http://dx.doi.org/10.15207/JKCS.2015.6.6.185

집단지성 콘텐츠에 적합한 저작권 인증 기법

윤성현[1*], 이근호[1], 임희석[2], 김대룡[3], 김정훈[4]
[1]백석대학교 정보통신학부, [2]고려대학교 컴퓨터공학과,
[3]미국 델라웨어주립대학교 경상학과, [4]영남대학교 새마을국제개발학과

The Method of Digital Copyright Authentication for Contents of Collective Intelligence

Sunghyun Yun[1*], Keunho Lee[1], Heuiseok Lim[2], Daeryong Kim[3], Jung-hoon Kim[4]
[1]Division of Information and Communication Engineering, Baekseok University
[2]Dept. of Computer Science and Engineering, Korea University
[3]Dept. of Business, Delaware State University, USA
[4]Dept. of Saemaeul Studies and International Development, Youngnam University

요 약 지혜 콘텐츠는 사람의 경험과 아이디어로 구성된다. 지혜 마켓은 [1] 지혜 콘텐츠를 거래하는 온라인 상거래 모델로 일반인들도 쉽게 경제 활동에 참여할 수 있다. 지혜 콘텐츠는 그 자체가 사람의 생각이기 때문에 유사하거나 중복된 콘텐츠가 많이 존재하게 된다. 기존의 저작권 보호 기법은 주로 원저자의 권리 보호에 초점을 맞추고 있다. 집단지성 콘텐츠는 여러 사람의 도움으로 만들어진 콘텐츠이기 때문에 개별 저작권을 통합 및 제거할 수 있는 동적인 저작권 보호 기법이 요구된다. 본 논문에서는 집단지성 콘텐츠에 적합한 집단 저작권 인증 기법을 제안한다. 제안한 기법은 집단 저작권 등록, 추가 그리고 검증 프로토콜로 구성된다. 유사한 콘텐츠를 통합하거나 또는 개별 콘텐츠에 대한 집단 권리가 필요한 다양한 비즈니스 모델에 적용할 수 있다.

• **주제어** : 집단지성, 콘텐츠 보호, 저작권 보호, 집단 저작권, 저작권 관리

Abstract The wisdom contents consists of an ordinary person's ideas and experience. The Wisdom Market [1] is an online business model where wisdom contents are traded. Thus, the general public could do business activities in the Wisdom Market at ease. As the wisdom contents are themselves the thought of persons, there exists many similar or duplicated contents. Existing copyright protection schemes mainly focus on the primary author's right. Thus, it's not appropriate for protecting the contents of Collective Intelligence that requires to protect the rights of collaborators. There should exist a new method to be dynamic capable of combining and deleting rights of select collaborators. In this study, we propose collective copyright authentication scheme suitable for the contents of Collective Intelligence. The proposed scheme consists of collective copyright registration, addition and verification protocols. It could be applied to various business models that require to combine multiple rights of similar contents or to represent multiple authorships on the same contents.

• **Key Words** : Collective Intelligence, Contents Protection, Copyright Protection, Collective Copyright, Authorship Management

*교신저자 : 윤성현(shyoon@bu.ac.kr)
접수일 2015년 10월 12일 수정일 2015년 11월 23일 게재확정일 2015년 12월 20일

1. 서론

스마트폰의 보급과 앱 수요의 가파른 증가로 디지털 콘텐츠 산업이 주목받고 있다[2,3]. 디지털 콘텐츠는 사진, 동영상, 음악, 게임 등과 같이 컴퓨터 및 모바일 기기에서 재생할 수 있는 콘텐츠로 정보화 사회에서 경제적 부가가치를 창출하는 핵심요소이다.

애플 앱스토어가 성공한 것은 일반인들도 경제 활동에 참여하여 수익을 낼 수 있는 콘텐츠 거래 플랫폼을 만들었기 때문이다. 앱스토어는 자본이 부족한 개인 개발자 또는 기업을 대신하여 콘텐츠 등록, 홍보, 판매 및 정산을 대행하고, 개발자가 만든 콘텐츠를 판매하여 얻은 수익의 일부를 수수료로 받는 비즈니스 모델이다. 개발자는 콘텐츠를 개발하여 앱스토어에 등록하는 것만으로 쉽게 수익을 창출할 수 있다. 따라서 앱 제작 능력을 갖춘 일반인들의 사업 참여가 가능해졌으며 1인 기업으로 대표되는 소규모 창업 또한 늘어나고 있다[3].

콘텐츠 산업에서는 개인의 창조적 비즈니스 능력에 따라 경제적 부가가치가 발생한다. 기존의 조직 기반의 경영은 정보화 시대의 콘텐츠 산업이 요구하는 다양성을 수용하기 어렵다. 애플 앱스토어와 같이 개인의 창의적 아이디어를 제품화하고 판매 해주는 다양한 솔루션을 갖추고 있어야 콘텐츠 산업에서 성공할 수 있다[4].

