SNS환경에서 워터마킹 기술을 활용한 콘텐츠 저작권 보호 기법 연구

위유경*, 곽진**
*순천향대학교 정보보호학과 정보보호응용및보증연구실
**순천향대학교 정보보호학과
e-mail : ykwi@sch.ac.kr, jkwak@sch.ac.kr

A Study on Watermarking Based Content Copyright Protection Scheme in SNS Environment

Yukyeong Wi*, Jin Kwak**
*ISAA Lab, Dept of Information security Engineering, Soonchunhyang University
**Dept of Information security Engineering, Soonchunhyang University

요 약

스마트 폰의 보급률이 증가함에 따라 시간과 공간의 제약 없이 의사소통이 가능한 SNS(Social Network Service)가 발달하고 있다. SNS는 기존의 단순한 의사소통에서 광고, 게임, 전자상거래 등 사회전반에 걸친 서비스로 확대되었다. 따라서 사용자에게 좀 더 효율적이고 유용한 서비스 제공이 가능하게 되었으며, 다양한 콘텐츠를 업로드 할 수 있다. 그러나 사용자의 지적재산인 해당 콘텐츠를 무단으로 다운로드 받을 경우 저작권에 침해를 받을 수 있다. 또한 악의적인 사용자의 불법 다운로드 경로를 파악하기 어렵다. 따라서 본 논문에서는 SNS환경에서 워터마킹 기술을 활용한 콘텐츠 저작권 보호 기법에 대해 제안한다. 제안하는 기법은 사용자의 SNS 계정에 업로드한 콘텐츠의 저작권을 보호하며, 악의적인 사용자의 불법 다운로드 경로를 추적하여 추가적인 불법행위를 방지할 수 있다.

1. 서론

스마트폰, 태블릿PC 등 다양한 모바일 디바이스의 보급률이 증가하고, 무선인터넷 서비스가 확장됨에 따라 시간과 공간의 제약 없이 의사소통이 가능한 SNS 사용자가 증가하고 있다. 초기의 SNS는 지인들과의 친목도모 및 엔터테인먼트의 용도로 주로 사용되었다. 이후 SNS는 점차 모바일 디바이스와 결합하면서 사회와 문화 전반에 걸쳐 다양한 사용자들의 의사소통, 참여, 광고 등의 서비스로 확대되었다.

대표적인 소셜 네트워크 서비스로 트위터, 싸이월드, 페이스북 등이 있다. 해당 서비스들은 사용자의 콘텐츠(사진, 비디오 등)들을 자신의 계정에 업로드 할 수 있다. 또한 이 콘텐츠들은 서로 다른 사용자들 끼리 공유할 수 있다. 하지만 '공유하기', '퍼가기' 등의 기능을 사용하지 않은 채 해당 콘텐츠를 무단으로 다운로드 받을 경우에 저작권에 침해를 받을 수 있다. 콘텐츠는 사용자의 지적재산 물품이다. 이에 따라 SNS환경에서 사용자의 콘텐츠 저작권을 보호하는 기법이 필요하다.

따라서 본 논문에서는 SNS환경에서 워터마킹 기술을 활용한 콘텐츠 저작권 보호 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구에 대해 분석하고, 3장에서 SNS환경의 콘텐츠 보안에 대하여 문제점과 그에 따른 보안 요구사항에 대해 분석한다. 4장에서는 SNS환경에서 워터마킹 기술을 활용한 콘텐츠 저작권 보호 기법을 제안한다. 5장에서는 제안한 기법의 안전성에 대해 분석하고, 마지막으로 6장에서는 결론을 맺는다.

본 연구는 방송통신위원회의 방송통신융합미디어원천기술 개발사업의 연구결과로 수행되었음.
(KCA-2012-12-912-06-003)

2. 관련연구

2.1 SNS

❒ 페이스북

페이스북은 2004년 당시 하버드대학교 재학생 마크 주커버그에 의해 개발되었다. 2011년 9월 현재 전 세계 8억 명 이상의 가입자가 활동 중인 세계 최대의 소셜 네트워크 서비스이다.

