디지털 워터마크에 대한 영지식 검증

*이형우, **김태윤
* 천안대학교 정보통신학부
** 고려대학교 컴퓨터학과

Digital Watermark Verification with Zero Knowledge Proofs

*Hyung-Woo Lee, Tai-Yun Kim
*Div. of Information & Communication Engineering,
**Dept. of Computer Science, Korea University
E-mail : hwlee@cheonan.ac.kr, tykim@netlab.korea.ac.kr

요 약

이미지와 같은 디지털 컨텐츠에 대한 저작권 보호 기능을 제공하기 위해서는 삽입된 워터마크에 대한 안전한 증명과 소유권에 대한 공개적인 검증 기술이 필요하다. 특히 워터마크된 컨텐츠에 비밀스럽게 은닉된 워터마크 정보에 대한 완전한 노출 없이도 증명하고자 하는 컨텐츠에 대한 소유권을 공개적으로 증명해 줄 수 있는 검증 기법이 필요하다. 본 연구에서는 기존의 영지식 증명 기법과 워터마킹 기법을 분석하였으며, 영지식 증명 기법을 디지털 워터마크 검증 구조에 적용하여, 워터마크에 대한 비밀정보 유출 없이도 소유권 및 저작권을 검증할 수 있는 영지식 기반 워터마크 검증 기법을 제시한다.

Abstract

Digital contents such as image need both secure proving and publicly verification scheme on embedded digital watermark for contents distribution and copyright protection. Specially, we must provide publicly verification mechanism on digital watermark without revealing any of the secret information hidden on digital contents. In this paper, we review on the existing zero knowledge proofs and digital watermarking system, and propose advanced interactive zero knowledge proofs mechanism for enhancing the performance and security of watermark verification process. And it provides a new watermark verification scheme without revealing any secret on the contents owner's copyright information.

Ⅰ. 서론

디지털 컨텐츠에 대한 소유권 및 저작권을 보장하기 위해서는 디지털 워터마킹 기법을 적용할 수 있다[1,2,3]. 워터마크된 컨텐츠는 검증 과정을 필요로 하며 이를 통해 컨텐츠에 대한 권한을 판별할 수 있다. 근래에 워터마크 검증 방식에서 영지식 증명 기법(zero knowledge proof)을 적용하여 검증을 수행하고자 하는 연구가 제시되었다[27]. 디지털 컨텐츠에 대한 저작권을 보장하기 위해서는 컨텐츠에 대한 저작권을 표기하고 이를 컨텐츠 내부에 은닉하는 구조를 사용하게 된다. 따라서, 컨텐츠에 대한 배포 및 판매 과정에서는 판매자가 생성한 저작권 정보, 즉 디지털 워터마크 정보를 컨텐츠 내부에 은닉시키게 된다.

그러나 컨텐츠에 대한 저작권 보호 기술에서 중요하게 연구되고 있는 분야로는 분쟁 발생시 이를 효율적으로 해결해 줄 수 있는 방안에 대한 연구가 필요하다. 즉, 컨텐츠를 판매한 후에 만일 불법적인 행위가 발생하여 소유자에 대한 판별 및 법적인 해결을 필요로하는 경우가 발생할 수 있다. 저작권자 A에 의해 생성된 컨텐츠 C_A가 만일 불법적인 유통자 B에 의해 불법적으로 도용되어 C_A를 불법적으로 배포하기 위하여 C_B를 생성하였다면, 법적인 판결 또는 검증 구조가 제시되어야 할 것이다. 합법적인 사용자 A는 자신이 생성한 컨텐츠 C_A에 자신이 생성한 워터마크 M_A를 삽입하였을 것이고, 불법적인 유통자 B는 C_A에 포함되어 있는 워터마크 M_A를 제거한 뒤에 자신이 생성한 워터마크 M_B를 삽입할 수도 있지만, M_A를 제거하지 못한 상태에서 자신의 워터마크 정보 M_B를 삽입하여 불법적인 컨텐츠 C_B를 생성하여 유통시킬 것이다. 따라서, 만일 컨텐츠에 대한 저작권 및 소유권을 증명하거나 유통되는 컨텐츠에 대한 판별 및 검증 과정이 필요할 경우 컨텐츠에 악의적인 방식으로 다중 은닉된 불법 워터마크를 검증할 수 있는 기법이 제시되어야 한다.

또한 검증 과정에서 합법적인 워터마크에 대한 정보가 유출되지 못하도록 안전한 검증 기법이 개발되어야 할 것이다. 디지털 컨텐츠에 대한 저작권 정보에 해당하는 워터마크 정보를 검증 과정에서 모두 외부에 공개하여야 한다면, 추후에 공격자에 의해서 공개된 워터마크 정보를 재삽입하여 불법적인 컨텐츠를 생성할 수도 있기 때문이다. 결국 디지털 컨텐츠에 대한 워터마크 정보는 일부 정보만이 검증자에게 제공되어야 하며, 워터마크 원래의 정보를 알고 있는 자만이 합법적으로 증명할 수 있는 기술 구조가 개발되어야 한다.

