디지털 핑거프린팅과 구매자/판매자 워터마킹의 기술동향

Technical Trends of Digial Figerprinting & Buyer-Seller Watermarking

유원영(W.Y. Yoo) 콘텐츠보호연구팀 연구원
서영호(Y.H. Seo) 콘텐츠보호연구팀 책임연구원, 팀장
최재귀(J.G. Choi) 부경대학교 정보보호학과 박사과정
박지환(J.H. Park) 부경대학교 전자컴퓨터정보통신공학부 교수

멀티미디어 기술의 발달과 기반 통신 시설의 발달에 따라 네트워크를 통한 디지털 데이터의 유통이 빈번해졌다. 하지만 이러한 네트워크를 기반으로 한 콘텐츠 시장이 활성화되기 이전에 콘텐츠가 의도된 목적과 콘텐츠에 대한 합법적이고 정당한 권리를 산 사용자에 의해서만 유통되어야 하는 메커니즘이 먼저 확고하게 놓여야 한다. 그러한 메커니즘을 위해서 최근 들어 DRM이나 디지털 워터마킹 같은 기술들이 많이 연구되고 있다. 디지털 핑거프린팅은 디지털 워터마킹 기술을 기반으로 한 새로운 형태의 멀티미디어 저작권 보호의 한 방법이다. 본 고에서는 계산량과 안전성을 개선하기 위해 연구되어 온 디지털 핑거프린팅과 판매자/구매자 워터마킹 기술에 대한 주요 연구들을 살펴본다.

I. 기술 개요

1. 디지털 핑거프린팅의 요구사항

디지털 워터마킹(digital watermarking) 기법이 인간의 의식 체계 또는 감지 능력으로는 검출할 수 없게 저작권자 또는 판매자의 정보를 멀티미디어 콘텐츠 내에 삽입하여 이후에 발생하게 될 지적 재산권 분쟁에서 정당함을 증명하는 데 사용되는 반면, 디지털 핑거프린팅(digital fingerprinting)은 기밀 정보를 디지털 콘텐츠에 삽입하는 측면에서는 디지털 워터마킹과 동일하다고 볼 수 있으나, 저작권자나 판매자의 정보가 아닌 디지털 콘텐츠를 구매한 사용자의 정보를 삽입함으로써 이후에 발생하게 될 콘텐츠 불법 배포자를 추적하는 데 사용되는 기술이다. 즉 디지털 워터마킹을 사용하였을 때는 판매되는 모든 콘텐츠에 삽입되는 정보가 동일한 반면, 핑거프린팅을 사용하였을 때는 판매되는 콘텐츠가 구매한 사용자들마다 조금씩 다른 정보를 가지므로 만약

<표 1> 디지털 핑거프린팅의 요구사항

비가시성 Imperceptibility)	콘텐츠의 가치를 그대로 유지함과 동시에 삽입 정보가 인간의 시각이나 감각에 의해 감지될 수 없어야 한다.
견고성 Robustness)	정보가 삽입된 콘텐츠의 변환, 재샘플링, 재양자화, 압축 등과 같은 일반적인 신호 처리뿐만 아니라 회전, 이동 등 기하학적 영상 변환에도 삽입정보가 유지되어야 한다.
유일성 Uniqueness)	검출된 삽입정보는 저작자/구매자를 명확하게 특정할 수 있어야 한다.
공모허용 Collusion olerance)	핑거프린팅된 콘텐츠는 삽입되는 내용이 구매자마다 다르므로 다수의 구매자들이 자신의 콘텐츠를 비교하여 삽입 정보를 삭제하거나 다른 사용자의 정보를 삽입한 콘텐츠로 위조하여 배포할 수 있으므로, 이와 같은 공격에 견고하기 위해 아무리 많은 콘텐츠가 주어지더라도 핑거프린트(삽입 정보)를 찾거나 삭제할 수 없어야 하고 새로운 핑거프린트를 생성할 수 없어야 한다.
비대칭성 Asymmetry)	핑거프린팅된 콘텐츠는 판매자는 알지 못하고, 구매자만이 알아야 한다.
익명성 Anonymity)	구매자의 익명성을 보장해야 한다.
조건부 추적성 Conditional raceability)	정직한 구매자는 익명으로 유지되는 반면, 불법 배포한 부정자는 반드시 추적할 수 있다.

콘텐츠가 불법적으로 재배포된다면 해당 콘텐츠 내에서 핑거프린팅된 정보를 추출하여 어떤 구매자에게 판매된 콘텐츠임을 식별할 수 있게 되어 법적인 조치를 가할 수 있게 된다. 따라서 일반적인 구매자들로 하여금 불법적인 재분배에 대한 의욕을 저하시키고, 생산자들의 창작의욕을 고취시켜 디지털 콘텐츠 산업의 발전에 좋은 영향을 줄 수 있을 거라 기대된다.

이러한 핑거프린팅 기술은 소유권에 대한 인증뿐만 아니라 개인 식별 기능까지 제공해야 하므로 기존의 워터마킹이 갖추어야 할 요구사항인 비가시성, 견고성, 유일성과 더불어 공모 허용, 비대칭성, 익명성, 조건부 추적성 등이 부가적으로 필요하다. <표 1>에 핑거프린팅의 요구사항을 나타낸다.

2. 디지털 핑거프린팅의 공모 공격

앞에서도 언급하였듯이 디지털 워터마킹이 삽입된 콘텐츠와는 달리 핑거프린팅이 삽입된 콘텐츠는 삽입되는 내용이 구매자마다 모두 다르다. 따라서 다수의 구매자들이 서로 공모하여 핑거프린팅이 삽입된 콘텐츠를 서로 비교하여 핑거프린팅 위치가 파악되면 핑거프린팅 비트를 지우거나, 전혀 상관없는 핑거프린팅 비트를 만들어 삽입해 콘텐츠를 재구성하여 이를 재분배할 수 있게 된다. 이렇게 공격자가 여러 개의 콘텐츠를 서로 비교하여 핑거프린팅 정보를 제거하거나 혹은 유추하여 다른 핑거프린팅 정보를 삽입할 수 있는 공격을 공모 공격(collusion attack)이라 한다. 대부분의 핑거프린팅 추출방법이 상관계수를 이용한 방법이기 때문에 공모 공격은 상관계수 값이 작게 나오도록 하는 방법이 주를 이룬다. <표 2>에 현재까지 연구된 공모공격의 유형을 나타낸다[1].

