

불법 복제 콘텐츠 추적을 위한 핑거프린팅 기술 동향

Trend of Fingerprinting Technique for Tracing Illegal Contents

김원경(W.G. Kim)
이선화(S.H. Lee)
장호욱(H.W. Jang)

영상컨텐츠연구팀 선임연구원
디지털저작권관리연구팀 연구원
디지털액터연구팀 선임연구원

인터넷 환경 하에서 멀티미디어 콘텐츠에 대한 저작권을 보호하는 방법으로 콘텐츠 자체에 다른 신호를 삽입하여 콘텐츠의 소유권을 증명하는 워터마킹과 핑거프린팅 방법이 있다. 핑거프린팅은 소유주의 정보를 삽입하는 워터마킹과는 달리 콘텐츠의 거래 시점에 구매자의 정보를 콘텐츠 자체에 삽입함으로써 불법 배포 행위를 한 구매자를 불법 콘텐츠로부터 역추적할 수 있는 저작권보호 기법이다. 이 기법은 서로 다른 구매자 정보를 삽입하기 때문에 같은 콘텐츠라 하더라도 핑거프린팅 후에는 콘텐츠의 내용이 서로 조금씩 다르게 되는데 이러한 콘텐츠간의 작은 차이를 이용하여 핑거프린팅 정보를 제거하려고 하는 공모공격이 발생하게 된다. 본 고에서는 공모공격에 강인한 핑거프린팅 방식에 대해 고찰한다.

I. 서론

인터넷을 통한 전자상거래가 활발해짐에 따라 MP3 형태의 음악 파일이나 각종 교육용 동영상 같은 디지털 멀티미디어 콘텐츠에 대한 제작과 판매가 활발해지고 있다. 또한 출판 및 교육, 영화산업 등 전통적인 콘텐츠 산업도 인터넷을 이용한 마케팅을 위하여 급속한 디지털화가 진행 중이다. 하지만 이러한 디지털 콘텐츠는 아날로그 데이터와는 달리 완전 복제가 가능하고 인터넷을 통한 다량배포도 어렵지 않게 이루어지기 때문에 불법복제와 재분배가 매우 쉽게 이루어지고 있고 이에 따른 콘텐츠 제작사의 재정적 손해로 콘텐츠 산업 활성화에 많은 걸림돌이 되고 있다.

불법복제로부터 저작권(copyright)을 보호하기 위한 초기 연구는 소프트웨어 콘텐츠를 중심으로 관

용적 암호화 방식을 적용하여 진행되어 왔다. 기존의 암호 방식에서의 저작권 보호는 다음과 같이 이루어졌다. 암호화된 콘텐츠를 구매자에게 전송하고 허가된 구매자는 적절한 키(key)에 의해 콘텐츠를 복호화 한다. 구매자는 등록절차에 의해 부여 받은 일련번호(serial number) 등을 이용하여 접근과 사용에 대한 권한을 부여 받는다. 후에 불법복제로 의심되는 콘텐츠가 발견되었을 때 복호화에 사용된 키나 일련번호로 불법배포자의 원천을 추적할 수 있도록 한다. 하지만 이러한 기존의 암호학적 방식은 적법구매자가 불법적인 의도를 가지고 콘텐츠를 복호화된 상태로 재배포 할 경우에는 대응 방법이 없다. 실제로 음악파일이나 동영상 같은 멀티미디어 콘텐츠의 경우 복호화된 상태 혹은 콘텐츠의 재생 시 다 시 캡처(capture)되어 암호화되지 않고 배포되는 경우가 대부분이다. 따라서 이러한 관용적 암호화 방

식은 멀티미디어 콘텐츠의 저작권을 보호하는 데 있어서는 제한적일 수 밖에 없다.

이러한 제한적인 암호화 방식을 보완하기 위하여 콘텐츠 자체에 구매자가 인지할 수 없도록 저작권 정보를 삽입하는 워터마킹(watermarking) 기술이 있다. 워터마킹 기술은 이미지, 오디오, 비디오 같은 멀티미디어 콘텐츠와 텍스트 및 특정 문서파일 등에 원래의 소유주를 표시하는 저작권 정보, 즉 워터마크를 넣어 배포하고 불법복제 후의 콘텐츠에 대해 워터마크를 다시 추출함으로써 원소유주를 증명할 수 있는 법적 근거를 제시한다.

핑거프린팅(fingerprinting) 기술은 워터마킹의 확장 기술로 콘텐츠의 상거래 시 소유자의 정보뿐만 아니라 구매자의 정보도 포함하는 핑거프린팅 정보를 콘텐츠에 삽입하여 후에 불법배포가 어느 구매자로부터 시작되었는지 추적할 수 있도록 해주는 저작권 보호 기술이다. 워터마킹 기술과의 차이는 서로 다른 구매자 정보를 삽입하기 때문에 핑거프린팅된 콘텐츠도 서로 조금씩 다르게 된다는 점이다. 이 차이점을 이용하여 핑거프린팅 정보를 제거하려 하는 공모공격(collusion attack)이 가능하게 되는데, 핑거프린팅 기술은 이 공모공격에 강인하도록 개발되어야 한다.

본 고에서는 워터마킹과 핑거프린팅 기술을 비교하고 공모공격에 강인한 핑거프린팅 기술에 대해 고찰한다. 이를 위해 II장에서는 워터마킹 기술과 핑거프린팅 기술의 차이점에 대해 고찰하고 III장에서는 핑거프린팅 콘텐츠에 대한 공모공격의 유형에 대해 기술한다. 그리고 IV장에서는 현재까지의 핑거프린팅 기술을 분류, 설명하고 V장에서 결론과 향후 연구방향에 대해 고찰한다.

II. 워터마킹 vs 핑거프린팅

1. 워터마킹

최근에 콘텐츠의 중요성과 함께 활발히 연구가 진행되고 있는 워터마킹 기술은 각각의 멀티미디어

콘텐츠의 특성상 조금씩 다른 기술 개발 특성을 갖는다. 즉, 워터마킹 기술은 기존의 콘텐츠에 저작권 정보를 구매자 혹은 사용자가 인지할 수 없도록 부가정보로 삽입하고 추출하는 신호처리 기술로 콘텐츠의 특성에 따라 삽입과 추출기술이 다르게 적용된다. 삽입한 워터마크를 구매자가 인지할 수 없어야 한다는 비인지성(imperceptibility)과 의도적 혹은 비의도적인 처리에도 제거되지 않아야 한다는 강인성(robustness)은 워터마킹 기술의 가장 중요한 요구 조건이다. 워터마킹 기술은 크게 삽입기술과 추출기술로 구성된다.

이미지 콘텐츠에 대한 워터마킹 기술은 워터마크의 삽입영역에 따라 크게 공간영역(spatial domain) 삽입방식과 주파수영역(frequency domain) 삽입방식 두 가지로 분류된다. 또한 추출 시 원본의 필요성에 따라 블라인드(blind) 추출방식과 논블라인드(non-blind) 추출방식으로도 구별된다.

