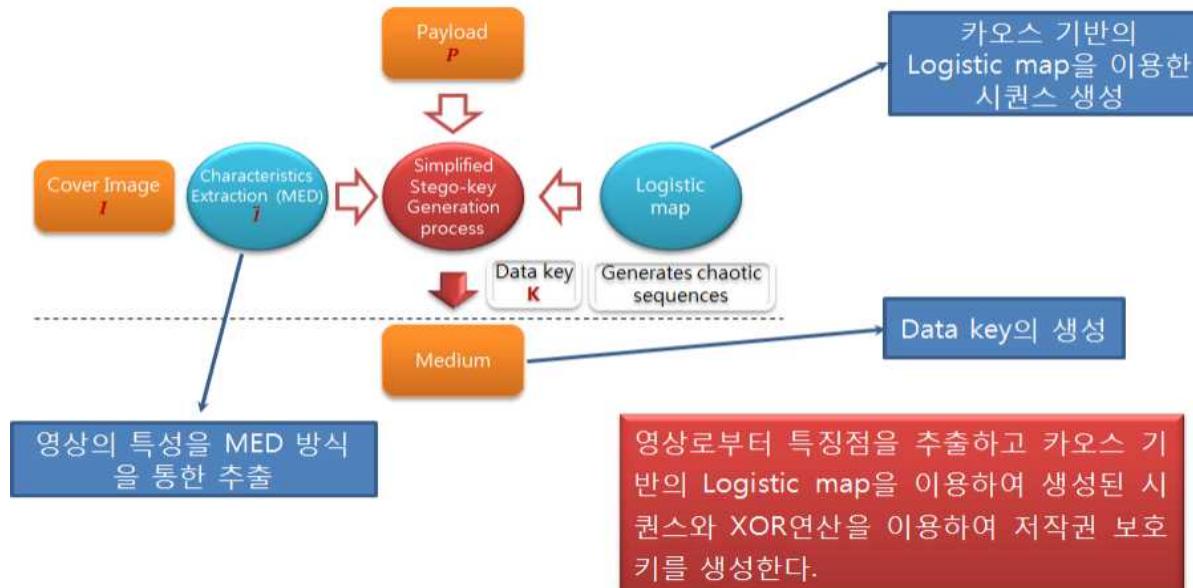


그림 25 카오스 기반의 제로스테가노그래피 기법의 키 생성 및 저작권 정보 삽입 절차

구현된 [그림 26]의 제로정보은닉기반 위변조 방지 및 저작권 정보 삽입프로그램으로 저작권 정보를 삽입할 이미지를 불러온 후 특징정보를 추출한다. 추출된 특징정보와 바이너리 이미지를 이용하여 저작권 정보를 삽입하는 프로그램이다.



그림 26 제로정보은닉 기반 위변조 방지 및 저작권 정보 삽입 프로그램

2. 제로정보은닉 기반 위변조 방지 및 저작권 정보 추출 프로그램

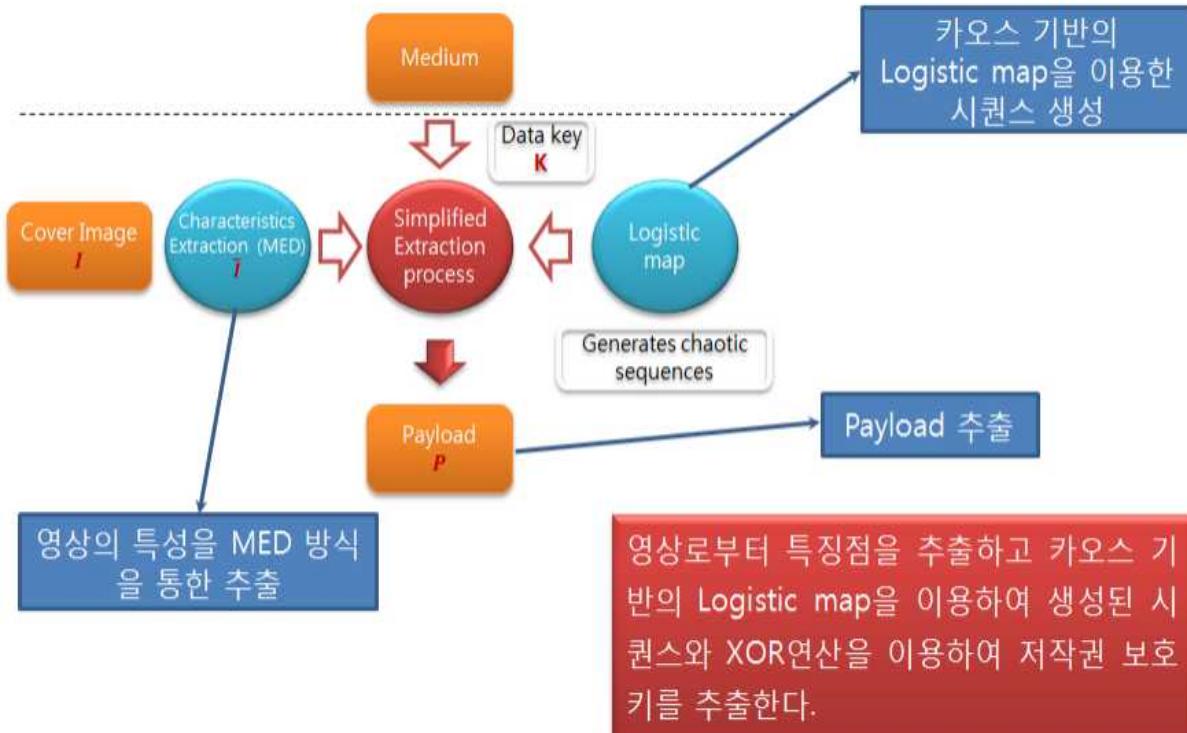


그림 27 카오스 기반의 제로스테가노그래피 기법의 키 추출 및 저작권 정보 추출 절차

[그림 27]은 본 과제에서 사용하는 카오스 기반의 제로스테가노그래피 기법의 정보 추출 절차이다. 이미지 I 로부터 특징점 \bar{I} 를 추출하고, 아래의 수식을 이용하여 원본 이미지 P 를 추출한다.

$$P_i = K_i \oplus \bar{I}_i \oplus C_i$$

여기서 C 는 카오스 기반의 Logistic map을 이용하여 생성되는 시퀀스로 키생성 과정에서 사용된 동일한 파라메터를 이용하여 생성되어진다. 키 K 는 XOR 연산을 이용하여 생성하기 때문에 고속의 연산이 가능함으로 고속 저작권 정보 추출이 가능하다.

구현된 [그림 28~그림 30]의 제로정보은닉기반 위변조 방지 및 저작권 정보 추출프로그램으로 저작권 정보가 삽입된 이미지를 불러온 후 특징정보를 추출한다. 추출된 특징정보와 저작권정보 삽입과정에서 생성된 키를 이용하여 저작권 정보를 추출하는 프로그램이다.

국가연구개발 보고서원문 성과물 전담기관인 한국과학기술정보연구원에서 가공·서비스 하는
연구보고서는 동의 없이 상업적 용도로 사용할 수 없습니다.

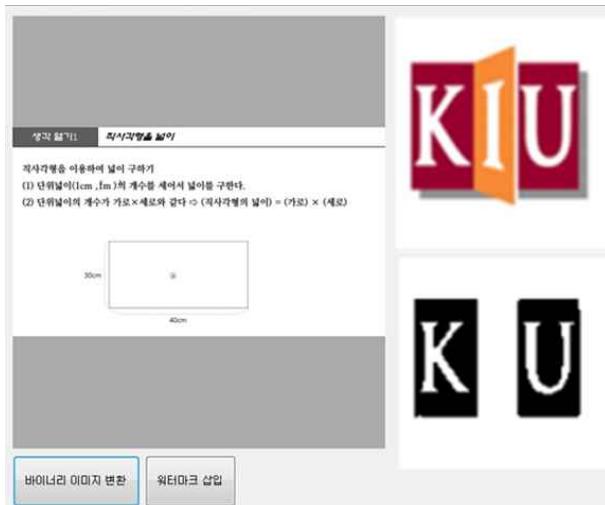


그림 28 바이너리 이미지 변환 및 저작권
정보 은닉 처리 과정

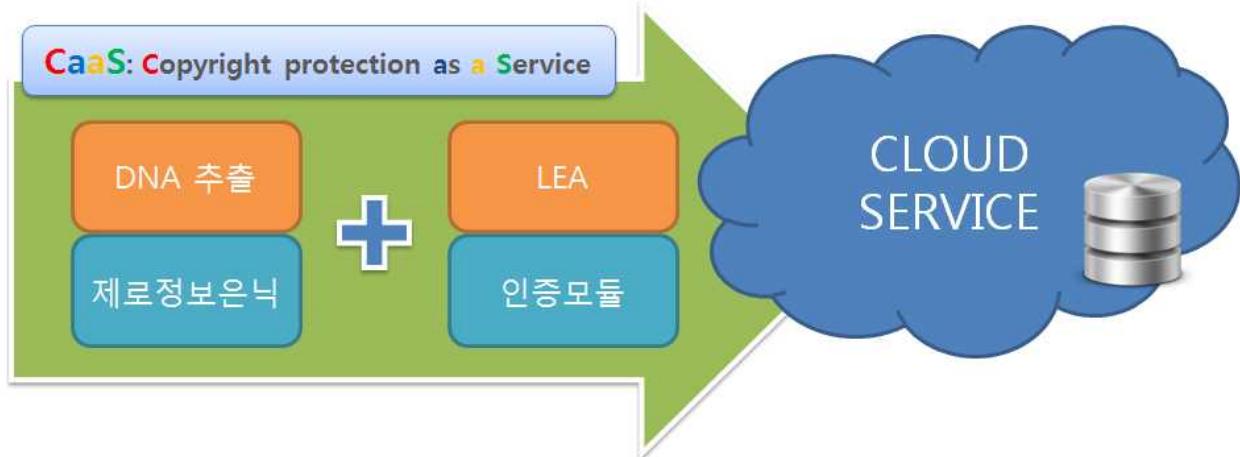


그림 29 저작권 정보 추출 및 원본 영상
복원 처리 과정



그림 30 제로정보은닉 기반 위변조 방지 및 저작권 정보 추출 프로그램

제3절 클라우드 기반의 웹툰/이미지 저작권보호서비스 개발 내용



클라우드 환경에서 콘텐츠 보호를 위해 경량암호 모듈인 LEA(Lightweight Encryption Algorithm)를 이용한 ① 경량 암호 기반 콘텐츠 인증 기술과 개발한 특징점(DNA) 기반 필터링 기술에 제로정보은닉 기반의 스테가노그레피 기법을 접목한 ② 특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술을 기반으로 하여 클라우드 기반의 웹툰/이미지 저작권 보호 시스템 개발을 통해 클라우드환경에서 정지영상에 대한 특징점(DNA) DB를 제공할 뿐만 아니라 저작권보호 및 안전한 콘텐츠 서비스를 제공을 하는 클라우드 저작권 보호 서비스 (CaaS Copyright protection as a Service)를 개발 목표로한다.

그림 31 클라우드 기반의 웹툰/이미지 저작권 보호 서비스 (CaaS: Copyright protection as a Service) 개발 목표

[그림 31]는 웹툰/이미지를 제작하는 개인 또는 영세기업의 콘텐츠에 대한 저작권 보호를 위해 클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS) 개발 목표를 보여준다.

클라우드 환경에서 콘텐츠 보호를 위해 상기에서 개발한 고속의 경량암호 모듈인 LEA(Lightweight Encryption Algorithm)를 이용한 ① 경량 암호 기반 콘텐츠 인증 기술과 특징 점(DNA) 기반 필터링 기술에 제로정보은닉 기반의 스테가노그레피 기법을 접목하여 ② 특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술을 기반으로 하여 클라우드 기반의 웹툰/이미지 저작권 보호 시스템 개발을 통해 클라우드 환경에서 정지영상에 대한 특징 점(DNA) DB를 제공할 뿐만 아니라 저작권보호 및 안전한 콘텐츠 서비스를 제공을 하는 클라우드 저작권 보호 서비스(CaaS: Copyright protection as a Service)를 개발 완료 하였다.

1. 최종 개발결과물인 클라우드 기반의 웹툰/이미지 저작권 보호 서비스 동작원리

[그림 32]와 같이 개발된 저작권 보호 서비스는 클라우드 환경에서 스토리지를 제공하여 콘텐츠를 안전하게 보관하고 인증된 콘텐츠를 제공하기 위해 LEA 경량암호기반 콘텐츠 인증 기술을 이용한다. 저장된 콘텐츠는 특징 기반 필터링을 이용하여 콘텐츠 DNA를 추출하고 DB로 저장이 되어 저작물인식조치, 검색제한조치, 송신제한조치 및 경고문구 발송 등의 기술적 조치를 할 수 있으며, 특징기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술을 이용하여 저작권 보호 정보를 은닉함으로 콘텐츠의 불법 유포자와 배포 경로를 추

적할 수 있는 저작권 보호를 제공해줄 수 있는 클라우스 서비스 환경에 적합한 고품질 콘텐츠 제공 서비스로 콘텐츠에 대한 저작권 보호 서비스를 제공한다.



그림 32 최종 개발결과물인 클라우드 기반의 웹툰/이미지 저작권 보호 서비스 동작원리

2. 클라우드 기반의 웹툰/이미지 저작권 보호 서비스 구성

[그림 33]은 서버, 스토리지, 모니터로 구성된 CaaS 시제품을 보여준다.



그림 33 클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS) 시제품

국가연구개발 보고서원문 성과물 전담기관인 한국과학기술정보연구원에서 가공·서비스 하는 연구보고서는 동의 없이 상업적 용도로 사용할 수 없습니다.

가. 클라우드 기반의 저작권보호 웹서버 및 웹 사이트

- [그림 34]과 같이 저작권보호 서비스를 위한 클라우드 서버 역할을 수행한다.
- 웹툰 및 이미지에 대한 파일 업로드를 통해서 개인 및 기관별 저작권보호를 제공해 준다.

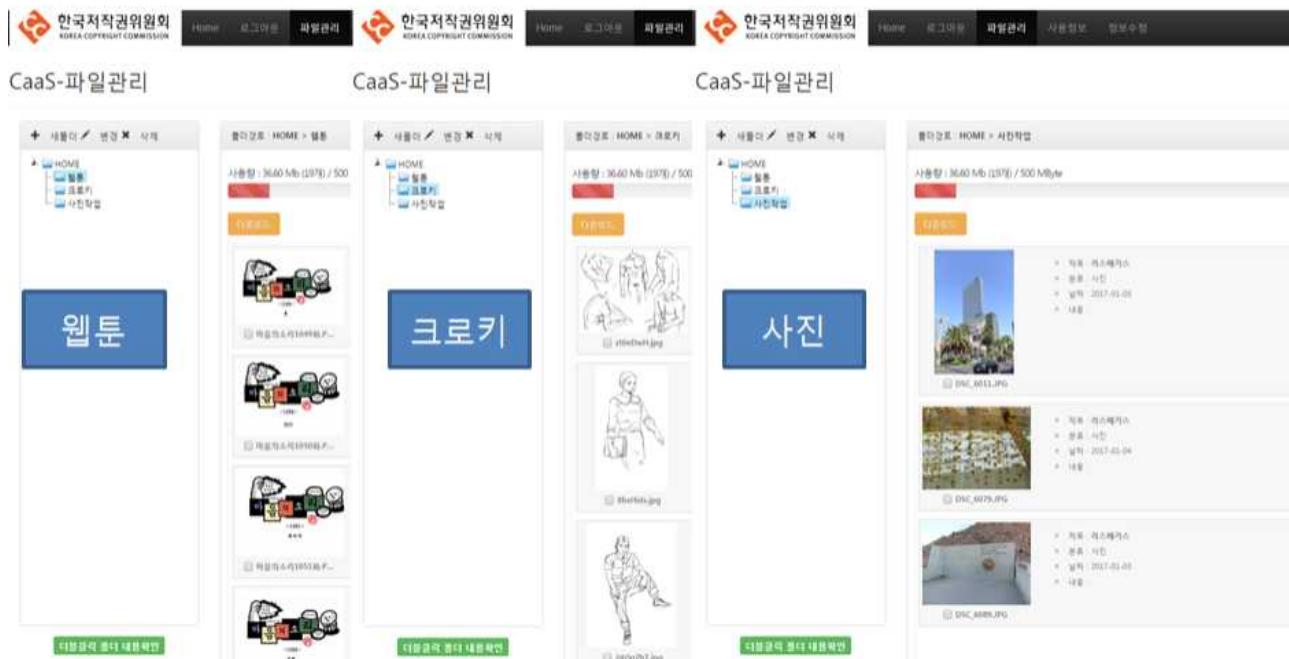


그림 34 클라우드 기반의 저작권 보호 웹 서버

나. 클라우드 기반의 저작권 보호 프로그램

- [그림 35]와 같이 클라우드 서버 스토리지에서 동작하는 프로그램 역할을 수행한다.
- 웹툰/이미지 파일에 대한 업로드가 감지되면 저작권 보호 및 암호화 조치를 한다.



그림 35 클라우드 기반의 저작권 보호 프로그램

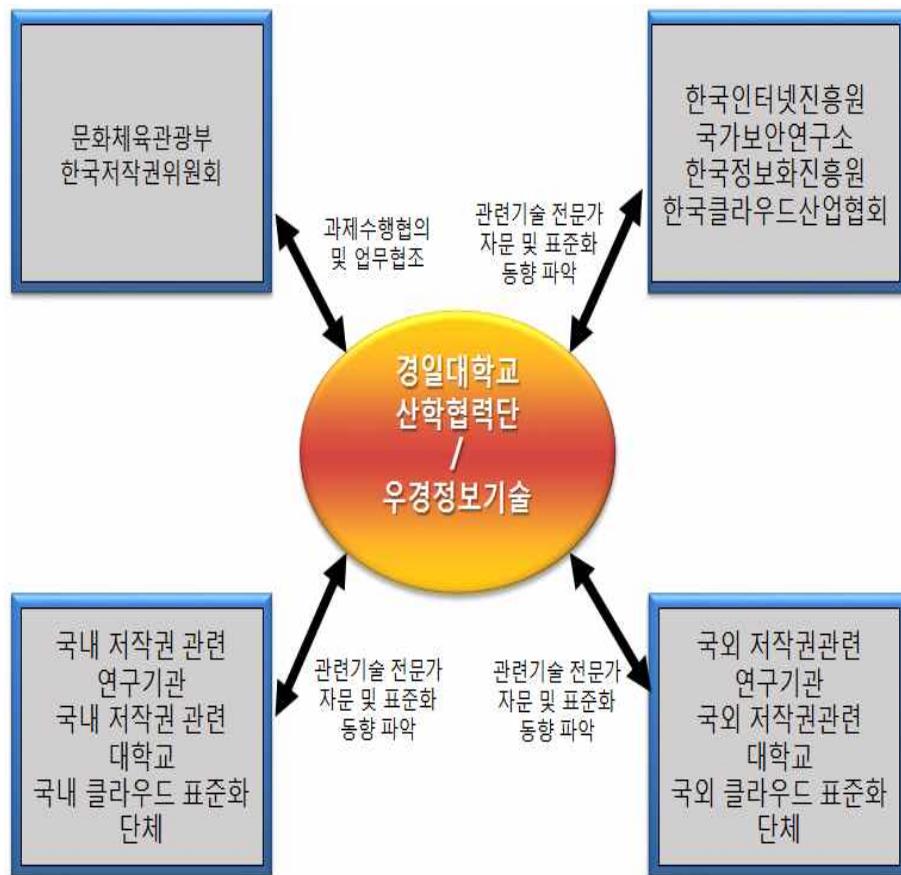
제4절 기술개발 방법

1. 추진일정

1차 년도 (8개월)										
순번	세부 개발 내용	추진일정								기타
		1월	2월	3월	4월	5월	6월	7월	8월	
1	계획 수립 및 자료조사									
2	경량 암호 기반 콘텐츠 인증 기술 개발									
3	클라우드 기반 경량 암호 콘텐츠 인증 서비스 구현									
4	특정 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술 개발									
5	클라우드 기반 저작권 보호기술 서비스 구현									
6	모듈별 통합									
7	클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS) 개발									
8	시제품 제작 및 테스트									

