유비쿼터스 네트워크 시스템에서의 미디어 보안에 관한 연구

주민성* · 안성수** · 우영환*** · 김용태**** · 김태훈**** · 박길철**** · 김석수****

요 약

본 논문에서는 디지털 콘텐츠의 저작권을 보호하기 위하여 공모공격에 강인한 BIBD 기반의 불법공모방지코드를 설계하였다. 또한 핑거프린트 정보는 디지털 콘텐츠의 전송 중 외부 공격 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 외부 공격에 의해 발생한 에러비트를 정정하기 위한 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 에러비트가 발생되었을 때 공모자를 정확히 검출할 수 있음을 확인하였다.

A Study on Media Security in Ubiquitous Network System

Min Seong Ju* · Seong Soo Ahn** · Young Hwan Woo***
Yong Tae Kim**** · Tai Hoon Kim**** · Gil Cheol Park**** · Seok Soo Kim****

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 technique which supports copyright protection to track redistributers 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 re-contributed 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.

Key words : Network Security, Media Security

* 한남대학교 멀티미디어학과
** KISA(한국정보보호진흥원) 선임 연구원
*** 거창 전문대학 컴퓨터정보시스템 교수
**** 한남대학교 멀티미디어학과 교수

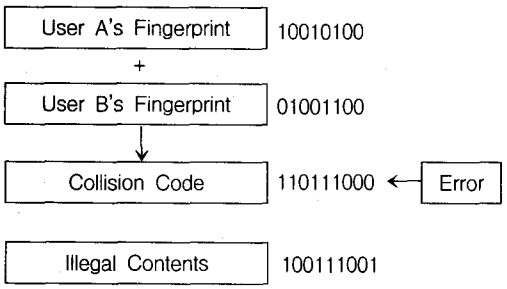
1. 서 론

디지털 콘텐츠 보호기술은 콘텐츠 제작자의 저작권 관련 정보를 외부공격에 강인하도록 콘텐츠에 삽입하는 기술로 정의할 수 있으며 이는 크게 워터마킹 기술과 핑거 프린팅 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 사용자정보가 삽입되어 각 사용자가 공모하여 다른 복제를 만들 수 있는 공모공격의 문제가 발생되었을 때, 공모 공격자들을 추적하여 검출할 수 있는 콘텐츠 보호기술로 그 기원은 대수표(algorithm 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 삽입 코드 자체를 공모 공격이 불가능하도록 설계하는 공모보안코드 개발 기법(collusion secure code)[3-6]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 공모 공격이 존재하게 된다. 대표적인 공모 공격방법에는 평균화 공모 공격(Averaging Attack), 최대-최소공격(Max-Min Attack), 상관계수 음수화공격(Negative-Correlation Attack), 제로-상관공격(Zero-Correlation Attack) 그리고 모자이크 공격(Mosaic Attack) 등이 있다. 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 핑거 프린트와 사용자를 검출한다. 실험을 통하여 BIBD 코드의 분산분석 및 제안된 알고리즘의 불법 공모공격에 대한 강인성과 에러정정 성능을 측정한다. 이를 위해 제 2장에서는 BIBD 코드 및 에러정정을 위한 홉필드 모델의 이론적 배경을 설명하고 제 3장에서는 핑거프린트의 불법공모 코드 검출 및 에러정정을 위해 본 논문에서 제안한 알고리즘을 기술한다. 그리고 제 4장에서 제안된 알고리즘의 성능 측정 및 결과 검토를 하고 마지막 제 5장에서 결론과 향후 연구방향에 대해 고찰한다.

2. 관련 연구

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 공모 공격자에

대한 모든 추적을 제거하려고 한다. (그림 1)은 공모공격의 기본적인 방법을 나타내며 사용자 ua와 ub가 자신들의 핑거프린트를 사용하여 공모코드 col(a, b)를 만들고, 에러 z(e)를 포함시켜 불법 공모 코드y(a, b)를 만들어 자신들이 공모자라는 것을 감추고 불법공모코드가 내포된 콘텐츠를 배포하는 과정이다.



