

비밀정보 분할 방식을 적용한 워터마크 삽입·추출 방법

서창호*, 김석우**, 성열욱*

* 공주대학교 응용수학과(정보보호전공)

** 한세대학교 컴퓨터정보통신공학부

요 약

본 논문에서는 디지털 매체의 저작권 보호하기 위해 비밀정보 분할(secret sharing) 방식을 적용하여 보다 효율적인 워터마크를 추출하는 기법을 제안 하였다. 이를 위해 원 영상을 DCT 변환한 후 주파수 영역에 (n,k) ($n \geq k$) 비밀정보 분할 방식을 적용하여, 생성된 원 마크의 n 개의 정보를 삽입하고, 추출시 마크의 n 개의 정보들 중 k 개만의 정보를 추출하여 마크를 복원할 수 있다.

On the watermark insertion and extraction methods using the secret sharing method

Chang-Ho Seo*, Seok-Woo Kim**, and Yeoul-Ouk Sung*

ABSTRACT

This paper proposes a method which inserts watermark created by secret sharing method and then extracts it from watermarked image for the protection of copyrights of digital images. To do this, after image's DCT transform, once some values created by Key sharing method which used Lagrange interpolation are inserted into a frequency domain, one can recreate original watermark even if only k seeds are extracted among n of inserted seeds ($n \geq k$).

+.이 논문은 2001년도 정보통신부 대학기초사업(2001-018-3) 지원에 의해 연구 되었음.

1. 서 론

컨텐츠의 저작권 보호를 실세계에서 이뤄내기 위해서는 컨텐츠의 복사방지가 원천적인 방법임에도 불구하고 이를 구현하여 사용하기에는 너무도 어려운 점이 있어, 컨텐츠의 사용 규제(control)를 통하여 디지털 컨텐츠의 저작권이나 보호를 하고 있는 사항이다. 이러한 보호의 방법은 위에서 설명한 것과 같이 사용 전에 시행하는 사용 규제(usage control)와 불법적인 사용을 발견했을 경우 이를 판별하는 사후 규제 방법으로 나눌 수 있다. 주로 저작권 보호(copyright protection)라고 하면 사용자의 인증(authentication)을 통한 사용 규제가 주된 내용이 되며, 워터마크(watermark)라는 방법은 사후 법적인 문제에 해결책으로 제시 될 수 있다. 이런 여러 가지 연구방법 중 저작권 보호를 위한 디지털 워터마크는 디지털 데이터에 저작자의 서명과 같은 변형을 가함으로써, 인간이 시각적으로 구별할 수 없도록 소유권 정보(마크)를 삽입함으로써 이후 저작권 문제가 발생했을 경우 소유권 인증의 한 방법으로 제시한다. 이러한 방법으로 n 개의 분할된 마크를 디지털 데이터에 삽입하고, 삽입된 정보로부터 분할된 n 개의 마크의 정보를 가지고 원상을 추출한다. 기존의 워터마킹에 대한 연구는 변환식을 이용하지 않는 방법으로 데이터에서 LSB(Least Significant Bit)를 임의로 선택하여 정보(information)를 넣는 방법, 문서 출력시에 문자간의 간격을 조정하여 정보를 넣는 방법, 희미한 기하 패턴을 첨가하는 방법 등이 있으며 주파수 변환 DCT[1,3], DFT[5], Wavelet[4] 등이 있다.

본 논문에서는 기존의 워터마크에서 n 개의 분할된 마크를 디지털 데이터에 삽입하여, 삽입된 데이터로부터 n 개의 분할된 마크를 추출하는데 반에서, (n,k) ($n \geq k$) 키 분할 방식을 이

용하여 원본 영상 1/4 영역 안에서 요구되는 분할 정보 k 개의 분할된 정보로부터 정확히 마크 및 효율적으로 마크를 추출할 수 있는 방법을 제안한다. 워터마크 삽입·추출에 대한 방식과 함께 정보보호 기법을 적용한 새로운 방법을 제시한다. 본 논문의 구성은 다음과 같다. 2장에서는 (n,k) 비밀정보 분할 방식 및 워터마크 기술에서 가져야 하는 요구 사항들을 살펴본다. 3장에서는 (n,k) 비밀정보 분할 방식을 적용한 효율적인 삽입·추출하기 위한 워터마크 생성 시스템의 전체적인 구성 및 삽입·추출 과정을 설명한다. 4장에서는 워터마크에서 가져야 할 안전성에 대한 실험 결과를 설명하며, 5장은 결론부이다.

