논문 2011-48CI-4-4

포렌식 마킹을 위한 특징점 기반의 동적 멀티미디어 핑거프린팅 코드 설계

(A Design on the Multimedia Fingerprinting code based on Feature Point for Forensic Marking)

이 강 현*

(Kang Hyeon RHEE)

요 약

본 논문에서는 멀티미디어 콘텐츠 보호에 대한 반공모 코드를 위한 동적 멀티미디어 핑거프린팅 코드를 설계하는 알고리즘을 제안한다. 기존의 반공모 코드(ACC: Anti-Collusion Code)를 위한 멀티미디어 핑거프린팅 코드는 BIBD(Balanced Incomplete Block Design)의 접속행렬을 보수행렬로 변환하여 k를 k+1로 증대시키는 수리적 방법으로 설계되었다. 그리고 보수행렬의 코드벡터를 사용자에게 핑거프린팅 코드로 부여하고, 콘텐츠에 삽입하였다. 제안된 알고리즘에서는 사용자가 구매하는 콘텐츠로부터 특징점을 추출하고, 이를 기반으로 동적으로 핑거프린팅 코드를 설계할 수 있도록 BIBD의 v와 k+1 조건을 만족하는 반공모 코드의 후보성 코드를 코드북(Codebook)에 구축하고 λ+1 조건을 만족하는 행렬(이하, Rhee행렬이라 함.)을 생성한다. 실험을 통하여 콘텐츠의 특징점 기반으로 생성된 Rhee행렬의 코드벡터는 v비트의 유의수준 (1-α)에서 신뢰구간에 k가 존재하며, Rhee행렬의 각 행과 행, 열과 열 사이의 유클리디안 거리가 BIBD 기반의 보수행렬과 그래프 기반의 보수행렬과 같은 k값이 산출되었다. 더욱이 Rhee행렬의 첫 행과 첫 열은 생성과정에서 초기 점화벡터로 콘텐츠 포렌식 마크 정보가 되며, 이와 관계가 있는 나머지 코드벡터들과의 관계성이 코드북에 기록되어 있기 때문에, 공모된 코드를 추적할 때 원 핑거프린팅 코드의 상관관계 계수를 구할 필요 없이 코드북의 탐색으로 공모자를 추적이 용이하다. 따라서 본 논문에서 생성된 Rhee행렬은 수리적으로 생성된 BIBD 기반의 행렬보다 ACC로서 강인성과 충실도가 우수하다.

Abstract

In this paper, it was presented a design on the dynamic multimedia fingerprinting code for anti-collusion code(ACC) in the protection of multimedia content. Multimedia fingerprinting code for the conventional ACC, is designed with a mathematical method to increase k to k+1 by transform from BIBD's an incidence matrix to a complement matrix. A codevector of the complement matrix is allowanced fingerprinting code to a user' authority and embedded into a content.

In the proposed algorithm, the feature points were drawing from a content which user bought, with based on these to design the dynamical multimedia fingerprinting code. The candidate codes of ACC which satisfied BIBD's v and k+1 condition is registered in the codebook, and then a matrix is generated(Below that it calls "Rhee matrix") with λ+1 condition. In the experimental results, the codevector of Rhee matrix based on a feature point of the content is generated to exist k in the confidence interval at the significance level (1-α). Euclidean distances between row and row and column and column each other of Rhee matrix is working out same k value as like the compliment matrices based on BIBD and Graph. Moreover, first row and column of Rhee matrix are an initial firing vector and to be a forensic mark of content protection. Because of the connection of the rest codevectors is reported in the codebook, when trace a colluded code, it isn't necessity to solve a correlation coefficient between original fingerprinting code and the colluded code but only search the codebook then a trace of the colluder is easy. Thus, the generated Rhee matrix in this paper has an excellent robustness and fidelity more than the mathematically generated matrix based on BIBD as ACC.

Keywords : Multimedia fingerprinting, BIBD(Balanced Incomplete Block Design) ACC(Anti-Collusion Code), Multimedia forensic

* 평생회원-교신저자, 조선대학교 전자정보공과대학 전자공학과
Dept. of Electronics Eng., Chosun University, Gwangju, Korea 501-759
※ 본 논문은 한국연구재단의 일반연구자지원사업 2010-0023580으로 수행되었습니다.
접수일자: 2011년5월9일, 수정완료일: 2011년7월6일

Ⅰ. 서 론

인터넷의 발전과 구축에 따라서, 멀티미디어 콘텐츠의 보급과 확산이 커지면서 이에 따른 불법복사와 재배포도 심각하게 이루어지고 있다.

미디어 콘텐츠를 보호하는 방법으로 워터마킹(Watermarking) 기법이 사용되고 있으나, 워터마킹 신호는 콘텐츠의 저작자에 대한 정보를 가지고 있을 뿐, 불법복제와 재배포를 시도한 공모자(Colluder)를 검출하고 추적할 수는 없다[1].

