워터마크 기법을 이용한 PACS 보안 알고리즘 설계

오근탁*·김용호*·이윤배**

PACS Security Algorithm Design using Watermark

keun-Tak Oh* · Yung-Ho Kim*· Yun-Bae Lee**

요 약

의료영상은 디지털이라는 속성으로 인해서 일상생활에 적용되는 저작권법으로 저작권을 보호한다는 것이 어렵다. 특히 의료 영상은 복사를 하면 또 하나의 원본이 생성되므로, 의료 영상 이미지를 생산해 내는 사람의 입장에서는 똑같은 원본을 자신도 모르는 사이에 다른 사람에게 전달하게 된다. 그렇게 되면 과연 누가 이 디지털 작품을 만들었는지에 대한 의료 분쟁이 생길 수밖에 없다.

디지털시대의 의료 환경에서 필수 불가결하게 제기될 수 있는 의료영상보안은 특히 우리나라처럼 의료보험의 부당 청구가 사회적인 큰 물의를 일으키고 있는 시점에서 많은 관심과 연구가 필요하다. 따라서 이 분야의 핵심적인 문제점을 도출하고, 문제점 개선을 위해서 워터 마크를 통해 영상 보안 기법을 제안하였다. 그러나 의료영상의 대표적인 특징인 무결성을 보장 받지 못해 법적인 인증에는 한계가 있음을 알 수 있었다.

ABSTRACT

It is hard to protect the copyright of the medical images by the Copyright Act because the medical images have the digital property. Especially, if people copy the medical image, another original one will be created. Thus, people send the original medical image to the others unconsciously. After all, it can not dispute about who made the image for the first time. Nowadays, the medical environment has been changed to the digital environment rapidly. So, the study on the security of the medical image is needed. In this paper, we search the significant problems of the part and we research the security of the medical image using the watermark for addressing the problems. However, we could know that our study has the limitation of the legal certification because we could not guarantee about the integrity that is the important feature of the medical images.

키워드

Watermark, image, PACS Image, Algorithm

Ⅰ. 서 론

디지털 혁명이 실현되고 있는 지금, 그 응용분야는 의료계까지 큰 영향을 미치고 있어서 디지털병원시대를 예고하고 있다. 디지털 시대의 사회변화 속도는 상상을 초월할 만큼 빠르게 진행 될 것으로 보인다. 이 변화에 어떻게 신속히 적응하고 대응하느냐에 의료기관의 성패가 달려 있다고 할 수 있다[1]. 각종영상 촬영장치(modality)로 촬영한 영상들을 CR(Computed Radiography)를 통해 디지털 화하여 하드 디스크와 같

* 조선대학교 대학원 전자계산학과 박사
** 조선대학교 대학원 전자계산학과 교수

접수일자 : 2005. 5. 9

은 저장매체에 저장, Network를 통해 각 단말기로 전송하여 진찰실, 병동 등의 Workstation이 있는 곳이면 어디에서든 실시간으로 환자의 영상을 조회할 수 있는 시스템인 PACS(Picture Archiving and Communication System)는 이러한 변화의 시기에 의료기관의 경쟁력 확보를 위한 핵심수단 중 하나라고 할 수 있다. 특히 환자의 생명과 직결되는 보안 분야의 문제해결을 위해 학계와 산업계의 공동 노력이 어느 때보다도 요구된다 뿐 만 아니라 정확한 환자 정보의 보존과 사생활 보호는 매우 필수 불가결한 문제라고 할 수 있다. 이에 의료기술과 정보통신기술이 융합된 PACS에서 발생할 수 있는 보안의 문제를 제기함으로서 그 문제점 개선을 위해서 워터마크를 이용한 영상 보안기법을 제안하고자 한다.

Ⅱ. 본 론

사전적인 의미로 워터마크(watermark)란 "투명한 이미지"이다. 즉, 워터마크란 오디오, 비디오 또는 이미지 등의 디지털 데이터에 삽입되는 이미지이다. 따라서 워터마킹(watermarking)이란 이미지, 오디오, 비디오 등과 같은 디지털 미디어에 저작권정보 등과 같은 워터마크를 삽입하는 과정을 말한다. 특히 워터마크를 삽입한 뒤 디지털 미디어의 화질저하는 아주 적어서 눈으로는 워터마크가 삽입되었는지 알 수 없는 경우, 이를 '보이지 않는 워터마크(invisible watermark)'라고 한다.