공간영역 삽입 방식은 이미지데이터의 RGB, LC_rC_b 혹은 YUV 영역에 직접 워터마크를 삽입하는 방식이며 주파수영역 삽입방식은 이미지를 FFT, DCT, DWT 등의 변환을 사용하여 주파수영역으로 변환한 뒤 적절한 주파수밴드를 선택하여 워터마크를 삽입한 후 다시 역변환하는 방식이다. 공간영역 삽입방식은 주로 RGB의 파랑색 영역이나 휘도(luminance) 영역에 워터마크를 삽입한다. 그 이유는 사람의 시각모델이 이 채널의 변화에 덜 민감하기 때문이다. 이 방식은 삽입방식이 간단하긴 하지만 여러 가지 공격이나 압축같은 신호처리에 취약한 단점이 있다.

주파수영역 삽입방식은 워터마크를 주파수변환을 거친 계수에 삽입하는 방식으로 연구초창기에는 DCT나 FFT를 이용한 방법이 많이 연구되었다가 현재에는 DWT를 이용한 방법이 주로 연구되고 있다. 이 방법은 워터마크를 주파수영역의 어떤 부분에 삽입할 것인지를 결정하는 것이 중요하다. 저대역(low frequency band) 부분에 워터마크가 삽입될 경우에는 압축이나 신호처리에는 강인하지만 비인지성의 품질을 저하시키는 반면에 고대역(high

frequency band) 부분에 마크가 삽입될 경우에는 비인지성의 품질은 높은 반면 강인성이 저하되는 성질이 있다. 따라서 두 가지 특성을 고려하여 적당한 삽입 대역을 정하는 것이 중요하다. 또한 비지각성의 품질을 높이기 위해서 시각심리모델(psychovisual model)을 이용하여 워터마크의 삽입강도를 조절한다. 이는 이미지상에서 사람의 시각모델이 상대적으로 변화에 민감한 부분과 덜 민감한 부분(예를 들면, 에지(edge))을 계산하여 민감한 부분에는 작은 강도로 삽입하고 덜 민감한 부분에는 큰 강도로 삽입함으로써 견고한 성질도 보완하고 비지각성의 품질도 높이는 삽입 방법이다.

2. 핑거프린팅

워터마킹 기술은 불법복제 콘텐츠로부터 소유자의 워터마크를 추출함으로써 소유권을 명확히 해주는 기능을 하지만 불법행위자를 가려낼 수는 없다. 반면에 핑거프린팅 기술은 콘텐츠 내에 소유자 정보와 구매자 정보를 함께 포함하는 핑거프린팅 정보를 삽입하여 후에 불법으로 배포된 핑거프린팅 콘텐츠로부터 배포자가 누구인지를 역추적할 수 있도록 해주는 기술이다. 불법배포자를 추적할 수 있다는 관점에서 핑거프린팅 기술은 부정자 추적(traitor tracing) 기술로도 논의될 수 있다.

핑거프린팅 기술에서는 핑거프린팅된 콘텐츠가 서로 다르기 때문에 공모(collusion)의 위협이 존재한다. 즉, 여러 명의 악의적인 구매자들이 콘텐츠간의 상이성을 이용하여 핑거프린팅 정보를 지우거나 공모자 이외의 다른 구매자의 핑거프린팅 정보를 포함한 새로운 콘텐츠를 생성할 수 있다. 불법 복제 추적을 위해서는 공모한 구매자를 찾아내는 것이 목적이고 공모자 입장에서는 자신의 신분을 보호하는 것이 목적이다. 핑거프린팅 기술은 불법 복제에 대한 방지 기술이기보다는 불법 복제에 대한 검출과 증명 과정을 통한 수동적인 불법 복제 억제기술이라 할 수 있다. 최근에는 핑거프린팅 기술과 웹검색 기술을 함께 활용하여 능동적으로 웹상에서 불법 복제 콘텐

츠를 검색해주는 불법 복제 콘텐츠 추적기술에 대한 연구가 진행중에 있다. 다음은 핑거프린팅 기술에서 불법배포자를 추적하기 위한 요구 사항이다.

□ 콘텐츠 품질 보장성

콘텐츠 내에 핑거프린팅 정보를 삽입하게 되면 콘텐츠에 노이즈(noise)가 삽입되어 있는 것과 같은 효과가 있다. 따라서 어떻게 얼마나 많은 양을 삽입하느냐에 따라 콘텐츠의 품질이 차이가 나게 된다. 콘텐츠의 품질에는 영향을 미치지 않으면서 가능한 많은 양의 부가정보를 삽입해야 한다는 조건이다.

□ 견고성

콘텐츠를 불법으로 재분배하려고 하는 공격자는 삽입된 핑거프린팅 정보에 손상을 가하기 위하여 여러 가지 조작을 하게 된다. 견고성(robustness)은 이러한 조작에 대해 삽입된 핑거프린팅 정보가 얼마나 잘 견디어 내는지를 평가하는 척도이다.

□ 비대칭성

콘텐츠를 구매할 시점에서 핑거프린팅된 콘텐츠를 구매자만이 알고 판매자는 알지 못하도록 하는 조건을 비대칭성(asymmetry)이라고 한다. 핑거프린팅된 콘텐츠를 판매자도 접근할 수 있다면 불법 재분배자 식별에 있어서 모호함이 발생할 수 있다. 단지 구매자만이 핑거프린팅된 콘텐츠를 소유할 수 있어야만 재분배했을 경우에 확실한 불법의 증거가 된다.

□ 익명성

인터넷을 통한 전자상거래와 관련하여 본 조건은 구매자에 대한 익명성(anonymity)을 보장해야 한다는 조건이다. 실제로 상거래의 특징은 익명으로 상품을 구매할 수 있다는 점이다. 구매자의 프라이버시를 존중하면서 핑거프린팅된 콘텐츠를 판매할 수 있어야 한다.

□ 공모허용

핑거프린팅된 콘텐츠는 워터마킹된 콘텐츠와는

달리 서로 다른 구매자 정보를 삽입하기 때문에 구매자에 따라 조금씩 다르다. 다수의 구매자들이 서로 공모하여 콘텐츠 내에서 핑거프린팅된 위치를 파악할 수 있고 또한 콘텐츠끼리의 상대적인 차이를 이용하여 핑거프린팅 정보를 지우거나 새로운 핑거프린팅 정보를 삽입하여 재분배함으로써 공모자의 신분을 숨길 수 있다. 공모허용(collusion tolerance) 조건은 이런 공모에 대비하여 많은 핑거프린팅된 콘텐츠가 공격자에게 제공되어 공모공격이 가해지더라도 최소 1명 이상의 공모자의 정보를 추출 가능해야 한다는 조건이다. 공모허용성을 높이기 위한 많은 연구가 진행되고 있지만 아직도 높은 계산 복잡도 때문에 개발수준은 초기단계이다.