페이스북에서 제공하고 있는 주요 서비스로는 지인들이 메시지 및 동영상을 포함한 콘텐츠를 게시할 수 있는 Wall, 사진 및 앨범 등을 게시 또는 관리할 수 있는 Photos, 자신의 현재 위치 및 활동 내용 등 현재 상태를 알려주는 Status, 친구의 프로파일 및 일정, 콘텐츠 추가 등 변경사항을 알려주는 News Feed 등이 있다. 또한 '좋아요' 기능을 적용한 웹사이트에서 사용자들은 이 사이트 내에서 다른 사람이 좋아하는 상품, 서비스, 콘텐츠가 무엇인지를 알 수 있고, 본인도 선호 표시를 할 수 있다[1].

❒ 트위터

트위터는 2006년 미국의 벤처 기업인 Obvious Corp에서 개발한 소셜 네트워크 서비스이다. 사용자들은 트위터 홈페이지에 접속해 간단한 자신의 정보를 입력한 후 계정을 만들고 140자 이내의 단문 메시지를 트위터 웹사이트에 전송하며 다른 사용자들과 공유할 수 있는 서비스이다. 또한 메시지 서비스, 이메일, 메신저 등을 통해 작성한 메시지를 트위터 웹사이트로 전송할 수 있다.

트위터는 페이스북과는 두 가지의 차별화된 서비스를 제공했다. 첫 번째로 텍스트를 140자의 단문으로 제한하여 모바일 디바이스에 적합했다. 따라서 메시지의 실시간성을 확보할 수 있었다. 두 번째는 following/follower의 개념이다. 온라인 지인들의 대등하지 않은 관계를 표현한 것이다. 이러한 개념을 바탕으로 수많은 follower를 거느린 정보 생산자의 메시지는 리트윗(retweet)을 통해 빠른 속도로 확대 전파되는 특징을 지니고 있다[2].

2.2 워터마킹 기술

디지털 워터마킹 기술은 용도에 따라 크게 강성, 연성, 핑거프린팅, 스테가노그라피 등 네 가지로 분류할 수 있으며, 이들 중 가장 기본적인 기술은 강성 워터마킹 기술이다[3].

❒ 워터마킹

강성 워터마킹 기술은 악의적인 사용자가 콘텐츠를 불법으로 이용할 목적으로 워터마크를 고의로 훼손 또는 변형하려는 시도를 방지하기 위해 사용되는 기술이다. 이를 위해 원본 워터마킹을 변조하려는 외부의 시도가 있을 때 콘텐츠의 품질이 크게 훼손되기 전에는 워터마크가 깨지지 않도록 설계한 것이 특징이다. 강성 워터마킹 기술을 활용하여 각종 민원서류를 포함한 다양한 증명서의 온라인 발급 업무가 가능하며, 인터넷 서명의 복제 및 위조로 인한 보안 사고를 사전에 막을 수도 있다.

연성 워터마킹의 개념은 병원의 임상 사진 파일 및 관공서의 문서, 군사 기밀 문서 등의 원본 문서 파일의 외부 유출을 막아야 하는 경우에 사용된다. 즉 데이터에 변형을 가하면 쉽게 워터마크가 깨지면서 원본 콘텐츠도 동시에 훼손되도록 설계한 워터마킹으로, 변형여부를 검사하여 인증과 무결성을 제공하기 위한 방법으로 사용된다.

❒ 핑거프린팅

핑거프린팅은 현재 사용되고 있는 '바코드'와 유사한 개념으로, 고유번호나 식별자를 콘텐츠에 삽입하는 것이다. 핑거프린팅 기술을 적용하면 콘텐츠가 누구에게 어디로 배포되었는지 알 수 있으므로 물류 분야에서 제품을 분류하는데 활용 또는 전송 경로를 확인할 수 있다. 또한 불법적으로 유통이 이루어질 경우 배포자를 추적할 수 있다[4].

❒ 스테가노그라피

스테가노그라피는 '감추어져 있다'는 뜻의 그리스어인 'stergano'와 '통신하다'라는 뜻의 'graphos'가 결합된 용어로써 정보를 숨기거나 또는 다른 형태로 위장하여 주고받을 때 사용할 수 있는 일종의 암호 통신기술이다. 음악 파일을 텍스트 파일처럼 가장할 수 있거나, 그림 파일 속에 음악 파일을 은닉하는 것도 가능하다.