2.1 워터마크 용도

워터마킹 방법은 다양한 목적으로 사용 될 수 있다. 다음은 워터마킹을 사용하는 여러 가지 용도를 보여준다[3].

1) Ownership assertion : 이것은 디지털 미디어 콘텐츠의 소유 관계를 주장하는 방법으로 워터마크를 사용하는 것이다. 콘텐츠에 대한 소유를 주장하기 위해서, 먼저 콘텐츠를 만드는 작가는 비밀 키를 사용해서 워터마크를 생성한 뒤 그것을 원본 콘텐츠에 삽입한다. 다음 작가는 워터마크가 삽입된 이미지를 공개한다. 나중에 다른 사람이 이 공개된 콘텐츠의 소유를 주장하면 원래 콘텐츠를 생성한 작가는 워터마크가 없는 원본 콘텐츠를 생성해서 소유를 주장하는 다른 사람의 이미지에 자신이 삽입한 워터마크가 있음을 보여주면 되는 것이다. 이때 작가의 원본 콘텐츠는 소유를 주장하는 다른 사람에게는 알려지지 않았으므로 다른 사람은 작가처럼 자신의 소유를 주장할 수 없게 된다. 하지만 이 방법이 동작하기 위해서는 이미지에 대한 압축, 확대, 축소 등과 같은 연산을 수행해도 워터마크가 소멸되지 않고 남아 있어야 한다.

2) Fingerprinting : 이 방법은 디지털 미디어의 무단 복제와 무단 배포를 막기 위한 방법이다. 먼저 콘텐츠의 저자는 각각의 데이터 카피에 대해서 유일한 워터마크를 부여해서 그 데이터 카피에 삽입을 한다. 만일 무단으로 복사된 콘텐츠가 발견되면 카피 내에 숨겨져 있던 워터마크 방법 중 여러 가지 방법을 보여주게 되는데 대표적인 몇 가지 방법은 다음과 같다.

(1) 공개키 암호 알고리즘을 이용한 방법

공개키 암호 알고리즘은 이미지 전체를 암호화하지 않고서도 이미지에 대한 인증을 수행할 수 있는 방법을 제공한다. 이미지에 대한 인증을 수행하는 방법은 아래와 같다.

먼저 A는 인증에 사용될 디지털 서명을 생성한다. 디지털 서명은 암호학적 해쉬 함수를 사용해서 만들어진다.

signature = hash(image); A는 자신의 비밀 키를 사용해서 디지털 서명을 암호화한다.

authenticator = Kpriv(signature); 이렇게 암호화된 authenticator와 image를 다른 사람들에게 보낸다.

Send(Image + authenticator); 다른 사람들은 A의 공개된 공개키를 사용해서 암호화된 authenticator를 복호화 한다. 그러면 원래 이미지의 hash값을 알 수 있게 된다. 그리고 A에게서 받은 이미지에 대한 해쉬 함수 값을 구한다. 그러면 원래 이미지의 hash값과 이미지에 대한 hash값을 비교하면 이미지가 변경되었는지 확인 할 수 있게 되고, A의 공개키를 사용해서 복호화 했으므로 A가 보낸 것이라는 것을 알 수 있게 된다.

compare(hash(image), Kpub(signature)); 이 방법은 암호 알고리즘을 사용하므로 안전하지만 인증을 수행하는데 필요한 authenticator와 이미지를 따로 처리해야 하는 문제를 가지고 있다.

(2) 타임스탬프를 이용한 방법

타임스탬프(TimeStamp)를 이용하는 방법은 어떤 누군가가 처음으로 이 이미지를 소유했다는 것을 증명하기 위해서 이미지에 스탬프를 찍는 방법이다. 이를 위해서 이미지의 소유자는 믿을 수 있는 제 3의 기관을 통해서 그 이미지의 해쉬 함수 값과 날짜를 등록하게 된다. 하지만 이 방법의 경우 제 3의 믿을 수 있는 기관이 필요하게 되는 문제를 가지고 있다.

(3) 체크 섬을 이용한 방법

체크섬(checksum)을 이용한 방법은 이미지의 LSB 부분에 체크 섬을 집어넣는 방법이다. 이 방법은 빠르게 수행할 수 있는 장점이 있지만 체크 섬을 모두 삭제하는 것이 가능하게 되는 단점도 있다.

