오디오 핑거프린팅 기술과 응용

서울시립대학교 최 혁
서울대학교 정해경
인포마크 윤영진

1. 서 론

전통적인 콘텐츠 산업들이 급속히 디지털화가 이루어져서 모든 콘텐츠는 디지털 콘텐츠가 될 전망이다. 이러한 디지털 콘텐츠 사업은 한계 비용이 0에 가까운 산업적 특성과 파생 시장의 시장규모와 이익이 커서 미래 성장 동력 산업으로 크게 주목받고 있다. 그러나, 디지털 콘텐츠 산업의 성장과 함께 네트워크의 발달 및 P2P 기술, 검색 엔진 기술 등 컴퓨터의 손쉬운 사용으로 인해 디지털 콘텐츠의 무분별한 복제와 유포로 인한 저작권 및 소유권에 대한 침해 또한 날로 급증하고 있다. 이를 막기 위해 암호화를 이용한 DRM(Digital Rights Management) 기술 및 디지털 워터마킹(Digital Watermarking) 기술이 개발되어 사용되고 있으나, 아직 시장 요구를 모두 만족시키기에는 미흡한 실정이며, 또 다양한 시장 상황에 따라 요구되는 기술 또한 변화하고 있다.

2. DRM 기술 개요 및 핑거프린팅

DRM 기술은 디지털 콘텐츠의 유통 과정에서 불법적인 사용을 막고 사용자의 사용 권한을 관리하는 기술로써, 콘텐츠를 암호화하여 서비스하고 암호화를 풀기 위한 암호화키는 라이센스로 분리하여 관리함으로써 정당한 사용자로 인증된 경우에만 허가된 사용 권한 하에서 암호화키를 획득하여 콘텐츠를 이용할 수 있게 하는 기술을 말한다. 최근에는 워터마킹 기술, DOI (Digital Object Identifier) 등 저작권 보호와 관련된 모든 기술을 넓은 의미에서의 DRM 기술로 보기도 한다.

암호화를 이용한 DRM 기술의 일반적인 적용 방식을 살펴보기 위해, Microsoft의 Windows Media DRM의 프로세스를 바탕으로 과정을 살펴보면 다음과 같다.

- 패키지화 : 패키징이란 보호 대상인 디지털 콘텐츠에 저작권자 정보, 미디어 정보, 유통 정보 등 각종 정보를 메타데이터로 결합시킨 뒤 허가된 사용자만이 이를 사용할 수 있도록 특정 "키"로 암호화하는 것을 말한다. 이 키는 암호화된 라이센스에 저장되어 개별적으로 배포되는데 라이센스 취득이 이루어지는 URL 등의 정보는 패키징된 파일에 포함되어 있다.
- 배포 : 패키징된 파일은 웹사이트 다운로드 및 스트리밍을 위한 디지털 미디어 서버에서 배포되며, CD 또는 전자 메일을 이용해서도 소비자에게 전달될 수 있다. 일반적으로 소비자는 패키징된 파일을 다른 사람에게 전송할 수 있도록 허용된다.
- 라이센스 서버 설정 : 콘텐츠 공급자는 특정 권한 또는 라이센스 규칙을 저장 및 관리하기 위해 라이센스 서비스를 구현하는 라이센스 정산소(License Clearing House)를 설정한다. 정산소의 역할은 소비자의 라이센스 요청을 인증하고 부여된 사용 권한에 따라 라이센스를 발급하고 내역을 관리하는 것이다. 디지털 미디어 파일 및 라이센스는 개별적으로 배포 및 저장되기 때문에 전체 시스템을 쉽게 관리할 수 있게 된다.
- 라이센스 취득 : 소비자가 패키징된 파일을 재생하려면 먼저 파일 잠금을 해제하기 위한 라이센스 키를 얻어야 한다. 소비자가 패키징된 파일을 얻으려고 시도하거나, 미리 제공된 라이센스를 취득하거나 파일을 처음으로 재생하려고 하면, 라이센스 취득 과정이 자동으로 시작된다. 이를 위해 사용자단의 DRM 관리자(Agent)는 정보 입력이나 비용 지불을 요청하는 등록 페이지를 소비자에게 표시하거나 정산소에서 라이센스를 자동으로 검색한다.
- 콘텐츠 재생 : 사용자는 라이센스에 포함된 규칙 또는 권한에 따라 파일을 재생할 수 있다. 라이센스에는 시작 시간 및 날짜, 사용 기간 및 작동 회수와 같은 다양한 권한이 포함될 수 있다. 예를 들어 사용자는 기본 권한에 따라 특정 컴퓨터에서 파일

을 재생할 수 있으며 휴대용 장치로 복사할 수도 있다. 하지만 라이센스는 전송이 불가능하며 사용자가 패키징된 파일을 다른 사람에게 전송한 경우 해당 사용자는 파일을 재생하기 위해 자신의 라이센스를 독립적으로 재취득해야만 한다.

