논문 2006-43CI-4-10

신경회로망에 의한 공모된 멀티미디어 핑거프린트의 검출

(Detection of Colluded Multimedia Fingerprint by Neural Network)

노 진 수*, 이 강 현**

(Jin Soo NOH and Kang Hyeon RHEE)

요 약

최근 인터넷 응용 프로그램과 관련 기술의 발전에 따라 디지털 멀티미디어 콘텐츠의 보급과 사용이 쉬워지고 있다. 디지털 신호는 복제가 용이하고 복제된 신호는 원신호와 동일한 품질을 갖는다. 이러한 문제점을 해결하고 저작권 보호를 위해 멀티미디어 핑거프린트가 연구되어지고 있다. 핑거프린팅 기법은 암호학적인 기법들을 이용하여 디지털 데이타를 불법적으로 재배포한 사용자를 찾아냄으로써 디지털 데이타의 저작권을 보호한다. 핑거프린팅 기법은 대칭적이나 비대칭적인 기법과 달리 사용자만이 핑거프린트가 삽입된 데이타를 알 수 있고 데이타가 재배포되기 전에는 사용자의 익명성이 보장되는 기법이다. 본 논문에서는 신경회로망에 의한 공모된 멀티미디어 핑거프린트의 검출 알고리즘을 제안한다. 제안된 알고리즘은 불법공모방지 코드 생성과 에러정정을 위한 신경회로망으로 구성되어 있다. BIBD(Balanced Incomplete Block Design) 기반의 불법공모방지 코드는 평균화 선형 공모공격에 대해 100% 공모코드 검출이 이루어졌으며, 에러비트 정정을 위해 (n,k)코드를 사용한 홉필드 신경회로망은 2비트 이내의 에러비트를 정정할 수 있음을 확인하였다.

Abstract

Recently, the distribution and using of the digital multimedia contents are easy by developing the internet application program and related technology. However, the digital signal is easily duplicated and the duplicates have the same quality compare with original digital signal. To solve this problem, there is the multimedia fingerprint which is studied for the protection of copyright. Fingerprinting scheme is a techniques which supports copyright protection to track redistributors of electronic information using cryptographic techniques. Only regular user can know the inserted fingerprint data in fingerprinting schemes differ from a symmetric/asymmetric scheme and the scheme guarantee an anonymous before recontributed data. In this paper, we present a new scheme which is the detection of colluded multimedia fingerprint by neural network. This proposed scheme is consists of the anti-collusion code generation and the neural network for the error correction. Anti-collusion code based on BIBD(Balanced Incomplete Block Design) was made 100% collusion code detection rate about the average linear collusion attack, and the hopfield neural network using (n,k)code designing for the error bits correction confirmed that can correct error within 2bits.

Keywords: Fingerprint, Hopfield neural network, BIBD, ACC, Digital copyright

I. 서 론

인터넷의 발달로 정보의 공유 및 배포는 전 세계로 계속 확장되고 있다. 이에 따라 디지털 미디어는 지난 수년간 우리의 생활 속에 깊숙이 침투하여 영상, 비디오, 오디오와 같은 다양한 디지털 콘텐츠의 사용이 급증하였다. 하지만 디지털 콘텐츠는 복제가 용이하고 복제된 디지털 콘텐츠와 원본과의 차이를 구분할 수 없으므로 불법복제와 불법배포도 성행하고 있다. 결국 디지털창작자의 경제적인 손실이 가져옴으로 이를 차단할 수 있는 신뢰성 있고 효율적인 디지털 미디어 보호 방법의 필요성이 증가하고 있다.

이에 따라 디지털 콘텐츠 보호기술이 개발되었다. 디지털 콘텐츠 보호기술은 콘텐츠 제작자의 저작권 관련 정보를 외부공격에 강인하도록 콘텐츠에 삽입하는

* 학생회원, ** 정회원, 조선대학교 전자공학과
(Dept. of Electronic Engineering, Chosun University)
접수일자: 2006년6월5일, 수정완료일: 2006년6월28일