2. 준비 정리

본 장에서는 워터마크가 갖추어야 할 요구 사항에 대해서 설명하고, 기존의 워터마크 삽입·추출 방법 및 비밀 정보 분할 방식에 대해서 설명한다.

2.1 워터마크

워터마킹(watermarking)은 어떤 미술 작품이나 책의 저자나 주인이, 이 작품은 자신의 것이라는 것을 표시하기 위해 육안으로는 보이지 않는 투명한 형태의 표시를 해 두는 것을 말한다. 이러한 개념을 컴퓨터에 적용한 것이 바로 디지털 워터마킹이다. 비디오나 오디오와 같은 멀티미디어 파일이나 영상 파일, 사진 파일 등에 보이지 않는 작은 수정을 가함으로써, 소유권 정보를 인코딩하는 과정이다.

주어진 원 영상(A)에 레이블(label) $S = \{S_1, S_2, \dots, S_n\}$ 을, 부호화 과정 E 을 통하여 삽입하면 워터마크가 내장된 영상 $A' = E(A, S)$ 를 얻을 수 있다. 이때 레이블 S는 영상에 표시된

워터마크가 된다. 테스트 영상 B(워터마크가 삽입되었거나, 삽입되지 않았거나, 손상된 영상)에 대한 소유권을 판정하는 과정은 B 또는 원 영상 A를 입력으로 받아 복호화 과정 D를 통해 레이블 $S'=D(A, B)$ 를 추출한다. 추출된 레이블 S' 와 S 사이의 유사도를 비교함으로써 소유권을 판정한다. 따라서 부호화 과정, 복호화 과정 그리고 유사도 비교를 어떻게 설정하는가에 따라서 여러 가지의 워터마킹 방법이 존재하게 된다. 워터마킹 기법은 다음과 같은 기본 요구 조건을 만족해야 한다[1,2].

- 워터마크 내장으로 인한 수정은 시각적으로 영상의 질을 저하시키지 않아야 한다. 그러나, 시각적으로 차이가 없다 하더라도 원 영상을 워터마크된 영상과 비교할 때는 뚜렷해야 한다. 그러므로 원 영상은 합법적인 소유자에게만 접근이 가능하고 그런 차이가 관찰자에 의해서는 인식되지 않게 남아 있어야 한다고 가정한다.
- 워터마크는 어떤 특정한 영상에 대해 충분하고 확실한 소유권 증명을 해야 한다. 워터마크 추출 실패는 나타나지 않아야 하지만, 만약 나타난다면 아주 드물게 나타나야 한다.
- 워터마크는 한 소유권자의 생산물의 불법적인 파괴에 대하여 네트워크 환경에서 공동으로 접근할 수 있는 영역을 조사하는 탐색 절차와 쉽게 결합되어야 한다.
- 워터마크는 통계적인 방법을 사용하여 회복되어서는 안 된다. 예를 들면 상당히 많이 워터마크된 디지털 영상물들의 소유는 같은 키를 이용하여 통계적인 방법을 적용함으로써 그 워터마크를 배치해서는 안 되고 워터마크는 영상의 존재적이어야 한다.
- 같은 영상에서 다른 워터마크를 충분히 많이 첨가할 수 있어야 한다. 각 워터마크는 유일한 키를 사용하여 추출할 수 있어야 한다. 이런 특징은 이미 워터마크된 영상

을 다른 사람이 다시 워터마킹 하는 것을 막을 수 없기 때문에 필요하다. 또 저작권 소유가 한 소유자로부터 다른 소유자로 이동된 경우에 편리하다.