지혜 마켓은 사람의 경험과 아이디어를 콘텐츠로 만들어 경제적 부가가치를 창출하는 허브이다. 지혜 마켓에서는 일반인들의 다양한 경험과 아이디어를 콘텐츠로 만들어 유통하기 때문에, 콘텐츠 저작이 쉬워야 하고 개인과 공동 저자의 권리를 보호해야 하며 콘텐츠 판매 수익의 공정한 분배가 이루어져야한다[1].

집단지성 콘텐츠는 원저자와 여러 사람의 도움으로 만들어진 콘텐츠이다. 원저자는 자신의 아이디어를 기획하여 소셜 네트워크 또는 클라우드 기반의 협업 플랫폼에 제공하고 여러 사람의 피드백을 통해서 콘텐츠를 완성한다. 애플 앱스토어의 경우에는 콘텐츠 판매를 통하여 얻은 수익을 원저자에게 일정한 비율로 분배하는데, 집단지성 콘텐츠를 유통하는 지혜 마켓에서는 원저자뿐만 아니라 협력자들도 고려해야 한다.

일반적으로 저작권 보호 기법은 태그 삽입 기법과 저작권 인증 기법으로 구분된다. 태그 삽입 기법은 저작권 정보를 콘텐츠에 삽입 및 검출하는 것으로 워터마킹 기법이 대표적이다[5]. 저작권 인증 기법은 콘텐츠 유통과 수익 분배에 필요하며 저작자의 권리를 법적으로 보장할 수 있어야한다[6,7].

본 논문에서는 집단지성 콘텐츠 거래에 적합한 집단 저작권 인증 기법을 제안한다. 제안한 기법은 집단 저작권 등록, 추가 그리고 검증 프로토콜로 구성된다.

2장에서 지혜 콘텐츠의 특징과 이에 적합한 비즈니스 모델 요구사항을 알아보고, 3 장에서 제안한 집단 저작권 인증 기법을 설명한다. 4 장에서는 제안한 기법의 안전성 및 응용 방안에 대해서 설명하고, 5 장에서 결론을 제시한다.

2. 연구 배경

2.1 지혜 콘텐츠 정의

일반적으로 디지털 기기에서 재생이 가능한 앱, 게임, 영화와 같은 전문 콘텐츠는 전문 저작 기술을 보유한 개인 또는 기업에 의해서 만들어진다. 전문 콘텐츠는 콘텐츠를 개발할 수 있는 전문 인력이 구매 인력보다 적고, 유통되는 콘텐츠의 종류 또한 매우 제한적이다.

지혜 콘텐츠는 사람의 경험과 아이디어로 만들어지기 때문에 고도의 전문 저작 기술을 요구하지 않는다. 콘텐츠 개발은 교육용 강의 동영상과 같이 상용화가 가능한 경험과 아이디어만 있으면 누구나 저작이 가능하다. 따라서 지혜 마켓은 기존 비즈니스 모델과 달리 콘텐츠의 양, 종류, 개발 인력 그리고 구매 인력이 매우 큰 대규모 시장 환경을 고려해야한다[1].

지혜 콘텐츠는 사람의 생각을 콘텐츠로 만든 것이기 때문에 특허와 같은 독점권 설정이 어렵고, 비슷한 경험과 아이디어로 만들어진 유사 콘텐츠들이 많이 존재한다. 따라서 지혜 마켓에서의 저작권은 특허와 같이 자신의 콘텐츠에 대한 독점적 권리를 인정받기 위한 것이 아니라, 콘텐츠 거래로 발생한 수익을 공정하게 배분받기 위한 권리로 정의하는 것이 타당하다.

2.2 비즈니스 모델 요구사항

지혜 마켓은 일반인들의 경험과 아이디어로 구성된 콘텐츠를 판매하는 곳으로, 비즈니스 모델 설계 시에 다음과 같은 요구사항을 만족해야 한다.

본 절에서는 (가)와 (나)를 만족하는 애플 앱스토어 모델과 (다)를 만족하는 Quirky.com 모델을 분석 한다[3,8].

(가) 전문 개발자가 아닌 일반인도 콘텐츠 제작 및 거래에 참여할 수 있다.
(나) 콘텐츠 판매, 유통, 정산을 대행해 주는 시스템이 있어야 한다.
(다) 여러 사람의 도움을 받아 제작된 콘텐츠인 경우에 집단 저작 권리를 보장할 수 있어야 한다.

