

논문 2009-46CI-6-10

# BIBD 기반의 멀티미디어 핑거프린팅 코드의 공모코드들에 대한 공모자 추적

(Colluders Tracing on the Collusion Codes of Multimedia Fingerprinting Codes based on BIBD)

이 강 현\*

(Kang Hyeon RHEE)

## 요 약

본 논문에서는 BIBD 기반의 멀티미디어 핑거프린팅 코드에 대한 공모코드들의 성능측정과 효용성 평가를 하여, 공모자 전체를 추적할 수 알고리즘을 제안한다. 공모코드들 중에는 "all 0" 또는 "all 1"의 비트 열이 생성되고, 또한 사용자의 핑거프린팅 코드와 동일한 공모코드, 비트반전 된 공모코드가 생성이 되어 공모자가 비공모자로 판정이 되거나, 비공모자가 공모자로 판정이 되는 경우가 발생한다. 따라서 공모자의 추적에 어려움이 발생한다.

본 논문에서 공모코드들의 성능측정 및 효용성 평가를 하기 위하여, 기존의 논문에서 부분적으로 처리되었던 평균화공격에 total solution으로 논리적 공모연산을 추가하여 실험하였다. 제안된 본 논문의 BIBD 기반의 멀티미디어 핑거프린팅 코드에 대한 공모공격 코드 생성의 성능측정, 효용성 평가의 실험을 통하여 공모자 추적이 100% 이루어짐을 확인하였다.

## Abstract

In this paper, it has the performance metrics and the utility evaluation of the collusion codes about multimedia fingerprinting code based on BIBD and then the tracing algorithm of all colluders is proposed. Among the collusion codes, the bit stream of "all 0" or "all 1" are generated, also same collusion code and bit reversed code with user's fingerprinting code are generated. Thus there was occurred some problems, in which a colluder is deciding to anti-colluder or anti-colluder is deciding to colluder.

In this paper, for the performance metrics and the utility evaluation of the collude codes, the experiment onto the total solution is processed by the logical collusion operation added with a partially processed averaging attack in the past papers. The proposed performance metrics and the utility evaluation about the collusion code generated from multimedia fingerprinting code based on BIBD is operated. Through the experiment, it confirmed that the ratio of colluder tracing is 100%.

**Keywords :** Multimedia Fingerprinting, BIBD, ACC(Anti-Collusion Code), Watermarking, Colluder tracing.

## I. 서 론

인터넷의 확산, 보급이 날로 증가하는 추세에서, 멀티미디어 콘텐츠의 불법복제, 배포도 심각한 증가 추세에

있다. 이에 따라 콘텐츠의 저작권 보호와 불법복제 차단과 그리고 불법배포의 추적이 가능해야 한다<sup>[1]</sup>.

콘텐츠 저작권 보호의 초기 연구는 암호화 방법으로 응용에 한계성이 있어서, 워터마킹 기술이 대안으로 소개되었다. 워터마킹 기술은 원 소유자 정보를 콘텐츠에 삽입하고, 불법복제 후에 워터마킹 정보를 콘텐츠로부터 추출, 비교하여 원 소유자를 증명하는 방법이다<sup>[2]</sup>.

그러나 워터마킹 방법은 불법으로 복제된 콘텐츠를 확인할 뿐이지, 불법으로 배포된 경로와 배포자를 확인

\* 평생회원, 조선대학교 전자정보공과대학 전자공학과  
(Chosun University, Electronics & Information Engineering College, Dept. of Electronics Eng.)

※ 본 연구는 교육과학기술부의 2009년도 일반연구자 지원사업(2009-0073050)의 수행 일부입니다.

접수일자: 2009년8월21일, 수정완료일: 2009년11월2일

할 수는 없다.

이에 따라 워터마킹의 진보된 기술로서 멀티미디어 핑거프린팅 기술<sup>[3~5]</sup>이 대두되었다. 멀티미디어 핑거프린팅 기술은 콘텐츠에 대한 소유자와 구매자의 정보를 포함하고 있다. 콘텐츠에 삽입된 구매자의 정보가 서로 다르기 때문에, 이를 이용하여 핑거프린팅 코드의 삽입 위치를 알아 낼 수 있다.

