2013년 7월 전자공학회 논문지 제 50 권 제 7 호
Journal of The Institute of Electronics Engineers of Korea Vol. 50, NO. 7, July 2013 http://dx.doi.org/10.5573/ieek.2013.50.7.175

논문 2013-50-7-22

XOR 공모공격에서 해밍거리를 이용한 공모된 멀티미디어 핑거프린팅 코드의 부정자 추적

(Traitor Traceability of Colluded Multimedia Fingerprinting code Using Hamming Distance on XOR Collusion Attack)

정 일 용*, 이 강 현**

(Il Yong CHUNG and Kang Hyeon RHEE©)

요 약

본 논문에서는 멀티미디어 콘텐츠의 부정자를 추적하기 위하여, 공모된 핑거프린팅 코드를 해밍거리를 이용하여 XOR 공모공격을 분류하는 알고리즘을 제안한다. 기존의 공모된 핑거프린팅 코드는 상관관계수를 이용하여 부정자를 판정하였지만 제안된 방법은 해밍거리를 이용하였다.

그 결과 상관관계 계수에 의한 XOR 공모공격은 XOR의 심각한 선형문제 때문에 50% 정도의 공모자 수에서 불가능 했던 부정자 추적이 해밍거리를 이용하여 최소한 1명의 부정자를 추적할 수 있는 추적도의 성능을 향상시켰으므로, 제안된 부정자 추적의 기능동작은 *Probabilistic Scheme*에 부합하였다.

Abstract

For the traitor tracing of multimedia content, this paper presents the classification algorithm of XOR collusion attack types using hamming distance, which applies to the colluded fingerprinting codes. The conventional traitor decision hinges on the colluded fingerprinting code used by a correlation coefficient, but the proposed scheme uses hamming distance.

While XOR collusion attack employing a correlation coefficient is impossible to trace the traitors about 50% colluders due to a serious XOR linear problem, our method improves the performance of traceability to trace at least 1 traitor using hamming distance, and thus, the functional behavior of the proposed traitor traceability is coincided with *Probability Scheme.*

Keywords : Multimedia fingerprinting, Traitor traceability, Hamming distance, XOR collusion attack.

Ⅰ. 서 론

멀티미디어 콘텐츠의 지적재산권을 보호하고, 불법배포를 방지하기 위한 멀티미디어 핑거프린팅 기술[1~3]이 대두되었다. 콘텐츠 사용자들이 연합으로 공모하여, 핑거프린팅 코드를 재생성하고, 이를 콘텐츠에 삽입한 불법 콘텐츠가 재배포 되었을 때, 공모에 가담한 부정자 (Traitor)를 추적할 수 있는 기능 (TA: Traceability)이 요구된다.

TA 관점에서 공모내성 (Collusion Resistance)이 있는 코드 구성[4~6]을 위한 연구가 진행되었다. TA의 만족성을 위한 반공모 코드 (ACC: Anti-Collusion Code)는 AND-ACC[7~8]의 공모공격이 주로 연구되었다. 여기에서 사용되는 BIBD (Balanced Incomplete Block Design) 코드[9]는 (k-1, k는 블록의 개수)의 부정자 추적을 증명하였는데, 이는 사용자의 각 핑거프린팅 코드 사이에 존재하는 마킹가정 (Marking Assumption)[10]을 이용하였다. Rhee는 [11]에서 BIBD 기반의 사용자 핑거프린팅 코드의 천이공격 (Shifting attack)에 대하

* 정회원, 조선대학교 컴퓨터공학과
(Dept. of Computer Eng., Chosun University)
** 평생회원, 조선대학교 전자공학과
(Dept. of Electronics Eng., Chosun University)
© Corresponding Author(E-mail: khrhee@chosun.ac.kr)
※ 본 논문은 2012년 조선대학교 교내학술 연구비지원 (322386)으로 수행되었습니다.
접수일자: 2013년3월4일, 수정완료일: 2013년6월26일

여 유클리드 거리에 의한 부정자 추적을 제안하였으나 공모공격의 종류가 제한된 점이 있다. 이후, [12]에서 마킹가정을 고려하지 않는 TA 코드의 생성을 위하여, 유클리드 거리 (Euclidean distance)를 이용하는 에러정정 코드 (ECC: Error Correcting Code)가 평가 되었으며, [13]은 [4-6]의 결과를 재정리하였다. [14]에서는 BIBD 코드에 RS(Reed-Solomon) 코드를 변조하여 사용자 핑거프린팅 코드를 생성하였으나, 부정자 추적은 inner 코드와 outer 코드를 사용하는 이중처리를 해야 하며, [15]에서는 RS 코드를 지원하는 AACS (Advanced Access Content System)를 사용하는 Set-cover를 제안하였으나, 이 또한 부정자 추적은 이중처리를 해야 한다.