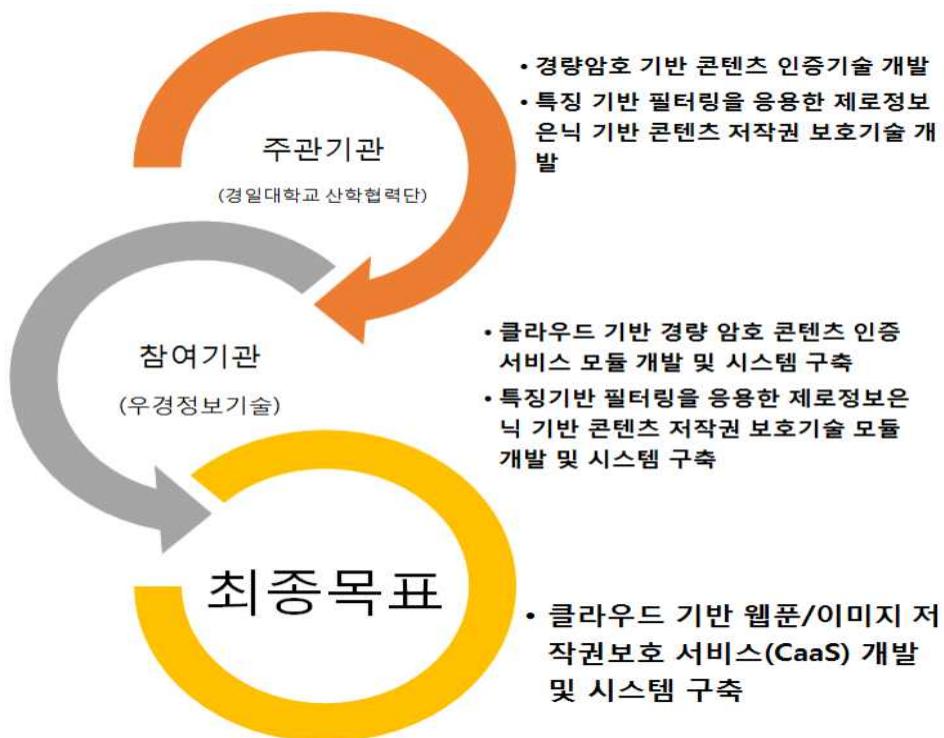
2. 기술개발 추진전략·방법 및 추진체계

가. 기술개발 추진전략·방법

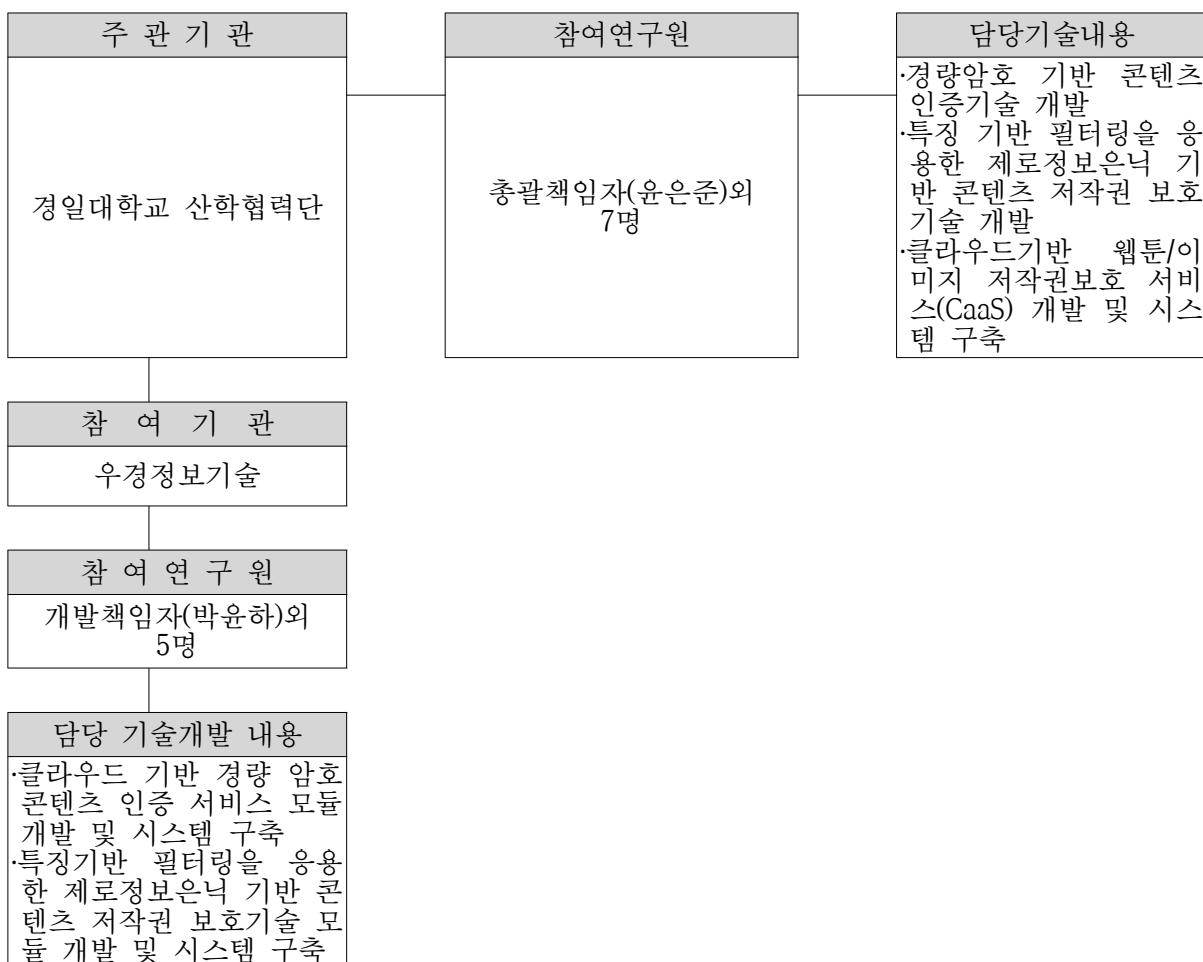


- 본 과제 기술개발팀은 위 그림과 같이 주기적으로 문화체육관광부, 한국저작권위원회의 “저작권 보호 및 이용활성화를 위한 기술 개발” 과제 관리자와 긴밀한 과제 수행협의 및 업무협조를 수행함
- 국내 클라우드, 저작권 보호 기술들에 대한 안전성 검증 지침 등을 제정하고 있는 한국 인터넷 진흥원, 국가보안연구소, 한국정보화진흥원, 한국클라우드산업협회 등의 클라우드 및 저작권 담당자와 과제수행과 관련하여 업무 협조 및 전략 회의등을 통해 원활한 업무 수행 환경 마련
- 본 과제 기술개발팀의 연구 책임자는 클라우드, 저작권에 대한 표준화 통합 포럼내의 워 킹그룹의 활동에 참여하면서 본 과제 수행 결과물을 국내 표준안으로 상정에 적극 노력
- 본 과제 기술개발팀은 클라우드, 저작권 기술에 관련한 국제 표준화 기구의 표준화 활동 동향을 능동적으로 분석
- 본 과제 기술개발팀은 국내 클라우드, 저작권 기술 산학연 단체와의 업무협조로 클라우드 및 저작권 보호 기술에 관한 자문 및 논의

나. 기술개발 추진체계



다. 기술개발팀 편성도



제5절 연구결과 성과물

1. 연구개발 성과물 평가항목의 평가방법 및 개발달성도

평가항목 (주요성능 Spec)	단위	비중(%)	개발달성도	비고
경량 암호 처리 속도	MB/s	20	250MB/s (LEA기반)	
저작권보호 정보 추출률	%	20	100%	
경량 암호 기반 콘텐츠 인증 모듈	SW 모듈	10	개발/동작	GS인증 2건 (향후 CC인증 연계)
특정 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호 모듈	SW 모듈	10	개발/동작	
클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS) 시스템	시제품	30	개발/동작	
FAU/FCO/FCS/FDP/FPR/FTP	인증	10	GS인증2건	

○ 목표 항목의 평가방법 및 결과치

- 경량암호 처리속도: 평가시 연구기관이 선정한 환경에서 LEA 암호 기법을 이용하여 웹툰/
이미지 파일에 대한 암·복호화 테스트를 진행하여 250MB/s 결과를 달성하여 고속
처리 목표를 달성함
- 저작권보호정보 추출율: 제로정보은닉 기법을 이용하여 저작권보호정보를 은닉한 영상에서
평가시 연구기관이 선정한 환경에서 저작권보호정보를 추출하는 테스트를 진행하
여 100% 추출률을 달성함
- 경량 암호 기반 콘텐츠 인증 모듈: 해당 모듈 개발/동작 유무로 검증하여 SW모듈이 인증
기능을 잘 수행함을 검증함
- 특정 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호 모듈: 해당 모듈 개발/
동작 유무로 검증하여 SW모듈이 저작권 보호 기능을 잘 수행함을 검증함
- 클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS) 시스템: 해당 시스템 시제품 개발/
동작 유무로 검증 후 시스템이 저작권 보호 서비스 기능을 잘 수행함을 검증함
- FAU/FCO/FCS/FDP/FPR/FTP: GS/CC인증을 위한 평가항목으로 해당 항목에 대해 중점적으로
테스트를 진행하여 최종 GS인증 2건을 달성함

국가연구개발 보고서원문 성과물 전담기관인 한국과학기술정보연구원에서 가공·서비스 하는
연구보고서는 동의 없이 상업적 용도로 사용할 수 없습니다.

2. 목표와 내용

가. 목표 및 내용

연구개발 목표	연구개발 내용 및 범위	계량화된 개발목표	가시적 결과물
콘텐츠 인증 기술	경량 암호 기반 콘텐츠 인증 기술 개발	SW 등록 2건	프로그램
콘텐츠 저작권 보호기술	특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술 개발	SW 등록 2건	프로그램
클라우드 기반 저작권 보호 서비스	클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS) 개발	특허출원 2건	시제품 (CaaS: Copyright protection as a Service)

나. 기관별 역할

구분	역할
주관기관	<ul style="list-style-type: none"> 경량암호 기반 콘텐츠 인증기술 개발 특징기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술 개발 클라우드기반 웹툰/이미지 저작권보호 서비스(CaaS) 개발 및 시스템 구축
참여기관	<ul style="list-style-type: none"> 클라우드 기반 경량 암호 콘텐츠 인증 서비스 모듈 개발 및 시스템 구축 특징기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술 모듈 개발 및 시스템 구축

3. 수행체계 및 수행계획

가. 수행체계

번호	연구개발 내용	개발기간		책임자
		시작일	종료일	
1	콘텐츠 인증 기술 개발	2016.08.01	2016.11.30	윤은준
1.1	경량 암호 기반 콘텐츠 인증 기술 개발	2016.08.01	2016.10.31	윤은준
1.2	클라우드 기반 콘텐츠 인증 서비스 구현	2016.10.01	2016.11.30	박윤하
2	콘텐츠 저작권 보호기술 개발	2016.09.01	2016.12.31	윤은준
2.1	특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술 개발	2016.09.01	2016.11.30	윤은준
2.2	클라우드 기반 저작권 보호기술 서비스 구현	2016.11.01	2016.12.31	박윤하
3	클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS) 개발	2016.12.01	2017.01.31	윤은준

나. 연구개발 수행계획

하위번호	1.1	
연구개발 명	경량 암호 기반 콘텐츠 인증 기술 개발	
목표일정	2016.08.01~2016.10.31	
목표	경량 암호 기반 콘텐츠 인증 기술 개발	
주요 결과물	S/W	
점검항목	점검기준	점검방법
콘텐츠 암호속도	국내외 표준암호 속도 기준	콘텐츠에 대한 암복호화 속도 측정
인증 정확도	콘텐츠 인증 정확도 측정	콘텐츠 인증 및 사용
하위번호	1.2	
연구개발 명	클라우드 기반 콘텐츠 인증 서비스 구현	
목표일정	2016.10.01~2016.11.30	
목표	클라우드 기반 콘텐츠 인증 서비스 구현	
주요 결과물	S/W 및 클라우드 시스템	
점검항목	점검기준	점검방법
콘텐츠 암호속도	국내외 표준암호 속도 기준	클라우드 환경에서 콘텐츠에 대한 암복호화 속도 측정
인증 정확도	콘텐츠 인증 정확도 측정	클라우드 환경에서 콘텐츠 인증 및 사용
하위번호	2.1	
연구개발 명	특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술 개발	
목표일정	2016.09.01~2016.11.30	
목표	특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술 개발	
주요 결과물	S/W	
점검항목	점검기준	점검방법
저작권보호정보 추출율	국내외 저작권보호정보 추출율 기준	다양한 이미지 포맷을 활용하여 콘텐츠에서 저작권보호정보 추출
특징 기반 필터링	DNA 추출 및 확인	DNA 추출 및 확인

국가연구개발 보고서원문 성과물 전담기관인 한국과학기술정보연구원에서 가공·서비스 하는
연구보고서는 동의 없이 상업적 용도로 사용할 수 없습니다.

하위번호	2.2	
마일스톤 명	클라우드 기반 저작권 보호기술 서비스 구현	
목표일정	2016.11.01~2016.12.31	
목표	클라우드 기반 저작권 보호기술 서비스 구현	
주요 결과물	S/W 및 클라우드 시스템	
점검항목	점검기준	점검방법
저작권보호정보 추출율	국내외 저작권보호정보 추출율 기준	클라우드 환경에서 다양한 이미지 포맷을 활용하여 콘텐츠에서 저작권보호정보 추출
특징 기반 필터링	DNA 추출 및 확인	클라우드 환경에서 DNA 추출 및 확인

4. 연구개발 실적

가. 콘텐츠 인증 기술 개발

1.1 경량 암호 기반 콘텐츠 인증 기술 개발

구 분	당초계획	연구개발 실적
목 표	경량 암호 기반 콘텐츠 인증 기술 개발	<ul style="list-style-type: none"> · S/W 등록 8건 · 특허등록 1건 · SCI(E) 논문 5건
주요 성과물	LEA 경량암호 기반 암호화 모듈	<ul style="list-style-type: none"> · S/W 등록 4건
	LEA 경량암호 기반 복호화 모듈	<ul style="list-style-type: none"> · S/W 등록 4건
	LEA 경량암호기반 콘텐츠 인증 기술	<ul style="list-style-type: none"> · 특허등록 1건 · SCI(E) 논문 5건

1.2 클라우드 기반 콘텐츠 인증 서비스 구현

구 분	당초계획	연구개발 실적
목 표	클라우드 기반 콘텐츠 인증 서비스 구현	<ul style="list-style-type: none"> · GS인증 1건 · 특허출원 1건 · S/W 등록 2건
주요 성과물	클라우드 기반 콘텐츠 암호화 모듈	<ul style="list-style-type: none"> · S/W 등록 1건
	클라우드 기반 콘텐츠 복호화 모듈	<ul style="list-style-type: none"> · S/W 등록 1건
	클라우드 기반 콘텐츠 인증 서비스	<ul style="list-style-type: none"> · 특허출원 1건 · GS인증 1건

나. 콘텐츠 저작권 보호기술 개발

2.1 특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술 개발

구 분	당초계획	연구개발 실적
목 표	특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술 개발	<ul style="list-style-type: none"> · S/W 등록 6건 · 특허출원 4건 · 특허등록 2건 · SCI(E) 논문 2건
주요 성과물	제로정보은닉 기반 저작권보호 기술 개발	<ul style="list-style-type: none"> · S/W 등록 2건 · 특허출원 4건 · 특허등록 2건 · SCI(E) 논문 2건
	제로정보은닉 기반 저작권추출 기술 개발	<ul style="list-style-type: none"> · S/W 등록 2건
	특징 기반 필터링을 이용한 저작권 보호기술 개발	<ul style="list-style-type: none"> · S/W 등록 1건
	특징 기반 필터링을 이용한 저작권 추출기술 개발	<ul style="list-style-type: none"> · S/W 등록 1건

2.2 클라우드 기반 저작권 보호기술 서비스 구현

구 분	당초계획	연구개발 실적
목 표	클라우드 기반 저작권 보호 기술 서비스 구현	<ul style="list-style-type: none"> · GS인증 1건(진행 중) · 특허출원 1건 · S/W 등록 1건
주요 성과물	클라우드 환경에서 특징기반 필터링 및 제로정보은닉 기반 저작권 보호기술 개발	<ul style="list-style-type: none"> · GS인증 1건(진행 중) · 특허출원 1건 · S/W 등록 1건
	클라우드 환경에서 특징기반 필터링 및 제로정보은닉 기반 저작권 추출기술 개발	<ul style="list-style-type: none"> · GS인증 1건(진행 중) · 특허출원 1건 · S/W 등록 1건

다. 클라우드 기반의 웹툰/이미지 저작권 보호서비스(CaaS) 개발

구 분	당초계획	연구개발 실적
목 표	클라우드 기반의 웹툰/이미지 저작권 보호서비스(CaaS) 개발	<ul style="list-style-type: none"> · S/W 등록 2건 · 특허 출원 4건 · 학진등재논문 1건/SCI(E) 논문 2건 · 저작권보호를 위한 웹서버 개발 · 시제품 1건 · 기술이전 1건 · 매출현황 50,000(천 원)
주요 성과물	1. 콘텐츠 인증 기술 개발	<ul style="list-style-type: none"> · S/W 등록 2건 · 특허 출원 4건 · 학진등재논문 1건/SCI(E) 논문 2건 · 저작권보호를 위한 웹서버 개발 · 시제품 1건 · 기술이전 1건 · 매출현황 50,000(천 원)
	2. 콘텐츠 저작권 보호기술 개발	<ul style="list-style-type: none"> · S/W 등록 2건 · 특허 출원 4건 · 학진등재논문 1건/SCI(E) 논문 2건 · 저작권보호를 위한 웹서버 개발 · 시제품 1건 · 기술이전 1건 · 매출현황 50,000(천 원)

5. 연구개발 실적 세부설명

연구개발 1 : 콘텐츠 인증 기술 개발

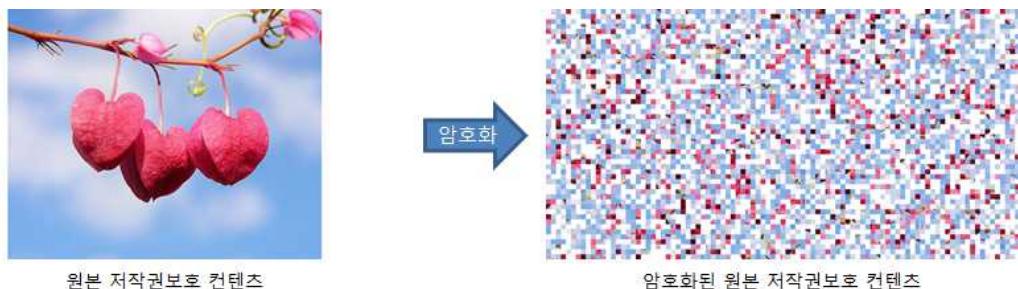
가. 경량 암호 기반 콘텐츠 인증 기술 개발

- o LEA 경량암호 기반 암호화 모듈: 대용량의 컨텐츠를 효율적으로 암복호화하기 위해 LEA 경량암호 알고리즘을 이용한 암호화 모듈 개발 및 모바일 환경에서 사용하기 위한 카오스 알고리즘 기반의 컨텐츠 암호화 모듈의 개발과 일반 PC 환경 뿐만 아니라 모바일, 테블릿 PC의 환경에서도 사용할 수 있도록 경량화된 암호화 모듈 개발을 진행하였다.

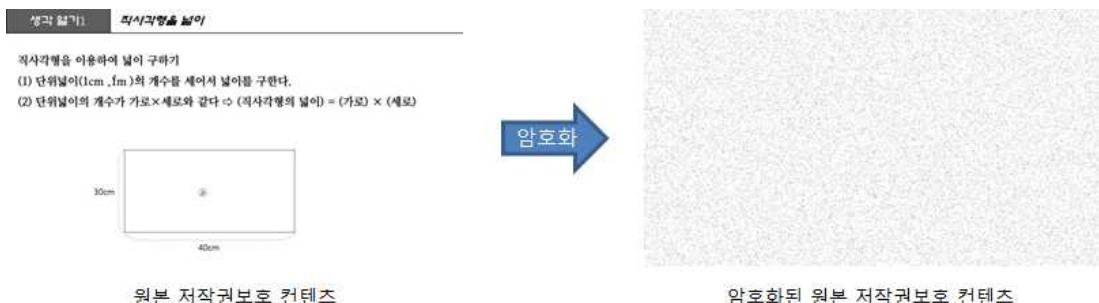
- S/W 등록 4건

순번	등록번호	제호	등록일자	저작자	발명자
1	C-2016-023709	JPEG(제피이지)영상 전용 컨텐츠 암호화 프로그램	2016-10-06	경일대학교 산학협력단	윤은준 외 4
2	C-2016-023713	Chaos(카오스) 알고리즘 기반 컨텐츠 암호화를 위한 서버전용 프로그램	2016-10-06	경일대학교 산학협력단	윤은준 외 4
3	C-2016-024828	안드로이드 환경을 위한 JPEG(제피이지)영상 전용 컨텐츠 암호화 프로그램	2016-10-20	경일대학교 산학협력단	윤은준 외 4
4	C-2016-024832	안드로이드 환경을 위한 Chaos(카오스) 알고리즘 기반 컨텐츠 암호화 프로그램	2016-10-20	경일대학교 산학협력단	윤은준 외 4

① JPEG(제피이지)영상 전용 컨텐츠 암호화 프로그램



② Chaos(카오스) 알고리즘 기반 컨텐츠 암호화를 위한 서버전용 프로그램



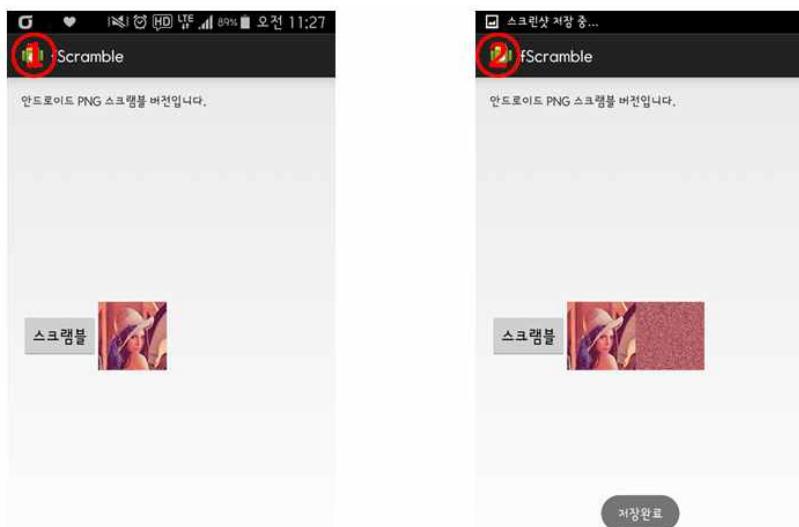
③ 안드로이드 환경을 위한 JPEG(제피이지)영상 전용 컨텐츠 암호화 프로그램



▶ 안드로이드 스크램블 (JPEG)

- ① 원쪽 화면은 안드로이드 스크램블 JPEG 버전 메인화면입니다.
오른쪽 이미지는 원본 이미지를 뜻합니다.
- ② 스크램블 버튼을 누르면 원래 순서를 기억한 뒤 카오틱 맵을 생성하고 그 생성된 값의 인덱스 값을 이용하여 블럭들의 값을 섞어줍니다.
- ③ 오른쪽 화면은 결과 화면입니다. 스크램블된 사진을 이미지뷰로 출력하고, 외장 메모리에 저장을 합니다.

