논문 2010-47CI-6-1

BCH 코드를 이용한 멀티미디어 핑거프린팅 알고리즘 구현

(An Implementation of Multimedia Fingerprinting Algorithm Using BCH Code)

최 동 민***, 성 해 경**, 이 강 현*

(Dongmin CHOI, Hae Kyung SEONG, and Kang Hyeon RHEE)

요 약

이 논문은 BCH (Bose-Chaudhuri-Hocquenghem) 코드 기반의 멀티미디어 핑거프린팅의 새로운 구현 알고리즘을 나타낸다. 공모자 검출의 평가는 n-1명 까지 이루어진다. 제안된 알고리즘에서, 사용된 공모공격은 논리조합(AND, OR 그리고 XOR) 과 평균화 계산(Averaging)이다. 핑거프린팅 코드의 생성 단계는 다음과 같다.

1, BIBD {7,4,1} 코드는 생기행렬로 생성된다.

2. BIBD 코드와 BCH 코드를 결합한 새로운 인코딩 방법에서, 두 종류의 코드들은 BCH 엔코딩 처리에 의해서 핑거프린팅 코드가 된다.

3. 단계 2에서 생성된 코드는 핑거프린팅 코드가 되며 BCH {15,7}코드와 유사한 특성을 갖는다.

4. 단계 3의 핑거프린팅 코드로, 공모자 검출을 위한 공모 코드북을 만든다.

실험을 통하여 공모자 검출비는 AND 공모에서 86.6%, OR 공모에서 32.8%, XOR 공모에서 0% 그리고 평균화 공모에서 66.4%임을 각각 확인하였다. 또한 XOR 공모는 전체 공모자를 검출할 수 없는 반면에, 평균화 공모는 n-1명의 공모자를 검출하고 OR 공모는 k명의 공모자를 검출할 수 있었다.

Abstract

This paper presents a novel implementation on multimedia fingerprinting algorithm based on BCH (Bose-Chaudhuri-Hocquenghem) code. The evaluation is put in force the colluder detection to n-1. In the proposed algorithm, the used collusion attacks adopt logical combinations (AND, OR and XOR) and average computing (Averaging). The fingerprinting code is generated as below step:

1. BIBD {7,4,1} code is generated with incidence matrix.

2. A new encoding method namely combines BIBD code with BCH code, these 2 kind codes are to be fingerprinting code by BCH encoding process.

3. The generated code in step 2, which would be fingerprinting code, that characteristic is similar BCH {15,7} code.

4. With the fingerprinting code in step 3, the collusion codebook is constructed for the colluder detection.

Through an experiment, it confirmed that the ratio of colluder detection is 86.6% for AND collusion, 32.8% for OR collusion, 0% for XOR collusion and 66.4% for Averaging collusion respectively. And also, XOR collusion could not detect entirely colluder and on the other hand, AND and Averaging collusion could detect n-1 colluders and OR collusion could detect k colluders.

Keywords : Multimedia Fingerprinting code, BIBD code, Collusion Attack, (ACC) Anti-Collusion Code, BCH code

* 평생회원, 조선대학교 전자정보공과대학 전자공학과
(Chosun University, Electronics & Information Engineering College, Dept. of Electronics Eng.)
** 평생회원, 한양여자대학 컴퓨터정보과
(Dept. of Computer Science & Information Systems, Hanyang Women's University)
*** 학생회원, 조선대학교 대학원 컴퓨터공학과
(Chosun University, Graduate School, Dept. of Computer Eng.)
※ 이 논문은 2009년도 조선대학교 학술연구비의 지원을 받아 연구되었음.
접수일자: 2010년9월23일, 수정완료일: 2010년10월25일

Ⅰ. Introduction

It would observe an enormous growth about a use and distribution of multimedia content in Internet, and an illegal copy and redistribution of multimedia content are also increased with a serious proclivity for a wrongdoer.

Multimedia fingerprinting is a technology for copyright protection of content's creators. It is a process of insertion in a distinct set of marks into a given host signal to produce a set of fingerprinted signals that each appears identical to use. If an illegal copy is detected, it's possible to trace the dishonest users. However, colluders may get together comparing their copies and make a new copy to avoid being incriminated, known as collusion attack [1].