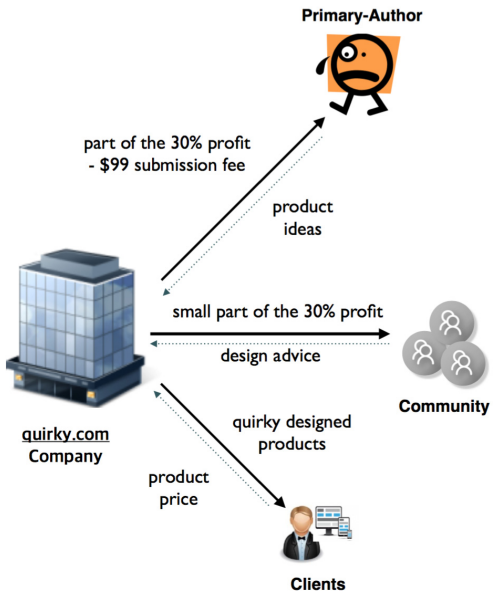
애플 앱스토어는 대규모 개발자를 상대하는 온라인 콘텐츠 유통 모델이다. 개발자들은 Xcode 라는 정형화된 툴을 이용하여 콘텐츠 개발 및 패키징을 하고, 앱스토어는 콘텐츠 판매, 유통, 정산과 같은 경영 프로세스를 담당한다. 따라서 자본이 부족한 일반인들도 전문 앱 개발 기술만 보유하고 있으면 콘텐츠 사업에 참여할 수 있다.

지혜 마켓에서는 비슷한 지식과 지혜를 가진 여러 형태의 콘텐츠가 존재하기 때문에 정형화된 저작 툴 보다는 다양한 형태의 콘텐츠를 수용할 수 있는 저작 도구와 유통 모델이 필요하다.

Quirky.com 모델에서 일반인들은 자신의 아이디어로 제품을 기획하고, Quirky.com은 이를 사업화하여 판매하는 역할을 한다. 제품을 직접 써 본 소비자들은 해당 상품을 어떻게 개선할 것인지에 대한 유용한 아이디어를 많이 가지고 있다. 하지만 아이디어를 제품화하여 판매하기 위해서는 제반 비용이 많이 요구되기 때문에 일반인들의 상품 기획 아이디어는 사업화되지 못하고 사장되는 경우가 대부분이다. Quirky.com 모델은 바로 이런 일반인들의 아이디어를 어떻게 사업에 연결시킬 수 있는지를 보여준다.

사용자는 Quirky.com 홈페이지에서 회원 가입을 하고, 자신의 상품 아이디어를 온라인으로 제출한다. 제출된 기획안은 기존 회원들의 피드백을 받아서 완성도를 높이고, Quirky.com 임원들은 회의를 통하여 해당 기획안의 제품화를 결정한다. Quirky.com은 제품의 생산, 유통, 판매를 대행해 주고 최종적으로 [Fig. 1]과 같이 수익 분배를 한다. Quirky.com 수익 분배 모델의 특징은 원저자뿐만 아니라 커뮤니티도 수익의 30%를 분배 받음으로써 커뮤니티의 저작권을 부분적으로 인정한다는 것이다 [8].

지혜 마켓에서는 콘텐츠 생산, 유통, 판매가 모두 온라인으로 이루어지기 때문에 원저자와 커뮤니티에 대한 집단 권리를 디지털로 표현하고 인증할 수 있어야 한다.



[Fig. 1] Quirky.com Profit Sharing Model

3. 집단 저작권 보호 모델

3장에서는 집단지성 콘텐츠에 적합한 저작권 인증 기법을 제안한다. 3.1 절에서 집단 저작권 인증 모델, 3.2 절에서 원저자의 저작권 등록 프로토콜 그리고 3.3 절에서 협력자의 권리 추가 프로토콜을 제시한다.

3.1 집단 저작권 인증 모델

제안한 모델은 원저자와 협력자 그룹 그리고 등록 센터로 구성된다. 협력자 그룹은 원저자의 콘텐츠 개발에 도움을 준 사람들이며, 원저자는 선택적으로 협력자의 권리를 집단 저작권에 추가할 수 있다. 등록 센터는 원저자와 협력자의 권리로 구성된 집단 저작권을 등록 및 검증한다.

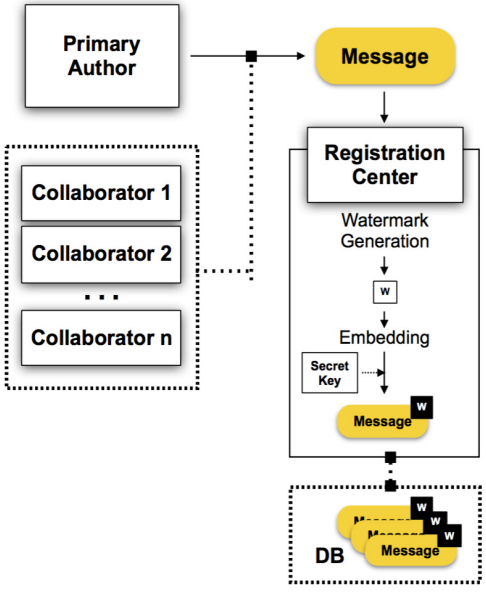
가정 1. 등록 센터는 법적 구속력을 갖는 전적으로 신뢰할 수 있는 기관으로 저작권 등록 및 검증 업무를 수행한다.

