심층암호 기술을 이용한 안전한 콘텐츠 유통과 응용

Secure Contents Distribution Scheme Using Steganographic Technique and Its Applications

이형우, 한군희
천안대학교 정보통신학부 교수
전병민
충북대학교 컴퓨터정보통신연구소

Hyung-Woo Lee, Kun-Hee Han
Professor, Div. of Info. & Com. Eng., Cheonan University
Byung-Min Jun
RICIC, Chungbuk National University

중심어 : 디지털 콘텐츠 유통, 심층암호, 저작권 보호, 전자서명 기술

요 약

본 연구에서는 심층암호 기반 정보은닉 기술을 디지털 콘텐츠 보호 기술에 적용하였다. 디지털 콘텐츠에 대한 안전한 유통을 위해 워터마킹, 핑거프린팅 기술을 종합적으로 고찰하여 새로운 패러다임을 제시하였다. 구체적으로 공개 검증 가능한 전자서명 기법을 콘텐츠 유통에 적용하여 디지털 콘텐츠에 대한 저작권 정보를 서명하고, 만일 저작권에 대한 판별 과정이 필요할 경우 이를 공개적으로 증명할 수 있다.

Abstract

In this study, we combine information hiding technique with digital contents protection scheme. For providing secure distribution on digital contents, a new paradigm can be proposed after considering both watermarking and fingerprinting techniques. In detail, publicly verifiable digital signature schemes are applied into digital contents. On signing digital copyrights, we can publicly verify its correctness if needed.

I. 서론

고전적인 암호(cryptography) 기법을 사용하여 메시지 자체에 대한 안전성을 확보하고자 하는 연구와 함께, 메시지 내에 디지털 정보에 대한 인증 또는 서명에 해당하는 정보를 은닉하고자 하는 연구가 계속되고 있다. 정보은닉(information hiding)[3,6] 분야는 최근 정보이론에 근간한 심층암호(steganography)[1,2,3,4,5,6,7] 기법과 디지털 워터마킹(digital watermarking)[7,8,9,10] 기술로 발전하면서 멀티미디어 시대에 저작권 또는 소유권 보호를 위해 필수적인 기술로 부상하고 있다. 이와 더불어 디지털 핑거프린팅(digital fingerprinting) 기술을 통해 고전적 암호 기술을 접목하고 DRM(Digital Right Managements) 기술을 통한 콘텐츠 관리 방식에 대한 연구가 계속되고 있다.

따라서 본 연구에서는 정보은닉기술에 대한 최신 연구 동향을 파악하며 기초 이론에 대한 분석을 통해 문제점을 파악하고 이를 개선할 수 있는 신기술을 제시하고자 한다. 특히 현재 활발한 연구가 되어왔던 디지털 워터마킹 기술인 경우 다양한 방법론과 기술들이 발표되었지만 체계적인 구조가 제시되지 않아 현실적인 한계에 도달하고 있으며, 핑거프린팅 기법인 경우 불법적인 사용 방지 및 추적 기술 제공에 중점을 두고 있기 때문에 수동적인 측면에서의 안전성을 확보하는 방식이다. DRM으로 대별되는 디지털저작권관리 기술인 경우 아직까지는 디지털 콘텐츠에 대한 추상적인 모델에 해당하므로 이를 현실적인 측면에서 종합적으로 재고찰하며 실세계에 직접 적용 가능하며 안전성이 확보된 콘텐츠 유통 기술에 대한 연구가 절실히 필요하다.

구체적으로 본 연구에서는 급속한 발전 및 보급 확대가 예상되는 인터넷 기반 전자상거래 환경에서 소프트웨어 저작권이라 할 수 있는 디지털 콘텐츠에 대한 저작권 보호[10,11,12,13]를 위해 정보 은닉 기술을 기반으로 심층암호와 디지털 워터마킹 기술을 포함한 디지털 콘텐츠 유통 기술에 대해 분석하며, 궁극적으로 암호학 기술과 접목하여 새로운 전자상거래 패러다임을 제시하고 안전성을 제공하는 디지털 콘텐츠 유통 기술을 제시하고자 한다.

II. 디지털콘텐츠 보호기술

현재 심층암호에 대한 관심이 급격히 증가하고 있으며 다양한 분야에 적용 가능한 새로운 핵심 기술로 인식되고 있다. 심층암호는 기존의 일반적인 암호학 분야와는 다른 목적 및 방향으로 발전한 것으로, 전체 메시지에 대한 특성을 유지하

면서 정보를 은닉하는 기법이다. 심층암호에서 특히 디지털 정보 및 멀티미디어 콘텐츠에 대한 보호 기법으로 고찰할 수 있는 것이 디지털 워터마킹 기법이다. 워터마킹 기술은 이미지, 오디오, 비디오 정보와 같은 디지털 멀티미디어 정보에 비밀 정보(secret information)를 은닉하는 방법이다.

디지털 워터마킹 기술의 주요 목적은 인간의 의식 체계 또는 인간의 감지 능력으로는 검출할 수 없는 저작권 정보(copyright information)와 같은 비밀 암호 정보를 전자상거래에서의 멀티미디어 콘텐츠, 디지털 정보(digital information) 또는 디지털 상품(digital product) 내에 포함시키는 것이다. 워터마킹 기술은 불법 사용자에 의해서 제거하기 어려워야 하며, 워터마크된 디지털 콘텐츠는 압축, 변조 및 변화되었을 때에서 안전성과 견고성을 제공할 수 있어야 한다. 디지털 콘텐츠 유통을 위한 기술 동향은 다음과 같다.

1. 디지털 워터마킹 기반 보호기술

디지털 콘텐츠에 대한 안전한 유통을 위해 디지털 워터마킹 기법을 적용하여 이를 보장하고자 하였다. 워터마크 방식을 적용하였을 경우 저작권에 대한 정보를 이진수 1과 0으로 암호화하여 이미지 콤포넌트를 재구성하는 방식이다.

디지털 콘텐츠에 대한 유통을 위한 기존의 접근 방법론은 대표적으로 아래와 같은 기법들로 구분할 수 있으며, 워터마킹 기법을 통해 저작권을 보호하고 이를 바탕으로 콘텐츠에 대한 유통 단계에서 안전성을 확보하고자 하였다.