핑거프린팅 기술은 사용자 정보를 삽입하는 것 외에도 워터마킹 기술과 동일하다. 워터마킹 기술의 관점으로 핑거프린팅 기술은 개인화 워터마킹(personalized watermarking) 기술에 해당된다고 할 수 있다. 구매자에 따라 독립적인 워터마크가 삽입되기 때문이다. 따라서 핑거프린팅 기술은 워터마킹 기술에서 적용되었던 여러 가지의 조건을 함께 고려하여 개발되어야 한다.

핑거프린팅 기술도 워터마킹 기술과 같이 삽입과 추출기술로 분류된다. 삽입기술은 삽입하는 정보만을 뿐 워터마킹 기술과 동일하다. 추출 시에는 핑거프린팅된 콘텐츠와 삽입한 핑거프린팅 정보와의 상관계수(correlation coefficient)를 구하여 핑거프린팅 추출 성공 여부를 결정한다.

III. 공모공격

워터마킹과는 달리 구매자 정보를 동일 콘텐츠에 삽입하는 핑거프린팅 기술은 같은 콘텐츠라 하더라도 핑거프린팅 이후 콘텐츠의 내용이 서로 다르게 된다. 이 차이점은 핑거프린팅된 위치나 상대적인 삽입 크기 같은 중요 정보를 공격자에게 제공한다. 공격자는 여러 개의 콘텐츠를 서로 비교하여 핑거프린팅 정보를 제거하거나 혹은 유추하여 다른 핑거프린팅 정보를 삽입할 수 있는데 이를 공모공격[1],[2]이라

한다. 대부분의 핑거프린팅 추출 방법이 상관계수를 이용한 방법이기 때문에 공모공격은 상관계수 값이 작게 나오도록 하는 방법이 주를 이루고 있다. 다음은 현재까지 연구된 공모공격의 유형이다.

1. 평균화공격(Averaging Attack)

평균화 공격은 핑거프린팅된 다수의 콘텐츠를 서로 평균하여 새로운 콘텐츠를 생성하는 공격법이다. 공모된 콘텐츠 d_j 를 만드는 수식은 (1)과 같다.

$$d'_j = d_j + \frac{1}{K} \sum_k w_{k,j} \quad (1)$$

d_j 는 콘텐츠의 계수값이고 $w_{k,j}$ 는 핑거프린팅 정보, K 는 공모공격에 사용된 콘텐츠의 개수다. 핑거프린팅 정보 $w_{k,j}$ 에 대한 상관계수의 값이 \sqrt{K} 에 반비례하여 감소하는 효과가 있다.

2. 최대최소공격(Max-Min Attack)

Stone에 의해 제안된 방법[1]으로 공모에 참가한 핑거프린팅된 콘텐츠에서 최소값과 최대값을 구한 후 그 평균값으로 새로운 콘텐츠를 생성하는 공격법이다.

$$d'_j = d_j + (w_{j,max} + w_{j,min})/2 \quad (2)$$

$w_{j,max}$ 는 공모에 참여한 핑거프린팅 콘텐츠의 계수 중 최대값을 나타내며 $w_{j,min}$ 은 최소값을 나타낸다. 핑거프린팅 정보 $w_{k,j}$ 에 대한 상관계수의 값이 K 에 반비례하여 감소한다.

3. 상관계수 음수화 공격(Negative-Correlation Attack)

이 공격은 상관계수를 이용하여 핑거프린팅 정보를 추출할 경우, 상관계수의 값을 음수로 만들어 공모자의 추출을 어렵게 만드는 공격으로 최대최소공격과 마찬가지로 Stone[1]에 의해 제안되었다. 공모된 콘텐츠를 만드는 수식은 (3)과 같다.

$$d'_j = d_j + \begin{cases} w_{j,max} & \text{if } w_{j,med} \leq (1-\alpha)w_{j,max} + \alpha w_{j,min} \\ w_{j,min} & \text{otherwise} \end{cases} \quad (3)$$

max(*), min(*), med(*)는 각각 최대값, 최소값, 중간값을 나타낸다. α 는 max(*)와 min(*) 값을 조정하는 계수로 일반적으로 0.5의 값을 갖는다. 공모에 참여한 콘텐츠에서 최대, 최소, 중간값을 구하고 최대값과 최소값의 평균이 중간값보다 작으면 최소값을 취하고 반대이면 최대값을 취한다. 이는 핑거프린팅 정보의 극성(polarity)을 반대로 하여 상관계수 값을 음수로 만드는 효과가 있다.

4. 상관계수 제로화 공격 (Zero-Correlation Attack)

Stone[1]의 상관계수 음수화 공격은 상관계수를 음수로 유도하지만 핑거프린팅 정보가 지워졌다는 의미는 아니다. 제로화 공격은 상관계수를 제로에 가깝게 유도하여 핑거프린팅 정보의 검출이 불가능하도록 만드는 공격으로 Wahadaniah[2] 등에 의해 제안되었다. 수식은 (4)와 같다.

$$d'_j = d_j + \begin{cases} w_{j,max} & \text{if } w_{T,j} \leq \frac{1}{2}(w_{j,max} + w_{j,min}) \\ w_{j,min} & \text{otherwise} \end{cases} \quad (4)$$

$w_{k,j}$ 는 공모에 참가한 콘텐츠 중의 하나로 목표콘텐츠이다. 상관계수 음수화 공격과는 달리 비교대상을 중간값으로 하는 것이 아니라 공모에 참가한 특정 콘텐츠의 핑거프린팅 정보와 비교하여 극성이 반대되는 공모 콘텐츠를 생성한다. 생성된 공모 콘텐츠는 다른 핑거프린팅 콘텐츠와도 상관도가 적다. 즉, 상관계수가 제로에 가깝게 유지된다.

5. 모자의 공격(Mosaic Attack)

공모에 참여한 콘텐츠의 최대, 최소값을 이용하여 상관계수의 값을 작게 만드는 위의 공격과는 달리 핑거프린팅된 콘텐츠를 기하학적 모양으로 작게 나누

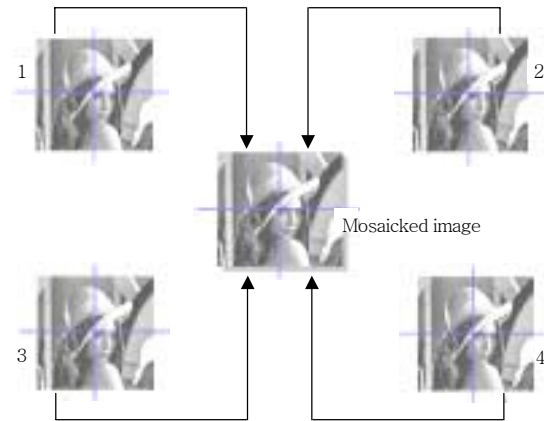
어 새로운 콘텐츠를 생성하는 공격법으로 워터마킹의 잘림(cropping) 공격과 유사하다. (그림 1)은 이미지 콘텐츠에 대해 4명의 구매자가 공모한 간단한 형태의 모자의 공격을 보인 예이다.

