논문 2011-48TC-7-6

BIBD AND-ACC 기반 핑거프린팅 삽입 기법

(Fingerprinting Embedding Technique based on BIBD AND-ACC)

사 공 명*, 박 요 한**, 박 영 호***, 문 상 재****

(Myoung Sakong, YoHan Park, YoungHo Park, and SangJae Moon)

요 약

최근 인터넷의 급속한 발달과 스마트폰의 부각으로 인해서 디지털 콘텐츠의 활용이 증가되고 있으나 다양한 공격으로 지적 재산권을 침해할 수 있다. 디지털 콘텐츠의 공모공격에 대처하기 위한 대표적인 핑거프린팅 기술인 BIBD AND-ACC 방식은 매트릭스 연산의 복잡성으로 많은 사용자가 사용하기에는 연산문제가 발생한다. 따라서 본 논문에서는 BIBD 이론을 기반으로 한 공모보안 코드를 생성하여 다수의 콘텐츠 구매자에게 분배 가능한 삽입 기법을 제안한다. 제안한 기법은 컴퓨터 시뮬레이션을 통해 증폭계수 α가 1일때 PSNR이 50.84dB로 실제 사용에 문제가 없는 화질임을 확인하였고 공모공격에 가담한 공모자 추출이 가능함을 실험을 통해 확인하였다.

Abstract

Recently, digital contents are used a lot due to the rapid development of Internet and the commercialization of smartphones. However variety of attacks, such as collusion attack, can violate the intellectual property rights. BIBD AND-ACC is typical method to protect digital contents from attacks, but it is hard to distribute many users because of the heavy complexity of matrix computation. In this paper, we propose embedding technique to distribute BIBD AND-ACC for many users more than primitive one. We checked the PSNR result as 50.84dB when amplication factor is one and found out the colluders who involved the collusion attack by simulation.

Keywords : 디지털 콘텐츠, 핑거프린팅, BIBD, AND-ACC, 공모공격

Ⅰ. 서 론

최근 인터넷의 발달과 멀티미디어 기술의 급속한 발전으로 디지털 콘텐츠의 제작 및 유통에 대한 사회적 요구가 증가함에 따라 콘텐츠 저작자의 저작권 보호에 대한 요청이 날로 증가하고 있는 추세이다. 디지털 콘텐츠의 경우 품질의 손상없이 쉽게 복사 및 변형 등을 통해 인터넷으로 재유포가 가능하기 때문에 지적 재산권에 대한 보호와 불법 행위자 추적에 대한 연구가 더욱 필요하다[1].

디지털 콘텐츠의 저작권을 보호하고 불법 행위자를 추적하기 위해서 디지털 워터마킹의 진보적인 기술인 디지털 핑거프린팅 기술이 대두되었다. 디지털 핑거프린팅 기술은 콘텐츠에 구매자를 식별할 수 있는 정보를 삽입하여 배포하기 때문에 불법 콘텐츠가 발견되면 삽입정보를 이용하여 불법행위에 가담한 구매자를 추적한다. 하지만 악의적인 구매자들끼리 공모를 통해서 새로운 삽입 정보를 생성하거나 제거하는 공모공격이 발생할 수 있으며 이러한 공모공격에 대한 방어책으로는 공모보안코드가 있다.

현재까지 연구된 공모보안코드 방식으로 Boneh의

* 학생회원, 경북대학교 전자전기컴퓨터학부
(Kyungpook National University)
** 정회원, **** 평생회원, 경북대학교 전자공학부
(Kyungpook National University)
*** 정회원-교신저자, 경북대학교 산업전자전기공학부
(Kyungpook National University)
※ 이 논문은 한국전자통신연구원의 IT 산업원천기술 개발사업 위탁연구비 지원에 의하여 연구되었음
접수일자: 2011년4월28일, 수정완료일: 2011년7월13일