그리고 Rhee는 [16,17]에서 4가지의 공모공격으로 (AND, OR, XOR and Averaging)-ACC를 분석하는 알고리즘을 제안하였다. 특히, XOR 연산의 문제점을 갖고 있는 XOR 공모공격에서 원 핑거프린팅 코드와 공모된 코드와의 상관관계 계수에 따른 공모자 추적에서 순결성 사용자 (Innocent user)가 악의성 사용자 (Malicious user)로 판정되는 문제점이 발생하는데 [18]에서 신경망을 이용하여 이를 해결하였으나, 퍼셉트론의 학습 연산량이 크다. 모든 부정자 추적은 불가능하므로 단 한명의 부정자라도 추적할 수 있도록 연산량 복잡도 O의 감소를 위하여 *Probability Scheme*[19]이 주로 사용된다.

본 논문에서는, TY의 효율성을 높이기 위하여 사용자의 BIBD 기반 핑거프린팅 코드와 공모된 코드의 해밍거리 (Hamming distance)를 이용하여, 선형분리가 불가능한 XOR 공모공격을 분류하고, 부정자를 추적하는 *Probabilistic Scheme*에 부합된 알고리즘을 제안한다.

제 Ⅱ장에서는 본 논문에 사용된 이론적 배경을 설명하고, 제 Ⅲ장에서는 공모공격의 분류와 부정자 추적을 위한 알고리즘을 제안하고, 제 Ⅳ장에서는 구현된 알고리즘의 성능평가를 위하여 실험결과의 분석을 통하여 제 Ⅴ장에서 결론을 맺는다.

Ⅱ. 핑거프린팅 코드의 추적성 이론

핑거프린팅 코드를 생성할 때, 공모내성의 목적을 위하여 추적성능 (Tracing Capability)이 포함되는데, 이를 위하여 TA 코드가 광범위하게 연구되었다, [20]에서 공모자의 수가 c 또는 c 이하에서 c-TA 코드는 공모된 코드워드가 순결성 사용자 코드보다 공모자들의 코드워드 중, 최소한 하나에서 가장 적은 거리의 조건을 만족한다고 하였다. M. Wu는 [14]에서 ECC를 사용하여 식 (1)과 같이 최소거리 dmin이 충분히 큰 c-TA 코드를 구성하였다.

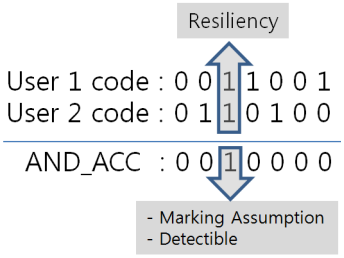

그림 1. 코드의 탄력성과 마킹 가정
Fig. 1. Code resiliency and Marking assumption.

$$d_{\min} > (1-\frac{1}{c^2})n \tag{1}$$

여기서 n은 코드길이, c는 공모자의 수로서 이 코드는 내성의 경향이 있고, 최소거리로 단집합 범위가 이루어지며, c-TA 코드 구성에 RS (Reed-Solomon) 코드가 선택되었다. RS 코드를 통하여 c-TA 코드워드의 수에 대한 크기 q의 알파벳 제산은 $N_u = q^k$이며, 여기서 $k = \lceil L/c^2 \rceil$이 된다.

그리고 ACC가 갖어야 할 특성으로 그림 1과 같이 사용자 1과 2의 코드 중에 "1"이 같은 위치에 있는 탄력성 (Resiliency)이 있어야 한다. 공모자들이 각자의 사용자 코드를 제공하여 공모연산을 한 후에도 공모코드의 이 위치는 마킹가정을 유지하는 검출성이 있어야 한다. 공모된 코드에서 마킹가정 위치의 "1"이 있는 사용자의 코드를 갖는 자가 공모자로 추적이 된다.