기술로 정의할 수 있으며 이는 크게 워터마킹 기술과 핑거프린팅 기술로 나누어진다. 워터마킹 기술은 디지털 콘텐츠 제작자의 저작권 정보를 워터마크로 변환시켜 비가시적으로 콘텐츠에 삽입하는 기술로써 콘텐츠 제작자의 소유권을 인증할 수 있는 기술이지만 삽입된 워터마크가 다양한 공격에 의하여 손실 및 파괴 되었을 때, 공격자를 추적하는 것이 불가능하다. 즉, 디지털 콘텐츠의 불법 유통 과정을 알 수 없다는 단점이 있다. 이를 해결하기 위하여 멀티미디어 핑거프린팅 기술에 대한 연구가 진행되어지고 있다. 핑거프린팅 기술은 원저작자의 지적재산 권리의 보호와 디지털 창작물의 불법복제 및 배포에 대한 방지책으로, 콘텐츠에 사용자 정보가 삽입되어 각 사용자가 공모하여 다른 복제를 만들 수 있는 공모공격의 문제가 발생되었을 때, 공모 공격자들을 추적하여 검출할 수 있는 콘텐츠 보호기술로 그 기원은 대수표(logarithm table)를 불법복제로부터 보호하기 위하여 사용된 변형 워터마킹(Transactional Watermarking)[1] 으로부터 시작되었다.

디지털 핑거프린팅 기술은 크게 Malvar[2] 등에 의해 제안된 듀얼 워터마킹/핑거프린팅 기법과 삽입코드 자체를 공모 공격이 불가능하도록 설계하는 공모보안코드 개발 기법(collusion secure code)[3~8]으로 나누어진다. 듀얼 워터마킹/핑거프린팅 기법은 저작권을 보호하기위한 워터마킹 모듈과 원구매자의 정보를 판별할 수 있는 핑거프린팅 모듈을 동시에 사용하는 기법으로 현재 MS사의 미디어 플레이어 플랫폼에 구현되어있다. 공모보안 코드 기법은 공모공격에 강인하도록 핑거프린팅 코드 자체를 공모가 어렵도록 설계한 코드로 Boneh와 Shaw가 제안한 c-secure와 c-frameproof 코드[3], Dittmann이 제안한 d-dtecting 코드[4], Domingo-Ferrer가 제안한 3-secure 코드[5,6] 그리고 Trappe가 제안한 Anti- Collusion 코드[9] 등이 있다.

이러한 핑거프린팅 기법은 사용자 마다 서로 다른 핑거프린팅 코드가 삽입되는 성질을 이용하여 여러개의 콘텐츠를 서로 비교하여 핑거프린팅 정보를 유추할 수 있는 공모공격이 존재하게 된다. 대표적인 공모 공격방법에는 평균화 공모공격(Averaging Attack), 최대-최소공격(Max-Min Attack), 상관계수 음수화공격(Negative-Correlation Attack), 제로-상관공격(Zero-Correlation Attack) 그리고 모자이크 공격(Mosaic Attack) 등이 있다[10].

본 논문에서 제안된 알고리즘은 불법공모방지코드(ACC: Anti-Collusion Codes)인 BIBD 기반의 코드를 설계하여 디지털 콘텐츠에 핑거프린트로 사용하였으며 디지털 콘텐츠로부터 핑거프린트를 정확하게 추출하기 위하여 홉필드 신경회로망[11]을 피드백형 연상메모리(Associative memory) 방식으로 설계하여 공모된 핑거프린트와 사용자를 검출한다.

실험을 통하여 BIBD 코드의 분산분석 및 제안된 알고리즘의 불법 공모공격에 대한 강인성과 에러정정 성능을 측정한다. 이를 위해 Ⅱ장에서는 BIBD 코드 및 에러정정을 위한 홉필드 모델의 이론적 배경을 설명하고 Ⅲ장에서는 핑거프린트의 불법공모 코드 검출 및 에러정정을 위해 본 논문에서 제안한 알고리즘을 기술한다. 그리고 Ⅳ장에서 제안된 알고리즘의 성능 측정 및 결과 검토를 하고 마지막 Ⅴ장에서 결론과 향후 연구방향에 대해 고찰한다.

Ⅱ. 이론적 배경

공모 공격자들은 콘텐츠에 삽입된 인식정보 즉 핑거프린트의 제거 및 검출 정보의 모호성을 증대하기 위하여 평균화, 최대-최소공격, 상관계수 음수화, 제로-상관공격 그리고 모자이크 등의 공격을 콘텐츠에 가하며, 결과적으로 공모공격자에 대한 모든 추적을 제거하려고 한다.