본 연구는 한국과학재단 목적기초연구(R05-2001-000-01468-0) 지원으로 수행되었음

따라서 본 연구에서는 기존 암호 기술에서 널리 사용되고 있는 영지식 증명 기법(Zero Knowledge Proofs)이 가지고 있는 증명 기능 및 안전한 검증 특성을 디지털 워터마크 검증 분야에 적용하고자 한다. 영지식 증명 기법은 건전성과 완전성을 제공하는 것으로 디지털 워터마크에 대한 검증 기능을 제공할 것이다. 물론 합법적인 워터마크 뿐만 아니라 불법적인 워터마크를 생성한 공격자 역시 자신이 삽입한 워터마크 M_B를 증명 방식으로 검증할 여지가 있기 때문에, 일종의 신뢰센터 또는 워터마크 인증 센터를 두어 합법적인 워터마크에 대한 등록 및 관리, 검증 기능을 지원하는 것이 필요하다.

구체적으로 기존의 영지식 증명 기법에 대한 분석을 바탕으로 디지털 컨텐츠에 대한 검증 기법을 제시한다. Schnorr기법과 같은 대화형(bi-directional) 영지식 증명 방식을 개선하였으며 워터마크에 대한 합법성을 검증하는 기술로 발전시켰다. 본 연구에서 제시하는 기법은 안전성 분석 및 성능 비교 분석을 바탕으로 다양한 워터마크 검증 분야에 직접 적용 가능하다.

본 연구의 구성은 다음과 같다. 2장에서 기존의 디지털 워터마크 검증 구조를 제시하고 3 장에서는 영지식 증명 기법을 고찰한다. 4장에서는 워터마크에 대한 대화형 영지식 검증 방식을 제시한다. 5장과 6장에서는 본 연구에서 제시한 기법에 대한 안전성 분석 과정과 성능에 대한 비교 분석 결과를 제시하고, 결론 및 향후 연구 방향을 제시한다.

Ⅱ. 디지털 워터마킹 검증

1. 디지털 워터마크

디지털 워터마킹은 크게 이미지 워터마킹, 오디오 워터마킹, 비디오 워터마킹으로 나눌 수 있다. 이미지 워터마킹은 디지털 이미지에 다른 사람이 제거할 수 없는 자신만의 정보를 넣어 나중에 필요할 때 검출할 수 있도록 한 기술이다. 이미지, 텍스트, 로고 등 다양한 정보를 삽입할 수 있으며 이를 통해서 저작권 침해를 억제하고, 저작자 증명 및 문서의 원본 증명이 가능하다. 나아가 본 기술은 각종 보안 관련 사업 및 전자 상거래에서의 거래 증명, 디지털 이미지를 이용한 다양한 온라인 파생 사업에 응용될 수 있다[1,2,3,25]

디지털 워터마킹에 대한 증명 방법은 크게 검증 부분과 추출 부분으로 나눌 수 있다. 워터마킹 검증(Watermark Verification)은 워터마크의 존재 여부만 검색하는 것이다. 따라서, 워터마크의 내용이나 형태는 알 수 없다. 워터마킹 추출(Watermark Extraction)은 삽입된 워터마크를 직접 검출한 후에 이를 제시하는 것이다. 따라서, 검출된 워터마크에 다양한 정보 등을 담아서 전달할 수 있다.

디지털 워터마크를 컨텐츠에 삽입하고 추출하는 과정은 다음 그림과 같다. 삽입하고자 하는 소유권 정보 또는 저작권 정보 등을 우선적으로 생성한 다음 이를 워터마크 형태로 생성한다. 생성된 워터마크는 비밀 정보에 해당하는 키를 사용하여 삽입 알고리즘을 수행하고 컨텐츠 내부에 은닉된다. 마킹된 컨텐츠를 복원하는 과정 역시 키를 사용하여 저작권 정보를 복원하는 구조로 이루어진다.

컨텐츠에 대한 메시지를 삽입하고 복원 과정에서는 은닉된 메시지가 복원되는 기술 구조를 확인할 수 있다. 삽입된 워터마크를 통해 컨텐츠에 대한 소유권을 증명하고, 궁극적으로는 컨텐츠를 보호할 수 있는 기술 구조에 해당된다.