그리고 콘텐츠 사용자의 멀티미디어 핑거프린팅 코드의 생성으로, 블록 설계(Block Design)는 탄력성의 마킹가정이 있는 코드를 생성할 수 있어서 사용자의 핑거프린트에 응용이 많이 되고 있으며, 공모공격에 대한 내성 (Resistance)이 있는 반공모 코드로 많은 연구[7~11]가 진행되어 왔다.

블록설계의 대표로 균형 불완전 블록설계에 의한 BIBD $\{v, b, r, k, \lambda\}$ 코드[9, 21]를 생성하여 사용자의 멀티미디어 핑거프린팅 코드로 할당한다.

여기서 v: 처리의 개수 (Number of treatments)
b: 블록의 개수 (Number of blocks)
r: 각 v의 반복 수 (Number of times each treatment is run, $k<v$)
k: 하나의 블록에 포함된 v의 개수 (Number of

treatments per block)

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

이다.

5개의 파라미터는 식(2)부터 (5)까지의 한정조건을 만족한다.

$$vr = bk \tag{2}$$

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

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

$$r = \frac{\lambda(v-1)}{k-1} \tag{5}$$

식(1)에서 $b=v$ or $r=k$ 이면 BIBD는 대칭성이며 $v\times b$의 크기를 갖는 BIBD의 접속행렬 (Incidence matrix) M은 식(6)에 의해 행렬 요소 m_{ij}의 값이 결정된다.

$$M=[m_{ij}]$$
$$m_{ij}=\begin{cases}1 & \text{if } (x_i\in A_j) \text{ or } (j_{th}blocks \in i_{th}blocks)\\ 0 & otherwise.\end{cases} \tag{6}$$

그러므로 M은 식(7)을 만족하게 된다[21].

$$MM^t=(r-\lambda)I+\lambda J \tag{7}$$

여기서 I: *the* $v\times v$ *identity matrix*

J: *the* $v\times v$ *matrix of all 1's*

이다. M의 보수행렬 C는 사용자의 핑거프린팅 코드로 할당된다.

Ⅲ. 핑거프린팅 코드의 해밍거리를 이용한 XOR 공모공격 분류

콘텐츠에 삽입되어 있는 사용자의 멀티미디어 핑거프린팅 코드가 공모자에 의하여 변조되었을 때, 부정자의 추적을 위해서는 각 사용자들 간의 핑거프린팅 코드 사이에 탄력성이 있어야 하고, 공모공격의 종류를 분류해야 한다.

본 논문에서는 추적의 효율성을 높이기 위하여, 블록설계의 BIBD 코드가 갖는 탄력성에 따라 공모연산 (AND, OR, XOR 그리고 Averaging)으로 생성된 공모코드의 공격을 해밍거리를 이용하여 선형분리가 불가능한 XOR 공모공격의 공모자 추적성이 *Probabilistic Scheme*에 부합되는 알고리즘을 제안한다. 표 1은 Ⅲ장에서 사용되는 기호를 설명한다.

표 1. Ⅲ장에서 사용하는 기호 설명
Table 1. Usage symbols used in Section Ⅲ.

Symbol	Usage	Symbol	Usage
c	공모자의 수	n	코드의 길이
ed	오류검출	k	n에서 1의 갯수
d_{min}	최소거리	H_d	해밍거리
Γ	콘텐츠 제공자 코드	Γ_c	사용자 코드
Desc(Γ_c)	공모코드	$\Gamma\backslash\Gamma_c$	참조코드

[정의1] 식 (1)에서 d_{min}는 n보다 커야하는데, 공모자의 수 c가 많을수록 사용자 코드와 공모된 코드의 H_d는 커야하고 n은 작아야 한다.

[정리1] [7]에서 사용된 ECC의 (n,k) RS 코드는 t개의 심볼 에러 정정으로 $t=n-k$, 그리고 $d_{min}=2t+1$이므로 $d_{min}=2(n-k)+1$이 된다. 그리고 오류검출은 $d_{min}\geq ed+1$의 조건이 필요하다.