- Tirkel[14]과 Schyndel[15] : 공격에 견고하고 여과(filtering)와 변형(cropping)에 저항하는 불확정 워터마크(oblivious watermark)를 만들기 위해 m-수열들의 특성을 적용하였다.
- Matsui와 Tanaka[16] : 워터마킹을 위해 선형 예시(predictive) 코딩을 적용했다. 워터마크를 숨기기 위한 시도는 워터마크가 양자 노이즈를 닮도록 만드는 것이었다.
- Tirkel과 Osborne[14] : 디지털 이미지 워터마킹을 위해 확산 스펙트럼 기술들의 응용성을 제시하였다. 확산 스펙트럼은 여러 가지 장점을 가지고 있다. 암호학적 안전성을 제공하고 최대 채널 용적에 의해 주어진 한계에서 워터마크를 에러 없이 전송할 수 있다.
- Ruanaidh[17]과 Cox[18] : 워터마킹을 위해 인식적으로 적응하는 변환 도메인 방법들을 제시했다. 이미지를 블록들로 나누었으며, 정보는 DCT, FFT magnitude 그리고 phase, wavelet, 선형 예시 코딩과 프랙탈을 사용해 삽입한다.
- Delaigle[19] : 디지털 이미지에 대한 저작권 보호를 위해 서명 라벨링 기술들을 응용했다.

2. 디지털 핑거프린팅 기반 보호기술

핑거프린팅의 적용범위는 traitor tracing, asymmetric traitor tracing, 그리고 broadcast encryption 등 다양하다[21,22,26]. 가장 최근에는 실용적인 면이 부각된 전자현금에 기반한 익명성 보장 핑거프린팅 방식이 제안되었다.

- 익명적 핑거프린팅 기법[25] : 개인의 프라이버시가 침해되는 문제점의 해결을 위해서 Pfizmann의 의해서 제안된 기법은 익명으로 핑거프린팅 되지만 불법 복제된 데이터가 발견되면 추적이 가능하도록 한다.

- 불법 유통자 검출 기법[21] : 이미지나 오디오와 같은 실제 데이터에 핑거프린팅하는 대신 데이터를 복호화하기 위해 키를 핑거프린팅한다. trator tracing 기법은 key initialization, key fingerprinting, session sending, tracing의 4단계로 구성된다.[21,22,26].

기존 기법에서 발생하는 문제점들은 대부분 B.Pfitzmann [22,24,25]에 의해 해결되고 있으며 Camenisch는 전자화폐에 기반한 방식을 그룹 서명(group signature)을 이용해서 다양한 구매를 한번의 인출과정으로만 할 수 있는 새로운 방법[28]을 제시하였다.

3. DRM 관련 보호기술

최근 저작권 보호와 콘텐츠 유통 활성화를 위한 디지털 저작권 관리 솔루션(DRM : Digital Rights Management)에 많은 관심이 집중되고 있다. 저작권 보호 기술업체들이 콘텐츠 불법복제 방지 뿐만아니라 콘텐츠 제작자, 유통업계 및 고객간 전자상거래가 가능한 DRM 솔루션 제시에 박차를 가하고 있다. 특히 이들 솔루션은 그동안 저작자나 ISP, CP들이 전자상거래의 문제점을 지적해 온 불법복제 문제와 유통·과금까지 일괄적으로 처리하고자 하는 것에 목적을 두고 있다. 그러나, DRM은 저작권법적인 측면에서의 보호측면을 강조한 결과 멀티미디어에 대한 워터마킹 삽입/검출/검증 시스템과의 접목이 절실하며, 객관적인 의미에서 디지털 저작권을 보호하기 위해서는 아직도 많은 분야에서 새로운 기술 및 개념이 제시되어야 한다.

III. 콘텐츠 보호를 위한 선행 연구의 문제점

1. 기존 디지털 워터마킹의 문제점

1.1 워터마킹 기술의 근본적 한계

지금까지의 주파수 영역 중심 워터마킹 기술은 공학적인 요소가 강한 만큼 알고리즘에 대한 안전성 판단 과정은 비정형적인 분석 방법을 사용하고 있으며, 전반적으로 공학적 측면에서의 확률론적 기법에 의존한 안전성에 의존하고 있기 때문에 체계적이지 못하다는 문제점을 갖고 있다. 즉 워터마킹 기술을 정보은닉 이론적 관점에서 보면 안전성을 제공할 수 있는 기초 연구 결과들이 반영되지 못하고 있다는 것이다. 또한 기존의 워터마킹 이론은 전반적인 학문적 체계가 구조화되어 있지 않다.

1.2 암호기술 기반 워터마킹으로의 발전

공학적 한계를 극복하는 데 연구의 관점이 모아져 있음으로 인해 이론적 체계화보다는 각 기술 또는 알고리즘에 따른 발전이 계속되었으며, 공학적으로 납득할 수준의 안전한 이론이 성립되었다 할 지라도 그것이 정말 안전한 지에 대한 검증 방법 또한 공학적 부분에만 치중되어 있다. 따라서 이러한 워터마킹 이론의 한계를 실질적으로 극복하려면 단순히 공학적 관점의 새로운 기술 접목은 지양되어야 하며, 암호학적 이론의 접목 또는 정보이론 관점을 접목하여 더 넓은 영역을 포괄적으로 고찰할 수 있어야 하며 할 것이라는 것이 최근의 연구성과들이 이를 조금씩 증명하고 있다.

표 1. 워터마킹 기법에 대한 분석

워터마킹 기법에 대한 분석		
구 분	공간영역	주파수영역
대 상	이산정보	연속정보
문제점	비정형기법	확률론적기법
개 선	암호기반 정형기법	

2. 기존 디지털 핑거프린팅의 문제점

2.1 정형화된 검증 과정의 부재

구매자 측면에서 디지털 워터마킹을 적용할 경우 디지털 핑거프린팅에 해당한다. 암호 기법을 적용하여 이미지와 같은 디지털 콘텐츠에 대한 불법복사 방지를 목적으로 활용된다. 지금의 핑거프린팅 관련 방법[10,11,15,16]들은 구매자에 대한 적법한 사용 권한을 증명해 주는 것에 해당한다. 지금까지의 핑거프린팅 기법은 구매자 중심의 정보를 콘텐츠 내에 삽입하게 된다. 따라서 콘텐츠 소유자인 판매자에 대한 정보와 구매자 정보가 공존하지 않은 경우 복잡한 과정을 통해 적법성을 판단하게 되며, 공개적인 검증 과정 및 타당성 증명 과정 역시 제한적으로 제공된다. 따라서 판매자/구매자 자신의 비밀 정보를 공개하지 않고 익명성을 보장해 주면서 구매자에 대한 소유권을 증명할 수 있는 기술이 필요하다.