가정 2. 원저자와 협력자 그룹 그리고 등록 센터는 법적 구속력이 있는 PKI(Public Key Infrastructure) 인증 센터로부터 인증서를 발급 받는다. 더불어, 인증서에 등록된 공개키와

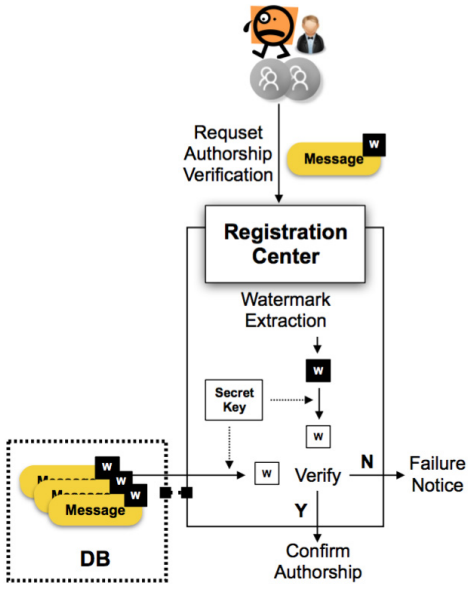
이와 쌍을 이루는 개인키는 암호학적으로 안전한 공개키 암호 알고리즘을 이용하여 생성된다[9,10].

가정 3. 집단 저작권 삽입 및 검출에 사용되는 워터마킹 기법과[11,12] 워터마크 암호화에 사용되는 대칭키 암호 알고리즘은[13] 암호학적으로 안전하다.

[Fig .2]는 집단 저작권 등록 과정을 보여준다. 원저자는 협력자 그룹의 도움을 받아서 디지털 콘텐츠를 개발한다. 원저자는 자신이 만든 콘텐츠의 저작권을 센터에 등록하고 콘텐츠 개발에 도움을 준 협력자에게 저작권 추가를 요청한다. 협력자는 센터에게 자신의 저작권 정보가 추가된 집단 저작권의 등록을 요청한다. 센터는 저자들의 저작권 정보와 서명이 포함된 워터마크를 생성한다. 센터는 자신의 비밀키로 워터마크를 암호화하고 이를 콘텐츠에 워터마킹한다. 센터는 저작권자 정보, 콘텐츠 ID, 집단 저작권, 워터마크가 삽입된 콘텐츠를 데이터베이스에 등록한다.



[Fig .2] Collective Copyright Registration Model



[Fig .3] Collective Copyright Verification Model

[Fig .3]은 집단 저작권 검증 과정을 보여준다. 검증자는 워터마크가 삽입된 콘텐츠를 센터로 보내서 저작권 인증을 요청한다. 센터는 콘텐츠에 삽입된 워터마크를 검출하고 이를 데이터베이스에 등록된 워터마크와 비교 검증하여 저작권을 인증한다.

<Table 1>은 본 논문에서 사용된 약어와 이에 대한 정의를 보여준다.

〈Table 1〉 Terms and Definitions

PA	Primary Author
CA	Collaborator
RC	Registration Center
$cert_{PA}$	PA's PKI Certificate
$cert_{CA}$	CA's PKI Certificate
$cert_{RC}$	RC's PKI Certificate
pk_{PA}	PA's Public Key
pk_{CA}	CA's Public Key
pk_{RC}	RC's Public Key
sk_{PA}	PA's Private Key
sk_{CA}	CA's Private Key
sk_{RC}	RCs Private Key
$cInfo_{USER}$	Copyright Information of USER
$reqMsg_{PA}$	PA's Request for Copyright
$reqMsg_{CA}$	CA's Request for Collective Copyright

$EN_{key}()$	RSA Encryption with the key
$DE_{key}()$	RSA Decryption with the key
$sig_{USER}()$	USER's Digital Signature
msg	Digital Contents
msg_{w*}	Watermarked Digital Contents, *=[0…]
H()	MD5 or SHA-1 Hash Function
SC()	Scramble with RC's master key
DESC()	Descramble with RC's master key
EB(w*→msg)	Embed Watermark w* to the msg
ET(w*←msg_{w*})	Extract Watermark w* from the msg_{w*}

