제로기반 코드 변조 기법을 통한 비디오 핑거프린팅 시스템

최 선 영[†] · 이 해 연[††] · 강 인 구[†††] · 이 흥 규[††††]

요 약

디지털 핑거프린팅은 워터마킹 기술에 기반한 콘텐츠 보호 기술로 디지털 콘텐츠에 구매자의 정보인 핑거프린트를 삽입하는 기술을 말한다. 콘텐츠 안에 삽입된 핑거프린트 정보는 다양한 공격을 받게 된다. 특히 동일한 콘텐츠 안에 서로 다른 구매자의 정보를 넣게 되는 핑거프린팅의 특성으로 인해 공모 공격이 가능하고, 그 중 평균화 공격은 빠르고 효과적인 공모 공격에 해당한다. 본 논문에서는 평균화 공격에 강인한 비디오 핑거프린팅 시스템을 제안한다. 공모 공격 후에도 특정 위치의 코드 값이 원래의 값을 유지할 수 있는 공모 방지 코드를 적용하였다. 또한 사용자의 수가 늘어남에 따라 핑거프린트 코드의 길이가 증가하는데 이와 같은 코드의 효율적인 삽입 및 검출을 위해 제로기반 코드 변조 기법을 적용함으로써 올바른 공모자 추적이 가능하도록 하였다. 제안한 방식을 사용하여 원본 비디오를 사용하지 않는 비디오 핑거프린팅 시스템을 구현하였고, 다양한 공모자의 수에 따른 실험을 수행하였다. 실험 결과에 따르면 대부분의 경우 공모자를 올바르게 추출할 수 있었고, 최소 한 명 이상의 공모자를 성공적으로 검출할 수 있었다.

키워드 : 디지털 핑거프린팅, 공모 방지 코드, 공모 공격

Video Fingerprinting System through Zero-based Code Modulation Technique

Sun Young Choi[†] · Hae-Yeoun Lee[††] · In Koo Kang[†††] · Heung-Kyu Lee[††††]

ABSTRACT

Digital fingerprinting is a contents-protection technique, where customer information is inserted into digital contents. Fingerprinted contents undergo various attacks. Especially, attackers can remove easily the inserted fingerprint by collusion attacks, because digital fingerprinting inserts slightly different codes according to the customers. Among collusion attacks, averaging attack is a simple, fast, and efficient attack. In this paper, we propose a video fingerprinting system that is robust to the averaging attack. In order to achieve code efficiency and robustness against the averaging attack, we adopt anti-collusion code (fingerprint code) from GD-PBIBD theory. When the number of users is increased, the size of fingerprint code also grows. Thus, this paper addresses a zero-based code modulation technique to embed and detect this fingerprint code efficiently. We implemented a blind video fingerprinting system based on our proposed technique and performed experiments on various colluding cases. Based on the results, we could detect most of colluders. In the worst case, our scheme could trace at least one colluder successfully.

Key Words : Digital Fingerprinting, Anti-collusion Code, Collusion Attack

1. 서 론

인터넷의 발달과 디지털 멀티미디어 기술의 발달로 동영상, 이미지, 오디오 등의 디지털 멀티미디어 콘텐츠를 쉽고 빠르게 접할 수 있게 되었다. 그러나 디지털 콘텐츠의 특성상 원본과 동일하게 복사할 수 있다는 점과 사이버 세계의 익명성을 이용해 불법 복제가 빈번히 일어나고 있다. 콘텐츠의 무분별한 불법 배포는 콘텐츠 유통 사업의 활성화와 시장 확대를 막을 뿐 아니라 청소년들을 유해환경으로부터 보호할 수 없는 상황을 만들어가고 있다. 이러한 문제점을 해결하기 위해 저작권 보호를 위한 DRM과 워터마킹 등의 기술이 활발히 연구되고 있다[1, 2, 3, 4].

디지털 핑거프린팅은 워터마킹 기술을 기반으로 하는 콘텐츠 보호 기술로 디지털 콘텐츠에 구매자의 정보인 핑거프린트를 삽입하는 기술을 말한다. 구매자의 정보가 삽입된 콘텐츠가 불법복제 또는 배포를 통해 발견됐을 경우 콘텐츠 안에 포함돼 있는 핑거프린트 정보를 검출함으로 불법 배포자를 찾아낸다[2, 3, 5].

눈에 보이지 않게 삽입된 핑거프린트 정보 역시 워터마킹과 마찬가지로 콘텐츠 안에 삽입된 정보를 없애기 위한 많

※ 본 연구는 첨단정보기술 연구센터를 통하여 과학재단 및 21세기 프론티어 연구개발사업의 일환으로 추진되고 있는 정보통신부의 유비쿼터스컴퓨팅 및 네트워크원천기반기술 개발사업의 지원을 받았음.
† 준 회 원 : LG 전자 Digital TV 연구소
†† 준 회 원 : 한국과학기술원 전산학과 박사과정
††† 정 회 원 : 한국과학기술원 전산학과 박사과정
†††† 정 회 원 : 한국과학기술원 전산학과 교수
논문접수 : 2005년 2월 26일, 심사완료 : 2005년 6월 21일

은 공격을 받게 된다. 이러한 공격 중에 공모 공격은 다른 공격들과 달리 동일한 콘텐츠 안에 서로 다른 구매자의 정보를 넣게 되는 핑거프린팅의 특성으로 발생되는 고유한 공격이라 볼 수 있다. 즉 여러 구매자들이 공모하여 콘텐츠간의 특성을 비교하여 서로 다른점을 찾아 없애려는 공격을 말한다. 이러한 공모 공격에는 공모에 가담한 콘텐츠를 평균화함으로 삽입된 핑거프린팅 정보를 약하게 하는 평균화 공격이 있고, 콘텐츠 사이의 최대값과 최소값 비교를 통한 Min-Max 공격 및 최대 및 최소값 외에 중간값을 이용하는 Negative-modified 공격 등이 있다[6, 10]. 이러한 공모 공격 중 평균화 공격은 공모자들이 가장 빠르고 효과적으로 핑거프린트를 제거할 수 있는 일반적인 공모 공격이고, 삽입된 핑거프린트 정보는 평균화 공격후에도 견고성을 유지하여 최소한 한 명 이상의 공모자 또는 배포자를 찾을 수 있어야 한다.