For the multimedia content protection, BIBD code was used for multimedia fingerprinting. BIBD code satisfies the characteristics of ACC (Anti-Collusion Code), so the application of BIBD code on the fingerprinting code was progressed in many researches[2~9]. The BIBD matrix is modified to form fingerprinting codes that had collusion resistant, even if all the users attend collusion[2]. And ACC was proposed to accommodate more users while providing collusion-resistance[9].

In author's recent investigation on multimedia fingerprinting code[10], the author totally consider to generate anti-collusion code against the attacks of AND, OR, XOR and Averaging operation.

The coded fingerprinting allows for a much more efficient detection than non-coded orthogonal fingerprinting[11], but it has rather limited collusion resistance[12].

The majority construction of fingerprinting code is based on BIBD matrix[13] and ACC based on BIBD is proposed[9]. Fingerprinting watermark insertion and detection algorithm can protect IPR (Intellectual Property Rights) by inserting a unique digital signature on single digital content.

In this paper, a new encoding method namely combines BIBD code with BCH code, these 2 kind codes are to be fingerprinting code by BCH encoding process for the colluder detection to n-1 according to the structured colluder codebook.

The rest of the paper is organized as follows. In Section Ⅱ, the theoretical background of BIBD characteristic and BCH code are introduced, and the generation algorithm of fingerprinting code is proposed in Section Ⅲ. Then in Section Ⅳ, the range of colluder detection by 4 kinds of collusion code was computed and evaluated. Lastly, the conclusion is drawn in Section Ⅴ.

Ⅱ. Theoretical Background

2.1 BIBD Characteristics

In this section, the BIBD code characteristics are briefly introduced as for a requirement of multimedia fingerprinting code. Multimedia fingerprinting is content's security technology based on watermarking technology. To improve the weak point that illegal content distribution process remains an unknown, fingerprinting technology has been being researched[4, 19~20].

Compounding a problem of BIBD code, which is using a matrix model to produce code satisfied with constraints[7].

Where v: number of processed.
k: number of processing contained in one block.
b: number of blocks.
r: number of repetition of each processing ($k<v$).
λ: number of blocks that each processed pair appears in.

5 parameters are satisfying following two limitation conditions.

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

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

BIBD is simply able to express with $\{v,k,\lambda\}$.

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

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

$b=v$ or $r=k$ then BIBD is symmetrical.

If $X = \{X_i\}_{i=1}^{v}$ and $A = \{A_j\}_{j=1}^{b}$, then BIBD's incidence matrix becomes matrix M as Eq. (5).

$$m_{ij} = \begin{cases} 1 \; if & x_i \in A_j \\ 0 & otherwise \end{cases} \tag{5}$$

Therefore, M satisfies Eq. (6).

$$\mathbf{M}\mathbf{M}^{t} = (\gamma - \lambda)I + \lambda J \tag{6}$$

The reader can be find more specific information in [18].

All row vectors of the incidence matrix M in BIBD became a multimedia fingerprinting code and then authorize users. This M can be used like ACC, which is presented in (7).

M =

m_{ij}	b_1	b_2	b_3	b_4	b_5	b_6	b_7
v_1	0	1	0	1	0	1	0
v_2	1	0	0	1	1	0	0
v_3	0	0	1	1	0	0	1
v_4	1	1	1	0	0	0	0
v_5	0	1	0	0	1	0	1
v_6	1	0	0	0	0	1	1
v_7	0	0	1	0	1	1	0

(7)

For example, BIBD code for multimedia fingerprinting is also appeared in (7). when $\{v,k,\lambda\}$ are {7,4,1}. This code requires 7bits for 7 users and 1-resiliency since any two column vectors share a unique pair of 1 bit.

In Eq. (7), v_n's row vector(n=1~7) will be *User n*'s fingerprinting code for his purchased media content.

2.2 BCH Code

For the generation of BCH code, a parity check code against an information code can be expressed as polynomial. The information width is 7bits. By adding 8 parity bits, the code length is 15bits. Then, we call BCH {15,7} system. The BCH {15,7} can correct 2bit errors in 15bits code.