이를 해결하기 위해서 콘텐츠를 구입할 때, 멀티미디어 핑거프린팅 코드(Fingerprinting code)를 삽입하여, 구매하는 사용자의 인식정보로 사용한다. 이러한 핑거프린팅기술은 원 저작자의 지적재산 권리의 보호와 디지털 창작물의 불법복제 및 배포에 대한 방지책으로, 콘텐츠에 사용자 정보를 삽입하고, 사용자들이 공모하여 다른 복제를 만드는 공모공격이 발생되었을 때, 공모공격자들을 추적하여 검출할 수 있는 콘텐츠 보호기술이다[2].

콘텐츠에 삽입된 핑거프린팅 코드의 검출은 사용자 각자가 구입한 콘텐츠를 서로 비교해 보았을 때, 코드가 삽입되지 않은 영역은 순수한 콘텐츠의 동일한 정보를 보여주지만, 코드가 삽입된 영역은 사용자 각자의 콘텐츠 정보가 상이하므로 이 영역이 사용자의 핑거프린팅 코드가 삽입된 것으로 쉽게 검출할 수 있다. 즉 사용자가 서로 동의한 가운데 자신들이 소유한 콘텐츠를 서로 비교해 본다.

사용자 몇 명이 함께 공모하여 각자의 미디어 콘텐츠에서 추출된 핑거프린팅 코드를 여러 가지 방법으로 조합하여 공모공격에 사용할 것이며, 공모된 코드를 미디어 콘텐츠에 재 삽입하여 불법복사와 재배포를 하게 된다. 이렇게 만들어진 공모코드는 사용자들 누구누구에 의해서 공모되었는지 추적이 어렵다. 그래서 반공모 코드(ACC: Anti-Collusion Code)의 설계가 필요하다. 이에 따라 BIBD(Balanced Incomplete Block Design)의 접속행렬(Incidence matrix) M에 대한 보수행렬(Complement matrix) C의 행벡터를 멀티미디어 핑거프린팅 코드로 사용하는 연구가 활발히 진행되었다[3]. 여러 연구를 통하여 BIBD를 생성하는 5가지 파라미터 (v, b, r, k, λ)에서, k명까지 공모자를 검출할 수 있다.[3, 12] BIBD 기반의 코드는 길이가 짧아서 실제로 핑거프린팅에 적용이 가능하다.

ACC 생성에 대한 초기 연구는 logarithm 표로부터 *C-Secure Codes*를 생성[4]하였다. 근래의 연구로는 [3]에서는 BIBD를 이용하여 n명의 사용자에 대해서 k-내성 AND_ACC를 구성하였고, [5]에서는 가우스분포 난수를 이용한 스케일러블 핑거프린팅이 제안되었다. 또한 완전한 핑거프린팅은 가능한가? [4]에서 또한 “Marking Assumption”을 다루었다. 그러나 핑거프린팅 코드의 bit 확장과 콘텐츠 사용자에게 할당하는 코드 수의 제한이 있으며, 핑거프린팅의 강인성(Robustness)과 충실도(Fidelity)도 큰 문제로 되어 있다.

본 논문에서는 BIBD의 특성에 만족하는 멀티미디어 콘텐츠에 사용할 ACC를 콘텐츠 보호의 포렌식 마킹을 위하여, 영상에서 특징점(Feature point)을 추출하고 이를 기반으로 동적으로 생성되는 멀티미디어 핑거프린팅 코드를 설계한다. 제안된 알고리즘은 영상의 압축과 배포, 전송을 하기 위하여 DCT(Discrete Cosine Transform) 처리과정에서, 영상의 주파수 영역(Frequency domain)에 대한 cosine 계수의 고역주파수 대역에서 자체 특징점을 추출하여 ACC의 후보성 코드북(Codebook)을 구축하고, 이 중에서 하나의 점화벡터를 선택하여, ACC를 위한 (v, k, λ) BIBD의 접속행렬에 대한 보수행렬 특성을 갖는 새로운 코드벡터의 행렬(이하 Rhee행렬이라 함)을 생성한다. 이는 (v, k, λ) BIBD의 조건이 (v, k+1, λ+1) Rhee 행렬로 직접 생성되며 행벡터가 사용자의 멀티미디어 핑거프린팅 코드로 사용된다.

제 Ⅱ장에서는 본 논문에 사용된 이론적 배경을 설명하고, 제 Ⅲ장에서는 동적 멀티미디어 핑거프린팅 코드 설계를 위한 Rhee행렬 생성의 제안된 알고리즘을 구현하고, 제 Ⅳ장에서는 기존의 BIBD 기반의 수리적으로 생성된 핑거프린팅 코드와 Rhee행렬 기반으로 생성된 핑거프린팅 코드의 실험적 비교분석을 통하여 제 Ⅴ장에서 결론을 맺는다.