2. 워터마킹 검증 기법

검증은 크게 비밀 워터마킹(private watermarking) 기법과 공개 워터마킹(public watermarking) 기법으로 나눌 수 있다. 비밀 워터마킹은 워터마크를 검출할 때 항상 원본 이미지가 필요하도록 한 방식이다. 어떤 경우에는 삽입된 워터마크가 필요한 경우도 있다. 따라서, 원본 이미지나 워터마크를 잃어버린 경우나 다른 사람에게 유출된 경우에는 난처한 상황이 발생할 수 있다. 하지만, 다른 방식에 비해서 상대적으로 강인성을 지닌 것으로 알려져 있다.

공개 워터마킹은 워터마크를 검출할 때 원본 이미지나 워터마크가 필요 없으며, 공개키만을 사용하여 워터마크의 존재 여부를 판단하는 방식이다. 이 방식이 현재 가장 일반적이고 보편적으로 사용되는 방식이며, 대부분의 디지털 워터마킹 기법이 이와 같은 방식을 사용하고 있다. 워터마킹에 대한 전체적인 구조는 [표 1]과 같다.

본 연구에서는 이상과 같은 디지털 워터마크 기법들에 대해 합법적인 검증 및 증명 구조를 개발하는 과정에서 영지식 증명(zero knowledge proof)을 접목하여 워터마크에 대한 공개 워터마킹 증명 기법을 제시하고자 한다. 즉, 원본 이미지나 워터마크 없이도 워터마크에 대한 존재 여부를 검증할 수 있는 방식을 제공하기 위해 암호학적인 기법 중에서 영지식 증명 기법을 적용하여 워터마크를 검증한다.

[표 1] 워터마크 기술 구조

구분 기준	워터마킹 종류
적용대상	오디오 워터마킹, 이미지 워터마킹, 비디오 워터마킹, 텍스트 워터마킹
용 도	핑거프린팅, 강인한 워터마킹, 약한 워터마킹, 가시적 워터마킹, 비가시적 워터마킹
방 법 론	공간영역 워터마킹, 주파수 영역 워터마킹, 생성키 기반 워터마킹
검증방식	비밀 워터마킹, 공개 워터마킹

Ⅲ. 영지식 증명 기법

디지털 워터마크에 대한 검증 기법에 영지식 증명을 적용하기 위해 기존의 영지식 증명 기법을 고찰해 보고자 한다. 대화형 증명 기법에서는 증명자와 검증자 사이에서 상호 작용을 통해서 증명자에 대한 신원을 검증자에게 증명한다. 이와 같이 두 엔티티에 대한 상호 증명 기법으로 사용되는 것이 영지식 증명이다.

영지식 증명에서 하나의 개체는 공개적으로 신뢰할만한 데이터베이스 또는 인증센터 기능을 수행할 수 있는 신뢰센터에 자신만이 알고 있는 비밀정보를 저장시켜 놓는다. 임의의 개체가 상대방에 대한 검증 또는 확인 기능을 수행하고자 할 경우 반복적인 영지식 증명 과정을 수행한다. 이때 영지식 증명 단계는 데이터베이스에 저장된 각 개체의 고유한 비밀 정보에 대한 노출 없이도 자신이 합법적인 개체임을 증명할 수 있다.

따라서 영지식 프로토콜을 사용하여 증명자는 검증자에게 어떠한 비밀 정보도 유출하지 않고도 자신을 검증자에게 확인할 수 있는 방법이라는 것을 의미한다. 영지식 프로토콜은 대화형 증명 시스템으로서 증명자와 검증자는 도전-응답에 해당하는 메시지를 보내게 된다. 일반적으로 난수를 사용하여 증명자는 검증자에게 자신을 증명하게 된다.

[정의 1] 영지식 증명(zero knowledge proofs: ZK)

L 을 만족하는 입력 x 를 확률적 다항 시간 튜닝 머신에 의해서 다항 시간 내에 계산된다면 L 에 대한 대화형 증명 시스템은 영지식 증명이라 한다.

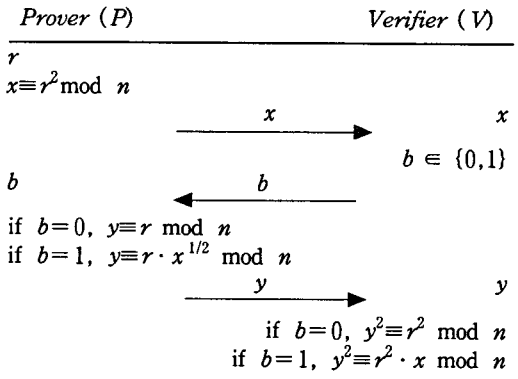
[정의 2] 대화형 증명 시스템(interactive proof systems: IP)

$L \in \{0,1\}^*$ 에서 ITM의 임의의 V 가 다음을 만족할 때 L 을 대화형 증명 시스템이라 한다. 구체적으로 아래 (조건 1)과 (조건 2)를 만족한다.