공모자들은 삽입된 핑거프린팅 코드를 제거하고, 공모코드를 재 생성하여 콘텐츠에 삽입하여 불법배포 할 수 있다. 공모자들에 의한 이러한 공모공격에 강인하도록 멀티미디어 핑거프린팅 코드가 생성되어야 한다<sup>[6]</sup>.

멀티미디어 콘텐츠 보호를 위한 핑거프린팅 코드로 반공모 코드(AAC: Anti-Collusion code)의 특성을 만족하는 균형불완비 불력코드(BIBD: Balanced Incomplete Block Design)의 응용이 여러 연구<sup>[7~16]</sup>에서 진행되었다.

본 논문에서는 BIBD 기반의 멀티미디어 핑거프린팅 코드에 대한 공모공격자들의 추적이 용이하도록 공모코드의 성능측정 및 효용성 평가를 한다. 실험을 통하여 공모코드들의 성능측정(Performance Metrics)을 평가하여, 공모공격에 사용할 수 없는 공모코드들을 정의함으로써 BIBD 기반의 핑거프린팅 코드를 효율적으로 관리할 수 있다.

## II. BIBD 코드의 생성이론

BIBD 코드<sup>[14, 19~21]</sup>는 반공모 코드의 특성을 만족한다. 즉, 공모공격에 강인성을 갖는 코드로서,  $n$  개의 코드 벡터 중에서  $(n-1)$ 명의 공모자를 검출할 수 있다. BIBD 코드는 5개의 파라미터 ( $v, b, r, k, \lambda$ )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)
- $\lambda$ : 각 처리 쌍이 나타나는 블록의 개수

(Number of blocks that processing pair appears)

5개의 파라미터는 식 (1)부터 (4)까지의 한정조건을 만족하며,

$$vr = bk \quad (1)$$

$$r(k-1) = \lambda(v-1) \quad (2)$$

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

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

$v \times b$ 의 크기를 갖는 BIBD코드는 접속행렬(Incidence Matrix)  $M$ 으로 식 (5)에 의해 내부 값이 결정되어진다.

$$M = [m_{ij}]$$

$$m_{ij} = \begin{cases} 1 & \text{if } j_{th} \text{ blocks} \in i_{jh} \text{ elements} \\ 0 & \text{otherwise,} \end{cases} \quad (5)$$

$M$ 의 행벡터는 핑거프린팅 코드가 되며  $b$ 명의 사용자들에게 부여되고, 이러한  $M$ 은 반공모 코드로 사용할 수 있다.

## III. BIBD 기반의 멀티미디어 핑거프린팅 코드의 공모공격 코드 생성과 성능측정

본 논문에서의 공모공격 코드 생성은 평균화공격

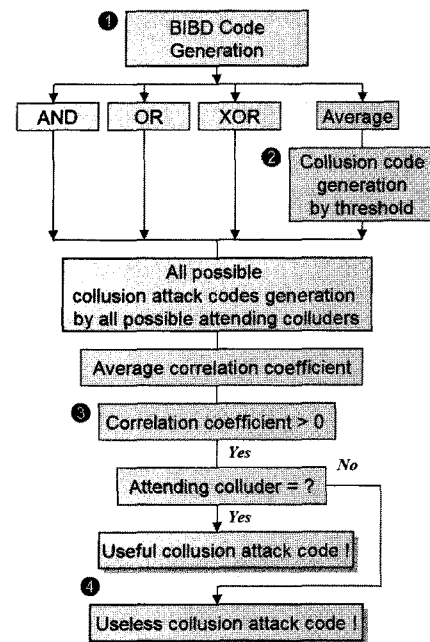


그림 1. BIBD 기반의 핑거프린팅 코드에 대한 공모코드의 성능측정 알고리즘 제안.

Fig. 1. The proposed algorithm of the performance metrics on the collusion codes of the fingerprinting codes based on BIBD.

표 1. BIBD(7,4,1)에 의한 핑거프린팅 코드  
Table 1. Fingerprinting codes by BIBD(7,4,1).