2.2 공개적인 검증이 가능한 핑거프린팅으로 발전

현재의 핑거프린팅 기법은 전자상거래 환경이 갖는 다중 판매자 및 다중 구매자 환경에 적합하지 않다는 문제점을 갖고 있다. 따라서 다중 개체에 안전한 프로토콜(multiparty secure protocol)을 통해 저작권 정보에 대한 유효성을 판단하는 구조가 필요하다. 결국 기존의 디지털 핑거프린팅 기법은 디지털 콘텐츠에 대한 안전한 유통보다는 불법적인 사용을 방지하기 위한 암호 프로토콜을 제시하고 있는 것이 현실이다. 기존의 디지털 핑거프린팅 기법은 단순히 콘텐츠에 대한 소유권 정보를 표시하고 이를 추적하는 기법에 중점을 두었으나 이와 더불어 디지털 콘텐츠에 대해 공개적인 검증이 가능한 핑거프린팅(publicly verifiable fingerprinting)기술로 발전하는 것이 필요하다. 이를 위해서는 현실적인 유통 구조에서 콘텐츠에 대한 안전성을 확보하면서도 효율성을 확보하기 위한 새로운 패러다임이 제시되어야 한다.

IV. 새로운 콘텐츠 보호 기법

1. 정보은닉 기반 콘텐츠 보호 기법

본 연구에서 제시하고자 하는 기법은 기존의 디지털 워터마킹, 핑거프린팅 기술이 개별적으로 갖는 문제점들을 극복하고 반면에 각각의 기술이 지니는 고유한 특징 및 장점을 조합하여 현실적인 측면에서 접근함으로써 앞으로 급속한 발전이 예상되는 디지털 콘텐츠 전자상거래(D-Commerce : Digital Electronic Commerce) 환경에 적합한 유통 기술을 제공하고자 한다.

1.1 새로운 접근방법

기존의 디지털 워터마킹 기술이 갖는 공학적인 한계와 제약조건을 개선하며, 핑거프린팅 기술에서의 검증 기술에서의 한계를 극복하는 방법을 제시한다.

물론 기존의 디지털 워터마킹 기법은 정보은닉 기술을 적용한 대표적인 기법으로서 소유권자에 해당하는 디지털 저작

권 정보를 견고하게 은닉하며, 특정 비밀 정보를 알고 있을 경우에만 검출/검증된다는 점에선 매우 우수한 저작권 표기 기술이다. 또한 핑거프린팅 기술인 경우 구매자 자신이 콘텐츠를 구입하고자 하는 경우 암호 기술을 적용하여 자신의 소유권을 증명할 수 있으며, 만일 불법적인 유통을 하였을 경우 이는 판매자에 의해 추적된다는 점에서 매우 적합한 저작권 추적 기술이다.

본 연구에서 제시하고자 하는 기술은 디지털 콘텐츠 저작권 보호를 위해 정보은닉(information hiding) 기술을 암호학적 측면에서 접근하고 심층암호기술을 적용하여 핑거프린팅 기술에서의 공개 검증 및 추적 기능을 제공하는 콘텐츠 유통 기술이다.

2. 제시한 기법의 구조

본 연구에서 제시한 기법에서는 워터마킹 계층에서는 삽입에 관련된 정보 은닉 체계를 제공하고, 상위에 핑거프린팅 계층을 설정하여 공모 또는 에러, 공격 등에 대처할 수 있는 기능을 제공하는 방식과 같이 상하 연계 구조를 설정하는 것이다.

기존의 연구에서 핑거프린팅은 에러 포용(error tolerance)적인 기능을 제공하기 위해 많은 노력이 계속되었다. 삽입하고자 하는 마크에 대한 복구 기능을 제공하기 위한 코딩 체계를 연구하며, 모델을 설정하고 핑거프린트 정보량의 하한을 설정한다. 결국 핑거프린팅 계층에서 이진 코드워드 값에 해당하는 마킹 정보를 생성하며 그 하부에 있는 워터마킹 계층에서 스프레드 스펙트럼을 사용하여 이를 삽입한다면 더욱더 효율적인 구조를 설정할 수 있을 것이다. 이는 삽입되는 마크에 해당하는 일종의 핑거프린트 생성 및 검증 단계와 워터마크에 의해 실행되는 삽입 검출 단계를 분리한다는 것을 의미한다.

V. 콘텐츠 유통을 위한 심층암호기술

1. 심층암호를 위한 전자서명 접목

심층암호와 암호학을 접목하기 위해서는 전자서명 기법의 특성을 활용할 수 있을 것이며, 구체적으로 은닉 채널에 해당하는 안전한 통신 방법(secure communication problem), 메시지 인증(message authentication problem) 및 서명 문제(signing problem)로 나눌 수 있다. 이와 같은 세 가지 문제에 기초하여 다양한 공격에 견딜 수 있는 강인성을 제공해야 한다.

심층암호 및 워터마킹 체계가 성공하기 위해서는 다양한 공격에 견딜 수 있는 특성을 제공해야 하며 이를 위해서는 암호학적 관점에서 영지식 증명(zero-knowledge proofs)과 결함 포용 프로토콜(fault-tolerant protocol)이라는 두 가지 개념적 근거에 바탕을 두고 연구되어야 한다. 심층암호와 워터마킹에서 사용하는 채널은 공개되어 있기 때문에 이에 대한 안전성이 취약하다. 따라서 영지식 기반 식별 및 증명 기법을 적용하여 전체 프로토콜에 대한 안전성을 높일 수 있으며, 정보은닉 프로토콜이 영지식으로 수행되므로 콘텐츠에 대한 정보유출을 최소화할 수 있다.

2. 심층암호 기반 콘텐츠 보호

영지식과 같은 암호학적 기법과 더불어 암호학 분야에서의 고급 전자서명 기술을 접목하는 방식이 있다. 그 중에서도 특히 특수 서명을 정보 은닉 및 워터마킹기술에 적용한다.

일반적인 전자서명에서 서명자는 자신이 서명하고자 하는 메시지의 내용을 이미 알고 있다. 또한 서명자의 공개키를 아는 사람은 누구나 서명자의 개입(동의)없이도 서명의 유효성을 검증할 수 있다. 이와 같은 전자서명의 안전성은 복잡도 이론에 근거한다.