Ⅱ. BIBD와 ACC의 이론적 배경

1. BIBD의 접속행렬

블록설계는 각 처리가 블록에 똑같은 비율로 나타나게 하는 관능검사 실험계획으로, 한 블록 안에서 처리수가 많아 모든 처리군을 포함할 수 없을 때 사용하는 방법이다. 이를 위한 조합문제는 행렬모델을 사용하여 제약조건을 만족하는 행렬로 생성할 수 있다. [6~7]에서 BIBD를 포함하여 많은 변분들(Variations)이 연구되

었다.

BIBD 설계[8~10]는 5개의 파라미터 (***v, b, r, k, λ***)로 생성되는데,

v: 처리의 개수(Number of treatments)

b: 블록의 개수(Number of blocks)

r: 각 *v*의 반복 수(Number of times each treatment is run, k<v)

k: 하나의 블록에 포함된 *v*의 개수(Number of treatments per block)

λ: 각 처리 쌍이 나타나는 블록의 개수 (Number of blocks that processing pair appears)

이다.

5개의 파라미터는 식 (1)부터 (4)까지의 한정조건을 만족한다.

$$vr = bk \tag{1}$$

$$r(k-1) = \lambda(v-1) \tag{2}$$

$$b = \frac{v(v-1)\lambda}{k(k-1)} \tag{3}$$

$$r = \frac{\lambda(v-1)}{k-1} \tag{4}$$

식 (1)에서 ***b***=***v*** or ***r***=***k*** 이면 BIBD는 대칭성이며 ***v***×***b***의 크기를 갖는 BIBD의 접속행렬 ***M***은 식 (5)에 의해 행렬 요소 m_{ij}의 값이 결정된다.

$$M = [m_{ij}]$$
$$m_{ij} = \begin{cases} 1 & \text{if } (x_i \in A_j) \text{ or } (j_{th}blocks \in i_{th}blocks) \\ 0 & otherwise. \end{cases} \tag{5}$$

$$\begin{bmatrix} 0101010 \\ 1001100 \\ 0011001 \\ 1110000 \\ 0100101 \\ 1000011 \\ 0010110 \end{bmatrix} \qquad \begin{bmatrix} 1110000 \\ 1001100 \\ 1000011 \\ 0101010 \\ 0100101 \\ 0011001 \\ 0010110 \end{bmatrix}$$

(a) (b)

(a) Hadamard 기반의 BIBD의 접속행렬
(a) Incidence matrix of BIBD base on Hadamard.
(b) Graph 기반의 BIBD의 접속행렬
(b) Incidence matrix of BIBD base on Graph.

그림 1. 접속행렬의 예
Fig. 1. Examples of Incidence matrix.

그러므로 ***M***은 식 (6)을 만족하게 된다[11].

$$MM^t = (r-\lambda)I + \lambda J \tag{6}$$

여기서 *I: the v× v identity matrix*

J: the v× v matrix of all 1's

이다.

그림 1은 (7,3,1) BIBD의 접속행렬로 (a) Hadamard 기반과 (b) Graph 기반이 수리적으로 생성된 예를 보여준다.

2. 반공모 코드

BIBD의 접속행렬(Incidence matrix)은 행렬의 대칭성을 부분적으로 분해할 수 있다. 그러므로 ACC의 제약조건을 만족할 수 있으며, 공모공격에 강인성을 갖는 특성을 만족한다[1~3].

그림 2에서 BIBD의 접속행렬 ***M***의 보수행렬 ***C***의 행벡터는 사용자의 핑거프린팅 코드로 사용하며, ***v***명 사용자의 각자에게 핑거프린팅 코드가 부여되는데, 이들 중 몇몇 사용자들이 자신의 핑거프린팅 코드를 가지고 공모코드를 생성하게 된다. 그리고 생성된 공모코드는 콘텐츠에 재삽입하여 불법배포가 된다. 이때, 불법 콘텐츠로부터 검출한 공모코드를 분석하면, 공모에 사용된 핑거프린팅 코드를 찾아 낼 수 있고, 공모자를 추적할 수 있다. 공모자 추적은 ***k***명까지 할 수 있기 때문에 BIBD가 멀티미디어 핑거프린팅 코드 생성에 응용이 된다[12].

공모코드를 생성하는 방법은 평균화 공모공격, 최대-최소공격, 상관계수 제로화공격, 상관계수 음수화공격, 모자이크공격 등이 있다[13]. 이 중에서 가장 용이한 공모공격은 그림 3과 같이 사용자가 구입한 콘텐츠를 서

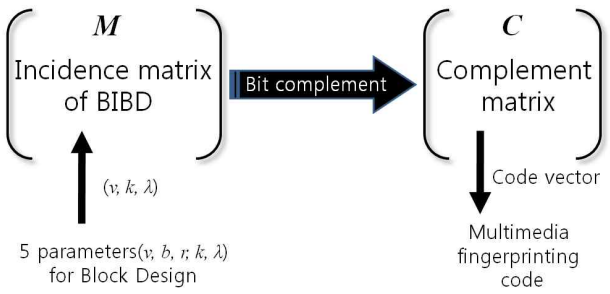

그림 2. 블록설계로부터 멀티미디어 핑거프린팅 코드의 생성과정
Fig. 2. Generation progress of multimedia fingerprinting code from a block design.