[증명1] n,k를 BIBD의 한정조건 식(2~5)의 v,k로 놓으면 그림 1과 같은 탄력성 ($k-1$)이 구해진다. ■

[정리 2.1] Γ는 길이 n의 q-ary 코드이며 크기는 q^k이다. $\Gamma\in Q^n$에서 Q는 유한 알파벳이며, $|Q|=q$와 $|\Gamma|=q^k$이다. Q^n의 요소는 워드(word)이며, Γ의 요소는 코드워드(codeword)로 $w=(w_1,w_2,...,w_n)$으로 표현하며 $w_i\in Q$이다.

[정리 2.2] $\Gamma_c=\{w^{(1)},w^{(2)},...w^{(c)}\}\subset\Gamma$으로 연합이라고 한다.

if $w_i^{(1)}=w_i^{(2)}=...=w_i^{(c)}$,

then i는 undetectible 이며,

otherwise detectible 이다.

$\Gamma_c\subseteq\Gamma$의 연합으로, Γ_c의 자손집합은 Desc(Γ_c)=$\{w\in Q^n: w_i\in\{w^{(1)},w^{(2)},...w^{(c)}\}\ \forall\ 1\leq i\leq n\}$으로 나타낸다.

[증명2] 집합 Desc(Γ_c)는 n-tuple로 구성되며, Γ_c의 c 연합으로 생성된다. Desc(Γ_c)의 요소 x는 Γ_c의 자손이 된다. ■

정리 2.1, 2.2로 표 2와 같이 콘텐츠 제공자가 갖는 메타키 (Meta Key) a 코드는 $\Gamma\in({}_vC_k)$, 사용자 코드 $\Gamma_c\in\Gamma$는 블록설계 코드의 탄력성을 높이기 위하여 증명 1과 식(5)의 결합행렬의 보수행렬을 만든다(예: $v,k,\lambda=\{7,3,1\}$).

[보조정리 2] 공모코드 Desc(Γ_c)는 Γ_c의 요소들 상호간에

표 2. 콘텐츠 제공자가 갖는 메타 키의 구성
Table 2. Content provider kept the structure of Meta keys.

콘텐츠 제공자 코드 Γ	사용자 코드 Γ_c	공모 가담자 수	공모코드 Desc(Γ_c)	참조코드 $\Gamma\backslash\Gamma_c$
a	y	c	x	z

c의 연합에 의한 AND, OR, XOR과 Averaging 연산에 의하여 생성된다.

그리고 공모자의 추적성 TA를 정의하기 위하여,

[정의 3.1] Γ의 c-코드를 갖는 부분집합 Γ_c가 그림 1의 탄력성을 갖으면 c-TA 코드이다.

[정의 3.2] $x \in \mathrm{Desc}(\Gamma_c)$ 이면 $y \in (\Gamma_c)$ 중에서 적어도 하나의 코드워드로서, $z \in \Gamma \backslash \Gamma_c$에서 $|\mathrm{I}(x,y)| > |\mathrm{I}(x,z)|$을 만족한다. 여기서 $\mathrm{I}(x,y)=\{i: x_i=y_i\}$이다.

[증명 3] Γ_c가 c-TA 코드라면, 최대 c의 연합크기로 공모코드 x를 생성한다. 연합 요소는 공모코드 x에 접근되고 참조 코드 z와 무관하다. ■

[정리 4] Γ_c가 길이 n의 (n, q^k), 차원 k, 최소거리 $d > n(1-(1/c^2))$를 갖으면, Γ_c는 c-TY 코드이다.

[증명 4] 정의 2의 $x \in \mathrm{Desc}(\Gamma_c)$에서, 최소 하나의 $y \in (\Gamma_c)$가 있으면, $|\mathrm{I}(x,y)| > n/c$을 만족하지만, $|\mathrm{I}(x,y)| < n/c$이면 $\sum_{i=1}^{c} |(x,y_i)| < n$ 으로 $x \in \mathrm{Desc}(\Gamma_c)$의 모순이다. ■

∴ 정리 4의 d에 따라 증명 4의 y는 TA의 *Probabilistic Scheme*에 부합된다.

그리고 정리 4의 $d > n(1-(1/c^2))$에서, 정의 3.2의 $z \in \Gamma \backslash \Gamma_c$에 의하여 $d(z,y) > n(1-(1/c^2))$이 되는데, 이는 $|\mathrm{I}(z,y)| < n - n(1-(1/c^2)) = n/c^2$이 된다.