(그림 1) Basic methods of collusive attack

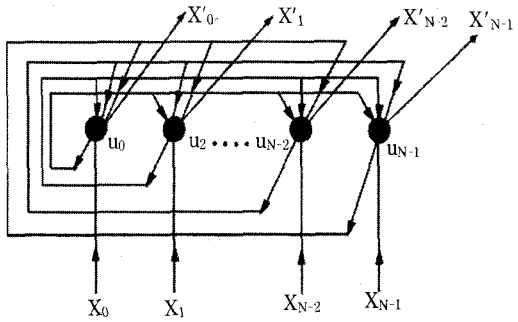
2.1 BIBD Code

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 부분 적으로 분해할 수 있다. 즉, 공모공격에 강인성을 가지는 반공모 코드로서, n개의 코드 벡터 중에서 (n-1)개 이하의 코드 벡터에 의한 조합이 모두 서로 다른 조합을 가지므로 (n-1)명 이하의 공모자를 검출할 수 있다.

2.2 Hopfield Networek

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) Basic Structure of Hopfield Network

홉필드 네트워크는 (그림 2)와 같이 자신을 제외한 모든 유니트들간에 양방향으로 상호 연결된 회로망으로 기존의 라인이 입력 패턴이되로 y열 라인이 회로망이 수렴하는 상태의 출력 패턴이다. 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 내용 지정 메모리 또는 연상 메모리라고 한다.

본 논문에서는 공격에 대한 강인성을 가지기 위하여 멀티미디어 데이터에 핑거 프린팅 기법 을 사용하고 BIBD 기반의 불법공모 방지 코드를 신경망회로(홉필드 네트워크)를 적용하여 작성한다.

이러한 구조는 기존의 핑거 프린팅 기법의 한계를 극복하는 방안으로, 기존 핑거 프린팅 기법의 무용성이 제기되었던 것중 하나로 불법 배포자의 발본색원이 어려우며 현재 불법 자료의 유통이 실제로는 유통의 배포자 p2p 시스템을 이용한 다대 다 구조이기에 실질적인 효과가 없다는 점을 보완 할 수 있으며 또한 기존의 핑거 프린팅 기법의 특성을 살려 구조적인 불법 배포의 루트를 확인할 수 있다는 장점이 있다.

이러한 복합적인 장점 이외에도 홉필드 네트워크는 (그림 2)와 같이 자신을 제외한 모든 유니트(뉴론) w0, w1, w2, …, wn-1들 간에 양방향으로 상호연결된 회로망으로 x0, x1, x2, …, xn-1은 입력패턴이고 y0, y1, y2, …, yn-1은 회로망이 수렴하는 상태의 출력 패턴이다.

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 각 유니트의 출력이 결정된다. 유니트에 기억된 내용은 에러가 있는 유사한 벡터와 전역 최적화를 이룰 수 있기 때문에 에러정정 기능을 수행한다

3. 멀티미디어 보안

본 논문에서는 공모공격에 강인성을 가지는 BIBD 기반의 ACC를 사용하였으며, 외부 잡음 공격에 강인성을 부여하기 위하여 홉필드 에러정정 회로를 사용하였다. 본 논문에서 제안된 신경회로망을 이용하여 불법공모자를 검출하고자 하였다. 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 다음 식과 같이 표현한다.

$$C(x) = D(x) \cdot G(x) \quad (1)$$

여기서, C(x)는 n-1차 이하의 확산된 코드다항식이며, D(x)는 k-1차 이하의 정보다항식으로 핑거프린트코드이다. 그리고 G(x)는 최소의 Hamming 거리를 고려해서 추가되는 체크비트로 다음 식에 의해 계산된다.

$$Check\_bit = 2 \cdot error\_bit + 1 \quad (2)$$

제안된 알고리즘에서 신경망 에러정정 블록은 식 (1)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 (2)에 의해 불법공모 여부가 결정되며, 최종적으로 코드북을 참조하여 공모자를 검출하게 된다. (그림 4)는 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 홍분과 억제상태로 제어됨에 따라서 입력 데이터의 에러가 정정되어진다.