디지털 핑거프린팅에는 하나의 직교 신호(orthogonal signals)를 콘텐츠에 삽입하는 직교 변조(orthogonal modulation) 방법과 여러 개의 직교 신호를 코드화시켜 삽입하는 코드 변조(coded modulation) 방법이 있다. 직교 변조 방식에서는 직교 신호 하나를 사용자 한명의 핑거프린트 정보로 사용해 콘텐츠에 삽입하는 방법으로 직교 신호의 수가 수용할 수 있는 사용자의 수가 된다. 가령 N개의 직교 신호를 사용할 수 있다면 N명의 사용자에게 핑거프린트를 제공할 수 있고, 공모자를 찾기 위해서는 추출한 핑거프린트를 N개의 각 사용자의 핑거프린트와 상관관계를 구해 공모자를 찾기 때문에 사용자의 수에 비례하여 높은 계산 복잡도의 문제가 발생한다. 코드 변조 방식은 여러 직교 신호를 코드화함으로 직교 변조 방식보다 많은 사용자를 처리할 수 있어 효율성이 높고 공모자 추적시 사용자 신호의 비교 횟수를 줄이는 장점을 갖고 있다. 그러나 코드를 효율적으로 설계하지 않으면 공모 공격이 일어날 경우 실제 공모에 가담하지 않은 사용자가 검출되는 경우가 발생할 수 있고, 이러한 문제를 해결하기 위한 코드가 공모 방지 코드이다[2, 7, 8]. 공모 방지 코드를 기존의 코드 변조 방법을 사용해 삽입할 경우 공모자의 수가 늘어나고 코드의 길이가 길어질수록 올바른 코드 검출이 어려워지며 이로 인해 올바른 공모자 추출이 불가능하다[7].

따라서 본 논문에서는 공모 방지 코드의 특성에 따른 보다 효율적인 제로기반 코드 변조 기법을 제안하고, 원본 비디오 데이터를 사용하지 않는 비디오 핑거프린팅 시스템을 구현하였다. 특히 기존 핑거프린팅 시스템의 경우에 있어서 문제가 되던 삽입된 코드의 검출을 위한 임계값 결정의 문제를 해결하여 올바른 공모자 추적이 가능하도록 하였다. 100개의 비디오 데이터와 다수의 공모자를 통한 실험 결과에 따르면 대부분의 경우에 있어서 올바르게 공모자를 추적할 수 있었고, 공격의 세기가 강하더라도 최소한 한 명 이상의 공모자를 성공적으로 추적할 수 있었다.

본 논문의 구성은 다음과 같다. 2장에서는 공모 방지 코드를 사용한 기존의 코드 변조 기법에 대해 살펴보고, 공모 공격에 대한 문제점을 기술한다. 3장에서는 코드의 길이가 커지는 경우 처리가 용이하고, 기존의 문제점을 해결한 제로기반 코드 변조 기법을 제안하고, 이를 기반으로 구현한 비디오 핑거프린팅 시스템에 대해 설명한다. 4장에서는 비디오 핑거프린팅 시스템의 실험 결과와 성능을 평가하고, 마지막으로 5장에서 결론과 향후 연구 방향을 제시한다.

2. 관련 연구

본 절에서는 공모 방지 코드를 사용한 기존의 코드 변조 기법에 대해 설명하고, 공모 공격중에 대표적인 평균화 공격에 있어서 나타나는 문제점에 대해 기술한다.

2.1 기존의 코드 변조 기법

코드 변조 방식은 여러 개의 직교 신호를 0 또는 1 (혹은 -1 또는 1)의 형태로 조합하여 하나의 핑거프린트로 사용하는 것을 말한다[2, 9, 14]. 이 경우 직교 변조 방식에 비해 같은 수의 직교 신호를 이용해 더 많은 사용자에게 핑거프린트를 배포할 수 있는 장점을 갖게 된다. 예를 들어 직교 신호 u_1과 u_2를 핑거프린트로 사용할 경우 직교 변조 방식에서는 두 직교 신호를 이용해 두 명의 사용자에게 줄 수 있다. 그러나 코드 변조 방식을 사용해 동일한 두 개의 직교 신호 u_1과 u_2를 코드 형태의 조합으로 핑거프린트를 만들 경우 다음과 같이 $-u_1-u_2(00)$, $-u_1+u_2(01)$, $+u_1-u_2(10)$, $+u_1+u_2(11)$ 4개의 핑거프린트를 생성해 4명의 사용자에게 배포할 수 있다. 그러나 코드를 효율적으로 설계하지 못할 경우 삽입된 코드가 공모자들에 의해 평균화 공격을 받게 되면 코드의 고유성을 잃게 되어 검출된 코드는 실제 공모자의 코드가 아닌 다른 사람의 핑거프린트 코드를 얻게 된다. 앞의 예에서 (그림 1)과 같이 사용자 2번(01)과 사용자 3번(10)이 평균화 공모를 할 경우 검출되는 코드의 값은 사용자 1번(00)로 실제 공모에 가담하지 않은 결백한 사용자가 불법 행위자로 누명을 쓰게 된다.

```
  0 1
∧ 1 0
-------
  0 0
```

(그림 1) 코드 변조 방식에서 평균화 공격의 영향

위와 같은 문제를 해결하기 위해 Stinson[7]은 "Frame-proof code"라는 명칭의 코드 체계를 제안했으며 Trappe[8]는 Stinson에 의해 제안된 조합 설계 이론 중의 하나인 BIBD를 공모 방지 코드라 이름하고 이를 핑거프린트로 사용하는 방법을 제안하였다.

공모 방지 코드는 공모 후에도 특정한 위치의 코드 값이 원래의 값을 유지하는 코드로서 BIBD와 GD-PBIBD와 같은 조합 설계 이론을 통해 생성할 수 있다. 이러한 공모 방지 코드를 핑거프린트로 사용할 경우 평균화 공격 후 검출된 코드를 통해 올바른 공모자를 추출할 수 있다. 결국 공모 방지 코드를 핑거프린트로 사용할 경우 평균화 공격에 강하면서 보다 많은 사용자를 수용하는 장점과 공모자 검출을

위한 상관관계 비교 횟수를 사용자 수가 아닌 코드 길이로 줄일 수 있다.