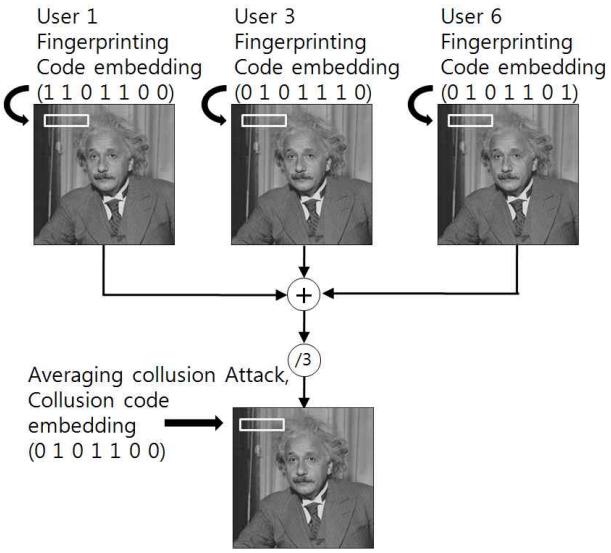

그림 3. 평균화 공모공격
Fig. 3. Averaging collusion attack.

로 더하여 평균을 하면 공모코드가 삽입된 불법 콘텐츠가 바로 이루어진다. 이 불법 콘텐츠는 인터넷 상에서 쉽게 배포가 이루어진다.

Ⅲ. Rhee행렬 생성의 제안 알고리즘

여기에 본 연구에서 구현하는 콘텐츠 보호의 포렌식 마킹을 위한 특징점 기반(Feature point based)의 동적 멀티미디어 핑거프린팅 코드를 설계하기 위하여 그림 4와 같이 Rhee행렬의 생성 알고리즘을 구현한다.

十Rhee행렬의 생성 알고리즘十

Step 1: BIBD의 v와 k값을 정하고, v값의 범위 내에서 영상의 분할되는 블록 사이즈 $n \times n$을 $v \leq n$(n은 2의 멱수배)으로 정한다.

Step 2: 임의의 위치에서 선택된 $n \times n$ 크기의 분할된 영상을 2D DCT 처리를 한다.

Step 3: DCT의 cosine 계수를 zigzag으로 정렬하여 고주파 대역을 $n^2/(n/2)$개 선택하고, 그 cosine 계수에 추가신호 w를 더한다

Step 4: 2D IDCT 처리를 하여 복원영상을 구한다.

Step 5: ACC의 후보성 코드북을 만들기 위하여,

i) 원영상과 복원영상의 차영상을 구해서, 차영상의 픽셀값이 1 이상이면 비트 '1'($GF(2)$)을 할당.

ii) 차 값이 0이면 비트'0'($GF(2)$)을 할당.

iii) 차영상의 각 행과 열에 대하여 $v$bits 중에서 k개의 '1'이 존재하는 코드벡터를 선택하고, 이 조건을 만족시킨 영상블록의 행 또는 열의 시작좌표 i_x, i_y를 ACC 후보성 코드북에 등록한다. 그리고 **Step 6**을 실행.

iv) iii)의 조건이 없으면 Step 2부터 다시 실행.

Step 6: ACC 후보성 코드북 중에서 점화벡터를 임의로 선택하여 Rhee행렬의 첫행과 첫열에 할당한다. 이 점화벡터의 좌표(**Step 5** (iii))가 콘텐츠 포렌식 마크가 된다.