<표 2> 디지털 핑거프린팅의 공모 공격의 유형

평균화공격 (Averaging Attack)	핑거프린팅된 다수의 콘텐츠를 서로 평균하여 새로운 콘텐츠를 생성하는 공격법이다.
최대최소공격 (Max-Min Attack)	공모에 참가한 핑거프린팅된 콘텐츠에서 최소값과 최대값을 구한 후 그 평균값으로 새로운 콘텐츠를 생성하는 공격법이다.
상관계수 음수화공격 (Negative-Correlation Attack)	상관계수를 이용하여 핑거프린팅 정보를 추출할 경우, 상관계수의 값을 음수로 만들어 공모자의 추출을 어렵게 만드는 공격이다.
상관계수 제로화공격 (Zero-Correlation Attack)	상관계수 음수화 공격이 상관계수를 음수로 유도하지만 핑거프린팅 정보가 지워졌다는 의미는 아닌 반면, 제로화 공격은 상관계수를 0에 가깝게 유도하여 핑거프린팅 정보의 검출이 불가능하도록 만드는 공격이다.
모자익공격 (Mosaic Attack)	공모에 참여한 콘텐츠의 최대, 최소값을 이용하여 상관계수의 값을 작게 만드는 공격과는 달리 핑거프린팅된 콘텐츠를 기하학적 모양으로 작게 나누어 새로운 콘텐츠를 생성하는 공격법으로 워터마킹의 잘림(cropping) 공격과 유사하다. 핑거프린팅 정보의 추출은 파일단위로 이루어지기 때문에 웹상에서 여러 조각으로 나누어진 이미지 콘텐츠의 경우 추출이 어려워진다.

Ⅱ. 최근 기술 동향

- 대칭형 방식(Symmetric scheme): 초기의 핑거프린팅 방식[2],[3]은 판매자가 콘텐츠에 삽입되는 구매자의 정보를 알고 있다는 점에서 대칭형 기법이다. 대칭형 핑거프린팅이란 의미는 구매자가 판매자에게서 콘텐츠를 구입하려고 할 때, 핑거프린트가 삽입된 콘텐츠를 판매자도 알고 구매자도 안다는 의미이다. 이것은 나중에 불법적으로 배포된 콘텐츠를 발견하고 이에 대한 구매자를 식별해 냈을 때, 지적 재산권 침해에 대한 완벽한 증명이 불가능함을 내재하고 있다. 왜냐하면 구매자가 핑거프린트된 콘텐츠를 구입하였다는 사실을 판매자도 알고 있기 때문에 구매자가 실제로 해당 콘텐츠를 불법 재분배하였는지 아니면 판매자가 구매자를 가장하여 불법 재분배를 하였는지 구별해 낼 수 없기 때문이다.
- 비대칭형 방식(Asymmetric scheme): Pfitzmann [4]과 Memon[5] 등은 비대칭형 핑거프린팅이라는 새로운 개념을 도입하여 대칭형 방식의 문제점을 해결하였다. 비대칭형 핑거프린팅 방식은 구매자가 콘텐츠를 구매하는 과정에서 판매자는 핑거프린트된 콘텐츠를 알지 못하도록 하는 핑거프린팅 프로토콜이다. 따라서 불법적인

재분배물로부터 핑거프린트를 추출하여 구매자를 식별하는 것이 가능하다면 그것 자체가 지적 재산권 침해의 완벽한 증거가 될 수 있는 것이다.

- 익명 비대칭형 방식(Anonymous scheme): Pfitzmann 등은 구매자의 익명성을 보장하는 익명 핑거프린팅 프로토콜을 제시하였다[6]. 이것은 비대칭형 핑거프린팅 개념을 포함하는 프로토콜로서 판매자는 구매자에게 콘텐츠를 판매하지만 프로토콜 진행과정에서 구매자의 신원을 알지 못하도록 하는 프로토콜이다. 이것은 구매자가 사전에 제3자에게 임시 ID를 등록하고 진행하는 프로토콜이기 때문에 판매자는 재분배자 식별 프로토콜을 진행할 때 제 3자의 도움을 받음으로써 구매자의 신분을 밝혀낼 수 있다.

최근의 핑거프린팅에 대한 연구는 공모에 대한 방지를 효과적으로 구현하는 공모 보안 코드에 관한 연구와 계산량과 안전성을 개선하여 디지털 핑거프린팅의 실현 가능성을 높이는 연구에 중점을 두고 진행되고 있다. 특히 후자의 경우는 디지털 핑거프린팅[6]-[11]과 소비자-판매자 워터마킹(buyer-seller watermarking protocol)[3],[5],[12],[13]이라는 개념으로 크게 나누어 연구되고 있다. 전자의 방식의 대부분은 구매자, 판매자 그리고 구매자의 익명성을 제공하기 위한 신뢰센터가 필수 참가 개체이고, 공모 보안 코드로 Boneh의 공모 보안 코드[14]를 사용한 반면, 후자의 방식은 콘텐츠에 구매자(소비자)의 워터마크와 판매자의 워터마크를 같이 삽입하는 방식으로 구매자, 판매자, 그리고 익명성 제공을 위한 신뢰센터 외에 구매자의 유일한 워터마크를 생성해 주는 워터마크 신뢰 센터가 참가 개체로 추가되며, 공모공격을 위해서는 이에 안전하다고 실험된 Cox의 워터마킹 삽입/추출 알고리듬[15]을 사용하는 차이가 있다. 두 방식 모두 콘텐츠를 판매하는 판매자가 핑거프린팅된 콘텐츠를 접근할 수 있는지 없는지에 따라 대칭형과 비대칭형으로 구분되며, 최근 연구방식은 주로 삽입 정보와 구매자에 대한 비대칭성과 익명성을 효율적으로 충족시키기 위한 방향으로 진행되고 있다.

Ⅲ. 기술 내용

1. 디지털 핑거프린팅

가. 대칭형 핑거프린팅[2]

대칭형 핑거프린팅은 초기의 연구기법으로 핑거프린팅 프로토콜, 구매자 판별 프로토콜의 두 가지 알고리듬과 구매기록을 위한 데이터 베이스로 구성된다. 두 알고리듬은 모두 판매자에 의해 수행되므로 판매자가 핑거프린팅된 콘텐츠를 생성할 수 있다.

먼저 핑거프린팅 할 콘텐츠와 구매한 사용자의 식별자, 현재까지 판매된 리스트를 입력으로 하여 핑거프린팅을 한다. 그에 대한 결과물로 핑거프린팅된 콘텐츠와 구매레코드가 생성된다. 만약 핑거프린팅된 콘텐츠가 어떤 구매자에 의해서 불법 복제되고 배포되었다면 판매자는 발견된 복사본과 핑거프린팅 되기 전의 콘텐츠, 그리고 구매기록을 입력으로 발견된 복사본의 원 구매자를 찾아내게 된다.