Users No. code	Fingerprinting Code
User 1 Code	0 1 0 1 0 1 0
User 2 Code	1 0 0 1 1 0 0
User 3 Code	0 0 1 1 0 0 1
User 4 Code	1 1 1 0 0 0 0
User 5 Code	0 1 0 0 1 0 1
User 6 Code	1 0 0 0 0 1 1
User 7 Code	0 0 1 0 1 1 0

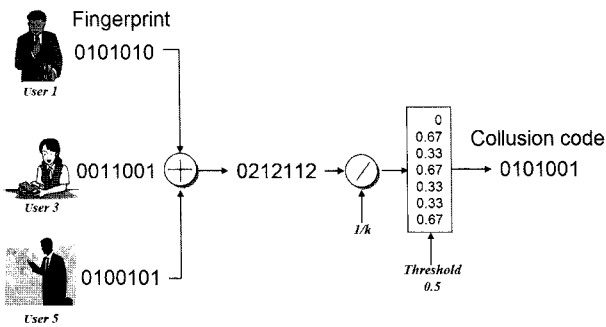


그림 2. 평균화 공모공격  
Fig. 2. Collusion attack by averaging.

표 2. 공모자 수에 따른 공모코드 생성 수  
Table 2. Number of the generated collusion codes by number of the colluders.

참여 공모자 수	공모코드 생성 수
2명 공모	21
3명 공모	35
4명 공모	35
5명 공모	21
6명 공모	7
계	119

(Averaging Attack)<sup>[12, 15~16]</sup>에 논리연산화 공격을 추가하여 실행한다. 그림 1은 본 논문에서 제안하는 반공모 특성을 만족하는 BIBD 기반의 핑거프린팅 코드에 대한 공모코드의 성능측정 알고리즘이다.

식 (5)로부터 그림 1의 ①에서 생성된 BIBD 코드를 콘텐츠 사용자에게 부여하는 핑거프린팅 코드는 표 1과 같다. 그리고 사용자가 자신을 포함하여 다른 사용자들과 서로 공모하여 생성할 수 있는 공모공격 코드 수는 표 2와 같이 총 119개의 가능한 공모코드가 생성된다. 그리고 표 1의 사용자 1,3,5가 공모하여 자신들에게 부여된 핑거프린팅 코드를 AND 공모연산으로 “all 0”의

표 3. 사용 불가능의 각 공모공격 코드 수  
Table 3. Number of the useless each attack codes.

공모공격 종류	논리연산화 공격					
	AND		OR		XOR	
공모연산 종류	“all 0”	“all 1”	“all 0”	“all 1”	“all 0”	“all 1”
비트열	“all 0”	“all 1”	“all 0”	“all 1”	“all 0”	“all 1”
사용 불가능 코드 수	91	0	0	63	7	7
공모자 수	2	-	-	-	-	-
	3	28	-	-	7	7
	4	35	-	-	28	7
	5	21	-	-	21	-
	6	7	-	-	7	-
계	91		63		14	

비트열이 되면, 이런 경우 공모자들은 평균화공격을 시도한다. 그림 2는 평균화공격의 공모코드 생성<sup>[16]</sup>을 보여준다.

표 1의 User 핑거프린팅 코드로 공모공격을 시도하여 새로운 공모코드를 생성하는데 AND 공모연산으로 공모공격 코드를 생성하면 “all 0”의 비트열을, OR 공모연산은 “all 1”의 비트열이 생성될 확률이 높다.

본 논문에서 사용하는 표 1의 BIBD(7,4,1) 코드를 기반으로 공모자 자신의 핑거프린팅 코드와 다른 공모자의 핑거프린팅 코드를 논리적으로 공모연산(AND, OR, XOR)하여 모든 가능한 공모코드를 생성한다. 표 3은 공모공격 종류와 공모연산의 참여공모자 수에 따라서, 공모코드의 비트가 “all 0”, “all 1”의 비트열로 생성되는 사용 불가능한 공모코드 수이다.