- 워터마크가 내장된 디지털 영상은 고의든 고의가 아니든 수정될 수 있다. 따라서 워터마크는 일반적인 영상 처리 등의 영상 변형[1,2](압축, 필터링, 잡음 첨가, 회전, 스케일링 등) 후에도 남아 있어야 한다.

2.2 주파수 영역에서의 디지털 워터마크

영상 데이터를 DCT domain[1,3], Wavelet domain[4], Fourier Mellin domain[5], Fourier Transform domain[6]등과 같은 변환으로 주파수 공간으로 변환하여 그 주파수 영역들 중에서 시각적으로 덜 민감한 부분에 적용적으로 워터마크를 삽입하는 방법이다. 단일 주파수 성분을 변화시킴으로써 변환 블록 내의 밝기 값 전체에 영향을 미치고, 따라서 불법적인 공격에 강한 워터마크를 만들 수 있다. 영상 데이터를 주파수 영역으로 변형했을 때 가질 수 있는 통신 채널이라고 가정한다면, 워터마크는 그 통신 채널로 통과하는 신호라고 볼 수 있다. 그 신호가 잡음, 필터링, 압축전송 등에 영향을 받지 않고 효과적으로 전송이 될 수 있도록 대역확산통신(spread spectrum communication) 방식을 도입한다. 특정 주파수 대역의 에너지를 감지할 수 없을 정도로 작지만 주파수의 위치와 변화량을 알고 있는 소유권자에 의해 산재해 있는 주파수 성분을 모으면 높은 신호 대 잡음비(signal to noise ratio)로 신호를 검출할 수 있다. 워터마크를 영상이 갖고 있는 여러 주파수 영역으로 확산시킴으로써 특정 주파수 대역의 에너지는 감지하기 어렵게 한다. 영상의 변화를 감지 못하도록 하면서 시각적으로 중요한 영역에 정보를 삽입하는 알고리즘은, 시각적 변형과 JPEG 압축, 그 외 영상 처리 기술에 대하여 장단점을

고려하여 삽입하고자 하는 주파수 영역을 선택하여 워터마크를 삽입한다. 이 방법도 잡음과 일반적인 신호 처리에 견고(robust)하지 못하다는 단점을 가지고 있다.

2.3 (n,k) 비밀 정보 분할 방식

(n,k) ($n \geq k$) 비밀 정보 분할 방식 알고리즘은 n개의 비밀 정보 중 k개의 비밀 정보만 알면, 비밀 정보를 찾아내는 비밀 분산 방법이다. 그러나, (k-1)개의 비밀 정보만 모아져도 비밀 정보를 복원 할 수 없다. 본 논문에서 사용된 (n,k) 비밀 정보 분할 방식 알고리즘은 Lagrange 보간 다항식[7]에 근거한 임계치 방식이다.

구체적인 예로 (n,2) 비밀 분산 방식은 비밀 정보 S 를 상수항으로 하는 직선 $y = a_2x^2 + a_1x + S$ 를 만든다. 그런 다음에 직선 y를 지나는 점 임의의 두 점 $S_1 = (x_1, y_1)$, $S_2 = (x_2, y_2)$, ..., $S_{n-1} = (x_{n-1}, y_{n-1})$, $S_n = (x_n, y_n)$ 을 구한다. 비밀정보 분배자는 n 개의 점 중에서 하나씩을 n명의 사용자에게 알려준다. n개의 점 중에서 하나의 점을 알고 있는 사람은 직선 y를 구할 수 없으며, 따라서 상수항인 비밀정보 S를 알 수 없다. 만약 두 사람이 모여서 서로의 좌표를 알려주면 두 점을 지나는 하나의 직선 y 를 구할 수 있으며, 이 직선이 y축과 만나는 점인 비밀 S를 구할 수 있다. 실제적인 구현 측면에서 언급하면, 다음과 같다.