3.2 원저자 권리 생성 및 등록

단계 1: PA는 자신이 만든 콘텐츠 msg를 해쉬하고, 자신의 개인키로 해쉬값을 암호화하여 $sig_{PA}(msg)$를 생성한다. PA는 저작권 등록을 요청하는 패키지 $reqMsg_{PA}$를 만들고, 자신의 개인키로 이 패키지에 다음과 같이 서명한다. $reqMsg_{PA}$ 패키지는 msg, $cert_{PA}$, $cInfo_{PA}$로 구성된다. $cInfo_{PA}$는 PA의 이름, 콘텐츠의 이름, 출판일 등과 같은 원저자의 저작권 정보로 구성된다.

$$sig_{PA}(msg) = EN_{sk_{PA}}(H(msg))$$
$$reqMsg_{PA} = \{msg, cert_{PA}, cInfo_{PA}\}$$
$$sig_{PA}(reqMsg_{PA}) = EN_{sk_{PA}}(H(reqMsg_{PA}))$$

단계 2: PA는 RC로 $sig_{PA}(msg)$, $reqMsg_{PA}$, $sig_{PA}(reqMsg_{PA})$를 전송한다.

단계 3: RC는 PA의 인증서 $cert_{PA}$를 검증하여 올바른 인증서이면 $cert_{PA}$에 포함된 PA의 공개키 pk_{PA}를 추출한다. RC는 pk_{PA}를 이용하여 다음과 같이 서명 $sig_{PA}(reqMsg_{PA})$를 검증한다. 검증식 3.1이 성립하지 않으면 PA에게 서명이 잘못되었음을 알리고 프로토콜을 종료한다. 그렇지 않으면, 단계 4로 이동한다.

$$H(reqMsg_{PA}) = DE_{pk_{PA}}(sig_{PA}(reqMsg_{PA})) \quad (3.1)$$

단계 4: RC는 다음과 같이 PA의 저작권 패키지 $cRight_{PA}$를 생성하고 자신의 개인키로 $cRight_{PA}$를 서명한다.

$$cRight_{PA} = \{cInfo_{PA}, sig_{PA}(msg), cert_{PA}\}$$
$$sig_{RC}(cRight_{PA}) = EN_{sk_{RC}}(cRight_{PA})$$

단계 5: RC는 자신의 비밀키로 $cRight_{PA}$를 다음과 같이 암호화 한다.

$$SC(cRight_{PA})$$

단계 6: RC는 단계 4에서 생성한 서명과 단계 5에서 암호화한 PA의 권리 정보를 다음과 같이 워터마킹 한다.

$$w0 = \{SC(cRight_{PA}),\ sig_{RC}(cRight_{PA})\}$$
$$msg_{w0} = EB(w0 \rightarrow msg)$$

단계 7: RC는 $cRight_{PA}$, $sig_{RC}(cRight_{PA})$, msg, msg_{w0}를 데이터베이스에 등록하고 PA에게 이 값들을 보낸다.

3.3 협력자의 권리 추가 및 인증

원저자는 협력자에게 집단 저작권 등록을 요청한다. 협력자는 센터에게 자신의 저작권을 추가해줄 것을 요청한다. 센터는 집단 저작권을 생성하여 데이터베이스에 등록한다.

단계 1: PA는 CA의 권리를 자신의 권리에 추가하도록 $reqAdd_{CA}$ 패키지를 만들고, 자신의 개인키로 서명 $sig_{PA}(reqAdd_{CA})$를 생성한다. $reqAdd_{CA}$는 원저자의 콘텐츠, 원저자의 인증서, 그리고 협력자의 인증서로 구성된다.

$$sig_{PA}(msg) = EN_{sk_{PA}}(H(msg))$$
$$reqAdd_{CA} = \{msg,\ cert_{CA},\ cert_{PA}\}$$
$$sig_{PA}(reqAdd_{CA}) = EN_{sk_{PA}}(H(reqAdd_{CA}))$$

단계 2: PA는 $sig_{PA}(reqAdd_{CA})$, $sig_{PA}(msg)$, $reqAdd_{CA}$를 CA에게 전송한다.

단계 3: CA는 PA가 보낸 메시지를 검증한다. 먼저 PA의 $cert_{PA}$를 검증하여 올바른 인증서이면 $cert_{PA}$에 포함된 PA의 공개키 pk_{PA}를 추출한다. pk_{PA}를 이용하여 $sig_{PA}(reqAdd_{CA})$와 $sig_{PA}(msg)$를 검증한다. 만약 식 3.2 또는 3.3이 성립하지 않으면 PA에게 서명이 잘못되었음을 알리고 프로토콜을 종료한다. 그렇지 않으면 단계 4로 이동한다.