모자의 공격은 기하학적 모양에 따라 여러 가지 공격 형태가 존재한다. (그림 2)는 이미지 콘텐츠에 대하여 공모에 참여하는 기하학적 모양에 따른 모자의 공격의 예이다.

실제로 웹상에서의 이미지 콘텐츠는 여러 파일로 나뉘어 있는 경우가 많다. 다만 브라우저를 통해 사용자에게 보여질 때 매핑(mapping) 기능을 이용해 하나의 이미지처럼 보일 뿐이다.

핑거프린팅 정보의 추출은 파일단위로 이루어지기 때문에 웹상에서 여러 조각으로 나누어진 이미지 콘텐츠의 경우 추출이 어려워진다.

모자의 공격에 강인하게 핑거프린팅 정보를 삽입하기 위해서는 핑거프린팅 정보를 최소화하고 삽입 영역도 최소로 단위화하여 어떤 형태의 잘림 공격 후에도 핑거프린팅 정보가 제거되지 않도록 해야 한다.



(그림 1) 네 명의 공모자에 의한 모자의 공격



(그림 2) 네 명의 공모자에 의한 다양한 형태의 모자의 공격

IV. 핑거프린팅 기술

현재까지의 핑거프린팅 기술은 워터마킹 기술을 바탕으로 위에서 언급한 공모공격에 강인하도록 연구가 진행되어 왔지만 아직까지는 초보적인 단계이다. 핑거프린팅 기술은 크게 대칭성과 익명성을 지원하는 암호학적 기법[3]-[5]과 Malvar[6] 등에 의해 제안된 듀얼(dual) 워터마킹/핑거프린팅 기법, 삽입코드 자체를 공모공격이 불가능하도록 설계하는 공모보안코드(collusion secure code) 개발 기법[7]-[12] 등으로 나누어진다.

1. 암호학적 기법

암호학을 이용한 핑거프린팅 기술은 판매자와 구매자 사이에서 향후 불법콘텐츠에서 구매자 추적을 어떻게 할 것인가에 초점을 둔 암호프로토콜을 의미하며 콘텐츠를 판매하는 판매자가 핑거프린팅된 콘텐츠를 접근할 수 있는지 없는지에 따라 대칭형과 비대칭형으로 구분된다. 암호학적 방식을 이용한 핑거프린팅 기술은 주로 핑거프린팅의 비대칭성과 익명성을 효율적으로 충족시킨다.

가. 대칭형 핑거프린팅

대칭형 핑거프린팅은 초기의 연구기법[13]으로 핑거프린팅 프로토콜, 구매자 판별 프로토콜의 두 가지 알고리즘과 구매기록을 위한 데이터베이스로 구성된다. 앞의 두 알고리즘은 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 원구매자를 찾아내게 된다.

하지만 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 위하여 비대칭형 핑거프린팅 방식[3]이 제안되었다. 이 방식은 판매자와 구매자가 2-party 프로토콜에 참여함으로써 구매자만이 핑거프린팅된 콘텐츠를 접근할 수 있도록 한다. 이는 판매자가 불법 복사된 콘텐츠를 찾은 후에 불법배포자의 잘못을 신뢰된 제3자를 통하여 증명함으로써 책임 규명을 분명히 한다.

비대칭형 핑거프린팅 기법은 키생성(key_gen), 핑거프린팅(fing), 판별(identity), 분쟁해결(dispute)의 4가지 알고리즘으로 구성된다. 모든 알고리즘은 보안 파라미터 k 를 갖는다.

□ 키 생성 프로토콜(key_gen)

구매자는 자신의 공개키/비밀키 쌍(pk_B, sk_B)을 생성한 후, 공개키 pk_B 를 모든 판매자 및 CA(Certification Authority)에게 전달한다.

□ 핑거프린팅 프로토콜(fing)

판매자 M과 구매자 B 사이의 핑거프린팅 생성과정이다. 판매자는 판매할 콘텐츠, 구매자의 공개키 pk_B , 그 구매를 나타내는 스트링 str , 동일한 콘텐츠에 대한 판매 리스트를 입력하고 구매자는 자신의 비밀키 sk_B, str 를 입력한다. 이렇게 입력된 값들을 기반으로 핑거프린팅이 이루어진다. 구매자에 대한 결과물로는 핑거프린팅된 콘텐츠와 $record_B$ (차후에 분쟁이 발생할 때 사용)가 생성되고 판매자에 대한 결과물로는 판매 레코드 $record_{M\rho}$ 가 생성된다.

□ 구매자 판별 프로토콜(identify)

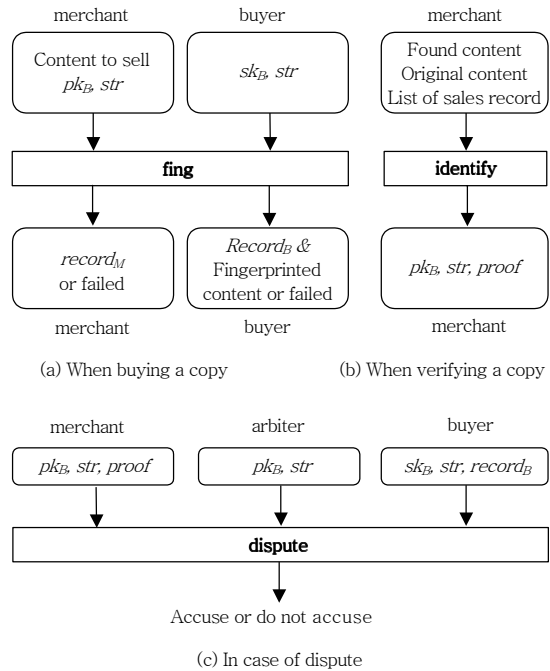
발견된 복사본에 대한 원래의 구매자를 알아 내기 위해서 판매자가 실행하는 알고리즘이다. 판매자는 발견된 복사본과 핑거프린팅 되기 전의 콘텐츠 및 판매한 리스트를 입력하여 identify 알고리즘을 통해서 구매자의 공개키와 구매자가 서명한 스트링 정보, *proof*를 얻는다.

□ 분쟁해결 프로토콜(dispute)

판매자와 구매자, 신뢰할 수 있는 제3자간의 3-party 프로토콜을 통해서 불법 사용자를 판단한다. 판매자와 중재자는 pk_B 와 str 을 입력하고 판매자는 추가로 스트링 *proof*를 입력한다. 이 프로토콜의 결과물로 구매자가 콘텐츠를 불법 유통시킨 범인인지의 여부를 판단한다.

(그림 3)은 비대칭형 핑거프린팅 방식을 도표로 나타낸 예이다. 암호학적 방식에 기반을 둔 핑거프린팅 방식은 판매기록과 구매자의 비밀키를 이용해 원 구매자를 추적한다는 의미에서 부정자 추적(trator tracing) 기법[13]으로도 적용될 수 있다. 부정자 추적 기법은 Pay-TV나 브로드캐스팅 분야에서 암호화한 수신 데이터를 불법으로 복호화하는 부정자를 구매자의 복호화 키로 찾아내는 기술이다.