2.3.1 비밀정보의 분산

- 소수(a_1, a_2, \dots, a_{k-1})을 랜덤하게 선택한다.
- 정수항 $a_0 = s$ 로 해서 (k-1)차의 다항식 $f(x) = s + a_1 x + a_2 x^2 + \dots + a_{k-1} x^{k-1}$ 를 생성 한다.
- n 명의 사용자에게 공유(share)로써 각 $f(1), f(2), \dots, f(n)$ 을 전달한다.

2.3.2 비밀정보의 복원

- (k-1)차 다항식은 k명 이상의 $f(i)$ 로부터 복원할 수 있기 때문에, k명 이상의 사용자는 다항식 f 를 복원할 수가 있다. 따라서, Lagrange 보간 다항식을 이용하여 비밀정보 S를 구할 수 있다.

3. 제안 방식

본 장에서는 (n,k) ($n \geq k$) 키 분할 방식을 이용하여 원본 영상 1/4 영역 안에서 요구되는 분할 정보 k개의 분할된 정보로부터 정확히 마크를 찾을 수 있는 방법을 제안한다. 워터마크 삽입 알고리즘은 원 영상을 이용하여 이산 코사인 변환(FDCT)을 한 후, 저주파 성분과 중간 주파 성분에 각각 물리적 픽셀 영역에 개인의 신상정보에 해당하는 워터마크를 생성시킨 후, 시각적으로 보이지 않게 삽입하는 방법이다. 이 때 생성한 워터마크는 ASCII 코드 값으로 변환하여 이용하게 되고, 일반적인 영상 변형에 강한 저주파 성분과 명도나 대비 변화에 강한 중간 주파 성분의 특성을 이용하여 두 부분에 모두 워터마크를 삽입하였다.

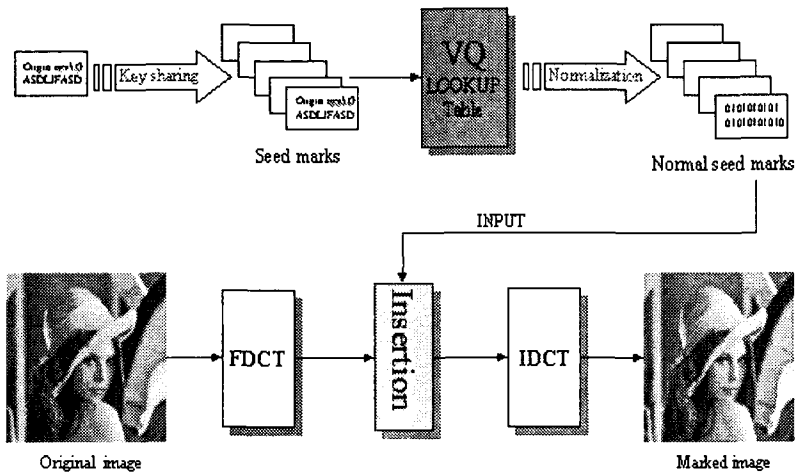
[그림 3-1]은 전체적인 삽입하는 과정으로서 키 생성 처리 과정과 VQ를 사용하는 정규화 과정이다. 또한 삽입하는 과정은 전체 워터 마크된 영상의 1/4영역에서도 마크가 추출될 수 있도록 삽입하는 방법이다. 이를 위하여 삽입될 원 마크의 크기가 제한적일 수 있으며, 따라서 text 가 아닌 IMAGE 마크일 경우 그 크기에 상당한 제약을 받을 수 있다. 영상인 경우에는 키 생성 과정 앞에 다양한 영역 축소(space reduction) 방법을 사용하여 크기 제한을 완화할 수 있다.

3.1 워터마크 삽입 과정

일반적인 방법으로 워터마크에 삽입되는 데이

터의 크기는 0~1사이의 랜덤 값(노이즈)을 사용하든가 0 이나 1 인 이진(binary) 값이 사용되므로, 이 값의 범위가 벗어날 경우 원 영상의 화질이 크게 손상되기 때문에 삽입하고자 하는 데이터, 즉 워터마크의 데이터 범위는 반드시 일정한 조건에 만족하여야 한다. 따라서 이의 조건을 준수하기 위하여 비밀정보 분할 방식의 결과치(output)를 0~1 사이로 사상(projection)시켜야 한다.