c-secure code와 dual binary hamming code[2], 2명의 공모자까지 추적 가능한 Dittmann의 d-detecting 코드[3], 3명의 공모자까지 추적 가능한 Domingo-ferrer의 3-secure code[4] 등이 있다. 하지만 위에 제시된 공모보안코드를 사용하여 공모자를 추적할 경우 공모자수가 극히 제한된다. 이러한 문제점을 해결하기 위한 공모보안코드가 W. Trappe에 의해 제안된 BIBD(balanced incomplete block designs)를 기반으로 한 AND-ACC (anti collusion code)[5]이다. BIBD AND-ACC는 공모공격 발생 시 코드의 특성을 바탕으로 k명이 공모에 가담하였을 때 k-1명까지 공모자를 추출할 수 있는 장점을 가지고 있다. 하지만 많은 사용자가 사용하기 위해서는 코드 생성시 BIBD 매트릭스 연산의 복잡성으로 연산 문제가 발생하므로 이러한 문제의 해결이 요구된다.

본 논문에서는 BIBD 이론을 기반으로 한 공모보안코드를 생성하여 다수의 콘텐츠 구매자에게 분배 가능한 새로운 삽입 기법을 제안한다. 제안한 삽입 기법은 동일한 크기의 BIBD AND-ACC를 n개의 그룹으로 확장하여 코드 그룹이 지정하는 이미지의 위치를 지정하여 삽입하는 기법이다. 본 논문에서는 컴퓨터 시뮬레이션을 통해 실제 사용에 문제가 없는 화질임을 확인하고 공모공격에 가담한 공모자 추출이 가능함을 실험을 통해 확인한다.

Ⅱ. BIBD 기반의 공모보안코드

1. BIBD AND-ACC 이론

공모보안코드를 생성하기 위해서는 공모공격에 강인하면서도 효율적인 코드 설계가 필요하다. 코드 설계 시 고려사항으로는 다양한 공격에도 삽입코드가 손상을 입지 않는 강인성을 가져야하며, 코드의 생성과 동시에 구매자를 분별할 수 있는 성질을 지녀야 한다. 또한 공모공격 발생 시 최소한의 공모자를 추적할 수 있어야 하며 코드 삽입 후 콘텐츠 구매자가 코드를 확인할 수 없는 비인지성의 조건을 만족해야 한다.

위의 요구사항을 만족하면서도 공모공격에 강인한 대표적인 코드가 BIBD이론을 기반으로 생성된 BIBD AND-ACC이다. BIBD를 이용한 공모보안코드는 W. Trappe에 의해서 제안되었으며 Boneh의 c-secure코드, Domingo-ferrer의 3-secure코드, Dittmann의 d-detecting코드 보다 더 많은 공모자가 검출 가능하며 동일한 콘텐츠 구매자에게 할당할 시 코드길이가 가장 짧은 코드 형태이다. BIBD AND-ACC는 0과 1의 심벌의 조합으로 구성된 BIBD 매트릭스를 생성하고 antipodal방식을 통해 삽입될 경우 binary symbol은 {0,1}은 $f(x)=2x-1$라는 함수를 통해 {-1,1}의 형태로 코드가 변환되어 BIBD 매트릭스의 열벡터를 각각의 구매자 식별코드로 가정하여 삽입한다. Combinatorial Designs의 한 부분인 BIBD을 기반으로 하는 BIBD AND-ACC는 공모보안코드의 요구조건을 충족시킬 뿐 아니라 기존의 trivial 코드보다 코드길이를 줄일 수 있어 코드 생성에서부터 코드 분배 후 관리 면에서까지 상당히 효율적이다[5].

2. BIBD 생성 파라미터

BIBD 매트릭스는 기본적으로 v,k,λ 3가지의 파라미터로 표현 하지만 생성시 내부적으로 v,b,r,k,λ 5가지의 파라미터를 사용한다.