3. 문제점 및 보안 요구사항

3.1 문제점

보급형 고해상도 디지털 카메라의 발달과 포토샵 등 일러스트 소프트웨어가 보편화 되었다. 그에 따른 사진, 영상, 그림 등 일반 콘텐츠의 지적재산권에 대한 관심이 높아지고 있다. 콘텐츠는 더 이상 무형물이 아닌 개인의 창작물로 인정받고 있다. 일반적으로 SNS환경에서는 사용자의 창작물을 본인의 계정에 게시하여 제 3자에게 공유되어 진다. 하지만 페이스북의 '공유하기', 싸이월드의 '퍼가기' 등의 정식적인 공유기능이 아닌 해당 콘텐츠의 무단 다운로드는 막을 수 없다. 또한 무단으로 다운로드 받은 콘텐츠는 악의적인 사용자에 의해 저작권을 침해받을 수 있다[5].

3.2 보안 요구사항

❒ 인증

SNS환경에서의 인증기능은 서비스 이용을 원하는 사용자가 전송한 메시지 또는 콘텐츠의 출처가 정확히 확인되고, 그 실체의 신분이 거짓이 아닌 정당한 사용자라는 것을 검증할 수 있어야 한다.

❒ 기밀성

사용자의 서명값은 기밀성이 보장되어야 한다. 서명값은 사용자가 SNS 서버로 접속하여 정당한 사용자인지 확인하는 과정에 사용된다. 또한 사용자의 서명값은 워터마킹 과정에서 콘텐츠의 저작권 정보를 가지고 있다. 이를 위해 SNS환경의 통신에 사용되는 서명값은 정당한 사용자만이 확인할 수 있어야 하며, 서명값의 발신지 및 수신지, 횟수, 길이 또는 통신선로 상의 트래픽 특성에 대하여 공격자가 알지 못하게 해야 한다.

❒ 무결성

사용자의 서명값은 해당 사용자의 SNS 계정 접속에 연관이 있기 때문에 무결성이 보장되어야 한다. SNS환경에서는 데이터베이스에 저장 또는 네트워크를 통해 전송되는 서명 정보가 위변조 및 파괴되지 않도록 해야 한다. 만약에 서명값이 유출되었다면 위조, 삭제 및 변조를 통해 서명값 내에 저장되어 있는 사용자 ID 정보를 분석하여 추가적인 보안문제를 야기할 수 있다. 따라서 전송받은 데이터의 위·변조를 감지하기 위해 해쉬함수 연산 및 전자

서명 등을 이용해야 한다.

❒ 콘텐츠 추적

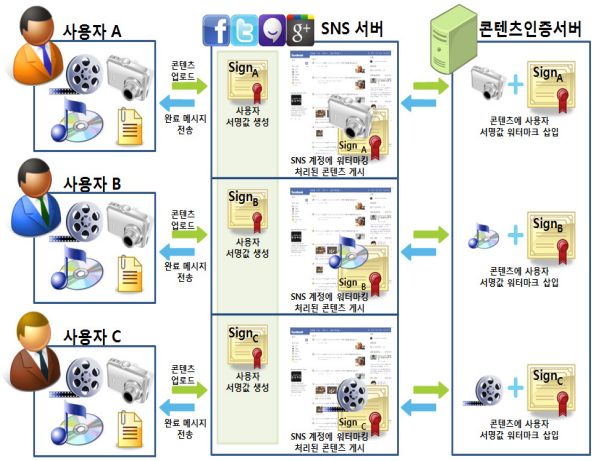
SNS환경에서는 콘텐츠가 불법으로 유출될 경우 해당 콘텐츠의 유출경로를 추적하는 기능이 필요하다. 시스템에서는 콘텐츠 추적 기능을 통해 사용자의 저작권을 보호할 수 있다. 또한 유출 경로를 데이터베이스화 하여 추가적인 불법행위를 사전에 방지할 수 있어야 한다[6].

4. 제안방식

본 논문에서는 안전한 SNS환경을 구축하기 위하여 콘텐츠의 저작권 보호를 위한 기법을 제안한다. 본 제안방식은 해당 사용자의 SNS계정에 업로드 한 콘텐츠를 '공유하기', '퍼가기' 등의 정식절차를 거치지 않고 다운로드를 받는 환경에서 적용된다.