$$H(reqAdd_{CA}) = DE_{pk_{PA}}(sig_{PA}(reqAdd_{CA})) \quad (3.2)$$

$$H(msg) = DE_{pk_{PA}}(sig_{PA}(msg)) \quad (3.3)$$

단계 4: CA는 자신과 PA의 저작권 정보가 포함된 패키지 $reqMsg_{CA}$를 만들고, 이 패키지에 대한 서명 $sig_{CA}(reqMsg_{CA})$을 생성한다. 더불어 CA는 msg에 대한 다중 서명 $sig_{CA}(sig_{PA}(msg))$를 생성한다.

$$reqMsg_{CA} = \{reqAdd_{CA}, sig_{PA}(reqAdd_{CA}), cInfo_{CA}\}$$

$$sig_{CA}(reqMsg_{CA}) = EN_{sk_{CA}}(H(reqMsg_{CA}))$$

$$sig_{CA}(sig_{PA}(msg)) = EN_{sk_{CA}}(sig_{PA}(msg))$$

단계 5: CA는 $reqMsg_{CA}$, $sig_{CA}(reqMsg_{CA})$, $sig_{CA}(sig_{PA}(msg))$를 RC에게 전송한다.

단계 6: RC는 CA의 인증서 $cert_{CA}$를 검증하여 올바른 인증서이면 $cert_{CA}$에 포함된 CA의 공개키 pk_{CA}를 추출한다. pk_{PA}와 pk_{CA}를 이용하여 $sig_{CA}(reqMsg_{CA})$와 $sig_{CA}(sig_{PA}(msg))$를 검증한다. 만약 식 3.4 또는 3.5가 성립하지 않으면, CA에게 서명이 잘못되었음을 알리고 프로토콜을 종료한다. 그렇지 않으면 단계 7로 이동한다.

$$H(reqMsg_{CA}) = DE_{pk_{CA}}(sig_{CA}(reqMsg_{CA})) \quad (3.4)$$

$$H(msg) = DE_{pk_{CA}}(DE_{pk_{PA}}(sig_{PA}(msg))) \quad (3.5)$$

단계 7: RC는 CA의 저작권을 추가한 집단 저작권 $cRight_{PA||CA}$를 다음과 같이 만들고 여기에 서명한다.

$$cRight_{PA||CA} = \{cInfo_{PA}||cInfo_{CA}, sig_{CA}(sig_{PA}(msg)), cert_{PA}||cert_{CA}\}$$

$$sig_{RC}(cRight_{PA||CA}) = EN_{sk_{RC}}(cRight_{PA||CA})$$

단계 8: RC는 자신의 비밀키로 $cRight_{PA||CA}$를 다음과 같이 암호화 한다.

$$SC(cRight_{PA||CA})$$

단계 9: RC는 단계 7에서 생성한 서명과 단계 8에서 암호화된 집단 저작권 정보를 다음과 같이 워터마킹 한다.

$$w1 = \{SC(cRight_{PA||CA}),\ sig_{RC}(cRight_{PA||CA})\}$$

$$msg_{w1} = EB(w1 \rightarrow msg)$$

단계 10: RC는 msg, msg_{w1}, $cRight_{PA||CA}$, $sig_{RC}(cRight_{PA||CA})$를 데이터베이스에 등록하고 CA와 PA에게 이 값들을 보낸다.

3.4 집단 저작권 검증

단계 1: RC는 콘텐츠에 삽입된 워터마크를 다음과 같이 추출한다.

$$w1 = ET(w1 \leftarrow msg_{w1})$$

$$w1 = \{SC(cRight_{PA||CA}),\ sig_{RC}(cRight_{PA||CA})\}$$

단계 2: RC는 암호화된 집단저작권을 다음과 같이 복호화 한다.

$$cRight_{PA||CA} = DESC(SC(cRight_{PA||CA}))$$

단계 3: RC는 자신의 공개키로 집단 저작권 $cRight_{PA||CA}$에 대한 서명 $sig_{RC}(cRight_{PA||CA})$을 검증한다. 만약 식 3.6이 성립하면 자신이 서명한 것임을 인증하고 단계 4로 진행한다. 그렇지 않으면 잘못된 것임을 통지하고 프로토콜을 종료한다.

$$cRight_{PA||CA} = DE_{pk_{RC}}(sig_{RC}(cRight_{PA||CA})) \quad (3.6)$$

단계 4: RC는 PA와 CA의 인증서를 검증하고 유효하면 단계 5로 진행하고, 그렇지 않으면 프로토콜을 종료한다.

단계 5: RC는 PA와 CA의 공개키를 이용하여 다중 서명을 검증한다. 만약 식 3.7이 성립하면 집단저작권을 인증하고, 그렇지 않으면 잘못된 것임을 통지한다.

$$H(msg) = DE_{pk_{PA}}(DE_{pk_{CA}}(sig_{CA}(sig_{PA}(msg)))) \quad (3.7)$$

4. 안전성 분석 및 모델 평가

4.1절에서 집단 저작권 프로토콜의 안전성에 대해서 분석하고, 4.2절에서 제안한 모델의 응용에 대해서 논의한다.