그러나 이 방법의 문제점은 판매자와 구매자 모두 핑거프린팅된 콘텐츠를 접근할 수 있으므로 불법 복제되어 유통된 콘텐츠가 발견된 경우, 이를 유통시킨 주체가 구매자인지 혹은 판매자인지를 판단하기가 모호하다. 따라서 책임 규명이 분명치 않다는 문제점을 갖는다.

나. 비대칭형 핑거프린팅

대칭형 핑거프린팅 방식의 문제점을 보완하기 위해 비대칭형 핑거프린팅 방식[4]이 제안되었다. 이 방식은 판매자와 구매자가 2-party 프로토콜에 참여함으로써 구매자만이 핑거프린팅된 콘텐츠를 접근할 수 있도록 한다. 이는 판매자가 불법 복사된 콘텐츠를 찾은 후에 불법 배포자의 잘못을 신뢰된 제3자를 통하여 증명함으로써 책임 규명을 분명히 한다. 초기의 비대칭형 핑거프린팅은 구매자의 익명성을 제공하지 못했으나, Pfitzmann에 의해 처음으로 익명 핑거프린팅의 개념[6]이 소개되면서 비대칭형 핑거프린팅 개념을 포함한 비대칭 익명 핑거프린팅[7]-[12]이 이 분야의 주를 이루게 되었다. 아래는 몇 가지 익명 비대칭 프로토콜에 대한 설명이다.

1) Pfitzmann 프로토콜[6]

Pfitzmann은 처음으로 익명 핑거프린팅의 개념을 소개하면서 공모가 없는 상황을 가정한 프로토콜을 먼저 제시하였다. 그리고 이 프로토콜을 공모 허용성을 가지는 프로토콜로 발전시키기 위한 프로시저에 대한 연구를 하였다. 아래는 전자의 설명이다.

- 등록(Registration): 구매자는 임시 공개키/비밀키 쌍을 만들어 등록센터(registration center)에 본인 확인 절차와 키 검증 절차를 거친 후, 임시 공개키에 대한 등록 센터의 인증서를 받는다. 이 과정에서 임시로 만든 공개키와 실제 본인의 신원이 등록 센터에 저장되게 된다.
- 핑거프린팅(Fingerprinting): 구매자는 콘텐츠를 구입한다는 내용의 문장 ***text*** 를 만들고, 여기에 자신이 등록 센터에 등록한 공개키에 해당하는 비밀키로 서명을 한다. 그리고 서명과 ***text*** , 구매자의 임시 공개키, 그리고 공개키에 대한 인증서를 연결하여 삽입정보 ***emb***를 만든다. 이제 만들어진 ***emb***는 Minimum Disclosure Proof of Knowledge(MDPK) 프로토콜을 사용하여 콘텐츠에 삽입하는 절차를 밟는다. 여기서 판매자는 삽입 정보 ***emb***의 내용은 알 수 없지만, 구매자의 임시 공개키와 그에 대한 인증서를 영지식 증명을 통해서 확인할 수 있으며 구매자의 서명의 유효성에 대해서도 영지식 증명을 통해서 확인받게 되기 때문에 삽입 정보의 유효성에 대해 확신할 수 있게 된다.
- 식별(Identification): 불법으로 재분배된 콘텐츠를 발견하게 되었을 때, 이 식별과정을 통하여 콘텐츠에 삽입된 정보 ***emb***를 추출해내게 된다. 이것이 지적 재산권 침해에 대한 첫번째 증거가 된다. 그리고 이것을 등록 센터에 보내고 임시 공개키에 해당하는 사람의 신원을 알려주도록 요청하거나 유죄를 입증해 주도록 요청하게 된다. 이 요청에 대한 등록 센터의 응답 내용이 두 번째 증거가 된다.
- 재판(Trial): 재판과정에서 3단계에서 추출된 2가지의 증거를 보이면, 재판관은 이것과 재분배한 것으로 고소된 구매자의 서명을 비교하여 최종적인 판결을 하게 된다.

Pfitzmann 프로토콜의 단점은 다음과 같다. 첫째로, 핑거프린팅 단계에서 MDPK 프로토콜을 블랙박스 형태로 삽입하여 구현하였는데 이 프로토콜은 내부적으로 이산 대수 문제 또는 그래프 동형 문제와 같은 어려운 문제를 기반으로 구현되어 있다. 일반적으로 워터마킹은 미리 오프라인에서 계산한 후, 판매 시에는 워터마킹된 콘텐츠를 제공하면 된다. 이에 반해 핑거프린팅의 경우에는 구매자마다 삽입 정보가 달라지기 때문에 임의의 구매자가 인터넷 상으로 판매자의 서버에 접속하여 실시간으로 핑거프린팅 프로토콜을 거치며 판매가 이루어져야 하므로, 복잡도가 높은 계산을 한다는 것은 실제 구현에 불합리하다는 결론을 내릴 수 있다. 핑거프린팅 과정에서의 계산적 복잡도는 프로토콜의 비교에서 중요한 기준이 된다.

둘째로, 식별 단계에서 판매자는 추출해 낸 증거를 등록 센터에 보내고 결과를 기다려야 한다. 이것은 등록 센터가 소수이고 판매자가 다수일 때 등록 센터가 처리할 일이 많아진다는 문제가 있으며, 등록 센터의 신뢰성이 높아져야 한다는 가정이 전제되어야만 한다.

2) 재분배자의 자동 식별 기능을 가지는 디지털 핑거프린팅[7]

위에서도 언급했듯이 등록 센터와 상호 작용을 통하여 재분배자를 식별하는 방식은 등록 센터의 작업량이 증가되는 문제를 가지게 된다. Domingo는 이를 개선하여 판매자 스스로 재분배자를 식별하는 방식을 제안하였다.

