

# Digital Watermarking 기술동향에 관한 연구

강민식\*

## 요약

최근 멀티미디어 산업의 팽창과 네트워크 기술의 발전으로 문서, 음성, 사진 및 동영상 데이터 등의 다양한 콘텐츠들에 대한 저작권 보호의 필요성이 절실히 요구되게 되었다. 현재 사용되는 암호화 기법의 콘텐츠 보호는 디지털 콘텐츠에 대하여 접근이 극히 제한된다는 단점과 한번 암호가 풀린 콘텐츠는 더 이상 보호 할 수 없다는 한계를 가지고 있다. 이러한 문제점을 해결하기 위한 하나의 수단으로 디지털 워터마크(Digital Watermark) 기법이 제안 되었다. 본 연구에서는 디지털 워터마크 기술에 대한 표준화, 기술 동향, 향후 발전방향등에 대한 국내의 연구 내용을 조사하고, 향후 기술적인 동향을 알아본다.

## A Study on the Trend of Digital Watermarking Technology

Min-Shik Kang\*

### Abstract

Recently it is important to protect the digital contents copyright because the multimedia industry is growing rapidly and the network technology is highly developed. Current digital content protection methods have disadvantage that there is very hardly accessible to the digital contents and also it has a limit that it cannot protect the contents once the encrypted contents decrypt. In order to solve this problem, digital watermarking technology has been introduced. This study presents the trend of digital watermarking technology, especially standardization and the trend of digital watermarking algorithms.

Key words : Digital Watermark, Information Security

### 1. 서론

최근 멀티미디어 산업의 팽창과 다양한 콘텐츠들이 디지털화 되어 효율적인 저장, 접근 및 이용이 가능하게 되었다. 이와 같은 디지털 매체의 수요의 증가는 웹(World Wide Web) 등을 통하여 데이터를 원본과 똑같은 형태로 개인용 컴퓨터를 통하여 저장 할 수 있다는 장점 때문이다. 그러나 바로 이 점이 사용자가 그 정보를 이용하는 데 필요한 허가, 보상 및 제한의 문제, 그리고 그 정보의 소유권에 관한 권리 등 다양한 문제를 발생시켰다. 현재 사용되는 암호화 기법의 콘텐츠 보호는 디지털 콘텐츠에 대하여 접근이 극히 제한된다는 단점과 한번 암호가 풀린 콘텐츠는 더 이상 보호 할 수 없다는 한계를 가지고 있다. 이러한 문제점을 해결하기 위하여 디지털 워터마크(Digital Watermark) 기법이 제안 되었다[1]. 디지털 워터마크는 멀티미디어 콘텐츠 데이터에 인간이 인지 할 수 없도록 삽입한 디지털 코드를 말하고 저작권 문제 발생 시 은닉된 정보를 추출하

여 콘텐츠에 대한 저작권을 보호받는 기술이다. 또한 워터마크라는 기술은 저작권 보호 뿐 만 아니라 인증이나 복사 제한(copy control)과 같은 기술로의 응용도 가능하다.

### 2. Digital Watermarking

1995년부터 디지털 워터마크 분야는 실험적 알고리즘의 분석에서 이미지 모델링, 디지털 통신 기술, 암호화 기술 등 여러 가지 다양한 분야의 알고리즘들을 활용하여 보다 정교하고 우수한 알고리즘과 시스템들이 발표되기 시작하였다. Visible Watermarking은 로고와 같은 가시적인 패턴을 이미지에 삽입하거나 오버레이(Overlay) 시킨다. IBM Digital Libraries project가 이러한 대표적인 사례이다[2]. Invisible Watermark는 I. J. Cox et al를 비롯하여 1995년 이후 다양한 워터마크 알고리즘들이 개발되었다[3].

\* 본 연구는 2005년 남서울대학교 교내연구비 지원에 의하여 수행되었음.