익명성(anonymity)과 비연관성(unlinkablity)을 제공하기 위해 제시된 서명 기법이 은닉 서명이므로 이를 활용하여 정보은닉 기술에 적용 가능할 것으로 판단된다. 또한 부인방지 전자서명(undeniable signature)인 경우 S/W에 대한 서명을 한 후에 회사가 이를 배포하는 과정에서 정당한 구매자만이 S/W를 구매하여 이를 검증한 후에 사용 가능한 방식에 해당한다. 또한 사용자 측면에서는 사용하는 S/W에 문제가 발생하였을 경우 서명을 생성한 회사측에 책임이나 의무를 요청할 수 있으며, 회사는 서명 사실을 부인할 수 없는 서명에 해당한다.

부인방지 전자서명은 서명자의 동의 없이는 서명문의 진위를 밝힐 수 없으며, 서명자는 필요시에 제 3 자에게 자신이 발행한 전자서명이 정당한 것임을 입증할 수 있는 방식이다. 이와 같은 부인방지 전자서명은 디지털 콘텐츠에 대한 워터마킹 기법에 적용 가능하다. 즉 부인방지 워터마킹(undeniable digital watermarking) 기법이 가능하다.

기존의 전자 서명은 증명자와 검증자 사이에 도전-응답 단계에 의한 영지식 증명 과정을 수행한다고 볼 수 있다. 그러나, 정보은닉 기법에 기반한 워터마킹 기법인 경우 은닉 정보를 커버 정보에 포함시켜 스테고 정보를 생성하고 이를 수신자에게 전달하게 된다. 따라서 수신자는 은닉된 정보를 검출하게 된다.

물론 공격자 역시 스테고 정보 내에 은닉되어 있을지도 모르는 정보에 대해 각종 공격 기법을 적용하게 된다. 워터마킹 생성자와 검증자간의 관련성을 고찰하였을 경우 기존의 영지식 대화형 기반의 증명보다는 비대화형으로 워터마킹에 대해 검증, 추출하는 과정이 중요할 것이다. 분쟁을 해결하기 위해 Fail-Stop 서명 기법도 사용될 수 있을 것이다. 또한 메시지 복원 기능을 제공하는 은닉 서명 기법이 제공된다면 더욱더 개선된 기법을 제시할 수 있다.

3. 제시한 기술에 대한 고찰

암호학은 효율성(efficiency)과 실행불가능성(infeasibility)이라는 두 가지 전제에 기초하고 있으며, 계산상의 어려움(computational difficulty)과 계산적 구별불가능성(computational indistinguish -ability) 및 시뮬레이션 체계(simulation paradigm)로 나눌 수 있다. 이와 같은 체계를 기반으로 크게 암호 정보에 대한 정의 활동(Cryptographic definitional activity)과 구축 활동(constructive activity)으로 나눌 수 있다.

암호화 체계가 효율성과 실행불가능성에 중점을 둔 반면에 심층암호 기법은 검출이 불가능하도록 하는 기술과 강인성에 기초하고 있다. 또한 엔트로피 기반 정보이론적 측면에 근거하고 있으며 전반적으로 정보은닉(information hiding)을 목적으로 한다고 볼 수 있다. 심층암호 기법 역시 정의 활동과 구축 활동으로 나눌 수 있으며 전체적으로 기존의 암호 체계와 유사한 점이 많다고 판단된다.

본 연구를 통해 기존의 디지털 콘텐츠 저작권 보호 및 유통 구조에 새로운 패러다임을 제시할 수 있을 것으로 예상되며 구체적인 구조는 다음 그림 1과 같다.

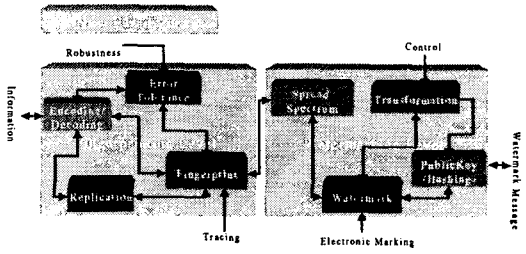

그림 1. 새로운 패러다임 기반 안전한 콘텐츠 유통 기술 구조

상위 계층에 해당하는 핑거프린팅 계층에서는 에러-포용 기능을 제공하는 마크 생성 단계로서 코딩 이론(coding theory)을 사용하여 안전성을 제공하면서 에러 복구 기능을 제공하는 은닉 정보를 생성한다. 핑거프린팅 정보에 의한 추적 기능 또는 저작권 증명 구조, 검출 단계에서의 안전성 역시 상위 계층에서 담당한다.

하위 계층에 해당하는 워터마킹 계층에서는 생성된 정보에 대해 심층암호 기술에 기반한 엔트로피 특성을 적용하고, 은닉하고자 하는 매체의 특성에 따라 적절한 삽입 기법을 적용하여 인식할 수 없으면서 감지불가능한 상태로 정보를 은닉하는 방식을 채택할 필요가 있다. 하위 계층에서는 물리적인 계층에 해당한다고 볼 수 있으며 워터마크에 대한 은닉 및 검출 과정을 담당하면서 스프레드 스펙트럼 방식과 같이 주파수영역에 해당하는 기술 또는 더욱더 견고한 삽입 알고리즘을 적용하여 마킹 과정을 수행한다. 물론 암호학적 접근 기법과 접목하는 것을 지속적으로 추진해야 할 것이다. 결국 정보은닉 구조는 계층적인 구조(*hierarchical architecture*)를 통해 더욱더 안전하고 강인한 정보 체계를 구성할 수 있을 것이다.

VI. 응용 : 공정은닉 기반 콘텐츠 보호기술

1. 공정은닉서명과의 관련성

은닉 서명 기법이 사용자에 대한 익명성을 제공하면서도 필요할 경우 특정 센터에 의한 검증 및 확인 과정을 제공해야 한다. 결국 디지털 콘텐츠에 대해 필요로 하는 경우 저작권에 대한 공개적인 검증 및 확인 기능을 제공할 수 있는 공정 암호화 시스템(fair cryptosystem)이 필요하다. 이와 같은 특성을 제공하는 공정 은닉 서명(fair blind signature)을 통해 콘텐츠에 대한 안전성을 확보할 수 있다. 공정성을 제공하는 디지털 서명 기법과 디지털 핑거프린팅과의 관련성에 대한 고찰을 통해서 암호학적 측면에서의 저작권 보호 기법을 제시한다. 제시하는 기법은 디지털 콘텐츠에 대한 불법 복제 방지 기법으로 발전시킬 수 있으며 다양한 분야에 적용 가능하다.