- 등록: 구매자는 다음과 같은 순서로 등록 센터에 등록하게 된다.
  먼저 등록 센터는 랜덤 비밀 값 $x_r \in Z_p$ 를 선택하고, $y_r = g^{x_r} \bmod p$ 를 계산하여 구매자에게 y_r 를 전송한다. 구매자는 $x_1 + x_2 = x_B$ 를 선택하고 $S_1 = y_r^{x_B}, S_2 = y_r^{x_2} \bmod p$ 를 계산하여 등록센터에 S_1 과 S_2 를 전송한다. 그러한 후에 구매자는 자

신이 x_1, x_2를 알고 있다는 사실을 영지식 증명을 이용하여 등록 센터에 증명한다. 구매자는 핑거프린팅에서 공개키로 사용할 $y_2 = g^{x_2}$를 계산하여 등록센터에 전송한다. 핑거프린팅 프로토콜에서 S_1은 익명성을 제공하기 위한 인증 정보로 사용된다. 등록센터는 구매자로부터 받은 S_1과 S_2가 $S_1 S_2 = y_B^{x_r}$을 만족하고, 익명성을 제공하는 공개키 y_2가 $y_2^{x_r} = S_2$를 만족하는지 검증한다. 2번의 검증이 성공한다면, 등록센터는 인증서 $Cert(S_1 \| y_r)$과 $Cert(S_2 \| y_r)$를 생성하고, 처음에 선택한 랜덤한 비밀 값 x_r과 함께 인증서를 구매자에게 전송한다.

- 핑거프린팅: 구매자 B는 콘텐츠를 구입한다는 내용의 문장 *text*를 만들고, 여기에 등록단계에서 설정한 x_2로 서명 *sig*를 생성한다. 그리고, y_r, y_2, $[S_1, Cert(S_1 \| y_r)]$, *text*를 판매자에게 전송한다. 이때 서명 *sig*는 보내지 않는다. 판매자는 S_1의 인증서를 검증해서 이상 유무를 파악한다.

  만약 이상이 없으면, 구매자와 판매자는 SMPC (Secure Multi-Party Computation) 프로토콜을 이용하여 핑거프린팅 프로토콜을 수행한다. SMPC 프로토콜은 서로의 입력을 보여주지 않으면서 올바른 입력을 하였는지 서로 확인할 수 있는 기능 및 계산된 결과값을 양측에 비밀리에 전달해주는 기능도 지원해준다. 이 프로토콜에 따라 구매자는 입력으로 x_r, *sig*, S_2, $Cert(S_2 \| y_r)$를 넣고, 판매자는 y_r, *text*, y_2와 판매할 콘텐츠를 입력으로 넣는다. 세 가지의 결과 값 중에서 처음 두 값은 판매자에게만 전달되는 것으로 구매자가 올바른 입력을 제공하였는지를 검증할 수 있는 참, 거짓의 출력이다. 만일 이 둘 중 하나라도 거짓이 출력되면 세번째 결과 값은 계산되지 않는다. 세번째 결과 값은 아래의 *emb*가 삽입된 콘텐츠이다.

$$emb = text \| sig \| y_2 \| x_r \| y_r \| S_2 \| Cert(y_r \| S_2)$$

  *emb*가 삽입된 콘텐츠는 구매자에게만 전달되며, 판매자는 자신의 판매 기록에 $[S_1, Cert(S_1 \| y_r)]$을 기록해 놓는다.

- 식별 프로토콜: 불법적으로 재분배된 콘텐츠가 발견되면 판매자는 콘텐츠에서 *emb*를 추출해낸다. 그리고 *emb* 값의 y_r 값과 연관되어 있는 값을 자신의 저장된 판매 기록에서 찾는다. 판매자는 *emb*를 구성하고 있는 요소들의 무결성을 검증한 후, $S_1 S_2 = y_B^{x_r}$을 만족하는 y_B가 나올 때까지 공개키 디렉토리를 검색한다.

이 방식은 재분배자의 자동식별을 제공한다는 장점이 있지만, 첫째로 재분배자를 식별하는 과정에서 만족하는 공개키가 발견될 때까지 지수 연산을 반복해야 하므로 평균 N/2번의 지수 연산(N: 공개키 디렉토리에 있는 공개키들의 수)을 요구한다는 단점이 있다. 이 단점은 후에 전자상거래에서 효율적으로 사용될 수 있도록 등록 프로토콜을 2-pass로 간소화하고, 식별 프로토콜에서 지수 연산을 한 번하여 재분배자를 식별하는 보다 효율적인 핑거프린팅 방식이 제안되어 해결되었다[8].

두번째의 단점은 앞의 Pfitzmann 프로토콜과 마찬가지로 핑거프린팅 단계에서 SMPC라는 블랙 박스 형태의 프로토콜을 도입하여 익명성을 구현하였다는 것이다. 이 SMPC의 계산적 복잡도는 MDPK 프로토콜의 계산적 복잡도와 비슷하므로, 이 방식 역시 핑거프린팅 단계에서 높은 계산적 복잡도가 필요하다는 단점은 극복하지 못했다.

3) Committed Oblivious Transfer 기반의 디지털 핑거프린팅[9]

Domingo-Ferrer은 최근 Committed Oblivious Transfer(COT) 기법을 응용하여 명확하게 분석되지 않은 계산량을 지니는 기존의 방식을 개선하였다. 이 방식은 등록 단계에서는 기존의 [7] 방식을 그대로 유지하나, 핑거프린팅 단계에서 COT를 이용함으로써 계산적 복잡도를 분석하여 핑거프린팅의 실현 가능성을 보여 주었다.

이 방식은 판매자가 콘텐츠의 각 비트마다 서로 다른 2개의 비트를 준비하고, 이를 COT의 입력 값으로 설정함으로써, 판매자는 후에 구매자가 어떤 비트를 선택하는지 알 수 없도록 하고, 구매자는 자

신이 선택한 이외의 정보는 알 수 없도록 하여 핑거프린팅의 비대칭성을 제공한 방식이다. 이 방식은 계산적 복잡도가 가장 높은 핑거프린팅 단계에서 COT를 사용하였기 때문에 익명 핑거프린팅 프로토콜의 실제 적용 가능성을 높였다고 평가된다. 실제로 COT는 명백하게 계산적 복잡도가 분석되어 있는 기법으로서 기존의 MDPK나 SMPC를 이용하던 익명 핑거프린팅 프로토콜보다 훨씬 구현 가능한 복잡도를 가진다고 볼 수 있다.

그러나 이 방식의 문제점은 [10]에서 지적되었듯이, 첫째 COT 프로토콜을 수행할 때 판매자가 2개의 입력 값을 같은 값으로 한다면, 판매자는 구매자가 어떤 콘텐츠를 선택하는지 쉽게 알 수 있으므로 대칭형 방식이 가지는 문제점을 여전히 가지고 있다. 둘째, 식별단계가 비효율적이라는 문제점이 여전히 남아 있다. 실제로 식별 단계에서는 해당 콘텐츠를 구매한 다수의 구매자들 각각에 대해서 모두 식별 프로토콜을 수행해야 하는 비효율성을 지니고 있다.