그림 1은 공모공격의 기본적인 방법을 나타내며 사용자 u_a와 u_b가 자신들의 핑거프린트를 사용하여 공모코드 col(a,b)를 만들고, 에러 $z(e)$를 포함시켜 불법공모 코드 $y(a,b)$를 만들어 자신들이 공모자라는 것을 감추고 불법공모코드가 내포된 콘텐츠를 배포하는 과정이다.

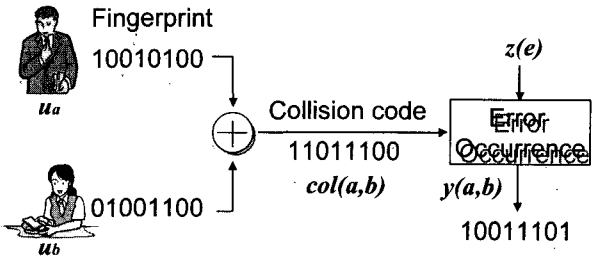

그림 1. 공모공격에 의한 불법 콘텐츠 생성과정
Fig. 1. Process of Illegal contents generation by collusion attack.

1. BIBD 코드

조합문제는 행렬 모델을 사용하여 제약조건을 만족하는 행렬로 생성할 수 있는데, BIBD 코드는 반공모(Anti-Collision) 코드의 제약조건을 만족하는 접속행렬

(Incidence Matrix)을 생성하므로 행렬의 대칭성을 부분적으로 분해할 수 있다. 즉, 공모공격에 강인성을 가지는 반공모 코드로서, n 개의 코드 벡터 중에서 $(n-1)$개 이하의 코드 벡터에 의한 조합이 모두 서로 다른 조합을 가지므로 $(n-1)$명 이하의 공모자를 검출할 수 있다.

BIBD 코드는 5개의 파라메터 (v, b, r, k, λ)로 생성되는데,

v: 처리의 개수
b: 블록의 개수
r: 각 처리의 반복 수($k<v$)
k: 하나의 블록에 포함된 처리의 갯수
λ: 각 처리 쌍이 나타나는 블록의 개수

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

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

5개의 파라메터는 식 (1)과 (2)의 한정조건을 만족하며 간단히 식 (3)과 (4)를 이용하여 (v, k, λ)로 표현할 수 있는 v×b 크기의 접속 행렬 M이 된다.

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

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

접속 행렬 M에서 $b=v$ 이거나 $r=k$이면 BIBD 코드는 대칭성(symmetric)을 갖는 정방행렬이 된다. $v \times b$의 크기를 갖는 접속행렬 M은 식 (5)에 의해 정의되어지며 식 (6)을 만족한다.

$$M = [m_{ij}]$$
$$m_{ij} = \begin{cases} 1 & \text{if } j_{th} \ blocks \in i_{th} \ elements \\ 0 & otherwise, \end{cases} \tag{5}$$

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

J : $v \times v$ 단위행렬

결과적으로 접속행렬 M의 행벡터는 핑거프린트 코드가 되며 b명의 사용자들에게 부여되고, 이러한 접속행렬 M은 반공모 코드로 사용할 수 있다.

2. 홉필드 에러정정회로

홉필드 네트워크는 상호결합형 신경망 모델로서 뉴런의 작용을 단지 임계값의 작용으로 생각하여 훈련에 의한 정보가 연결강도에 의해 표현된다는 이론으로 연상메모리 구조를 제안하여 최적화 문제 해결에 적용하였다. 홉필드 망은 많은 수의 비동기적이고 국소적인 계산을 통하여 전역적 최적화 (Global optimization)를 이룰 수 있으며 특히 연상메모리에 있어서는 일정한 범용 패턴들을 연결강도로 저장하였다가 미지의 입력패턴이 주어질 때 이와 가장 유사한 패턴을 찾아낸다.

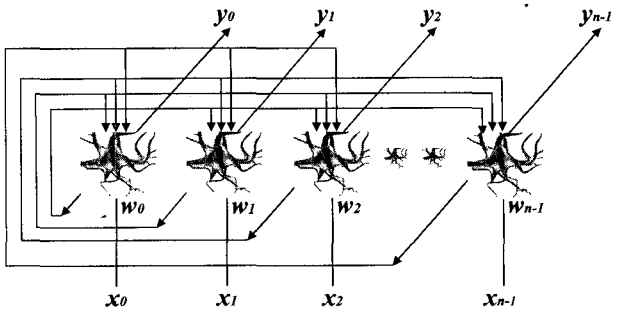

그림 2. 홉필드 네트워크 구조
Fig. 2. Hopfield network structure.

