

# 불법 복제 추적을 위한 영상 워터마킹 알고리즘 설계

이진홍<sup>†</sup>, 한승우<sup>†</sup>, 박지환<sup>†</sup>

<sup>†</sup>부경대학교 대학원 정보보호학과

<sup>†</sup>부경대학교 대학원 전자계산학과

## Design of Image Watermarking Algorithm for Illegal Copy Tracing

Jin-Heung Lee<sup>†</sup>, Seung-Wu Han<sup>†</sup>, Ji-Hwan Park<sup>†</sup>

<sup>†</sup> Interdisciplinary Program of Information Security, Pukyong Nat'l University

<sup>†</sup> Department of Computer Science, Pukyong Nat'l University

### 요약

디지털 평거프린팅은 컨텐츠 유통 시, 구매자의 정보를 컨텐츠에 삽입함으로써 불법 유통 행위된 컨텐츠에 대하여 불법 배포자를 추적할 수 있는 기법이다. 이러한 평거프린팅 코드는 워터마크 기술로서 컨텐츠 내에 삽입되어지고, 공모 공격(collusion attacks)등과 같이 불법적인 제거 공격으로부터 삽입된 정보가 안전하게 유지되어야 한다. 본 논문에서는 효율적이고 공모 공격에 강인한 평거프린팅 코드를 구성하고, MPSK(M-ary Phase Shift Keying) 워터마킹 기술을 이용하여 안전하게 삽입, 추출하는 알고리즘을 제안한다. 제안 방법은 다양한 영상 데이터에 적용하여 공모 공격 및 기타 영상 처리에 대한 안전성을 확인하였다.

### 1. 서론

디지털 워터마킹 기술은 멀티미디어 저작물을 보호하기 위하여 특정 형태의 워터마크 정보(저작권 정보, 로고, 일련번호 등)를 원 데이터에 감추고 추출하는 모든 기술적 방법을 말한다. 초기에는 원래의 멀티미디어 데이터 자체의 조작으로 워터마크 정보를 은닉시키는 방법이 개발되다 현재에는 많은 기술적 변환 방법을 이용하여 강인한 워터마킹 기술이 개발되고 있다[1].

디지털 평거프린팅 기술은 워터마킹의 확장 기술로 컨텐츠의 상거래 시 소유자의 정보뿐만 아니라 구매자의 정보도 포함하는 평거프린팅 정보를 컨텐츠에 삽입하여 불법 배포가 어느 구매자로부터 시작되었는지 추적할 수 있도록 해주는 기술이다[2,3]. 디지털 평거프린팅 기술은 고유한 저작권 정보를 삽입하여 소유권 분쟁의 증거로 활용하는 디지털 워터마킹과는 달리 복수개의 워터마크를 평거프린팅 코드로 삽입해야 한다. 따라서, 다수의 사용자에 의한 공모 공격이 가능하게 된다.

이와 같은 공모 공격에 대한 대책으로 Dittmann은 사영 평면(projective plane)을 바탕으로 공모 공격에

강인한 평거프린팅 코드를 생성하고 이것을 영상에 적용하였다[4]. 이 방법은 3명의 배포자중 2명이 서로 공모하였을 때 공모자를 추출 가능하다. 또한, 유한 사영 기하학을 기반으로 하여 공모자가 d명일 때 모든 공모자를 검출할 수 있는 d-detecting 코드를 제안하였다. 그러나, 이 방법에서는 구매자의 증가에 따른 사영평면 구성의 어려움으로 구매자 수에 제한을 받는 문제점을 가지고 있다. 또한, Trappe와 Wu는 BIBD(Balanced Incomplete Block Design)를 이용하여 멀티미디어 데이터를 위한 ACC(Anti-Collusion Code)를 이용하여 공모자를 검출할 수 있는 알고리즘을 제안하였다[5].