※ 제1저자(First Author) : 강민식

접수일 : 2005년 4월 3일, 완료일 : 2005년 4월 10일

\* 남서울대학교 교수

mshang@nsu.ac.kr

Digimarc사는 각 픽셀에서 작은 랜덤한 수를 더하거나 빼는 방법을 사용하여 워터마크를 삽입하였다[4]. 영상 데이터를 DFT, DCT, Wavelet 등과 같은 변환으로 주파수 공간으로 영상 데이터를 변환한 후 주파수 영역 중에서 시각적으로 덜 민감한 성분에 적응적으로 워터마크를 삽입하는 방법이다[5],[6]. 이 방법은 여러 가지 신호처리에 취약한 공간영역 워터마크의 단점을 보완해 줄 수 있었다. 또한 MPEG-1, 2에 적합한 워터마크 알고리즘들도 개발되었다[7],[8]. 응용 분야에 따라 검출 방식을 달리 하게 되는데, 일반적으로 1990년대 중반까지 원본 영상을 이용한 검출 방식(Private water marking)을 중심으로 개발되어지다가 현재는 원본 영상을 이용하지 않는 검출 방식(Oblivious Water marking)을 적용하여 개발되어지고 있다[9],[10]. 또한 영상에 은닉 정보의 삽입량을 늘리는 방법이나 고화질 영상인 HDTV 등에서 콘텐츠의 화질 열화를 최소화하는 문제 등에 대한 다양한 연구가 진행되고 있다.

### 3. Digital Watermarking 기술의 활용 방안

Digital Watermarking 기술의 활용 방안의 경우 매우 광범위하다.

- 저작권 보호 : 지적 재산권의 보호를 위해서 콘텐츠 소유자가 자신의 콘텐츠에 저작권 정보를 나타내는 워터마크를 삽입하여 사용자가 자신의 저작권을 침해하거나, 불법으로 사용했을 때 자신의 소유권을 증명할 수 있는 자료로 사용할 수 있다.
- Copyright 제어 : 복사 횟수의 제한 및 복사의 권한, 복제 방지 등을 제어 할 수 있고, 재생의 횟수 역시 제어할 수 있다. 예를 들면 MP3 플레이어, PDA 등의 휴대용 기기(Portable Device)나 DVD 플레이어에 워터마크 decoder를 장착하여 오디오, 비디오 등의 불법 사용을 방지 할 수 있다.
- 방송 모니터링 : 상업 광고 속에 워터마크를 삽입한 후 자동화된 모니터링 시스템에 의해 광고가 계약대로 방송되고 있는지를 확인할 수 있다. 광고뿐만 아니라 TV 프로그램도 이러한 방법으로 보호 될 수 있다. 방송 감시 시스템은 모든 방송 채널을 체크 할 수 있어 발견 여부에 따라 TV 방송국에서 과금 할 수 있다.
- 불법 복제 추적(fingerprint) : 워터마크로서 삽입하는 정보를 저작권자나 판매자가 아닌 구매자의 정보를 삽입하게 되는데, 이를 핑거 프린트라고 부른다. 만약 불법으로 유통되고 있는 콘텐츠에서 핑거 프린트 정보를 추출하게 되면, 그 콘텐츠가 어떤 구매자에게 판매된 콘텐츠인지를 식별(Identification) 할 수 있게 된다. 또한, 소비자의 소비 행태와 유통의 경로에 대한 정보 역시 획득할 수 있다.
- 위/변조 방지 : 각종 계약서류, 사진이나 그림 등의 작품, 그리고 동영상 등이 디지털로 되어 있다면 디지털의 특성상 여러 가지 프로그램을 사용하여 누구나

쉽게 위조나 변조를 가할 수 있다. 이런 일들을 방지하기 위해 디지털 콘텐츠에 워터마크를 삽입하여, 위조나 변조를 시도하면 원본이 아니라는 것을 증명해줌과 동시에 변조된 위치 파악을 할 수 있다. 또한, 의료 영상 등과 같이 특수한 목적에 따라서는 인종된 콘텐츠의 경우 워터마크가 삽입되기 이전의 콘텐츠를 다시 만들 수 있는 경우도 있다. 최근에는 깨진 부분을 복구할 수 있는 워터마크 기법과 압축이나 보통의 처리에는 반응하지 않고, cut-and-paste와 같은 의도적인 공격에만 반응하는 기법이 활발히 연구되고 있다.

### 4. Digital Watermarking 기술의 표준화 동향

오디오 분야는 SDMI(Secure Digital Music Initiative)이다. SDMI는 디지털 음악파일 포맷개발을 추진하기 위한 미국 레코딩 협회인 RIAA (Recording Industry Association of America)를 중심으로 한 인터넷 음반업계의 컨소시엄을 말한다. 특히 최근 우리나라를 포함한 일본, 미국 등 인터넷을 통해 급속도로 확산되고 있는 MP3의 불법 복제의 경우 저작권 침해에 관한 논란이 되고 있는데, SDMI에서는 워터마크 기술로 이러한 문제를 해결하려 했다.