- v=처리의 개수(number of treatment)
- b=블록의 개수(number of blocks)
- r=각 v의 반복수
  (number of times each treatment run)
- k=하나의 블록에 포함된 v의 개수
  (number of treatment per block)
- λ=각 처리쌍이 나타나는 블록의 개수
  (number of blocks that processing pair appears)

위의 파라미터를 BIBB AND-ACC 속성과 연관지어 보면 v는 삽입될 코드의 길이를 나타내고, b는 분배될 수 있는 코드의 수 k는 공모공격 발생시 k-1명까지 공모자를 검출할 수 있음을 나타낸다. 또한 위의 5가지 파라미터 값이 모두 양의 정수로 표현되어야 코드 생성이 가능하며 아래의 4가지 조건식과 연관되어 만족해야 된다. 또한 BIBD AND-ACC특성상 λ값은 항상 1로 고정한다[6~7].

1) $vr=bk$
2) $r(k-1)=\lambda(v-1)$
3) $b=v(v-1)\lambda/k(k-1)$
4) $r=\lambda(v-1)/(k-1)$

3. BIBD AND-ACC의 문제점

W. Trappe는 작은 크기의 BIBD 매트릭스를 사용하

여 영상 전체에 삽입 하는 방법을 제안하였다. BIBD 매트릭스는 0과 1의 이진 형태의 구성요소가 BIBD 조건인 5가지 파라미터와 4가지 조건식을 함께 만족되며 생성된다. 생성과정 중 조건 불만족시 무수히 많은 반복과정을 거쳐 최종적으로 BIBD 매트릭스를 생성한다. 또한 공모보안코드 특성상 5가지 파라미터 중 λ값이 항상 1로 고정해야 코드의 유일성을 만족하기 때문에 수행 연산은 늘어나게 된다. BIBD 매트릭스 생성시 v값과 b 값이 커지고 λ값이 1로 고정된 상태에서 코드를 생성하면 연산의 복잡도는 커지고 많은 조건 확인 과정이 필요하기 때문에 코드 생성시 생성자 입장에서는 무한 루프 과정에 빠지는 것처럼 느껴질 수 있는 단점을 가지고 있다. 또한 v와 b값이 크면 다수의 사람들에게 코드를 할당할 수 있지만 상대적으로 코드의 길이가 길어지기 때문에 코드 삽입시 영상의 화질에 영향을 줄 수 있다.

Ⅲ. 제안된 삽입 기법

본 논문에서 제안된 삽입 기법은 다수의 콘텐츠 구매자에 할당 가능한 BIBD AND-ACC 코드를 생성할 시에 생성의 어려움을 보완하고자 작은 크기로 생성된 BIBD 매트릭스를 이용하여 코드가 삽입되기 전에 동일한 BIBD 매트릭스를 n개의 그룹으로 분할하고 그룹별로 해당되는 삽입 영상의 위치를 선정하여 삽입하는 방식이다. n개의 그룹으로 나눌 때는 각각의 그룹에 그룹 번호를 지정한다. BIBD 매트릭스를 n개의 그룹으로 분할하여 삽입할 경우 BIBD 생성 파라미터와 연관 지어 보면 하나의 BIBD 매트릭스를 이용한 BIBD AND-ACC는 총 b명에게 코드를 할당할 수 있으나 제안된 방식을 사용하면 $b \times n$명에게 코드를 할당할 수 있다.

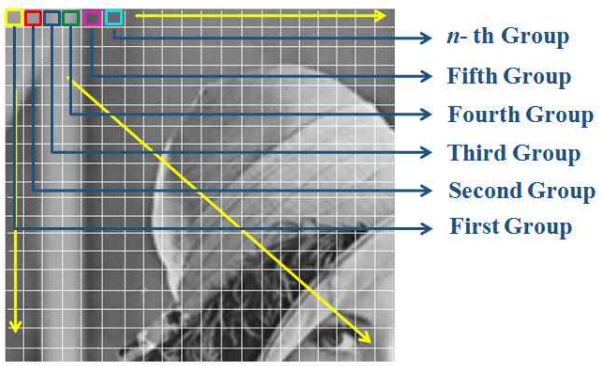

그림 1. 제안된 삽입 기법
Fig. 1. Proposed embedding technique.

(v,k,λ)-BIBD 매트릭스가 생성되고 n개의 그룹이 결정되면 그룹별로 해당하는 삽입될 이미지의 주파수 도메인상의 변환 블록을 선정한다. 그림 1은 해당 그룹별로 삽입될 DCT변환블록의 위치정보를 나타낸다.