(4) 해쉬 함수를 이용한 워터마킹 방법

Wong은 암호학적 해쉬함수인 MD5를 사용하는 방법을 제안했다[2]. 먼저 이미지는 I*J 픽셀 크기를 가지는 여러 블록들로 나누어진다. (I*J < 128) 그런 다음 각 블록의 LSB (least significant bit) 부분은 모두 제거가 된다. 그러면 남아있는 MSBs (most significant bits) 부분과 이미지의 크기 그리고 비밀키(secret-key)를 암호학적 해쉬함수에 통과시켜서 디지털 서명을 생성한다. 이렇게 생성된 서명은 삽입될 워터마크 이미지와 XOR연산을 통해서 합쳐진 뒤 이미지 블록의 LSB 부분에 다시 삽입이 되는 것이다. 아래 그림[1]은 Wong이 제안한 알고리즘을 도식으로 표현한 것이다.

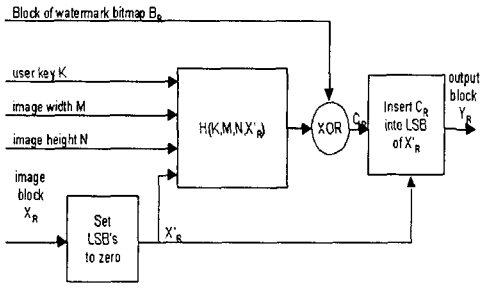


그림 1. 워터마크 삽입
Fig. 1 Watermark Insert

[그림2]는 워터마크가 삽입된 이미지에서 워터마크를 뽑아내는 과정을 도식적으로 나타낸 것이다. 먼저 이미지를 I*J 픽셀 크기의 블록들로 나눈다. 그런 다음 각 블록 의 MSBs와 이미지 크기 그리고 비밀 키를 사용해서 디지털 서명을 만든다. 그런 뒤 블록의 LSB와 앞에서 구한 디지털 서명과 XOR 연산을 수행하면 처음에 삽입한 워터마크 이미지가 나타나게 된다.

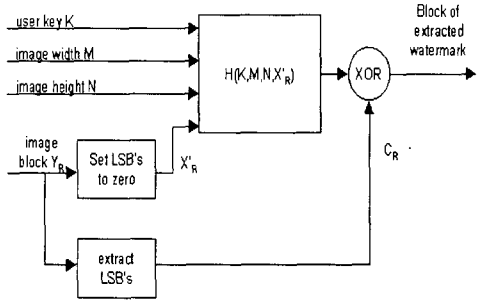


그림 2. 워터마크 추출
Fig. 2 Watermark Extract

[그림3]은 Wong의 알고리즘이 가지는 성질을 나타내고 있다. 먼저 A는 비밀키 를 사용해서 이미지에 워터마크를 삽입한다. 만일 b가 인증과 무결성을 확인하기를 원하면 올바른 비밀 키를 사용해서 올바른 워터마크 이미지를 뽑아 낼 수 있다. 그러나 B가 잘못된 키를 사용해서 워터마크를 확인하려 하거나, 이미지가 확대 또는 일부분만 잘려진 경우 워터마크 이미지 대신 노이즈가 나타내게 된다. 또한 이미지 픽셀의 일부분 이 변경되는 경우 어느 부분의 픽셀이 변경 되었는지 확인 할 수 있다.

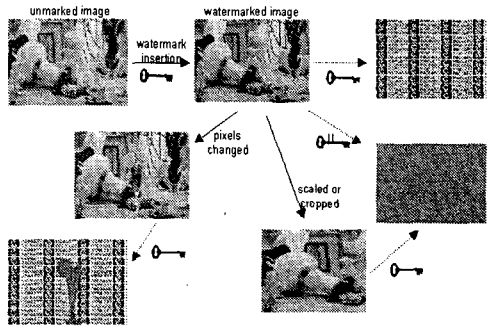


그림 3. 추출된 워터마크 이미지
Fig. 3 Random Sample Watermark Image

Ⅲ. 의료영상 변조 실험

일반적인 필름에서 디지털환경으로 바뀌는 의료영상을 임의로 조작하여 변조할 수 있는지 실험해 보고 변조된 의료영상이 과연 판독에 영향을 미칠 수 있는지 알아본다.

3.1 실험 내용

정상인의 요추를 HNP(추간원탈출증)의 M. R. I (자기공명영상 : Magnetic Resornance Imaging) 영상으로 변조한다. 그리고 변조된 영상을 의사(방사선과 전문의 2명, 레지던트 4년차 2명, 레지던트 3년 1명)들의 판독을 받아 그 결과를 고찰한다.