2. 콘텐츠 유통을 위한 은닉 서명 모델

콘텐츠에 대한 유통을 위해서는 콘텐츠에 대한 저작권 또는 사용권에 대해 워터마킹 또는 핑거프린팅 기법을 적용하게 된다. 저작권 정보에 대해 전자서명한 디지털 콘텐츠는 저작권 메시지에 대한 복원 기능을 제공하는 은닉 서명 기술과 접목할 수 있다.

저작권 복원 기능을 제공하는 은닉 서명에 대한 정의는 다음과 같이 일반적인 은닉 서명 기법과 키 생성 알고리즘은

동일하다. 그러나 대화형 은닉 서명 프로토콜과 검증 알고리즘은 디지털 콘텐츠에 대한 메시지 복원 기능을 제공한다.

[정의 1] 메시지 복원 은닉 서명 (SKG, IP_{MR}, Ver_{MR}).

- SKG - 서명에 필요한 비밀키 및 공개키 (x, y) 를 생성하는 키 생성 알고리즘(signature key generation algorithm).
- IP_{MR} - 서명자와 전송자간의 $(sender(m, y), signer(x))$ 에 해당하고 메시지 복원 기능을 제공하는 대화형 은닉 서명 프로토콜(interactive blind signature protocol). 전송자의 입력은 메시지 m 과 공개키 y 이고 서명자의 입력은 비밀키 x 이다. 서명자는 서명 $s = sender(m, y)_{signer(x)}$ 를 전송한다.
- $Ver_{MR}(y, m, s)$ - 서명 검증 알고리즘은 입력 공개키 y , 서명 s 에 대해서 검증 과정에서 메시지 m 과 동일하면 올바른 서명으로 받아들인다.

디지털 콘텐츠의 저작권에 대한 복원 기능을 제공하는 은닉 서명 기법에 대한 일반화 과정을 통해서 콘텐츠에 대한 안전한 유통 구조를 제시하고자 한다.

3. 제안한 콘텐츠 유통 기법

본 연구에서 제시하는 콘텐츠 유통 기법은 공정 은닉 서명 기법에 기반하여 신뢰 센터가 필요로 하는 경우에 디지털 콘텐츠에 대해 서명 과정을 수행하고 추후에 공개적인 검증 단계를 수행할 수 있다. 구체적인 공정 은닉 서명에 대한 등록 프로토콜과 메시지 복원 공정 은닉 서명 기법은 다음과 같다.

3.1 공정성 확보를 위한 등록 프르토콜

디지털 콘텐츠에 대한 공정성을 확보하기 위해서는 신뢰 센터에 의해서 공개적 검토 가능한 기능을 제공해야 한다. 따라서 전송자 A는 신뢰 센터에 대한 사전 등록 단계를 수행하여 콘텐츠 유통을 위한 비밀 정보를 할당받는다. 전송자는 신뢰 센터로부터 받은 비밀 정보를 사용하여 서명자에게 전달한다. 서명자는 은닉 서명을 수행한다. 서명자에 의해 은닉 서명된 메시지는 다시 전송자에게 전달된다. 등록 프로토콜 RP 는 다음과 같다.

[정의 2] 콘텐츠 유통을 위한 등록 프로토콜 RP

- RP - 전송자와 신뢰 센터간의 $(sender(\delta, y), judge(x))$ 에 해당하고 공정 은닉 서명에 필요한 비밀 정보를 제공하는 대화형 등록 프로토콜. 전송자의 입력은 자신이 생성한 δ 와 신뢰 센터의 공개키 y_J 이고 신뢰 센터의 입력은 자신의 비밀키 x_J 이다. 신뢰 센터는 등록 결과 $v' = sender(\delta, y_J)_{judge(w, x_J)}$ 를 전송한다. 전송자는 v' 에서 콘텐츠에 사용될 정보 v 를 추출한다. 전송자의 δ, v 와 신뢰 센터의 c, v' 는 공정성을 확인할 수 있는 기본 정보에 해당된다. c 는 신뢰 센터에 의한 공개 검증 정보를 포함하고 있다.

3.2 콘텐츠에 대한 공개 검증 기능 제공

안전한 콘텐츠 유통 구조를 제공하기 위해서 구체적으로 공개 검증기능을 제공하는 메시지 복원 전자서명 기법으로 확장하였다. 사전 등록 프로토콜을 수행하여 전송자에 해당하는 키를 할당받고 키 생성 알고리즘을 통해 서명자에 해당하는 키를 생성한다. 또한 메시지 복원 기능을 제공하는 대화형 은닉 서명 프로토콜을 기반으로 콘텐츠에 대한 공개 검증 기능을 제공한다.

[정의 3] 은닉 서명 기반 유통 구조

$(RP, SKG, FIP_{MR}, R, FVer_{MR})$.

- SKG - 사전 등록 프로토콜 RP 에 기반하여 공정 은닉 서명에 필요한 비밀키 및 공개키 (x, y) 를 생성하는 키 생성 알고리즘.
- FIP_{MR} - 전송자와 서명자간의 $(sender(v, m, y), signer(c, x))$ 에 해당하고 메시지 복원 기능을 제공하는 대화형 공정 은닉 서명 프로 전송자의 입력은 등록 단계에서 생성된 v 와 메시지 m 및 공개키 y 이고 서명자의 입력은 공정 프로토콜을 위한 정보 c 와 서명자의 비밀키 x 이다. 서명자는 서명 $s = sender(v, m, y)_{signer(c, x)}$ 를 전송한다.
- R - 은닉 서명에 대해 연관성을 복구할 수 있는 특성을 제공하는 알고리즘. 연관성 정보를 포함하는 $type_I$ 형태의 r_I 과 $type_{II}$ 형태의 r_{II} 를 생성한다. r_I - 서명자의 서명 메시지 (m^*, s^*) 로부터 신뢰 센터 J 는 서명자의 서명에 해당하는 전송자의 메시지 (m, s) 를 연관지을 수 있다. r_{II} - 전송자의 메시지와 서명 (m, s) 에 대해서 신뢰 센터 J 는 해당하는 서명자의 서명 (m^*, s^*) 를 서로 연관지을 수 있다.

o $FVer_{MR}(r, y, m, s)$ - 서명에 대한 공정 검증 알고리즘은 입력으로 연관성 정보 r 과 공개키 y 을 사용하여 해당하는 서명 정보 s 와 메시지 m 을 공개적으로 검증한다.