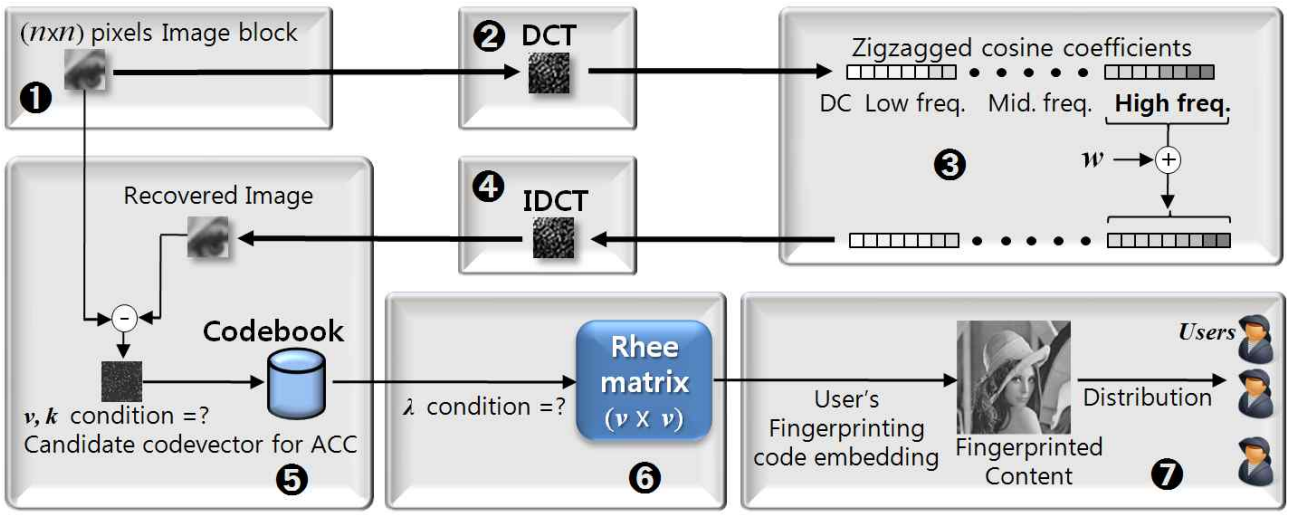

그림 4. 영상의 특징점을 이용한 동적 멀티미디어 핑거프린팅 코드 설계를 위하여 제안된 Rhee행렬의 생성 알고리즘
Fig. 4. The proposed Rhee matrix generation algorithm for dynamic multimedia fingerprinting code design using an image feature point.

i) ACC 후보성 코드 중에서 점화벡터와의 관계가 λ가 되는 코드벡터를 선택하여 Rhee행렬의 다음 행과 열에 할당을 $v \times v$의 크기 까지 반복하고 Step 7을 실행.

ii) ACC 후보성 코드북 전체를 참조하여 $v \times v$의 크기까지 Rhee행렬을 생성하지 못하면 Step 2 부터 다시 실행. .

Step 7: 생성된 Rhee행렬의 각 행벡터는 콘텐츠 사용자에게 부여하는 멀티미디어 핑거프린팅 코드로서 콘텐츠에 삽입하여 구매자들에게 배포한다.

Ⅳ. 시뮬레이션 및 평가

제안된 알고리즘의 실행을 위하여 테스트 영상은 Lena(256×256)를 사용하였다. 표 1에서 BIBD의 접속행렬이 보수행렬로 변환될 때, 동일 v 값에서 접속행렬의 k 값이 보수행렬에서 커질 때만이 의미가 있다. 이 영역이 음영부분이다.

표 1. 접속행렬의 보수행렬 변환에 따른 (v, k, λ)의 값

Table 1. (v, k, λ) values according to transform from the incidence matrix to the complement matrix.

	Incidence Matrix		Complement Matrix	
v	k	λ	k	λ
7	3	1	4	2
	4	2	3	1
11	5	2	6	3
	6	3	5	2
15	7	3	8	4
	8	4	7	3
19	9	4	10	5
	10	5	9	4
23	11	5	12	6
	12	6	11	5
27	13	6	14	7
	14	7	13	6
31	10	3	21	14
	15	7	16	8
	16	8	15	7
	21	14	10	3
	25	20	6	1

표 2. Rhee행렬의 (v, k, λ) 값의 선택

Table 2. Selection of (v, k, λ) values of Rhee matrix.

v	k	λ	n	w
7	4	2	8	0.5
11	6	3	16	0.5
15	8	4	16	0.5
19	10	5	32	0.5
23	12	6	32	0.5
27	14	7	32	0.5
31	16	8	32	0.5

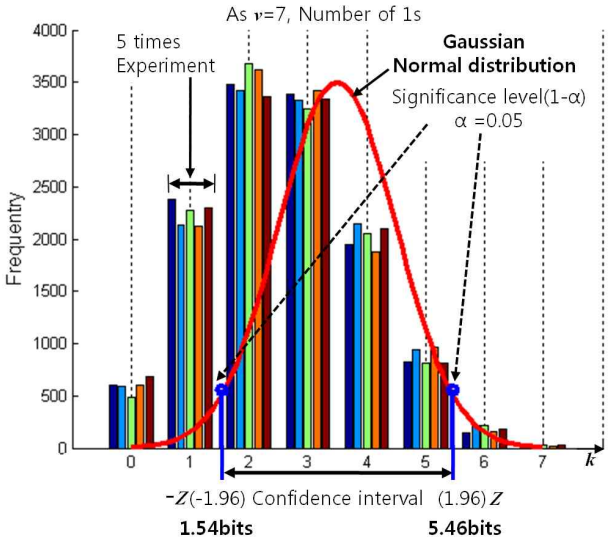

그림 5. Rhee행렬의 k 할당을 위한 신뢰구간 추정

Fig. 5. Estimation of the confidence interval for k assignment of Rhee matrix.