3.2 실험 도구

실험을 위해서 조선대학교 M. R. I (자기공명영상 : Magnetic Resornance Imaging) 실에서 1.5T의 자장을 이용하여 영상을 획득했으며, DICOM 파일의 이미지 영상으로 추출하고 변조된 이미지를 DICOM 파일에 첨가하기위해 VISUAL C++로 프로그램을 구현 하였다. 실험에 사용한 시스템 사양은 다음과 같다.

- Microsoft WindowsTM NT/2000SEVER
- CPU Pentium IIII 800 MHz
- RAM 128 MB 20G hard disk space
- Ethernet network card
- 32bit color display
- Screen resolution of 1280*1024

3.3 수행 과정

MRI 장치에서 획득한 의료영상을 네트워크 통해 VisualGate를 이용하여' DICOM표준영상을 raw data로 변환한다. 다음 프로그램에서 raw data를 JPEG으로 변환 이미지를 조작한다. 조작한 이미지는 DICOM표준영상으로 변환시켜 원 data에 삽입한다. DICOM 영상을 일반 영상으로 변환하는 것은 대부분의 PACS 프로그램에서 지원하므로 큰 어려움은 없었다. 그러나 일반 파일을 DICOM 영상으로 변환시키는 것은 쉬운 일은 아니다.

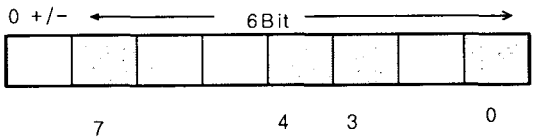
실험을 하기 위한 필수 조건은 다음과 같다.

첫째, DICOM 영상은 Header 와 Body로 이루어지므로 일반 영상 파일에 없는 DICOM Header내용을 채워줄 수 있는 기초 정보가 필요하다. 예를 들면 PatientName, ID, Study Data 등의 기본 정보부터 Study Instance UID 같은 각종 UID값 등이 된다.

둘째, Transfer Syntax의 결정이다. DICOM영상은 각종 형태의 압축과 다양한 형식의 포맷을 지원하기 때문에 변환하고자 하는 원본 영상이 어떤 타입인지에 맞추어 이를 결정해야 한다. 원본 영상이 압축되어 있지 않다면 Explicit VR little endian으로 처리하면 되며, 만약 JPEG 등의 파일일 경우는 JPEG 파일을 압축을 풀어서 Explicit VR little로 할 수 있겠지만 가능하면 압축된 형태 그대로 DICOM JPEG으로 만들어 주는 것이 좋다.

셋째, UID 발급에 관한 공신력이다. 일반 영상을 DICOM 영상으로 만들 때는 여러 가지 UID를 넣어 주게 되는데 그 중에서도 가장 중요한 것은 Study Instance UID, Series Instance UID, SOP Instance UID 이다. SOP Instance UID는 사실상 현재 만들어지는 DICOM영상이 전 세계에서 유일한 영상임을 증명할 수 있도록 고유하게 만들어져야 한다. 그리고 이러한 UID에는 UID Prefix가 붙게 되는데 이 Prefix값은 DICOM 영상을 생성하는 모든 장비나 소프트웨어 개발사 별로 고유의 값을 부여 받게 된다. 그렇게 함으로써 타 업체의 영상과 UID 충돌을 근본적으로 막게 되는 것이다.

일반적으로 DICOM의 표준 FORMAT은 다음과 같은 성질을 가지고 있다.



이러한 정보를 가지고 실험을 하여 보았다.

위에서 얘기한 3가지 조건을 모두 지원하고 RAW Data를 DICOM으로의 변환도 가능했다.