(조건 1) $\exists ITM\ P$ 에서 (P, V) 는 대화형 프로토콜이고, $|x|$ 가 충분히 큰 $\forall x \in L$ 에 대해서 $prov(V\ accepts) > \frac{2}{3}$ 을 만족할 경우.

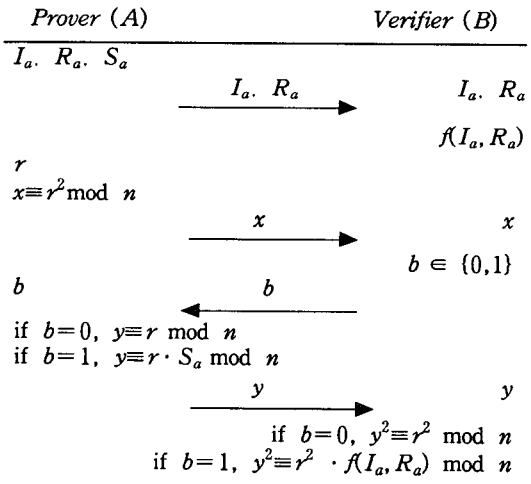
(조건 2) $\forall ITM\ P$ 에서 (P, V) 는 대화형 프로토콜이고, $|x|$ 가 충분히 큰 $\forall x \notin L$ 에 대해서 $prov(V\ accepts) > \frac{1}{3}$ 을 만족할 경우.

구체적인 영지식 증명 시스템 (P, V)는 아래 <그림 4>의 과정을 t 회 반복한다.



〈그림 4〉 영지식 증명 시스템 *(P,V)*

또한 β_i, β_{1-i}를 사용하여 A는 임의의 두 비밀 난수 z_0, z_1을 선택한 후에 γ_0, γ_1을 생성한다. 불확정 전송 기반 비대화형 워터마크 검증을 위해 $z_0, z_1 \in \{0, \ldots, p-2\}$ 에 대한 $a_0 = g^{z_0} \bmod p$ 및 $a_1 = g^{z_1} \bmod p$를 생성한다. $0 \equiv \gamma_0 * \sigma_0 \bmod 2$와 $1 \equiv \gamma_1 * \sigma_1 \bmod 2$를 만족하도록 σ_0, $\sigma_1 \in \{0,1\}^k$ $(k = |p|)$을 설정한다. 선정된 σ_1, σ_2는 비대화형 영지식 증명 기법에서 증명자와 검증자가 공통으로 공유하게 되는 부가적인 워터마크 정보에 해당한다. 부가적인 워터마크 정보를 삽입하게 되어 증명자는 검증자로부터의 도전 e, c 없이도 공개적인 검증이 가능하다. 또한 증명자는 워터마크 시스템에서의 데이터량의 최소화와 성능의 최적화를 유도할 수 있다.



〈그림 5〉 영지식 증명 시스템 *(A,B)*

결국 영지식 증명 기법의 특성을 활용하여 컨텐츠에 대한 적법한 소유권자는 자신이 컨텐츠에 합법적인 과정을 통해 삽입한 디지털 워터마크에 대해 관련되는 비밀 정보를 유출하지 않고도 자신에 대한 소유권을 공개적으로 증명할 수 있다는 것을 의미하고, 기존의 공개 워터마크 기법에서의 검증 구조를 조금 더 안전하게 발전시킬 수 있는 기술 구조를 제공할 수 있다. 또한 검증과정에서 워터마크와 관련된 비밀정보를 공개하는 것이 아니라, 증명자는 워터마크와 관련된 정보만을 검증자에게 전달하여 자신이 적법한 워터마크 소유자라는 것을 증명하는 구조이기 때문에, 영지식 증명 기법을 적용하면 효율적인 공개 워터마크 구조를 제공할 수 있다.

Ⅳ. 제안한 영지식 증명 기반 워터마크 검증

본 연구에서는 영지식 증명 기법에 기초한 대화형 워터마크 검증 기법을 제안하한다. 워터마크에 대한 검증 기능을 수행하기 위해 신뢰 센터에 워터마크 정보를 사전 등록한다. 등록 단계는 대화형 형태로 디지털 워터마크의 합법성을 검증하기 위한 전처리 과정에 해당한다.