그림 1은 유료사이트에서 영화와 같은 동영상을 DRM을 이용하여 안전하게 서비스하는 과정을 요약한 것으로, 원시 동영상이 변환기를 통해 패키징되고 패키징 과정에 사용된 키를 라이센스로 분리하여 사용권한을 관리할 수 있도록 라이센스 정산소에 저장하는 과정과 사용자단에서는 패키징된 미디어 파일을 배포받아 이를 사용하기 위해서는 사용자 인증 및 결제 확인 과정을 거쳐 라이센스를 획득한 뒤 동영상을 이용하게 되는 과정을 도시하였다.

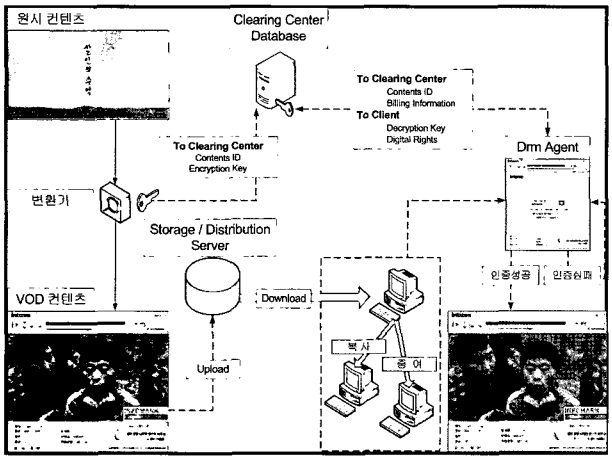


그림 1 DRM 적용 예

현재 DRM 기술은 인터넷 환경하에서 다양한 유료사이트에 적용되어 안전한 디지털 콘텐츠 유통을 가능하게 하고 있으며, 모바일의 경우에도 SKT, KTF 등에서 OMA(Open Mobile Alliance) 표준을 따르는 DRM 기술이 사용되고 있는 등 디지털 콘텐츠의 유통에 있어 핵심적인 기술로 널리 사용되고 있다. 그러나 유통 환경의 변화 및 기술적인 한계에 의해 보완 기술의 필요성 및 새로운 DRM 기술의 응용 방법 등이 지속적으로 연구되고 있다.

DRM 기술은 암호화를 이용하여 정당한 사용권한을 가지고 있는 사용자만이 콘텐츠를 이용할 수 있도록 관리할 수 있지만 허가받은 사용자가 콘텐츠를 재생하면서 그림 2와 같이 캡처툴을 이용하여 화면 캡처를 하거나, 오디오의 경우 재생 중 아날로그 출력을 받아 디지털로 다시 저장하는 방법으로 DRM이 적용되지 않은 콘텐츠를 얻어낼 수 있는 문제점이 있다. 즉, DRM 기술에서는 정당한 사용자의 경우 암호화를 푼 뒤에 아날로그 캡쳐 방식으로 콘텐츠를 얻어낼 수 있는 위험성(security hole)이 항상 존재하고 있는 것이다.

이러한 문제의 해결을 위해 최근 DRM 기술과 핑거프린팅 (Fingerprinting) 기술의 접목이 적극적으로 검토되고 있다. 핑거프린팅 기술은 디지털 워터마킹의 일종으로 워터마킹이 소유권자의 저작권 정보를 콘텐츠 내에 인간 지각에 거슬리지 않게 삽입하고 이를 이용하여 콘텐츠의 저작권 확인 및 증명에 이용하는 기술이라면, 핑거프린팅은 인간 지각에 거슬리지 않게 정보를 삽입하는 면에서는 워터마킹과 같지만 삽입되는 정보가 소유권 정보 뿐만 아니라 배급받는 사용자의 정보를 담고 있어 불법적인 복제를 한 사용자를 추적하고 확인할 수 있는 보다 적극적인 저작권 보호 기술이라고 할 수 있다. 즉, DRM이 적용되어 있는 콘텐츠 유통 시 사용자단에서 콘텐츠를 재생할 때 재생되는 콘텐츠에 실시간으로 사용자 정보를 삽입함으로써 불법 복제가 이루어져도 복제된 콘텐츠 내에서 사용자의 정보를 확인할 수 있어 불법 복제를 시도한 사용자를 추적할 수 있게 된다.

그림 2 캡쳐솔루션을 이용한 영화 캡쳐 예

핑거프린팅 기술은 DRM 기술과 독립적으로 단일 상품으로도 제공 가능하며, DRM이 적용되어 있는 경우에는 DRM 시스템의 큰 변화없이 핑거프린팅 기술을 추가 적용하여 전체 시스템의 보안성을 극대화할 수 있다.