(v, k, 1)-BIBD 공모 방지 코드는 코드의 길이 v와 추적 가능한 공모자의 수 k-1로 표현된다. (v, k, 1)-BIBD 공모 방지 코드가 수용하는 사용자의 수 b는 $(v^2 - v) / (k^2 - k)$이다. 예를 들어, (그림 2)에 나타난 것과 같이 (7, 3, 1)-BIBD의 경우 코드 길이가 7비트인 코드를 총 7명에게 배포하여 2명의 공모자까지 추적할 수 있다. 코드의 효율성은 "직교신호 하나 당 배포 가능한 사용자의 수"를 나타내는 것으로 주어진 직교 신호를 이용해 얼마나 많은 사용자에게 배포할 수 있는지를 의미한다. 따라서 코드의 효율성이 클수록 많은 사용자에게 핑거프린트를 제공할 수 있다.

$$code\ efficiency = \frac{b}{v} \qquad \text{(식 1)}$$

v는 코드 길이가 되며 b는 전체 사용자 수가 된다. 따라서 공모 방지 코드를 선택할 때 공모자의 수에 따른 코드 효율성 비교를 통해 효율성이 높은 코드를 선택하게 된다.

$$C = \begin{pmatrix} \text{user1} & \text{user2} & \text{user3} & & & & \text{user7} & \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & \text{bit1} \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & \text{bit2} \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & \text{bit3} \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & \text{bit4} \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & \text{bit5} \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & \text{bit6} \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & \text{bit7} \end{pmatrix}$$

(그림 2) (7, 3, 1)-BIBD 공모 방지 코드 및 공모자 추적

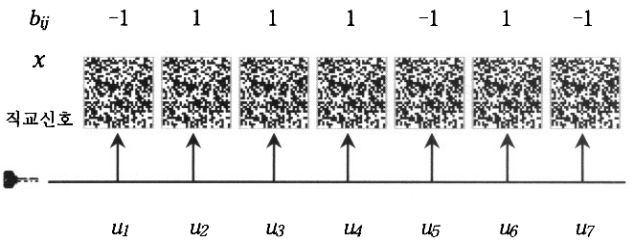
2.1.1 코드 변조 방식을 통한 핑거프린트 삽입

공모 방지 코드를 핑거프린트 코드로 사용하여 콘텐츠에 삽입하는 방법은 다음과 같다. 먼저 코드의 길이에 해당하는 직교 신호(u_1~u_i)를 생성한 뒤 공모 방지 코드의 각 비트 값에 따른 코드 변조를 통해 (식 2)와 같이 하나의 핑거프린트(w_j)를 만든다[9].

$$w_j = \sum_{i=1}^{M} b_{ij} u_i \qquad \text{(식 2)}$$

각 직교 신호를 핑거프린트 코드의 해당 비트 값에 따라 정반대(antipodal, $b_{ij} \in \{+1, -1\}$) 형태 또는 OOK(on-off keying, $b_{ij} \in \{0, 1\}$) 형태로 처리할 수 있으나 검출 단계에서 추출한 코드에서 1과 0의 분리성을 높이기 위해서 정반대 형태가 효율적이다[8]. 공모 방지 코드를 정반대 형태의 코드 변조 방법으로 삽입할 경우 각 코드의 비트 값(x)은 식 $f(x) = 2x-1$에 의해 각각 {-1, 1}로 변조된다. (7, 3, 1)-BIBD 코드에서 사용자 3번의 코드 (0, 1, 1, 1, 0, 1, 0)를 정반대 형태의 코드 변조 방법을 이용해 핑거프린트로 만들기 위해 직교 신호 u_1~u_7를 코드 값에 맞게 변조시키는 과정을 (그림 3)에 도식화하였다. 동일한 방법으로 사용자 7번의 핑거프린트 (1, 1, 1, 0, 0, 0, 1)를 생성하면 (식 3)과 같다.

$$w_3 = -u_1 + u_2 + u_3 + u_4 - u_5 + u_6 - u_7$$
$$w_7 = +u_1 + u_2 + u_3 - u_4 - u_5 - u_6 + u_7 \qquad \text{(식 3)}$$



(그림 3) 공모 방지 코드를 사용한 코드 변조 예

2.1.2 코드 변조 방식을 통한 핑거프린트 검출 및 공모자 추적

공모자 추적은 불법 복제나 불법 배포로 발견된 콘텐츠에서 먼저 공모 코드 검출한 후에 검출된 공모 코드를 사용해 공모자나 불법 배포자를 추출하게 된다. 공모 코드 검출은 콘텐츠에서 추출한 직교 신호 (u')와 핑거프린트 삽입시 사용된 직교 신호 (u_1~u_i, i는 코드 길이)와의 상관관계 즉 유사성 (식 4) 비교를 통해 공모 코드의 각 비트값 (1 또는 0)을 결정한다. 임계값보다 큰 검출 판별 값을 갖는 경우 1의 값으로 그렇지 않은 경우 0의 값으로 판별하여 공모 코드를 검출하게 된다. 여기서 N은 직교 신호의 길이이다.

$$similarity = \frac{1}{N}\sum_{i} u' \cdot u_i \geq \text{threshold} \qquad \text{(식 4)}$$

예를 들어, 공모자 세 명이 평균화 공격을 했을 때 코드의 첫 번째 비트가 모두 1의 값을 갖는 경우 검출되는 코드는 $1+1+1 = \{u_1+u_1+u_1\}/3 = 1$이 되며 0의 값이 포함된 경우 $1+1-1 = \{u_1+u_1-u_1\}/3 = 1/3$의 값으로 검출된다. 따라서 검출 값 1과 1/3을 임계값과 비교하여 공모 코드 1 또는 0의 값으로 결정한다. 2.1.1절의 예에서 사용자 3번과 사용자 7번의 핑거프린트가 삽입된 콘텐츠 간에 평균화 공격이 일어나면 콘텐츠 안의 직교 신호 계수는 $(w_3 + w_7)/2 = (0, 1, 1, 0, -1, 0, 0)$이 되고, 임계값과 비교를 통해 공모 코드 (0, 1, 1, 0, 0, 0, 0)을 추출할 수 있다.

공모 방지 코드에서 각 사용자의 핑거프린트는 각 열의 벡터 값이 되며 이때 평균화 공격은 공모자 코드간의 AND 비트 연산에 해당한다. (그림 2)의 (7, 3, 1)-BIBD 코드에서 사용자 3번(0, 1, 1, 1, 0, 1, 0)과 사용자 7번(1, 1, 1, 0, 0, 0, 1)이 평균화공격에 가담했을 경우 두 코드간의 AND 비트 연산의 결과값 (0, 1, 1, 0, 0, 0, 0)이 두 코드간의 평균화 값이 된다. 평균화된 결과 코드 (0, 1, 1, 0, 0, 0, 0)를 보면 두 번째와 세번째 자리의 값이 1임을 알 수 있다. 따라서 공모 방지 코드 중 두번째와 세번째 자리의 값이 1에 해당하는 값을 갖는 코드를 찾아보면 세번째 열과 일곱번째 열의 코드가 되고, 사용자 3번과 7번이 평균화 공격의 공모자임을

알 수 있다.