비디오의 경우에는 MPEG의 동영상 표준화 그룹 중 MPEG-4 IPMP (Intellectual Property Management and Protection)가 있다. MPEG- 4는 관련된 요소들의 다양성을 기초로 하므로 결국 지적 소유보호를 위한 특정 물의 설계에 대한 요구를 표준 내에서 실행하기란 어려운 일이다. IPMP는 이러한 응용들의 다양성을 포괄하는데 있다. MPEG-4의 IPMP 구조는 특정 IPMP Solution Domain이 가장 폭 넓게 적용하게 하고 충돌 해결을 해결 할 수 있는 여러 형태로 디자인되었다. IPMP의 일반적 인터페이스는 그림 1과 같다.

그림 1에서 국제 표준안인 MPEG과 비표준인 IPMP System을 나타내며 이 두 가지(MPEG-4와 IPMP)가 독립적인 점을 설명하고 있다. 이 독립성의 요점은 IPMP 인터페이스다.

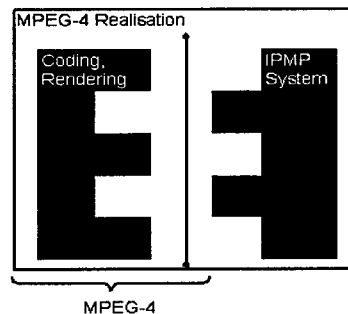


그림 1. High Level view of The IPMP Architecture

MPEG-4에서 IPMP 시스템이 정형화 된 것이 아니

라 MPEG-4 IPMP 인터페이스가 표준화 된 것이며 MPEG-4 시스템 구조의 확장에서 디자인되었다.

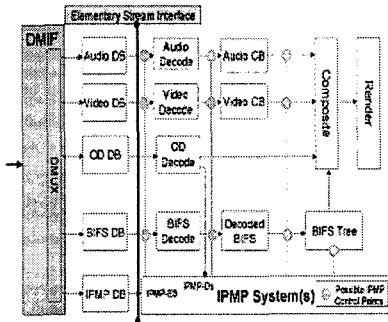


그림 2. IPMP Framework in the ISO/IEC 14496 Terminal Architecture

그림 2는 모든 메커니즘의 바이패스(Bypass) 옵션을 포함하여 최대한 포용력 있게 설계되었다.

### 5. 디지털 워터마크 기술의 동향

일반적으로 Digital Watermarking 기술은 공격에 대한 내성에 따라서 크게 두 가지 정도로 나눌 수 있다. 하나는 Robust Watermarking 기술로 이는 가장 일반적인 형태의 워터마크로 일반적인 영상 혹은 음성 처리 등에 강인하게 디자인 하고 주로 소유권 주장 등에 관련한 목적으로 사용한다. 또 하나는 Fragile Watermarking 기술로서 대부분 인증이나 무결성에 관련된 목적에 적합하도록 디자인한다. 이 경우 영상 혹은 음성이 변형될 경우 이 변형 여부를 판단하여 변형된 위치 등에 대한 정보를 확인할 수 있다.

본 장에서는 현재까지 개발된 이미지 알고리즘을 중심으로 고려하여 최근 제안된 알고리즘을 소개 하고자 한다. 5.1에서는 워터마크 알고리즘의 개발 시 고려 사항을 5.2에서는 최근 제안된 원본을 사용하지 않는 워터마크 기법(Oblivious Watermarking)을 중심으로 소개한다.

#### 5.1 워터마크 알고리즘의 개발 시 고려 사항

워터마크의 적용분야와 목적에 따라, 워터마크 알고리즘은 다양하게 디자인 되고 있다. 현재 워터마크의 비가시성(Imperceptibility)은 일반적인 고려 사항이다. 부가적인 고려 사항들은 다음과 같이 정리 할 수 있다.