④ 안드로이드 환경을 위한 Chaos(카오스) 알고리즘 기반 컨텐츠 암호화 프로그램



▶ 안드로이드 스크램블 (PNG)

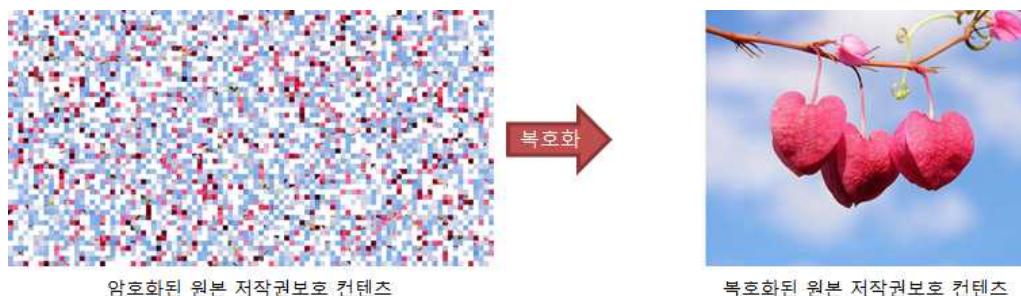
- ① 원쪽 화면은 안드로이드 스크램블 PNG 버전 메인화면입니다.
오른쪽 이미지는 원본 이미지를 뜻합니다.
- ② 스크램블 버튼을 누르면 원래 순서를 기억한 뒤 카오틱 맵을 생성하고 그 생성된 값의 인덱스 값을 이용하여 블럭들의 값을 섞어줍니다.
- ③ 오른쪽 화면은 결과 화면입니다. 스크램블된 사진을 이미지뷰로 출력하고, 외장 메모리에 저장을 합니다.

- o LEA 경량암호 기반 복호화 모듈: 대용량의 컨텐츠를 효율적으로 암복호화하기 위해 LEA 경량암호를 이용한 복호화 모듈 개발 및 모바일 환경에서 사용하기 위한 카오스 알고리즘 기반의 컨텐츠 복호화 모듈의 개발과 일반 PC 환경 뿐만아니라 모바일, 테블릿 PC의 환경에서도 사용할 수 있도록 경량화된 복호화 모듈 개발을 진행하였다.

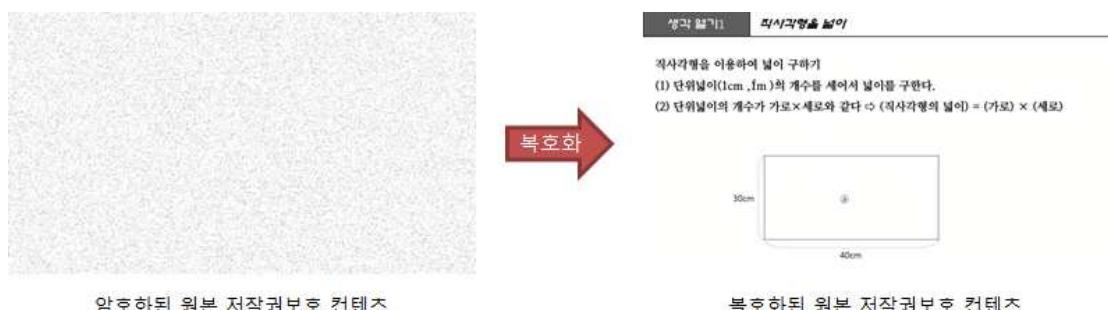
- S/W 등록 4건

순번	등록번호	제호	등록일자	저작자	발명자
1	C-2016-023708	JPEG(제피이지)영상 전용 컨텐츠 복호화 프로그램	2016-10-06	경일대학교 산학협력단	윤은준 외 4
2	C-2016-023712	Chaos(카오스) 알고리즘 기반 컨텐츠 복호화를 위한 서버전용 프로그램	2016-10-06	경일대학교 산학협력단	윤은준 외 4
3	C-2016-024827	안드로이드 환경을 위한 JPEG(제피이지)영상 전용 컨텐츠 복호화 프로그램	2016-10-20	경일대학교 산학협력단	윤은준 외 4
4	C-2016-024831	안드로이드 환경을 위한 Chaos(카오스) 알고리즘 기반 컨텐츠 복호화 프로그램	2016-10-20	경일대학교 산학협력단	윤은준 외 4

① JPEG(제피이지)영상 전용 컨텐츠 복호화 프로그램



② Chaos(카오스) 알고리즘 기반 컨텐츠 복호화를 위한 서버전용 프로그램



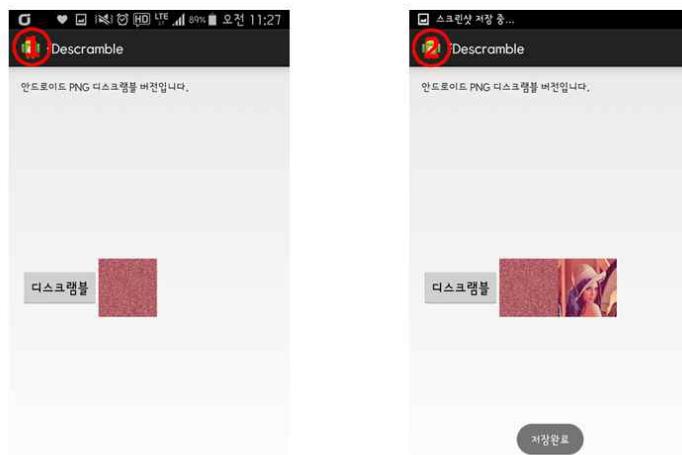
③ 안드로이드 환경을 위한 JPEG(제피이지)영상 전용 컨텐츠 복호화 프로그램



▶ 안드로이드 디스크램블 (JPEG)

- ① 원쪽 화면은 안드로이드 스크램블 JPEG 버전 메인화면입니다.
오른쪽 이미지는 스크램블 된 이미지를 뜻합니다.
- ② 디스크램블 버튼을 누르면 카오틱 맵 생성을 통해 원래 블럭들의 값을 불러와 이미지를 복원합니다.
- ③ 오른쪽 화면은 결과 화면입니다. 디스크램블된 사진을 이미지뷰로 출력하고, 외장 메모리에 저장을 합니다.

④ 안드로이드 환경을 위한 Chaos(카오스) 알고리즘 기반 컨텐츠 복호화 프로그램



▶ 안드로이드 디스크램블 (PNG)

- ① 원쪽 화면은 안드로이드 디스크램블 PNG 버전 메인화면입니다.
오른쪽 이미지는 스크램블된 이미지를 뜻합니다.
- ② 디스크램블 버튼을 누르면 카오틱 맵 생성을 통해 원래 블럭들의 값을 불러와 이미지를 복원합니다.
- ③ 오른쪽 화면은 결과 화면입니다. 디스크램블된 사진을 이미지뷰로 출력하고, 외장 메모리에 저장을 합니다.

- o LEA 경량암호기반 콘텐츠 인증 기술: 다수의 사용자가 이용하는 클라우드환경에서 효율적인 콘텐츠 인증을 위해 LEA 경량암호를 이용한 콘텐츠 인증, 키 동의 프로토콜, 생체정보와 스마트카드를 이용한 인증, 모바일 환경을 고려하여 ECC를 이용한 경량화 인증, 상호인증 등의 연구를 통하여 LEA 경량암호기반 콘텐츠 인증 기술을 확보하였다.

- 특허 등록 1건

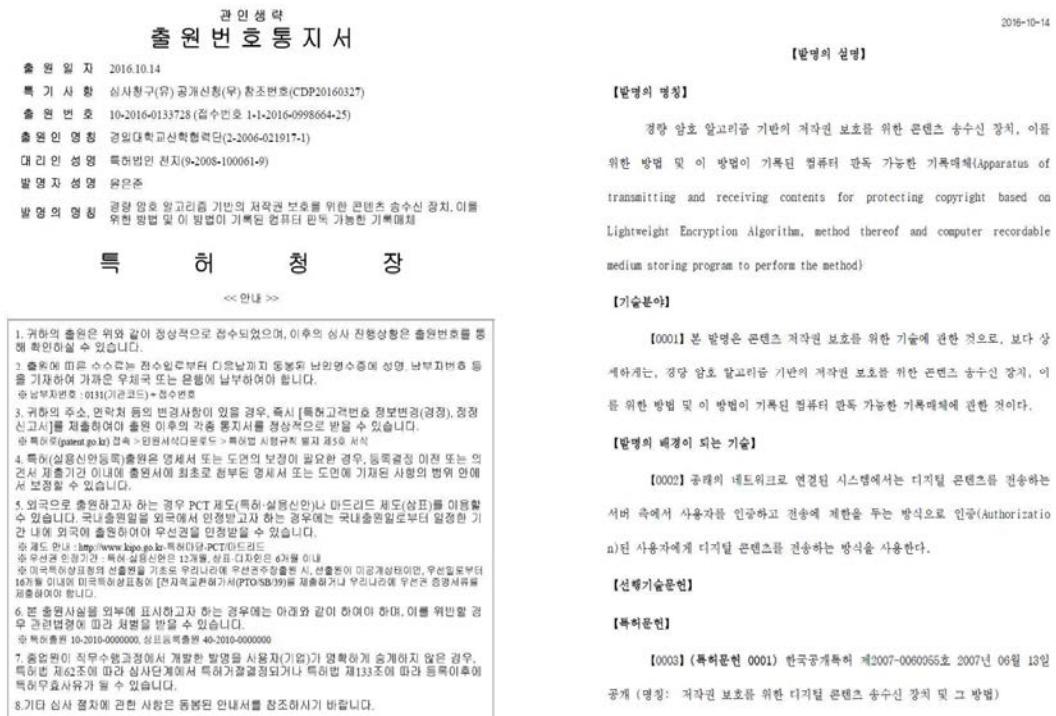
등록 특허				
등록일	특허명	출원인	출원국	등록번호
2016/09/15	손동작 인식을 이용한 접근 제어 시스템, 이를 위한 방법 및 이 방법이 기록된 컴퓨터 판독 가능한 기록매체	윤은준	대한민국	10-1656212

국가연구개발 보고서원문 성과물 전담기관인 한국과학기술정보연구원에서 가공·서비스 하는
연구보고서는 동의 없이 상업적 용도로 사용할 수 없습니다.



- 특허 출원 1건

등록 출원				
등록일	특허명	출원인	출원국	출원번호
2016/10/14	경량 암호 알고리즘 기반의 저작권 보호를 위한 콘텐츠 송수신 장치, 이를 위한 방법 및 이 방법이 기록된 컴퓨터 판독 가능한 기록매체	윤은준	대한민국	10-2016-0133728



Erratum: 'Lightweight authentication with key-agreement protocol for mobile network environment using smart cards'

Alavalapati Goutham Reddy, Eun-Jun Yoon, Ashok Kumar Das,
Kee-Yong Yoo, 'Lightweight authentication with key-agreement protocol for mobile network environment using smart cards', IET Information Security, 2(1), (5)

The authors have identified some drawbacks to the protocol presented in their paper and would like to point these out to the reader along with an improved protocol.

Drawbacks:

Foreign agent impersonation attack: In Rddy et al.'s protocol, U cannot verify the authenticity of F_A from the received message (P, Q, M_1) . Keeping this in mind, an adversary can impersonate a legitimate F_A as explained below.

Step 1: An adversary captures the message (P, Q, M_1) while sending from U to H over a public channel. Then, the adversary generates a random number $K = h(R_U, P)$ and authenticates H_A using K and M_1 . Now, U generates a nonce N_2 and computes $R_2 = K \oplus P, R = K \oplus Q, K = h(R_U, R_2), K' = K \oplus N_2, M_2 = MAC_{H_A}(ID_{H_A}, R_2, K, A)$, and forwards (R_2, K', M_2) to H .

Step 2: The adversary generates R_3, K', M_3 and computes $R = R_2 - R_3, K = h(R_3, R_2), K' = h(R_U, R_3), M_3 = MAC_{H_A}(R, K, M_3)$. Finally, the adversary forwards (R', K', M_3) to H .

Step 3: The adversary generates R_4, K', M_4 and computes $R = R_3 - R_4, K = h(R_4, R_3), K' = h(R_U, R_4), M_4 = MAC_{H_A}(R, K, M_4)$. Now, the adversary generates a nonce N_3 and computes $R' = R \oplus K \oplus N_3, M_5 = MAC_{H_A}(R', K, M_4) \oplus M_3$.

Step 4: U computes $N_3 = R \oplus R', S_{UH} = h(R_3, N_3) \oplus M_5$ and verifies $M_5 = MAC_{H_A}(R, K, S_{UH})$. It is obvious that the condition holds, subsequently U trusts the adversary F_A .

Table 2 Notations used in the proposed protocol

U	A mobile user
ID_U	Identity of U
PWU	Password of user
b	Random number chosen by U
F_A	A foreign agent
ID $_A$	Identity of F_A
HA	A home agent
ID $_A$	Identity of H_A
X, K $_A$, USK, FSK	H's secret keys
N_1, N_2	Randomly generated nonce
P	A point on elliptic curve
SK	Session key
$\{ \cdot \}$	A secure one-way hash function
\oplus	Blowfish XOR operation
\otimes	A concatenation operation

IET Inf. Secur., 2015, Vol. 10 Iss. 5, pp. 283-285

© The Institution of Engineering and Technology 2016

Lack of anonymity: In Rddy et al.'s protocol, U transmits the login request message $(ID_{H_A}, ID_{F_A}, M_1, M_2, T_1) \rightarrow H$. The parameter T_1 is unique for every session and gives the possibility of tracking the U . Hence, the protocol does not achieve perfect user anonymity.

Failure session-key update between U and F_A : During the session-key update phase, U sends $(ID_{H_A}, ID_{F_A}, T_2, P, K, R, K') \rightarrow F_A$. The session-key update phase between U and F_A and password update phase between U and H_A are similar. Here, $K' = h(R_U, P, K, R, K')$. The random numbers are not warranted by H_A and questions the mutual trust between U and F_A .

Corrections:

4. The improved protocol

This section presents a lightweight two-factor remote mutual authentication protocol for mobile network environment. The proposed protocol consists of four phases: user registration phase, foreign agent (F_A), home agent (H_A) and six phases: user registration phase, login phase, mutual authentication with key-agreement phase, password update phase, user registration phase, and password update phase between U and F_A and password update phase between U and H_A . The session-key update phase between U and F_A and password update phase between U and H_A are similar. The proposed protocol is given in Table 2.

4.1. User registration phase

This section presents a lightweight two-factor remote mutual authentication protocol for mobile network environment. The proposed protocol consists of four phases: user registration phase, foreign agent (F_A), home agent (H_A) and six phases: user registration phase, login phase, mutual authentication with key-agreement phase, password update phase, user registration phase, and password update phase between U and F_A and password update phase between U and H_A . The session-key update phase between U and F_A and password update phase between U and H_A are similar. The proposed protocol is given in Table 2.

4.2. User registration phase

Step 1: U chooses an identity ID_U , password PW_U , and a random number b , and computes $A = h(PW_U, b)$ and $PID_U = h(ID_U, b)$. PID_U is sent to H_A via a secure channel.

Step 2: Upon receiving the request from U , H_A computes $B_1 = h(ID_A, A, D_1, C_1, P, R, h(PID_U, b))$ and $T_1 = h(R_U, P, R, b)$, where D_1 and C_1 are H_A 's secret keys for all users.

Step 3: H_A chooses a point P on the elliptic curve and computes $R_1 = h(A, P)$ and then personalizes the parameters $(ID_{H_A}, C_1, T_1, R_1, P)$ on a smart card and delivers it to U via a secure channel.

Step 4: After receiving the smart card, U computes $D_1 = h(b \oplus PID_U, E_1 + C_1 \oplus A_1, P, R, h(PID_U, b))$ and $T_2 = h(D_1, P, E_1, R_1, F_1)$ on the smart card. Thus, the smart card finally contains the parameters $(ID_{H_A}, D_1, P, R_1, T_1, R_1, P, h(PID_U, b))$.

Step 5: The smart card computes $PID_U = h(ID_U \oplus PW_U, b) = D_1 \oplus h(PID_U, A_1) = h(PW_U, b)$.

4.3. Login phase

When U wants to access the network services of foreign agent F_A via a public channel, U sends the login request by inserting the smart card, inputs ID_U and PW_U .

Step 1: The smart card computes $PID_U = h(ID_U \oplus PW_U, b) = D_1 \oplus h(PID_U, A_1) = h(PW_U, b)$.

[3]

A Secure Anonymous Authentication Protocol for Mobile Services on Elliptic Curve Cryptography

ALALAPATI GOUTHAM REDDY¹, (Student, IEEE), ASHOK KUMAR DAS²,

EUN-JUN YOON³, AND KEE-YOUNG YOO⁴, (Member, IEEE)

¹School of Computer Science and Engineering, Kyungpook National University, Daegu 702-401, South Korea

²Department of Computer Science and Engineering, Kyungpook National University, Daegu 702-401, South Korea

³Department of Cyber Security, Kyungpook National University, Gyeongsan 760-701, South Korea

⁴Computer author, K.-Y. Yoo (yook@knu.ac.kr)

This work was supported in part by the R&D Project funded by Human Resource Development Program for Supporting Smart Life under the Ministry of Science, Science and Engineering, Kyungpook National University, South Korea under Grant 2012-0250000001, and in part by the Basic Science Research Programs within the Ministry of Education through the National Research Foundation of Korea under Grant NRF-2015H1D1A1009008.

ABSTRACT Mobile user authentication is an essential topic to consider in the current communications technology due to greater deployment of two-handheld devices and advanced technologies. Memon et al. recently proposed an efficient and secure two-factor authentication protocol for location-based services using asymmetric key cryptosystem. This paper identifies the security vulnerabilities that Memon et al.'s protocol has and proposes a new enhanced secure authentication protocol for mobile services on elliptic curve cryptography. The proposed protocol is also a two-factor authentication protocol and is suitable for practical applications due to the composition of light-weight operations. The proposed protocol's formal security is verified using Automated Validation of Internet Security Protocols and Applications tool to certify that the proposed protocol satisfies security requirements. The proposed protocol is analyzed and formal security analyses along with the performance analysis sections determine that the proposed protocol performs better than Memon et al.'s protocol and other related protocols in terms of security and efficiency.

INDEX TERMS Authentication, key-agreement, mobile services, security, AVISPA.

1. INTRODUCTION

A mobile device is an indispensable part of daily life among human beings due to the extensive range of applications such as voice communication and text messages. Progressively more mobile devices are being adopted in our daily lives, which features that allows to connect with other devices, internet and location based services. Besides, new security challenges are also mounting in conjunction with the evolution of mobile computing technologies. For instance, if a user discloses his/her mobile device to a third party, the user's privacy is easily breached. The data exchange over the wireless communication channels undoubtedly brings into question the privacy and integrity of conversations. The extensive deployment of handheld electronic devices, networks, mobility and flexibility necessitates the authentication process of every remote user. Mobile user authentication identifies the identity of user through a mobile device and permits access to the network services. The user authentication process through different means, namely passwords, smartcards and biometrics, is possible due to the provision of built-in advanced technologies in the mobile devices [1]–[3]. For example, Android supports face recognition, fingerprint and iris scanning for user authentication. The user authentication ensures the legitimacy of only the user and not the network service provider. The chances of attacks still exists when the user is unaware about the second party. Therefore, assuring the authenticity of all communicating parties is pretty much crucial, which is called mutual authentication.

In the mobile architecture, mutual authentication with key-agreement protocol affords the authentication between user and foreign agent via home agent, and enables both to generate a communal session-key to encrypt further communication through insecure networks. During the past decade, various authors have put forward diverse authentication protocols

2145-0457/16/042145-06\$17.80 © 2016 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but reproduction, distribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

VOLUME 4, 2016

[4]

The screenshot shows a comment on an article titled "Comment on Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards". The comment is from Alavalapati Goutham Reddy, Eun-Jun Yoon, Kee-Young Yoo, dated 2016-05-20. It discusses the security of the protocol and its correctness. The page includes navigation links for Journals & magazines, Conferences, eBooks, Reference, Subjects, Collections, and About. There are also sections for Logon system and Logout.

[5]

Comment on 'Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards'

Alavalapati Goutham Reddy¹, Eun-Jun Yoon², Kee-Young Yoo³

¹School of Computer Science and Engineering, Kyungpook National University, Daegu, Korea

²Department of Cyber Security, Kyungpook National University, Gyeongsan, Korea

³E-mail: yook@knu.ac.kr

Abstract: This comment paper refers to an article published by Leu and Hsieh in *IET Information Security* in the year 2014. Leu and Hsieh proposed a user authentication protocol for distributed systems using smart card. Their protocol affords user authentication and key exchange. The main idea of their protocol is to use the storage space available with the smart card to store the session key and the session key update attack is effectively overcome with few message protocols in terms of computational cost. However, this comment paper brings questions about the correctness of the design of Leu and Hsieh's protocol.

1 Preliminary One-way hash function.

A one-way hash function $h: \{0,1\}^n \rightarrow \{0,1\}^m$ is an algorithm [1, 2] which takes an arbitrary length string inputs $x \in \{0,1\}^n$ and gives fixed length outputs $y \in \{0,1\}^m$. The fundamental property of one-way hash function is that it is difficult to invert or preimage. The one-way hash function is widely used in encryption algorithms along with databases to index and retrieve data items. The one-way hash functions are message digest functions and secure hash algorithms.

The ideal hash function has the following properties:

1) One-way function: h is one-way function if it is hard to make R capable of computing the R value, which will be necessary for subsequent communications between U and R .

2) Collision resistance: The computation of h is a one-way function. If h is a collision resistant function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

3) Preimage resistance: The computation of h^{-1} is a hard problem. It is impossible to find an input x given its hash value $h(x)$.

4) Second preimage resistance: Two different inputs x_1, x_2 will have same hash output values, i.e. such that $h(x_1) = h(x_2)$.

5) Resistance to length extension: If h is a one-way function, then it is hard to find x such that $h(x) = h(x \parallel y)$, where \parallel denotes concatenation operator.

6) Resistance to chosen prefix attack: If h is a one-way function, then it is hard to find x such that $h(x) = h(x \parallel p)$, where p is a prefix of x .

7) Resistance to chosen suffix attack: If h is a one-way function, then it is hard to find x such that $h(x) = h(p \parallel x)$, where p is a suffix of x .

8) Resistance to chosen prefix-suffix attack: If h is a one-way function, then it is hard to find x such that $h(x) = h(p \parallel q \parallel x)$, where p is a prefix and q is a suffix of x .