4. 에러검출알고리즘

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 2>는 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 핑거 프린트 코드에 가우시안 잡음공격에 의해 변형되는 비트에러 정정에 대한 강인성을 실험하였다. BIBD 코드를 사

용하여 7명의 사용자중 2명의 공모공격자를 구분하는 과정을 설명하고 있다. 공모된 코드와 코드북의 상관계수를 구하여 상관계수가 임계값 이상이면 공모자로 처리한다. 공모자 추적을 회피하기 위하여 공모된 코드에 잡음및 고의적인 비트 조작의 공격을 가할 수 있는데 본 논문에서는 이러한 공모공격에 대한 강인성을 가지기 위하여 2비트 에러정정 홉필드 신경회로망을 설계하였다.

본 논문에서 제안된 신경회로망에 의한 핑거프린트 검출 알고리즘은 설계된 BIBD 기반의 코드에 의해 평균화 공모공격에 대해서 공모자 검출이 가능하며, 홉필드 신경회로망에 의해 공모코드의 비트 변환 공격에 대해서 공모자를 검출할 수 있다.

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

참 고 문 헌

[1] J. Dittmann, "Combining Digital Watermarks andCollusion Secure Fingerprints for Customer Copy Monitoring", Proc. IEE Seminar Sec. Image &Image Auth., pp. 128-132, Mar. 2000.

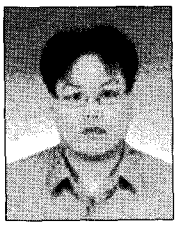
[2] W. Trappe, M. Wu, Z. Jane Wang, and K. J. R. Liu, "Anti-Collusion Fingerprinting for Multimedia", IEEE Trans. on Signal Processing, Vol. 51, No. 4, pp. 1069-1087, Apr. 2.

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

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

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

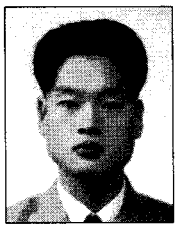
[6] F. Sebe and J. Domingo-Ferrer, "Short 3-Secure Fingerprinting Codes for Copyright Protection."



주 민 성

2005년 한남대학교 멀티미디어 (공학사)

2007년 한남대학교 멀티미디어 (공학석사과정)



안 성 수

1998년 부경대학교 정보통신 (공학석사)
1999년~현재 KISA 보안성 평가단 선임연구원

우 영 환

1987년 서울산업대학교 전자공학 (공학사)
1994년 한양대학교 전자통신과 (공학석사)
2006년 성균관대학교 정보공학 (공학박사)
1997년~현재 거창 전문대학 컴퓨터 정보시스템 교수

김 용 태

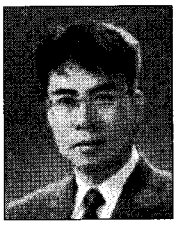
1984년 한남대학교 계산통계학과 (이학사)
1988년 숭실대학교 전자계산학과 (공학석사)
1998년 충북대학교 전산학과 박사 과정
2002~2006 (주)가림정보기술 이사
2006~현재 한남대학교 공과대학 멀티미디어학부 강의전담 교수

김 태 훈

1995년 성균관대학교 학사
1997년 성균관대학교 석사
2002년 성균관대학교 박사
2004년 한국정보보호진흥원 선임연구원
2006년 국군기무사령부 사무관
2007년 이화여자대학교 연구교수
2007년~현재 한남대학교 멀티미디어 학부 조교수

박 길 철

1983년 한남대학교 전자계산학 (공학사)
1986년 숭실대학교 전자계산학 (공학석사)
1988년 성균관대 대학원 전자계산학(공학박사)
1998년~현재 한남대학교 멀티미디어공학 교수



김 석 수

1989년 경남대학교 계산통계학 (이학사)
1991년 성균관대학교 대학원 (공학석사)
1991년 정풍물산(주)중앙연구소 주임연구원
1997년 한국 탑웨어 책임연구원
1998년 경남 도립 거창전문대학교 교수
2000년 동양대학교 컴퓨터공학부 교수
2002년 성균관대학교 대학원(공학박사)
2003년~현재 한남대학교 멀티미디어공학 교수