Assume the 7bits information is $\{i_0, i_1, i_2, i_3, i_4, i_5, i_6\}$, then polynomial notation can be used to show the information such as Eq. (8). Here, the bit position n from 0 to 7 corresponds to the power of x such as $x^{n[14\sim15]}$.

$$I(x)=i_0+i_1 \cdot x^1+i_2 \cdot x^2+i_3 \cdot x^3+i_4 \cdot x^4+i_5 \cdot x^5+i_6 \cdot x^6 \tag{8}$$

Then 15bits code can express as Eq. (9).

$$\begin{aligned} SB(x)=&i_0 \cdot x^8+i_1 \cdot x^9+i_2 \cdot x^{10}+i_3 \cdot x^{11}+i_4 \cdot x^{12}+i_5 \cdot x^{13} \\ &+i_6 \cdot x^{14}+p_0+p_1 \cdot x^1+p_2 \cdot x^2+p_3 \cdot x^3+p_4 \cdot x^4+p_5 \cdot x^5 \\ &+p_6 \cdot x^6+p_7 \cdot x^7 \end{aligned} \tag{9}$$

$p_0,p_1,\cdots,p_7$ bits are 8bits parity. These parity coefficients are 0 to 7th power of x. And information coefficients are 8 to 14th power of x. Then once it calculates $P(x)$, $SB(x)$ is easily obtained.

$$\begin{aligned} P(x)=&p_0+p_1 \cdot x^1+p_2 \cdot x^2+p_3 \cdot x^3+p_4 \cdot x^4+p_5 \cdot x^5 \\ &+p_6 \cdot x^6+p_7 \cdot x^7 \end{aligned} \tag{10}$$

In BCH code, $P(x)$ is remainder of $I(x) \cdot x^8$ divided by $G(x)$.

$$\begin{aligned} I(x)=&i_0 \cdot x^8+i_1 \cdot x^9+i_2 \cdot x^{10}+i_3 \cdot x^{11}+i_4 \cdot x^{12}+i_5 \cdot x^{13} \\ &+i_6 \cdot x^{14} \end{aligned} \tag{11}$$

$$G(x)=1+x^4+x^6+x^7+x^8 \tag{12}$$

Here, $G(x)$ is called as the generation polynomial.

$I(x) \cdot x^8$ in Eq. (11) means the coefficients $i_0,\cdots,i_6$ are shift to higher bit by 8bits. The order of $G(x)$ is 8. The remainder $P(x)$ will be order of 7 or less. However, the calculation uses Galois field rule.

In reality, the remainder calculation is very easy. Using the Eq. (13) iteratively, polynomial with order more than 8 can be reduced to less than 7. The result of polynomial is the remainder polynomial.

$$x^8=1+x^4+x^6+x^7 \tag{13}$$

Remember the generator polynomial of Eq. (12) is

used in BCH {15,7} encoding.

Since $SB(x)$ is defined as Eq. (9), $SB(x)$ can be divided by $G(x)$, in other words, remainder is 0. Then we can judge if the remainder is 0, no error exists in a code. Actually, BCH {15,7} can correct 2bit errors in 15bits codes.

The generator polynomial $G(x)$ can be obtained as shown in Eq. (14).

$$G_1(x)=1+x+x^4, \quad G_2(x)=1+x+x^2+x^3+x^4$$
$$G(x)= G_1(x)\cdot G_2(x) \tag{14}$$

Then, $SB(x)$ can be divided by either $G_1(x)$ or $G_2(x)$. If no error in a code, both remainder of $G_1(x)$ and $G_2(x)$ are both 0s.

Here it defines Syndrome $S_1(x)$=remainder of $SB(x)$ divided by $G_1(x)$, Syndrome $S_2(x)$=remainder of $SB(x)$ divided by $G_2(x)$. According to $S_1(x)$ and $S_2(x)$, error status can be obtained.

Ⅲ. PROPOSED THE GENERATION OF FINGERPRINTING CODE

Multimedia fingerprinting is an up-and-coming technology to identify the content creator and protect copyright about illicit copy and distribution, and can trace a colluder and the distributed path.