9) Resistance to birthday attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

10) Resistance to quantum attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

11) Resistance to side-channel attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

12) Resistance to differential attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

13) Resistance to linear attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

14) Resistance to integral attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

15) Resistance to meet-in-the-middle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

16) Resistance to related-key attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

17) Resistance to quantum key distribution attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

18) Resistance to quantum search attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

19) Resistance to quantum oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

20) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

21) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

22) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

23) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

24) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

25) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

26) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

27) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

28) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

29) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

30) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

31) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

32) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

33) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

34) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

35) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

36) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

37) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

38) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

39) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

40) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

41) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

42) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

43) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

44) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

45) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

46) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

47) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

48) Resistance to quantum padding oracle attack: If h is a one-way function, then it is hard to find two different inputs x_1, x_2 such that $h(x_1) = h(x_2)$.

나. 클라우드 기반 콘텐츠 인증 서비스 구현

- o **클라우드 기반 콘텐츠 암호화 모듈:** 클라우드 환경에서 대량의 콘텐츠를 효율적으로 암호화하기 위해 LEA 경량암호를 이용한 암호화 모듈 개발 및 서버환경에서 고속의 병렬처리 모듈을 이용하여 효율적인 암호화 모듈 개발을 진행하였다.
 - S/W 등록 1건

순번	등록번호	제호	등록일자	저작자	발명자
1	C-2017-001597	클라우드 환경에서 경량화암호 기반 콘텐츠 암호화 모듈	2017-01-18	우경정보기술	박윤하

- 클라우드 환경에서 경량화암호 기반 콘텐츠 암호화 모듈(핵심 P/G소스)

```
// SWMain.cpp : 구현 파일입니다.

//



#include "stdafx.h"
#include "SWEnc.h"
#include "SWMain.h"
#include <minwinbase.h>

// SWMain
CCriticalSection cs; //크리티컬섹션 선언

IMPLEMENT_DYNAMIC(SWMain, CWnd)

SWMain::SWMain()
{
    m_iCount = ENCKEY_LENGTH;
    m_bInitialized = false;
}

SWMain::~SWMain()
{
}

void SWMain::SetPath(CString FNAME, CString FindFilePath)
{
    CString strIRoute = FindFilePath;

    int j = strIRoute.ReverseFind('.');
    CString strEncFileExt = strIRoute.Right(strIRoute.GetLength() - j); // 파일의 확장자
```

(.EXT) 가져오기

```
/////////////////////////////// c:\\Ark에 저장. TTA 테스트시에는 이부분 주석처리
CString strArk = _T("C:\\Ark\\");
//CString strAvi = _T(".avi");
CString strEncRoute = strArk + FNAME + strEncFileExt;
CString strArkFolder;

strArkFolder = L"C:\\Ark";

if (GetFileAttributes(strArkFolder) == -1)
{
   .CreateDirectory(strArkFolder, NULL);
    SetFileAttributes(strArkFolder, FILE_ATTRIBUTE_HIDDEN);
}

int iStrlen1 = (strIRoute.GetLength0+1)*2;
m_szInputPath = new char[iStrlen1 + 1];
WideCharToMultiByte(CP_ACP, 0, strIRoute, -1, m_szInputPath, iStrlen1 + 1, NULL,
NULL);

int iStrlen2 = (strEncRoute.GetLength0+1)*2;
m_szEncOutput = new char[iStrlen2 + 1];
WideCharToMultiByte(CP_ACP, 0, strEncRoute, -1, m_szEncOutput, iStrlen2 + 1,
NULL, NULL);

StartMain(FNAME, strIRoute, strEncRoute);

MoveFile(strEncRoute, strIRoute);
}

void SWMain::StartMain(CString FileName, CString Input, CString Ouput)
{
    LEA_Key mKey;
    mKey.makeKey(FileName);
    for (int i = 0; i<m_iCount; i++) m_iKey[i] = mKey.m_iKey[i];

    // moguai
    m_Enc.setEncrypt(m_iKey, m_iCount, m_szInputPath, m_szEncOutput);
    m_Enc.doEncrypt0;
```

```
m_bInitialized = false;
cs.Lock();
Enc_Num_Check++;
cs.Unlock();
CSWEncDlg* pDlg = (CSWEncDlg*)AfxGetApp()->m_pMainWnd;
COPYDATASTRUCT CpStructData;
HWND hHwd;
hHwd = pDlg->hHwd;

CpStructData.cbData = strlen((CStringA)m_szInputPath);
CpStructData.dwData=0;
CpStructData.lpData = m_szInputPath;

::SendMessage(hHwd, WM_COPYDATA, 0, (LPARAM)&CpStructData);

DeleteFile(Input);
delete[] m_szInputPath;
delete[] m_szEncOutput;
m_szInputPath = NULL;
m_szEncOutput = NULL;

}

BEGIN_MESSAGE_MAP(SWMain, CWnd)
END_MESSAGE_MAP()

// SWMain 메시지 처리기입니다.
```

- o **클라우드 기반 콘텐츠 복호화 모듈:** 클라우드 환경에서 대량의 콘텐츠를 효율적으로 복호화하기 위해 LEA 경량암호를 이용한 복호화 모듈 개발 및 서버환경에서 고속의 병렬처리 모듈을 이용하여 효율적인 복호화 모듈 개발을 진행하였다.
 - S/W 등록 1건

순번	등록번호	제호	등록일자	저작자	발명자
1	C-2017-001598	클라우드 환경에서 경량화암호 기반 콘텐츠 복호화 모듈	2017-01-18	우경정보기술	박윤하

- 클라우드 환경에서 경량화암호 기반 콘텐츠 복호화 모듈(핵심 P/G소스)

```
// DecMain.cpp : 구현 파일입니다.  
//  
  
#include "stdafx.h"  
#include "DecMain.h"  
  
IMPLEMENT_DYNAMIC(DecMain, CWnd)  
  
DecMain::DecMain()  
{  
    m_iCount = ENCKEY_LENGTH;  
    m_bInitialized = false;  
}  
  
DecMain::~DecMain()  
{  
}  
  
void DecMain::SetPath(CString FNAME, CString FindFilePath,CString fileExt)  
{  
    CString strPath;  
    TCHAR path[_MAX_PATH];  
    GetModuleFileName(NULL, path, sizeof path);  
    strPath = path;  
    int i = strPath.ReverseFind('\\');//실행 파일 이름을 지우기 위해서 왼쪽에 있는 '\'를 찾는다.  
    strPath = strPath.Left(i);//뒤에 있는 현재 실행 파일 이름을 지운다.  
  
    CString strArk = _T("\\Decrypt\\");  
    //CString strAvi = _T(".avi");  
    CString strAvi = _T(".") + fileExt;  
    CString strIRoute = FindFilePath;  
    CString strEncRoute = strPath + strArk + FNAME + strAvi;  
    CString strArkFolder;  
  
    int iStrlen1 = (strIRoute.GetLength0 + 1) * 2;  
    m_szInputPath = new char[iStrlen1 + 1];  
    WideCharToMultiByte(CP_ACP, 0, strIRoute, -1, m_szInputPath, iStrlen1 + 1, NULL,
```

```
NULL);

int iStrlen2 = (strEncRoute.GetLength() + 1) * 2;
m_szEncOutput = new char[iStrlen2 + 1];
WideCharToMultiByte(CP_ACP, 0, strEncRoute, -1, m_szEncOutput, iStrlen2 + 1, NULL,
NULL);

strArkFolder = strPath + strArk;

if (GetFileAttributes(strArkFolder) == -1)
{
    CreateDirectory(strArkFolder, NULL);
    SetFileAttributes(strArkFolder, FILE_ATTRIBUTE_HIDDEN);
}

StartMain(FNAME, strRoute, strEncRoute);
}

void DecMain::StartMain(CString FileName, CString Input, CString Ouput)
{
    LEA_Key mKey;
    mKey.makeKey(FileName);
    for (int i = 0; i < m_iCount; i++) m_iKey[i] = mKey.m_iKey[i];

    m_Dnc.setDecrypt(m_iKey, m_iCount, m_szInputPath, m_szEncOutput);
    m_Dnc.doDecrypt();
    m_bInitialized = false;

    delete[] m_szInputPath;
    delete[] m_szEncOutput;
    m_szInputPath = NULL;
    m_szEncOutput = NULL;
}

BEGIN_MESSAGE_MAP(DecMain, CWnd)
END_MESSAGE_MAP()
// DecMain 메시지 처리기입니다.
```

- **클라우드 기반 콘텐츠 인증 서비스:** 다수의 사용자와 대량의 콘텐츠를 사용하는 클라우드 환경에서 효율적인 콘텐츠 인증을 위해 LEA 경량 암호기반 콘텐츠 인증 기술을 확보하였다.

- GS인증 1건

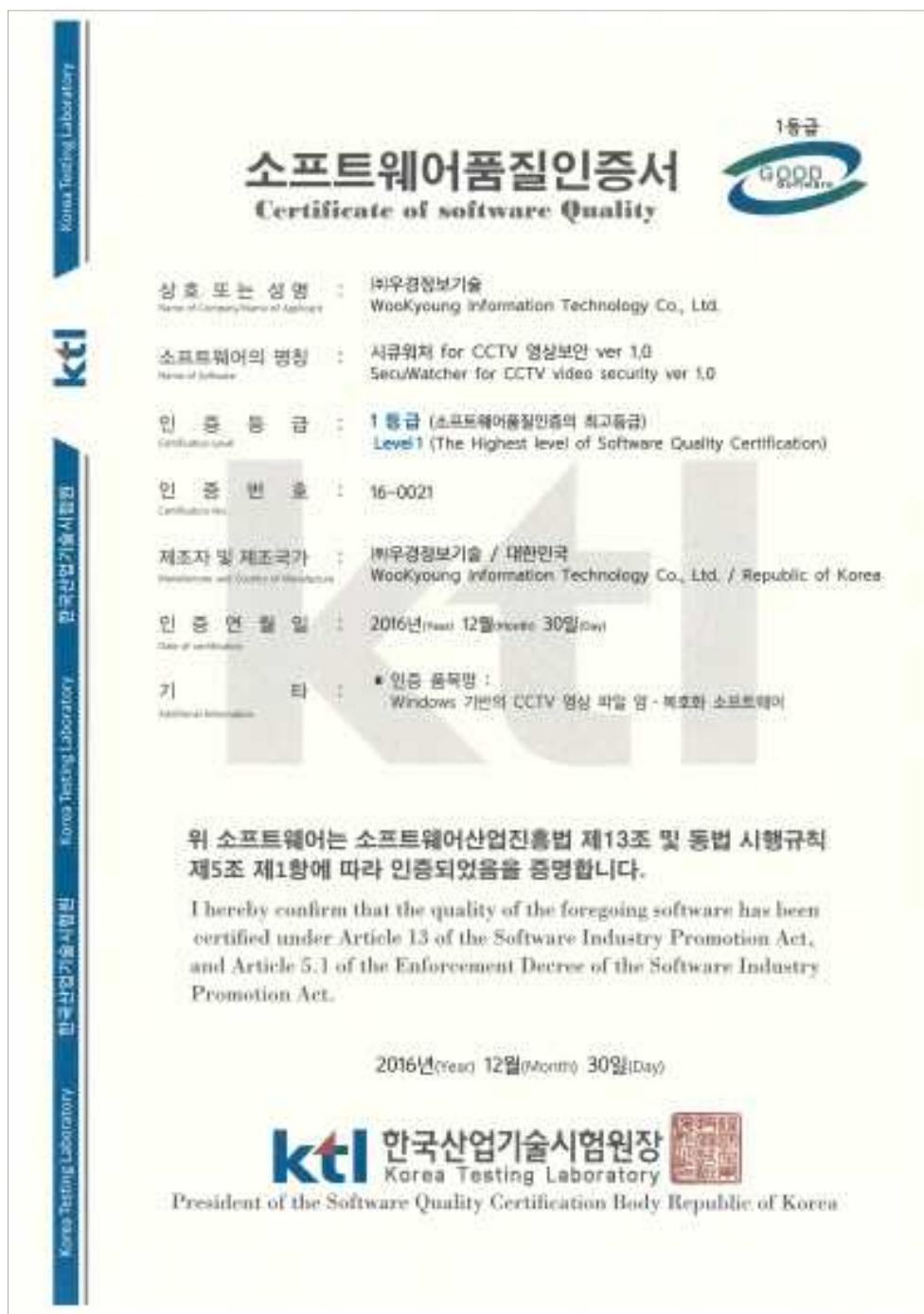
GS인증		
인증일	인증제품명	인증결과
2016/12/31	시큐워처 for 저작권 (시큐워처 for CCTV 영상보안 ver 1.0)	GS인증 적합판정

① **시큐워처 for 저작권(시큐워처 for CCTV 영상보안 ver 1.0, GS인증 적합판정)**

본 제품은 대용량의 CCTV 영상을 LEA 경량암호 모듈을 이용하여 서버환경에서 고속의 병렬 처리 모듈을 이용하여 안전하고 효율적으로 영상파일에 대한 보안을 제공해주는 프로그램이다. 클라우드 스토리지 서비스의 환경과 유사한 환경에서 본 과제에서 개발한 LEA 경량암호 기반 암·복호화 모듈과 LEA 경량암호기반 콘텐츠 인증기술을 이용하여 GS인증을 통과하여 해당 개발 모듈의 적합 판정을 받았다.



[시큐워처 for 저작권 ver 1.0]



연구개발 2 : 콘텐츠 저작권 보호기술 개발

다. 특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술 개발

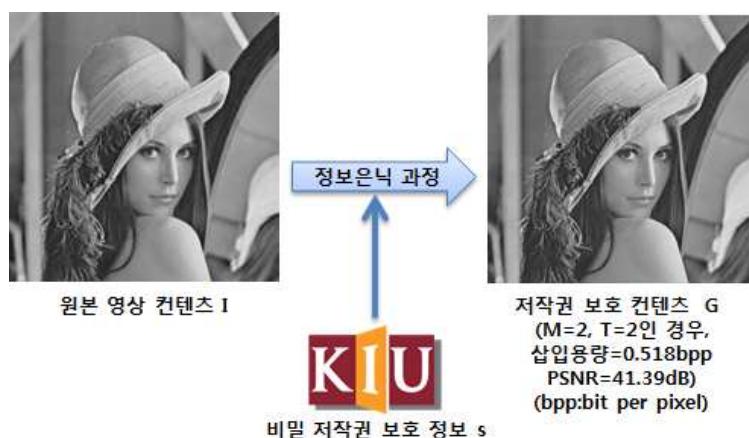
- 제로정보은닉 기반 저작권보호 기술 개발: 컨텐츠의 위변조 방지 및 저작권 정보를 컨텐츠의 손상없이 삽입할 수 있는 제로정보은닉 기반 저작권보호기술의 확보를 위해 특허등록 및 출원, 프로그램 개발과 함께 관련 연구를 진행하였다.
- S/W 등록 3건

순번	등록번호	제호	등록일자	저작자	발명자
1	C-2016-023711	Steganography(스테가노그래피) 기반 컨텐츠 위변조 방지 및 저작권 정보 은닉 프로그램	2016-10-06	경일대학교 산학협력단	윤은준 외 4
2	C-2016-024830	안드로이드 환경을 위한 Steganography(스테가노그래피) 기반 컨텐츠 위변조 방지 및 저작권 정보 은닉 프로그램	2016-10-20	경일대학교 산학협력단	윤은준 외 4

- ① Steganography(스테가노그래피) 기반 컨텐츠 위변조 방지 및 저작권 정보 은닉 프로그램



(a) (M=2, T=0인 경우, 삽입용량=0.120bpp, PSNR=41.39dB)



(b) (M=2, T=2인 경우, 삽입용량=0.518bpp, PSNR=41.39dB)

② 안드로이드 환경을 위한 Steganography(스테가노그래피) 기반 컨텐츠 위변조 방지 및 저작권 정보 은닉 프로그램



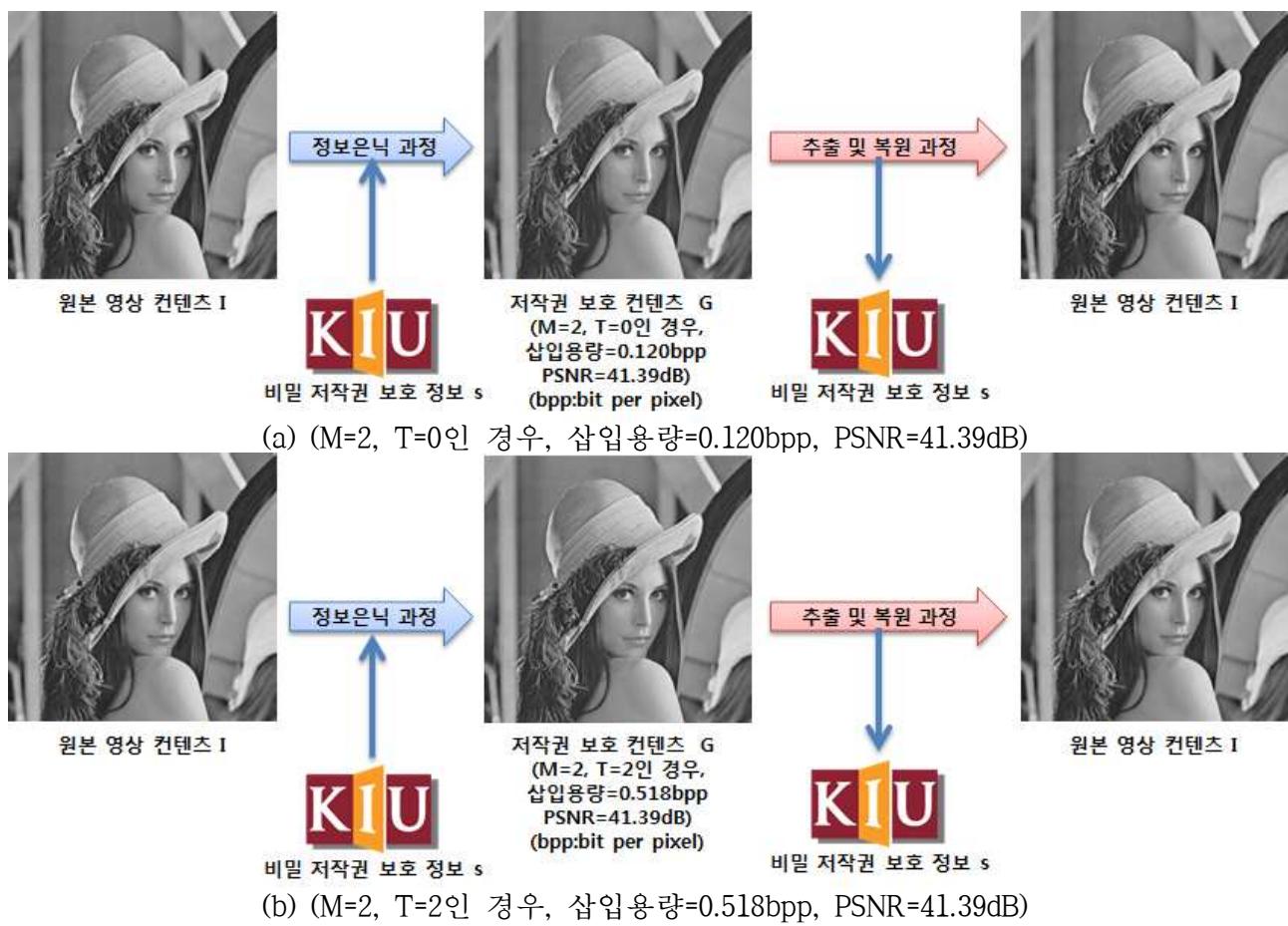
▶ 안드로이드 워터마크 생성 및 삽입 (PNG)

- ① 본 화면은 안드로이드 워터마크 생성 및 삽입 버전입니다.
버튼위에 마크는 워터마크를, 오른쪽은 원본 이미지를 뜻합니다.
- ② 워터마크 생성 버튼을 누르면 원래 워터마크 이미지를 바이너리 이미지로 변환하여 이미지 뷔로 출력을 한뒤 외장 메모리에 저장을 합니다.
- ③ 워터마크 삽입 버튼을 누르면 바이너리 이미지를 원래 이미지크기로 변환하여 크기를 동일하게 한 후에 2개의 이미지를 XOR연산을 통해 삽입한 후, 마찬가지로 외장 메모리에 저장을 합니다.

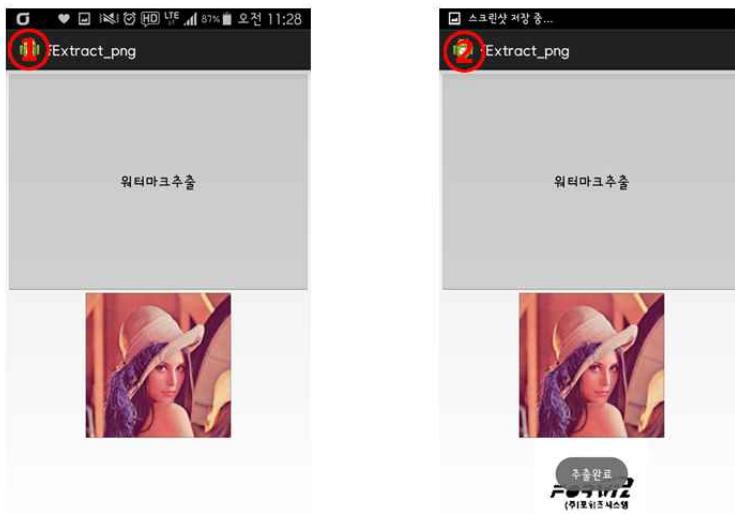
- 제로정보은닉 기반 저작권추출 기술 개발: 삽입된 정보를 효율적으로 추출하는 방법의 연구를 위해 컨텐츠 위변조 방지 및 저작권 정보 추출검증 프로그램을 개발하였다.
 - S/W 등록 2건

순번	등록번호	제호	등록일자	저작자	발명자
1	C-2016-023710	Steganography(스테가노그래피) 기반 컨텐츠 위변조 방지 및 저작권 정보 추출검증 프로그램	2016-10-06	경일대학교 산학협력단	윤은준 외 4
2	C-2016-024829	안드로이드 환경을 위한 Steganography(스테가노그래피) 기반 컨텐츠 위변조 방지 및 저작권 정보 추출검증 프로그램	2016-10-20	경일대학교 산학협력단	윤은준 외 4

- ① Steganography(스테가노그래피) 기반 컨텐츠 위변조 방지 및 저작권 정보 추출검증 프로그램



- ② 안드로이드 환경을 위한 Steganography(스테가노그래피) 기반 컨텐츠 위변조 방지 및 저작권 정보 추출검증 프로그램



▶ 안드로이드 워터마크 추출 (PNG)

- ① 왼쪽 화면은 안드로이드 워터마크 추출 버전 메인화면입니다.
아래 사진은 워터마크가 삽입된 이미지입니다.
- ② 스크램블 버튼을 누르면 원래 순서를 기억한 뒤 카오틱 맵을 통해 픽셀 값을 섞어줍니다.
- ③ 오른쪽 화면은 결과 화면입니다. 복원된 이미지와 추출된 워터마크를 이미지뷰로 출력하고,
외장 메모리에 저장을 합니다.