이러한 방법들은 2,3명의 사용자들이 공모하여 만든 컨텐츠로부터 최소 한 명의 공모자를 추출하기 위한 방법이다. 이러한 코드의 단점은 구매자가 많아질수록 필요로 하는 코드의 길이가 기하급수적으로 증가하기 때문에 구매자가 많은 인터넷 환경에서는 적용이 매우 어렵게 된다. 또한 코드의 형태도 단순하여 공격자에 의해 쉽게 예측 가능한 문제점을 가지고 있다.

본 논문에서는 새로운 평거프린팅 코드 생성 방법을 제안하고, 제안된 방법에 적용 가능한 워터마킹 알고리즘을 설계하였다. 논문의 구성은 2장에서 공모 공

격에 강인한 평거프린팅 알고리즘을 제안하고, 3장에서 평거프린팅 코드에 적용 가능한 워터마킹 알고리즘을 제시한다. 그리고, 4장에서 제안 방법에 대한 실험적 평가에 의한 안전성을 검토하고, 끝으로 향후 연구 방향에 대하여 기술한다.

## 2. 공모 공격에 강인한 평거프린팅 알고리즘

디지털 평거프린팅 코드는 일반적으로 합법적인 사용자와 불법적으로 유통한 사용자를 정확하게 검출하여야 하고, 다른 시스템 내에서 효율적으로 수행가능해야 한다. 그리고, 완벽한 저식이 없는 공격자들에 의해 삭제 및 변경이 어려워야 하며, 불법 배포된 컨텐츠의 작은 부분에서도 배포자를 구분 가능해야 한다. 이러한 전제 조건을 만족시키기 위해서 원시 다항식에 의한 trace의 순환 수열을 이용한 효율적이고 공모 공격에 강인한 평거프린팅 코드를 구성한다.

### 2.1 원시 다항식

주어진 다항식  $f(x)$ 에 대하여 인수분해 가능한 경우와 인수분해 불가능한 다항식이 있을 때  $m$ 차인 인수분해 불가능한 다항식으로서  $x^n+1 (n=2^m-1)$ 은 나눌 수 있고,  $x^i+1 (1 < i < 2^m-1)$ 은 나눌 수 없을 때, 이때의 다항식을 원시 다항식이라 한다. GF(2)상의 벡터공간 GF( $2^m$ )은 원시 다항식으로 정의될 수 있으며, 다음식(1)과 같이 표현된다.

$$p(x) = x^m + p_{m-1}x^{m-1} + \cdots + p_1x + p_0 \quad (p_i \in GF(2), 0 \leq i \leq m-1)$$

표준 기저에서 기저 벡터는  $\alpha^0, \alpha^1, \dots, \alpha^m$ 이고, 이 때의  $\alpha$ 를 원시 다항식의 근으로서 필드의 원시 원소(primitive element)라 한다. 어떠한 GF( $2^m$ )상의 원소 A도 식(2)로 나타낼 수 있으며, 원시 원소를 이용하여 A를 식(3)과 같은 다항식으로 표현할 수 있다. 즉, GF(2)상의  $m$ 차원 벡터로서  $\{a_0, a_1, \dots, a_m\}$ 로 나타낼 수 있다.

$$A = a_0\alpha^0 + a_1\alpha^1 + \cdots + a_{m-1}\alpha^{m-1} \quad (2)$$

$$(a_i \in GF(2), 0 \leq i \leq m-1)$$

$$A(x) = a_0x^0 + a_1x^1 + \cdots + a_{m-1}x^{m-1} \quad (3)$$

### 2.2 trace

$F=GF(q)$ ,  $K=GF(q^n)$ 이라고 두면, 아래의 정리에 의해  $K$ 의 서브필드로서  $F$ 를 볼 수 있다. 만일  $\alpha$ 가  $K$ 의 요소라면, 서브필드  $F$ 에 대한 trace relative는 식(4)와 같이 규정할 수 있다[6].

$$Tr_K^F(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}} \quad (4)$$

정리.  $n$ 의 모든 약수  $d$ 에 의해,  $GF(p^n)$ 은 정확하게 1개의  $GF(p^d)$ 와 동형의 서브필드를 포함한다.