그림 3은 표 3의 각 공모연산 종류에 대한 공모코드

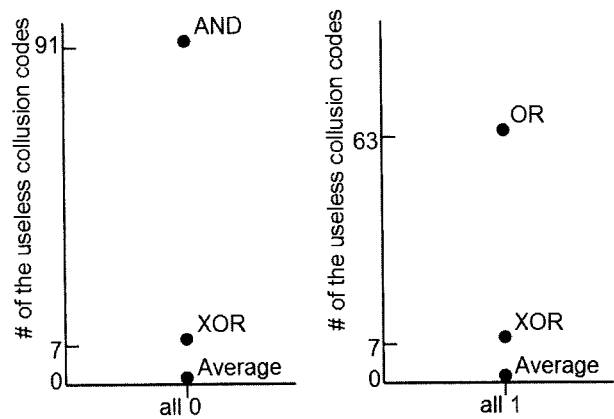


그림 3. 공모코드가 all 0, all 1 비트열에서 사용 불가능 공모코드의 수와 공모연산 종류  
Fig. 3. Number of the useless collusion codes and kind of the collusion operation at “all 0”and “all 1”bit stream in the collusion codes.

표 4. 공모연산에 따른 사용 불가능의 공모코드 수  
Table 4. Number of the useless collusion codes by the collusion operation.

연산종류	$L_1$	$L_2$	$Y_c$
	all 0	all 1	# of the useless collusion codes
AND	1	0	91
OR	0	1	63
XOR	1	1	14

가 "all 0", "all 1"의 비트열로 사용 불가능한 공모코드의 수를 나타낸다.

표 3에 대한 사용 불가능의 공모코드 산출은 식 (6)과 같이 공모연산의 종류에 따라

$$Y_c = -49L_1 - 79L_2 + b_0 \quad (6)$$

이다. 여기서  $L_1, L_2$ 는 표 4와 같이 "all 0", "all 1"을 각각 의미하며  $b_0=140$  이다.

#### IV. 제안된 공모코드의 효용성 평가

본 논문에서 제안한 그림 1의 BIBD 기반의 멀티미디어 핑거프린팅 코드의 공모코드들에 대한 효용성 평가를 위한 실험은 Matlab으로 응용프로그램을 구현하여 실행하였다.

그림 4는 본 논문에서 실행한 실험의 순서도이다. 그림 1의 ③에서 User 6,7이 표 1의 각자의 핑거프린팅 코드를 공모연산 한 공모코드는 표 5와 같고, 공모코드와 각 User의 핑거프린팅 코드와 상관계수는 표 6과 같다. 각 User의 AND, OR, XOR, Average의 상관계수 평균값이 0이상이면 이는 공모된 코드가 되며, 이 User는 그림 1의 ③에서 공모 참여자가 된다.

표 3의 내용에서 AND 공모연산에서 "all 0"비트열이 약 90% 정도 생성이 되는데, 이 경우 User 5,6,7이 공모

표 5. 공모연산에 따른 User 6,7의 공모코드  
Table 5. Collusion codes of the User 6 and 7 by collusion operation.

공모연산 종류	공모코드(User 6,7)
AND	0000010
OR	1010111
XOR	1010101
Average	1010111

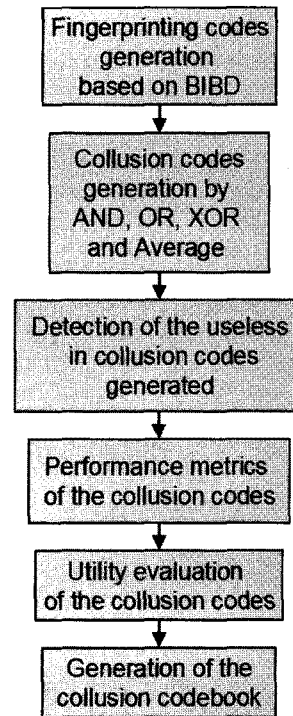


그림 4. 공모코드의 효용성 평가  
Fig. 4. The utility evaluation of the collusion codes.

표 6. 표 5의 핑거프린팅 코드와 공모코드의 상관계수.

Table 6. Correlation Coefficient between the collusion codes and the fingerprinting codes in Table 5.