- 특허 등록 2건

등록 특허				
등록일	특허명	출원인	출원국	등록번호
2016/08/08	개별 객체 프라이버시 보호를 위한 영상 처리 장치, 이를 위한 방법 및 이 방법이 기록된 컴퓨터 판독 가능한 기록매체	윤은준 외 1	대한민국	10-1648188
2016/08/08	환경 변화에 따른 프라이버시 보호를 위한 동적 객체 영상 처리 시스템, 이를 위한 방법 및 이 방법이 기록된 컴퓨터 판독 가능한 기록매체	윤은준	대한민국	10-1648190



[1]

[1]



[2]

[2]

- SCI(E) 논문 게제 2편

번호	논문 종류	제재 일자	논문명	제재 저널명 (FullName)	ISSN	Vol (No.)	저자
1	SCI(E)	(제재 예정)	Reversible data hiding scheme with edge-direction predictor and modulo operation	Journal of Real-Time Image Processing	1861-8219 (IF=1.564)	(제재 예정)	윤은준 외 3
2	SCI(E)	(제재 예정)	Reversible data hiding scheme with edge-direction predictor and modulo operation	Journal of Real-Time Image Processing	1861-8219 (IF=1.564)	(제재 예정)	윤은준 외 3

J Real-Time Image Proc
DOI 10.1007/s12554-015-0549-9
SPECIAL ISSUE PAPER



J Real-Time Image Proc
DOI 10.1007/s12554-015-0558-7
SPECIAL ISSUE PAPER



Reversible data hiding scheme with edge-direction predictor
and modulo operation

Due-Soo Kim¹ · Eun-Jun Yoon² · Cheonshik Kim³ · Kee-Young Yoo⁴

Received: 23 July 2015/Accepted: 23 November 2015
© Springer-Verlag Berlin Heidelberg 2016

Abstract Since the first histogram shifting technique was proposed by Ni et al., many histogram-based data hiding methods were proposed to improve the scheme. One of the methods is using different values between cover image and prediction image. Another method is using two point pairs and absolute value for improving Ni et al.'s scheme. In this paper, novel reversible data hiding scheme with edge-direction predictor and modulo operation was proposed. The proposed scheme can be applied to various image types. We considered so much as possible area pixels by using edge-direction predictor with odd and even line embedding. Also, we utilize two point pairs and absolute value at the same time by using modulo operation with wrap around. In the experimental results, the proposed scheme shows a good quality image result about 48dB as similar other schemes and enhanced hiding capacity over 50 % than other schemes.

✉ Kee-Young Yoo
yook@knu.ac.kr
Due-Soo Kim
stswns@knu.ac.kr
Eun-Jun Yoon
ejyoon@knu.ac.kr
Cheonshik Kim
cskim@paran.com

¹ School of Computer Science and Engineering, College of IT Engineering, Kyungpook National University, 120 Sankuk-Dong, Buk-Gu, Daegu 702-701, South Korea

² Department of Cyber Security, Kyungpook National University, 80 Daehak-Ro, Taegu, Gyeongsangbuk-Do, 702-701, South Korea

³ Department of Digital Media Engineering, Anyang University, 708-113 Anyang 5-dong, Mureung-gu, Anyang-si, Kyunggi-do 439-714, South Korea

Published online: 09 December 2015

© Kee-Young Yoo
yook@knu.ac.kr
Gild-Je Lee
vill@jilin.knu.ac.kr
Eun-Jun Yoon
ejyoon@knu.ac.kr
Cheonshik Kim
cskim@paran.com

Received: 28 August 2015/Accepted: 16 December 2015
© Springer-Verlag Berlin Heidelberg 2016

Abstract When traditional secret image sharing techniques reconstructed the secret, they input the shares over 2. While in our scheme, the secret is reconstructed about 1 share. The secret, the problems arises when there are more than 2 shares. The cheater can use this to put their share in the last. Therefore, fairness is an important objective of the secret image sharing. Tian et al. proposed the fairness secret sharing scheme in 2012. However, they generated a polynomial with degree $n-1$, which is perfect for reconstructing the polynomial using Lagrange interpolation. Therefore, their scheme is unsuitability to the real-time processing. The proposed scheme generates one polynomial for the one secret data based on the fairness concept of Tian et al.'s scheme. For the providing fairness, the proposed scheme hides the verification value at the random coefficient of the polynomial. During the secret image reconstruction procedure, each shadow image brought by a participant is verified for its fairness using XOR operation. Our scheme not only satisfies the fairness, but also is suitable for the real-time processing. The higher the degree of the participants from internal provision of a false or cheating. In addition, our scheme uses the steganography technique for increasing the security protection purpose. The proposed scheme as a whole offers a high secure and effective mechanism for the secret image sharing that is not found in existing secret image sharing schemes. In the experimental result, PSNR of the proposed scheme is average 44.67 dB. It is higher 4 dB than the previous schemes. The embedding capacity is also similar to the other schemes.

Keywords Fairness · Secret image sharing · Lagrange interpolation · PSNR · Real-time

1 Introduction

Due to the rapid development of computer networking and digital technology, transmitting multimedia data, such as digital images and videos, has become the fastest, convenient and popular. However, the transmission of sensitive information over insecure networks causes one of the most challenging security issues. Especially military and medical images are confidential and must be protected from illegal user. The confidential images may be destroyed or be lost accidentally when they are handled by one person. That is, one person can reveal the images. Steganographic techniques distribute materials to involve participants, as the generated data does not reveal any information if they are not combined in the prescribed way [1–3, 5, 6, 16].

The secret sharing scheme was proposed by [13] and [4], respectively. The concept of secret sharing scheme shares a secret data among n participants which is

[1]

[2]

○ 특징 기반 필터링을 이용한 저작권 보호기술 개발: 콘텐츠 원본이 훼손되지 않으면서 저작권 보호 정보를 은닉할 수 있는 제로정보은닉 기반의 스테가노그레피 기법과 DNA 필터링 기법을 융용한 저작권 보호 기법을 개발하였다.

- S/W 등록 1건(등록예정)

순번	등록번호	제호	등록일자	저작자	발명자
1	C-2017-001599	특징 기반 저작권 보호 프로그램	2017-01-18	우경정보기술	박윤하

- 특징 기반 필터링을 이용한 저작권 보호 모듈(핵심 P/G소스)

IMPLEMENT_DYNAMIC(Watermarking, CWnd)

```
Watermarking::Watermarking()
{
    InitChaos();
}

Watermarking::~Watermarking()
{
}

void Watermarking::InitChaos()
{
    count = 0;
    ki = 0;
    // chaos 초기값 설정
    double initial_x = 0.1;
    initial_m = 3.5699456;
    C = initial_x;
    chaos = floor((C+0.5));
}

void Watermarking::FastCorner(IplImage* m_image)
{
    Mat img_1 = cvarrToMat(m_image);
    DenseFeatureDetector detector(1.f,1,0.1f,20,0,true,false);
    detector.detect( img_1, keypoints_1 );
    w_count = 0;
    for(int i=0; i < keypoints_1.size(); i++ )
    {
        FastValue = ((int)(keypoints_1[i].pt.x + keypoints_1[i].pt.y))%2;
        KeyGeneration();
    }
}

void Watermarking::KeyGeneration()
{
    count++;
    int value = load->imageData[w_count];
    w_count++;
    if(w_count < (load->height * load->width))
    {
        w_count = 0;
    }
    payload = (abs(int(value)))%2;
    k_i[ki] = GetXOR(GetXOR(payload, FastValue),chaos);
    //Key값 생성
    ki++;
}
```

```
chaos = Generate_Chaos();
if(count % 8 == 0){
    number = BinaryToDecimal(k_i, number);
    fwrite(&number, sizeof(number), 1, Fast); //키 값 10진수로 변환 후 저장
    ki = 0;
}
if(keypoints_1.size() % 8 != 0 && keypoints_1.size() == count)
{
    number = BinaryToDecimal(k_i, number);
    fwrite(&number, sizeof(number), 1, Fast);
    ki = 0;
    count = 0;
}
if(keypoints_1.size() == count)
{
    count = 0;
}

}

double Watermarking::Generate_Chaos()
{
    //chaos 값 생성
    C = initial_m * C*(1-C);
    return floor((C+0.5));
}

void Watermarking::ThresholdValue(IplImage *Pay)
{
    //Threshold
    load = cvCreateImage( cvGetSize( Pay ), IPL_DEPTH_8U, 1);
    cvCvtColor( Pay, load, CV_RGB2GRAY );
    cvThreshold(load, load, 128, 255, CV_THRESH_BINARY);
}

byte Watermarking::BinaryToDecimal(int k_i[8], int Decimalnumber)
{
    Decimalnumber = 0;
    Decimalnumber +=k_i[0]*128;
    Decimalnumber +=k_i[1]*64;
    Decimalnumber +=k_i[2]*32;
    Decimalnumber +=k_i[3]*16;
    Decimalnumber +=k_i[4]*8;
    Decimalnumber +=k_i[5]*4;
```

```

        Decimalnumber +=k_i[6]*2;
        Decimalnumber +=k_i[7]*1;

    return Decimalnumber;
}

int Watermarking::GetXOR(int a, int b)
{
    if(a==0&&b==0) return 0;
    else if(a==0&&b==1) return 1;
    else if(a==1&&b==0) return 1;
    else if(a==1&&b==1) return 0;
    else
    {
        return -1;
    }
}

```

- 특징 기반 필터링을 이용한 저작권 추출기술 개발: 콘텐츠 원본이 훼손되지 않으면서 저작권 보호 정보를 은닉할 수 있는 제로정보은닉 기반의 스테가노그래피 기법과 DNA 필터링 기법을 응용한 저작권 추출 기법을 개발하였다.

- S/W 등록 1건

순번	등록번호	제호	등록일자	저작자	발명자
1	C-2017-001600	특징 기반 저작권 추출 및 위변조 방지 프로그램	2017-01-18	우경정보기술	박윤하

- 특징 기반 저작권 추출 및 위변조 방지 모듈(핵심 P/G소스)

```

IMPLEMENT_DYNAMIC(Markingcheck, CWnd)

Markingcheck::Markingcheck()
{
    InitChaos();
}

Markingcheck::~Markingcheck()
{
}

void Markingcheck::HarrisCorner(IplImage* m_image)
{
    Mat img_1 = cvarrToMat(m_image);

```

```
DenseFeatureDetector detector(1.f,1,0.1f,20,0,true,false);

detector.detect( img_1, keypoints_1 );

w_count = 0;
for(int i=0; i < keypoints_1.size(); i++ )
{
    FastValue = ((int)(keypoints_1[i].pt.x + keypoints_1[i].pt.y))%2;

    KeyExtraction();
    if(TimerKill == true)
    {
        break;
    }
}

}

void Markingcheck::InitChaos()
{
    count = 0;
    ki = 0;
    //chaos 초기값
    double initial_x = 0.1;
    initial_m = 3.5699456;
    C = initial_x;
    chaos = floor((C+0.5));
}

void Markingcheck::KeyExtraction()
{
    payload = 0;
    int value = load->imageData[w_count];
    w_count++;
    if(w_count < (load->height * load->width))
        w_count = 0;
```

```
payload = (abs(value))%2;
if(count == 0 || count % 8 == 0){
    fread(&number,sizeof(number), 1, Fast);
    DecimalToBinary(k_i,number);
}
count++;

if(keypoints_1.size() >= count){
    if(payload != GetXOR(GetXOR(k_i[ki], FastValue),chaos)) //마킹체크
    {
        TimerKill = true;
        count = keypoints_1.size();
        MessageBox(L“영상이 변경되었습니다.”);
    }
}

ki++;
if(keypoints_1.size() == count){
    ki = 0;
    count = 0;
}
if(ki == 8)
{
    ki = 0;
}

Generate_Chaos();

}

int Markingcheck::GetXOR(int a, int b)
{
    if(a==0&&b==0) return 0;
    else if(a==0&&b==1) return 1;
    else if(a==1&&b==0) return 1;
    else if(a==1&&b==1) return 0;
    else
    {
        return -1;
    }
}
```

```
void Markingcheck::ThresholdValue(IplImage *Pay)
{
    //Threshold
    load = cvCreateImage( cvGetSize( Pay ), IPL_DEPTH_8U, 1);
    cvCvtColor( Pay, load, CV_RGB2GRAY );
    cvThreshold(load, load, 128, 255, CV_THRESH_BINARY);
}

int Markingcheck::DecimalToBinary(int ToBinaryk_i[8],int Decimalnumber)
{
    //10진수를 2진수로변환
    if(Decimalnumber >= 128)
    {
        ToBinaryk_i[0]= Decimalnumber/128;
        Decimalnumber -= 128;
    }
    else
    {
        ToBinaryk_i[0] = 0;
    }
    if (Decimalnumber < 128 && Decimalnumber >= 64)
    {
        ToBinaryk_i[1] = Decimalnumber/64;
        Decimalnumber -=64;
    }
    else
    {
        ToBinaryk_i[1] = 0;
    }
    if(Decimalnumber < 64 && Decimalnumber >= 32)
    {
        ToBinaryk_i[2] = Decimalnumber/32;
        Decimalnumber -=32;
    }
    else
    {
        ToBinaryk_i[2] = 0;
    }
    if(Decimalnumber < 32 && Decimalnumber >= 16)
    {
        ToBinaryk_i[3] = Decimalnumber/16;
        Decimalnumber -=16;
    }
}
```

```

    }
    else
    {
        ToBinaryk_i[4] = 0;
    }
    if(Decimalnumber < 8 && Decimalnumber >= 4)
    {
        ToBinaryk_i[5] = Decimalnumber/4;
        Decimalnumber -=4;
    }
    else
    {
        ToBinaryk_i[5] = 0;
    }
    if(Decimalnumber < 4 && Decimalnumber >= 2)
    {
        ToBinaryk_i[6] = Decimalnumber/2;
        Decimalnumber -=2;
    }
    else
    {
        ToBinaryk_i[6] = 0;
    }
    if(Decimalnumber < 2 && Decimalnumber >= 0)
    {
        ToBinaryk_i[7] = Decimalnumber/1;
    }

    Decimalnumber = 0;
    return ToBinaryk_i[8];
}

```

라. 클라우드 기반 저작권 보호기술 서비스 구현

- 클라우드 환경에서 특징기반 필터링 및 제로정보은닉 기반 저작권 보호기술 개발:
클라우드 환경에서 스토리지에 저장된 콘텐츠에 특징기반 필터링을 응용한
제로정보은닉 기반 콘텐츠 저작권 보호기술을 이용하여 저작권 보호 기술을
개발하였다.
- 특허 등록 1건

등록 특허				
등록일	특허명	출원인	출원국	등록번호
2016/11/17	제로널리지 기반의 영상 위변조 방지와 탐지를 위한 워터마킹 삽입과 추출 장치 및 그 방법	우경정보 기술	대한민국	10-1677110

국가연구개발 보고서원문 성과물 전담기관인 한국과학기술정보연구원에서 가공·서비스 하는
연구보고서는 동의 없이 상업적 용도로 사용할 수 없습니다.

수신처: 95-23-684272811
수령일자: 2018.09.08.

0815

정부

YOUR INVENTION PARTNER
특허청
특허결정서

3년의
30년의
혁신
성장

그로 인해 학생들은 주제에 대한 이해를 확장하고, 다양한 관점에서 문제를 해결하는 능력을 키울 수 있다.

[특기사항]
이 런 발명의 출원현에 대한 검색은 2016.09.05 까지 출원된 자료로 대상으로 하였으며, 그 날짜 이후 등록된 출원현과 주장을 통한 전자출원에 의한 특허현 제29조제8항 및 제4항 제36조제1항 내지 제3항 위반 여부는 판단하지 아니하였습니다. - 끝.

[참고문헌]

[1]

- 특히 출원 1건

출원 특허				
출원/등록일	특허명	출원인	출원국	출원번호
2016/10/14	가역 정보 은닉 기반의 콘텐츠 위변조 방지를 위한 저작권 보호 장치, 이를 위한 방법 및 이 방법이 기록된 컴퓨터 판독 가능한 기록매체	윤은준 외 2	대한민국	10-2016-0133734

관인생략
출원번호통지서

출	원	일	자	2016.10.14
록	기	사	황	심사청구(유) 공개신청(무) 참조번호(CDP20160328)
출	원	면	호	2016-0133734 (접수번호 1-1-2016-0998699-12)
출	원	인	명	경인대학교신학협회단(2-2006-021917-1)
대	리	인	성	명
발	행	자	성	명
발	행	의	명	정

2016-10-14

【한명의 한명】

【발명의 명칭】
가액 정보 은닉 기반의 콘텐츠 위변조 방지 위한 저작권 보호 장치, 이를 위한 방법 및 이 방법이 기록된 컴퓨터 판독 가능한 기록매체(Apparatus for protecting contents copyright for preventing forgery based on reversible data hiding, method thereof and computer recordable medium storing program to perform the method).

[기술분야]

【0001】 본 발명은 저작권 보호를 위한 기술에 관한 것으로, 보다 상세하게는, 가액 정보 은닉 기반의 콘텐츠 위변조 방지에 위한 저작권 보호 장치, 이를 위한 바탕 및 이 바탕이 기본적 기록디바이스에 기록되는 방법, 그리고 이를 위한 바탕 및 이 바탕이 기본적 기록디바이스에 기록되는 방법이다.

【반영의 배경이 되는 기술】

【0002】 데이터 온너 기술은 음악, 영상, 동영상, 전자 문서, 교육 자료, 애니메이션과 같은 디지털 미디어 콘텐츠에 기밀 정보를 비가시적으로 삽입하는 기술이다.

[解説] 今泉洋

【특허문헌】

39-4

[17]

- 75 -

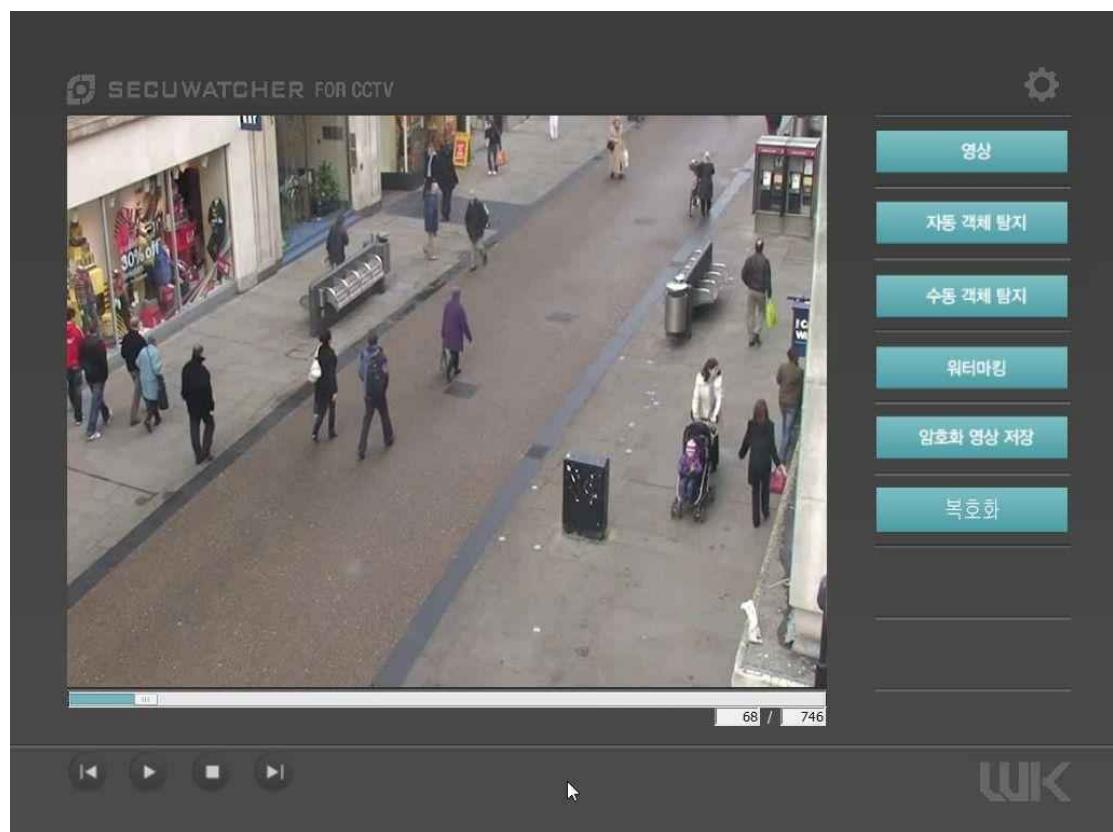
- 클라우드 환경에서 특징기반 필터링 및 제로정보은닉 기반 저작권 해제기술 개발:
클라우드 환경에서 스토리지에 저장된 콘텐츠에 특징기반 필터링을 응용한
제로정보은닉 기반 콘텐츠 저작권 보호기술을 이용하여 저작권 추출 기술을
개발하였다.
 - GS인증 1건

GS인증		
인증일	인증제품명	인증결과
2016/12/31	시큐워처 for 클라우드 저작권보호 (시큐워처 for CCTV 영상반출 ver 1.0)	GS인증 진행 중 (4월 말 인증완료 예정)

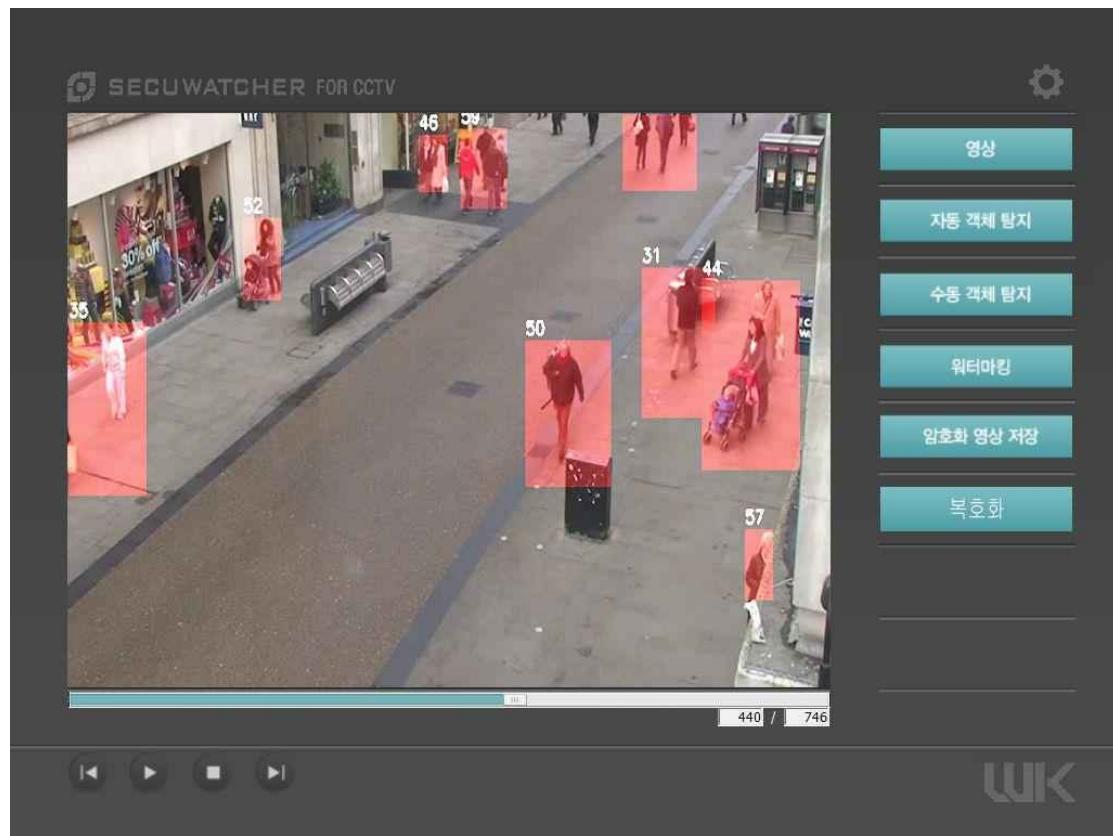
- ① 시큐워처 for 클라우드 저작권보호(시큐워처 for CCTV 영상반출 ver 1.0, GS인증 진행중)

본 제품은 CCTV 영상을 외부 반출을 위해 영상에 보안조치를 취하는 프로그램으로 영상 위변조 방지를 위해 본 과제에서 개발한 특징기반 필터링 및 제로정보은닉 기술을 이용한 저작권 보호기법을 이용하였다. 현재 GS 인증을 진행 중이다.