원시 다항식  $p(x)=x^4+x+1$ 에 대하여, 원시 원소와 trace를 구하면 표1과 같다.  $GF(q)$ 에서 원의 수  $q$ 를 order라 부르며, 여기에서  $ord(\alpha)$ 는 ' $2^m$  원소의 총

개수-1'의 약수로 정의된다.

### 2.3 공모 공격에 강인한 평거프린팅 코드 구성

공모 공격에 강인한 평거프린팅 코드 구성은 다음과 같은 절차에 의해 이루어진다.

① 주어진 원시 다항식  $p(x)$ 에 대하여 근  $\alpha$ 를 구한다.

②  $\alpha$ 로부터 trace를 계산한다.

$$\bullet Tr(\alpha) = 1 + 1 + 1 + 1 = 0$$

$$\bullet Tr(\alpha^2) = \alpha + \alpha^2 + \alpha^4 + \alpha^8 = \alpha + \alpha^2 + \alpha^4 + \alpha^8 \\ = 0$$

$$\bullet Tr(\alpha^4) = \alpha^2 + \alpha^4 + \alpha^8 + \alpha^{16} = \alpha^2 + \alpha^4 + \alpha^8 + \alpha^1 \\ = 0$$

.....

$$\bullet Tr(\alpha^{14}) = \alpha^{14} + \alpha^{14^2} + \alpha^{14^4} + \alpha^{14^8} \\ = \alpha^{14} + \alpha^{13} + \alpha^{11} + \alpha^7 = 1$$

[표 1] GF( $2^4$ )의 원시 다항식  $p(x)=x^4+x+1$

$i$	$\alpha^i$	다항식표현	벡터표현	$ord(\alpha^i)$	$Tr(\alpha^i)$
0	$\alpha^0$	1	0001	1	0
1	$\alpha^1$	$\alpha$	0010	15	0
2	$\alpha^2$	$\alpha^2$	0100	15	0
3	$\alpha^3$	$\alpha^3$	1000	5	1
4	$\alpha^4$	$\alpha+1$	0011	15	0
5	$\alpha^5$	$\alpha^2+\alpha$	0110	3	0
6	$\alpha^6$	$\alpha^3+\alpha^2$	1100	5	1
7	$\alpha^7$	$\alpha^3+\alpha+1$	1011	15	1
8	$\alpha^8$	$\alpha^2+1$	0101	15	0
9	$\alpha^9$	$\alpha^3+\alpha$	1010	5	1
10	$\alpha^{10}$	$\alpha^2+\alpha+1$	0111	3	0
11	$\alpha^{11}$	$\alpha^3+\alpha^2+\alpha$	1110	15	1
12	$\alpha^{12}$	$\alpha^3+\alpha^2+\alpha+1$	1111	5	1
13	$\alpha^{13}$	$\alpha^3+\alpha^2+1$	1101	15	1
14	$\alpha^{14}$	$\alpha^3+1$	1001	15	1

③ trace를 이용한  $2^m-1 \times 2^m-1$  순환수열 M을 생성한다.

$$M = \begin{pmatrix} 0001001101011111 \\ 0010011010111110 \\ 0100110101111100 \\ 1001101011111000 \\ 0011010111110001 \\ 0110101111100010 \\ 1101011111000100 \\ 1010111110001001 \\ 0101111000100111 \\ 1011110001001110 \\ 0111100010011101 \\ 1111000100111010 \\ 1110001001110101 \\ 1100010011101011 \\ 1000100110101111 \end{pmatrix} \quad (5)$$

④ 생성된 M으로부터 각 행의 수열을 평거프린팅 정보로서 유통될 컨텐츠에 삽입한다.