4) 전자 화폐 기반의 디지털 핑거프린팅[11]

실제적으로 이 방식의 프로토콜을 크게 두 부분으로 나누어 보면, 첫번째 부분은 등록센터에 구매자가 자신의 임시 공개키를 등록하고 인증서를 발급받아서, 이것이 나중에 식별 단계에서의 구매자의 신분을 밝혀 내는 중요한 요소로 작동하게 하는 부분이며, 두번째 부분은 실제적으로 삽입 정보를 콘텐츠에 삽입하여 핑거프린팅된 콘텐츠를 만들어 내는 부분이다. 이 방식에서는 첫번째 부분의 효율성을 높이기 위한 시도를 하였다. 기존의 방식들이 등록센터에 구매자가 임시 공개키를 등록하는 것으로 했지만, 이 방식에서는 이것을 전자 화폐의 개념을 응용하는 것으로 대체하였다. 여기서 사용되는 전자화폐는 단순히 등록 및 식별 단계에서 사용될 뿐이지 화폐적인 가치는 지니지 않는다. 이러한 접근 방식은 전자 화폐가 기본적으로 내포하고 있는 특성을 이용하여 사용자의 익명성을 유지하면서도 조건부 추적성을 이용한 재분배자 식별을 가능하게 만들었다. 그러나 핑거프린팅 단계에서의 계산적 복잡도는 역시 해결되지 못한 상태로 남아 있는 단점이 존재하나, 첫번째 부분을 명확하게 분석이 가능한 암호학적 요소들을 사용했다는 측면은 장점이라고 본다.

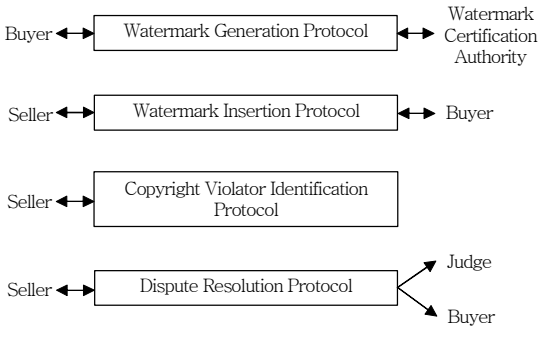
현재까지 제안된 핑거프린팅 기법 중에서 사용자의 등록 및 식별단계의 계산적 복잡도를 낮춘 프로토콜로는 전자화폐를 기반으로 한 방식[11]을, 콘텐츠에 정보를 삽입하는 단계에서의 시간적 복잡도를 명백하고 실제적으로 낮춘 프로토콜로는 안전성에 문제를 지니고 있으나 COT를 기반으로 한 방식[9]을 각각 현재까지의 최선의 해결책이라 평가되고 있다.

2. 구매자-판매자 워터마킹

가. Memon의 방식[5]

Memon 등은 워터마킹 기법(private watermarking)과 동형 속성(homomorphic property)을 가지는 공개키 암호 알고리듬에 기반하여 구매자-판매자 워터마킹이라는 용어를 사용하여 콘텐츠 불법 배포자 추적 방식을 제안하였다. (그림 1)은 Memon의 방식을 도표로 나타낸 것이다.

- 워터마크 생성(Watermark generation): 구매자는 유용한 워터마크를 얻기 위해 자신의 인증서와 공개키 (K_B)를 워터마크 신뢰센터(watermark certification authority)에게 전송한다. 워터마크 신뢰센터는 워터마크를 생성하고, 이를 구매자



(그림1) Momen의 구매자-판매자 워터마킹 프로토콜

의 공개키로 암호화한 $E_{K_B}(W)$ 과 이에 대한 서명 $Sign_C(E_{K_B}(W))$ 을 구매자에게 전송한다. 이 때 $E_{K_B}(W)$ 는 (1)을 의미한다.

$$E_{K_B}(W) = E_{K_B}(\{w_1, w_2, ..., w_{n)}\}) = \{E_{K_B}(W_1), E_{K_B}(w_2), ..., E_{K_B}(w_n)\} \quad (1)$$

그리고 $Sign_C(E_{K_B}(W))$ 은 $E_{K_B}(W)$ 가 신뢰센터에서 생성된 타당한 워터마크임을 입증한다.

- 워터마크 삽입(Watermark insertion): 구매자는 암호화된 워터마크 $E_{K_B}(W)$ 와 신뢰센터의 서명 $Sign_C(E_{K_B}(W))$ 를 판매자에게 보내고, 판매자는 이것이 검증되면, 구매자에게 유일하게 연결되는 새로운 워터마크 V 를 생성하여 콘텐츠 X 에 삽입한다. 워터마크 V 가 삽입된 콘텐츠를 X' 라 두자. V 는 불법 배포된 콘텐츠의 부정 배포자에 대한 명확한 증거는 아니지만, 후에 부정 배포자를 식별하기 위해 사용되어진다. 판매자는 구매자로부터 받은 $E_{K_B}(W)$ 을 치환하기 위해 치환함수 σ : $\sigma(E_{K_B}(W)) = E_{K_B}(\sigma(W))$ 를 생성한다. 판매자는 먼저 $E_{K_B}(W)$ 를 치환하고, 이를 X' 에 삽입하기 위해 X' 를 K_B 를 이용해 암호화한 후, (2)의 과정을 수행한다.

$$E_{K_B}(X'') = E_{K_B}(X') \oplus E_{K_B}(\sigma(W)) = E_{K_B}(X' \oplus \sigma(W)) = E_{K_B}(X \oplus W \oplus V) \quad (2)$$

이때 사용되는 암호 방식은 동형 속성을 지니는 공개키 암호 알고리듬이고, $\oplus$ 는 콘텐츠에 워터마크를 삽입하는 연산 기호이다. 그리고 공모 공격에 안전하기 위해서 워터마크 삽입 및 추출 알고리듬으로 Cox의 알고리듬을 사용한다. 판매자는 판매 기록에 구매자의 ID (K_B) 와 $E_{K_B}(W)$, V , $Sign_C(E_{K_B}(W))$, σ 를 저장하고, $E_{K_B}(X'')$ 는 구매자에게 전송한다. 이 때 판매 기록 레코드는 해당 콘텐츠 X 를 구매한 전 구매자에 대한 정보를 저장한 것이다. 암호화된 콘텐츠를 받은 구매자는 자신의 비밀키를 이용하여 이를 복호한 후 사용한다.