(가) 영상재생 - 영상을 불러와 재생할 수 있습니다.



(나) 자동 객체 탐지 - 불러온 영상에서 움직이는 객체를 자동으로 탐지합니다.



- 특허 등록 1건

등록 특허				
등록일	특허명	출원인	출원국	등록번호
2016/09/06	보행자의 얼굴 검출 기반의 동적 객체 영상 프라이버시 보호 장치 및 그 방법	우경정보기술	대한민국	10-2016-00300 090

【특기사항】

이 건 발명의 선출원에 대한 검색은 2016.09.05 까지 출원원 자료를 대상으로 하였으며, 이 날짜 이후 조작우선권 주장을 통해 진입하는 출원에 의한 특허는 제29조제3항 및 제4항 또
는 제29조제1항 (나) 제2항 첨단 기기부는 판단하지 아니됩니다. 과

- [참고문헌]
1. KR1020120036299 A

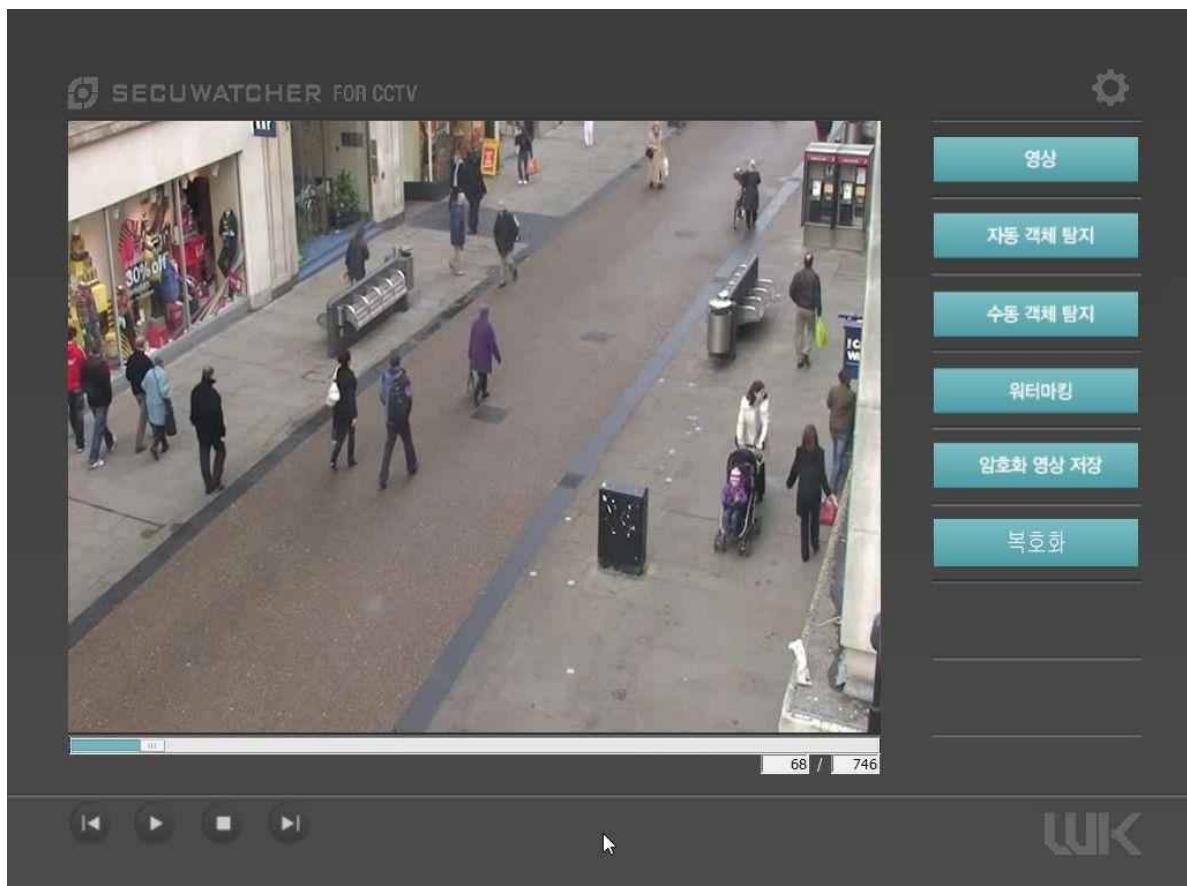


- 시큐워처 for CCTV 영상반출 ver 1.0 (S/W)

순번	등록번호	제호	등록일자	저작자	발명자
1	C-2016-033818-2	시큐워처 for CCTV 영상반출 ver 1.0	2016-12-30	우경정보기술	박윤하

① 시큐워처 for CCTV 영상반출 ver 1.0 프로그램

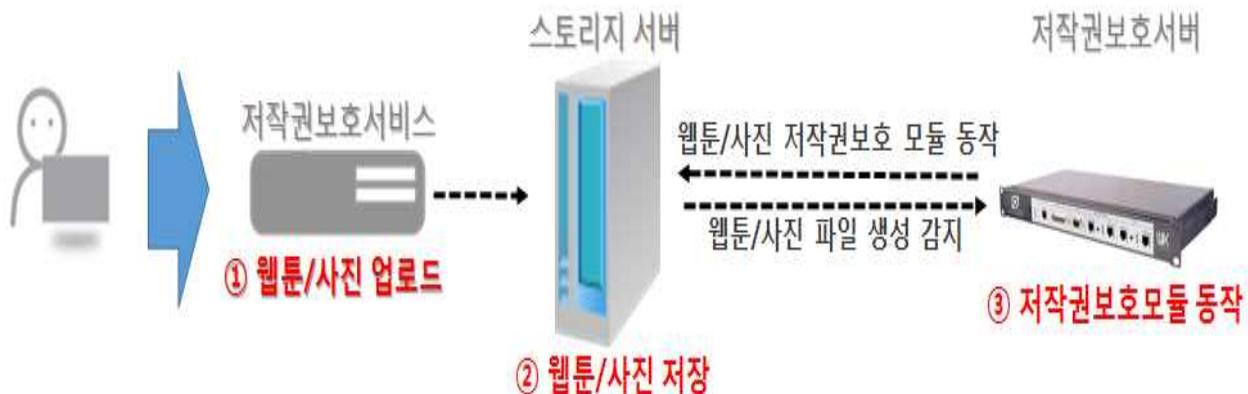
본 제품(시큐워처 for CCTV 영상반출 ver 1.0)은 외부로 반출되는 CCTV 영상의 보호조치를 위한 프로그램이다. 본 제품은 단일 소프트웨어로 구성되며, 영상반출서버(EXV)에 탑재되어 제공된다. 영상반출관리자는 반출영상에 대해 마스킹, 워터마킹, 암호화의 반출영상보호조치 후 CCTV 영상을 반출한다.



[시큐워처 for CCTV 영상반출 ver 1.0 프로그램]

연구개발 3 : 클라우드 기반의 웹툰/이미지 저작권 보호서비스(CaaS) 개발

클라우드 환경에서 스토리지를 제공하여 콘텐츠를 안전하게 보관하고 인증된 콘텐츠를 제공하기 위해 LEA 경량암호기반 콘텐츠 인증 기술을 이용한다. 저장된 콘텐츠는 특징기반 필터링을 응용한 제로정보온닉 기반 콘텐츠 저작권 보호기술을 이용하여 저작권 보호 정보를 은닉함으로 저작권 보호를 제공해줄 수 있는 클라우스 서비스 환경에 적합한 고품질 콘텐츠 제공 서비스로 콘텐츠에 대한 저작권 보호 서비스(CaaS: Copyright protection as a Service)를 개발 중에 있다.



[최종 개발결과물인 클라우드 기반의 웹툰/이미지 저작권 보호 서비스 동작원리]

- S/W 등록 2건

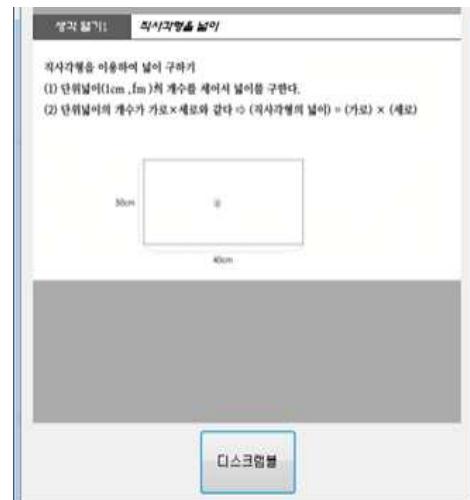
순번	등록번호	제호	등록일자	저작자	발명자
1	C-2016-024826	사물인터넷보안 기반 안전한 양방향 수업진행 솔루션	2016-10-20	경일대학교 산학협력단	윤은준 외 5
2	C-2016-028908	저작권보호 콘텐츠 암복호화를 위한 고속타원곡선암호시스템	2016-11-24	경일대학교 산학협력단	윤은준 외 5

- ① 클라우드 환경을 위한 사물인터넷보안 기반 안전한 양방향 수업진행 솔루션
 스크램블 버튼을 누르면 LEA 경량 암호알고리즘 기반 스마트교육 컨텐츠 픽셀을 1x1 또는 8x8 블록 단위로 스크램블 처리하여 암호화된 스마트교육 컨텐츠를 생성한다. 디스크램블 버튼을 누르면 스크램블된 암호화된 스마트교육 컨텐츠를 가져와 스크램블 시 사용된 키 값을 활용하여 LEA 경량 암호알고리즘 기반 암호화된 스마트교육 컨텐츠 픽셀을 1x1 또는 8x8 단위로 디스크램블 처리한다.

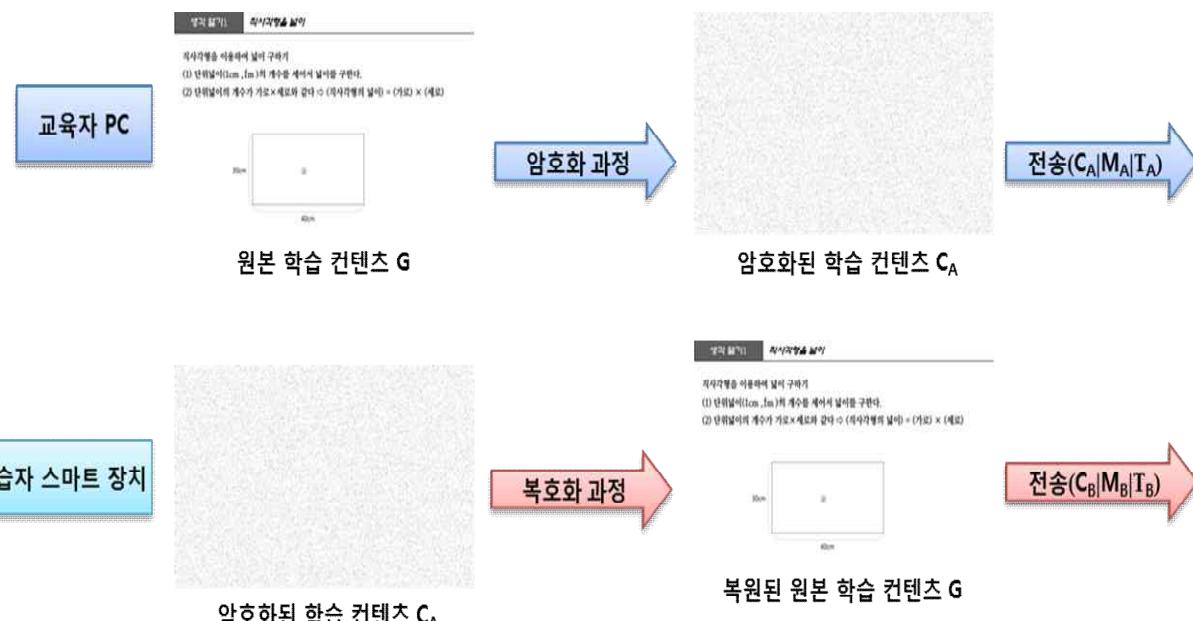
국가연구개발 보고서원문 성과물 전담기관인 한국과학기술정보연구원에서 가공·서비스 하는 연구보고서는 동의 없이 상업적 용도로 사용할 수 없습니다.



[스크램블링 처리 과정]



[디스크램бл링 처리 과정]

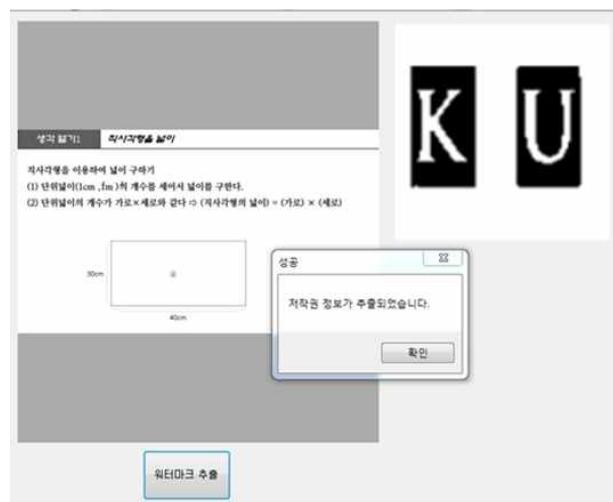


[클라우드 환경을 위한 사물인터넷보안 기반 안전한 양방향 수업진행 솔루션]

저작권 보호를 위한 워터마크 삽입을 위하여 워터마크로 삽입될 이미지를 바이너리 이미지로 변환 시켜야 한다. 버튼을 누를 시 이미지는 흑백 이미지로 변환된다. 워터마크 삽입 버튼을 누를 시 비밀키가 생성되며, 원본 스마트 교육 영상 컨텐츠 I_A 내에 상기에서 소개한 [정보은닉 기반 컨텐츠 위변조 방지 및 저작권보호 알고리즘]기반의 연산을 수행하여 바이너리 워터마크를 삽입된 저작권 보호 컨텐츠 G 를 생성한다. 워터마크 추출 버튼을 누르면 상기에서 소개한 [정보은닉 기반 컨텐츠 위변조 방지 및 저작권보호 알고리즘]기반의 연산을 수행하여 은닉 과정에서 저작권 보호 컨텐츠 G 내에 은닉된 비밀 저작권 보호 정보인 워터마크를 추출하고, 워터마크의 은닉으로 변경된 원본 스마트 교육 영상 컨텐츠 I 를 완벽하게 복원한다.



[바이너리 이미지 변환 및 저작권 정보 읍닉 처리 과정]



[저작권 정보 추출 및 원본 영상 복원 처리 과정]

구현된 아래 [그림]의 제로정보은닉기반 위변조 방지 및 저작권 정보 삽입프로그램으로 저작권 정보를 삽입할 이미지를 불러온 후 특징정보를 추출한다. 추출된 특징정보와 바이너리 이미지를 이용하여 저작권 정보를 삽입하는 프로그램이다. 구현된 아래 [그림]의 제로정보은닉기반 위변조 방지 및 저작권 정보 추출프로그램으로 저작권 정보가 삽입된 이미지를 불러온 후 특징정보를 추출한다. 추출된 특징정보와 저작권정보 삽입과정에서 생성된 키를 이용하여 저작권 정보를 추출하는 프로그램이다.



[제로정보은닉 기반 위변조 방지 및 저작권 정보 삽입 프로그램]



[제로정보은닉 기반 위변조 방지 및 저작권 정보 추출 프로그램]

② 안드로이드 환경을 위한 사물인터넷보안 기반 안전한 양방향 수업진행 솔루션



▶ 안드로이드 통합버전 (PNG)

- ① 왼쪽 화면은 안드로이드 스크램블 PNG 버전 메인화면입니다.
- ② 워터마크 생성 및 삽입버튼을 눌렀을 때화면입니다. 워터마크와 원본이미지와 크기를 맞춘 후에 xor연산을 합니다.
- ③ 이미지 뷰를 통해 워터마크 삽입된 이미지로 출력합니다.
- ④ 아래사진은 워터마크 삽입된 이미지를 스크램블 한 결과입니다.
- ⑤ 디스크램블 한 결과입니다.
- ⑥ 디스크램블된 이미지에서 워터마크를 추출한 결과입니다.

- 특허 출원 4건

출원 특허				
출원/등록일	특허명	출원인	출원국	출원번호
2016/10/07	스마트 교육 시스템에서 교육 콘텐츠 저작권을 보호하기 위한 보안 및 인증 장치, 이를 위한 방법 및 이 방법이 기록된 컴퓨터 판독 가능한 기록매체	윤은준 외 1	대한민국	10-2016-0130 105
2017/01/09	경량암호 알고리즘 기반의 스마트 기기 내의 개인정보 및 콘텐츠 암복호화를 통한 정보 보안 시스템, 이를 위한 방법 및 이 방법을 수행하기 위한 프로그램이 기록된 컴퓨터 판독 가능한 기록매체	윤은준 외 1	대한민국	10-2017-0002 187
2017/01/09	모바일 환경에서 생체 인증 기반 경량 상호 인증 프로토콜을 이용한 정보 은닉 시스템, 이를 위한 방법 및 이 방법을 수행하기 위한 프로그램이 기록된 컴퓨터 판독 가능한 기록매체	윤은준 외 1	대한민국	10-2017-0002 188
2017/01/09	모바일 환경에서 저전력 및 저연산 기반 스마트 콘텐츠 및 개인정보를 보호하기 위한 보안 시스템, 이를 위한 방법 및 이 방법을 수행하기 위한 프로그램이 기록된 컴퓨터 판독 가능한 기록매체	윤은준 외 1	대한민국	10-2017-0002 189

- 클라우드 기반의 웹툰/이미지 저작권 보호서비스(CaaS)를 위한 웹서버 개발

[클라우드 기반의 웹툰/이미지 저작권 보호서비스(CaaS)를 위한 웹서버 개발 내용]

개요

본 문서는 클라우드 기반 저작권 보호기술개발 과제의 시제품 제작을 위한 웹서버 구축 요구사항을 정리한 문서입니다.

개발목표

클라우드 형태의 스토리지 서비스 제공을 위한 웹서버 구축을 목표로 한다.
시제품 형태의 웹서버로 필요기능만 구현한다.

요구기능

- 회원가입
- 회원가입은 아이디와 패스워드, 패스워드확인 입력을 기본적으로 받는다.
- 추가적인 사항으로 등록권리자 정보를 입력받는다.

▶ 신청인 (등록권리자)

성명 (한글)	주식회사우경정보기술		
성명 (한자)			
성명 (영문)			
국적	대한민국 ▾		
주민등록번호 (법인등록번호)	170111 - 0367814	※ 외국인인 경우 외국인등록번호 입력	
우편번호	41519	<input type="button" value="우편번호 찾기"/>	
주소	대구광역시 북구 동북로 117 소프트웨어벤처타워 904호		
전자우편주소	wkit	@	직접입력 ▾ wkit.co.kr
휴대전화 ?	::휴대전화:: ▾	-	
전화번호 (주택) ?	::전화번호:: ▾	-	
전화번호 (회사) ?	053	-	792 - 3031

등록권리자 본인은 다음 중 어디에 해당하십니까?