### 3. 평거프린팅 코드에 적용 가능한 워터마킹 알고리즘 설계

대역 확산을 이용한 워터마킹 기술은 기존의 디지털 통신에서 많이 쓰이는 Pseudo-Noise Sequence를 이용하여 워터마크 정보를 확산시켜서 컨텐츠 내에 삽입하게 된다. 워터마크 정보는 확산되어 삽입되므로 쉽게 암호화할 수 있고, 삽입되는 신호의 에너지를 주파수 전대역으로 확산함으로써 청각적으로 들리지 않는 작은 신호로 삽입하게 되고 쉽게 검출할 수 있게 된다[7,8].

본 논문에서는 삽입될 평거프린팅 정보를 PN sequence를 이용한 대역 확산 방법에 의해 삽입하고 검출하는 알고리즘을 제안한다. PN sequence에 의해 삽입된 평거프린팅 정보는 컨텐츠 내의 백색잡음과 같은 노이즈로 생각할 수 있다. 평거프린팅 정보는 삽입 과정시, 주파수 영역에서 변형 및 삽입되기 때문에 PN sequence의 특성을 그대로 유지하면서 시각적인 효과를 최대화 하였다.

#### 3.1 MPSK을 이용한 워터마킹 삽입 기술

PSK(Phase Shift Keying)는 신호의 위상차를 이용하여 다양한 전송 속도를 제공하는 통신 기술이다. 무선 통신에서는 PSK 혹은 Binary PSK의 확장된 개념인 QPSK(Quadrature PSK)가 많이 사용된다. BPSK가 1과 0의 두 가지 신호만을 구분하는데 반해, QPSK는 4가지의 디지털 신호를 구분한다. 따라서, 전송 가능한 신호는 (00, 01, 10, 11)의 2bit 디지털 신호이므로 같은 시간 내에 2배의 데이터를 전송할 수 있는 기술이다.

MPSK는 BPSK와 QPSK를 포함한 것으로 M 만큼 신호의 레벨을 가지는 방법이다. 예를 들어, 16단계로 양자화된 신호를 한번에 보내려면 적어도 16가지의 신호좌표를 가진 multilevel signaling 변조를 해야 한다. 이러한 경우에는 하나의 반송파 신호를 16가지의 위상차를 두어 서로 구분되는 신호를 보내는 16 PSK를 이용할 수 있다. MPSK에서 M=2인 경우, 두 종류의 신호를 사용하므로 BPSK가 되고, M=4인 경우 QPSK가 된다[9].

제안 기술에서는 워터마크 시퀀스에 대하여 MPSK 방식을 적용한 MPSK 워터마킹 알고리즘을 이용한다. MPSK를 이용한 워터마크  $w$ 는 다음 식(6)과 같이 구성된다.

$$w = \begin{cases} S_{128 \cdot i + j}, & 0 \leq j \leq 127 \text{ (if } b_i = 1\text{)} \\ S_{128 \cdot (i+1) - j}, & 0 \leq j \leq 127 \text{ (if } b_i = 0\text{)} \end{cases} \quad (6)$$

여기서,  $b_i$ 와  $S$ 는 각각 삽입될 평거프린팅 정보와 PN-시퀀스를 나타낸다. 각 사용자는 서로 다른 평거프린팅 코드  $b_i$ 에 의해 변경된 PN-시퀀스를 워터마크 정보로써 컨텐츠에 삽입한다.

#### 3.2 평거프린팅 코드 추출 알고리즘

평거프린팅 추출 과정은 두 가지로 구성된다. 먼저 삽입한 워터마크 시퀀스  $S'$ 를 검출한다. 본 논문에서  $S'$ 의 검출은 원본을 이용한 방법을 적용하였다. 그리

고, 검출된 시퀀스로부터 삽입시 사용한 PN sequence 와의 위상차에 따른 상관도를 이용하여 삽입된 평거프린팅 코드를 추출하게 된다.

다음 식(7)은 예측된 워터마크 정보와 삽입한 PN-시퀀스 정보를 이용하여 각각의 위상차에 따른 상관계수(cross correlation)를 구하는 식을 나타내고 있다.