- 식별: 불법 배포된 콘텐츠 Y 가 발견되면, 판매자는 여기에서 먼저 V' 를 추출한다. 강인한 워터마킹 알고리듬이 전제된다면, 판매자는 Y 에서 V' 를 추출할 수 있을 것이다. 이 V' 와 해당 콘텐츠의 판매 기록 레코드의 V 와 비교하여 상관도가 가장 높은 V 를 찾고, 이에 해당하는 구매자의 ID도 찾을 수 있을 것이다. 이 구매자가 부정 배포자가 된다.
- 재판: 만약 부정자로 규정된 구매자가 판매자의 결정에 동의하지 않는다면, 판매자는 부정자로 규정된 구매자의 정보와 불법 배포된 콘텐츠 Y 를 재판관(제3자)에게 전송한다. 이 때 재판관은 구매자에게 구매자의 비밀키 (K'_B) 또는 W 를 요구한 후, 해당 콘텐츠 내에 W 가 삽입되어 있는지 확인한다. 불법 배포된 콘텐츠 Y 내에 $\sigma(W)$ 가 존재하면 그 구매자는 부정자로 확정되는 것이고, 그렇지 않으면 무죄로 결정된다.

이 방식은 동형 속성을 가진 공개키 알고리듬과 코드가 긴 Boneh의 공모 보안 코드 대신에 상대적으로 짧은 코드 길이를 가지는 Cox의 알고리듬을 적용하여 처음으로 구매자-판매자 워터마킹 프로토콜에 비대칭성을 도입한 방식이라는 점에서 의의를 가진다. 그러나 이 방식은 구매자의 익명성을 제공하지 않는다는 단점을 지닌다.

나. 익명의 소비자-판매자 워터마킹[12],[13]

후에 [12]에서 구매자의 익명성을 제공하고, 구매자의 참가 없이 식별 프로토콜(분쟁, 재판 프로토콜)을 수행할 수 있는 방식이 제안되어졌다. 이 방식은 Memon의 방식을 기본 구조로 가지고, 구매자의 익명성을 제공하기 위해 verifiable encryption 방식을 도입하였다.

- 워터마크 생성: 구매자는 익명으로 사용될 공개키와 비밀키 쌍 $(K_B^*, K_B'^*)$ 을 생성하고, 비밀키 $(K_B'^*)$ 를 verifiable encryption 알고리듬을 사용하여 제3의 신뢰센터(재판관)의 공개키 (K_J) 로 암호화한 값 $C = E_{K_J}(K_B^*)$ 과, $K_B'^*$ 를 노출하지 않

고도 K'^{*}_{B}가 K^{*}_{B}와 연관된 비밀키임을 증명할 수 있는 $Cert$를 생성한다.

구매자는 유용한 워터마크를 얻기 위해 K'^{*}_{B} $Sign_{K_B}(K'_{B^*}), C, Cert$를 워터마크 신뢰센터에게 전송한다.

워터마크 신뢰센터는 구매자의 K'_B와 서명 $Sign_{K_B}(K'^{*}_{B})$을 가지고 구매자의 익명 공개키 K'^{*}_{B}를 인증하고, 이것이 인증되면 구매자의 워터마크를 생성하여, 구매자의 공개키 K'^{*}_{B}로 암호화한 값 $w=E_{K'^{*}_{B}}(W)$와 이것에 대한 서명 값 $s=Sign_{K_C}(w\|K'^{*}_{B})$을 전송해준다. 이때 서명 값은 워터마크의 타당성과 이 워터마크가 해당 구매자의 익명 공개키로 암호화 되었음을 증명해 주는 역할을 한다. 그리고 워터마크 신뢰센터는 구매자의 공개키와 $c, Cert, w, s, K'_{B^*}, Sign_{K_B}(K'_{B^*})$를 저장해둔다.

- 워터마크 삽입: 구매자는 암호화된 워터마크 $w=E_{K'^{*}_{B}}(W)$와 신뢰센터의 서명 $s=Sign_{K_C}(w\|K'_{B^*})$를 판매자에게 보내고, 판매자는 이것을 검증하고, 이것이 검증되면, 구매자에게 유일하게 연결될 새로운 워터마크 V를 생성하여 콘텐츠 X에 삽입한다. 워터마크 V가 삽입된 콘텐츠를 X'라 두자. V의 역할은 Memon의 방식과 동일하다. 판매자는 구매자로부터 받은 $E_{K'^{*}_{B}}(W)$을 치환하기 위해 치환함수 σ를 생성한다. 판매자는 먼저 $E_{K'^{*}_{B}}(W)$를 치환하고, 이를 X'에 삽입하기 위해 X'를 K'^{*}_{B}를 이용해 암호화한 후, (3)의 과정을 수행한다.

$$\begin{aligned} E_{K'^{*}_{B}}(X'') &= E_{K'^{*}_{B}}(X') \oplus E_{K'^{*}_{B}}(\sigma(W)) \\ &= E_{K'^{*}_{B}}(X' \oplus \sigma(W)) \\ &= E_{K'^{*}_{B}}(X \oplus W \oplus V) \end{aligned} \quad (3)$$

이 방식 역시 동형 속성을 지니는 공개키 암호 알고리듬과 워터마크 삽입 및 추출 알고리듬으로 Cox의 알고리듬을 사용한다. 판매자는 판매 기록에 구매자의 K'^{*}_{B}와 $w=E_{K'^{*}_{B}}(W)$, V, $s=Sign_{K_C}(w\|K'^{*}_{B})$, σ를 저장하고, $E_{K'^{*}_{B}}(X'')$는 구매자에게 전송한다. 암호화된 콘텐츠를 받은 구매자는 자신의 비밀키를 이용하여 이를 복호한 후 사용한다.

- 식별: 불법 배포된 콘텐츠 Y가 발견되면, 판매자는 여기에서 먼저 V'를 추출한다. 강인한 워터마킹 알고리듬이 전제된다면, 판매자는 Y에서 V'를 추출할 수 있을 것이다. 이 V'와 해당 콘텐츠의 판매 기록 레코드의 V와 비교하여 상관도가 가장 높은 V를 찾을 수 있을 것이다. 판매자는 추출한 V와 관계된 구매자의 정보 K'^{*}_{B}, $w=E_{K'^{*}_{B}}(W)$, V, $s=Sign_{K_C}(w\|K'_{B^*})$, σ를 재판관에게 제출한다.

  재판관은 서명 $s=Sign_{K_C}(w\|K'^{*}_{B})$를 검증하고, 이것이 검증되면 워터마크 신뢰센터에게 K'^{*}_{B}와 $s=Sign_{K_C}(w\|K'^{*}_{B})$를 보내고, 해당 구매자의 w, s, C를 요청한다. 재판관은 자신의 비밀키를 이용하여 워터마크 신뢰센터로부터 받은 $C=E_{K_J}(K^{*}_{B})$를 복호하고, 이를 이용해 w가 불법 배포된 콘텐츠에 존재하는지 확인한다. 불법 배포된 콘텐츠 Y내에 $\sigma(W)$가 존재하면 그 구매자는 부정자로 확정되는 것이고, 그렇지 않으면 무죄로 결정된다.