2.2 공모 공격에 의한 영향

앞에서 설명한 것과 같이 핑거프린팅에서는 동일한 콘텐츠 안에 서로 다른 구매자의 정보를 넣게 되므로 여러 구매자들이 공모하여 콘텐츠간의 특성을 비교하여 서로 다른점을 찾아 없애기 위한 공격을 하게 되고, 이를 공모 공격이라고 한다. 공모 공격에는 선형 공격에 해당하는 평균화 공격과 비선형 공격에 해당하는 Min-Max 공격, Median 공격 및 Negative-modified 공격 등이 있다. 비선형 공격의 경우 대부분 선형 공격과 유사한 성능을 나타내므로 본 논문에서는 선형 공격인 평균화 공격에 초점을 맞추도록 하겠다[10].

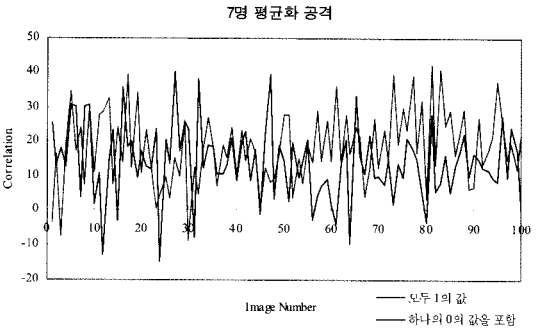
평균화 공격은 공모자들이 가장 빠르고 효과적으로 핑거프린트 정보를 제거 할 수 있는 공모 공격이다. 일반적으로 핑거프린트 정보로는 -1 또는 1(혹은 0과 1)의 값을 갖는 난수열의 집합이 되며 평균화 공격은 삽입된 핑거프린트 신호를 약하게 함으로 핑거프린트를 검출하지 못하도록 한다[11].

$$y_{avg} = y + \frac{1}{n}\sum_{n} s_n \qquad \text{(식 5)}$$

(식 5)는 평균화 공격에 대한 모델이다. 여기서 y는 원본 콘텐츠에 해당하고, y_{avg}는 평균화 공격된 콘텐츠이다. n명의 공모자들이 평균화 공격에 가담한 경우 원본 콘텐츠의 값은 그대로 임에 반해 삽입된 핑거프린트 정보 s_n의 크기값은 $1/n$으로 줄어들게 된다. 따라서 공모자의 수가 증가할수록 핑거프린트의 영향이 줄어들어 원본 콘텐츠와 비슷하게 된다.

코드 변조 기법에서 사용자의 수가 증가하여 코드의 길이가 늘어나고, 공모자의 수가 증가하게 되면 올바른 공모 코드 검출은 어려워진다. 예를 들어 공모자의 수가 7명으로 증가했을때 첫 번째 비트에 0을 갖는 공모자 한 명이 포함된 경우 평균화 공격에 의한 검출 값은 5/7이 되며 공모자의 수가 증가할수록 이 값은 점점 1에 가까운 값이 되고, 공모 코드 검출을 위한 임계값 결정이 쉽지 않다. 특히 검출 과정에서 원본데이터를 사용하지 않거나, 핑거프린트된 콘텐츠가 공격을 당할 경우 올바른 공모 코드 검출을 위한 임계값 결정이 더욱 어려워진다. 이는 실제 핑거프린트 코드가 삽입된 콘텐츠 간의 평균화 공격이 AND 비트 연산의 결과값과 동일하지 않다는 문제로 인해 발생되는 결과이다.

(그림 4)는 실제 100개의 비디오 프레임에서 상관계수를 검출한 결과값이다. 7명의 공모자들이 평균화 공격을 했을 때 동일한 위치의 코드 값이 모두 1의 값을 갖는 경우와 하나의 0을 포함한 경우에 대한 상관관계 값을 나타낸 것이다. 각 점들은 정해진 임계값에 의해 1 또는 0의 값으로 결정되게 된다. 그러나 그림에서 보듯이 두 값 사이의 유사성으로 인해 1과 0의 값 분리를 위한 임계값 결정이 어렵다는 것을 볼 수 있다. 또한 0이 포함된 경우가 1의 값만으로 구성된 코드보다 높은 값을 갖는 경우도 볼 수 있다. 결국 이러한 검출 결과는 올바른 공모 코드를 검출하지 못하도록 함으로 결백한 사용자를 공모자로 누명을 씌우는 결과를 초래할 수 있다.



(그림 4) 100장의 비디오 프레임에 대한 공모공격시의 상관관계 값 비교

3. 제안한 제로기반 코드 변조 기법

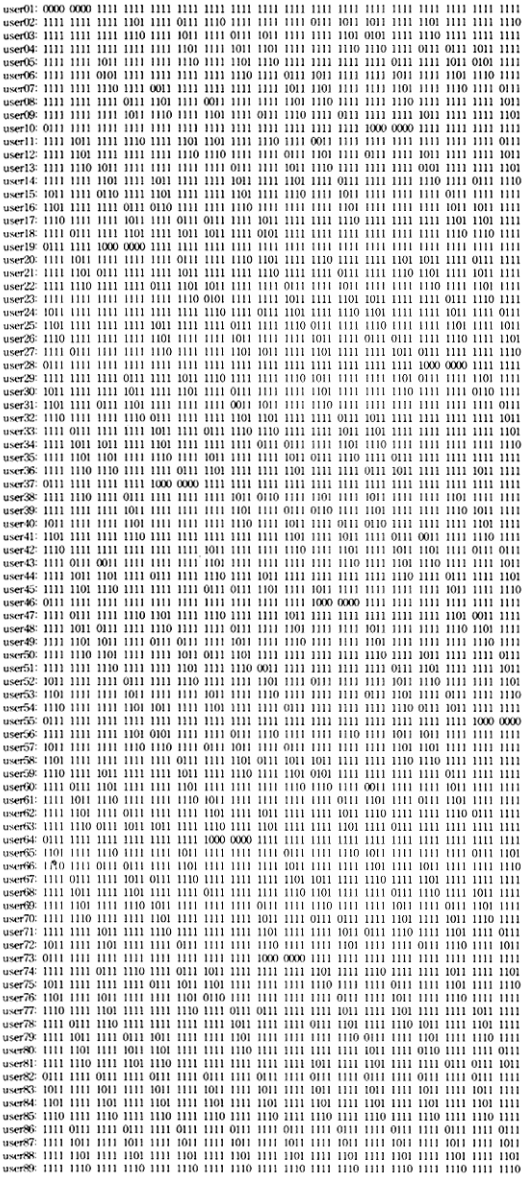
기존의 코드 변조 기법을 통해 삽입된 핑거프린트 코드는 평균화 공격 후 임계값 결정의 어려움으로 인해 올바른 공모 코드 검출이 어렵다는 것을 알 수 있다. 공모 방지 코드를 핑거프린트로 사용하기 위해서는 임계값 결정의 문제를 해결하여 올바른 공모 코드 검출을 통한 공모자 추출을 가능하도록 해야 한다. 이를 위해 제로기반 코드 변조 기법을 제안한다.