3.3 콘텐츠 사용자 등록 단계

디지털 콘텐츠에 대한 불법 복제 및 이중 사용이 발생하였을 경우 이를 공개적으로 검증하기 위해 디지털 콘텐츠에 대한 핑거프린팅 기법을 제시한다. 메시지 복원 기능을 제공하는 은닉 서명 기법을 확장하여 공정성을 확보한다. 우선 신뢰 센터에 대한 등록 단계를 수행한 다음 서명자와의 공정 은닉 서명 단계를 수행한다. 우선 전송자 A는 신뢰 센터 J 에 공정 은닉 서명을 위한 등록 단계를 수행한다. 구체적인 수행 단계는 다음과 같다.

단계 1: 등록 요청 단계

단계 1-1: 전송자 A는 랜덤 비밀 정보 $s_A \in Z_q$ 를 생성한다.

단계 1-2: A는 $\delta \equiv g^{s_A} \bmod p$ 를 만족하는 δ 와 신원 정보 ID_A를 신뢰 센터 J 에게 전송하여 등록을 요청한다.

단계 2: 등록 단계

단계 2-1: 신뢰 센터 J 는 공정 은닉 서명에 사용될 정보 $v_j, v_{1-j} \in Z_q$ 와 난수 $w_J \in GF(q)$ 에대한 $t_J \equiv g^{w_J} \bmod p$ 를 생성한다.

단계 2-2: J 는 자신의 데이터베이스에 A에 대한 정보 ID_A, δ 와 공정 은닉 서명 해지 키에 해당하는 v_j, v_{1-j} 를 저장한다.

단계 2-3: J 는 v_j, v_{1-j} 에 대해 해쉬 함수를 적용하여 $c = h(\delta \cdot v_j \| \delta \cdot v_{1-j} \| t_J)$ 를 생성한다.

단계 2-4: 신뢰 센터는 Schnorr 기반 알고리즘을 통해서 s_J 를 생성하고 A에게 메시지 $(\delta \cdot v_j, \delta \cdot v_{1-j}, s_J, c)$ 를 전달한다.

단계 3: 등록 확인 단계

단계 3-1: A는 자신이 생성한 난수 δ 을 사용하여 메시지에 대한 검증에서 J 가 생성한 v_j, v_{1-j} 를 확인한다.

단계 3-2: 등록 단계에서 전달되는 c 값은 전송자가 불확정 전송 단계에서 β_j, β_{1-j} 에 사용하는 것으로 공정 은닉 서명에 대해 서명자가 검증할 수 있다.

3.4 공개 검증 기능 기반 콘텐츠 유통 단계

신뢰 센터에 대한 등록 단계를 거친 후에 전송자와 서명자는 디지털 콘텐츠에 대한 핑거프린팅의 일종으로 은닉 서명 단계를 수행한다. 본 연구에서는 기존의 은닉 서명 기법에 불확정 전송 기법을 적용하여 공정성을 제공하고자 한다. 제시하는 불확정 전송 기반 메시지 복원 공정 은닉 서명 기법은 전송자가 비밀 난수로 선택한 α, β 대신에 등록 단계에서 신뢰 센터로부터 받은 v_j, v_{1-j} 를 사용한다.

단계 1: 불확정 전송 단계

단계 1-1: 전송자 A는 v_j, v_{1-j} 를 사용하여 β_j, β_{1-j} 를 생성한다.

$$\beta_j \equiv g^{v_j + v_{1-j}} \bmod p, \quad \beta_{1-j} \equiv c \cdot (g^{v_j + v_{1-j}})^{-1} \bmod p$$

단계 1-2: A는 β_j, β_{1-j} 를 서명자 B에게 전송한다.

단계 2: 공정 은닉 파라메터 생성 단계

단계 2-1: 서명자 B는 $c \equiv \beta_j \cdot \beta_{1-j} \bmod p$ 를 검증하여 이것이 신뢰 센터가 생성한 c 값과 동일한지 확인할 수 있다.

단계 2-2: 서명자는 자신만의 비밀 난수 $z_j^*, z_{1-j}^* \in Z_q$ 를 생성한다.

단계 2-3: B는 은닉 파라메터에 해당하는 λ_0^*, λ_1^* 및 γ_0, γ_1 를 생성하여 전송자 A에게 전달한다.

$$\lambda_j^* \equiv g^{z_j^*} \bmod p, \quad \lambda_{1-j}^* \equiv g^{z_{1-j}^*} \bmod p$$

단계 3: 메시지 전송 단계

단계 3-1: 전송자 A는 메시지 m 에 대해 아래 수식을 적용하여 r_j 와 m_j^* 를 생성한다.

$$r_j \equiv m^{-1}(\lambda_j^*)^{v_j} y^{v_{1-j}} \bmod p,$$

$$m_j^* \equiv v_j^{-1} \cdot (r_j - v_{1-j}) - \lambda_j^* \bmod q$$

단계 3-2: A는 r_j 와 m_j^* 를 서명자 B에게 전송한다.

단계 4: 공정 은닉 서명 생성 단계

단계 4-1: 서명자 B는 m_j^* 를 사용하여 서명자의 은닉 서명에 해당하는 s_j^* 를 생성한다.

$$s_j^* \equiv x \cdot (m_j^* + \lambda_j^*) - z_j^* \bmod q$$

단계 4-2: B는 s_j^* 를 다시 전송자 A에게 전달한다.

단계 5: 공정 은닉 서명 확인 단계

단계 5-1: 전송자 A는 메시지 복원 공정 은닉 서명에 대한 검증을 위해서 s_j^* 에 대해 $s_j \equiv v_j \cdot s_j^* \bmod q$ 를 계산한다.

단계 5-2: 전송자 A는 s_j 에 대해

$m \equiv g^{-s_j} y^{r_j} r_j^{-1} \bmod p$ 와 같은 메시지 복원 및 검증 단계를 수행한다.