3. 핑거프린팅 기술

3.1 공모 공격

하나의 콘텐츠의 경우 저작권 정보로 동일한 코드가 삽입되는 워터마킹 알고리즘과 달리 같은 콘텐츠라도 사용자마다 각기 다른 코드를 삽입하는 핑거프린팅 알고리즘에서는 새로운 형태의 공격이 가해질 수 있다. 즉, 워터마킹에서는 모두 같은 코드가 삽입되기 때문에 한 명의 공격자가 신호처리 형태의 공격을 가할 수 있는데 반해 핑거크린팅에서는 사용자 마다 서로 다른 코드가 삽입되기 때문에 핑거프린팅 코드가 서로 상이한

성질을 이용하여 여러 명이 같이 공격에 참여하는 공모공격(Collusion attack)이 존재하게 된다[1][2]. 이러한 공모공격에는 다음과 같이 크게 선형공격과 비선형공격으로 나눌 수 있다.

3.1.1 선형공모공격(Linear collusion attacks)

선형공격의 대표적인 예로는 평균화 공모공격이 있다. 원본 오디오 신호를 x라 하고 i번째 사용자의 핑거프린팅 코드 s_i가 삽입된 오디오 신호를 y_i라 할 때 평균화 공모 공격으로 생성된 신호 y'은 다음과 같다.

$$y' = \frac{1}{K}\sum_{i=1}^{K} y_i = x + \frac{1}{K}\sum_{i=1}^{K} s_i \tag{1}$$

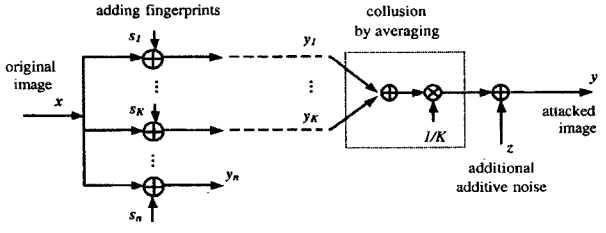


그림 3 평균화 공모공격의 블록선도

이러한 평균화 공모공격을 받았을 때 y'에서 추출된 핑거프린팅 코드 s'과 원래의 핑거프린팅 코드 s_i와의 상관도는 다음과 같이 같다.

$$\rho(s', s_i) = \frac{1}{\sqrt{K}}\rho(s_i, s_i) \tag{2}$$

위의 식에서와 같이 공모자수 K가 커지면 그에 따라 상관도가 줄기 때문에 상관도 검사를 수행하는 일반적인 검출기의 경우 어느 문턱치 이상이 되면 핑거프린팅 코드는 더 이상 검출할 수 없게 된다. 이렇듯 원래의 핑거프린팅 코드와 추출된 핑거프린팅 코드의 상관도를 낮추는 문제가 공모공격의 관심대상이 된다. 그림 3은 일반적인 평균화 공모공격의 블록선도를 나타낸다.

3.1.2 비선형공모공격(Non-linear collusion attacks)

비선형공모공격에는 다음 세가지 방법이 알려져 있다.

1) 최대-최소공격(Max-Min attack)

최대-최소공격은 공모공격자들의 코드들에서 서로 상이한 부분을 그 위치에서의 최대값과 최소값의 평균값으로 대치하는 공격이다. 최대-최소공격은 다음과 같은 수식으로 표현할 수 있다.

$$y' = x + \frac{1}{2}(s_{\max_{i=1,\cdots,K}} + s_{\min_{i=1,\cdots,K}}) \tag{3}$$

이 때의 원래 상관도는 다음과 같다.

$$\rho(s', s_i) = \frac{1}{K}\rho(s_i, s_i) \tag{4}$$

따라서 선형공모공격인 평균화 공모공격보다 공모자수에 더 민감함을 볼 수 있다.

2) 제로-상관도공격(Zero-correlation attack)

제로-상관도공격은 아래의 식과 같은 규칙으로 공격된 오디오 신호를 만들어 내는 공격이다.

$$y' = x + \begin{cases} s_{\max_{i=1,\cdots,K}}, & \text{if } s_{\text{median}_{i=1,\cdots,K}} \le (1-\alpha)s_{\max_{i=1,\cdots,K}} + \alpha s_{\min_{i=1,\cdots,K}} \\ s_{\min_{i=1,\cdots,K}}, & \text{otherwise} \end{cases} \tag{5}$$