홉필드 네트워크는 그림 2와 같이 자신을 제외한 모든 유니트(뉴론) w_0, w_1, w_2 ... w_{n-1}들 간에 양방향으로 상호연결된 회로망으로 x_0, x_1, $x2$ ... x_{n-1}은 입력패턴이고 y_0, y_1, y_2 ... yn-1은 회로망이 수렴하는 상태의 출력패턴이다.

홉필드 네트워크 구조는 인간의 기억방식과 유사한 방법으로 일부분의 정보를 가지고 그와 연관된 많은 부분을 기억해 내는 방법으로 x에 입력되는 데이터에 의해서 w에 저장된 정보를 찾아내는 것으로 내용지정메모리(CAM:Content Addressable Memory) 또는 연상메모리라 한다. 입력벡터가 x에 입력되고 출력 y는 모든 유니트 w에 피드백 되어 식 (7)과 같이 각 유니트의 출력이 결정된다.

$$\sum_{i=0}^{n-1} \frac{\sigma_i \cdot \mu_i}{R_i} = \begin{cases} > 0 & : \ V_{out} = 'high' \\ < 0 & : \ V_{out} = 'low' \end{cases} \tag{7}$$

n : 유닛의 수
σ_i : 입력벡터의 요소
μ_i : 저장벡터의 요소
R_i : 연결저항

식 (7)의 연결저항은 식 (8)로 정의 되어지며 $R_{i,j}$는 유니트 j로부터 유니트 i로의 연결저항이고, x_i는 s번째 패턴의 i번째 요소이다.

$$R_{i,j}=\begin{cases}\sum_{s=0}^{M-1}x_i^s x_j^s & i\neq j\\ 0 & i=j\end{cases} \quad (8)$$

for $0\le i,\ j\le M-1$

결과적으로 유니트에 기억된 내용은 에러가 있는 유사한 벡터와 전역 최적화를 이룰 수 있기 때문에 에러 정정 기능을 수행한다.

III. 핑거프린트의 불법공모 코드 검출

본 논문에서는 공모공격에 강인성을 가지는 BIBD 기반의 ACC를 사용하였으며, 외부 잡음 공격에 강인성을 부여하기 위하여 홉필드 에러정정회로를 사용하였다. 본 논문에서 제안된 신경회로망을 이용하여 불법 공모자를 검출할 수 있는 알고리즘은 그림 3과 같다.

제안된 알고리즘은 BIBD 기반에 의해 생성된 핑거프린트의 신뢰성을 높이기 위하여 (n,k)코드 기반으로 확장 처리한다. 즉 에러 정정을 위한 홉필드 신경망을 구축할 때 외부 공격에 대한 각 유니트의 고유성을 유지하기 위하여 생성된 핑거프린트를 확장 시키는 것으로 (n,k) 코드어는 식 (9)와 같이 표현한다.

$$C(x)=D(x)\cdot G(x) \quad (9)$$

여기서, $C(x)$는 n-1차 이하의 확산된 코드다항식이며, $D(x)$는 k-1차 이하의 정보다항식으로 핑거프린트 코드이다. 그리고 $G(x)$는 최소의 Hamming거리를 고려해서 추가되는 체크비트로 식 (10)에 의해 계산된다.

$$Check\_bit=2^{r}error\_bit+1 \quad (10)$$

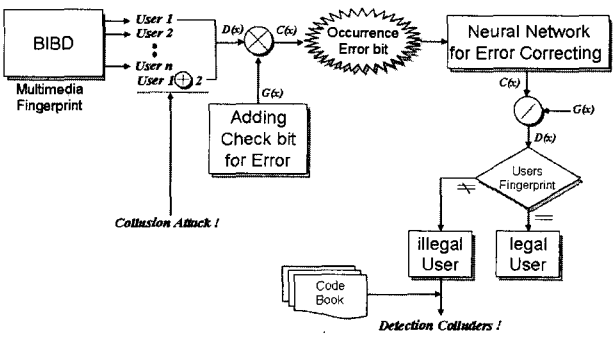

그림 3. 제안된 멀티미디어 핑거프린트의 불법공모코드의 검출 흐름도

Fig. 3. The proposed multimedia fingerprint detection flow diagram.

표 1은 BIBD 기반의 {7,3,1} 코드와 $G(x)$의 정보다항식을 사용하여 생성된 전송 코드이다.