4.1 안전성 분석

정리 1. 원저자와 협력자의 권리가 포함된 집단 저작권은 위조 및 가장 공격으로부터 안전하다.

(증명) 3.2절에서 원저자는 해쉬함수를 이용하여 콘텐츠를 해쉬하고 자신의 개인키로 해쉬값을 서명한다. 3.3절에서 협력자는 자신의 개인키로 콘텐츠에 대한 다중 서명을 생성한다. 다중 서명을 위조하려면 원저자와 협력자의 개인키를 추출하거나, 또는 임의의 개인키를 생성하여 원저자 및 협력자인 것처럼 가장해야 한다. 서명에 사용된 개인키는 공개키 암호 기법의 안전성에 기반을 둔다. 가정 2에서 원저자와 협력자의 키는 암호학적으로 안전한 공개키 암호 기법으로 생성된다. 더불어 신뢰할 수 있는 PKI 인증 센터로부터 키 인증을 받는다. 따라서 해커는 서명에 사용된 개인키를 추출할 수 없고 제안한 모델은 해커의 가장 공격으로부터 안전하다. Q.E.D.

정리 2. 원저자와 협력자의 권리가 포함된 집단 저작권은 부인될 수 없다.

(증명) 3.4절에서 센터는 법적 구속력이 있는 인증서를 이용하여 원저자와 협력자의 그룹 서명을 검증한다. 서명을 부정하려면 검증에 사용된 공개키가 자신의 것이 아님을 증명해야 한다. 가정 2에서 원저자와 협력자는 PKI 인증 센터로부터 인증서를 발급받는다. 더불어 가정 3에서 저작권 삽입 및 검출에 사용된 워터마킹 알고리즘은 암호학적으로 안전하다. 따라서 원저자와 협력자는 집단 저작권을 부인할 수 없다. Q.E.D.

4.2 응용 및 평가

DRM 모델의 세부적인 정책과 구현은 적용되는 환경에 따라서 각기 다르다[14]. 제안한 집단 저작권 기법은 지혜 마켓과 같이 일반인들이 참여하는 비즈니스 모델에 적용되어 다양한 세부 운용이 가능하도록 모델을 확장할 수 있다.

기존의 저작권 보호 모델은 대부분 원저자의 저작권 생성 및 인증에 초점을 두고 있다[15]. 하지만 인터넷과 소셜 네트워크 서비스의 발전으로 Quirky.com과 같이 협업에 기반을 둔 제품 개발이 가능해지면서 원저자뿐만 아니라 협력자들의 권리도 표현할 수 있는 저작권 보호 기법이 요구되고 있다.

지혜 콘텐츠는 사람의 경험과 아이디어로 구성된다. 이것은 사람의 생각을 콘텐츠로 만든 것이기 때문에 특허와 같은 독점적 권리를 부여하기가 어렵고, 더불어 유사하거나 중복된 콘텐츠가 많아지게 된다. 특히 전문 콘텐츠로 사람들의 수요가 몰리게 되면 경쟁력이 떨어지는 일반인들의 사업 참여는 저하될 수밖에 없다. 지혜 마켓의 활성화를 위해서는 유사하거나 중복되는 콘텐츠를 서로 통합하여 상품 경쟁력을 확보할 수 있는 권리 통합 기술이 필요하다.

본 논문에서는 다양한 콘텐츠 비즈니스 모델에 적용할 수 있는, 집단 권리 및 개별 권리의 통합이 가능한 저작권 보호 모델을 제시하였다. 제안한 모델은 원저자의 권리를 보장하고 여기에 협력자의 권리를 추가하는 방식으로, 콘텐츠 개발 기여도에 따라서 가중치를 두어 수익 분배를 할 수 있는 보다 유연한 비즈니스 모델로 확장이 가능하다.

5. 결론

본 연구에서는 집단지성 콘텐츠에 적합한 집단 저작권 인증 기법을 제안하였다. 제안한 기법은 집단 저작권 등록, 추가 및 검증 프로토콜로 구성된다. 제안한 집단 저작권 인증 기법의 안전성을 분석하였고, 더불어 응용 및 확장성에 대해서 논의하였다. 제안한 기법은 집단 권리를 생성할 수 있을 뿐만 아니라 기존의 개별 권리를 통합할 수 있기 때문에 지식 콘텐츠 기반의 신규 비즈니스 모델을 창출하거나 기존 모델을 확장하는데 사용할 수 있다.