아래 식은 BIBD AND-ACC를 다수의 구매자에게 확장 분배 하기 위해서 코드 그룹별 삽입될 위치를 나타낸다.

First Group:
(Block Position) *mod* (Group number)≡0
Second Group:
(Block Position) *mod* (Group number)≡1
Third Group:
(Block Position) *mod* (Group number)≡2
⋮
***n*-th Group**:
(Block Position) *mod* (Group number)≡n-1

각각의 해당그룹의 코드가 삽입될 전체 이미지를 DCT변환한다. DCT변환 블록의 위치는 (DCT 블록 위치 번호) *mod* (그룹 수)를 하였을 때 (삽입코드의 그룹 번호-1)과 합동인 위치에 삽입된다. 제안하는 삽입 기법은 동일한 BIBD AND-ACC를 확장하여 삽입하므로 기존보다 많은 디지털 콘텐츠 구매자에게 분배할 수 있는 장점을 가진다.

코드 삽입 시에는 Cox가 제안한 DCT 상에서의 삽입과 삽입 시에는 공격자들이 코드를 쉽게 추출 하지 못하게 암호화 키 역할의 PN sequence와 압축 및 변형 등에서도 삽입코드를 유지하기 위해 코드의 강인성을 높이기 위한 증폭계수(α)를 사용한다[8].

원본 이미지에 코드를 삽입하기 위해서는 전체 이미지를 8×8 DCT 변환 블록으로 나누고 삽입될 AND-ACC 코드 그룹별에 해당하는 DCT의 선정과 계수를 추출 한다. DCT변환 후 주파수 영역별로 해석하면 저주파수 영역(DC)인 경우 화질에 직접적인 영향을 미치는 중요한 정보는 포함하고 있고 고주파수(AC) 영역의 경우 이미지 화질에는 큰 영향을 미치지 않는 성분을 포함하며 압축 및 이미지 변형 등에 취약점을 보이고 있다. 만약 저주파수 영역에 코드를 삽입할 경우에 코드의 강인성은 높아지나 비가시성이 현저히 떨어

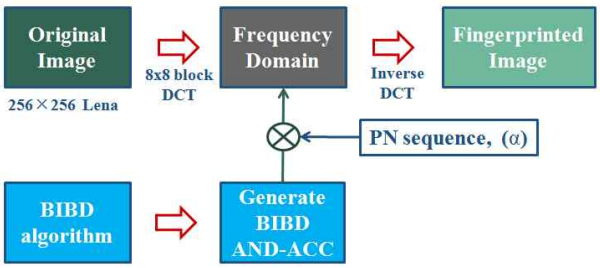

그림 2. BIBD AND-ACC 코드 삽입과정
Fig. 2. Insertion procedure of BIBD AND-ACC.

지기 때문에 화질에 큰 영향을 준다. 반면 고주파수 영역에 삽입 시 콘텐츠 복사 및 압축 등이 발생으로 인해 삽입 코드 정보를 손실될 우려가 있다. 위의 문제점을 고려하여 중간주파수 영역의 적절한 위치를 선정하여 코드를 삽입하는 것이 효과적이다[7]. 그림 2는 코드 삽입의 전반적인 과정을 나타낸다.

Ⅳ. 실험 및 분석

본 장에서는 Ⅱ장에서 제시한 BIBD 생성 이론을 바탕으로 BIBD AND-ACC를 생성하고 256×256 Lena 원본 이미지를 바탕으로 그룹별로 확장하여 코드 삽입한다. 이후 콘텐츠의 공모공격형태가 평균화 공격임을 가정하여 이미지의 공간 도메인 상에서 각각 다른 코드가 삽입된 이미지를 이용하여 평균화 공격을 시도한다. 그리고 평균화된 새로운 이미지를 수집하여 공모된 코드를 추출하고 최종적으로 공모에 가담한 유저의 코드를 추적한다.