In this paper, the generation of multimedia fingerprinting code that is based on BCH code. Each code of media creator, provider and user must not know each other to be inserted to media content. In this paper, a creator code $G_1(x)$ and a provider code $G_2(x)$ of media content is given in Fig. 1.

In Eq. (14), $G_1(x)$ and $G_2(x)$ is becoming $G(x)$ by convolution, $G(x)$ is to be BCH encoder's parity bit. And BIBD code is to be BCH encoder's information code.

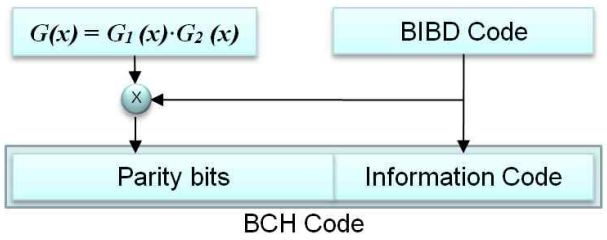

그림 1. 제안된 핑거프린팅 코드의 포맷
Fig. 1. The format of proposed fingerprinting code.

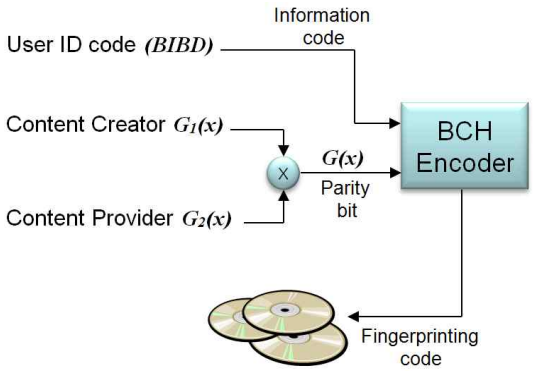

그림 2. 제안된 핑거프린팅 코드의 생성
Fig. 2. The generation of proposed fingerprinting code.

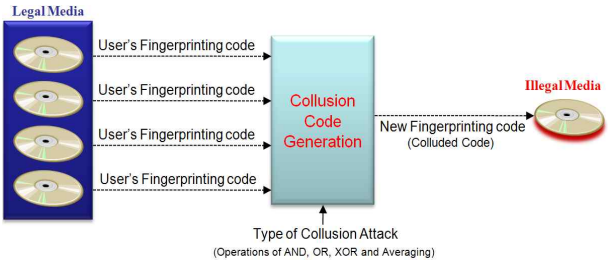

그림 3. 공모코드의 생성
Fig. 3. The generation of collusion code.

In Fig. 1, the generated BCH code is transformed into fingerprinting code for the user of media content. This progress is shown in Fig. 2.

Some users generate a collusion code with their fingerprinting code that is inserted in legal media according to the type of collusion attacks such as, the operation of AND, OR, XOR and Averaging.

In Fig. 4, a fingerprinting code of media content is transferred to BCH decoder. This fingerprinting code is used for generating syndrome code through BCH decoding process. As a result, if the value of syndrome code S_1 and S_2 is '00' both, the fingerprinting code of media content is a right user's code. However if the value of S_1 and S_2 is not '00', then the fingerprinting code is collusion code① which would be searched in the collusion codebook in Fig. 5. And also, the attending colluder④ would be traced by value of S_1 and S_2 ② and collusion attack type③ in the collusion codebook.

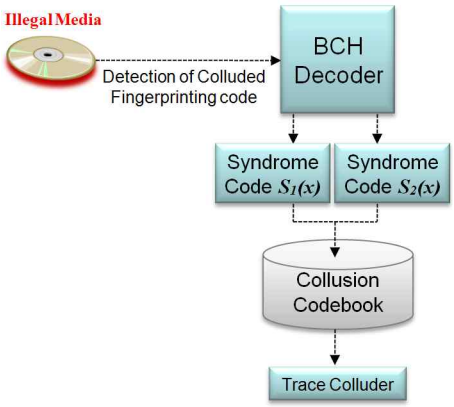

그림 4. 공모된 핑거프린팅 코드의 검출과 공모자 추적
Fig. 4. The detection of colluded fingerprinting code and the trace of colluder.