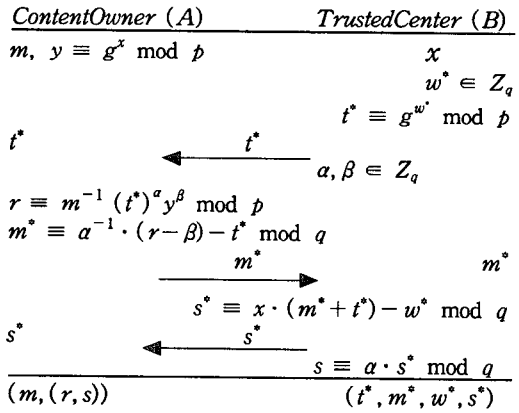
1. 워터마크 생성

증명자는 자신이 저작하였거나 적법한 형태로 소유하고 있는 컨텐츠에 대한 워터마크를 생성하여야 한다. 워터마크는 증명자에 관련된 고유 비밀정보로 구성된다. 따라서 안전한 시스템을 구축하기 위해 일반적인 암호 기술을 적용하며, 특히 공개키 암호 기법을 적용하여 증명자에 관련된 비밀 정보를 할당받는다.

컨텐츠 소유자에 해당하는 증명자는 이제 자신과 관련된 정보를 사용하여 워터마크 정보를 생성한다. 자신이 소유한 컨텐츠에 대한 저작권 정보를 m이라고 하자. 그리고, 신뢰센터의 비밀키를 x라고 하고, 신뢰센터는 t^*값을 증명자에게 전달한다. 증명자는 컨텐츠에 대한 저작권 정보 m에 대한 워터마크를 생성하기 위해 m^* 값을 생성하고 이를 신뢰센터에 전달한다. 신뢰센터는 증명자로부터 전달받은 값 m^*을 저장하고 이에 대한 확인값 s^*를 전달한다.

이제 증명자는 α와 s^*를 사용하여 s를 생성할 수 있으며 이 값은 다시 $m \equiv g^{-s} y^r r^{-1} \bmod p$ 라는 계산 과정을 통해 저작권에 관련된 비밀정보로 복원된다.

즉, 증명자는 자신이 소유한 컨텐츠에 대한 저작권 정보 m에 대해서 신뢰센터에 m^* 값을 등록하였고, 신뢰센터로부터 전달받은 s^* 값을 사용하여 워터마크 s를 생성하였다.



〈그림 6〉 워터마크 생성 프로토콜

2. 워터마크 삽입 단계

생성된 워터마크는 워터마크 삽입 과정을 수행한다. 생성된 워터마크에 관한 영지식 증명을 위해 워터마크 생성 과정에서 등록된 정보를 활용하고 부가적인 정보를 전달한다. 컨텐츠에 대한 타임스탬프 정보 T_A와 컨텐츠 소유자에 대한 정보 ID_A로 구성된 δ 값과, 센터로부터 생성된 워터마크 정보 $s \equiv \alpha \cdot s^* \bmod q$를 사용한다. 증명자 A는 검증자 B에게 증명자 A가 소유한 컨텐츠에 대한 비밀정보를 모아 $u_i \in \{0, \ldots, p-2\}$ 를 생성하고, A가 소유한 디지털 컨텐츠에 은닉하고자 하는 의사 워터마크(pseudo watermark) β_i, β_{1-i}를 생성한다. 의사 워터마크인 β_i, β_{1-i} 값은 증명자만

이 알고 있으며, 컨텐츠에 은닉된 두 값을 곱하면 워터마크 비밀정보인 s값이 나오는 구조이다. 이때 생성된 워터마크 정보는 이미지 컨텐츠인 경우 이미지 내부에 디지털 형태로 은닉되는 형태를 의미하며 오디오, 비디오와 같은 다양한 형태의 미디어에 독립적인 형태를 의미한다. 이와 같은 프로토콜을 통해 컨텐츠에 대한 워터마크 삽입 과정을 수행할 수 있고, 추후에 비대화형 검증 과정을 요청할 수 있다.

ContentOwner (A)		*DigitalContents* (D)
$\delta = (ID_A \mid T_A)) \ , \ s$		
$i \in \{0,1\} \ , \ u_i \in \{0, \ldots, p-2\}$		
$\beta_i \equiv \delta \cdot g^{u_i} \bmod p$		
$\beta_{1-i} \equiv s \cdot (\delta \cdot g^{u_i})^{-1} \bmod p$		
	$\beta_i, \ \beta_{1-i}$ ⟶	$\beta_i, \ \beta_{1-i}$
$s \overset{?}{\Longleftrightarrow} \beta_i \cdot \beta_{1-i}$		

〈그림 7〉 워터마크 삽입 프로토콜

2. 영지식 기반 워터마크 검증

워터마크에 대한 소유권 및 저작권 분쟁이 발생하였을 경우 이를 해결할 수 있는 방안으로 본 연구에서는 대화형 영지식 증명 기법을 적용한 워터마크 검증 기술을 제시한다. 워터마크를 검증할 필요가 있을 경우 컨텐츠 소유자는 신뢰센터에 컨텐츠에 대한 적법성 확인을 요청할 것이다. 따라서 우선 증명을 원하는 개체인 증명자는 컨텐츠에 대한 워터마크 정보 s 를 k개의 서브 워터마크 값으로 분할하여 $s \equiv \sum_{i=1}^{k} s_i \bmod q$ 값을 만족하도록 s_i값을 선택한다. 이렇게 해서 분할된 값에 대해 $t \equiv g^s \bmod p$ 값을 검증자에게 전달한다.