핑거프린팅 코드	공모연산 종류				상관계수 평균값	공모 참가
	AND	OR	XOR	Average		
User 1 code	0.4714	-0.7303	-1.0000	-0.7303	-0.4973	
User 2 code	-0.3536	-0.0913	0.1667	-0.0913	-0.0924	
User 3 code	-0.3536	-0.0913	0.1667	-0.0913	-0.0924	
User 4 code	-0.3536	-0.0913	0.1667	-0.0913	-0.0924	
User 5 code	-0.3536	-0.0913	0.1667	-0.0913	-0.0924	
User 6 code	0.4714	0.5477	0.1667	0.5477	0.4334	●
User 7 code	0.4714	0.5477	0.1667	0.5477	0.4334	●

하여 생성된 공모코드는 표 7과 같고, 표 1의 핑거프린팅 코드와의 상관계수는 표 8과 같다. XOR 연산에 의해 생성된 공모코드는 User 4의 코드와 상관계수가 1이 되어 그림 1의 ④의 부분에서 공모자 참가로 판정하게 된다.

표 4의 내용에서 공모연산이 OR에서 "all 1" 비트열이 약 60% 정도 생성이 되는데, 이 경우 User 1,2,3,4가 공모하여 생성된 공모코드는 표 9와 같고, 표 1의 핑거프린팅 코드와의 상관계수는 표 10과 같다. XOR 연산에 의해 생성된 공모코드는 User 4의 코드와 비트반전

표 7. User 5,6,7의 공모코드

Table 7. Collusion codes of the User 5,6 and 7.

공모연산 종류	공모코드(User 5,6,7)	비 고
AND	0000000	"all 0" 비트열
OR	1110111	
XOR	1110000	User 4와 같은 코드생성
Average	0000111	

표 8. 표 7의 공모코드와 User들의 핑거프린팅 코드와의 상관계수 및 공모자 추적.

Table 8. Correlation coefficient between the users fingerprinting codes and the collusion codes in Table 7, and the colluders tracing.

핑거프린팅 코드	공모연산 종류				상관계수 평균값	공모 참가	예리 판단
	AND	OR	XOR	Average			
User1 code	-	-0.4714	-0.1667	-0.1667	-0.2682		
User2 code	-	-0.4714	-0.1667	-0.1667	-0.2682		
User3 code	-	-0.4714	-0.1667	-0.1667	-0.2682		
User4 code	-	0.3536	1.0000	-0.7500	0.2012		☹
User5 code	-	0.3536	-0.1667	0.4167	0.2012	●	
User6 code	-	0.3536	-0.1667	0.4167	0.2012	●	
User7 code	-	0.3536	-0.1667	0.4167	0.2012	●	

표 9. User 1,2,3,4의 공모코드

Table 9. Collusion codes of the Users 1,2,3 and 4.

연산종류	공모코드(User 1,2,3,4)	비 고
AND	0000000	"all 0" 비트열
OR	1111111	"all 1" 비트열
XOR	0001111	User 4와 비트열 반전 코드생성
Average	1111000	

되어 상관계수가 -1이 되어 그림 1의 ④의 부분에서 공모자 참가에서 제외되게 판정된다.

표 8과 10에서 XOR 공모연산에서 표 1의 핑거프린팅 코드 User 4와의 동일한 공모코드, 비트반전으로 된 공모코드가 생성이 되어 상관계수가 1 또는 -1이 된다. 공모자 추적에서 표 8에서는 역울하게 공모자가 되고, 표 10에서는 공모자에 참여하고도 공모자 추적에서 벗어난 결과가 된다. 이러한 경우의 결과가 표 11과 같이 참여 공모자 수가 3에서 상관계수 1이 28개, 참여 공모자 수가 4에서 상관계수 -1이 28개로 각각 나타난다.

표 10. 표 9의 공모코드와 User들의 핑거프린팅 코드와의 상관계수 및 공모자 추적.

Table 10. Correlation coefficient between the Users fingerprinting codes and the collusion codes in Table 9, and the colluders tracing.

핑거프린팅 코드	공모연산 종류				상관계수 평균값	공모 참가	예리 판단
	AND	OR	XOR	Average			
User1 code	-	-	0.1667	0.1667	0.1667	●	
User2 code	-	-	0.1667	0.1667	0.1667	●	
User3 code	-	-	0.1667	0.1667	0.1667	●	
User4 code	-	-	-1.0000	0.7500	-0.1250	●	☹
User5 code	-	-	0.1667	-0.4167	-0.1250		
User6 code	-	-	0.1667	-0.4167	-0.1250		
User7 code	-	-	0.1667	-0.4167	-0.1250		

표 11. XOR 공모연산에서 상관계수 1과 -1의 사용 불가능 공모코드의 수

Table 11. Number of the useless collusion codes of the correlation coefficient 1 and -1 on XOR collusion operation.