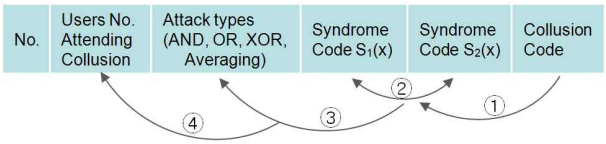

그림 5. 공모 코드북의 포맷
Fig. 5. The format of the collusion codebook.

Ⅳ. EXPERIMENTAL RESULT

For experiment of the proposed algorithm, it assigns (1 0 0 1 1) into G_1 for the creator and (1 1 1 1 1) into G_2 for the provider, and generates the generator polynomial by $G_1(x)\cdot G_2(x)$ for BCH code. And user code i that using BIBD matrix row vector of (7) and $G(x)$ which is (1 1 1 0 1 0 0 0 1) generate BCH code. The multimedia fingerprinting code using BCH encoding is shown in Fig. 6.

In the theoretical collusion attack, BCH {15,7} code able to make 119 numbers of collusion codes, and n-1

User 1 : (0 1 0 1 0 1 0 0 0 0 1 1 0 1 0)
User 2 : (1 0 0 1 1 0 0 0 0 0 1 0 0 1 1)
User 3 : (0 0 1 1 0 0 1 1 1 1 1 0 1 1 0)
User 4 : (1 1 1 0 0 0 0 1 0 1 0 0 1 1 0)
User 5 : (0 1 0 0 1 0 1 0 1 0 0 0 0 1 1)
User 6 : (1 0 0 0 0 1 1 0 1 0 0 1 0 1 0)
User 7 : (0 0 1 0 1 1 0 1 0 1 0 1 1 1 1)

그림 6. BCH {15,7} 엔코딩을 이용한 멀티미디어 핑거프린팅 코드
Fig. 6. Multimedia fingerprinting code using BCH {15,7} encoding.

or fewer users have attended with collusion attack.

The evaluation algorithm of the collusion code which are generated by Logical combinations (AND, OR and XOR) and Averaging operation for the colluder detection to n-1. And also the colluded collusion code will be defined as the usable or useless attack codes.

According to the collusion attack type, the number of detected colluders is presented in Table 1 and also, the detected colluders by number of attending colluders (2~6) and the ratio of colluder detection is presented. In the experiment of the proposed algorithm, it confirmed that the ratio of colluder detection is 86.6% for AND collusion, 32.8% for OR collusion, 0% for XOR collusion and 66.4% in Averaging collusion respectively. It is shown in Table 1 and Fig.7. In Table 2, XOR collusion could

표 1. 검출된 공모자들과 공모 검출비의 실험결과
Table 1. Experimented results of detected colluders and the ratio of colluder detection.

Collusion Attack Type	Detected Colluders	Detected Colluders by Number of Attending Colluders.					Ratio of Colluder Detection
		2	3	4	5	6	
AND	103	9	31	35	21	7	86.6%
OR	39	9	24	6	0	0	32.8%
XOR	0	0	0	0	0	0	0%
Averaging	79	9	15	30	18	7	66.4%

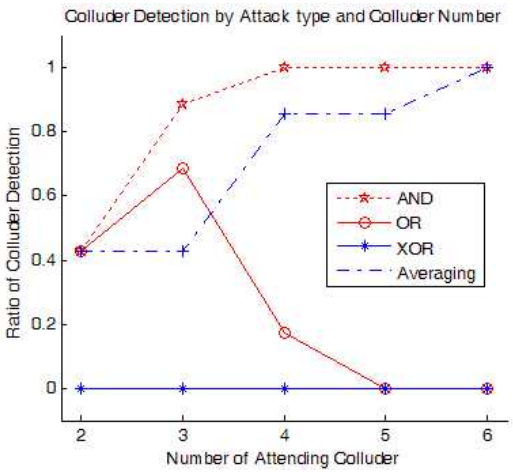

그림 7. 공모공격 타입에 의한 공모자들 검출과 공모자의 수
Fig. 7. Colluder detection by collusion attack type and colluder number.