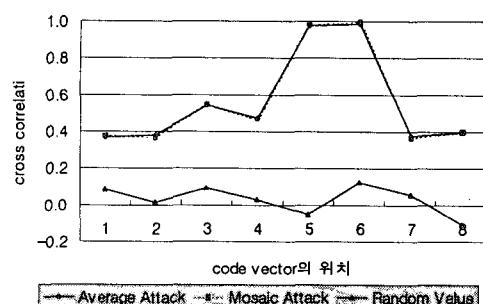
$$\text{Corr}_{[n, n]}[n] = \frac{1}{k} \sum_k S_{[128 \cdot n + k]} \cdot S_{[128 \cdot n + k]}, \quad 0 \leq k \leq 127$$

여기에서  $n$ 은 삽입된 평거프린팅 코드 길이를 나타내며, 코드 길이와 삽입 블록의 크기 그리고 위상을 변경할 PN-시퀀스의 길이는 trade-off 관계를 가진다.

### 4. 제안 방식에 대한 실험 결과

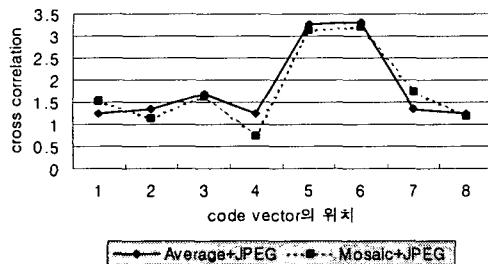
제안 방식에 대하여 5개 영상(Lenna, Barbara, Boat, Cameraman, Bridge)을 대상으로 평거프린팅 정보를 삽입하고, 압축 및 공모 공격을 시도하여 삽입된 평거프린팅 정보를 추출 하였다. 평거프린팅된 영상들의 PSNR은 38dB 이상 유지하도록 워터마크 삽입 강도를 고정함으로써 시각적으로 차이점을 느낄 수 없게 하였다. 3차 원시 다항식  $x^3 + x + 1$ 를 이용하여 평거프린팅 정보를 생성하고, 각각을 서로 다른 사용자에게 분배하였다. 평거프린팅 코드는 3차의 원시 다항식에 의해 생성된 순환수열 M의 각 행벡터와 동기비트 1비트로 구성된 코드 벡터(code vector)로 이루어진다. 다음은 사용자1(User1)과 사용자2(User2)에게 할당된 평거프린팅 코드 벡터를 나타내고 있다. 여기서, Average 코드 벡터는 두 명의 공모자가 자신의 정보가 삽입된 컨텐츠를 평균하여 새로운 컨텐츠를 생성하였을 때, 컨텐츠 내에 변경된 코드 벡터를 나타낸다. 따라서, 공모 공격이 이루어진 컨텐츠 내의 코드 벡터로부터 두 명의 공모자를 정확하게 검출할 수 있다.

- User1 : { 0 0 1 0 1 1 1 0 }
- User2 : { 0 1 0 1 1 1 0 0 }
- Average : { 0 0 0 0 1 1 0 0 }



[그림1] 두 명의 공모자에 의해 공모 공격이 이루어진 파일에 대한 상관도 검출

제안된 평거프린팅 코드는 두 개의 서로 다른 평거프린팅된 영상으로부터 공모 공격을 시도하였을 때 두 명의 공모자를 검출할 수 있다. 그림1은 두 명의 공모자 사용자1과 사용자2에 의해 공모된 영상으로부터 삽입된 평거프린팅 코드의 검출 결과를 나타내고 있다. 그림과 같이 공모 공격이 이루어진 영상으로부터 삽입된 워터마크의 상관 계수는 모두 0.3 이상을 나타내고 있으며 공모한 사용자를 규정하는 공통의 위치 벡터의 상관도는 0.9 이상의 높은 상관도를 나타낸다. 따라서, {00001100}과 같이 5번째와 6번째의 평거프린팅 코드가 공통으로 1을 가지는 두 명의 사용자가 공모한 것임을 알 수 있고, 각각의 사용자에게 할당된 평거프린팅 코드로부터 {00101110}, {01011100}의 코드 벡터를 가지는 사용자1과 사용자2가 공모 하였음을 알 수 있다.