공모연산종류	XOR		
	상관계수	Corr=1	Corr=-1
사용 불가능 코드수		28	28
공모자 수	2	-	-
	3	28	-
	4	-	28
	5	-	-
	6	-	-
계		56	

그동안 부분적으로 연구되었던 평균화 공모공격에 대하여 본 논문에서 지향하는 total solution으로 논리적 공모연산을 포함하여 공모자 추적을 하였다. 표 12는 참여 공모자에 따른 공모코드, 공모코드와 핑거프린팅 코드의 상관계수, 상관계수의 평균값 그리고 공모자추적의 판정결과로 구성되어 있다.

이상의 실험결과 본 논문에서 제안된 BIBD 기반의 핑거프린팅 코드에 대한 공모공격 코드들의 성능측정과 효율성 평가를 하였다.

그리고 표 4의 결과에 따라 공모연산 종류와 공모자의 수에 따른 사용 불가능의 공모코드 수  $Y_c$  산출은 식 (7) 과 같고, 공모연산 종류에 따른 다항계수는 표 13과 같다.

$$Y_c = \sum_{C_n=2}^v P_k C_n^{(-C_n+6)} + C \quad (7)$$

표 12. 공모자 추적 판정

Table 12. Decision of the colluders tracing.

일련 번호	참여 공모자	공모코드				상관계수				상관 계수 평균	공모자 추적 판정
		AND	OR	XOR	Average	AND	OR	XOR	Average		
1	1,2	0	1	1	1	0.471	0.547	0.166	0.547	0.433	☹☹☹☹☹☹☹
		0	1	1	1	0.471	0.547	0.166	0.547	0.433	
		0	0	0	0	0.471	-0.730	-1.000	-0.730	-0.497	
		1	1	0	1	-0.353	-0.091	0.166	-0.091	-0.092	
		0	1	1	1	-0.353	-0.091	0.166	-0.091	-0.092	
		0	1	1	1	-0.353	-0.091	0.166	-0.091	-0.092	
		0	0	0	0	-0.353	-0.091	0.166	-0.091	-0.092	
:	:	:	:	:	:	:	:	:	:	:	
68	1,3,4,6	0	1	0	1	0	0.3536	0	0.3536	0.3536	☹☹☹☹☹☹☹
		0	1	0	1	0	-0.471	0	-0.471	-0.471	
		0	1	0	1	0	0.3536	0	0.3536	0.3536	
		0	1	0	1	0	0.3536	0	0.3536	0.3536	
		0	0	0	0	0	-0.471	0	-0.471	-0.471	
		0	1	0	1	0	0.3536	0	0.3536	0.3536	
		0	1	0	1	0	-0.471	0	-0.471	-0.471	
:	:	:	:	:	:	:	:	:	:	:	
119	2,3,4,5,6,7	0	1	1	1	0	0	-1.000	-1.000	-1.000	☹☹☹☹☹☹☹
		0	1	0	0	0	0	0.167	0.167	0.167	
		0	1	1	1	0	0	0.167	0.167	0.167	
		0	1	0	0	0	0	0.167	0.167	0.167	
		0	1	1	1	0	0	0.167	0.167	0.167	
		0	1	0	0	0	0	0.167	0.167	0.167	
		0	1	1	1	0	0	0.167	0.167	0.167	

표 13. 식 (7)의 다항계수  $P_k$

Table 13. Polynomial coefficient  $P_k$  of Eq. (7).

$k$	AND	OR	XOR
1	0.88	2.63	0.58
2	-12.25	-43.75	-8.17
3	51.63	256.38	37.92
4	-54.25	-614.25	-65.33
C	-14	-511	-35

여기서  $v$ : BIBD의  $v$ ,  $C_n$ : 공모자의 수,  $k$ :  $C_n-1$ 의 값이다.