- 워터마크의 삽입 강도  
화질 열화와 워터마크 삽입 강도의 관계(trade-off)는 일반적으로 잘 알려져 있다. 따라서 인간시각 특성(HVS : Human Visual System) 등을 고려해서 알고리즘을 디자인해야 한다.
- 강인성

지금까지 제안된 알고리즘 중 모든 공격에 완벽하게 대응하는 알고리즘은 존재하지 않는다. 따라서 실제 적용할 수 있는 일반화 된 공격 및, 각 적용분야에서 일어날 수 있는 공격에 대한 강인성을 우선적으로 고려해야 한다. 영상에 대한 공격 방법은 상당히 다양한데, 이를 정리해 보면 다음과 같다.

- ▶ Signal processing 공격
  - noise-like 공격: Gaussian noise 등
  - filtering : low-pass filtering 등
  - 압축 : JPEG, MPEG 등
  - desynchronization 공격
  - rotation, aspect ratio change, cropping 등
  - D/A & A/D
- ▶ Cryptographic 공격
  - deadlock problem 공격 등
- ▶ Statistical 공격
  - collusion 공격, frame averaging 등
- ▶ Protocol 공격
  - copy Attack 등
  - Watermark security and Keys

저작권 보호와 같은 분야에서는 삽입된 정보에 대한 비밀성이 절대적으로 필요하다. 따라서 비밀키(secret key)를 적용하여 키의 소유자만이 워터마크 삽입과 검출을 할 수 있게 한다. 이 때 인증되지 않은 사용자에 대해서는 워터마크의 삽입 유무나 삽입 정보에 대한 어떠한 정보도 알 수 없게 하는 방식이 있고, 사용자 누구에게나 워터마크의 삽입 유무에 대한 정보는 제공하지만 삽입 정보에 대해서는 인증된 사용자에게만 제공하는 방식이 있다. 이러한 방식을 제공할 수 있는 것은 다중 워터마크(Multiple Watermark) 알고리즘을 적용하여 Joint public/ private watermark 방식을 사용할 수 있기 때문이다[11]. 위에서 언급한 모든 방식은 워터마크 알고리즘이 알려져도 워터마크를 추출할 수 없게 해야 한다.

#### 5.2 디지털 워터마크 알고리즘 동향

현재 제안되는 대부분의 알고리즘들은 Oblivious Detection을 위한 알고리즘들이 대부분이다. 이러한 알고리즘들의 예는 다음과 같다.

##### 5.2.1 The Patchwork Algorithm

1995년 Bender et al 을 예로 들면 비밀키(secret-key)로 의사랜덤(pseudorandom) 방식의 수열을 삽입함으로써 워터마크 검출 시 저작권자만이 이 키를 소유하고 있어 워터마크를 검출 할 수 있다[12]. 기본적으로 워터마크 삽입 과정에서는 비밀키 K를 적용하여 영상을 두개의 셋으로 랜덤 하게 분리한다. 분리한 각각의 서브셋(subset) 안의 픽셀을 다음과 같이 변형한다.

$$\tilde{b}_i = b_i - 1 \quad (1)$$

따라서  $a_i$ 에는 1씩을 luminance 성분에서 더하고  $b_i$ 에는 1씩을 감소한다. 검출 과정에서는 K를 적용하여 다음과 같이 검출한다.

$$S = \sum_{i=1}^n (\tilde{a}_i - \tilde{b}_i) \quad (2)$$

영상에 워터마크가 삽입되어 있다고 가정하면 S는  $2n$ 에 근접한 값이 될 것을 예상할 수 있다. 반면에 워터마크가 삽입되지 않은 영상은 0에 가까운 값을 나타낸다. 이러한 검출 과정은 다음과 같은 통계적 가정에 기인한다.

$$E[S] = \sum_{i=1}^n (E[a_i] - E[b_i]) = 0 \quad (3)$$

랜덤 하게 영상을 몇 개의 영역으로 나누었을 때 각 서브셋의 픽셀들은 i.i.d. (independent identically distributed)라고 가정하기 때문에 비밀 키의 소유자만이  $2n$ 에 가까운 값을 추출할 수 있게 된다.

### 5.2.2 Public Key 기반의 워터마크 삽입 및 검출

이 시스템에서는 공개키와 비밀키 두 가지를 사용하는데 워터마크 삽입 시에는 비밀키를 적용하고 워터마크 검출 과정에서는 공개키를 적용하는 것이다. Hartung 과 Girod는 SS(spread spectrum) 방식의 공개키 기반 워터마크 방식을 소개하고 있다[11]. 여기서 direct sequence technique은 확산과 역 과정을 위하여 확산된 수열 S가 필요하다. 비밀키를 가진 소유자만이 워터마크로 삽입된 정보를 모두 확인 할 수 있는 반면에 공개키를 소유한 자는 워터마크 정보의 일부만을 검출 할 수 있게 된다.