[그림2] JPEG와 공모 공격을 동시에 수행한 파일에 대한 상관도 검출

일반적으로 인터넷 상에서 사용되는 영상들은 JPEG, GIF 등의 손실 압축된 영상을 사용하게 된다. 따라서 평거프린팅된 영상은 손실 압축에 의해 삽입된 코드의 삭제, 변경되어서는 안된다. 그림2는 제안 방식에 대하여 평균 공격과 모자의 공격을 가한 각각의 영상으로부터 50%의 quality factor에 의한 JPEG 압축한 뒤, 평거프린팅 정보를 검출한 결과를 나타내고 있다.

## 5. 결론

본 논문에서는 공모 공격에 강인한 평거프린팅 코드를 새롭게 생성하고, 생성된 평거프린팅 코드를 효율적으로 삽입할 수 있는 MPSK 워터마킹 알고리즘을 제안하였다. 제안된 평거프린팅 코드는 2명의 불법 유통자에 의한 평균공격 및 모자의 공격과 같은 공모 공격에 대하여 추적 가능함으로 보였다. 또한, 제안된 MPSK 워터마킹 알고리즘은 다수의 평거프린팅 코드를 삽입할 수 있는 효율적인 알고리즘임을 확인할 수 있다. 따라서, 기존의 불법 컨텐츠 추적 시스템에서 문제가 되는 평거프린팅 코드의 길이를 trace의 순환 행렬에 의해 짧고, 쉽게 확장 가능하게 하였다. 또한, 상대적으로 긴 코드 길이를 삽입할 수 있는 워터마킹 알고리즘을 제시함으로써 평거프린팅을 이용한 불법 배포자 추적 시스템 구현을 가능하게 하여 안전한 컨

텐츠 유통 체계를 확립하는데 기여하게 될 것이다.

향후 연구 방향으로는 다수의 불법 유통자에 대하여 공모 공격으로부터 안전한 평거프린팅 코드 구성과 기하학적 공격에 강인한 워터마킹 알고리즘 연구가 진행되어야 한다.

## [참고문헌]

- [1] M. Swanson, M. Kobayashi, A. Tewfik, "Multimedia Data Embedding and Watermarking Technologies," Proc. of IEEE, Vol. 86, No. 6, pp.1064-1087, June. 1998.
- [2] B.Pfitzmann and M.Schunter, "Asymmetric Fingerprinting", EUROCRYPT'96, LNCS 1070, pp.84-95, 1996.
- [3] D.Kirovski, H.S.Malvar, and Y.Yacobi, "Multimedia Content Screening Using a Dual Watermarking and Fingerprinting System", ACM Multimedia, 2002.
- [4] J.Dittmann, A.Behr, M.Stabenau, P.Schmitt, J. Schwenk and J.Ueberberg, "Combining Digital Watermarks and Collusion Secure Fingerprints for Digital Image", SPIE J. Electron. Image, Vol. 9, pp.456-467, 2000.
- [5] W.Trappe, M.Wu, J.Wang, and K.J.Ray Liu, "Anti-collusion Fingerprinting for Multimedia", IEEE Transaction on Signal Processing, Vol. 51, NO. 4, pp.1069-1087, 2003.
- [6] Robert J. MacEliecs, Finite Fields for Computer Scientists and Engineers, Kluwer, 1986.
- [7] L. Boney, A. H. Tewfik and K. N. Hamdy, "Digital Watermarks for Audio Signals", IEEE Proceedings of Multimedia, pp. 473-480, 1996
- [8] I. J. Cox, J. Kilian, T. Leighton and T. Shnmoor, "A Secure, Robust Watermark for Multimedia", Proc. Workshop on Information Hiding, 1996
- [9] Richard B. Wells, Applied Coding and Information Theory for Engineers, Prentic Hall