그러나 핑거프린팅 코드의 목적이 공모자의 추적이기 때문에, 결과적으로 XOR 공모연산의 56개(47%)가 효용성 평가(역울한 공모자참가의 의심인지? 비공모자의 판단인지?)에서 제외되지만, 표 8과 10에서 Average 상관계수 값만을 고려함으로써 공모자를 100% 추적할 수 있다. 때문에 표 3의 사용 불가능한 공모코드는 공모자 추적에 고려하지 않아도 무관함을 확인하였다.

그리고 공모연산에 따른 사용 가능한 공모공격 코드와 사용 불가능한 공모공격 코드, 공모자 추적 불가능

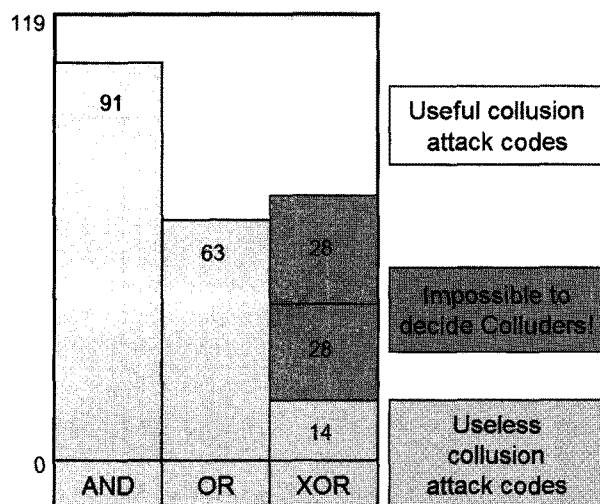


그림 5. 공모연산에 따른 공모코드의 특성 및 수  
Fig. 5. Number and characteristics of the collusion code by collision operation.

의 코드 수 구성은 그림 5와 같다.

표 14는 기존의 논문과 본 논문의 알고리즘 성능비교로서, n명의 전체사용자 중, 참여 공모자의 수를 n-1명까지 추적할 수 있다.

표 14. 제안된 알고리즘과 기존 알고리즘의 성능비교  
Table 14. Performance comparison between the proposed algorithm and the conventional algorithms.

Fingerprinting algorithms	Method	Possible to trace the colluders
Dittman[17]	d-detecting	2
Boneh[3]	c-secure	2
Trappe[16]	AND ACC	2
Domingo Ferrer[18]	3-secure	3
Proposed Algorithm	AND, OR, XOR, Average	n-1

(n: Number of the total Users)

### V. 결 론

본 논문에서는 제안된 BIBD 기반의 멀티미디어 핑거프린팅 코드의 공모공격 코드들에 대한 성능측정과 효용성 평가를 실행하였다. 반공모에 강인한 BIBD 코드의 평균화 및 논리연산의 공모공격 코드는 53% 효용성이 있다. 공모에 참여하고도 은익이 된 경우가 23.5%로 핑거프린팅 코드와 상관계수가 1이며, 공모에 참여하지 않고도 공모자로 판정된 경우가 23.5%로 핑거프린팅 코드와 상관계수가 -1이었다. 이는 XOR 공모연산에서 모두 이루어졌으며, 이 경우 평균화공격의 상관계수만을 고려하면 공모자 추적을 n-1명까지 100% 확인할 수 있다.

본 논문에서 구현한 알고리즘은 논리적 공모연산공격 및 평균화공격으로 이루어진 다양한 공모공격에 대하여 멀티미디어 콘텐츠의 불법배포자 추적에 광범위하게 사용할 수 있다.

### 감사의 글

본 연구분야의 선행연구자들에게 진심으로 경의를 표하며, 뒤의 보이지 않은 심사위원들의 세심한 심사의 견에 감사를 드립니다.