### 5.2.3 Psychovisual 워터마크를 위한 Predictive coding

Predictive coding은 소스코딩에서 널리 사용되는 방식이며 이전 신호로부터 새로운 값을 예측하는 것이다. 예를 들어 영상의 픽셀은 이웃 픽셀의 값과 높은 상관도를 가진다. 따라서 Predictive coding이라는 것은 원 픽셀 값과 예측 값 사이의 에러를 코딩하는 것이다. 실제로 이러한 에러는 평균이 0이고 분산 값이 매우 작은 상태의 분포를 가지고 있다. 이 분포는 HVS (Human Visual System)에 의해서 texture, 그리고 에지 부분이 평탄 영역에 비해서 워터마크 삽입 위치로 적합한 것으로 알려져 있다[13]. 또 이러한 코딩방식은 원본데이터를 사용하지 않는다.

### 5.2.4 그 밖의 워터마크 알고리즘

일반적인 영상처리와 영상 혹은 동영상 압축에 관련

해서 워터마크를 삽입하기 적절한 공간은 주파수 공간이라고 알려져 있다. 그 중 한가지로 DFT(Discrete Fourier Transform)를 이용하여 워터마크를 삽입하는 방법이 있다. 이 공간은 진폭 성분과 위상 성분으로 이루어지는데 진폭성분은 워터마크 삽입강도나 화질열화에 대한 조절이 비교적 쉽다는 장점을 가지고 있으나 영상 대부분의 중요 정보가 위상성분에 포함되어 있다는 단점이 있다. 이와는 반대로 위상성분의 경우 삽입강도나 화질열화에 대한 조절이 어려운 단점을 가지고 있다. DCT(Discrete Cosine Transform)공간을 사용하는 방법의 경우에는 JPEG이나 MPEG의 특성을 이용할 수 있는 장점이 있다. 또한, Fourier-Mellin Transform의 경우 일반적인 주파수 공간과는 다른 독특한 특성을 가지고 있는데 DFT한 후 진폭성분만을 이용하여 log-polar mapping을 적용하고 다시 DFT한 경우 영상 이동이나 회전 사이드변화에 대해 불변의 공간을 만들 수 있다[14]. 이 공간에 워터마크를 삽입할 경우 이러한 변화에 대해서는 아무런 영향을 받지 않는다. 하지만 이 공간 역시 모든 공격에 대해서 불변한 것이 아니어서 극히 제한적이다. Wavelet Domain의 경우 JPEG-2000에 적용되면서 이 공간을 이용하여 워터마크 알고리즘을 적용하는 사례가 늘어났다. Kunder et al이 대표적인 사례이다[15].

## 6. 향후 개발 방향

앞에서 언급한 워터마크 알고리즘들은 일반적으로 사용되어 지는 기법들의 몇 가지를 제시한 것에 불과하다. 현재 다양한 알고리즘들이 워터마크라는 기술이 적용 대상과 관련해서 발전되어 지고 있다. 3차원 그래픽 이미지에 적용하는 워터마크 알고리즘이나 문서에 적용되는 알고리즘 등의 저작권 보호를 위한 워터마크 기법들뿐만 아니라 인증을 위한 워터마크 알고리즘도 현재 개발되거나 개발 중에 있다. 하지만 오디오 워터마크나 이미지 혹은 비디오 워터마크 분야 외의 나머지 분야들에서는 아직 이렇다 할 성과를 나타내고 있지 못하고 있고 다양한 공격 기법에 따라 현재 개발된 알고리즘들의 단점이 파악되고 있는 것도 사실이다. 또한 표준화에 관련되어서도 아직 구체적인 성과를 나타내고 있지 못하는 실정이다. 또한 현재 신호처리에 관련된 분야나 특히 통신 분야(실질적으로 통신 개념을 디지털 워터마크 분야에서 많이 적용하였다.)등 관련 분야의 발전에 따라서 워터마크라는 분야도 발전할 수 있는 가능성과 이와 반대로 예상치 못한 공격 또한 새로 발생할 수 있다.