저작자 본인 ? 공동저작자 ?

명 중 1인

4. 입력받은 데이터는 데이터베이스에 저장된다.
5. 회원가입시 생성한 아이디로 저장공간 할당이 이루어진다.
6. 로그인
7. 로그인을 통해 회원가입시 입력한 아이디와 패스워드로 로그인시 해당 아이디의 최상위 폴더의 파일 리스트가 보인다.
8. 로그아웃
9. 로그아웃시 초기 로그인화면으로 이동한다.
10. 파일업로드
11. 업로드 버튼을 이용하여 단일 파일을 업로드한다.
12. Drag&Drop을 이용하여 파일을 업로드한다.
13. 업로드 가능한 파일은 이미지파일로 한정한다 : 가능한 확장자 bmp, jpg, png
14. 업로드하기 전 폼을 이용하여 저작권정보를 입력한다.

▶ 저작물

The screenshot shows a form for submitting work. It includes fields for the title (제호) containing 'test', the type (종류) set to '미술저작물 > 만화', a search button (검색), a link for work category explanation (저작물 분류 설명), and a date input field for creation date (창작연월일) showing '2017년 1월 1일'.

15. 입력한 데이터는 데이터베이스에 파일제목과 함께 저장된다.
16. 파일다운로드
17. 다운로드 버튼을 이용하여 단일 파일 및 다중파일을 다운로드한다.
18. Drag&Drop을 이용하여 파일을 다운로드한다.
19. 공유
20. 공유버튼을 클릭시 공유 URL을 생성하여 해당 이미지에 대한 접근 URL이 생성된다.
21. 소스코드를 선택시 공유 URL을 이용하여 HTML 태그가 생성된다.

국가연구개발 보고서원문 성과물 전담기관인 한국과학기술정보연구원에서 가공·서비스 하는
연구보고서는 동의 없이 상업적 용도로 사용할 수 없습니다.

- 프로그램 등록 실적 18건 중 8

순번	등록번호	종류	제호	등록일자	저작자
1	C-2017-001597	컴퓨터프로그램 저작물	클라우드 환경에서 경량화암호 기반 콘텐츠 암호화 모듈	2017-01-18	주식회사무경정보기술
2	C-2017-001598	컴퓨터프로그램 저작물	클라우드 환경에서 경량화암호 기반 콘텐츠 복호화 모듈	2017-01-18	주식회사무경정보기술
3	C-2017-001599	컴퓨터프로그램 저작물	특정 기반 저작권 보호 프로그램	2017-01-18	주식회사무경정보기술
4	C-2017-001600	컴퓨터프로그램 저작물	특정 기반 저작권 보호 프로그램	2017-01-18	주식회사무경정보기술

국가연구개발 보고서원문 성과물 전담기관인 한국과학기술정보연구원에서 가공·서비스 하는
연구보고서는 동의 없이 상업적 용도로 사용할 수 없습니다.

- 클라우드 기반 콘텐츠 인증 서비스(LEA 경량화 암호기법 기반의 효율적인 콘텐츠 암복호화 모듈 개발을 위한 SDK 및 솔루션)



[클라우드 기반 콘텐츠 인증 서비스 SDK 및 SW솔루션]



[클라우드 기반 콘텐츠 인증 서비스 SDK 및 SW솔루션]

국가연구개발 보고서원문 성과물 전담기관인 한국과학기술정보연구원에서 가공·서비스 하는
연구보고서는 동의 없이 상업적 용도로 사용할 수 없습니다.

- 클라우드 기반 저작권 보호기술 서비스(클라우드 환경에서 특정기반 필터링 및
제로정보온닉 기반 저작권 보호 및 추출 SDK 및 솔루션)



[클라우드 기반 저작권 보호기술 서비스 SDK 및 솔루션]



[클라우드 기반 저작권 보호기술 서비스 SDK 및 솔루션]

제4장 목표달성도 및 관련분야에의 기여도

제1절 목표달성도

항 목	계 획	실 적	달성도 (%)
개발목표	클라우드 기반의 웹툰/이미지 저작권 보호 시스템인 CaaS 개발을 통해 클라우드환경에서 정지영상에 대한 특징점(DNA) DB를 제공할 뿐만 아니라 저작권보호 및 제공을 목표로 함	클라우드 기반의 웹툰/이미지 저작권 보호 시스템인 CaaS 개발을 통해 클라우드환경에서 정지영상에 대한 특징점(DNA) DB를 제공할 뿐만 아니라 저작권보호 및 제공을 목표로 함	100
기술개발 내용	1. 계획수립 및 자료수집	경량 암호알고리즘 자료수집, 제로 스테가노그래피 정보은닉 기법 자료수집, 클라우드 저작권 보호기술 자료수집	100
	2. 경량 암호 기반 콘텐츠 인증 기술 개발	①저전력, 계산자원을 효율적으로 사용하는 고속의 블록암호모듈이며 경량 환경에서 기밀성을 제공하기 위한 경량의 블록암호 모듈인 LEA 기술 개발 ②LEA 경량고속블록암호 모듈 기반의 경량 상호인증 프로토콜 개발 ③LEA 기반의 경량 암호 알고리즘을 이용한 영상 암복호화 기술 개발 ④LEA 기반의 경량 상호인증 및 키동의 프로토콜을 이용한 보안 인증 기술 개발	100
	3. 클라우드 기반 경량 암호 콘텐츠 인증 서비스 구현	①경량 암호 기반 콘텐츠 인증 기술 개발 ②LEA 경량암호 기반 콘텐츠 암복호화 프로그램 개발	100
	4. 특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술 개발	①카오스 기반의 제로스테가노그래피 기법의 키 생성 모듈 개발 ②제로정보은닉 기반 위변조 방지 및 저작권 정보 삽입 프로그램 개발 ③제로정보은닉 기반 위변조 방지 및 저작권 정보 추출 프로그램 개발	100
	5. 클라우드 기반 저작권 보호기술 서비스 구현	특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호 모듈 개발	100
	6. 클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS) 개발	①경량 암호 기반 콘텐츠 인증 기술 개발 ②클라우드 기반 경량 암호 콘텐츠 인증 서비스 구현 ③특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술 개발 ④클라우드 기반 저작권 보호기술 서비스 구현	100
관련분야 기술발전의 기여도	당초 계획 대비 목표하였던 ①경량 암호 기반 콘텐츠 인증 기술 개발, ②클라우드 기반 경량 암호 콘텐츠 인증 서비스 구현, ③특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술 개발, ④클라우드 기반 저작권 보호기술 서비스 구현 등을 개발 완료하였고, 본 과제에 최적화된 클라우드 환경을 구축하여 클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS) 개발을 통해 실용적이고 안전한 클라우드 저작권 보호기술 개발을 통해 클라우드 콘텐츠 보안 뿐만 아니라 저작권 보호기술의 발전에 큰 기여를 할 수 있다.		

제2절 기술개발의 성과목표 및 지표

성과 항목	성과 지표	당해연도 성과목표	성과달성	달성을 (%)	비고
1. 논문	-비SCI(E) 학술지 게재 논문건수	국 내	2건	2건	100
		국 외	건	1건	초과
	-SCI(E) 학술지 게재 논문건수	국 내	건	건	
		국 외	2건	9건	450
2. 학술대회	-학술대회 발표건수	국 내	4건	23건	575
		국 외	4건	7건	175
3. 포상	-국내외 학회 수상 건수		1건	2건	200
	-정부 및 민간기관으로부터의 포상 건수		건	건	
	-각종 인증 획득 건수		1건	2건(완료1, 진행1)	200 GS 인증
4. 연구 성과확산 노력	-기술개발 관련 홍보건수		4건	5건	125
5. 특허 및 등록	-특허출원 건수	국 내	2건	8건	400
		국 외	건	건	
	-특허등록 건수	국 내	2건	5건	250
		국 외	건	건	
	-실용신안 건수		건	건	
6. 기술거래	-디자인 건수(의장)		건	건	
			4건	18건	450
	-소프트웨어(SW) 등록 건수				
7. 실용화 및 상용화	-기술이전 건수	유 상	1건	2건	200
		무 상	2건	2건	100
	-기술료 수입액		5,000천원	10,000천원	+5,000
8. 산업발전효과	-시제품 출시 건수		1건	2건	200
	-사업화/제품화 건수		1건	1건	100
	-신제품 매출액		10,000천원	10,000천원	100
	-사업화 성공률		90%	90%	100
	-배포 건수		0 건	0 건	
	-현장 시험 건수		0 건	0 건	
	-현장 만족도		0 %	0 %	
9. 기술선진화	-기존시장 확대 기여도		10%	10%	100
	-신시장 창출 기여도		50%	50%	100
10. 산학연협력	-기술수준 향상도		30%	30%	100
	-미래기술 수요에 대한 대처 능력		0 건	0 건	
11. 국제공동연구	-산학연 강좌건수		0 건	0 건	
	-산학연 기술지원 건수		0 건	2 건	초과
12. 표준화	-국제 정보교류 정도		0/0 건/명	0/0 건/명	
			0 건	0 건	
13. 별도 추가 항목	-표준화 건수	국 내	0	0	
		국 외	0	0	
13. 별도 추가 항목	-클라우드 기반 콘텐츠 저작권 보호기술 API 기술 문서		1건	1건	100
	-추가 2		없음	없음	
	-추가 3		없음	없음	

제3절 관련분야에의 기여도

1. 수행 실적(지식재산 및 기술이전, 사업화 등, 2017년 2월말 기준)

구분	논문(건)				학술대회 발표(건)		특허 및 등록(건)				자기실시 (사업화 /제품화) (건)	기술 이전 (건)	매출 현황 (천원)	신규 고용 (명)	표준화 (건)				
	SCI		비 SCI				특허출원		특허등록										
	국내	국외	국내	국외	국내	국외	국내	국외	국내	국외	국내								
당해연도 목표치	-	2	2	-	4	4	2		2		4	1	3	10,000	-	-			
실적	-	9	2	1	23	7	8		5		18	2 (GS인증 완료1,진 행1)	4 (유상2, 무상2)	50,000	3	-			

논문 실적 (건, '16.7 ~ '17.02)

- SCI(E) 9건 (게재4건, 예정5건)

- Alavalapati Goutham Reddy, Ashock Kumar Das, Eun-Jun Yoon, Kee-Young Yoo "An anonymous Authentication with Key-Agreement Protocol for Multi-Server Architecture Based on Biometrics and Smartcards", KSII Transactions on internet and information systems Vol.10, No. 7 pp. 3371-3396, July 31, 2016.
- Alavalapati Goutham Reddy, Eun-Jun Yoon, Ashock Kumar Das, Kee-Young Yoo "Lightweight authentication with key-agreement protocol for mobile network environment using smart cards", IET Information Security Vol.10, Issue. 5 pp. 272-282, Sep, 2016.
- Alavalapati Goutham Reddy, Eun-Jun Yoon, Ashock Kumar Das, Kee-Young Yoo "Erratum: 'Lightweight authentication with key-agreement protocol for mobile network environment using smart cards'", IET Information Security Vol.4, Issue. 5 pp. 283-285, Sep, 2016.
- Alavalapati Goutham Reddy(Student IEEE), Ashock Kumar Das, Eun-Jun Yoon, Kee-Young Yoo(Member IEEE) "A Secure Anonymous Authentication Protocol for Mobile Services on Elliptic Curve Cryptography", IEEE Access Vol. 4 pp. 4394-4407, July 29, 2016.
- Alavalapati Goutham Reddy, Eun-Jun Yoon, Kee-Young Yoo "Comment on 'Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards'", IET Information Security. (게재예정)
- Gil-Je Lee, Eun-Jun Yoon, Cheonshik Kim, Kee-Young Yoo "A real-time secret image sharing with fairness", Journal of Real-Time Image Processing Vol. 12 Issues 45, 2016. (게재예정)
- Dae-Soo Kim, Eun-Jun Yoon, Cheonshik Kim, Kee-Young Yoo "Reversible data hiding scheme with edge-direction predictor and modulo operation", Journal of Real-Time Image Processing Vol. 12 Issues 45, 2016. (게재예정)
- Alavalapati Goutham Reddy, Eun-Jun Yoon, Ashok Kumar Das, Vanga Odelu, and Kee-Young Yoo(Member IEEE) "Design of Mutually Authenticated Key Agreement Protocol Resistant to Impersonation Attacks for Multi-Server Environment", IEEE Access Vol. x pp. xxxx-xxxx, 2017. (게재예정)
- Sravani Challa, Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, Alavalapati Goutham Reddy, Eun-Jun Yoon, and Kee-Young Yoo(Member IEEE) "ASecure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications", IEEE Access Vol. x pp. xxxx-xxxx, 2017. (게재예정)

- 비SCI 국내 1건(등재지 게재 1건)

- 김혜정, 윤은준, "악성코드로부터 빅데이터를 보호하기 위한 이미지 기반의 인공지능 딥러닝 기법," 대한전자공학회국
문논문지, 전자공학회 논문지 제 54 제 2호 (2017년 2월 25일), pp. 246-252, 2017.

- 비SCI (1건)

- Anneke Soraya Hidayat, Gil-Je Lee, Eun-Jun Yoon and Kee-Young Yoo, "An in-depth analysis of strong t-consistency on secret image sharing," International Journal of Pervasive Computing and Communications, Vol. 12, Issue.1, pp. 107-126, 2016

학술대회 실적 (30건)

- 국외학술대회 (발표7건)

1. Goutham Reddy Alavalapati, Eun-Jun Yoon, Ashok Kumar Das, Kee-Young Yoo, "An Enhanced Anonymous Two-factor Mutual Authentication with Key-agreement Scheme for Session Initiation Protocol" SIN 2016 9th International Conference on Security of Information and networks, ACM, pp. 145-149, New Jersey, USA, July 20-22, 2016.
2. Anneke Soraya Hidayat, Dae-soo Kim, Eun-Jun Yoon, Kee-Young Yoo, "A new Group-based Secret Function Sharing with Variate Threshold" SAM 2016 International Conference. Security and Management , ACM, pp. 313-317, Las Vegas, USA, July 25-28, 2016.
3. Goutham Reddy Alavalapati, Eun-Jun Yoon, Young-Ju Kim, Kee-Young Yoo, "Design of A Secure Mutual Authenticated Key-Agreement Protocol for Multi-Server Architecture" ICICA 2017 6th International Conference on Intelligent Computing and Applications, IACSIT, pp. xxx-xxx, Canberra, Australia, January 20-23, 2017.
4. Kwang-Yeol Jung, Dae-Soo Kim, Young-Ju Kim, Kee-Young Yoo, "Improved Reversible Data Hiding Scheme using Weighted Matrix with Overlapping" ICCT2017, International Conference on Cultural Technology, IACST, pp. xxx-xxx, Chiang Mai, Thailand, January 12-14, 2017.
5. Anneke Soraya Hidayat, Rosemary Koikara, Pyung-Han Kim, Kee-Young Yoo, "Application of Biometric Key in Practical Secret Sharing for DNSsec" ICCT2017, International Conference on Cultural Technology, IACST, pp. xxx-xxx, Chiang Mai, Thailand, January 12-14, 2017.
6. Kwang-Yeol Jung, Eun-Jun Yoon, Kee-Young Yoo, "Analysis and Improvement of Jana's High Payload Reversible Data Hiding Scheme using Weighted Matrix" ICGHIT2017, International Conference on Green and Human Information Technology, IEIE/IEEE, pp. xxx-xxx, Hangzhou, China, Feb. 15-17, 2017.
7. Young-Ju Kim, Eun-Jun Yoon, Kee-Young Yoo, "Comments on Nguyen-Chang's Reversible Data Hiding Scheme based on Sudoku Technique" ICGHIT2017, International Conference on Green and Human Information Technology, IEIE/IEEE, pp. xxx-xxx, Hangzhou, China, Feb. 15-17, 2017.

- 국내학술대회 (발표23건)

1. Alavalapati Goutham Reddy, 윤은준, 유기영, "Mishra 등이 제안한 스마트카드를 사용한 생체기반 멀티서버 인증된 키 동의 프로토콜의 보안 취약점 분석" 2016년 의료전자융합 공동 워크샵, 학술대회, 경상북도 구미시 구미코 대회의실, pp. 85-86, 2016.
2. 정광열, Rosemary Koikara, 윤은준, 유기영, "기중치 행렬을 이용한 의료영상 서비스 환경의 정보 은닉 기법에 대한 연구." 2016년 의료전자융합 공동 워크샵, 학술대회, 경상북도 구미시 구미코 대회의실, pp. 87-88, 2016.
3. 김평한, 김대수, 윤은준, 유기영, "이중 이미지 기반의 가역 정보 은닉 기법을 이용한 의료영상 보안에 관한 연구." 2016년 의료전자융합 공동 워크샵, 학술대회, 경상북도 구미시 구미코 대회의실, pp. 91-93, 2016.
4. 김영주, 서경윤, 윤은준, 유기영, "스도쿠 기술에 기반한 의료 영상에 대한 가역 정보 은닉 기법 연구." 2016년 의료전자융합 공동 워크샵, 학술대회, 경상북도 구미시 구미코 대회의실, pp. 89-90, 2016.
5. 권시현, 윤은준, "임베디드 플랫폼을 위한 그래피컬 패스워드 인증 스킴의 보안 취약점 분석과 개선." 2016년 의료전자융합 공동 워크샵, 학술대회, 경상북도 구미시 구미코 대회의실, pp. 78-81, 2016.
6. 김영주, 윤은준, 유기영, "스도쿠와 비밀 공유를 이용한 가역 정보 은닉 기법 연구" 대한전자공학회 주관 2016년도 융합/스마트/클라우드 컴퓨팅 학술대회, pp. 8-9, 10월 15일, 2016.
7. 정광열, 김대수, 윤은준, 유기영, "비밀 공유 기법에 기반한 실용적인 랩탑 정보 보호 기법에 대한 연구" 대한전자공학회 주관 2016년도 융합/스마트/클라우드 컴퓨팅 학술대회, pp. 16-17, 10월 15일, 2016.
8. 김해니, 백광민, 윤은준, "ColorLogin 기법의 보안성 분석" 대한전자공학회 주관 2016년도 융합/스마트/클라우드 컴퓨팅 학술대회, pp. 28-30, 10월 15일, 2016.
9. 서경윤, 윤은준, 유기영, "적용 가능한 히스토그램 이동과 픽셀 값 분류를 이용한 가역 정보 은닉과 이미지 대비 향상 기법에 대한 연구" 대한전자공학회 주관 2016년도 융합/스마트/클라우드 컴퓨팅 학술대회, pp. 45-47, 10월 15일,

2016.

10. 김평한, 윤은준, 유기영, “PRESENT 블록 암호에 대한 키 관리 방법” 대한전자공학회 주관 2016년도 융합/스마트/클라우드 컴퓨팅 학술대회, pp. 71-73, 10월 15일, 2016.
11. 권시현, 윤은준, “안전한 스마트 식물농장 시스템 설계 및 구현” 대한전자공학회 주관 2016년도 융합/스마트/클라우드 컴퓨팅 학술대회, pp. 82-85, 10월 15일, 2016.
12. 최세호, 윤은준, “아두이노 기반 스마트 홈 시큐리티 시스템 설계 및 구현” 대한전자공학회 주관 2016년도 융합/스마트/클라우드 컴퓨팅 학술대회, pp. 90-93, 10월 15일, 2016.
13. 윤은준, “서비스 거부 공격에 강인한 클라우드 기반 안전한 인증(CSA) 프로토콜의 보안 취약점 분석” 2016년도 대한전자공학회 추계학술대회, pp. 1134-1137, 11월 25일~26일, 2016.
14. 권시현, 윤은준, “원형 암호 공간을 이용한 그레피컬 패스워드 인증 스킴의 보안 취약점 분석과 개선” 2016년도 대한전자공학회 추계학술대회, pp. 1138-1141, 11월 25일~26일, 2016.
15. 김영주, 윤은준, 유기영, “저작권 보호 응용을 위한 더욱 개선된 스도쿠와 비밀 공유 기반 가역 정보 은닉 스킴” 2016년도 대한전자공학회 추계학술대회, pp. 1142-1144, 11월 25일~26일, 2016.
16. 서경윤, 윤은준, 유기영, “카오톡 맵을 활용한 저작권 정보 삽입 및 추출에 대한 연구” 2016년도 대한전자공학회 추계학술대회, pp. 1131-1133, 11월 25일~26일, 2016.
17. 김평한, 윤은준, 유기영, “LEA 기반의 컨텐츠 암복호화 기법을 적용한 저작권 보호 시스템” 2016년도 대한전자공학회 추계학술대회, pp. 1113-1115, 11월 25일~26일, 2016.
18. 정광열, Rosemary Koikara, 윤은준, 유기영, “가중치 행렬을 이용한 정보 은닉 스킴 기반 저작권 보호 기술 개선에 관한 연구” 2016년도 대한전자공학회 추계학술대회, pp. 1119-1121, 11월 25일~26일, 2016.
19. 최세호, 윤은준, “클라우드 기반 스마트 홈 서비스 환경에서의 상호인증 및 디지털 컨텐츠 저작권보호 기술” 2016년도 대한전자공학회 추계학술대회, pp. 1116-1118, 11월 25일~26일, 2016.
20. 남주호, 전지원, 윤은준, “안전한 컨텐츠 보호를 제공하는 스마트 헬스케어 시스템 설계 및 구현” 2016년도 대한전자공학회 추계학술대회, pp. 1122-1124, 11월 25일~26일, 2016.
21. 윤은준, “클라우드 환경에서의 모바일 기기를 활용한 안전한 저작권보호 컨텐츠 업로드 스킴” 2016년도 대한전자공학회 추계학술대회, pp. 1125-1126, 11월 25일~26일, 2016.
22. 서경윤, 김대수, 윤은준, 유기영, “평균값에 기반한 암호화된 이미지의 가역정보은닉 기법에 관한 연구” 2017년도 한국통신학회 동계종합학술발표회, pp. 957-958, 1월 18일~20일, 2017.
23. 정준민, 김평한, 정광열, 윤은준, 유기영, “LEA 경량 블록 암호에 대한 키 관리 방법” 2017년도 한국통신학회 동계종합학술발표회, pp. 959-960, 1월 18일~20일, 2017.