이제는 영지식 증명 방식에 따라 워터마크에 대한 비밀정보에 대한 노출 없이 워터마크에 대해 검증하는 과정을 수행한다. 검증자는 도전(challenge) 값에 해당하는 $e, \ c$ 값을 생성한 후에 이를 증명자에게 전달한다. 증명자는 응답(response)에 해당하는 y_i^e 를 생성하여 검증자에게 전달한다. 검증자는 검증단계를 수행하여 증명자에 대한 영지식 증명 과정을 수행하게 된다. 만일 증명자가 보내온 정보가 모두 검증식에 의해 정확한 식이라면, 검증자는 증명자가 워터마크에 해당하는 정보 s 를 알고 있는 적법한 컨텐츠 소유자라는 것일 믿을 수 있다. 또한 이 정보는 신뢰센터에 저장되에 있는 정보와도 일치한다는 것을 확인할 수도 있기 때문에 컨텐츠 소유자 A가 보내온 정보를 바탕으로 컨텐츠에 대한 합법성을 검증할 수 있는 구조이다. 제안한 기법은 비밀 분산 기법을 접목한 것으로 다중 워터마크 검증 환경에도 적용할 수 있는 특성을 제공한다.

Prover		*Verifier*
$s \equiv \sum_{i=1}^{k} s_i \bmod q$		
$(\ s_1, \ s_2, \ldots, \ s_k \ < \ p-1 \ )$		
$t \equiv g^s \bmod p$		
	t ⟶	t
		$e \in \{0,1\} \ , \ c$
$e, \ c$	⟵ $e, \ c$	
$y_i^e = \begin{cases} y_i^0 \equiv (s_i \cdot c + w_i) \bmod q \\ y_i^1 \equiv (s_i + w_i \cdot c) \bmod q \end{cases} \quad (1 \le i \le k)$		
	y_i^e ⟶	y_i^e
		$t^{c^{1-e}} \equiv \prod_{i=1}^{k} g^{y_i^e} \bmod p$

〈그림 8〉 워터마크 검증 프로토콜

V. 안전성 분석 및 성능 분석

디지털 컨텐츠에 대한 소유권을 증명하고 분쟁 발생을 억제하기 위해서는 신뢰센터에 컨텐츠에 대한 합법적인 워터마크 정보가 포함되어야 할 것이다. 컨텐츠 소유자 A는 신뢰센터 B에게 자신이 소유한 컨텐츠에 대한 비밀 정보에 해당하는 $u_i \in \{0, \ldots, p-2\}$를 생성하였고, 컨텐츠 소유자의 디지털 컨텐츠에 대한 저작권을 표기하기 위해 워터마크 $\beta_i, \ \beta_{1-i}$를 생성하였다. 생성된 정보는 신뢰센터에 해당하는 검증자에게 전달되며, 의사 워터마크인 $\beta_i, \ \beta_{1-i}$ 값에 대한 확인 과정을 일차적으로 수행한다. 이때 생성된 워터마크 정보는 이미지 컨텐츠인 경우 이미지 내부에 디지털 형태로 은닉되는 형태를 의미하며 오디오, 비디오와 같은 다양한 형태의 미디어에 독립적인 형태를 의미한다. 또한 $\beta_i, \ \beta_{1-i}$값에는 워터마크를 삽입하는 시점에 대한 타임스템프 T_A가 저장되어 있기 때문에 불법적인 워터마크와 합법적인 워터마크에 대한 삽입 시점에 대한 우선순위를 판단할 수 있는 주요 정보가 되기도 한다. 즉, 증명 과정에서 필요로 할 경우 타임스템프 정보를 공개하여 워터마크를 삽입한 시점을 공개하여 컨텐츠에 대한 소유권을 주장하는데 사용할 수 있다.

검증 프로토콜의 구성을 살펴보면 본 영지식 기반 워터마크 검증 단계는 이산대수 문제에 근거하고 있기 때문에 전체적인 안전성에서도 기존의 기법과 동일한 안전성을 제공한다. 또한 증명자와 검증자는 최적의 영지식 증명을 수행하기 위해서 Schnorr 기법에서 비밀 분산 기법을 적용하여 워터마크 정보를 k개의 서브 워터마크 정보 $s_1, \ s_2, \ldots, \ s_k$로 분할하였기 때문에 성능면에서도 개선된 결과를 제공한다. 결국 증명 단계가 개선된 대화형 방식으로 수행되므로 검증과정에서의 대역폭을 높이는 효과를 가져온다.