(증명) $m \equiv g^{-s_j} y^{r_j} r_j^{-1} \bmod p$ 에 대한 은닉 서명 검증.

$$\begin{aligned} g^{-s_j} y^{r_j} r_j^{-1} &\equiv g^{-(v_j \cdot s^*)} \cdot g^{(x \cdot r_j)} \cdot m \cdot g^{-z_j^* \cdot v_j} \cdot g^{-x \cdot v_{1-j}} \\ &\equiv m \cdot g^{-v_j \cdot s^*} \cdot g^{x \cdot r_j} \cdot g^{-z_j^* \cdot v_j - x \cdot v_{1-j}} \\ &\equiv m \cdot g^{-v_j \cdot (x \cdot (m_j^* + \lambda_j^*) - z_j^*)} \cdot g^{x \cdot r_j} \cdot g^{-z_j^* \cdot v_j - x \cdot v_{1-j}} \\ &\equiv m \cdot g^{-v_j \cdot x \cdot (m_j^* + \lambda_j^*)} \cdot g^{x \cdot r_j - x \cdot v_{1-j}} \\ &\equiv m \cdot g^{-v_j \cdot x \cdot v_j^{-1} \cdot (r_j - v_{1-j})} \cdot g^{x \cdot (r_j - v_{1-j})} \\ &\equiv m \bmod p \end{aligned}$$

3.5 제안한 기법에 대한 안전성 분석

본 연구에서 제안한 기법인 경우 ElGamal 기반 이산 대수 문제의 어려움에 근거하고 있다. 또한 제안한 기법인 경우 메타-ElGamal 기법의 안전성 및 특성을 나타낸다. 제안한 기법에서 적용한 불확정 전송 기법인 경우 신뢰 센터에 대한 사전 등록 단계를 수행하고 키 생성 단계 및 은닉 파라메터 생성 단계에서 적용된다. 또한 제안한 기법은 신뢰 센터에 의해 $type_I$ 과 $type_{II}$ 형태의 검증 과정을 제공한다. 제안하는 기법의 공정성을 확인하기 위해 $type_I$ 형식의 r_I 과 $type_{II}$ 형식의 r_{II} 에 대해 고찰한다.

신뢰 센터 J 는 r_I 을 통해 서명자의 서명 메시지 (m^*, s^*) 로부터 서명자의 서명에 해당하는 전송자의 메시지 (m, s) 를 연관지을 수 있다. 또한 r_{II} 를 통해 전송자의 메시지와 서명 (m, s) 에 대해서 해당하는 서명자의 서명 (m^*, s^*) 를 서로 연관지을 수 있다. 결국 디지털 콘텐츠에 대한 불법적인 유통이 있을 경우 이를 공개적으로 검증하는 기능을 제공한다.

메시지 복원 기능을 제공하는 은닉 서명 기법은 서명을 수행하는 전송자와 서명자 사이에서 전송자는 자신의 디지털 콘텐츠에 해당하는 메시지 내용을 서명자에게 공개하지 않으면서 서명자에 의해 전자 서명을 수행하는 방식이다. 이때 전송자는 서명자가 서명한 은닉 서명에 대한 확인 과정에서 자신이 생성한 메시지와 동일한 메시지를 복원하게 된다.

또한 본 연구에서 제시한 메시지 복원 공정 은닉 서명 기법인 경우 기본적인 은닉 서명 기능을 제공하면서도 필요로 하는 경우에 신뢰 센터에 의해서 공개적으로 디지털 콘텐츠에 대한 공정성을 확인할 수 있다. 따라서 일반적인 디지털 콘텐츠 시스템에서의 저작권 표기 문제 및 불법 복제 방지와 관련하여 상호 신뢰성을 더욱 향상시킬 수 있다.

VII. 결론

본 연구에서는 심층암호 기반 정보은닉 기술을 디지털 콘텐츠 보호 분야에 적용하였다. 워터마킹, 핑거프린팅 및 DRM 기술을 종합적으로 접목한 새로운 패러다임으로서 오디오, 동영상, 텍스트 등 디지털 콘텐츠의 불법 복제, 불법 사용을 방지하고 콘텐츠의 질, 사용 기간 등에 따라 효율적인 사용 및 유통 구조를 제공하는 것을 목적으로 하였다. 기존의 단일 계층 중심 저작권 보호 기법을 개선하여 전자서명기법을 적용한 저작권 보호 기법을 제시하였다.

본 연구에서 제시된 기술을 적용한다면 콘텐츠 제공자는 인터넷이나 개방된 콘텐츠 유통 채널에서 저작권을 보호하면서 콘텐츠를 배포할 수 있으며, 콘텐츠 사용자는 합법적으로 다양한 판매 조건 하에 콘텐츠를 구매할 수 있고, 구매한 콘텐츠에 관련된 자신의 권리에 따른 권리 행사를 할 수 있다.

콘텐츠의 유통은 콘텐츠의 제작, 판매, 사용, 그리고 보고 과정으로 이루어져 있으며, 전통적인 콘텐츠 유통에 비하여, 패키지화된 콘텐츠, 사용 규칙, 통제 기관 등의 모듈이 추가되어 있다. 콘텐츠 제공자가 제공하는 메타데이터는 사용 규칙을 포함하고 있으며, 콘텐츠와 함께 패키지로 제공될 수도 있고, 독립적으로 제공될 수도 있다. 앞으로 콘텐츠 유통 기술을 구체적인 유통 모델로 정립하고 이를 프로토타입으로 제시하는 것이 필요하다고 판단된다.

참 고 문 헌

[1] Ross Anderson, "Stretching the Limits of Steganography," Information Hiding, Lecture Notes in Computer Science,

Vol.1174, pp.39-48, Springer-Verlag, 1996.

[2] Mike Burmester, Yvo Desmedt, Toshiya Itoh, Kouichi Sakurai, Hiroki Shizuya, Moti Yung, "A Progress Report on Subliminal-Free Channels," Information Hiding, Lecture Notes in Computer Science, Vol.1174, pp.157-168, Springer-Verlag, 1996.

[3] Birgit Pfitzmann, "Information Hiding Terminology," Information Hiding, Lecture Notes in Computer Science, Springer-Verlag, Vol.1174, pp.347-350, 1996.

[4] C. Cachin, "An Information-Theoretic Model for Steganography," Proc of IHW'98, pp.306-318, Springer-Verlag, 1998.

[5] J.Zollner, H.Federrath, H.Klimant, A.Pfitzmann, R.Piotraschke, A.Westfeld, G.Wickee, G.Wolf, "Modeling the Security of Steganographic Systems," Proc. of IHW98, pp.344-354, Springer-Verlag, 1998.