제안된 알고리즘에서 신경망 에러정정 블록은 식 (9)에 의해 생성된 핑거프린트 $C(x)$에 어떤 요인에 의해 에러가 추가되었을 때, 홉필드 모델의 피드백형 연상메모리 방식에 의해 에러가 정정되고 $D(x)$가 산출되며 식 (11)에 의해 불법공모 여부가 결정되며, 최종적으로 코드북을 참조하여 공모자를 검출하게 된다.

$$R=\begin{cases}0 & \text{if} \quad IV(x)=OV(x)\\ 1 & \text{if} \quad IV(x)\neq OV(x)\end{cases} \quad (11)$$

$R(0)$: 공모 없음, $R(1)$: 불법 공모 검출

표 1. {7,3,1} 코드에서 생성된 전송코드

Table 1. Transmission code generated in {7,3,1} code.

{7,3,1} 코드, $G(x)$: (x^4+x^2+x+1)		
사용자 번호	핑거프린트코드: $D(x)$	전송코드: $C(x)$
1	0101010	001111000110
2	1001100	011011010100
3	0011001	001000111111
4	1110000	101000010000
5	0100101	001101010011
6	1000011	011000000101
7	0010110	000111111010

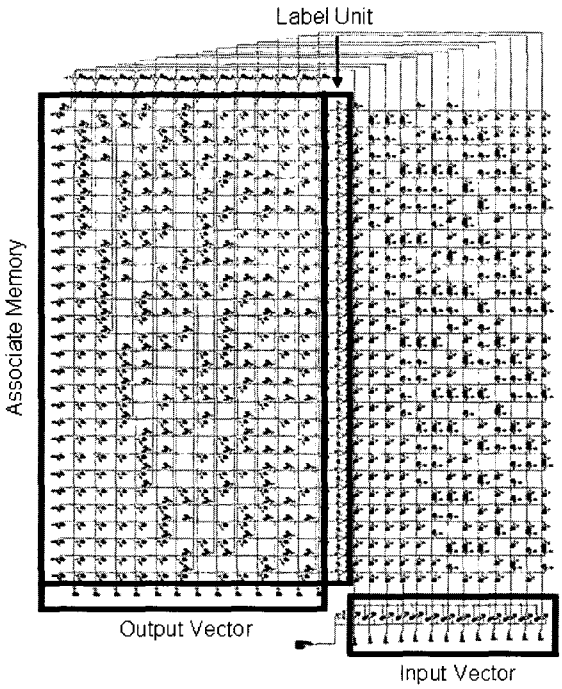

그림 4. 신경회로망를 이용한 에러정정회로

Fig. 4. Error correction circuit using neural network.

IV(x) : 신경망에 입력되는 데이터
OV(x) : 신경망에서 출력되는 데이터

그림 4는 본 논문에서 설계한 홉필드 신경망 에러정정회로이며, 12비트의 핑거프린트 코드 중 2비트의 에러를 정정하여 불법공모의 여부를 확인할 수 있다. 전체회로는 N과 P형의 MOSFET으로 구현하였으며 MOSFET의 채널폭과 채널길이 및 게이트에 연결되는 입력값의 변화에 따라 MOSFET의 상태가 흥분과 억제상태로 제어됨에 따라서 입력 데이터의 에러가 정정되어진다.

Ⅳ. 실험 및 결과 검토

제안된 알고리즘의 성능 측정을 위하여 Matlab으로 시뮬레이션 환경을 구현하였으며, 인텔 펜티엄Ⅳ 3.0GHz CPU와 4.0GB RAM 환경의 IBM PC를 사용하였다. 본 논문에서는 ACC 생성 파라미터 {v,k,λ}가 {7,3,1}, {15,7,3}, {23,11,5}, {31,15,7}의 조건을 가지는 코드를 생성하여 실험하였다. 표 2는 공모공격에서 공모자 수에 따른 조합이 가능한 경우의 수를 나타내며, 공모자 수를 6명으로 제한하여 공모자를 검출하는 실험을 진행하였다. 실험 방법은 크게 공모자들의 평균화 공격에 대한 강인성과 공모공격된 핑거프린트 코드에 가우시안 잡음(AWGN: Additive White Gaussian Noise)공격에 의해 변형되는 비트에러 정정에 대한 강인성을 실험하였다.