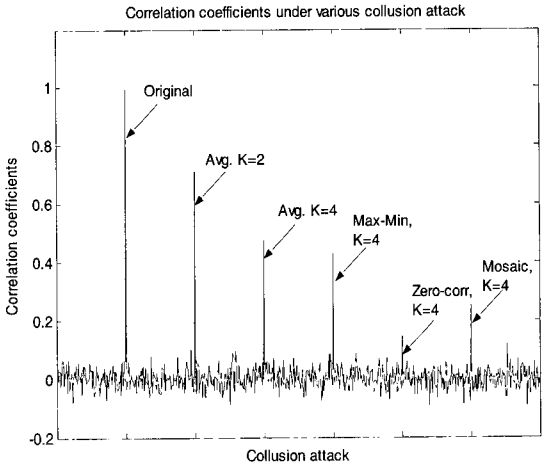


그림 4 공모공격에 따른 상관도 변화

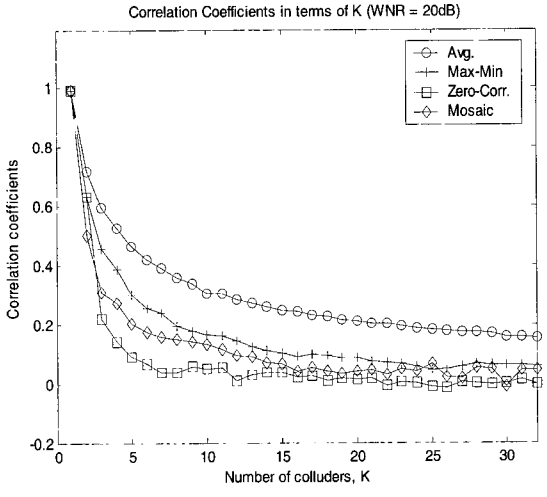


그림 5 공모공격과 공모자수에 따른 상관도 변화

3) 모자이크공격(Mozaic attack)

모자이크공격은 핑거프린팅이 삽입된 각 공모자의 오디오 신호에서 일정부분을 조금씩 조합해서 공격된 신호를 만드는 공격방식이다.

3.1.3 각 공모공격의 성능

위에 열거된 각 공모공격들의 성능을 알아보기 위해 간단한 실험을 수행하였다. 실험은 Trappe 등의 논문에 제시된 가우시안 신호를 이용한 실험방법으로 구현하였다[3]. 그림 4와 5에서 보듯 공모공격 중 제로상관도공

격이 가장 상관도를 낮추는 공격임을 확인할 수 있다. 하지만 가장 일반적인 경우가 평균화 공모공격이므로 본 논문에서는 평균화 공모공격만을 고려하기로 한다.

3.2 기존 핑거프린팅 코드 분석

핑거프린팅 코드는 본래 암호학 분야에서 널리 연구되었다. 알고리즘이나 기타 문서자료와 같은 일반적인 파일 형태의 데이터를 보호하기 위해 시작된 핑거프린팅 코드는 처음에는 파일의 처음이나 끝에 사용자를 식별하기 위한 코드를 붙이면서 출발하였다. 이에 반해 현재에는 멀티미디어 데이터에 관한 보호가 중요하게 여겨지면서 기존의 방식과는 달리 데이터 속에 사용자 식별 코드를 은닉하는 방법이 활발히 연구되고 있다[3]-[6]. 여기서는 편의상 전자의 경우를 일반적 핑거프린트(generic fingerprint), 후자를 워터마크 핑거프린팅 (watermark fingerprinting)이라 부르기로 한다. 표 1은 본 논문의 관심 대상인 워터마크 핑거프린팅과 일반적 핑거프린트와의 차이점을 보여주고 있다. 표 1에서 보는 바와 같이 워터마크 핑거프린팅은 멀티미디어 데이터에 핑거프린팅 정보를 은닉해야 하기 때문에 삽입할 수 있는 코드의 길이가 한정되어있고 공격 시 원본 데이터의 변경이 일어나게 되므로 여러 가지 신호처리적인 공격도 가능해지는 특성이 있다.

이제 몇가지 일반적 핑거프린트와 워터마크 핑거프린팅 방식에 대해 기존의 방식들을 살펴보면 표1과 같다.

표 1 일반적 핑거프린트와 워터마크 핑거프린팅 비교

	일반적 핑거프린트	워터마크 핑거프린팅
적용 대상	일반 파일 데이터	멀티미디어 데이터
원본 데이터의 변경	불가능	가능
삽입방법	첨부	은닉
삽입할 코드의 길이	제한 없음	제안 있음
코드의 노출성과 공격용이성	쉽다	어렵다

3.2.1 c-secure 코드

Boneh와 Shaw는 c-secure 코드라 불리는 일반적 핑거프린트를 제안하였다[4]. 이 방식은 표시가정(marking assumption)을 기반으로 하여 개발되었는데 표시가정이란 N 명의 사용자 중에 K 명의 공모자가 공모공격을 했을 경우 생성된 코드는 나머지 $N-K$ 명의 사용자를 절대 지목할 수 없는 코드를 말한다. 표시가정에 따르는 코드는 따라서 기본적으로 무고한 사람을 잡아내지 않는다는 것을 보장한다고 할 수 있다. 하지만 c-secure 코드는 코드의 길이가 너무 길어 현실에 적용하기 힘든 단점이 있다.

3.2.2 듀얼이진해밍 코드(dual binary hamming codes)

Domingo와 Herrera에 의해 제안된 듀얼이진해밍 코드는 공모공격에 강인하고 c-secure 코드보다 길이가 짧은 코드이다[5]. 하지만 이 코드는 공모공격에 강인한 공모자 수가 2명으로 제한되어있다는 단점 때문에 실제로 사용되기는 힘들다.