최근에는 실용적인 면이 부각된 전자현금에 기반한 익명 핑거프린팅 방식[4],[14]이 제안되었다. 이 방식은 신뢰할 수 있는 제3자 즉, 인증센터(registration center)를 이용해서 불법적으로 재 배포한 구매자를 구별한다. 즉, 판매자는 인증센터의 도움 없이 부정자를 단독으로 구별할 수 없다. 인증센터를 사용함으로써 판매자는 핑거프린트를 구매자와 연결시키는 상세한 기록들을 보관할 필요가 없게 된다. 그러나 이 방식은 한 번의 인출에 단 한 번의 구매만이 가능하다. 또한 판매자가 불법 복사시켜준 부정자를 찾아 법정에서 증명하기 위해서 불법 복사한 사용자(accused buyer)가 참여해야 하는 3-party 프로토콜로 구성되어 있다. 현재 연구동향은 이런 문제점



(그림 3) 비대칭형 핑거프린팅

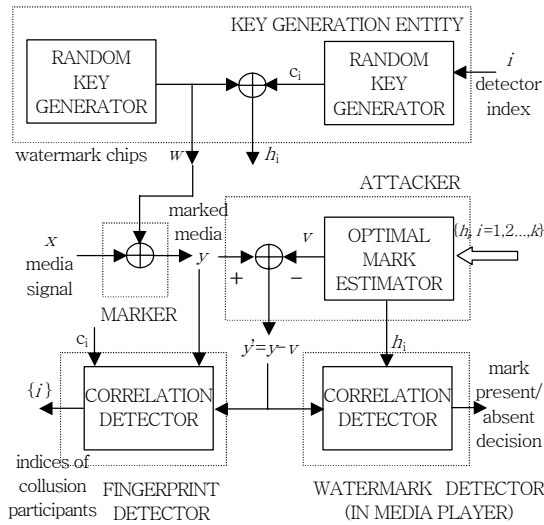
들을 해결하기 위한 연구가 진행되고 있으며, 위의 전자화폐에 기반한 방식을 그룹 서명(group signature)을 이용해서 다양한 구매를 한 번의 인출과정으로만 할 수 있는 새로운 방법들도 제시되고 있다.

2. 듀얼 워터마킹/핑거프린팅 기법

Malvar에 의해 제안된 듀얼 워터마킹/핑거프린팅(dual WM/FP) 기법[6]은 기존의 워터마킹 시스템의 보안성을 보완하고 여기에 핑거프린팅 기능까지 포함시켜 MS사의 미디어 플레이어 플랫폼에 구현되었다.

본 기법에서 워터마크는 콘텐츠의 저작권을 보호하고 콘텐츠를 사용하려고 하는 클라이언트(client) 모듈, 즉 미디어 플레이어에 허가를 부여하는 역할을 하고 핑거프린팅 정보는 원구매자를 판별하는 역할을 한다. (그림 4)는 듀얼 WM/FP 시스템의 전체구조를 보여주고 있다.

기존의 워터마킹 기법은 하나의 비밀키만을 사용하여 워터마크를 삽입하여 여러 구매자한테 배포한



(그림 4) 듀얼 워터마킹/핑거프린팅 시스템

다. 이러한 방법은 단지 한 명의 불법 배포자가 여러 가지 공격으로 비밀키를 근사하게 예측했을 경우 같은 워터마크를 삽입한 모든 다른 콘텐츠의 저작권도 보호될 수 없다는 단점이 있다. 듀얼 WM/FP 기법에서는 삽입하는 워터마크는 같으나 각각의 구매자에게 다른 워터마크 검출키(Watermark Detection Key: WDK)를 배포하여 한 명의 구매자가 자기의 키를 예측하더라도 다른 콘텐츠에는 영향이 없도록 하여 이러한 단점을 보완하였다. 검출키(WDK) h_i 는 (5)와 같이 정의된다.

$$h_i = c_i + w \quad (5)$$

여기서 w 는 대역확산 방법에 의해 생성된 워터마크 패턴이고 c 는 워터마크를 숨길 반송 신호이다. c 는 $M \times N$ 의 2차원 행렬로 표준편차가 B 인 정규분포를 따른다($c_{ij} = N(0, B^2)$). 2차원 행렬 c 에서 하나의 열 c_i 가 워터마크 w 와 더해져 워터마크 검출키로 할당된다. 이는 공격자가 한 구매자의 검출키 h_i 를 근사하게 예측한다 해도 다른 구매자의 검출키가 예측한 것과 다르며 또한 B 의 값이 클수록 w 를 알아내기는 어렵기 때문에 다른 워터마크된 콘텐츠에는 영향이 없게 된다.

이 기법에서는 워터마크의 검출은 사용자측의 미디어 플레이어 안에서 실시간으로 이루어진다. 하지

만 핑거프린트의 검출은 원본을 필요로 하기 때문에 성능 좋은 서버에서 따로 이루어진다. (그림 4)에서도 알 수 있듯이 핑거프린트 검출기의 입력은 c_i, y, y' 이다. y 는 워터마크가 삽입된 원래의 콘텐츠이고 y' 는 공격자들에 의해 공모공격이 가해진 콘텐츠이다. 핑거프린트 검출기에서는 y 와 y' 로부터 c_i' 을 만들고($c_i' = y - y'$) 상관계수 검출방법을 이용하여 2차원 행렬 c_i 로부터 c_i' 와 상관도가 높은 i 를 선택하여 공모에 참여한 구매자를 검출한다. i 는 구매자의 인덱스이다.

3. 공모보안코드 개발 기법

핑거프린팅된 콘텐츠간의 차이점을 이용한 공모 공격은 상당히 위협적인 공격이다. 적은 수의 콘텐츠만으로도 핑거프린트를 완전히 제거할 수 있기 때문이다. 따라서 이러한 공모공격에 강인하도록, 삽입하는 핑거프린팅 코드 자체를 공모가 어렵도록 설계하는 연구가 진행되고 있다. 일반적인 핑거프린팅 코드는 구매자마다 완전히 다른 코드, 즉 무작위순열을 사용한다[5]. 무작위순열은 그 길이에 따라 어느 정도 공모공격에 강인성을 갖는다[15]. 하지만 공모자가 많아질수록 필요한 코드의 길이가 기하급수적으로 증가한다. 그래서 구매자끼리마다 다른 위치에서 공통된 부분을 갖도록 하여 무작위순열보다 효율적인 코드를 설계할 필요가 있다. 코드의 공통된 부분은 공모공격을 해도 제거되지 않으므로 이 부분의 위치 정보가 공모에 참여한 구매자의 정보를 나타내게 된다. 이러한 코드를 공모보안코드(collusion secure code)[7]-[12]라고 하며 많은 연구가 진행중이다. 다음에는 공모보안코드의 개발기법을 소개한다.