본 연구에서 제시한 기법인 경우 검증자에게 전달될 때에 아래와 같은 의사 워터마크 정보가 전달된다. 즉, 워터마크에 대한 저작권 정보 m 자체를 저장하는 것이 아니라, 신뢰센터에 등록한 워터마크 정보 s를 변형된 워터마크 방식으로 삽입하는 과정을 수행한다.

$$\beta_i \equiv \delta \cdot g^{u_i} \bmod p$$

$$\beta_{1-i} \equiv s \cdot (\delta \cdot g^{u_i})^{-1} \bmod p$$

공격자의 입장에서 얻을 수 있는 정보는 검증 프로토콜에서의 t 와 y_i^e 정보이다. y_i^e인 경우 기존의 Schnorr기법보다 복잡성이 증대된 응답(response)을 생성하게 된다.

$$y_i^e = \begin{cases} y_i^0 \equiv (s_i \cdot c + w_i) \bmod q \\ y_i^1 \equiv (s_i + w_i \cdot c) \bmod q \end{cases} \quad (1 \le i \le k)$$

따라서 공격자가 얻을 수 있는 정보는 기존의 Schnorr 기법보다 계산 측면에서 더욱 복잡한 형태로 전달된다. 따라서 제시한 기법은 기존의 기법보다 외부로부터의 공격에 더욱 안전하다는 것을 알 수 있다. 결국 본 연구에서 제시하는 기법인 경우에 워터마크 검증 시스템에 접목할 수 있으며 이산 대수에 근거한 기법으로서 수학적인 안전성을 보장할 수 있으며, 컨텐츠에 대한 다중 검증 시스템으로도 발전시킬 수 있다.

VI. 결론

컨텐츠에 대한 저작권 보호 기술에서 중요하게 연구되고 있는 분야로는 분쟁 발생시 이를 효율적으로 해결해 줄 수 있는 방안에 대한 연구가 필요하다. 즉, 컨텐츠를 판매한 후에 만일 불법적인 행위가 발생하여 소유자에 대한 판별 및 법적인 해결을 필요로하는 경우가 발생할 수 있다.

따라서 본 연구에서는 암호화 프로토콜을 적용하여 워터마크에 대한 소유권 및 저작권을 증명하고자 하였다. 기존의 프로토콜들은 비밀 워터마크 방식으로 원본 정보가 필요한 시스템이다. 그러나, 본 시스템인 경우 공개 워터마크 방식으로 원본이나 이미지 없이도 공개적으로 워터마크를 검증할 수 있는 기능을 제공한다. 이러한 목적에서 적용된 영지식 증명 기반 워터마크 검증 기법은 대화형 검증 기반 증명 방식으로서 많은 대역폭을 필요로 한다는 단점이 있다.

즉, 영지식 증명 기법의 특성을 활용하여 컨텐츠에 대한 적법한 소유권자는 자신이 컨텐츠에 합법적인 과정을 통해 삽입한 디지털 워터마크에 대해 관련되는 비밀 정보를 유출하지 않고도 자신에 대한 소유권을 공개적으로 증명할 수 있다는 것을 의미하고, 기존의 공개 워터마크 기법에서의 검증 구조를 조금 더 안전하게 발전시킬 수 있는 기술 구조를 제공하였다. 본 연구에서는 Schnorr 방식에 기초한 대화형 기반 검증 기법을 개선하여 워터마크 검증에 적합한 검증 기법으로 발전시켰다. 제안한 검증 기법은 증명자로부터의 영지식 증명 과정을 통해서 워터마크 검증 과정이 수행되므로 안전성과 검증 성능을 향상시켰다.

또한 워터마크 값에 대한 확인 과정을 수행하고 이때 생성된 워터마크 정보는 다양한 형태의 미디어에 독립적인 형태이다. 또한 워터마크를 삽입한 시점에 대한 타임스탬프 값을 통해 불법적인 워터마크와 합법적인 워터마크에 대한 삽입 시점을 비교할 수 있다. 결국 증명 과정에서 타임스탬프 정보를 공개하여 워터마크를 삽입한 시점을 공개한다면 컨텐츠에 대한 우선순위를 판별할 수도 있다. 향후 연구 과제로는 워터마크에 대한 양도 및 워터마크 정보 분할 기능을 갖는 고급 워터마크 검증 기법으로 더욱 발전시키는 것이다.