1. 공모 평균화 공격에 대한 강인성

그림 5는 {7,3,1} BIBD 코드를 사용하여 7명의 사용자중 2명의 공모공격자를 구분하는 과정을 설명하고 있다. 공모된 코드와 코드북의 상관계수를 구하여 상관계수가 임계값 이상이면 공모자로 처리한다. 그림 5에서는 공모된 코드와 b_1 그리고 b_6의 상관계수가 임계값 이상이므로 공모된 코드임을 알 수 있다.

상관계수는 식 (12)를 사용하여 계산하였다.

$$r = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sigma_x \sigma_y} \tag{12}$$

$-1 \le r \le 1$

$\bar{x}, \bar{y}$: 평균 (average)

σ_x, σ_y : 표준편차 (standard deviation)

그림 6은 공모코드와 코드북과의 상관계수를 나타내며 상관계수(r)가 0보다 큰 경우에 공모자, 0보다 작은 경우에는 비공모자로 판별하였다.

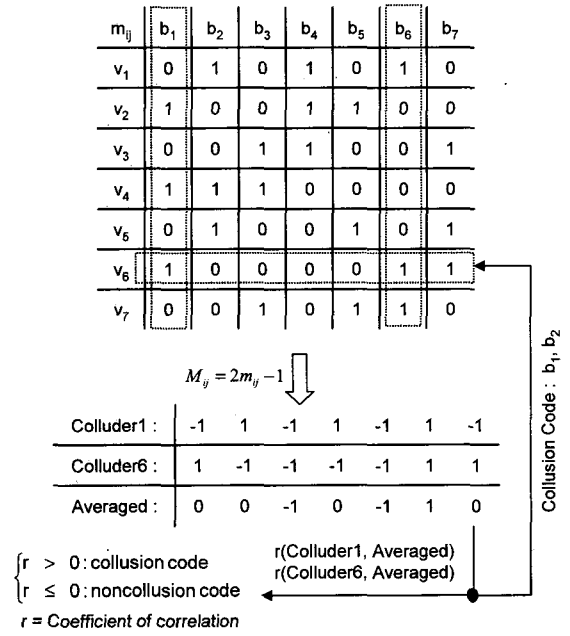

그림 5. {7,3,1} 코드를 이용한 공모자 검출 과정
Fig. 5. Colluder detection process using {7,3,1} code.

표 2. 공모자수에 따른 공모 경우의 수
Table 2. Number of collusion cases by colluder's number.

공모자수	공모 경우의 수			
	{7,3,1}코드	{15,7,3}코드	{23,11,5}코드	{31,15,7}코드
2	21	105	231	465
3	35	455	1,540	4,495
4	35	1,365	7,315	31,465
5	21	3,003	26,334	169,911
6	7	5,005	74,613	736,281

표 3. 평균화 공격에 대한 검출된 공모자수
Table 3. Number of the detected colluders by average attack.

공모자수	검출된 공모자수																			
	{7,3,1} 코드					{15,7,3} 코드					{23,11,5} 코드					{31,15,7} 코드				
	2	3	4	5	6	2	3	4	5	6	2	3	4	5	6	2	3	4	5	6
2	•					•					•					•				
3		•					•					•					•			
4			•					•					•					•		
5				•					•					•					•	
6					•					•					•					•

표 4. AWGN 변화에 따른 검출된 공모자수
Table 4. Number of the detected colluders by changing AWGN.

공모자수	검출된 공모자수											
	{7,3,1} 코드			{15,7,3} 코드			{22,11,5} 코드			{31,15,7} 코드		
	12dB	10dB	8dB	12dB	10dB	8dB	12dB	10dB	8dB	12dB	10dB	8dB
2	2.00	1.99	1.18	2.00	1.79	0.36	2.00	1.18	0.16	2.00	0.70	0.10
3	3.00	2.99	1.76	3.00	2.68	0.53	3.00	1.77	0.24	3.00	1.05	0.15
4	4.00	3.99	2.35	4.00	3.58	0.71	4.00	2.37	0.32	4.00	1.40	0.20
5	5.00	4.99	2.94	5.00	4.47	0.89	5.00	2.96	0.41	5.00	1.76	0.24
6	6.00	5.98	3.53	6.00	5.36	1.07	6.00	3.55	0.49	6.00	2.11	0.29