3.2.3 유한투영기하 코드(finite projective geometry codes)

Dittmann은 유한투영기하 이론에 기반한 이미지 워터마크 핑거프린팅 기법을 제안하였다[6]. 여기서 사용된 핑거프린트 코드의 길이는 사용자 수가 n이고 공모공격자 수가 c일 때 $l = n^c + n^{c-1} + \cdots + n + 1$로 주어지는데 실제에서 사용하기에는 그 길이가 너무 크다는 단점이 있다.

3.2.4 Anti-collusion 코드(ACC)

Anti-collustion 코드는 Trappe 등에 의해 제안된 이미지 워터마크 핑거프린팅 기법이다. Balanced Incomplete Block Design(BIBD) 기법에 기반한 이 코드는 그 코드 길이가 짧아 실제로 사용 가능하다[3]. 하지만 공모공격이 논리적AND연산으로 구성되었다고 가정하고 있기 때문에 다양한 공모공격에 적용하기 힘든 단점이 있다.

이외에 Boneh와 Shaw에 의해 제안된 c-frameproof 코드가 있다. c-secure 코드가 공모공격자를 추적할 수 있지만 코드의 길이가 너무 긴 반면 c-frameproof code는 공모공격자를 추적할 수는 없지만 표시가정에 만족하고 코드길이가 실제 상황에 사용할 수 있을 정도로 적다. 이것은 위에서 언급한 핑거프린트의 코드 길이를 비교해서 보여주고 있는 표 2와 3에서 확인할 수 있다. 따라서 이 c-frameproof 코드가 공모공격자 추적이 가능해지면 실생활에도 사용 가능한 코드가 된다. 만약 c-frameproof 코드가 코드의 모든 공모 가능한 집합을 알 수 있다면 공모공격자를 추적할 수 있게 된다.

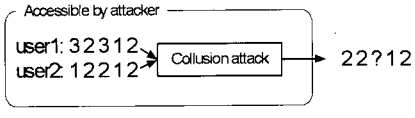
표 2 일반적 핑거프린팅 코드의 길이(n: 사용자 수, c: 공모공격자 수)

Generic fingerprint	Code length	Complexity
c-secure code	$l = 2cLd, (L = 2c\log_2(2n/$ $d = 8c^2\log_2(8cL/\varepsilon))$	$l = O(c^4\log_2(n/\varepsilon)$ $\log_2(1/\varepsilon))$
Finite geometry	$l = n^c + n^{c-1} + \cdots + n + 1$	$l = O(n^c)$
Anti-collusion code	$l = \sqrt{(c^2 + c)n}$	$l = O(c\sqrt{n})$
c-frameproof code	$l = c^2\log_2^2(n)$	$l = O(c^2\log_2^2(n))$

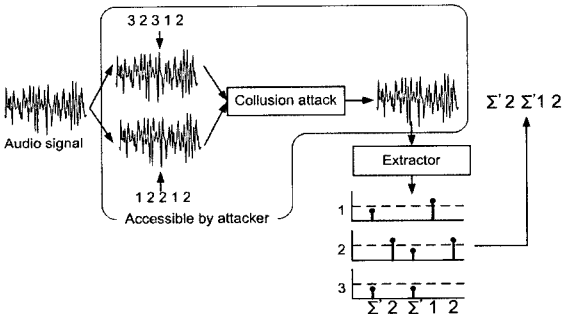
표 3 사용자가 100만 명일 때 공모공격자 수에 따른 각 코드의 길이 비교

c	c-secure code	Finite geometry	Anti-collusion code	c-frameproof code
2	5.35×10^{5}	1.00×10^{12}	2449	1589
5	2.29×10^{7}	1.00×10^{30}	5477	9932
10	3.90×10^{8}	1.00×10^{60}	10488	39727
20	6.63×10^{9}	1.00×10^{120}	20493	158910
50	2.79×10^{11}	1.00×10^{300}	50497	993170
100	4.70×10^{12}	1.00×10^{600}	100498	3972700