참 고 문 헌

[1] Minerva M. Yeung, "Digital Watermarking," Commuinications of the ACM, Vol 41, No. 7, pp.31-33, 1998.

[2] Christian Collberg, Clark Thomborson, "Software watermarking: model : models and dynamic embeddings," Proceeding of the 26th ACM SIGPLAN-SIGACT symposium on Principles of Programming Languages, pp.311-324, 1999.

[3] Feng Bao, "Multimedia Content Protection by Cryptography and Watermarking in Tamper-Resistant Hardware," Proceeding of the fourth ACM international conference on Multimedia, pp.139-142, 2000.

[4] G. J. Simmons, "A Survey of Information Authentication," *Proceedings of the IEEE*, Vol. 76, No. 5, pp. 603-620, May, 1988.

[5] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, pp. 472-492, Nov. 1976.

[6] W. Diffie, "The First Ten Years of Public-Key Cryptography," *Proceedings of the IEEE*, Vol. 76, No. 5, pp. 560-577, 1988.

[7] C. P. Schnorr, "Efficient Identification and Signatures for Smart Cards," *Advances in Cryptology, Proceedings of Crypto'89, Springer-Verlag*, pp. 239-252, 1990.

[8] T. Okamoto, "Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes," *Advances in Cryptology, Proceedings of Crypto'92, Springer-Verlag*, pp. 31-53, 1993.

[9] B. Schneier, *Applied Cryptography, 2nd Edition*, John Wiley & Sons Press, 1996.

[10] A. J. Menezed, P. C. van Oorschot, S. A. Vanstone, Handbook of Applied Cryptography, *CRC Press*, 1996.

[11] A. Fiat and A. Shamir, "How to Prove Yourself: Practical Solution to Identification and Signature Problems," *Advances in Cryptology, Proceedings of CRYPTO'86, Springer-Verlag*, pp. 186-199, 1987.

[12] U. Feige, A. Fiat, A. Shamir, "Zero Knowledge Proofs of Identity," Proceedings of the 19th Annual ACM Symposium of Theory of Computing, pp. 210-217, 1989.

[13] L. C. Guillou and J. J. Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory," *Advances in Cryptology, Proceedings of Eurocrypt'88, Springer- Verlag*, pp. 123-128, 1989.

[14] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms," *IEEE Transactions on Information Theory*, Vol. IT-30, No. 4, pp. 469-472, Jul. 1985.

[15] R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, Vol. 21, No. 2, pp. 120-126, 1978.

[16] S. Goldwasser, S. Micali, C. Rackoff, "The Knowledge Complexity of Interactive Proofs," SIAM Journal of Computing, Vol. 18, No. 1, pp. 186-208, 1989.

[17] K. Ohta and T. Okamoto, "A Modification of the Fiat-Shamir Scheme," *Advances in Cryptology, Proceedings of Crypto'88, Springer-Verlag*, pp. 232-243, 1989.

[18] M. Rabin, "How to exchange secrets by oblivious transfer," Technical Reports TR-81, Harvard Aiken Computation Laboratory, 1981.

[19] M. Bellare, S. Micali, "Non-Interactive Oblivious Transfer and Applications," Advances in Cryptology - Crypto 89, Lecture Notes in Computer Science, Vol. 435, Springer-Verlag, 1989.

[20] M. Blum, P. Feldman, S. Micali, "Non-Interactive Zero-Knowledge Proof Systems and Applications," *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, 1988.

[21] A. D. Santis, G. D. Crescenzo, P. Persino, "Randomness-Efficient Non-Interactive Zero Knowledge," ICALP'97 Conference, 1997.

[22] A. D. Santis, S. Micali, G. Persiano, "Non-Interactive Zero-Knowledge Proof-Systems," *Advances in Cryptology - Crypto'87*, Vol. 293, 1988.

[23] A. D. Santis, S. Micali, G. Persiano, "Non-Interactive Zero-Knowledge Proof-Systems with Preprocessing," *Advances in Cryptology - Crypto'88*, Vol. 403, 1989.

[24] S. Micali, "Fair Cryptosystems," Technical Reports MIT/LCS/TR-579-b, 1993.

[25] Jian Zhao, "A Digital Watermarking System for Multimedia Copyright Protection," Proceeding of the fourth ACM international conference on Multimedia, pp.443-444, 1996.

[26] Gang Qu, Jennifer L. Wong, Miodrag Pothonjak, "Fair Watermarking Techniques," Proceedings of the 2000 Conference on Asia and South Pacific Design Aotumation, pp.55-60, 2000.

[27] Scott Craver, "Zero Knowledge Watermark Detection," Information Hiding Workship, Lecture Notes in Computer Science, Vol. 1768, pp.101-116, 1999.