표 2. 기존의 핑거프린팅 스킴과 본 논문의 검출된 공모자들 수의 비교(n과 k는 BIBD의 파라메터)
Table 2. Comparison of the number of detected colluders between the conventional fingerprinting schemes and this paper.(n and k in here: BIBD parameter)

Fingerprinting Schemes	Method	Number of Detected Colluders.
Dittman[17]	d-detecting	2
Boneh [13]	c-secure	2
Trappe [9]	AND ACC	2
Domingo_Ferrer [16]	3-secure	3
Multimedia Fingerprinting based on BCH code, in this paper.	**AND and Averaging Attacks**	***n*-1**
	OR Attacks	***k***

not detect entirely colluder. On the other hand, AND and Averaging collusion could detect n-1 colluder and OR collusion could detect k colluder. The experimental results are compared the conventional schemes[9, 13, 16~17] in Table 2.

V. Conclusion

In the examination, XOR collusion type is entirely useless. On the other hand, AND and Averaging collusion types have the better detection rate comparing to other conventional schemes, and OR collusion shows good performance relatively.

The proposed algorithm in this paper could be widely applied to trace up the illegal distributor of multimedia content on the various colluded attacks, which consisted of Logical operation and Averaging of fingerprinting code base on BIBD code combined with BCH code.

표절논문 인용주의

{**"유비쿼터스 네트워크 시스템에서의 미디어 보안에 관한 연구," 한국사이버테러정보전학회, [7권 1호-04], pp. 29-34, 2007.3**}은 참고문헌 [6]을 표절한 논문으로 이를 인용할 시에 주의를 요합니다.
참조: http://paper.chosun.ac.kr (원저자 및 선임변호사)

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.

REFERENCES

[1] Jie Yang, Xiaoxia Xu, "A Robust Anti-collusion Coding in Digital Fingerprinting System," The 8th International Conference on Signal Processing, Vol. 4, 2006.
[2] 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.
[3] 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.
[4] Zang Li and Trappe W, "Collusion-resistant fingerprints from WBE sequence sets," IEEE International Conference on Communications, ICC 2005, Vol. 2, pp. 1336-1340, 16-20 May 2005.
[5] 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.
[6] J. S. Noh, Kang Hyeon RHEE, "Detection of Colluded Multimedia Fingerprint by Neural Network," IEEK Computer Society, Vol. 43, No. 4, pp. 80~87, July 2006.
[7] Kang Hyeon RHEE, "Detection of Colluded Multimedia fingerprint using LDPC and BIBD," IEEK Computer Society, Vol. 43, No. 5, pp. 68~75, Sept. 2006.
[8] 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.
[9] 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.
[10] Kang Hyeon RHEE, "An Evaluation Algorithm of Multimedia Fingerprinting using BIBD code," APIC-IST & ICONI 2009, pp. 411-415, Dec. 2009.
[11] Z. J. Wang, M.Wu, H. Zhao,W. Trappe, and K.J.R. Liu, "Resistance of Orthogonal Gaussian Fingerprints to collusion Attacks," *Proc. of ICASSP*, pp. 724-727, Apr. 2003.
[12] Shan He andMin Wu, "Performance Study on Multimedia Fingerprinting Employing Traceability Codes," Vol. 3710/2005, pp. 84-96, 2005.
[13] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Tran. on Information Theory*, Vol. 44, pp. 1897-1905, September 1998.
[14] http://www.lsi-contest.com/index_e.html
[15] http://www.lsi-contest.com/shiyou_2e.html
[16] F. Sebe and Domingo-Ferrer, "Short 3-Secure Fingerprinting Codes for Copyright Protection," Lecture Notes in Computer Science, Vol. 2384, pp. 316-327, 2002.
[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] http://mathworld.wolfram.com/BlockDesign.html
[19] 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.
[20] 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)-제1저자
대한전자공학회논문지,
제47권 CI편 제1호 참조

성 해 경(평생회원)-교신저자
현재 한양여자대학 컴퓨터정보과 교수

최 동 민(학생회원)
현재 조선대학교 대학원 컴퓨터공학과 박사과정