∴ $|\mathrm{I}(z,y)| \le |\mathrm{I}(z,\Gamma_c| \le \sum_{i=1}^{\omega} |\mathrm{I}(z,y_i)| < c \cdot (n/c^2) = n/c \le \mathrm{I}|(x,y)|$가 되며 정의 1은 참이 된다.

이상의 정의, 정리에 따라 공모된 코드로부터 공모공격 종류의 판정과 공모자 추적을 위한 알고리즘 구현의 흐름도는 그림 2와 같다.

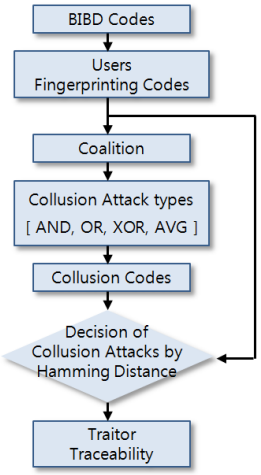

그림 2. 제안된 공모공격의 분류와 부정자 추적의 흐름도

Fig. 2. Flow-chart of the collusion attack classification and traitor tracing proposed.

Ⅳ. 부정자 추적성능 평가

본 논문의 제안된 알고리즘의 성능평가를 위하여 식 (7)의 보수행렬 C에 의한 콘텐츠 제공자 코드 Γ는 (7,4) 코드로 ${}_7C_4$이며 이중에서 {7,3,1} BIBD를 만족하는 코드 Γc를 사용자 코드로 하고 공모코드 Desc(Γc)는 4가지 공모공격의 종류에 따라 공모자의 수는 2~7명의 연합으로 AND, OR, XOR 그리고 AVG 공격으로 표 3과 같이 생성한다.

표 3의 콘텐츠 제공자의 코드로부터 사용자의 BIBD 기반 멀티미디어 핑거프린팅 코드의 공모내성을 실험한다. 사용자 코드 Γ_c와 공모코드 $\mathrm{Desc}(\Gamma_c)$의 해밍거리 H_d는 정리 3.2의 $|\mathrm{I}(x,y)|$에 따라 결과는 표 4와 같다.

AND 공격의 추적도를 $f_{AND}(x)$, OR 공격은 $f_{OR}(x)$, XOR 공격은 $f_{XOR}(x)$ 및 AVG 공격은 $f_{AVG}(x)$라 하고, 식(8)과 같이 표현하여 4차까지 다항식 계수를 구하면 표 5와 같고, 각 공격의 추적도는 그림 3과 같다.

$$\mathrm{TA}(x) = f_{AND}(x) + f_{OR}(x) + f_{XOR}(x) + f_{AVG}(x) \qquad (8)$$

표 3. 콘텐츠 제공자 코드로부터, 사용자 코드, 공모코드 그리고 참조코드의 생성

Table 3. Codes generation of User, Collusion and Reference from the content provider.

콘텐츠 제공자 코드 Γ		사용자 코드 Γ_c	공모코드 $\mathrm{Desc}(\Gamma_c)$	참조코드 $\Gamma \backslash \Gamma_c$
a	1111000	y 1010101 0110011 1100110 0001111 1011010 0111100 1101001	x	z
	1110100			
	1110010			
	1110001			
	• •			
	1001110			
	1001101			
	1001011			
	1000111			
	• •			
	0011101			
	0011011			
	0010111			
	0001111			

표 4. $|\mathrm{I}(x,y)|$의 실험 결과

Table 4. Experimental results of $|\mathrm{I}(x,y)|$.

공모자 수	2	3	4	5	6	7
AND	2	3	0	0	0	0
OR	2	3	4	5	6	7
XOR	0	0	1	1	0	0
AVG	2	3	3	5	6	7

표 5. 공격종류에 따른 추적도의 다항식 계수
Table 5. Polynomial coefficients of the traceability by attack types.