제로기반 코드 변조 기법은 공모 코드를 위한 1의 값 검출 문제를 0의 값 검출로 문제로 바꾼 것이다. 즉, 핑거프린트 코드 중 0에 해당하는 직교 신호만을 핑거프린트로 사용해 콘텐츠에 삽입하게 된다. 핑거프린트가 삽입된 콘텐츠는 해당 직교 신호와의 상관관계를 구한 뒤 공모 코드를 결정한 후에 공모자를 추적한다. 이렇게 0에 대한 신호만을 사용하여 처리하면 콘텐츠에 삽입해야 하는 데이터의 양이 줄어들므로 알고리즘의 견고성을 높일 수 있다. 또한 공모코드 검출에 있어서 임계치 결정의 문제가 콘텐츠에 0에 해당하는 워터마크 신호의 존재 여부를 결정하면 되기 때문에 손쉽게 해결이 된다.

본 논문에서는 BIBD 보다 코드의 효율성이 높은 GD-PBIBD 코드를 디자인하여 사용하였다. (v, b, r, k, λ_1, λ_2) GD-PBIBD 공모 방지 코드는 코드의 길이 v, 코드가 수용하는 사용자의 수 b 및 추적 가능한 공모자의 수 $k-1$로 표현된다. 기타 파라미터 (r, λ_1, λ_2)는 코드를 설계하는데 있어서 코드가 갖추어야 할 제약조건에 해당한다. 본 연구에서 사용한 (72, 89, 9, 8, 0, 1) GD-PBIBD 코드는 (그림 5)에 나타나있다. 이 공모 방지 코드이 경우 72비트 정보를 이용해 총 89명의 사용자를 수용할 수 있으며 최대 7명까지의 공모자 검출이 가능한 코드이다.

3.1 핑거프린트 삽입

2절에서 설명한 것과 같이 공모 방지 코드는 0 과 1의 행렬 형태로 표현할 수 있고, 각각의 열이 사용자에게 할당되는 핑거프린트 코드이다. (그림 5)에 나타난 GD-PBIBD 코

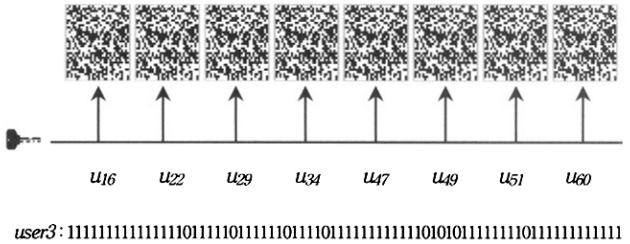


(그림 5) (72,89,9,8,0,1) GD-PBIBD 핑거프린트 코드.

드의 경우 편의상 행/열을 치환하여 표시하였다. 따라서 각 행이 사용자에게 할당되는 코드이다. 제로기반 코드 변조 기법에서는 각 사용자의 핑거프린트 코드에서 0에 해당하는 직교 신호만을 콘텐츠에 삽입하여 핑거프린팅을 수행한다. 제로기반 코드 변조 기법을 사용하여 핑거프린트를 삽입하는 과정은 다음과 같이 요약할 수 있다.

① 핑거프린트 코드의 길이(비트 수 M)만큼 직교 신호($u_1 \sim u_M$)들을 생성한다.
② 각 사용자의 핑거프린트 코드에 대해
A. 0의 위치에 해당하는 직교 신호들(u_i)를 선택한다.
B. 선택된 직교 신호(u_i)들을 콘텐츠에 삽입한다.

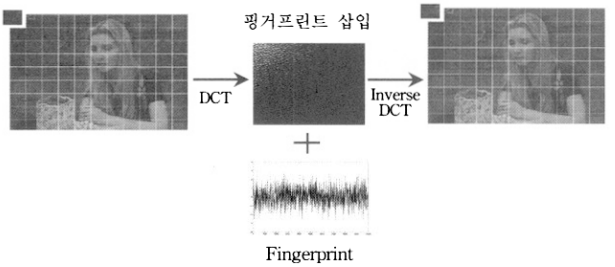
예를 들어, (72, 89, 9, 8, 0, 1) GD-PBIBD 공모 방지 코드를 핑거프린트로 사용할 경우 사용자 1번에서 80번까지는 각 코드마다 8개의 0이 포함되어있고 사용자 81번에서 89번은 9개의 0이 존재한다. 따라서 최대 9개의 직교 신호를 조합하여 사용자 한 명을 표현할 수 있다. (그림 6)은 사용자 3번의 핑거프린트를 만드는 과정을 그림으로 나타낸 것이다. (72, 89, 9, 8, 0, 1) GD-PBIBD 공모 방지 코드에서 사용자 3번의 코드를 살펴보면 16^{th}, 22^{nd}, 29^{th}, 34^{th}, 47^{th}, 49^{th}, 51^{st}, 60^{th} 값이 0이고 나머지는 모두 1인 코드이다. 따라서 직교 신호($u_1 \sim u_{72}$) 중 0의 위치에 해당하는 직교 신호만을 핑거프린트로 콘텐츠에 삽입하여 해당 비트값이 0임을 나타낸다.



(그림 6) 사용자 3번의 핑거프린트 생성

콘텐츠에 핑거프린트 정보를 삽입할 수 있는 영역은 크게 공간 영역과 주파수 영역이 있다. 삽입 영역의 선택은 해당 어플리케이션에 맞게 각 영역의 장단점을 고려한 후 적절히 선택하게 된다. 본 논문에서는 비디오 핑거프린팅 시스템을 목적으로 하고 있으므로, 압축 공격에 강인한 Discrete Cosine Transform을 통한 주파수 영역에 핑거프린트 정보를 삽입한다. (그림 7)에는 선택된 직교 신호들을 비디오 영상에 삽입하는 과정을 나타냈다.

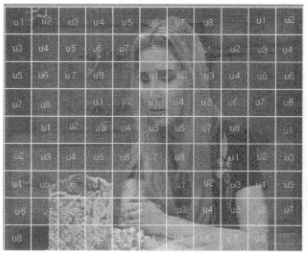
① 비디오 영상을 블록으로 분할하고 DCT 변환을 한다 (그림 7 참조).
② 선택된 직교신호를 각각의 블록에 견고성과 비인식성을 고려하여 DCT의 중간 주파수 영역에 삽입한다[12, 13].
③ 각 블록을 Inverse DCT 변환을 통해 영상으로 복원한다.