이를 고려하여 Rhee행렬 생성은 (v, k, λ) 값을 표 2와 같이 하고, 각 v값에서 $v$bits 내에 '1'의 개수 분포를 통하여 Rhee행렬 생성에 필요한 v와 k의 정당성 확인이 필요하다.

그림 5는 v=7에서 7bits 내에 '1'의 개수 분포를 구하기 위하여, '1'의 발생 빈도수를 10,000번에 걸쳐 5회 실행으로 구하고, 이를 가우시안 정규분포와 비교하였다.

그림 5에서 유의영역(Significant level) $(1-a)$는 a =0.05에서 기각영역 $Za/2$=1.96과 $-Za/2$=-1.96을 제외한 신뢰구간(Confidence interval)에서 k의 범위를 1.54bits와 5.46bits를 얻었다. 이 범위에서 표 2의 k는 v의 정당성을 갖는다.

표 3은 코드북의 포맷의 일부를 보여준다. 코드북에서 순번은 #이며, v와 k의 조건에 맞는 ACC 후보성 코드와 이에 대한 특징점의 영상좌표 i_x, i_y 그리고 이에 대응되는 2D DCT 처리후의 F_u, F_v 주파수좌표의 코사인 계수

표 3. 코드북 포맷의 일부
Table 3. A part of the codebook format.

No.	v	Candidate code	k	i_x	i_y	PSNR
463	7	1 0 0 1 1 1 0	4	86	18	70.87781
465	7	1 0 0 1 1 1 0	4	86	19	70.87781
466	7	1 0 0 1 1 1 0	4	86	20	70.87781
467	7	1 1 1 0 1 0 0	4	64	16	70.62958
468	7	1 1 1 0 1 0 0	4	64	17	70.62958
469	7	1 1 1 0 1 0 0	4	65	28	70.62958

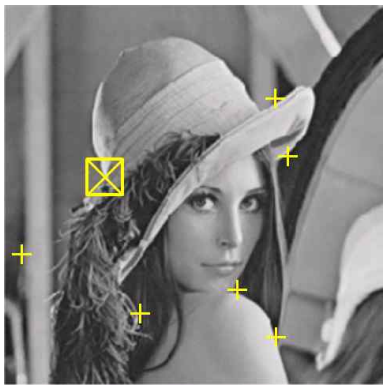

그림 6. 제안된 알고리즘에 의한 영상의 특징점 추출 (v=7)
Fig. 6. Detection of image' feature points by the proposed algorithm (v=7).

값에 w=0.5 신호를 더하였다. 2D IDCT를 처리하여 복원된 영상과 원영상과의 PSNR 값을 구하였다. 코드북 전체를 통하여 PSNR의 범위는≒69dB~71dB 범위를 유지하였다.

그림 6에서, Rhee행렬 생성에 사용된 초기 점화벡터의 특징점은 영상에 ⊠으로 콘텐츠 포렌식 마크가 되며, 이 점화벡터와의 λ 관계성을 갖는 나머지 행벡터의 특징점은 +로 각각 표시되어 있다.

각 사용자를 위하여 특징점(영상좌표 i_x, i_y)에 의한 코드벡터는 멀티미디어 핑거프린팅 코드로 부여되고, 콘텐츠에 삽입하여 7개의 핑거프린팅 된 영상과 원 영상과의 PSNR은 표 4와 같다.

그리고 그림 6의 ⊠의 특징점은 이 코드벡터의 군을 대표하는 점화벡터이기 때문에 콘텐츠 포렌식 마킹으로 이용하여 공모코드의 분석에 적용한다. 각 사용자의 핑거프린팅 코드는 서로의 λ 관계가 ACC 후보성 코드북에 모두 기록되어 있다.

그림 1의 (a), (b)와 [3]의 보수행렬 (c) 그리고 본 논문에서 생성된 Rhee행렬 (d)는 그림 7과 같다. (a), (b),

표 4. Rhee행렬의 코드벡터 특성
Table 4. Characteristics of Rhee matrix's codevector. (Image size: 256×256, v=7, k=4, λ=2)

User No.	Fingerprinting code	Feature point		PSNR
		i_x	i_y	
1	1 1 0 0 1 0 1	68	116	90.2750
2	1 1 1 1 0 0 0	184	62	90.2750
3	0 1 0 1 1 1 0	191	101	90.2750
4	0 1 1 0 0 1 1	12	168	90.2750
5	1 0 1 0 1 1 0	158	193	90.2750
6	0 0 1 1 1 0 1	91	208	90.2750
7	1 0 0 1 0 1 1	179	220	90.2750

$$\begin{bmatrix}1010101\\0110011\\1100110\\0001111\\1011010\\0111100\\1101001\end{bmatrix}\quad\begin{bmatrix}0001111\\0110011\\0111100\\1010101\\1011010\\1100110\\1101001\end{bmatrix}$$