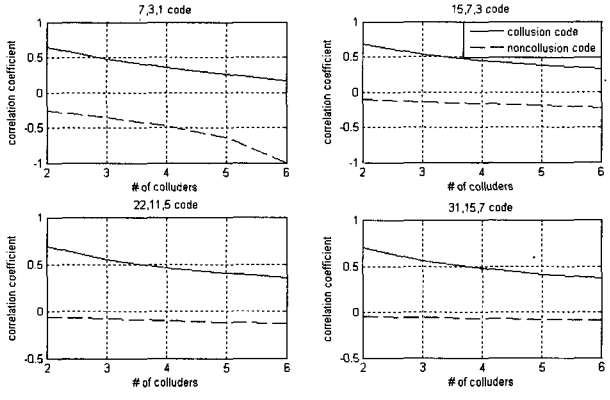

그림 6. 공모코드와 비공모코드의 상관계수
Fig. 6. Correlation coefficient of collusion and anti-collusion code.

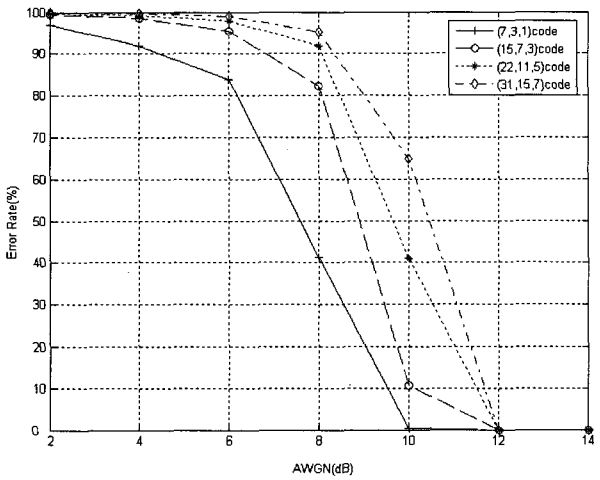

그림 7. AWGN에 따른 신경회로망의 에러정정 성능
Fig. 7. Error correction performance of neural network by AWGN.

표 3은 본 논문에서 제안한 알고리즘을 사용하여 공모평균화 공격에 대한 공모자 검출결과로 공모평균화 공격에 한하여 공모자를 100% 검출하였다.

2. 신경회로망을 이용한 비트 에러정정

공모자 추적을 회피하기위하여 공모된 코드에 잡음 및 고의적인 비트 조작의 공격을 가할 수 있는데 본 논문에서는 이러한 공모공격에 대한 강인성을 가지기 위하여 2비트 에러정정 홉필드 신경회로망을 설계하였다.

본 논문에서는 성능평가를 위하여 생성된 핑거프린트 코드에 2비트의 에러정정을 위해 식 (10)에 의해 5비트의 에러정정 비트를 추가하였다.

그림 7은 AWGN의 증가에 따른 정정회로의 성능을 나타내었다. AWGN이 12dB 이상일 때 설계된 신경망 회로의 에러정정율이 100%임을 알 수 있다. 즉, 한 코드에서 2비트 이내의 에러비트가 발생함을 알 수 있다.

표 4는 각각의 코드를 1,000개씩 생성하여 AWGN의 변화에 따른 공모자 검출 결과표이다. AWGN이 12dB까지는 공모자수를 정확히 검출할 수 있지만 10dB 이하부터는 코드길이에 비례하여 검출할 수 있는 공모자의 수가 감소함을 알 수 있다.

결과적으로 본 논문에서 제안된 신경회로망에 의한 핑거프린트 검출 알고리즘은 설계된 BIBD 기반의 코드에 의해 평균화 공모공격에 대해서는 100% 공모자 검출이 가능하며, 홉필드 신경회로망에 의해 공모코드의 비트 변환 공격에 대해서 2비트 이내의 코드변화에 대해서 공모자를 정확히 검출할 수 있다.