비밀정보 분할 방식을 적용하여 생성된 파일의 데이터 값을 정규화(normalization) 과정을 거쳐 요구하는 데이터 범위로 사상시켰으며, 이의 빠른 구현 및 정확성을 위하여 LOOKUP 테이블로 작성하여 사용 하였다. 이 데이터를 삽입할 위치는 8*8 DCT 블록의 고주파와 중간 주파수 영역이다. [그림3-1]은 워터마크를 삽입하는 과정이며, 단계별로 설명하면 다음과 같다.



(그림 3-1) 워터마크 삽입 과정

알고리즘 1. 워터마크 삽입 과정

- [단계 1] 원 마크를 (n,k)인 임계치 키 분할 알고리즘에 입력하여 마크의 n 개의 분할된 정보인 시드 마크(seed marks)를 생성한다.
- [단계 2] n 개의 분할된 시드 마크(seed marks)를 0~1 값 사이로 정규화하여 정규화된 시드 마크를 얻는다.
- [단계 3] 이산 코사인 변환을 통하여 원 영상을 주파수 영역으로 변환한다.
- [단계 4] 물리적 픽셀 영역, 즉 공간 영역에서

워터마크를 삽입하는 가장 간단한 방법은 픽셀들을 임의적으로 선택하여 그것의 밝기 값의 LSB(least significant bit)를 변형시키는 것이다. 이 데이터를 삽입할 장소가 8*8 DCT 블록으로써 값의 범위가 정확히 맞는지 확인한 후 주파수 영역에 삽입한다.

- [단계 5] 역 이산 코사인 변환을 통하여 마크가 삽입된 워터마크를 얻는다.
- 삽입 알고리즘에서 삽입 메커니즘은 대략 3

가지가 있지만 그 중에서 가장 많이 사용되는 방법으로 $data = \beta(data + \alpha * mark)$ 방법을 사용하였다. 이때 α 값은 대략 0~1사이의 값이며, 여기서 $\alpha, \beta = \{0.1, 0.2, 0.5, 1\}$ 에서 선택한다. 위의 워터마크 삽입하는 과정은 워터마크 데이터의 크기만큼, 미리 지정해둔 위치에 n개의 분할된 정보를 삽입하게 된다.

3.2 워터마크 추출 과정

워터마크 추출 알고리즘은 손실 압축과 잡음 등의 변형된 영상에서 워터마크를 효율적으로 추출하기 위하여, 원 영상과 워터마크가 삽입된 영상에 대하여 각각 이산 코사인 변환을 한 후 차이 값을 구하고, 그 값에 임계치를 적용한 다음 삽입된 워터마크를 추출한다. 워터마크 추출 과정은 삽입 과정의 역으로 진행된다.

알고리즘 2. 워터마크 추출 과정

- [단계 1] 변형이 가해진 영상(워터마크가 삽입되었거나, 삽입되지 않았거나, 손상된 영상)과 원 영상을 각각 이산여현 변환을 한다.
- [단계 2] 주파수 영역에서, 원 영상과 변형된 가해진 영상 사이의 계수 값들의 차를 구한다.
- [단계 3] 임계치(Threshold value)를 설정하고, 그 임계치를 [단계 2]에서 구한 값에 적용하여 워터마크가 삽입된 위치를 찾아내고 추출한다.
- [단계 4] 추출된 워터마크가 소유권자가 사용한 워터마크인지 아닌지, VQ방법을 이용하여 마크를 재구성함으로써 판단하여 인증한다.

4. 실험 결과

실험은 PENTIUMIII-550, WIN98에서 VC++

을 이용하여 코딩되었으며 원본 영상은 256 × 256 크기의 Lena 등 영상을 사용하였으며 삽입된 워터마크로는 64 × 64 크기와 128 × 128 크기의 이진 영상을 사용하였다. 실험의 목적은 워터마크를 원본 영상에 삽입하였을 때 워터마크가 삽입된 영상의 질(quality)이 얼마나 보전되는지와 마크를 추출했을 시에 가시적으로 확인할 수 있을 정도의 영상의 질을 유지하는지가 주된 관점이었다.