가. c-secure code

Boneh[7]는 코드끼리의 중복성을 이용하여 공모공격에 강인한 c-secure 코드를 제안하였다. 이 기법에서는 구매자에게 할당되는 마크의 길이가 l 이고 개수가 n 개인 워드(word)로 구성된 (l, n) -code를 (6)과 같이 정의한다.

$$\Gamma = \{w^{(1)}, \dots, w^{(m)}\} \subseteq \Sigma^l \quad (6)$$

Σ^l 은 길이가 l인 워드를 나타내며, Γ 는 핑거프린트로 삽입될 마크의 집합이다. 즉, 각각의 구매자에게 워드, $w^{(j)}$ 가 할당된다.

Boneh는 제안한 기법에서 공모공격의 경우에 삽입된 마크가 서로 다른 경우에만 마크를 검출할 수 있고 검출되지 않은 마크는 콘텐츠의 손상 없이 구매자가 변경할 수 없다는 삽입가정(marking assumption)을 제시하여 공모의 범위를 제한하였다. 따라서 이 가정에 따라 공모에 의해 발생할 수 있는 공모가능집합(feasible set), F 를 (7)과 같이 정의하였다.

$$F(C; \Gamma) = \{w \in (\Sigma \cup \{?\})^l \text{ s.t. } w|_R = w^{(u)}|_R\} \quad (7)$$

C 는 구매자의 공모를 나타내고, u 는 공모에 참여한 공모자의 인덱스, R 은 검출되지 않은 마크의 위치를 나타낸다. $\{?\}$ 는 검출되지 않은 위치의 마크값이다. 즉, 삽입가정을 전제로 공모가능집합에서는 코드끼리 중복되어 검출되지 않은 값을 반드시 포함하는 새로운 모든 공모코드를 포함하고 있다. 예를 들면 (8)과 같다. 구매자 A, B 가 있을 때,

구매자 A: 3 2 3 1 2
 구매자 B: 1 2 2 1 2

공모가능집합은,

$$F(AB) = \Sigma' \cdot 2 \cdot \Sigma' \cdot 1 \cdot 2 \quad (8)$$

$$(\Sigma' = \Sigma \cup \{?\})$$

이다.

Boneh는 공모의 과정에서 공모에 의해 생성된 코드가 공모에 참여하지 않은 구매자의 코드를 포함하는 경우를 배제하기 위해 c-frameproof 코드를 다음과 같이 정의하였다.

- **c-frameproof code**: 모든 핑거프린팅 코드, $W \subset \Gamma$ 에 대해 $F(W) \cap \Gamma = W$ 를 만족하는 코드
 예를 들어, 간단한 (n, n) -code는 c-frameproof

코드이다. $\Gamma_0(n)$ 을 1의 개수가 단지 1개인 n -bit 이진코드라 하면 3명의 구매자를 위한 $\Gamma_0(3)$ 코드는 (9)와 같다.

구매자 1 : 1 0 0
 구매자 2 : 0 1 0
 구매자 3 : 0 0 1

3개의 코드에서 생성될 수 있는 공모가능코드는 공모가능집합의 정의에 따라 다시 $\Gamma_0(3)$ 코드가 된다. 따라서 3명의 공모자는 공모에 의해 생성된 다른 새로운 코드로 다른 구매자에게 누명을 씌울 수가 없게 된다.

Boneh는 이러한 가설들을 바탕으로 c-secure 코드와 참여한 공모자를 추적할 수 있는 추적 알고리즘을 제안하였다. (10)은 4명의 구매자를 위한 $\Gamma_0(4, 3)$ 코드이다. 4는 코드의 개수, 3은 반복횟수이다.

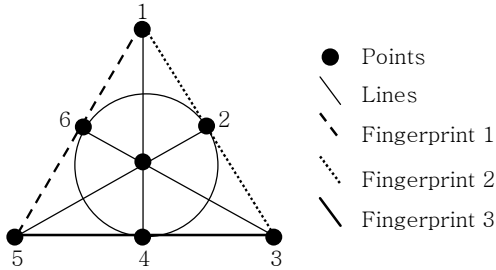
구매자 1 : 111111111
 구매자 2 : 000111111
 구매자 3 : 000000111
 구매자 4 : 000000000

할당된 코드 각각을 랜덤하게 재조합하여 콘텐츠에 삽입한다. 추출한 후에도 다시 역조합으로 원래의 삽입코드를 찾는다. 공모가 이루어진 후에는 위치에 따른 1의 개수에 따라 공모자를 추적한다.

Boneh의 방법은 제한된 공모자 환경에서 공모공격에 강인한 코드를 생성하지만 코드가 간단하여 공모자의 추적이 쉽고 또한 공모자가 증가할수록 필요한 코드의 길이가 기하급수적으로 증가하기 때문에 제한된 크기의 콘텐츠에 적용하기에는 무리가 있다.

나. d-detecting 코드

공모보안코드를 생성하기 위한 다른 방법으로 Dittmann[8]은 공모자의 수가 2명으로 제한되어 있을 때 모든 공모자를 색출할 수 있는 d-detecting 코드를 제안하였다. 이 코드는 유한사영기하학을 기반으로 공모자가 d 명일 때 강인하도록 설계된 공모보안코드라고 할 수 있다. 예를 들어 공모자가 2명



(그림 5) 2-detecting 코드

이라고 할 때 3명의 구매자에 대한 핑거프린팅 코드는 (그림 5)에 의해 (11)과 같이 생성된다.

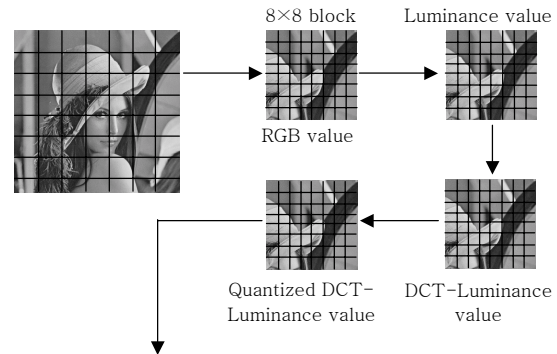
$$\begin{aligned}
 v_1 &= \{1, 0, 0, 0, 1, 1, 0\} \\
 v_2 &= \{1, 1, 1, 0, 0, 0, 0\} \\
 v_3 &= \{0, 0, 1, 1, 1, 0, 0\}
 \end{aligned} \tag{11}$$

(11)에서 생성된 3명의 구매자에 대한 핑거프린팅 코드에서 코드끼리의 유일한 공통된 부분이 있다는 것을 알 수 있다. 즉, v_1 과 v_2 에서는 첫번째 위치, v_2 와 v_3 에서는 3번째 위치, v_1 과 v_3 사이에서는 5번째 위치가 같다. 1은 핑거프린팅 코드의 삽입을 의미하고 0은 아무것도 삽입하지 않는다.