그림 3은 (16,4,1)-BIBD AND-ACC의 생성 알고리즘을 나타낸다. v와 k를 입력받아 4가지의 조건식을 비교해 b, r이 결정된 후 Matrix Searching 과정을 통해 조

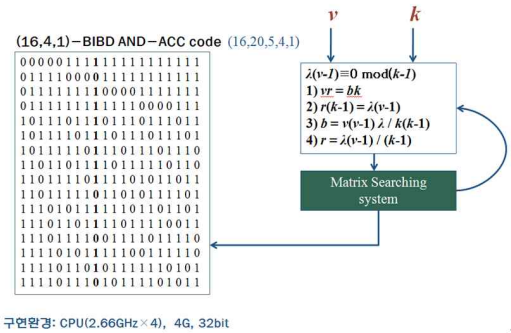

그림 3. BIBD AND-ACC 생성 과정 및 결과
Fig. 3. Generation procedure and result of BIBD AND-ACC.

표 1. 시뮬레이션 구현 환경
Table 1. Implementation environment for simulation.

구현환경	
CPU	Intel(R) Core Quad 2.66GHz×4
RAM	4G
Software	Microsoft Visual Studio 2008
Language	C++

그림 4. 구현된 (16,4,1)-BIBD 매트릭스
Fig. 4. Implemented (16,4,1)-BIBD matrix.

건에 부합하는 BIBD 매트릭스를 생성한다.

시뮬레이션을 하기 위한 구현환경은 표 1과 같다.

(16,4,1)-BIBD의 경우 코드 길이가 16bits이고 20명에게 분배할 수 있고 3명의 공모자까지 추출 가능한 코드 형태이다.

그림 4는 생성된 BIBD 매트릭스의 정보를 나타낸다. 생성시간은 0.253초가 소요되었지만 4명까지 공모자를 추출 가능한 (25,5,1)-BIBD의 경우 8:38초의 시간이 소요되었다. 하지만 코드 길이가 31인 (31,3,1)-BIBD 경우 4:27:18초의 BIBD 매트릭스 생성시간이 소요되었다.

코드 생성 후 Lena 256×256 원본 이미지를 이용하여 코드를 삽입한다. 그림 5-(a)는 원본 이미지를 나타내고, 그림 5-(b)는 제안된 삽입 기법을 사용하여 16bits의

(a)Lena 원본이미지 (b)핑거프린팅 이미지

그림 5. 원본과 핑거프린팅 이미지 비교
Fig. 5. Comparison between original image and fingerprinted image.

표 2. 증폭 계수에 따른 PSNR 측정
Table 2. Measurement of PSNR about amplification factor.

Block	α	PSNR
Proposed technique	3	48.127192dB
	1	50.837729dB

BIBD AND-ACC가 삽입된 이미지를 나타낸다.

본 실험에서는 제안된 삽입 기법을 바탕으로 동일한 (16,4,1)-BIBD AND-ACC를 6개의 그룹으로 확장하여 삽입하였다. Lena 256×256 이미지를 DCT 변환을 하면 총 1024개의 블록으로 나눠지고 코드 그룹별로 지정된 위치에 삽입된다. 하나의 그룹에 해당하는 코드는 전체의 DCT 블록 총 170개의 블록위치 및 영상 전체에 삽입된다. 기존의 20명에게 분배 가능한 (16,4,1)-BIBD AND-ACC의 경우 제안된 삽입 기법을 사용하면 총 120명에게 분배가 가능해 진다.

표 2는 핑거프린팅 코드의 강인성을 나타내는 증폭계수(α)를 달리 하였을 때의 원본 이미지와 핑거프린팅 된 이미지의 PSNR을 확인하였다. 위의 삽입방식 모두 PSNR이 40dB 이상으로 주관적인 화질의 저하는 시각적으로 인지할 수 없었으나 증폭계수(α)값이 5이상일 경우에는 시각적으로도 화질의 차이를 느낄 수가 있고 PSNR 값 역시 현저히 떨어짐을 확인하였다.