특허 및 등록 실적 (13건)

- 특허출원 (8건)

1. 제로널리지 기반의 영상 위변조 방지와 탐지를 위한 워터마킹 삽입과 추출 장치 및 그 방법, 주식회사우경정보기술, 박윤하, 제 10-2016-0030088호
2. 보행자의 얼굴 검출 기반의 동적 객체 영상 프라이버시 보호 장치 및 그 방법, 주식회사우경정보기술, 박윤하, 제 10-2016-0030090호
3. 스마트 교육 시스템에서 교육 컨텐츠 저작권을 보호하기 위한 보안 및 인증 장치, 이를 위한 방법 및 이 방법이 기록된 컴퓨터 판독 가능한 기록매체, 윤은준, 제 10-2016-0130105호
4. 경량 암호 알고리즘 기반의 저작권 보호를 위한 컨텐츠 송수신 장치, 이를 위한 방법 및 이 방법이 기록된 컴퓨터 판독 가능한 기록매체, 윤은준, 제 10-2016-0133728호
5. 가역 정보 은닉 기반의 컨텐츠 위변조 방지를 위한 저작권 보호 장치, 이를 위한 방법 및 이 방법이 기록된 컴퓨터 판독 가능한 기록매체, 윤은준 외 2명, 제 10-2016-0133734호
6. 경량암호 알고리즘 기반의 스마트 기기 내의 개인정보 및 컨텐츠 암복호화를 통한 정보 보안 시스템, 이를 위한 방법 및 이 방법을 수행하기 위한 프로그램이 기록된 컴퓨터 판독 가능한 기록매체, 윤은준 외 1명, 제

10-2017-0002187호

7. 모바일 환경에서 생체 인증 기반 경량 상호 인증 프로토콜을 이용한 정보 은닉 시스템, 이를 위한 방법 및 이 방법을 수행하기 위한 프로그램이 기록된 컴퓨터 판독 가능한 기록매체, 윤은준 외 1명, 제 10-2017-0002188호
8. 모바일 환경에서 저전력 및 저연산 기반 스마트 콘텐츠 및 개인정보를 보호하기 위한 보안 시스템, 이를 위한 방법 및 이 방법을 수행하기 위한 프로그램이 기록된 컴퓨터 판독 가능한 기록매체, 윤은준, 제 10-2017-0002189 호

- 특허등록 (5건)

1. 개별 객체 프라이버시 보호를 위한 영상 처리 장치, 이를 위한 방법 및 이 방법이 기록된 컴퓨터 판독 가능한 기록매체, 경일대학교 산학협력단 외 1명, 윤은준, 박윤하, 특허 제 10-1648188호 (2016/08/08)
2. 환경 변화에 따른 프라이버시 보호를 위한 동적 객체 영상 처리 시스템, 이를 위한 방법 및 이 방법이 기록된 컴퓨터 판독 가능한 기록매체, 경일대학교산학협력단, 윤은준, 특허 제 10-1648190호 (2016/08/08)
3. 손동작 인식을 이용한 접근 제어 시스템, 이를 위한 방법 및 이 방법이 기록된 컴퓨터 판독 가능한 기록매체, 경일대학교산학협력단, 윤은준, 특허 제 10-1656212호 (2016/09/15)
4. 제로널리지 기반의 영상 위변조 방지와 탐지를 위한 워터마킹 삽입과 추출 장치 및 그 방법, 주식회사우경정보기술, 박윤하, 제 10-1677110-00-00호 (2016/11/11)
5. 보행자의 얼굴 검출 기반의 동적 객체 영상 프라이버시 보호 장치 및 그 방법, 주식회사우경정보기술, 박윤하, 제 10-1677111-00-00호 (2016/11/11)

- 프로그램등록 (등록18)

1. JPEG 영상전용 컨텐츠 암호화 프로그램 (C-2016-023709, 2016.10.06)
2. 카오스 알고리즘 기반 컨텐츠 암호화를 위한 서버전용 프로그램 (C-2016-023712, 2016.10.06)
3. 안드로이드 환경을 위한 JPEG 영상전용 컨텐츠 암호화 프로그램 (C-2016-024828, 2016.10.20)
4. 안드로이드 환경을 위한 카오스 알고리즘 기반 컨텐츠 암호화 프로그램 (C-2016-024832, 2016.10.20.)
5. JPEG 영상전용 컨텐츠 복호화 프로그램 (C-2016-023708, 2016.10.06)
6. 카오스 알고리즘 기반 컨텐츠 복호화를 위한 서버전용 프로그램 (C-2016-023712, 2016.10.06)
7. 안드로이드 환경을 위한 JPEG 영상전용 컨텐츠 복호화 프로그램 (C-2016-024827, 2016.10.20)
8. 안드로이드 환경을 위한 카오스 알고리즘 기반 컨텐츠 복호화 프로그램 (C-2016-024831, 2016.10.20)
9. 안드로이드 환경을 위한 스테가노그래피 기반 컨텐츠 위변조 방지 및 저작권 정보 은닉 프로그램 (C-2016-023711, 2016.10.06)
10. 스테가노그래피 기반 컨텐츠 위변조 방지 및 저작권 정보 은닉 프로그램 (C-2016-024830, 2016.10.20)
11. 안드로이드 환경을 위한 스테가노그래피 기반 컨텐츠 위변조 방지 및 저작권 정보 추출검증 프로그램 (C-2016-023710, 2016.10.06)
12. 스테가노그래피 기반 컨텐츠 위변조 방지 및 저작권 정보 추출검증 프로그램 (C-2016-024829, 2016.10.20.)
13. 사물인터넷보안 기반 안전한 양방향 수업진행 솔루션 (C-2016-024826, 2016.10.20.)
14. 저작권보호 콘텐츠 암복화를 위한 고속 타원곡선암호시스템 (C-2016-028908, 2016.11.24.)
15. 클라우드 환경에서 경량화암호 기반 콘텐츠 암호화 모듈 (C-2017-001597, 2017.01.31.)
16. 클라우드 환경에서 경량화암호 기반 콘텐츠 복호화 모듈 (C-2017-001598, 2017.01.31.)
17. 특징 기반 필터링을 이용한 저작권 보호기술 모듈 (C-2017-001599, 2017.01.31.)
18. 특징 기반 필터링을 이용한 저작권 추출기술 모듈 (C-2017-001600, 2017.01.31.)

신규 인력 채용 실적(3명)

1. (주)우경정보기술에서 영상정보보호 분야 개발자 “문지민”외 2명 채용

자기실시(사업화/제품화)(GS인증 2건)

1. GS인증 신청(GS인증완료1,진행1) ((주)우경정보기술 시큐워처 2개 부문 GS인증을 9월 27일 신청 및 진행)
 - 시큐워처 for CCTV 영상보안 v1.0 (인증완료)
 - 본 과제에서 개발한 LEA 경량암호 기반의 암복호화와 인증 모듈을 이용한 영상 보안 S/W
 - 시큐워처 for CCTV 영상반출 v1.0 (진행)
 - 본 과제에서 개발한 제로정보온닉 기반 저작권보호 및 추출 모듈을 이용한 영상 저작권보호 S/W

기술이전(4건, 유상2/무상2)

1. 대경기술지주 및 연구개발특구진흥재단을 통한 연구소기업 설립을 위한 협약출자용 특허(얼굴 인식 기반 프라이버시 보호를 위한 영상 처리 장치, 이를 위한 방법 및 이 방법이 기록된 컴퓨터 판독 가능한 기록매체(특허등록번호 제 10-1621723호)") 기술이전(유상1건, 31백만원, 2016.10.13)
2. (주)우경정보기술에서 본 사업 연계 총 3건(유상1건/무상2건)의 기술이전 추진 중

매출현황(천원)

1. (주)우경정보기술에서 본 사업 연계 매출 50,000(천원) 발생

기타 실적

1. 기술개발 관련 홍보건수 (5건)

- [보안·IT산업 동향] 우경정보기술, 영상정보보안 '시큐워처 for CCTV' 공개 외
 - 보안뉴스, <http://www.boannews.com/media/view.asp?idx=51228>
- [이슈&컴퍼니] 영상정보보안 분야 대표주자, 우경정보기술
 - 보안뉴스, http://www.boannews.com/media/view.asp?idx=51544&kind=3##target=_blank
- 중구난방 CCTV 컨드롤타워 역할론…자산관리솔루션 뜬다
 - 아주경제, <http://www.ajunews.com/view/20160906131905108>
- [이코노피플] 박윤하 (주)우경정보기술 대표
 - 매일신문, http://www.imaeil.com/sub_news/news_print.php?news_id=34456&yy=2016

2. 두바이 정보통신박람회(GITEX 2016) 참가 및 저작권보호 솔루션 전시 홍보 마케팅 (2개 솔루션)

- 제로스테가노그래피 솔루션 및 영상 암호 솔루션을 기반으로 한 시큐워처 제품을 두바이정보통신박람회(GITEX 2016)에 전시함 (2016.10.16 ~ 20, 두바이, 아랍에미레이트)
- 클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS) 기술에 관한 홍보 마케팅 진행함

3. 기술개발 관련 학술대회 개최 및 참가 (3건)

- 2016년도 대한전자공학회 주관 융합스마트/클라우드 컴퓨팅 학술대회를 과제 책임자가 직접 개최함
 - 2016년 10월 15일(토), 대구 팔공산 평산아카데미 연수원에서 40여편의 논문 발표 및 관련 전문가 간담회 개최 예정임
- ISEC 2016(제10회 국제 사이버 시큐리티 컨퍼런스) 참가 및 저작권보호 솔루션 전시 홍보 마케팅
 - 2016년 10월 15일(토), 대구 팔공산 평산아카데미 연수원에서 40여편의 논문 발표 및 관련 전문가 간담회 개최 예정임
- 차세대 콘텐츠보안 기술 워크샵 개최
 - 2016년도 대한전자공학회 추계 학술대회에서 과제 책임자가 차세대 콘텐츠보안 기술 워크샵을 직접 개최하여 관련 주제의 10여편의 논문 발표 및 3인(ETRI, KETI, 제주대)의 전문가 초청 특강 진행 (2016. 11. 26, 대구 EXCO, 대한민국)

제5장 기술개발결과의 활용계획

본 과제의 결과물인 클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS) 개발로 사업화 뿐만 아니라 세부 목표인 경량 암호 기반 콘텐츠 인증기술과 특징기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술을 응용하여 사업화를 진행할 계획에 있다.

본 결과물의 사업화 전략은 다음과 같다.

사업화 가능 아이템 명	사업화 유형	결과물 Type	형태	예상시기
경량 암호 기반 콘텐츠 인증 기술	기술이전	요소기술	SW	‘16. 10
특징 기반 필터링을 응용한 제로정보은닉 기반 콘텐츠 저작권 보호기술	기술이전	요소기술	SW	‘16. 12
클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS) 개발	자체사업화	제품	SW-System	‘17. 03

본 과제의 결과물인 클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS)의 사업화를 위하여 최종결과물을 이용하여 솔루션 개발을 통해 저작권 보호서비스 형태로 클라우드 업체에 콘텐츠 보안 솔루션으로 제공할 것이며, 클라우드 서버 구축후 자체 서비스를 개시하여 개인이나 중소기업의 콘텐츠를 대상으로 시범사업을 진행하여 국내 클라우드 저작권 시장 개척을 할 것이다. 향후 저작권 위원회와 연계하여 콘텐츠 저작권보호 서비스를 저작권위원회에 제공하여 현 시스템에서 보다 효율적인 저작권보호 시스템을 구축하고, 향후 국내 뿐만 아니라 국외 클라우드 업체 및 포털사이트를 연계하여 저작권 시장을 선도해 나갈 것이다.

본 결과물의 향후 사업화 추진일정은 다음과 같다.



1. 활용방안

가. 활용분야 및 활용방법

- 본 과제의 결과물을 이용하여 기존 클라우드 서비스에 추가적으로 웹툰/이미지 저작권 보호 서비스(CaaS)를 제공할 수 있어 기존 시장을 활용한 시장 가치확대, 저작권 관련 산업의 안정적 기반 조성 및 육성을 유발함
- 개인 및 영세·중소기업을 대상으로 클라우드 스토리지 서비스를 제공하면서 콘텐츠에 대한 저작권 보호를 제공함으로 클라우드 저작권 관련 시장을 선점 및 시장가치를 확대할 기반 핵심 기술들을 갖추게 됨
- 본 과제를 통해 확보된 원천 기술들의 로열티(royalty)를 받고 역수출 하는 등의 기술 수입 대체 효과 유발
- 본 과제의 결과물은 향후 웹툰/이미지 뿐만 아니라 영상, 문서, 음악 등의 다양한 콘텐츠에 활용가능함으로 전반적인 콘텐츠에 대한 저작권 보호를 하여 불법 콘텐츠에 의한 경제적인 손실을 최소화 할 수 있음

나. 활용상 예상 문제점 및 극복방안

- 기존 선점하고 있는 클라우드 업체에 대한 서비스 제공을 선택사항이 아닌 저작권 관련 법안 통과 및 제정으로 인한 클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS) 제공
- 저작권위원회를 통한 개인 및 영세·중소기업대상의 클라우드 기반의 웹툰/이미지 저작권 보호 서비스(CaaS) 제공을 위한 홍보 및 저작권에 대한 교육
- 국외 CaaS 제공을 위해 해당 국가의 저작권법에 맞춰 서비스 모듈 변경

2. 기대성과

가. 기술적 성과

- 본 과제의 연구내용은 기준에 구축되어있는 클라우드 관련 기술들이 가지는 다양한 저작권 문제점을 해결하며 클라우드 기반 저작권 기술에 관한 최근 연구를 보다 발전시켜 안전성 및 효율성 보장은 물론 실용성을 가지는 강력한 웹툰/이미지 저작권 보호 서비스(CaaS) 제공으로 차세대 클라우드 시스템 개발 및 구축을 목표로 함으로 해당 기술 개발 및 기술확보는 클라우드 산업 뿐만아니라 저작관 산업 발전을 위해 반드시 고려되어야함
- 본 연구결과를 토대로한 클라우드 기반 웹툰/이미지 저작권 보호 서비스(CaaS) 응용 및 활용을 유도하여 한층 강화된 저작권 보호 서비스 표준화 제정으로 인한 개선된 콘텐츠 저작권 보호 서비스(CaaS) 기술 개발 및 판매를 할 수 있으며 기술검증과 이전을 통한 해당 산업체의 기술가치 향상 및 국내 클라우드 및 저작권 산업의 전반적인 발달을 가져옴
- 클라우드 기반 웹툰/이미지 저작권 보호 서비스(CaaS)에 대한 원천기술 확보로 웹툰/이미지에 한정되지 않은 다양한 콘텐츠에 응용 및 추가개발을 통해 기술적 경쟁력을 갖춤
- 클라우드 기반 콘텐츠 저작권 보호 서비스(CaaS)를 전세계 최초로 개발함으로 국제 및 국내 표준제정에 기여함으로 기술에 개발 및 시장도입에 유리함

나. 경제·산업적 성과

- 클라우드 기반 콘텐츠 저작권 보호 서비스(CaaS)는 개발이 전무한 상태이므로 시장 형성 초기에 본 개발로 인하여 높은 시장성을 선점할 수 있을 것이다.
- 국내·외에 서비스하고 있는 클라우드 업체를 대상으로 콘텐츠 저작권 보호 서비스(CaaS)를 제공해 줌으로 새로운 클라우드를 구축하여 서비스하는 것보다 추가적인 서비스 토입으로 저비용 고효율의 저작권 보호를 제공하는 것으로 해당 시장의 위험도를 낮출 수 있다.
- 콘텐츠 저작권 보호 서비스(CaaS) 개발과 관련하여 국가적 차원의 중장기적 표준 기술 개발과 국내 산업과 국제 기술과의 연계 역할을 통해 국내 실용적인 CaaS 활용에 따른 e-비즈니스 산업의 국제화 및 정부 3.0의 Creative-Korea 실현에 기여

제6장 기술개발과정에서 수집한 해외과학기술정보

제1절 경량암호 기술

2012년 ISO/IEC 29192-2[15]에서 경량화 블록 암호인 PRESENT[16]와 CLEFIA가 제정되었다. PRESENT는 64bits의 블록크기와 80/128bits의 키길이를 가진다. CLEFIA는 소니사에서 개발된 경량화 블록 암호 기법으로 자사 DRM 시스템에서 주로 사용된다. 128bits의 블록크기와 128/192/256bits의 키길이를 가진다. 경량화 암호는 동일한 키길이를 사용함으로 동일 레벨의 보안을 제공하면서 알고리즘을 단순화함으로 빅데이터, 클라우드, 모바일과 같은 환경에 적합하다.

1. PRESENT 경량 암호

- 가. PRESENT는 64bits의 블록크기와 80/128bits의 키길이를 가진다.
- 나. PRESENT는 동일한 키길이를 사용함으로 동일 레벨의 보안을 제공하면서 알고리즘을 단순화함으로 기존의 DES와 AES보다 3배정도 빠른 암호 기술이다.

2. CLEFIA 암호

- 가. 128bit 블록크기, 128/192/256 bit 키길이
- 나. Sony에서 개발되어 자사 DRM 시스템에서 사용됨. 널리 상용되어 사용되어지지는 않음

제2절 정보은닉 기술

1. 정보은닉 기법은 제 3자가 디지털 컨텐츠에 비밀정보를 삽입된 것을 알지 못하게 비밀정보를 디지털 컨텐츠에 삽입하는 방법이다[17].
2. 주로 이미지와 동영상 분야에서 다양한 연구가 이루어지고 있다. 이러한 정보은닉 방법을 이용하여 영상 정보의 인증, 데이터 무결성의 정보보호 서비스를 제공할 수 있다.
3. 디지털 이미지에서의 정보은닉 기법은 정보를 삽입할 때 원본 이미지(cover-image)의 픽셀의 변경으로 인하여 비밀 정보가 삽입된 스테고 이미지(stego-image)의 왜곡이 발생하게 된다. 이러한 문제점을 해결하기 위해 삽입된 정보를 추출하는 과정에서 원본 이미지도 복원 할 수 있는 가역 정보 은닉 기법(reversible data hiding)이 많이 연구된다.
4. 가역정보은닉 기법에는 히스토그램이동기법과 차이값 확장 기법으로 크게 나누어진다.
5. 보다 많은 양의 비밀정보를 왜곡이 적게 발생시키면서 삽입하는 연구방향으로 진행되어진다.
6. 최근에는 제로정보은닉기법을 통해 이미지의 왜곡없이 비밀정보를 삽입하고 추출한다.

제7장 참고문헌

- [1] 최찬호, 최윤희, 엄현상, 엄현영, “클라우드 스토리지 시스템에 대한 연구”, 한국정보과학회 학술발표논문집, 2012.11
- [2] 김민전, 박성갑, 권호열, “클라우드 스토리지 서비스의 신뢰성 확보를 위한 데이터보호 모델에 관한 연구”, 대한전자공학회 학술대회, 2012.11
- [3] 신경아, 이상진, “클라우드 컴퓨팅 서비스에 관한 정보보호관리체계”, 한국정보보호학회, 정보보호학회논문지 22(1), 2012.2, 155-167
- [4] 유우영, 임종인, “클라우드 컴퓨팅 서비스 제공자의 개인정보보호 조치 방안에 대한 연구”, 한국정보보호학회, 정보보호학회논문지 22(2), 2012.4, 337-346
- [5] 전정훈, “클라우드 컴퓨팅 보안의 취약성에 관한 연구”, 한국정보보호학회, 정보보호학회 논문지 23(6), 2013.12, 1239-1246
- [6] 최상필, “클라우드 컴퓨팅 환경에서 제공되는 서비스의 저작권적 문제”, 동아대학교 법학 연구소, 동아법학 55, 2012.5, 325-342
- [7] 김태형, 김인혁, 민창우, 엄영익, “클라우드 컴퓨팅 보안 기술 동향”, 한국정보과학회, 정보과학회지 30(1), 2012.1, 30-38
- [8] D. Hong, J.-K. Lee, D.-C. Kim, D. Kwon, K.H. Ryu, and D.-G. Lee, ‘LEA: A 128-bit block cipher for fast encryption on common processors’, Proc. of WISA 2013, LNCS, vol. 8269, 2014.
- [9] J. Park et al., “128-Bit Block Cipher LEA”, TTAK.KO-12.0223, 2013.12
- [10] 박제홍, ‘128비트 블록 암호 LEA’, TTA Journal Vol. 157, 2015.01.02.
- [11] Li C T. An enhanced remote user authentication scheme providing mutual authentication and key agreement with Smart Cards. The 5th International Conference on Information Assurance and Security, Xi , a` ran: IEEE Computer Society, 2009: 517-520.
- [12] Hwang M S, Liu C Y. Authenticated encryption schemes: Current status and key issues. International Journal of Network Security, 2005, 1(2): 61-73.
- [13] Kim M, Koc C K. A simple attack on a recently introduced hash-based strong-password authentication scheme. International Journal of Network Security, 2005, 1(2): 77-80.
- [14] Lee N Y, Chiu Y C. Improved remote authentication scheme with smart card. Computer Standards and Interfaces, 2005, 27(2): 177-180.
- [15] ISO/IEC, Information technology Security techniques Lightweight cryptography Part 2: Block ciphers, ISO/IEC 29192-2:2012
- [16] A Bogdanov, L Knudsen, G Leander, and C Paar. “PRESENT: An ultralightweight block cipher”, Systems-CHES, 2007.
- [17] A. Cheddad, J. Condell, K. Curran and P.M. Kevitt. “Digital image steganography: survey and analysis of current methods.” Signal Processing Journal. 90(3), pp. 727-752. Aug. 2011.

국가연구개발 보고서원문 성과물 전담기관인 한국과학기술정보연구원에서 가공·서비스 하는
연구보고서는 동의 없이 상업적 용도로 사용할 수 없습니다.

주 의

1. 이 보고서는 문화체육관광부에서 시행한 저작권기술개발사업의 연구보고서입니다.
2. 이 보고서 내용을 발표하는 때에는 반드시 문화체육관광부에서 시행한 사업의 연구결과임을 밝혀야 합니다.
3. 국가과학기술 기밀유지에 필요한 내용은 대외적으로 발표 또는 공개하여서는 아니됩니다.