또한 제안된 방법은 마크가 삽입된 영상을 크래핑했을 시에 1/4보다 작은 영역에서도 마크를 추출할 수 있어야 하며 추출된 마크가 가시적으로 확인 가능해야 한다는 것을 말해주고 있다.



(a) 원본 영상 (b) 워터마크가 삽입된 영상

(그림 4-1) 원본 영상과 워터마크가 삽입된 영상

이 또한 실험의 주된 관점이 되었다. [그림 4-1]에서 보는 바와 같이 원본 영상과 마크가 삽입된 영상은 육안으로 관찰하기에 거의 동일했으며 삽입된 영상의 질은 평균 44dB 이상을 유지하였다. 이는 삽입할 때의 α 값에 따라서 약간의 변동이 생기게 됨을 고려한다면 아주 좋은 영상의 질을 유지하고 있다고 볼 수 있다. 원본 영상에 삽입하고, 추출된 마크 영상은 [그림 4-2]에서 보는 바와 같다.



(a)마크 영상



(b) 복원된 마크 영상

(그림 4-2) 마크 영상과 복원된 마크 영상

삽입된 마크는 일련의 문자 스트림이 아닌 영상이기 때문에 문자열 보다 많은 정보를 삽입해야 하는 문제가 있을 수 있으나 어느 정도의 영상의 질만 유지된다면 육안으로 식별이 가능하다는 점에서 저작권 정보나 소유권을 주장할 시에 좋은 방법이 될 것이다. 위의 [그림 4-2]에서 보는 바와 같이 추출된 마크 영상은 삽입한 영상과 비교했을 때, 가시적으로 판별이 가능한 형태를 유지하고 있었으며 따라서 소유권의 판별이나 저작권의 판별도 가능한 상태라고 말할 수 있다.

<표 1>에서는 제안된 워터마킹 방법론의 강건성을 실험한 결과를 나타내고 있다. 강건성의 정도를 1부터 50까지로 설정하여 단계적으로 각 이미지 왜곡에 따른 워터마크 강건성을 실험하였다. PSNR추변에서 35dB이상의 값을 가지면 인간 시각으로는 원 영상과 워터마킹된 영상, 또는 워터마크와 추출된 워터마크의 구분을 할 수 없는 수준이다. 각 공격방법에서 uniform error를 제외하고는 워터마크의 저작권을 확인할 수 있었다. 그러므로 제안된 방법에서는 변환 영역에서 워터마크의 삽입으로 인한 화질의 열화 문제를 해결하였다. 또한 시각적으로 저작권의 확인이 가능한 워터마크를 삽입하므로 효용성이 높다고 할 수 있다.

<표 1> 제안한 워터마크의 강건성 실험 결과

Robustness	Image Processing								
	Add uniform error	Median cutting	Edge enhance-ment	Blurring	Sharpe-ning	Equaliz-ation	Resizing	Compre-ssing	PSNR
1	0.53	0.78	0.99	0.74	1.00	0.99	0.72	0.75	55.11
10	0.51	0.89	1.00	0.81	1.00	1.00	0.75	0.81	48.12
20	0.50	0.94	1.00	0.82	1.00	0.99	0.80	0.88	45.87
30	0.49	0.92	0.99	0.84	1.00	1.00	0.82	0.91	41.99
40	0.48	0.95	1.00	0.85	1.00	1.00	0.86	0.92	38.12
50	0.50	0.94	1.00	0.85	1.00	1.00	0.85	0.93	37.47

5. 결 론

영상을 이산 코사인 변환을 통하여 주파수 공간으로 변환한 뒤, 인간이 감지하지 못하는 주파수 공간을 찾아 물리적 픽셀 영역에 워터마크를 삽입하였다. 이 때 주파수 영역에서의 저주파 성분과 중간 주파 성분의 각각의 특성을 고려하여 워터마크를 삽입하였다.