구매자 1(v_1)과 구매자 2(v_2)가 공모했다고 가정했을 때 핑거프린팅 정보가 삽입되어 있는 2, 3, 5, 6번째 위치는 그 차이에 의해 제거가 가능하지만 첫번째 위치는 차이점이 발견되지 않아 제거가 불가능하다. 만약 어떤 공모콘텐츠에서 첫번째 위치에서만 핑거프린팅 코드가 검출되었을 경우 이는 구매자 1과 2가 공모에 참여했다는 것을 나타낸다.

Dittmann은 위의 코드를 이미지의 DCT 영역에 삽입/추출하였다. 먼저 이미지를 8×8의 작은 블록으로 나눈 후 휘도값에 DCT를 적용한다. 삽입대상은 적당한 밴드 내의 계수 10개를 선택하였다. 삽입강도는 -4와 +4 사이에서 키에 의해 랜덤하게 결정되고, 삽입할 핑거프린트 코드에 따라 선택된 블록 내 DCT 계수에 직접 삽입된다. 즉, 선택된 블록에 삽입할 핑거프린트 코드가 1이라면 10개의 DCT 계수에 마크를 삽입하고 0이면 삽입하지 않는 방식이다. (그림 6)은 Dittmann이 제안한 핑거프린팅 정보

삽입과정을 보인 것이다. 핑거프린팅 정보의 추출은 원본과 비교하여 이루어진다. 이 방식은 DCT 영역에 삽입하므로 압축이나 필터링 같은 공격에는 강인하지만 추출 시에 원본을 필요로 한다.



If fingerprint code is 1, then add mark to coefficients in DCT domain

(그림 6) 2-detecting 코드를 이용한 삽입

Dittmann의 2-detecting 코드는 코드끼리의 공통된 부분을 서로 다른 위치에 생성함으로써 2명의 공모공격(평균화 공격)에는 어느 정도 강인성을 보이지만 검출할 수 있는 공모자의 수가 너무 제한적이며 c-secure 코드와 같이 삽입하는 코드가 단순하여 공격자가 쉽게 추정할 수 있다는 단점이 있다. 또한 유한사영기하학을 이용한 코드생성방식은 공모자가 증가할수록 코드 길이도 무한급수로 증가하기 때문에 2명 이상의 공모자 환경에 적용하기에는 무리가 있다.

다. 3-secure 핑거프린팅 코드

Domingo-Ferrer[9],[12]에 의해 제안된 3-secure 핑거프린팅 코드는 Boneh[7]의 방법을 보완한 기술로 3명의 공모자를 색출하면서도 요구되는 코드의 길이는 Boneh의 방법보다 작도록 설계되었다. 본 기법에서는 3명의 공모자를 색출하기 위한 공모보안코드로 듀얼이진해밍코드(dual binary hamming code)를 사용하였다. 듀얼이진해밍코드, $DH(n)$ 은 코드의 개수가 2^n 이고 길이가 2^n-1 , 그리고 모든 2개의 코드 사이의 해밍거리, d 가 2^{n-1} 인 코

<표 1> n=3인 듀얼이진해밍코드

	inv	minor (a ³ ; a ¹ , a ²)		minor (a ¹ ; a ² , a ³)		minor (a ² ; a ¹ , a ³)	
a ¹	1	0	1	1	0	1	0
a ²	1	0	1	0	1	0	1
a ³	1	1	0	0	1	1	0
a ⁴	1	1	0	1	0	0	1
a ⁵	0	0	0	1	1	1	1
a ⁶	0	1	1	0	0	1	1
a ⁷	0	1	1	1	1	0	0
a ⁸	0	0	0	0	0	0	0

드를 말한다. <표 1>은 n=3인 듀얼이진해밍코드의 예이다. 코드개수가 8, 코드의 길이는 7, 그리고 코드간의 해밍거리는 4이다.

함수 inv는 세 개의 코드 a¹, a², a³에서 모두 같은 값을 가지는 비트의 위치이며 (12)와 같이 정의된다.

$$inv(a^1, a^2, a^3) = \{i, 1 \leq i \leq N, a_i^1 = a_i^2 = a_i^3\} \quad (12)$$

함수 minor는 세 개의 코드 a¹, a², a³에서 두 개의 코드에서는 같은 값을 가지고 다른 하나의 코드가 다른 비트의 위치를 나타낸다.

$$minor(a^1; a^2, a^3) = \{i, 1 \leq i \leq N, a_i^1 \neq a_i^2, a_i^1 \neq a_i^3\} \quad (13)$$

<표 1>에서 알 수 있듯이 하나의 코드에 하나의 inv와 minor가 각각 존재한다. 각각의 코드가 구매자에게 할당된다.

코드간의 해밍거리가 일정한 DH 코드가 공모에 강한 이유는 3명의 공모자가 각각 자기의 코드로 공모를 할 경우에 공모코드의 근접코드(closest code)는 공모자의 코드집합에 반드시 포함되기 때문이다. 예를 들어 세 개의 코드 a¹, a², a³로부터 (14)와 같은 공모코드를 만들 수 있다.

$$C(a^1, a^2, a^3) = a^{coll} = 1010110 \quad (14)$$

이 공모코드는 DH(3)에 속하지 않지만 근접코드를 구해보면

$$d(a^1, a^{coll}) = d(a^2, a^{coll}) = d(a^3, a^{coll}) = 2 \quad (15)$$

임을 알 수 있다. 즉, 공모코드 a^{coll}은 a¹, a², a³으로부터 공모되었음을 역추적할 수 있다.

하지만 공모공격이 가해질 때 다음과 같은 문제가 발생할 수 있다. inv 위치에서는 공모가 불가능하다고 가정하고 공모자가 공모코드를 모두 minor로부터 생성할 경우 세 개의 코드 a¹, a², a³로부터 (16)과 같은 공모코드를 만들 수 있다.

$$C(a^1, a^2, a^3) = a^{coll} = 1101001 \quad (16)$$

이 공모코드는 a⁴와 같다. 이는 공모에 참여하지 않은 구매자에게 누명을 씌우는 것과 같다.

Domingo-Ferrer[12]는 이러한 문제점을 해결하기 위해 산재코드(Scattering Code: SC)와의 조합을 제안하였다. 파라미터 d와 t를 갖는 산재코드, SC(d, t)의 길이는 (2t+1)이다. SC(4, 3)의 예가 <표 2>에 나타나 있다.

<표 2> 산재코드 SC(4, 3)의 코드표

En-codes	Zone-A	Zone-B	Zone-C
'1'	1111	1111 0000 0000	0000 0000 0000
	1111	0000 1111 0000	0000 0000 0000
	1111	0000 0000 1111	0000 0000 0000
'0'	0000	0000 0000 0000	1111 0000 0000
	0000	0000 0000 0000	0000 1111 0000
	0000	0000 0000 0000	0000 0000 1111

각 구매자의 DH 코드는 다음과 같은 규칙에 의해 산재코드로 변환된다.