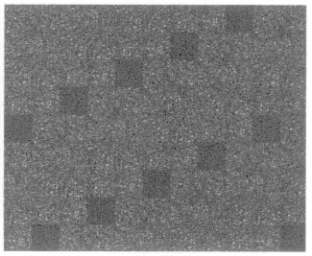
(그림 7) 핑거프린트 코드 삽입과정

CIF 포맷(352*288) 영상에 선택된 직교 신호들을 삽입하기 위해 영상을 32*32 블록으로 나누고 99개의 각 블록에 선택된 직교 신호를 여러번 반복해서 넣게 된다. 예컨데 (72, 89, 9, 8, 0, 1) GD-PBIBD 공모 방지 코드에서 사용자 1번의 핑거프린트의 경우 $1^{st} \sim 8^{th}$ 비트 값이 0에 해당하고,

따라서 직교 신호 $u1 \sim u8$를 (그림 8)에 나타난 것과 같이 각 블록에 삽입할 수 있다. (그림 9)는 원 영상과 핑거프린트된 영상 사이의 잔차를 나타낸 영상이다.



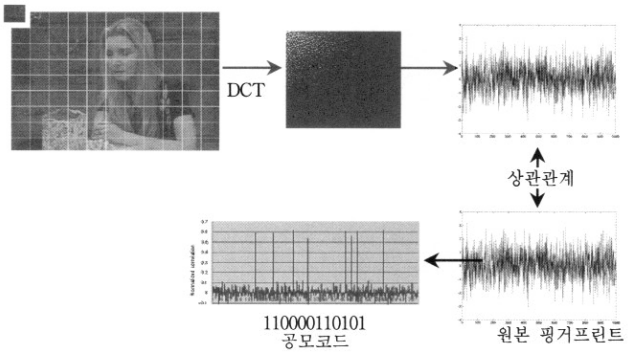
(그림 8) 블록화된 CIF 비디오 영상



(그림 9) 원영상과 핑거프린트 영상 사이의 잔차

3.2 핑거프린트 검출 및 공모자 추적

제로기반 코드 변조 기법에서 삽입된 핑거프린트를 검출하는 과정을 설명하도록 하겠다. 삽입한 직교 신호를 검출하기 위해서는 일반적인 워터마크 검출 방법과 같이 콘텐츠에서 핑거프린트를 추정하고, 삽입 과정에서 사용된 직교 신호와의 유사성 비교를 통해서 해당 직교 신호의 존재 여부를 판단한다. (그림 10)에 삽입된 핑거프린트 코드를 추출하는 과정을 도식화하였다.

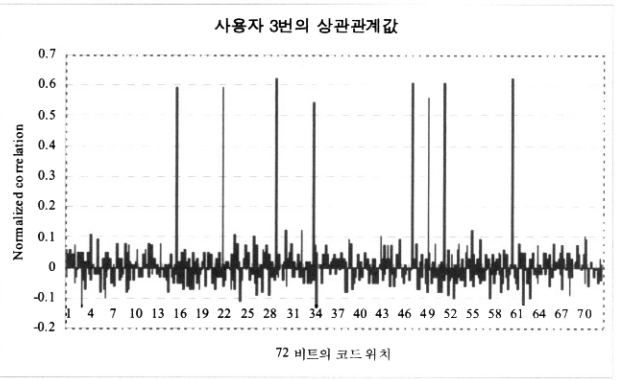


(그림 10) 공모 코드 검출과정

① 핑거프린트 삽입 과정에서 사용한 직교 신호($u1 \sim uM$)들을 생성한다.
② M 비트 길이의 공모 코드의 모든 비트 값을 1로 초기화 한다.
③ 콘텐츠에서 검출한 신호와 각 직교 신호($u1 \sim uM$)와의 유사성 비교를 통해 해당 직교 신호의 유무를 판단 한다.
④ 검출된 직교 신호와 동일한 위치의 공모 코드의 비트 값을 0으로 설정한다.
⑤ 생성된 공모 코드를 사용하여 공모자를 추적한다.

이 과정을 통해 본 논문에서 구현한 비디오 핑거프린팅 시스템에서 핑거프린트 검출 및 공모자 추적을 위한 과정은 다음과 같다.

① 삽입 과정과 같이 비디오 영상을 블록으로 분할하고 DCT로 변환한다.
② 변환된 DCT의 중간 주파수 영역에 삽입된 직교 신호를 추출한다. 동일한 직교 신호가 삽입된 블록에서 추출한 직교 신호들은 하나로 통합한다.
③ 추출한 직교 신호와 삽입 과정에서 사용한 직교 신호 사이의 정규상관관계를 비교하여 직교 신호의 유무를 판별하여 공모 코드의 각 비트 값을 결정한다[12, 13].
④ 기존의 코드 변조 기법에서와 동일하게 검출된 공모 코드와 동일한 위치에 1을 포함한 코드를 공모 방지 코드에서 검출하여 공모자를 추적한다.



(그림 11) 공모코드 검출을 위한 상관관계값

(그림 11)은 공모자 추적을 위해 실제 콘텐츠에서 공모 코드를 검출한 결과값이다. 검출된 결과값을 보면 72 비트의 상관관계값 중 16^{th}, 22^{nd}, 29^{th}, 34^{th}, 47^{th}, 49^{th}, 51^{st}, 60^{th}에서의 상관관계 값이 임계값보다 높은 값을 갖는 것을 알 수 있다. 즉 해당 위치에 0의 값이 포함됐다는 것을 의미하게 된다. 따라서 72 비트의 공모 코드는 16^{th}, 22^{nd}, 29^{th}, 34^{th}, 47^{th}, 49^{th}, 51^{st}, 60^{th} 비트가 0의 값을 갖고, 나머지는 모두 1의 값을 갖는다. 검출된 공모 코드를 (72, 89, 9, 8, 0, 1) GD-PBIBD 공모 방지 코드에서 동일한 위치에 1의 값은 갖는 코드를 검색하면 사용자 3번을 추적할 수 있다.

4. 성능 평가

본 장에서는 제안한 제로기반 코드 변조 방식에 따른 비디오 핑거프린팅 시스템의 성능을 평가한다. 제안한 비디오 핑거프린팅 시스템은 평균화 공격에 초점을 맞추어서 구현하였고, 이 장에서는 평균화 공격에 대한 건고성을 중심으로 실험을 수행하고, 그 결과를 정리한다.