본 제안방식은 사용자의 서명값을 콘텐츠에 워터마킹하여 업로드 한다. 이는 콘텐츠의 무단도용을 방지하여 저작권을 보호한다. 또한 콘텐츠의 무단도용시 사용자의 서명값으로부터 역추적 하여 해당 공격루트를 데이터베이스화 하여 공격루트를 확보한다. 따라서 추가적인 공격 또한 사전에 방지할 수 있다. 제안하는 프로토콜은 서명 생성 단계와 워터마킹 단계의 2단계로 구분된다[7].

(그림 1)는 본 논문에서 제안하는 워터마킹 기반 콘텐츠 저작권 보호 시스템의 개념도를 나타낸다.



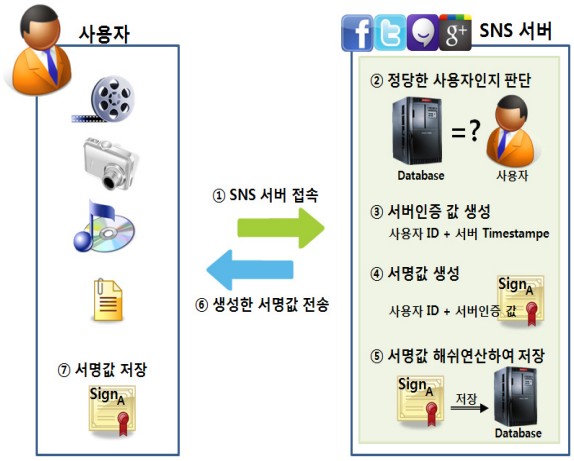
(그림 1) 제안방식 개념도

4.1 서명 생성 단계

① 사용자는 본인의 SNS 계정 서버에 접속한다.

② SNS 서버는 해당 사용자가 정당한 사용자인지 확인한다.

③ SNS 서버는 입력받은 사용자 ID와 서버의 타임스탬프 값을 연산하여 서버인증 값을 생성한다. 이는 워터마킹에 삽입될 서명값의 생성에 사용된다.



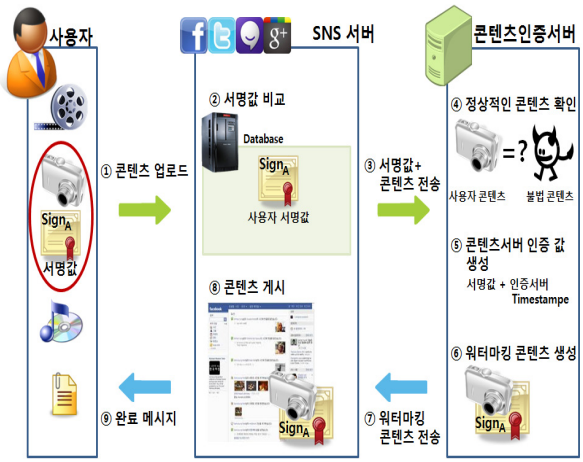
(그림 2) 서명생성 단계

④ SNS 서버는 콘텐츠 워터마킹에 사용되는 사용자 서명값을 생성한다. 사용자 서명값은 사용자의 ID 값과 서버인증 값을 지수승하여 생성한다.

⑤ SNS 서버는 생성한 서명값과 사용자의 ID를 해쉬연산하여 저장한다.

⑥ 해쉬연산한 서명값을 암호화하여 사용자에게 전송하고, 사용자는 이 값을 저장한다.

4.2 워터마킹 단계



(그림 3) 워터마킹 단계

① 사용자는 자신의 SNS 계정에 콘텐츠를 업로드 한다.

② SNS 서버는 전송받은 사용자의 서명값과 서버인증 값을 통해 정당한 사용자인지 확인한다.

③ 그 후 SNS 서버는 서명값과 콘텐츠 파일을 콘텐츠인증서버로 전송한다.

④ 콘텐츠인증서버는 콘텐츠가 정상적인 콘텐츠인지 여부를 확인한다.

⑤ 콘텐츠인증서버는 입력받은 사용자 서명값과 인증서버의 타임스탬프 값을 연산하여 콘텐츠서버 인증 값을 생성한다. 이는 콘텐츠의 워터마킹과정에 삽입되어 해

당 서버의 인증에 대해 유효성을 지니게 된다.