따라서 디지털 워터마크는 적용 대상에 따라, 혹은 관련 분야의 성과 또는 현존하는 공격에 관한 구체적인 연구 등에 관련하여 개발되어 질 것이다.

## 참 고 문 헌

- [1] Tanaka, K., Y. Nakamura, and K. Matsui, "Embedding Secret Information Into a Dithered Multilevel Image," in Proceeding of the 1990 IEEE Military Communications Conference, 1990, pp. 216-220.
- [2] Braudaway, G. W., K. A. Magerlein, and F. Mintzer, "Color correct Digital Watermarking of Images," US patent No. 5,530,759, 1996.
- [3] I. J. Cox, J. Kilian, F. Thomson Leighton and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. on image processing, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.
- [4] F. Takahashi, "Digital watermak safe- gurards multimedia copyright", Nikkei Electronics Asia, Vol.6, No.5, pp.46-52, 1997
- [5] I. J. Cox, J. Kilian, T. Leighton, T. Shamoon, "Secure spread spectrum watermarking for images, audio, and video", Proc. IEEE internet. Conf. on Image Processing(ICIP'96) Vol.III, Lausanne, Switzerland. 16-19, September 1996. pp.243-246
- [6] F. Hartung and B. Girod: "Digital Watermarking of Raw and Compressed Video", Proc. European EOS/SPIE Symposium on Advanced Imageing and Network Technologies, Berlin, Germany, Oct. 1996
- [7] F. Hartung and B. Girod, "watermarking of MPEG-2 Encoded Video Without Decoding and Re-encoding", Proceedings Multimedia Computing and Networking 1997 (MMCN97), San Jose, CA, February 1997.
- [8] G.C.Langelaar, R.L. Lagendijk, J.Biemond "Real-time Labeling Methods for MPEG Compressed Video" 18th Symposium on Information Theory in the Benelux, 15-16 May 1997, Veldhoven, The Netherlands.
- [9] Wenjun Zeng, Bede Lium, "A Statistical Watermark Detection Technique Without Using Orginal Images for Resolving Rightful Ownerships of Digital Images", IEEE Transactions on Image Processing, Vol. 8, N.11, 1999.
- [10] Sviatoslav Voloshynovskiy, Alexander Herrigel, Nazanin Baumgarther and Thierry Pun, "A stochastic approach to content adaptive digital image watermarking," In International Workshop on Information Hiding, Vol. LNCS 1768 of Lecture Notes in Computer Science, pp. 212-236, Springer Verlag, Dresde, Germany, 29 September-1 October 1999.
- [11] Hartung, F., and B. Girod, "Fast Public-Key Watermarking of Compressed Video," in Proceeding IEEE International Conference on Image Processing 1997, vol. 1, Santa Babara, California, USA, Oct. 1997, pp 528-531.
- [12] Bender, W., D. Gruhl., and N. Morimoto, "Techniques for Data Hiding," in proceedingf of the SPIE 2420, Storage and Retrieval for Image and Video Databases III, 1995, pp.164-173.
- [13] Matsui, K., and K. Tanaka, "Video- steganography: How to Secretly Embed a Signature in a picture," Jornal of the Interactive Multimedia Association Intellectual Property project, vol. 1, no. 1, 1994, pp.187-206
- [14] Ruanidh, J. J. K., and T. Pun, "Rotation, Translation and Scale Invariant Digital Image Watermarking," in Proceedings of the International Conference on Image Processing, vol. 1, Santa Babara, California, Oct. 1997, pp. 536-539.
- [15] Kunder, D., and D. Hatzinakos. "A Robust Digital Image Watermarking Method Using Wavelet-Based Fusion," in Proceedings of the Internatinal conference on Image Processing, vol. 1, Santa Babara, California, Oct. 1997, pp.544-547.

## 강 민 식



1986년 한양대학교 산업공학과(학사)  
 1988년 한양대학교 산업공학과(석사)  
 2002년 한양대학교 산업공학과(박사)

1990년 ~ 2000년 : 신도리코 경영정보실 개발팀장  
 2000년 ~ 2002년 : kcc정보통신 기술솔루션사업부장  
 2003년 ~ 현재 : 남서울대학교 교수  
 관심분야 : IT컨설팅, 정보보호, ERP, SCM