(a) (b)

$$\begin{bmatrix}0001111\\0110011\\1010101\\0111100\\1100110\\1011010\\1101001\end{bmatrix}\quad\begin{bmatrix}1100101\\1111000\\0101110\\0110011\\1010110\\0011101\\1001011\end{bmatrix}$$

(c) (d)

(a) 그림 1 (a)의 보수행렬
(b) 그림 1 (b)의 보수행렬
(c) [3]의 보수행렬
(d) 본 논문의 Rhee행렬
(a) Complement matrix of Fig. 1 (a).
(b) Complement matrix of Fig. 1 (b).
(c) Complement matrix of [33].
(d) Rhee matrix in this paper.

그림 7. 그림 1의 (a), (b), (c)의 보수행렬과 본 논문의 Rhee행렬 (d)
Fig. 7. Complement matrix of Fig. 1 (a), (b) and (c), and Rhee matrix (d) in this paper.

(c) 각각의 보수행렬 C와 Rhee행렬 (d)는 BIBD 특성으로 행벡터 코드의 1의 개수 4개와 모든 벡터코드들 간에 1의 요소가 2번 반복되는 2-resiliency를 만족한다. 그리고 (a), (b), (c)와 Rhee행렬 (d)의 각 행렬에서 모

표 5. 그림 7의 각 행렬 (a), (b), (c)와 Rhee행렬 (d)의 행과 행, 열과 열의 유클리디안 거리

Table 5. Euclidean distances between row and row, and column and column each other on the matrices (a), (b) and (c), andRhee matrix (d) in Fig. 7. (v=7, k=4,)

Euclidean distances	Between row and row each other.	Between column and column each other.
Fig. 7 (a)	4	4
Fig. 7 (b)	4	4
Fig. 7 (c)	4	4
Rhee matrix in Fig. 7(d)	4	4

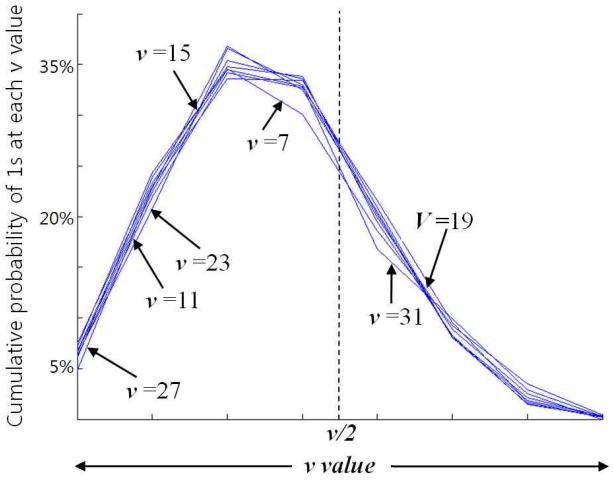

그림 8. v값에 따른 1의 개수의 누적확률

Fig. 8. Cumulative probability of the number of 1s by v values.

든 벡터들 간의 유클리디안 거리는 식 (7)에 의해 산출된 값이 표 5와 같이 all 4이며 BIBD의 k를 또한 만족한다.

$$Euclidean\ distance = \sqrt{\sum_{i=0}^{l-1}(a_i - b_i)^2} \qquad (7)$$

그림 7에서, 본 논문에서 생성한 Rhee행렬의 각 코드벡터간의 유클리디안 거리가 기존의 ACC로 사용된 BIBD 기반 행렬의 각 코드벡터간의 유클리디안 거리가 동일하므로 Rhee행렬은 ACC 특성을 만족하며, 사용자의 핑거프린팅 코드가 될 수 있다.

본 논문의 실험을 확장하고자 v값 7, 11, 15, 19, 23, 27, 31에 따른 각 값에서 k값을 실행한 결과는 그림 8과 같고, 전 영역에서 그림 5와 같은 동일한 누적확률의 특성을 가지고 있다.

V. 결 론

본 연구에서는 멀티미디어 핑거프린팅에 사용되는 BIBD의 접속행렬 M에 대한 보수행렬 C를 미디어 콘텐츠 자체의 특징점을 이용하여 생성시키는 알고리즘을 제안하였다.

실험을 통하여 사용자의 핑거프린팅 코드에 사용되는 Rhee행렬의 행벡터는 미디어 콘텐츠의 특징점으로부터 동적으로 직접 생성되기 때문에, 공모자들은 기존의 수리적으로 생성된 BIBD기반의 코드벡터를 공모코드로 연산하는 것 보다 Rhee행렬의 코드벡터가 공모에 용이하지 않으므로 강인성이 있다.