본 논문에서는 디지털 영상의 소유권을 보호하기 위해 DCT 영역 변환을 이용하여 시각적으로 인식할 수 없는 부분에 $(n,k) (n \geq k)$ 키분할 방식을 이용하여 원본 영상 1/4 영역 안에서 요구되는 분할 정보 k 개의 분할된 정보를 찾아서, 강인한 워터마크를 추출하는 과정을 구현하였다. 비밀 정보 분할 방식을 사용한 목적은 보다 강인한 워터마크를 형성하기 위한 방법이며, 추출시에 데이터를 보다 완벽하게 복원하기 위한 방법이다. 앞으로 더 연구되어야 할 부분으로는 원본 영상의 크기에 상관없이 워터마크를 삽입하는 처리 과정과 삽입할 워터마크의 크기를 완화하는 처리과정이 반드시 필요하다.

참고문헌

[1] I. J. Cox, J. Kilian, T. Leighton and T. Shamoan, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Trans. on Image Processing, 6, 12, pp. 1673-1687, 1997.

[2] I. J. Cox, M. L. Miller, "A Review of Watermarking and the Importance of Perceptual Modeling," Proc. SPIE Conf. on Human Vision Electronic Imaging II, Vol. 3-16, pp. 92-99, Feb., 1997.

[3] A. Piva, M. Barni, F. Bartolini, V. Cappellini, "DCT-based watermark

recovering without resorting to the uncorrupted original image," Proceedings of ICIP'97, Santa Barbara, CA, USA, Oct., 26-29, Vol. I, pp. 520-523, 1997.

[4] D. Kundur, D. Hatzinakos, "A Robust Digital Image Watermarking Method using Wavelet-Based Fusion," Proceedings of ICIP'97, Santa Barbara, CA, USA, Oct., 26-29, Vol. I, pp. 544-547, 1997.

[5] J. J. K. O' Ruanaidh, T. Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking," Proceedings of ICIP'97, Santa Barbara, CA, USA, Oct., 26-29, Vol. I, pp. 536-539, 1997.

[6] J. J. K. O' Ruanaidh, W. J. Dowling, F. M. Boland, "Phase watermarking of digital images," Proc. 1996 IEEE Int. Conference on Image Processing(ICIP'96), Vol. III, pp. 239-242, 1996.

[7] A. Shamir, "How to Share a Secret", Comm. of the ACM, Vol. 22, pp. 612-613, 1979.

[8] C. Wang, S.Tai, and C.Yu, "Repeating Image Watermarking Technique by the Visual Cryptography", IEICE Trans. Fundamentals, Vol. E83-A, 2000.



서 창 호

1990년 고려대학교 수학과 졸업(학사)
 1992년 고려대학교 일반대학원 수학과(이학석사)
 1996년 고려대학교 일반대학원 수학과(이학박사)
 1996년-1999년 국방과학연구

소 선임연구원

1996년-2000년 한국전자통신연구원 선임연구원,
팀장

2000년 - 현재 공주대학교 응용수학과(정보보호
전공) 조교수

관심분야: 암호 알고리즘, PKI, 무선 인터넷 보
안, 시스템 보안 등

김 석 우



1979년 한국항공대학교 통신정
보공학과(학사)

1989년 뉴저지 공과대학 전자
계산학과(공학석사)

1995년 아주대학교 컴퓨터공학
과 정보통신전공(공학박사)

1980년 - 1997년 한국전자통신연구원 책임연구
원, 실장

1997년 - 현재 한세대학교 IT학부/대학원 정보
보호공학과 교수

관심분야: 시스템 보안, 네트워크 보안, 시스템
평가 등

성 열 옥



1979년 공주사범대학교 수학
교육학과 졸업(학사)

1984년 고려대학교 일반대학
원 수학과(이학석사)

1993년 한남대학교 일반대학
원 수학과(이학박사)

1985년 - 1998년 공주대, 한남대, 대전산업대,
대전대, 충남대 시간강사

1998년 - 현재 공주대학교 응용수학과 조교수

관심분야: 암호 알고리즘, 퍼지이론 및 시스템