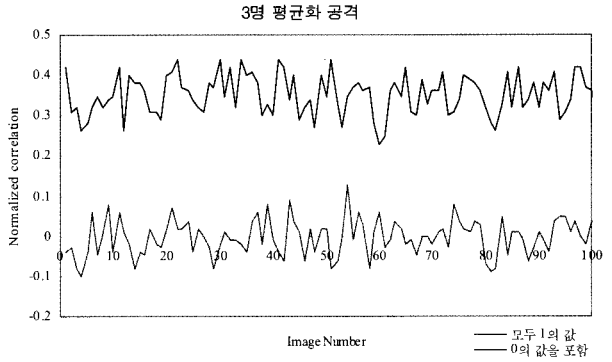
비디오 핑거프린팅 시스템의 요구 사항은 MPEG-4 형태의 동영상 데이터를 사용하였고, 최소 CIF(352*288) 크기의 200 프레임 이상의 데이터를 기준으로 하였다. 또한 핑거프린트 삽입 후의 영상의 화질(PSNR)은 38dB 이상으로 하였다. 사용한 공모 방지 코드는 (72, 89, 9, 8, 0, 1) GD-PBIBD로서 추적 가능한 최대 공모자의 수는 7명이다.

공모 코드를 결정하기 위해 유사성의 판단하는 방법으로는 상관관계(Correlation)과 정규상관관계(Normalized Correlation)가 사용된다. 그러나 기존의 코드 변조 기법의 경우 정규상

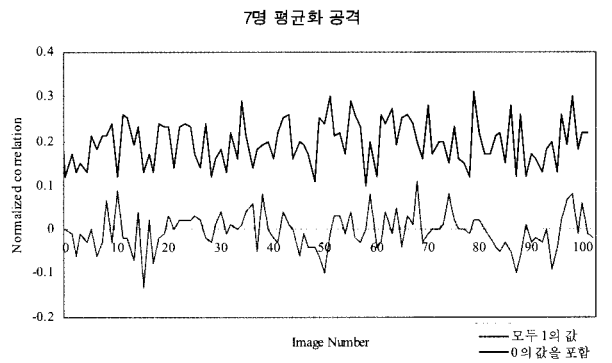
관관계를 사용할 경우 유사성을 계산하기 전에 핑거프린트가 정규화되므로, 평균화 공격에 의한 영향이 없어진다. 즉 올바른 코드의 검출이 불가능하므로 상관관계를 유사성 판단을 위해 사용해야 한다. 그러나 제안한 방법에 있어서는 유사도를 핑거프린트의 존재 여부를 판단하는데 사용하므로 정규상관관계를 사용해도 영향이 없으므로 값의 범위가 -1에서 1로 제한되는 정규상관관계를 사용하였다.

4.1 평균화 공격에 대한 시스템의 견고성

본 절에서는 비디오 핑거프린트 시스템의 견고성, 즉 평균화 공격 후에도 올바른 공모 코드를 검출할 수 있는지를 테스트 하였다. 이를 위해 100장의 비디오 프레임에 대해 공모자들의 코드값 중에 동일한 위치에 모두 1의 값을 갖는 경우와 0을 포함한 두 경우에 대한 정규상관관계를 분석하였다. 3명과 7명이 평균화 공격을 수행한 후의 결과를 (그림 12)와 (그림 13)에 각각 나타내었다.



(그림 12) 세 명 평균화 공격 후 1과 0의 상관관계값 비교



(그림 13) 일곱 명 평균화 공격 후 1과 0의 상관관계값 비교

두 경우의 실험 결과를 보면 공모자의 수가 늘어날수록 0의 값으로 검출되는 상관관계 값이 점차 줄어들어 1의 값으로 검출되는 상관관계 값에 가까워짐을 확인할 수 있다. 그러나 (그림 4)에 나타난 기존의 코드 변조 기법과는 다르게 상관관계값 사이에 일정한 간격 차가 존재하여 이를 임계값을 통해 0 또는 1의 값으로 결정할 수 있음을 볼 수 있다. 따라서 공모 코드의 값을 정확히 1과 0으로 결정지어 공모 코드 검출을 통한 올바른 공모자 추적이 가능하다.

4.2 공모자 수에 따른 검출률

본 실험에서는 공모자 수 증가에 따른 공모자 검출률을 분석한다. 표 1은 100개의 비디오 데이터에 대해 공모자 수 (1, 2, 3, 4, 5, 6, 및 7 명)에 따라 평균화 공격을 수행한 뒤 공모자들을 추출하고, 실제 사용된 공모자의 수와 비교를 통해 얻은 결과이다. 결과를 살펴보면 4명의 공모자까지는 해당 공모자들을 모두 검출했으나 공모자의 수가 5명에서 7명으로 증가할수록 검출률이 떨어지는 것을 알 수 있다. 공모자의 수의 증가에 따라 검출이 저하되는 이유는 공모자의 수가 증가할수록 평균화 공격에 의해 상관관계값의 차이가 줄어들고, 특히 MPEG-4 동영상 압축을 통한 데이터 손실로 인해 발생하였다. 그러나 7명의 경우에도 최소 2명의 공모자는 찾아낼 수 있으며 87% 이상 모든 공모자를 찾는 결과를 볼 수 있다. 즉 핑거프린팅 시스템의 요구사항인 최소 한 명 이상의 공모자를 올바르게 검출할 수 있음을 확인할 수 있다.

〈표 1〉 공모자 수 증가에 따른 평균화 공격 후의 공모자 검출률

	Number of extracted colluders						
	1	2	3	4	5	6	7
1 colluder	100	-	-	-	-	-	-
2 colluders	-	100	-	-	-	-	-
3 colluders	-	-	100	-	-	-	-
4 colluders	-	-	-	100	-	-	-
5 colluders	-	2	3	3	92	-	-
6 colluders	-	-	1	3	5	91	-
7 colluders	-	4	1	4	1	3	87

5. 결론 및 향후 연구 계획

본 논문에서는 공모 방지 코드를 이용하고, 평균화 공격에 강인한 비디오 핑거프린팅 시스템을 위해 제로기반 코드 변조 방식을 제안하였다. 공모 방지 코드는 하나의 직교 신호를 핑거프린트로 사용하는 직교 변조 방식에 비해 보다 많은 사용자에게 핑거프린트를 제공하는 장점을 갖고 있지만 이러한 공모 방지 코드를 기존의 코드 변조 방식을 통해 핑거프린트로 삽입했을때 임계값 결정의 어려움으로 인해 잘못된 공모자 추적 및 공모자 추적 실패라는 문제점이 발생한다. 이러한 문제점은 실제 비디오 응용 프로그램에 적용된 결과값을 통해 확인 할 수 있었다.