또한 불법 콘텐츠의 공모코드를 분석하기 위해서, BIBD 기반의 공모코드는 원 핑거프린팅과의 상관관계 계산이 필요하지만, 본 논문의 Rhee행렬 코드벡터는 생성단계의 정보가 코드북에 기록되어 있다. Rhee행렬의 점화코드벡터가 포렌식 마크용이며, 나머지 코드벡터는 점화코드벡터와의 할당되는 관계성이 코드북에 가지고 있기 때문에, 코드북에서 공모코드를 참조할 수 있는 충실도도 있다.

따라서 본 논문에서 생성되는 Rhee행렬의 코드벡터는 적용할 콘텐츠로부터 직접 동적으로 생성되는 핑거프린팅 코드로 포렌식 마킹의 특성을 가지고 있기 때문에 기존의 수리적 BIBD 기반의 코드벡터보다 공모내성이 우수하다. 그리고 포렌식 마크를 결정할 수 있으므로 “Marking Assumption”에 광범위하게 응용할 수 있다.

감사의 글

본 연구 분야의 선행연구자들이 수행해 주신 연구결과가 있었기에 본 연구를 수행할 수 있어서, 선행연구자님들께 진심으로 경의를 표합니다. 그리고 뒤의 보이지 않은 심사위원들께서 세심히 지적해 주신 사항으로 보다 논문의 완성도를 이룰 수 있어서 감사의 말씀을 드립니다.

본 연구의 알고리즘을 구현하는데 조언을 아낌없이 해주신 조선대학교 컴퓨터공학과 정일용 교수님께도 저자의 따뜻한 마음을 드립니다.

표절논문 인용주의

{“유비쿼터스 네트워크 시스템에서의 미디어 보안에

관한 연구," 한국사이버테러정보전학회, [7권 1호-04], pp. 29-34, 2007.3}과
{"A Study on Digital Media Security by Hopfield Neural Network," LNCS4493, ISNN '07 Proceedings of the 4th international symposium on Neural Networks: Advances in Neural Networks, Part III, pp.140-146}은 참고문헌 [2]의 내용전체를 표절한 논문으로 이를 인용할 시에 주의를 요합니다.
참조: http://paper.chosun.ac.kr (원저자 및 선임변호사)

참 고 문 헌

[1] K.H. Rhee, "DRM Implementation by Multimedia Fingerprint," IEEK Computer Society, Vol.46, No.3, pp.50-56, 2009. 5.
[2] 노진수, 이강현 "신경회로망에 의한 공모된 멀티미디어 핑거프린트의 검출," 대한전자공학회논문지 제43권 CI편 제4호, 80~87쪽, 2006년 7월.
[3] Trappe, W., Wu, M., Wang Z. J., Liu, K. J. R., "Anti-collusion fingerprinting for multimedia," IEEE Trans. Signal Proc. vol. 51, Apr. (2003) 1069-1087
[4] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," IEEE Tran. on Information Theory, vol. 44, pp. 1897-1905, September 1998.
[5] J.M. Seol and S.W. Kim, 'Scalable and Robust Fingerprinting Scheme Using Statistically Secure Extension of Anti-collusion Code," LNCS,Volume 3802/2005, pp.1086-1091, 2005.
[6] van Lint, J.H., and R.M. Wilson (1992), A Course in Combinatorics. Cambridge, Eng.: Cambridge University Press.
[7] S. S. Shrikhande, and Vasanti N. Bhat-Nayak, Non-isomorphic solutions of some balanced incomplete block designs I - Journal of Combinatorial Theory, 1970.
[8] http://mathworld.wolfram.com/BlockDesign.html
[9] Dinitz, J. H. and Stinson, D. R. "A Brief Introduction to Design Theory," Ch. 1 in Contemporary Design Theory: A Collection of Surveys (Ed. J. H. Dinitz and D. R. Stinson). New York: Wiley, pp.1-12, 1992.
[10] Ryser, H. J. "The (b, v, r, k, lambda) - Configuration." §8.1 in Combinatorial Mathematics. Buffalo, NY: Math. Assoc. Amer., pp.96-102, 1963.
[11] Jeffrey H. Dinitz and Douglas R. Stinson, "Contemporary Design Theory: A Collection of Surveys," Wiley, 1992.
[12] Trappe W., Min Wu, Ray Liu K.J., "Collusion-resistant fingerprinting for multimedia," IEEE International Conference on Acoustics, Speech, and Signal Processing 2002, Proceedings(ICASSP '02), vol.4, pp. IV-3309-IV-3312, 13-17 May 2002.
[13] H. Stone, "Analysis of Attacks on Image Watermarks with Randomized Coefficients," NEC Technical Report, 1996.

저 자 소 개

이 강 현(평생회원)-교신저자
대한전자공학회논문지,
제47권 CI편 제1호 참조