[6] Scott Craver, "On Public-Key Steganography in the Presence of an Active Warden," Proc. of IHW98, pp.355-368, Springer-Verlag, 1998.

[7] Thomas Mittelholzer, "An Information-Theoretic Approach to Steganography and Watermarking," Proc of IHW'99, pp.1-16, Springer-Verlag, 1999.

[8] A. Piva et al., "DCT-based watermark recovering without resorting to the uncorrupted original image," Proceedings of ICIP97, Vol.1, pp.520-523, 1997.

[9] Andreas Westfeld, Andreas Pfitzmann, "Attacks on Steganographic Systems," Information Hiding, Lecture Notes in Computer Science, Vol.1768, pp.61-76, Springer-Verlag, 1999.

[10] I. Cox et al., "Secure spread spectrum watermarking for multimedia," IEEE Trans. On Image Processing, Vol.6, No.12, pp.1673-1687, Dec. 1997.

[11] Ingemar J. Cox, Joe Kilian, Tom Leighton, Talal Shamoon, "A Secure, Robust Watermark for Multimedia," Information Hiding, Lecture Notes in Computer Science, Springer-Verlag, Vol.1174, pp.185-206, 1996.

[12] C. Collberg and C. Thomborson, "Software Watermarking: Models and dynamic embeddings," In Principles of Programming Languages 1999, POPL'99, San Antonio, TX, January 1999.

[13] Lampson, W. B., "A Note on the Confinement Problem," Communications of the ACM, Vol.16, No.10, pp. 613-615, 1973.

[14] A. Z. Tirkel, G. A. Rankin, R. G. Schyndel, W. J. Ho, N. R. A Mee, C. F. Osborne, "Electronic watermark," Dicta-93, pp.666-672,1993.

[15] A. Z. Tirkel, R. G. Schyndel, C. F. Osborne, "A two-dimensional digital watermark," ACCV'95, pp. 378-383, 1995.

[16] K. Matsui, K. Tanaka, "Video-Steganography : How to secretly embed a signature in a picture," IMA Intellectual Property Project Proceedings, Jan, pp.187-206, 1994.

[17] J. K. O Ruanaidh, W. J. Dowling, F. M. Boland, "Phase watermarking of images," IEEE International Conference on Image Processing, Sept. 1996.

[18] C. Cox, J. Killian, T. Leighton, T. Shamoon, "Secure spread spectrum communication for multimedia," Technical Report, NEC, Research Institute, 1995.

[19] J. F. Delaigel, J. M. Boucqueau, J. J. Quisquater, B. Macq, "Digital Images protection techniques in a broadcast framework: an overview," Univ. Catholique de Louvain, 1996.

[20] J. Zhao and E. Koch, "Embedding robust labels into images for copyright protection," Proceedings of Intern. Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, pp.242-251, 1995.

[21] Chor, B., A. Fiat, and M. Naor, "Tracing Traitors," in Advances in Cryptology - Crypto94, Lecture Notes in Computer Science, Springer-Verlag, pp.257-270, 1994.

[22] Brigit Pfitzmann, "Trials of Traced Traitors," Information Hiding, Lecture Notes in Computer Science, Vol.1174, pp.49-64, Springer-Verlag, 1996.

[23] Dan Boneh, James Shaw, "Collusion-Secure Fingerprinting for Digital Data," Advances in Cryptology - Crypto95, Lecture Notes in Computer Science, Springer-Verlag, Vol.963, pp.251-263, 1995.

[24] Birgit Pfitzmann, Matthias Schunter, "Asymmetric Fingerprinting," Advances in Cryptology - EuroCrypt'96, Lecture Notes in Computer Science, Springer-Verlag,

Vol.1070, pp.84-95, 1996.

[25] Birgit Pfitzmann, Michael Waidner, "Anonymous Fingerprinting," Advances in Cryptology - EuroCrypt'97, Lecture Notes in Computer Science, Springer-Verlag, Vol.1233, pp.88-102, 1997.

[26] Dan Boneh, Matthew Franklin, "An Efficient Public Key Traitor Tracing Scheme," Advances in Cryptology - Crypto99, Lecture Notes in Computer Science, Springer-Verlag, Vol.1666, pp.338-353, 1999.

[27] Hans-Jurgen Guth, Brigit Pfitzmann, "Error- and Collusion-Secure Fingerprinting for Digital Data," Information Hiding, Lecture Notes in Computer Science, Vol.1768, pp.134-145, Springer-Verlag, 1999.

[28] Jan Camenisch, "Efficient Anonymous Fingerprinting with Group Signatures," Advances in Cryptology - ASIACRYPT 2000, Kyoto, Japan, LNCS 1976, pp.415-428, 2000.

[29] Andre Adelsbach, Birgit Pfitzmann, Ahmad-Reza Sadeghi, "Proving Ownership of Digital Content," Information Hiding, Lecture Notes in Computer Science, Vol.1768, pp.117-133, Springer-Verlag, 1999.

이 형 우(Hyung-Woo Lee) 정회원

1994년 2월 고려대학교 전산과학과 (이학사)
1996년 2월 고려대학교 전산과학과 (이학석사)
1999년 2월 고려대학교 전산과학과 (이학박사)
1999년 3월 ~ 현재 천안대학교 정보통신학부 교수
<관심분야> : 암호학, 정보보호, 전자상거래, 디지털 콘텐츠

한 군 희(Kun-Hee Han) 종신회원

1989년 2월 충북대학교 컴퓨터공학과 (공학사)
1994년 8월 경남대학교 컴퓨터공학과 (공학석사)
2000년 8월 충북대학교 컴퓨터공학과 (공학박사)
2001년 3월 ~ 현재 천안대학교 정보통신학부교수
<관심분야> : 영상신호처리, 패턴인식

전 병 민(Byung-Min Jun) 종신회원
1976년 2월 한국항공대 전자공학과(공학사)
1978년 2월 연세대학교 전자공학과(공학석사)
1988년 8월 연세대학교 전자공학과(공학박사)
1978년 8월 ~ 1982년 3월 공군사관학교 전자과 전임강사
1982년 4월 ~ 1986년 2월 동양공전 통신과 조교수
1986년 3월 ~ 현재 충북대학교 컴퓨터공학과 교수
1991년 1월 ~ 1992년 1월 미국 미시간대학교 교환교수
<관심분야> : 영상처리, 디지털 신호처리