본 논문에서는 공모 방지 코드로 사용되는 GD-PBIBD 또는 BIBD의 코드의 특성을 고려하여 제로기반 코드 변조 기법을 제안함으로 임계값 결정의 문제를 해결하도록 하였다. 제안된 제로기반 코드 변조 기법으로 공모 방지 코드를 삽입할 경우 코드 전체가 아닌 0의 정보만을 반복적으로 삽입하여 견고성을 높였다. 또한 평균화 공격 후에도 콘텐츠에서 0의 위치를 검출함으로 올바른 공모자 추출이 가능하도록 하였다. 실제 (72, 89, 9, 8, 0, 1) GD-PBIBD 공모 방지 코드를 핑거프린트로 사용해 비디오 시스템에 적용하였을 때 성공적으로 공모자들을 찾을 수 있었다. 실험 결과에 따르면 본 논문에서 제안한 제로기반 코드 변조 방식은 공

모 방지 코드 사용을 위한 효과적인 삽입 및 검출 방법이라 할 수 있다. 또한 공모자와 사용자의 수가 증가함에 따라 코드의 길이가 길어지는 공모 방지 코드를 핑거프린트로 사용할 수 있도록 확장성을 제공한다. 앞으로 더 연구해야 할 부분은 복합 공격이라하여 평균화 공격 후에 일어날 수 있는 다양한 신호처리 공격 및 다른 종류의 공모 공격에도 대비해야 할 것이다.

참 고 문 헌

[1] I. Cox, J. Bloom, and M. Miller, Digital Watermarking: Principles & Practice. San Francisco, CA: Morgan Kaufmann, 2001.

[2] M. Wu, W. Trappe, Z.J. Wang, and K.J.R. Liu, "Collusion-resistant Fingerprinting for Multimedia," *IEEE Signal Processing Magazine*, Vol.21, pp.15-27, 2004.

[3] Z. J. Wang, M. Wu, H. Zhao, W. Trappe, and K.J.R. Liu, "Anti-Collusion Forensics of Multimedia Fingerprinting Using Orthogonal Modulation," *IEEE Trans. on Image Processing*, Vol.14(6), pp.804-821, 2005.

[4] E.T. Lin, A.M. Eskicioglu, R.L. Lagendijk, and E.J. Delp, "Advances in Digital Video Content Protection," *Proc. of the IEEE*, Vol.93(1), pp.171-183, 2005.

[5] B. Chor, A. Fiat, M. Naor, and B. Pinkas, "Tracing traitors," *IEEE Trans. Information Theory*, Vol.46, pp.893-910, 2000.

[6] H. S. Stone, "Analysis of attacks on image watermarks with randomized coefficients," *Technical Report*, TR 96-045, NEC Research Institute, 1996.

[7] D.R. Stinson and R. Wei, "Combinatorial properties and constructions of traceability schemes and frameproof codes," *SIAM Journal on Discrete mathematics*, Vol.11, pp.41-53, 1998.

[8] W. Trappe, M. Wu, Z.J. Wang, and K.J.R. Liu, "Anti-collusion Fingerprinting for Multimedia," *IEEE Trans. on Signal Processing*, Vol.51, pp.1069-1087, 2003.

[9] M. Wu and B. Liu, "Modulation and multiplexing techniques for multimedia data hiding," *Proc. of SPIE*, Vol.4518, pp.228-238, 2001.

[10] H. Zhao, M. Wu, Z.J. Wang, and K.J.R. Liu, "Nonlinear collusion attacks on independent fingerprints for multimedia," *IEEE Int. Conf. on Multimedia and Expo*, Vol.1, pp.613-616, 2003.

[11] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. on Image Processing*, Vol.6, pp.1673-1687, 1997.

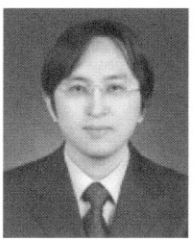
[12] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT domain system for robust image watermarking," *Signal Processing*, Vol.66, pp.357-372, 1998.

[13] C. Podilchuk and W. Zeng, "Image adaptive watermarking using visual models," *IEEE J. Select. Areas on Communications*, Vol.16, pp.525-540, 1998.

[14] W. Trappe, M. Wu, and K.J.R. Liu, "Collusion-Resistant Fingerprinting for Multimedia," *IEEE Int. Conf. on Acoustics, Speech, and Signal Processing*, Vol.4, pp.3309-3312, 2002.

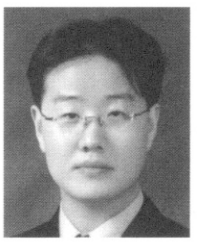
최 선 영

e-mail : choisun05@lge.com
2002년 한동대학교 전자전산학과(학사)
2002년~2003년 (주)essucom 연구원
2005년 한국과학기술원 전산학과(공학석사)
현 재 LG전자 Digital TV 연구소
관심분야 : 디지털워터마킹, 핑거프린팅



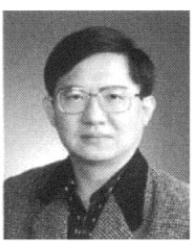
이 해 연

e-mail : hytoiy@casaturn.kaist.ac.kr
1997년 성균관대학교 정보공학과(학사)
1999년 한국과학기술원 전산학과(공학석사)
1997년~2001년 한국과학기술원 인공위성 연구센터
1999년~현재 한국과학기술원 전산학과 박사과정
2001년~현재 (주)쎄트렉아이 선임연구원
관심분야 : 디지털워터마킹, 원격탐사, 멀티미디어시스템



강 인 구

e-mail : ikkang@mmc.kaist.ac.kr
2002년 건국대학교 컴퓨터공학과(학사)
2004년 한국과학기술원 전산학과(공학석사)
2004년~현재 한국과학기술원 전산학과 박사과정
관심분야 : 콘텐츠정보보호 (DRM, 디지털 워터마킹, 디지털핑거프린팅)



이 흥 규

e-mail : hklee@casaturn.kaist.ac.kr
1979년 서울대학교 전자공학과(학사)
1981년 한국과학기술원 전산학과(공학석사)
1984년 한국과학기술원 전산학과(공학박사)
1984년~1986년 Univ. of Michigan 연구원
1998년~1999년 정보통신부 바이러스해킹 센터 보안기술 연구부장
1999년~현재 한국과학재단지정 첨단정보기술연구센터 부소장
1986년~현재 한국과학기술원 전산학과 교수
관심분야 : 디지털워터마킹/핑거프린팅, 정보은닉, Digital Right Managements