또한 공모공격 실험에서는 공모공격형태가 평균화 공격이라 가정하고 다수의 이미지를 이용하여 새로운 이미지를 생성한다. 서로 다른 코드가 삽입된 이미지를 공간 도메인 영역에서 픽셀의 값을 이용하여 서로 평균화하여 새로운 이미지를 생성하고 생성된 이미지를 이용하여 공모에 가담한 유저의 코드를 추출하였다.

검출 방식은 원본 이미지와의 비교를 통해 계수 값을 추출한다. 동일한 그룹에 소속된 코드가 평균화 공격에

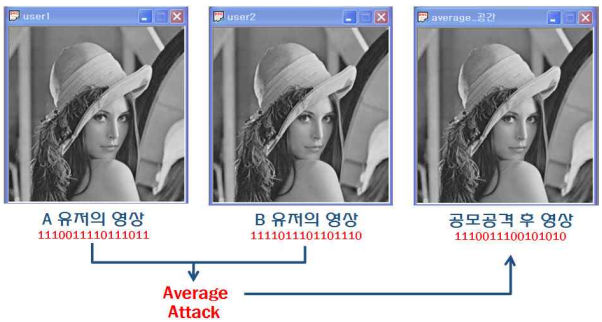

그림 6. 공간 도메인 상에서의 평균화 공격
Fig. 6. Average attack in spatial domain.

그림 7. 공모된 이미지의 코드 추출
Fig. 7. Detection of code in colluded image.

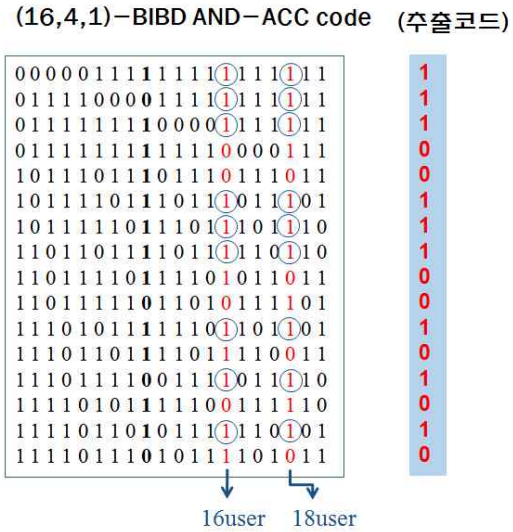

그림 8. 추출 코드를 이용한 공모자 추적
Fig. 8. Trace of colluder using the detection code.

가담하면 동일한 그룹이 지정하는 DCT 블록 위치에서 공모된 코드가 추출 되고 서로 다른 그룹의 코드가 평균화 공격에 가담하면 서로 다른 그룹이 지정된 DCT 블록에서 코드를 추출할 수 있다. 이후 추출된 코드를 BIBD이론을 기반으로 공모자가 k명 공모하였을 때 k-1명까지의 공모자가 추출 가능함을 확인하였다.

그림 6은 동일한 그룹의 서로 다른 코드가 삽입된 A 유저와 B유저가 공모공격 후 새로운 공모된 이미지를 생성한 과정이다. 만약 공모자의 이미지의 코드를 모른다고 가정하였을 때 공모된 이미지를 이용하여 코드를 추출한다. 추출 코드는 그림 7과 같다.

또한 코드 추출시 적절한 임계치(threshold)를 설정하고 추출된 코드를 이용하여 최종적으로 공모자를 추적하면 그림 8과 같다. 공모자 확인은 추출 코드의 1이 나타난 계수별 위치를 파악하여 해당그룹의 16번 유저와 18번 유저가 평균화 공격에 가담했음을 확인할 수 있다.