다항계수	x^4	x^3	x^2	x	C
$f_{AND}(x)$	-0.15	2.73	-17.98	48.26	-42.02
$f_{OR}(x)$	-5.E-18	1.1E-16	-7.4E-16	1	0
$f_{XOR}(x)$	0.08	-1.5	9.42	-24	21
$f_{AVG}(x)$	-0.04	0.71	-4.21	10.97	-8.10

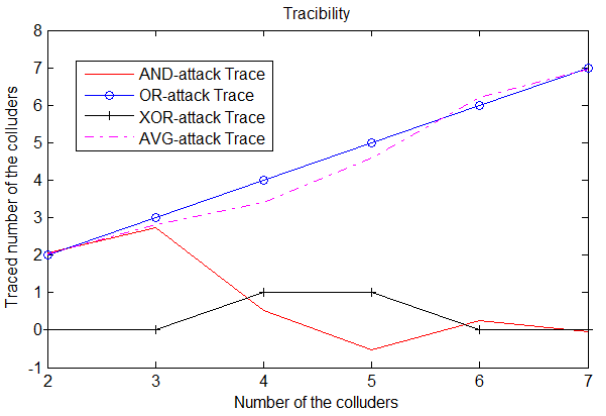

그림 3. 공모자 수에 따른 부정자 추적율 (AND, OR, XOR 그리고 AVG 공격)
Fig. 3. Traitor traceability according to the number of colluders (AND, OR, XOR and AVG attack).

표 6. XOR 공모연산에서 상관관계 계수 1과 -1의 사용 불가능 공모코드의 수
Table 6. Number of the useless collusion codes of the correlation coefficient 1 and -1 on XOR collusion operation.

공모공격 종류		XOR		
부정자 추적 연산방법		상관관계 계수 [17]		해밍거리 [본 논문]
		Corr=1	Corr=-1	H_d
공모자 수	2	-	-	-
	3	추적불가능	-	-
	4	-	추적불가능	**1**
	5	-	-	**1**
	6	-	-	-
	7	-	-	-

표 4의 공모공격의 종류와 식 (8)의 추적도 결과에 의한 추적성능은 다음과 같다.

1) AND 공격의 추적도는 공모자의 수에 반비례하고,
2) XOR 공격은 공모자의 수에 따라, 일부 추적도가 존재하고,
3) OR 및 AVG 공격은 추적도가 공모자 수에 거의 비례한다.

그러므로 본 논문에서 제안된 BIBD 기반의 핑거프린팅 코드의 공모공격에 따른 해밍거리를 이용한 부정자 추적에서, AND 공격은 공모자의 수가 적을 때, XOR공격은 중간정도의 공모자의 수, 그리고 OR 및 AVG 공격은 전체 공모자의 수를 추적할 수 있음이 성능평가 면에서 확인되었다.

그리고 표 6[17]에서 XOR 공격은 c가 3~4명에서 상관관계 계수를 이용하면 공모자를 추적할 수 없었으나, 본 논문에서 사용하는 해밍거리를 이용한 공모코드의 판정은 그림 3에서 c가 4~5명에서 최소한 각각 1명씩의 부정자를 추적할 수 있다. 따라서 제안된 알고리즘의 기능적 동작은 *Probabilistic Scheme*에 부합된다.

V. 결 론

본 논문에서는 BIBD 기반의 멀티미디어 핑거프린팅 코드가 공모자의 공모공격으로 변조되었을 때, 해밍거리를 이용하여 부정자의 추적에 대한 성능측정을 실행하였다. 제안된 해밍거리를 이용한 알고리즘이 기존의 상관관계 계수를 이용한 판정보다 XOR 공격에서 추적성이 있음을 확인하였다.

본 논문에서 사용된 블록설계의 BIBD 기반 핑거프린팅 코드는 v값의 확장에 따라 대규모의 코드장으(code length)로 확장할 수 있으므로 대규모 사용자를 위한 핑거프린팅 코드장에 그대로 적용할 수 있다.

본 논문에서 구현한 해밍거리를 이용한 부정자 추적의 알고리즘은 XOR 공격의 선형문제를 해결할 있으므로 XOR 공모공격에 의한 멀티미디어 콘텐츠의 불법배포자 추적에 응용할 수 있다.

감사의 글

본 연구분야의 선행연구자들이 계셨기에 본 논문을 작성할 수 있어서 그 분들께 경의를 표합니다. 또한 뒤의 보이지 않은 심사위원님들의 소중한 의견으로 본 논문의 완성도를 높일 수 있어서 감사의 마음을 드립니다.

REFERENCES

[1] Minoru Kuribayashi, "Recent Fingerprinting Techniques with Cryptographic Protocol," www.intechopen.com, Signal Processing, Ch. 10, pp. 197-206, 2010.
[2] Min Wu, Wade Trappe, Z. Jane Wang, and K. J.