3.3 공모 공격과 핑거프린팅 검출



(a) 일반적 핑거프린트



(b) 워터마크 핑거프린팅

그림 6 핑거프린팅과 공모공격

그림 6은 일반적 핑거프린트의 공모공격과 워터마크 핑거프린팅의 공모공격에서의 차이를 보여주고 있다. 그림 6(a)와 같이 사용자1과 사용자2에 32312와 12212의 코드가 할당되어 있고 이 두 사용자가 공모공격을 했을 경우 공모공격으로 생성된 코드는 22?12가 될 수 있다. 여기서 첫 번째 위치와 세 번째 위치는 두 사용자에게 다른 값이 할당되기 때문에 코드의 위치가 식별 가능하고 나머지 위치는 같은 값을 같기 때문에 공모공격자가 코드가 들어있는지 식별할 수 없다. 따라서 공모공격자는 식별 가능한 위치인 첫 번째와 세 번째 위치의 값을 바꾸게 되는데 위의 예처럼 공격 후의 코드에서 첫 번째 위치의 2는 원래의 알파벳에 속한 값으로 변경한 경우이고 세 번째 위치의 ?는 원래의 알파벳에 속하지 않는 값으로 변경한 경우이다. 일반적 핑거프린팅의 경우에는 세 번째 위치의 ?가 공모공격을 받았다는 것은 알 수 있지만 첫 번째 위치의 2는 변경된 것인지 아닌지 식별할 수 있는 방법이 없다. 따라서 일반적 핑거프린트로서의 c-frameproof 코드는 공모공격이 일어났을 때 공모자를 추적할 수 없게 된다. 반면, 워터마크 핑거프린팅의 경우에는 그림 6(b)처럼 코드의 추출부를 워터마킹 기법의 추출부를 사용한다. 따라서 위의 예에서 첫 번째 위치의 값이 1과 3에서 조금씩 값을 갖게 되므로 어떤 문턱치 이하로 만들 수 있기 때문에 이 위치를 공모공격을 받은 것으로 최종 판별할 수 있게 된다. 따라서 워터마크 핑거프린팅의 경우 이 예에서 첫 번째와 세 번째가 공모공격을 받았다는 것을 알 수 있다. 워터마크 핑거프린팅 코드로서의 c-frameproof 코드는 표시가정을 만족하기 때문에 공모공격을 받지 않은 나머지 3개의 값과 그 위치를 토대로 공모공격자를 추적할 수 있게 된다.

공모공격자의 추적측면에서 주요 관심사항은 공모공격을 받은 부분과 아닌 부분을 식별해 내는 능력이다. 핑거프린팅 코드로 이진코드를 사용한다면 공모공격을 받지 않은 부분은 0또는 1의 값을 갖게 되고 공모공격을 받은 부분은 $0<x<1$의 값을 갖게 된다. 만약 공모공격을 받은 부분이 0또는1에 가까워지면 공모공격을 받지 않은 것으로 오인할 확률이 높아지게 된다. 따라서 다음 두 가지 측면에서 성능의 개선을 고려해 볼 수 있다. 하나는 공모공격 받은 값이 공모공격자의 수에 상관없이 0.5근처가 되도록 코드를 설계하거나 다른 하나는 0또는1에 가까워도 이를 식별해 내는 능력을 갖도록 추적기를 개선하는 것이다. 이를 위한 개선은 향후 과제로 남겨두고 현재는 그림 7과 같은 간단한 문턱치 비교기로 추적기를 구현해 볼 수 있다.

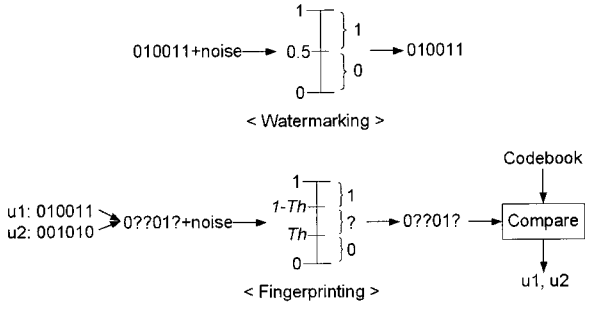


그림 7 핑거프린팅 검출기

4. 오디오 핑거프린팅 응용

사용자 정보를 추적하기 위한 핑거프린팅 기술은 기존의 워터마킹 기술보다 더 큰 정보량을 제공할 수 있어야 하며, 같은 콘텐츠라도 다른 사용자 정보가 삽입되기 때문에 공모 공격 등 추가적인 공격에 대해서도 강인해야 한다. 따라서 기존 워터마킹 기술에 요구되는 요건들 이외에도 핑거프린팅 기술의 요건을 함께 충족시켜야 하기 때문에 세계적으로 매우 어려운 기술로 알

려져 있으며, 제안 기술 또한 매우 드문 실정이다. 그러나, DRM 기술을 보완할 수 있는 적극적인 보호 기술이기 때문에 향후 핑거프린팅 기술의 적용은 필수적이라고 예상되며 현재 미국의 디지털 시네마의 경우를 보더라도 그 효용성을 매우 높게 평가하고 있다.

디지털 시네마란 헐리우드의 대형 스튜디오들이 영화 배급을 기존의 필름 배급과 영사기를 통한 상영에서 벗어나 영화를 디지털로 각 극장에 배포하고 이를 대형 프로젝터로 상영하는 차세대 극장 방식을 말한다. 현재 디지털 시네마와 관련된 기술적 문제는 모두 해결되었으나 이에 대한 적극적인 보급이 더디게 이루어지고 있는 이유는 헐리우드 스튜디오 입장에서 배급되는 영화 콘텐츠가 불법 유통되는 것을 우려하고 있기 때문이다. DC28과 같은 워킹그룹에서 이러한 저작권 보호 문제를 해결하기 위한 기술로 CAS(Control Access System)와 핑거프린팅 기술을 제시하고 있는데, CAS는 영화를 암호화하여 위성으로 전세계 극장에 전송해 대용량 하드에 저장하는 것으로 안전한 인증 과정을 거쳐 영화 상영 전과정에서 콘텐츠의 불법 유출을 제한하게 되며, 핑거프린팅 기술은 CAS 기술로는 막을 수 없는 캠코더를 이용한 불법 복제를 해결하기 위해 사용된다.