ACKNOWLEDGMENTS

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였음. [2014, 개인과 집단지성의 디지털콘텐츠화를 통한 유통 및 확산 서비스 기술 개발]

REFERENCES

[1] Development of distribution and diffusion service technology through individual and collective Intelligence to digital contents, ICT R&D program of MSIP/IITP, 1st Year Annual Report, Korea University, 2014.

[2] Want, R., “iPhone: Smarter Than the Average

Phone," IEEE Pervasive Computing, Vol. 9, No. 3, pp. 6-9, IEEE, 2010.
[3] Dion Hinchcliffe, "The app store: The new "must-have" digital business model", http://www.zdnet.com/article/ the-app-store-the-new-must-have-digital-business-model/, 2010.
[4] Christopher A. H. Vollmer, Sebastian Blum, Kristina Bennin, "How Media Companies Can Make Multichannel Networks Profitable," Forbes, http://www.forbes.com/2014/12/19/how-media/a-companies-can-make-multichannel-networks-profitable/, 2014.
[5] Zhao J, "A WWW service to embed and prove digital copyright watermarks," Proc. Of the European Conference on Multimedia Application, Services and Techniques, pp. 695-710, 1996.
[6] Mason A, Salmon RA, Devlin J, "User requirements for watermarking in broadcast applications," International broadcasting convention (IBC 2000), Amsterdam, The Netherlands, 2000.
[7] Piva A, Bartolini F, Barni M, "Managing copyright in open networks," IEEE Internet Computing, pp. 18-26, 2002.
[8] Business Model Breakdown - Quirky.com, http://www.lumosforbusiness.com/blog/722/28-06-2010/Business+Model+Breakdown++Quirkycom, Lumos Business Solutions Inc.
[9] Rivest R, Shamir A, Adleman L, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM 21 (2), pp. 120 - 126, 10.1145/359340.359342, 1978.
[10] Taher ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory 31 (4), pp. 469 - 472, 10.1109/TIT.1985.
[11] Samtani R, "Ongoing innovation in digital watermarking," Computer 42, pp. 92-94, 10.1109 /MC.2009.93, 2009.
[12] Kirstein M, "Beyond traditional DRM: moving to digital watermarking & fingerprinting in media," MultiMedia Intelligence, 2008.
[13] "Announcing the ADVANCED ENCRYPTION STANDARD (AES)," FIPS 197, NIST, 2012.
[14] Rosenblatt. Bill, Trippe. Bill, Mooney. Stephen, Digital Right Management: Business and Technology. M&T Books, 2002.
[15] Eric Diehl, Securing Digital Video: Techniques for DRM and Content Protection. Springer, 2012.

저자소개

윤 성 현(Sunghyun Yun) [종신회원]

- 1994년 2월 : 고려대학교 일반대학원 컴퓨터학과 (이학석사)
- 1997년 2월 : 고려대학교 일반대학원 컴퓨터학과 (이학박사)
- 1998년 3월 ~ 2002년 2월 : LG전자 중앙연구소 선임연구원
- 2002년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수

<관심분야> : 모바일 보안, 바이오메트릭 인증, DRM, 전자선거

임 희 석(Heuiseok Lim) [종신회원]

- 1994년 2월 : 고려대학교 일반대학원 컴퓨터학과 (이학석사)
- 1997년 8월 : 고려대학교 일반대학원 컴퓨터학과 (이학박사)
- 2004년 3월 ~ 2008년 2월 : 한신대학교 컴퓨터정보소프트웨어학부 부교수
- 2008년 3월 ~ 현재 : 고려대학교 컴퓨터공학과 교수

<관심분야> : 인공지능, 자연어처리, 컴퓨터교육

이 근 호(Keun-Ho Lee) [종신회원]

- 2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)
- 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
- 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수

<관심분야> : M2M 보안, 이동통신 보안, 융합 보안, 개인정보보호

김 정 훈(Jung-Hoon Kim) **[정회원]**

- 1991년 2월 : 서울대학교 환경대학원 환경계획학과 (도시계획석사)
- 2001년 12월 : 영국 뉴카슬대학교 건축, 계획 및 조경학부 (도시 및 지역계획학 박사)
- 1990년 9월 ~ 2010년 2월 : 국토연구원 연구위원
- 2010년 3월 ~ 현재 : 영남대학교 새마을 국제개발학과 교수

<관심분야> : U-City, GIS, 도시 및 지역개발

김 대 룡(DaeRyong Kim) **[정회원]**

- 1992년 5월 : Iowa State University (MS, Management/MIS)
- 1996년 8월 : University of Mississippi (Ph.D., MIS)
- 1996년 9월 ~ 2001년 6월 : 조교수, 울산대학교
- 2001년 8월 ~ 현재 : Professor, Delaware State University

<관심분야> : Mobile IT, Ubiquitous, Human Interface in IT