Ray Liu, "Collusion-resistant fingerprinting for multimedia," *IEEE Signal Processing Magazine*, pp.15-27, Mar. 2004.
[3] Yu-Tzu Lin and Ja-Ling Wu, "Practical fingerprinting system for images," *Optical Engineering* 46(5), 057004, May 2007.
[4] R. Safavi-Naini and Y. Wang, "New results on frame-proof codes and traceability schemes," *IEEE Trans. Inform. Theory*, vol. 47, no. 11, pp. 3029-3033, Nov. 2001.
[5] J. N. Staddon, D. R. Stinson, and R. Wei, "Combinatorial properties of frameproof and traceability codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 3, pp. 1042-1049, Mar. 2001.
[6] D. R. Stinson and R. Wei, "Combinatorial properties and constructions of traceability schemes and frameproof codes," *SIAMJ. Discrete Math.*, vol. 11, pp. 41-53, Feb. 1998.
[7] 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.
[8] Yongdong Wu and Zhigang Zhao, "Collusion attack to a scalable AND-ACC fingerprinting scheme," *Proc. SPIE* 6508, Visual Communications and Image Processing, January 29, 2007.
[9] Block Design, http://mathworld.wolfram.com/BlockDesign.html, 2012.08 참조
[10] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Tran. on Information Theory*, vol. 44, pp. 1897-1905, Sept. 1998.
[11] Kang Hyeon RHEE, "Detection on the Shift Operation of Multimedia Fingerprinting Code using PCA Method," *International Journal of Information Processing and Management*(IJIPM), Vol. 3, No. 2, pp.1-6, April 2012.
[12] Xin Huang and Hongwei Lv, "A C-secure Digital Fingerprinting Scheme Combined with Error-Correcting Code," *Multimedia Information Networking and Security (MINES)*, 2011 Third International Conference on, pp. 297-299, 2011.
[13] Minquan Cheng and Ying Miao, "On Anti-Collusion Codes and Detection Algorithms for Multimedia Fingerprinting," *IEEE Transactions on Information Theory*, Vol. 57, Issue: 7, pp. 4843-4851, 2011.
[14] Yongsheng Yu, Jinshu Cheng, Zhihua Wei and Ruhan He, "A scheme of betrayal checking and traitor tracing for confidential image in Internet," *Measurement, Information and Control (MIC), 2012 International Conference on*, Vol. 2, pp. 572-575, 2012.
[15] Fen Liu, Gui Zhang, "Analysis of Set-cover traitor tracing scheme," *Consumer Communications and Networking Conference (CCNC)*, 2012 IEEE, pp. 512-517, 2012.
[16] Y. Wu, "Linear Combination Collusion Attack and its Application on an Anti-Collusion Fingerprinting," *Proc ICASSP 05*, vol. 2, pp. 13-16, Mar. 2005.
[17] 이강현, "BIBD 기반의 멀티미디어 핑거프린팅 코드의 공모코드들에 대한 공모자 추적," *대한전자공학회, 전자공학회논문지*-CI, 제46권 제6호, pp. 79-86, 2009.
[18] 이강현, "신경망을 이용한 멀티미디어 핑거프린팅의 XOR-ACC 구현," *대한전자공학회, 전자공학회논문지*-CI, 제48권 제6호, pp. 1-8, 2011.
[19] Laarhoven T., Oosterwijk J. and Doumen, J. "Dynamic traitor tracing for arbitrary alphabets: Divide and conquer," *Information Forensics and Security (WIFS), 2012 IEEE International Workshop on*, pp. 240-245, 2012.
[20] Shan He and Min Wu, "Performance Study on Multimedia Fingerprinting Employing Traceability Codes," DIGITAL WATERMARKING, *Lecture Notes in Computer Science*, Vol. 3710/2005, pp. 84-96, 2005.
[21] Jeffrey H. Dinitz and Douglas R. Stinson, "*Contemporary Design Theory: A Collection of Surveys*," Wiley, 1992.

저 자 소 개

정 일 용(정회원)-제1저자
1983년 한양대학교 공학사
1987년 뉴욕시립대학원 공학석사
1991년 뉴욕시립대학원 공학박사 (컴퓨터공학)
<주관심분야 : 네트워크 보안, 코딩이론>

이 강 현(평생회원)
전자공학회 논문지 CI편 2012년 49-4호 참조