V. 결 론

본 논문에서는 불법복제 및 공모공격 등으로부터 디지털 콘텐츠의 저작권을 보호하기위하여 공모공격에 강인한 BIBD 기반의 불법공모방지코드를 설계하였다. 또한 핑거프린트 정보는 디지털 콘텐츠의 전송 중 외부공격 및 잡음 등에 의해 손실이 발생할 수 있는데 이러한 점을 개선하기 위하여 홉필드 신경회로망을 이용하여 손실이 발생한 코드를 정정할 수 있는 핑거프린트 알고리즘을 제안하였다. 제안된 알고리즘은 크게 선형 공모 공격에 강인성을 가지는 BIBD 기반의 불법공모방지코드 설계와 외부공격에 의해 발생한 에러비트를 정정하기위한 피드백형 연상메모리방식의 홉필드 신경회로망으로 구성되어있다. 실험 결과 BIBD 기반의 불법공모방지코드는 평균화 선형 공모공격에 대해 100% 공모코드 검출이 이루어졌으며, 에러비트 정정을 위해 설계한 (n,k)코드를 사용한 홉필드 신경회로망은 2비트 이내의 에러비트를 정정할 수 있음을 확인하였다. 결과적으로 제안된 알고리즘은 평균화 공모공격 및 공모코드에 2비트 이내의 에러비트가 발생되었을 때 공모자를 정확히 검출할 수 있음을 확인하였다.

앞으로의 연구는 제안된 멀티미디어 핑거프린트 알고리즘을 사용하여 실제 멀티미디어에 삽입할 수 있는 효과적인 알고리즘 개발에 관한 연구와 제로-상관공격 등의 비선형 공모공격에 대한 강인성을 갖는 연구가 진행되어야겠다.

참 고 문 헌

[1] Ingemar J. Cox, Miller M. L. and Bloom J. A., "Watermarking applications and their properties," International Conference Information technology'2000, Las Vegas, 2000.

[2] D. Kirovski, H.S. Malvar, and Y. Yacobi. "Multimedia Content Screening using a Dual Watermarking and Fingerprinting System," ACM Multimedia, 2002.

[3] D. Boneh and J. Shaw, "Collusion-Secure Fingerprinting for Digital Data," IEEE Trans. Inf. Theory, Vol. 44, No. 5, pp. 1897-1905, Sep. 1998.

[4] 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.

[5] J. Domingo-Ferrer and J. Herrera- Joancomarti, "Simple Collusion-secure Fingerprinting Schemes for Images," in IEEE International Conference on Information Technology: Coding and Computing, ITCC'2000, ISBN 0-7695-0540-6, pp. 128-132.

[6] F. Sebe and J. Domingo-Ferrer, "Short 3-Secure Fingerprinting Codes for Copyright Protection," Lecture Notes in Computer Science, Vol. 2384, pp. 316- 327, 2002.

[7] Yiwei Wang, John F. Doherty, and Robert E. Van Dyck, "A Watermarking Algorithm for Fingerprinting Intelligence Images," 2001 Conference on Information Sciences and Systems, The Johns Hopkins University, March 21-23, 2001.

[8] W. Trappe, M. Wu, and K.J.R. Liu, "Collusion-Resistant Fingerprinting for Multimedia," Proc. of IEEE Int. Conf. on Acoustics, Speech, and Signal Processing (ICASSP'02), Vol. IV, pp. 3309-3312, Orlando, FL, May 2002.

[9] W. Trappe, M. Wu, Z. Jane Wang, and K. J. R. Liu, "Anti-Collusion Fingerprinting for Multimedia," IEEE Trans..on Signal Processing, Vol. 51, No. 4, pp. 1069-1087, Apr. 2003.

[10 H. Stone, "Analysis of Attacks on Image Watermarks with Randomized Coefficients," NEC Technical Report, 1996.

[11] John. J. Hopfield, "Artificial Neural Network," IEEE Circuits and Device Magazine, pp. 3-9, 1986.

저 자 소 개

노 진 수(학생회원)
2002년 조선대학교 전자공학과 학사졸업.
2004년 조선대학교 전자공학과 석사졸업.
2006년 조선대학교 전자공학과 박사과정.
<주관심분야 : UWB, 생체인식, 양자컴퓨팅>

이 강 현(평생회원)-교신저자
1979년, 1981년 조선대학교 전자공학과 공학사 및 석사
1991년 아주대학교 대학원 공학박사
1977년~현재 조선대학교 교수
1991년, 1994년 미 스탠포드대 CRC 협동연구원.
1996년 호주 시드니대 SEDAL 객원교수
2000년~현재 한국 멀티미디어기술사협회 이사
2002년 영국 런던대 객원 교수
2002년 대한전자공학회 멀티미디어연구회전문위원장
2003년 한국 인터넷 방송/TV 학회 부회장
2003년~현재 대한전자공학회 상임이사
2005년~현재 조선대학교 RIS 사업단장
<주관심분야 : 멀티미디어 시스템설계, Ubiquitous convergence>