### 표절논문 인용주의

{“유비쿼터스 네트워크 시스템에서의 미디어 보안에 관한 연구,” 한국사이버테러정보전학회, [7권 1호-04], pp. 29-34, 2007.3}은 참고문헌 [13]을 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] 이강현, “디지털 영상의 다중 하위 비트플랜에 삽입되는 워터마크,” 대한전자공학회 논문지 CI, 43 권 8호, pp.101-109, 2006. 11.
- [3] D. Boneh and J. Shaw, “Collusion-secure fingerprinting for digital data,” IEEE Tran. on Information Theory, vol. 44, pp. 1897-1905, September 1998.
- [4] 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.
- [5] Lin W.S., Zhao H.V., Ray liu K.J., “Scalable Multimedia Fingerprinting Forensics with Side Information,” IEEE International Conference on Image Processing, 2006, pp.2293-2296, 8-11 Oct. 2006
- [6] 김원겸, 이선화, 서용석, “공모공격에 강인한 디지털 핑거프린팅 기술,” 정보과학회지, 23권 8호, pp.52-60, 2005.8.
- [7] Jie Yang, Xiaoxia Xu, “A Robust Anti-collusion Coding in Digital Fingerprinting System,” IEEE Asia Pacific Conference on Circuits and Systems, APCCAS 2006, pp.996-999, 4-7 Dec. 2006.
- [8] Shashanka D., Bora P.K, “Collusion Secure Scalable Video Fingerprinting Scheme,” International Conference on Advanced Computing and Communications, ADCOM 2007, pp.641-647, 18-21 Dec. 2007.
- [9] Jie Yang, Ping Liu, GuoZhen Tan, “The digital fingerprint coding based on LDPC,” Signal Processing, 2004. Proceedings. ICSP '04. 2004 7th International Conference on Volume 3, pp. 2600-2603, 31 Aug.-4 Sept. 2004.
- [10] Jie Yang, Xiaoxia Xu, “A Robust Anti-collusion Coding in Digital Fingerprinting System,” The 8th International Conference on Signal Processing, Volume 4, 2006.
- [11] Zang Li, Trappe W, “Collusion-resistant fingerprints from WBE sequence sets,” IEEE International Conference on Communications, ICC 2005, Volume 2, pp. 1336-1340, 16-20 May 2005.
- [12] In Koo Kang, Choong-Hoon Lee, Hae-Yeoun Lee, Jong-Tae Kim, Heung-Kyu Lee,

- “Averaging attack resilient video fingerprinting,”  
IEEE International Symposium on Circuits and  
Systems, ISCAS 2005, Vol. 6, pp.5529-5532,  
23-26 May 2005.
- [13] 노진수, 이강현 “신경회로망에 의한 공모된 멀티미  
디어 핑거프린트의 검출” 전자공학회논문지, 제43  
권 CI편 제4호, pp.80-87, 2006. 7
- [14] K.H. Rhee, “Detection of Colluded Multimedia  
fingerprint using LDPC and BIBD,” IEEK  
Computer Society, Vol.43, No.5, pp.68-75, Sept.  
2006.
- [15] J. Kilian, T. Leighton, L. R. Matheson, T. G.  
Shammon, R. E. Tarjan and F. Jane, “Resistance  
of Digital Watermarks to collusive Attacks,”  
Tech. Rep., TR-585-98, Dept. of Computer  
Science, Princeton University, 1998.
- [16] Wade Trappe, Min Wu, Jane Wang and K.J.  
Ray Liu “Anti-collusion Fingerprinting for  
Multimedia,” IEEE Tran. on Signal Processing,  
VOL.51, NO.4, pp.1069-1087, April 2003.
- [17] J. Dittmann, “Combining Digital watermarks and  
Collusion Secure Fingerprints for Customer  
Copy Monitoring,” Proc. IEE Seminar Sec. Image  
& Image Auth., pp.128-132, Mar. 2000.
- [18] F. Sebe and Domingo-Ferrer, “Short 3-Secure  
Fingerprinting Codes for Copyright Protection,”  
Lecture Notes in Computer Science, Vol. 2384,  
pp.316-327, 2002.
- [19] <http://mathworld.wolfram.com/BlockDesign.html>
- [20] 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.
- [21] Ryser, H. J. “The  $(b,v,r,k,\lambda)$ -Configuration.”  
§8.1 in Combinatorial Mathematics. Buffalo, NY:  
Math. Assoc. Amer., pp.96-102, 1963.

---

저 자 소 개

이 강 현(평생회원)  
대한전자공학회 논문지  
제46권 CI편 제3호 참조