캠코더로 영화를 찍어서 불법 배포하는 문제를 해결하기 위해서는 각 극장별로 이를 막기위한 적극적인 노력이 필요한데 핑거프린팅 기술을 이용하여 각 극장에 배급되는 영화 콘텐츠에 극장에 대한 정보를 삽입한다면 캠코더 버전의 불법 콘텐츠가 유통되었을때 삽입된 핑거프리팅 정보를 검출하고 불법 복제가 일어난 극장을 확인한 뒤 이후 이 극장에 대한 영화 배급을 제한하게 함으로써 각 극장으로 하여금 적극적으로 불법적인 캠코더 복제 감시 및 관리에 나서게 할 수 있을 것이다.

이와 같이 핑거프린팅 기술은 DRM, CAS 등과 결합되어 실제 시스템에 사용될 수 있다. 예를 들어 DRM 솔루션과 같이 Client/Server 환경의 시스템에 하나의 모듈로써 포함될 수도 있고 DRM이 필요하지 않은 콘텐츠에 사용자 정보만을 기록하는 클라이언트의 작은 부분으로도 포함될 수 있는 유연성을 갖고 있다. 핑거프린팅을 DRM 시스템에 적용한 예를 그림 8에 도시하였다. 여기에서는 DRM 시스템의 안전성 취약 부분이 클라이언트단에서 정당한 사용자가 불법 캡쳐를 시도하는 경우라고 보고, 핑거프린팅 기술을 클라이언트단에 적용하여 DRM이 해제되어 플레이되는 콘텐츠에 핑거프린팅 코드를 실시간으로 삽입하여 추후 캡쳐된 콘텐츠가 유포되었을 때 불법 사용자를 추적할 수 있도록 전체 시스템을 구성하였다.

핑거프린팅 적용 부분을 좀더 자세히 살펴보기 위하

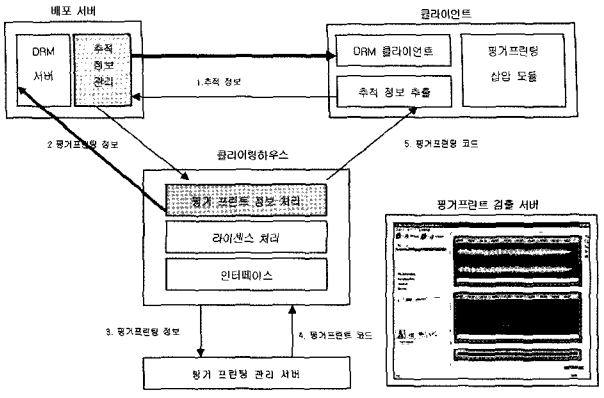


그림 8 DRM 및 핑거프린팅 시스템

여 사실상 업계표준이라고 말할 있는 Microsoft사의 Windows 계열의 OS상에서 구현되는 경우를 기준으로 오디오 핑거프린팅을 적용한 결과를 살펴보면 다음과 같다.

핑거프린팅 코드 삽입 : 일반 사용자가 오디오 핑거프린팅이 적용될 콘텐츠를 이용하려고 할 때, 메모리상에 로드되어 사용자 PC의 사운드카드에서 오디오가 플레이(Rendering) 되기 직전에 사용자의 정보가 주기적으로 PCM 웨이브 데이터에 삽입되도록 한다. 삽입 방법은 강인성 및 정보량, 복잡성 등을 고려하여 기존의 워터마킹 방법 중 적합한 방법을 채택하여 사용한다. 이러한 과정을 거치는 이유는 사용자의 악의적인 불법 캡쳐시 사용자의 정보가 실시간으로 콘텐츠에 삽입되어 추후에 불법 복제에 대한 추적을 가능하게 하기 위한 것이다. 기 개발된 오디오핑거프린팅 삽입모듈은 Microsoft사의 Direct Show에 기반한 Filter를 사용하였다. Microsoft사의 Windows계열의 OS에서 대부분의 미디어 플레이어들은 Direct Show에 기반한 Filter를 사용해서 각종 콘텐츠들을 디코딩한다. 모든 오디오 데이터를 포함한 콘텐츠는 디코딩 과정을 거쳐서 최종적으로는 PCM 웨이브 데이터로 변환되기 때문에 이와 같이 오디오핑거프린팅 삽입에 필터를 이용하면 어떠한 미디어 플레이어와도 유연하게 결합될 수 있다.