이 방식은 구매자/소비자 워터마킹 프로토콜에 구매자의 익명성을 제공하였을 뿐 아니라, 식별 과정에서 구매자의 참가를 배제시켰다는 점에서 의의를 찾을 수 있다. 그러나 이 방식은 첫째, 판매자와 워터마크 신뢰센터, 또는 판매자와 재판관의 공모가 가능하다면, 판매자는 쉽게 구매자의 워터마크와 워터마크가 삽입된 콘텐츠를 복호할 수 있다는 문제점이 있다. 둘째, 구매자의 익명성을 제공하기 위해 Memon의 방식에 비해 verifiable encryption을 추가적으로 더 사용하였으므로, 이의 안전성 제공을 위한 부가적인 전제 조건을 필요로 하는 문제점을 가지고 있다. 셋째, 식별 단계에서의 재판관은 워터마크 생성 단계에서 구매자가 선택한 재판관으로 제한되어져야 하므로, 재판관은 임의의 3자가 될 수 없다.

[13]에서 가환 알고리듬(commutative cryptosystems)을 이용하여 [12]방식의 안전성을 개선하였다. 이 방식에서는 판매자와 워터마크 신뢰센터와의 공모 공격을 제거하기 위해 워터마크 신뢰센터는

구매자의 워터마크는 생성해 줄 수 있으나, 구매자가 어떤 워터마크를 선택했는지는 알 수 없도록 하는 방식을 제안하였고, 둘째 재판관의 개입을 배제하면서도 구매자의 익명성을 제공할 수 있도록 구매자의 비밀키를 나누어 사용하는 기법을 제안하였다.

3. 기존 방식의 비교와 분석

<표 3>은 기존에 제안된 핑거프린팅 방식을 비교, 분석한 것이다.

JK02 방식[12]에서 워터마크 신뢰센터를 완전한 신뢰센터로 가정한다면, 즉 어떤 판매자와의 공모도 하지 않는다면 비대칭성을 제공하지만, 그렇지 않다면 판매자도 구매자의 정보가 삽입된 콘텐츠를 생성할 수 있으므로, semi-asymmetry로 기재하였다. 이와 같은 맥락으로 [9]방식에서도 판매자가 핑거프린팅 단계에서 COT의 2개 입력 값을 같은 값으로 설정한다면 구매자의 콘텐츠를 생성할 수 있으므로 semi-asymmetry로 기재하였다. 기본적으로 디지털 핑거프린팅 기술에서 공모 보안 코드로 Boneh의 코드를 사용할 경우는 코드 자체는 길다는 단점이 있지만, 구매자의 정보만 삽입하면 되나, 구매자-판매자 워터마킹 기술에서는 공모 공격 방어용으로 공모 보안 코드가 아닌 Cox의 워터마킹 알고리듬[15]을 사용하므로, 기본적인 공격뿐만 아니라 공모 공격에도 안전한 워터마킹 알고리듬이 전제되어져야 한다는 단점이 있다.

<표 3> 디지털 핑거프린팅과 구매자-소비자 워터마킹 프로토콜의 비교

	초기 기법 [2],[3]	PW97 [6]	Do98 [7]	Do99 [9]
비대칭성	X	O	O	△
익명성	X	O	O	O
No two-party protocol	X	X	X	O
공모보안 코드	Boneh [14]	Boneh [14]	Boneh [14]	Boneh [14]
식별단계의 참가개체	판매자	판매자, 등록센터, 구매자	판매자, 등록센터	판매자, 등록센터, 전 구매자
	PS99[11]	MW01[4]	JK02[12]	CPK03[13]
비대칭성	O	O	△	O
익명성	O	X	O	O
No two-party protocol	O	O	O	O
공모 공격 방어	Boneh [14]	Cox's algorithm [15]	Cox's algorithm [15]	Cox's algorithm [15]
식별단계의 참가 개체	판매자, 등록 센터	판매자 워터마크 신뢰센터, 구매자	판매자, 워터마크 신뢰센터, 재판관	판매자, 워터마크 신뢰센터, 구매자

Ⅳ. 관련 기술 표준화 현황

디지털 핑거프린팅 기술은 저작권 보호 기술의 한 분류이다. DRM 시스템은 주로 인터넷을 통하여 콘텐츠가 안전하게 등록/유통/분배/사용될 수 있도록 하는 기술적 안전 장치로서 콘텐츠 저작권자, 콘텐츠 저작권 관리단체, 콘텐츠 공급자, 콘텐츠 신디케이터(유통자), 콘텐츠 분배자, 콘텐츠 소비자에 이르기까지 다양한 거래주체들 간에 가치 고리(value chain)를 형성할 수 있도록 지원해야 하는 기반구조의 성격을 갖는다. 따라서, 콘텐츠 식별자(예: DOI), 콘텐츠 메타데이터(예: INDECS), 권리명세언어(예: XrML, ODRL, XACML, RMI) 등의 저작권 관리 표준들, 저작권 보호기술에 적용되는 PKI(X.509, PKCS 등) 표준들, 그리고 전자책 관련 표준 OEBF의 EBX, 동영상관련 표준 MPEG, 인터넷 관련 표준 W3C, 디지털 방송표준 DVB 등 관련 응용분야의 국제 표준들과 밀접한 관련이 있다[16].