- Encoding
 - 1) '1' 일 경우: 위 3개의 코드워드(codeword) 중 하나를 랜덤하게 선택하여 인코딩
 - 2) '0' 일 경우: 아래 3개의 코드워드 중 하나를 랜덤하게 선택하여 인코딩
- Decoding
 - 1) 'Zone-A'의 모든 비트가 1이고 'Zone-C'의 모든 비트가 0이면 1로 디코딩
 - 2) 'Zone-A'의 모든 비트가 0이고 'Zone-B'의 모든 비트가 0이면 0으로 디코딩
 - 3) 'Zone-B'의 2개 블록에서 각 블록 내에 1인

- 비트가 하나 이상일 때 1로 디코딩
- 4) 'Zone-C'의 2개 블록에서 각 블록 내에 1인 비트가 하나 이상일 때 0으로 디코딩
 - 5) 'Zone-A'에 0인 비트보다 1인 비트가 더 많으면 1로 디코딩
 - 6) 'Zone-A'에 1인 비트보다 0인 비트가 더 많으면 0으로 디코딩
 - 7) 그 외에는 'Unreadable' 상태로 디코딩

위와 같이 정의된 산재코드로 인코딩된 핑거프린팅 코드는 임의의 구매자 3명이 공모하여 새로운 코드를 생성하더라도 그 공모코드가 공모자의 핑거프린팅 코드에 속하게 되어 공모자를 역추적할 수 있다.

V. 결론

본 고에서는 최근에 활발히 연구가 진행되고 있는 저작권보호 기술인 핑거프린팅 기술 동향에 대하여 고찰하였다. 핑거프린팅 기술은 콘텐츠의 거래 시에 구매자에 대한 정보를 삽입함으로써 콘텐츠가 불법 복제되었을 때 원 구매자를 추적할 수 있도록 해준다. 워터마킹 기술과는 달리 소유자의 정보가 아닌 구매자의 정보를 각각의 콘텐츠에 삽입하기 때문에 콘텐츠의 내용이 약간씩 상이하게 되며 이를 이용한 공모 공격이 존재한다. 따라서 워터마킹 기술과는 달리 공모공격에 강인하도록 삽입/추출해야 한다.

공모공격에 강인한 방법으로는 주로 공모보안코드 개발방법이 있는데 이는 구매자의 코드를 부분적으로 중복되도록 설계하여 삽입하고 공모가 이루어진 뒤에 중복된 코드의 위치 정보로부터 공모에 참여한 구매자를 추적하는 방식이다. 하지만 공모보안코드의 주된 문제점은 삽입패턴이 단순하여 공모자가 추측하기 쉽고 공모자가 많아질수록 코드의 복잡도와 그 길이가 기하급수적으로 늘어난다는 것이다. 이런 이유로 현재에는 실제 제한된 크기의 콘텐츠에 삽입하기에는 무리가 있다.

앞으로의 연구는 공모공격에 강인하면서도 제한된 크기의 콘텐츠에 효율적으로 삽입하기 위한 코드

의 개발과, 다양한 핑거프린팅 정보를 수용할 수 있는 대용량 핑거프린팅 코드체계의 개발이 절실하다 하겠다. 또한 멀티미디어 콘텐츠에 대한 핑거프린팅과 워터마킹의 기능을 함께 하는 통합코드의 개발도 앞으로의 과제이다.

참고 문헌

- [1] H. Stone, "Analysis of Attacks on Image Watermarks with Randomized Coefficients," *NEC Technical Report*, 1996.
- [2] V. Wahadaniah, Y.L. Guan, and H.C. Chua, "A New Collusion Attack and Its Performance Evaluation," *Proceedings of IWDW*, 2002, pp. 88 - 103.
- [3] B. Pfitzmann and M. Schunter, "Asymmetric Fingerprinting," *Journal of the ACM*, Vol. 33, 1986, pp. 792 - 807.
- [4] B. Pfitzmann and M. Waidner, "Anonymous Fingerprinting," in *Advances in Cryptology, Proc. of EUROCRYPT'97*, Vol. 1233, of Lecture Notes in Computer Science, Springer-Verlag, 1997, pp. 88 - 102.
- [5] B. Pfitzmann and A. Sadeghi, "Coin-Based Anonymous Fingerprinting," in *Advances in Cryptology, Proc. of EUROCRYPT'99*, Vol. 1592, of Lecture Notes in Computer Science, Springer-Verlag, 1999, pp. 150 - 164.
- [6] D. Kirovski, H.S. Malvar, and Y. Yacobi. "Multimedia Content Screening Using a Dual Watermarking and Fingerprinting System," *ACM Multimedia*, 2002.
- [7] D. Boneh and J. Shaw, "Collusion-Secure Fingerprinting for Digital Data," *IEEE Trans. Inf. Theory*, Vol. 44, No. 5, Sep. 1998, pp. 1897 - 1905.
- [8] J. Dittmann, "Combining Digital Watermarks and Collusion Secure Fingerprints for Customer Copy Monitoring," *Proc. IEE Seminar Sec. Image & Image Auth.*, Mar. 2000, pp. 128 - 132.
- [9] J. Domingo-Ferrer and J. Herrera-Joancomartí, "Simple Collusion-secure Fingerprinting Schemes for Images," in *IEEE International Conference on Information Technology: Coding and Computing, ITCC'2000*, ISBN 0-7695-0540-6, pp. 128 - 132.
- [10] Yiwei Wang, John F. Doherty, and Robert E. Van

- Dyck, "A Watermarking Algorithm for Fingerprinting Intelligence Images," *2001 Conference on Information Sciences and Systems*, The Johns Hopkins University, March 21-23, 2001.
- [11] W. Trappe, M. Wu, and K.J.R. Liu, "Collusion-Resistant Fingerprinting for Multimedia," *Proc. of IEEE Int. Conf. on Acoustics, Speech, and Signal Processing(ICASSP'02)*, Vol. IV, Orlando, FL, May 2002, pp. 3309 - 3312.
- [12] F. Sebe and J. Domingo-Ferrer, "Short 3-Secure Fingerprinting Codes for Copyright Protection," *Lecture Notes in Computer Science*, Vol. 2384, 2002, pp. 316 - 327.
- [13] B. Pfitzmann, "Trials of Traced Traitors," *Information Hiding*, Lecture Notes in Computer Science, Vol. 1174, Springer-Verlag, 1996, pp. 49 - 64.
- [14] J. Domingo-Ferrer, "Anonymous Fingerprinting of Electronic Information with Automatic Identification of Redistributors," *Electronics Letters* Vol. 34, No. 13, 1998, pp. 1303 - 1304.
- [15] J. Kilian, T. Leighton, L.R. Matheson, T.G. Shamoan, R.E. Tarjan, and F. Zane, "Resistance of Digital Watermarks to Collusive Attacks," *Tech. Rep.*, TR-585-98, Dept. of Computer Science, Princeton University, 1998.