⑥ 그 후 사용자의 서명값과 콘텐츠서버 인증 값을 해당 콘텐츠에 워터마킹하여 생성한다.

⑦ SNS 서버는 워터마킹 콘텐츠를 전송받아 사용자의 계정에 게시한다.

⑧ SNS 서버는 사용자에게 완료 메시지를 전송한다.

5. 안전성 분석

❒ 인증

제안하는 기법에서는 사용자의 ID 정보를 사용하여 서버인증 값을 생성하고, 또한 사용자의 서명값을 사용하여 콘텐츠서버 인증 값을 사용하기 때문에 안전한 인증기능을 제공한다.

❒ 기밀성

제안하는 기법의 서명값은 사용자 ID와 서버의 타임스탬프 정보를 지수승하여 생성된다. 따라서 해당되는 지수의 값을 알기 어렵기 때문에 해당 서명값을 탈취하더라도 SNS를 사용할 수가 없다. 또한 워터마킹 과정에도 사용자 서명값이 사용되기 때문에 콘텐츠의 저작권을 임의로 변경할 수 없다.

❒ 무결성

제안하는 기법은 해쉬함수 연산을 사용하여 사용자 서명값을 생성하여 저장하게 된다. 생성된 서명값은 콘텐츠 업로드 과정에서 SNS 서버 정보와 비교를 통해 등록된 콘텐츠인지 여부를 판별하므로 무결성을 제공한다.

❒ 콘텐츠 추적

사용자의 서명값이 워터마킹된 콘텐츠를 불법으로 다운로드 할 때 서명값을 추적할 수 있다. 해당 콘텐츠의 워터마킹을 복호화하여 서명값을 비교함으로써 추적이 가능하다. 또한 추적된 불법 사용자의 유출 경로를 데이터베이스화 하여 추가적인 불법 행위를 방지할 수 있다.

6. 결론

시간과 공간의 제약 없이 의사소통이 가능한 SNS는 모바일 디바이스와 결합하면서 사회와 문화 전반에 걸쳐 빠르게 다양한 사용자들 간의 의사소통, 참여, 광고 등의 서비스로 확대되었다. 또한 보급형 고해상도 디지털 카메라의 발달과 포토샵 등 일러스트 소프트웨어가 보편화로 인해 사진, 영상, 그림 등 일반 콘텐츠의 지적재산권에 대한 관심이 높아지고 있다.

이러한 SNS환경에서는 사용자의 콘텐츠를 서로 다른 사용자들 간 공유할 수 있다. 하지만 해당 콘텐츠를 무단으로 다운로드 받을 경우 저작권에 침해를 받을 수 있다. 따라서 SNS환경에서 사용자의 콘텐츠 저작권을 보호하는 기법이 필요하다.

본 논문에서는 SNS환경에서 워터마킹 기술을 활용한 콘텐츠 저작권 보호 기법을 제안하였다. 이를 통해 SNS 환경에서 사용자의 지적재산권을 보호할 수 있다. 또한 불법 다운로드를 추적함으로써 공격루트를 확보할 수 있을 것으로 기대된다.

참고문헌

[1] 이형효, 최향창, 김지혜, 조상래, 진승헌, “SNS 환경의 아이덴티티 공유 및 보호에 관한 연구”, 정보보호학회지, 제 19권 1호, 2009

[2] 김지용, 손동환, 김현진, “소셜 네트워크 서비스 기술동향”, 전자통신동향분석, 제 26권 3호, 2011

[3] 오병택, 문병주, 이동일, “디지털 워터마킹 기술동향 및 전망”, 전자통신동향분석, 제 17권 6호, 2002

[4] 김원겸, 이선화, 장호욱, “불법 복제 콘텐츠 추적을 위한 핑거프린팅 기술 동향”, 전자통신동향분석, 제 18권 4호, 2003

[5] 김병일, “인터넷과 SNS에서의 저작권 관련 문제연구”, 한국언론법학회, 언론과 법, 제 9권 2호, 2010

[6] 정혜원, 이준석, 서영호, “불법콘텐츠 추적 기술 연구동향”, 전자통신동향분석, 제 20권 4호, 2005

[7] M. Kutter and S. Winkler, “A Vision-Based Masking Model for Spread-Spectrum Image Watermarking”, IEEE Transactions on Image Processing. 1,11, 2002