디지털 핑거프린팅의 평가 방법에 대한 논의는 현재 MPEG21의 Part11 PAT(Persistent Association Technologies)에서 진행되고 있다[17]. MPEG21의 목적은 디지털 콘텐츠의 거래를 지원하는 멀티미디어 프레임워크를 정의하고, 프레임워크에서 필요한 엔티티를 도출하여 상호 운용성을 지원할 수 있는 규격을 제시하는 것이다. DRM을 포함하는 훨씬 더 큰 범위에서의 작업으로 볼 수 있다. DRM과 특히 밀접하게 관련 있는 작업으로 RDD(Rights Data Dictionary) 및 REL(Rights Expression

Language)에 대한 표준화 작업이 현재 진행되고 있다. 2001년 12월 MPEG 회의에서, RDD에 대해서는 INDECS가, REL에 대해서는 XrML, ODRL 등이 제안되었는데, INDECS와 XrML의 표준 채택이 유력시되고 있다. IRTF/IETF에서는 DRM 시스템 표준화를 위한 연구 그룹인 IDRM(Internet DRM)이라는 RG(Research Group)을 발족시켰다. IDRM은 DRM 그 자체보다는 DRM을 지원하는 네트워크 기반 유통기술에 대한 표준화 작업에 초점이 맞춰져 있다. URI(Uniform Resource Identifier) resolution 중 하나인 handle system과 subset-difference 알고리듬에 기반한 멀티캐스팅 통신 세션을 위한 키 관리 메커니즘에 대한 표준안이 제안된 상태이다. W3C에서는 DRM 표준 작업과 관련하여 2001년 1월 이틀간에 걸쳐 워크샵을 개최하였다. 그 결과 MPEG21과는 다른 형태로서, 기존에 W3C가 개발한 표준을 바탕으로 프로토콜, 패키징, API 수준에서 표준을 진행하기로 하였다. 이메일 reflector를 통하여 토의를 지속적으로 진행시키기로 하였으나 현재까지는 별다른 진척사항이 없는 상황이다.

Ⅴ. 향후 비전

현재까지 제안된 익명 핑거프린팅 프로토콜의 공통적인 단점은 첫째, 디지털 콘텐츠 자체에 대한 공격으로 인해 핑거프린팅 정보가 손상되는 것에 적극적으로 고려하지 않았다는 점이다. 이 문제점은 최근까지 제안된 익명 핑거프린팅 프로토콜에 모두 다 존재하는 단점이라고 할 수 있다. 둘째, 구매자의 익명성에 관한 것이다. 대부분의 핑거프린팅 프로토콜은 한 명의 신뢰센터를 통해 구매자의 익명성을 제공 받는다. 이 방식은 판매자가 한 명의 신뢰센터와 공모를 한다면 판매자는 구매자의 신원을 쉽게 알 수 있는 문제점이 있다. 이 문제 역시 대부분의 익명 핑거프린팅 프로토콜에 존재하는 것이다. 그러나 디지털 콘텐츠의 지적 재산권 보호를 위해서는 콘텐츠에 대한 공격을 고려하는 프로토콜과 구매자의 익명성을 안전하게 제공해 주는 방향으로 발전해야 한다.

최근에는 방송 환경 하에서 암호학적 키를 이용한 부정자 추적 방식이 아닌 복호된 후의 콘텐츠 재배포에 대한 실시간 추적을 가능하게 하기 위한 방식으로 핑거프린팅 기술을 이용한 방식도 제안되어 졌다. 이러한 방법은 pay-TV나 브로드캐스팅 분야에서 수신 데이터를 불법으로 복호한 후 배포하는 부정자를 해당 콘텐츠 내에 삽입된 구매자의 핑거프린트 정보로 찾아내는 기술이다. 이 방식도 실효성을 거두기 위해서는 실시간적으로 핑거프린팅 정보를 삽입하고 추출할 수 있는 계산량과 전송량이 적은 프로토콜로 나아가야 된다. 디지털 핑거프린팅 프로토콜에 대한 연구는 디지털 콘텐츠 산업과 방송 산업의 발전에 있어서 중요한 역할을 하리라 전망된다.

참 고 문 헌

[1] V. Wahadaniah, Y.L. Guan, and H.C. Chua, "A New Collusion Attack and Its Performance Evaluation," International Workshop on Digital Watermarking 2002, *LNCS2613*, 2002, pp.64-80.

[2] Neal. R. Wanger, "Fingerprinting," *IEEE Symposium on Security and Privacy*, 1983.

[3] L. Qian and K. Nahrstedit, "Watermarking Schemes and Protocols for Protecting Rightfuk Ownership and Customer's Rights," *J. Visual Commun. Image Represent*, Vol. 9, Sep. 1998, pp.194-210.

[4] B. Pfitzman and M. Schunter, "Asymmetric Fingerprinting," *Eurocrypt'96, LNCS1070*, Springer-Verlag, 1996, pp.84-95.

[5] N. Memon and P.W. Wong, "A Buyer-Seller Watermarking Protocol," *IEEE Transactions on Image Processing*, Vol. 10, No. 4, Apr. 2001, pp.643-649.

[6] B. Pfitzman and W. Waidner, "Anonymous Fingerprinting," *Eurocrypto'97, LNCS1233*, Springer-Verlag, 1997, pp.88-102.

[7] J. Domingo-Ferrer, "Anonymous Fingerprinting of Electronic Information with Automatic Identification of Redistributors," *Electronics Letters*, Vol. 34, No. 13, 1998.

[8] Chanjoo Chung and Soohyun Oh et al., "Efficient Anonymous Fingerprinting with Improved Automatic Identification of Redistributors," *Trans. of KIISC*, Vol. 10, No. 4, 2000.

[9] J. Domingo-Ferrer, "Anonymous Fingerprinting Based on Committed Oblivious Transfer," *PKC99, LNCS1560*, Springer-Verlag. 1999.

[10] Ahmad-Reza Sadeghi, "How to Break a Semi-anonymous Fingerprinting Scheme," *IH2001, LNCS 2137*, 2001, pp.384-394.

[11] B. Pfitzman and Ahmad-Reza Sadeghi, "Coin-Based Anonymous Fingerprinting," *Eurocrypt'99, LNCS 1592*, 2000, pp.150-164.

[12] Hak-Soo Ju, Hyung-Jeong Kim, Dong-Hoon Lee, and Jong-In Lim., "An Anonymous Buyer-Seller Watermarking Protocol with Anonymity Control," *ICISC2002, LNCS2587*, Springer-Verlag, 2003, pp.421-432.

[13] J.G. Choi, K. Sakurai, and J.H. Park, "Does It Need Trusted Third Party? Design of Buyer-Seller Watermarking Protocol without Trusted Third Party," *ACNS2003, LNCS2846*, 2003, pp.265-279.

[14] D. Boneh and J. Shaw, "Collusion-Secure Fingerprinting for Digital Data," *Crypto'95, LNCS963*, Springer-Verlag, 1995, pp.452-465.

[15] I.J. Cox, J. Kilian, T. Leighton, and T. Shamnon, "Secure Spread Spectrum Watermarking for Image, Audio and Video," *IEEE Transactions on Image Processing*, Vol.6, No 12, 1997, pp.1673-1678.

[16] 한국 디지털 콘텐츠 포럼, "URN 표준동향 및 국내 대응," 2002.

[17] 국제 디지털 콘텐츠 컨퍼런스, "디지털 워터마킹 기술 현황 및 동향," 2003.