V. 결 론

BIBD이론은 여러 분야에서 널리 응용되고 있고 특히 코드의 특성 때문에 디지털 콘텐츠 저작권보호를 위한 디지털 핑거프린팅 기술에 많이 적용되고 있다. 하지만 코드 생성 시 생성 파라미터와 조건식을 만족해야 하기 때문에 다수의 콘텐츠 구매자에게 할당될 BIBD AND-ACC를 생성할 경우 무수히 많은 반복 과정과 연산의 복잡도가 높아진다. 본 논문에서는 다수의 사용자를 위한 코드 생성의 어려움을 보완하기 위해 BIBD AND-ACC의 삽입시 이미지의 삽입 위치를 고려한 삽입 기법을 제안하였다. 실험을 통해 BIBD AND-ACC를 생성한 후 제안된 삽입 기법을 사용하면 하나의 BIBD AND-ACC를 사용하였을 때 보다 더 많은 유저에게 코드를 할당 가능함을 확인 하였다. 또한 코드가 삽입된 다수의 이미지를 바탕으로 공모공격 실험을 하였을 때 k-1명까지의 공모자가 검출됨을 확인 하였다. 향후 평균화 공격 이외의 공격에도 방어 가능한 기법의 연구가 이루어져야 한다.

참 고 문 헌

[1] S. Oliverira, M .A .Nascimento and O. R. Zaiane, “Digital Watermarking: its status, limitations and prospects.”, Technical Report, Jan. 2002

[2] D. Boneh and J. Shaw, “Collusion-Secure Fingerprinting for Digital Data,” IEEE Trans. Inf. Theory, Vol. 44, No. 5, pp. 1897-1905, Sep. 1998.

[3] J. Dittmann, “Combining Digital Watermarks and Collusion Secure Fingerprints for Customer Copy Monitoring,” Proc. IEEE Seminar Sec. Image & Image Auth., pp. 128-132, Mar. 2000.

[4] J. Domingo-Ferrer and J. Herrera-Joancomarti, “Simple Collusion-secure Fingerprinting Shemes for Images,” in IEEE International Conference on Information Technology: Coding and Computing, ITCC’2000, pp. 128-132, 2002.

[5] W. Trappe, M. Wu, Z. Jane Wang, and K.J.R. Liu, “Anti-Collusion Fingerprinting for Multimedia,” IEEE Trans., on Signal Processing, Vol. 51 No. 4, pp. 1069-1087, Apr. 2003.

[6] C. J. Colbourn and J. H. Dinitz, The CRC *Handbook of Combinatorial Designs*, CRC Press, Roca Raton, FL, 1996.

[7] 이강현, “BIBD 기반의 멀티미디어 핑거프린팅 코드의 공모코드들에 대한 공모자추적,”, 전자공학회 논문지, 제 46권, 제6호, 79-85쪽, 2009년 11월

[8] J. Cox, J. Kilian, F.Leighton, and T. Shamoon, “Secure Spread Spectrum Watermarking for Multimedia,” IEEE Trans. Image Process., Vol. 6, No. 12, pp. 1673-1687, Dec. 1997.

저 자 소 개

사 공 명(학생회원)

2008년 동국대학교 정보통신공학과 학사

2010년～현재 경북대학교 전자전기컴퓨터학부 석사과정

<주관심분야 : 컨텐츠보호, 무선통신, 네트워크보안>

박 요 한(정회원)

2006년 경북대학교 전자전기컴퓨터학부 학사

2008년 경북대학교 전자공학과 석사

2008년～현재 경북대학교 전자공학부 박사과정

<주관심분야 : 무선통신, 네트워크 보안, 모바일 컴퓨팅>

박 영 호(정회원)-교신저자

1989년 경북대학교 전자공학과 학사

1991년 경북대학교 전자공학과 석사

1995년 경북대학교 전자공학과 박사

1996년～2008년 상주대학교 전자전기공학부 교수

2003년～2004년 Oregon State University 방문 교수

2008년～현재 경북대학교 산업전자전기공학부 교수

<주관심분야 : 무선통신, 네트워크 보안, 모바일 컴퓨팅>

문 상 재(평생회원)

1972년 서울대학교 공업교육(전자전공)과 공학사

1974년 서울대학교 전자공학과 공학석사

1984년 미국 UCLA 전기공학과 공학박사

1984년～1985년 미국 OMNET 회사 컨설턴트

1984년～1985년 미국 UCLA 포스트닥터

2001년～2002년 한국정보보호학회회장

1974년～현재 경북대학교 전자공학부 교수

<주관심분야 : 무선통신, 네트워크 보안, 암호학>