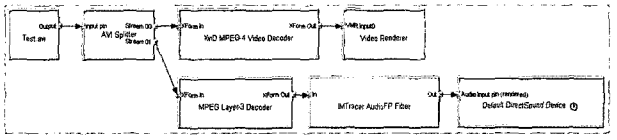


그림 9 미디어플레이상에서 구성된 필터의 예 (Graph Manager)

그림 9에서 오디오핑거프린팅 필터는 사운드카드에 PCM 웨이브 타입의 데이터가 보내지기 직전의 과정에서 삽입되는 것을 볼 수 있다. 필터는 파일로 사용자의 PC에 설치될 수도 있고, 플레이어상에 소스레벨로 포

함되어 메모리로만 로드되어 악의적 사용자의 파일접근을 근본적으로 막을 수도 있다. 또한, Streaming 방식이 아닌 File 자체에 오디오 핑거프린팅 코드를 삽입하는 방법도 가능하다. 이는 음반사의 오디오 CD에 제작사의 신호를 직접 삽입하거나 각종 블로그 동영상에 사용자의 저작권을 보호하기 위한 신호 삽입 등을 하는 경우에 고려할 만하다.

- 핑거프린팅 코드 검출 : 이 과정은 사용자 정보가 오디오 데이터에 삽입된 콘텐츠가 캡쳐되어 인터넷상에서 유포되었을 때, CP(Content Provider) 측에서 수집된 콘텐츠에서 사용자 정보를 추적하기 위한 것으로 그림 10에 구현된 예를 볼 수 있다.
- 검색/배포 서버 : 오디오핑거프린팅 기술을 이용한 실제 불법 복제 추적 시스템을 구현하기 위해서는 인터넷상에서 유포되는 파일들을 자동적으로 다운로드 받아서 의심되는 파일들에서 핑거프린팅 코드를 자동적으로 검출하는 것이 효과적일 것이다. 따라서, 이러한 부분은 필수적인 요소는 아니지만 사이트의 규모가 커질수록 자동화된 검색 서버를 함께 개발할 필요가 있다. 배포서버는 사용자의 PC 상에 설치될 Filter를 다운로드 시켜주는 서버로서 플레이어에 직접 내장시키는 방법 또는 Filter 서버에 등록하는 방법 등으로 사용자 편의를 증대시킬 수 있다.

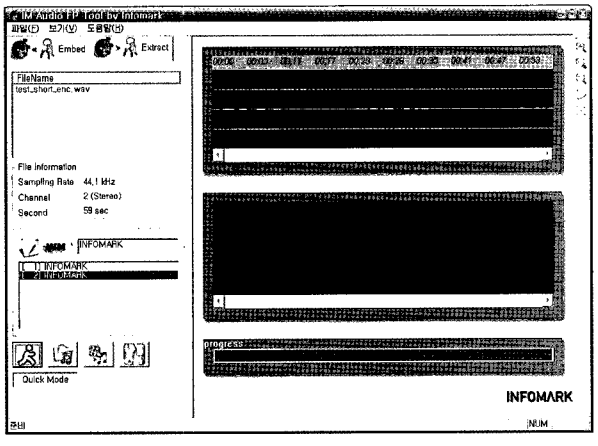


그림 10 오디오핑거프린팅 신호 추출과정

참고문헌

[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 in: *IWDW*, 2002, pp. 88-103.

[3] W. Trappe, M. Wu, J. Z. Wang, and K.J.R. Liu, "Anti-collusion fingerprinting for multimedia," *IEEE Trans. on Signal Processing*, Vol. 51, No. 3, pp. 1069-1087, 2003.

[4] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. on Information Theory*, Vol. 44, pp. 1897-1905, 1998.

[5] J. Dittmann, "Combining digital watermarks and collusion fingerprints for customer copy monitoring," in *Proceeding of IEE Seminars on Secure Images and Image Authentication (SIIA'00)*, pp.128-132, 2000.

[6] J. Domingo-Ferrer and J. Herrera-Joancomarti, "Short collusion-secure fingerprints based on dual binary hamming codes," *Electronic Letters*, Vol. 36, No. 20, pp. 1697-1699, 2000.

최 혁

1994. 2 서울대학교 전자공학과(학사)
1996. 2 서울대학교 전자공학과(석사)
2002. 2 서울대학교 전기컴퓨터공학부 (박사)
2003. 3~현재 서울시립대학교 컴퓨터과학부 교수
관심분야 : 정보보호, 신호처리
E-mail : chyuk@venus.uos.ac.kr

정 해 경

1999. 2 서울대학교 전기공학부(학사)
2001. 2 서울대학교 전기,컴퓨터공학부 (석사)
2001. 3~현재 서울대학교 전기,컴퓨터공학부 박사과정
관심분야 : 음성신호처리, 생체신호처리, 패턴인식, 오디오 워터마킹 및 핑거프린팅
E-mail : shizuka@infolab.snu.ac.kr

윤 영 진

1997. 8 서울대학교 농업기계학과(학사)
1999. 2~2000. 2 (주) 정문정보
2000. 3~2001. 5 (주) KGI증권
2002. 5~현재 (주) 인포마크
관심분야 : 정보보호, EDMS, 소프트웨어
E-mail : mrformis@infomark.co.kr