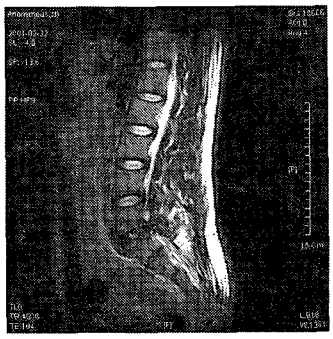


그림 4. 요추 측면부 MRI 영상
Fig. 4 MRI of normal patient's L-Spine Latera

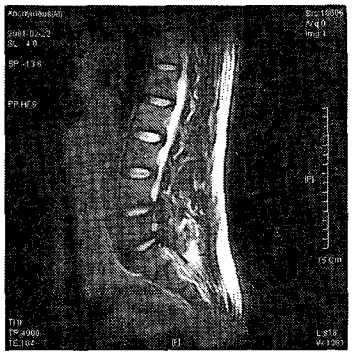


그림 5. 변조된 MRI 영상
Fig. 5 Fabricated image

그림[4]는 정상인의 요추 측면부 MRI영상으로서 L-SPINE LATERAL을 나타낸다. 특히 그림[4] 는 정상적인 MRI요추 측면부 영상에서 요추 2-3번째와 요추 4-5번째의 DISC부위를 조작하여 DISC 질환영상으로 변조할 수 있었다. 변조된 그림[5]를 보면 RAW DATA에서 DICOM표준 이미지로 변환과정에서 DICOM Header에 속해 있는 UID 값을 새롭게 채워 하는 문제로 기존 Header 값 위에 덮어진 것을 알 수 있었다.

실험을 통해 충분히 디지털의료영상의 변조 가 능하다는 사실과 변조된 영상이 진단에 많은 영향을 미칠 수 있다는 결론을 얻었다.

3.4 실험 방법

1. 완벽한 변조를 위해서는 의학적인 지식이 충분해야 하며, DICOM에서도 보안을 지원하고 있기 때문에 수많은 사진들을 위/변조하기 위해서는 고도의 컴퓨터 그래픽기술을 요구하고 있었다.

2. 아직까지 많은 임상의들이 디지털 의료 환경에서 발생할 수 있는 위/변조의 요소들을 생각하지 못하고 있기 때문에 앞으로 열릴 디지털의료시대의 영상보안에 대한 중요성을 인식해야 하며, 그 대책을 마련해야 할 것이다.

3.5 실험 고찰

일반적으로 가장 많이 쓰이고 있는 Spatial Method (데이터를 공간적 관점에서 삽입하는 방법)를 사용하였다. 비록 손실압축(JPEG)이나 필터링과 같은 이미지 처리에 약하다는 단점이 있지만, 워터마크의 삽입이 쉽고, 화면 화소 값에 미세한 변화를 워터마크로 사용하는 방법이기 때문에 사용했다. 프로그램 구현은 Visual C++로 작성 하였다.

먼저, 원 영상에 워터마크를 삽입한 후, 삽입된 영상을 위/변조하였다. 그리고 워터마크가 삽입된 영상을 추출하여 위/변조 사실을 알아보았다. 이 실험에 사용되어진 Algorithm은 다음과 같다.

- 전체 Algorithm
  - O : original Image
  - W':보이지 않는 워터마크
  - M :워터마크에 삽입된 이미지
  - M = O + W'

* Insert Algorithm

C = M * O

R: 워터마크에 곱해지는 factor (이 실험에서는 2값 을 부여)

W: 보이지 않는 워터마크

T: Threshold (이 실험에서는 128값으로 정의함)

W' = T * R

T <= 1 if W > threshold

T <= o else

* Extract Algorithm

O: original Image

M: 워터마크가 삽입된 이미지

S: 복원된 마크영상

C: 차이 영상 (=W')

C: = M * O

S <= High-value if C > threshold

S <= Low-value if C < threshold

이러한 알고리즘을 적용시켜 워터마크가 삽입 되어지는 과정은 [그림6]과 같다.

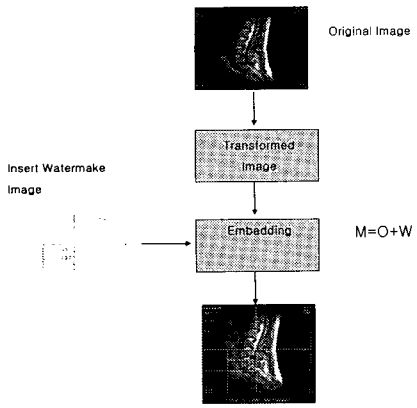


그림 6. 워터마크 알고리즘 처리과정
Fig. 6 Watermark Algorithm Procedure

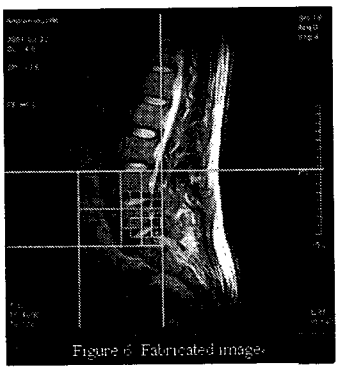


그림 7. 워터마크 삽입된 이미지
Fig. 7 Fabricated image

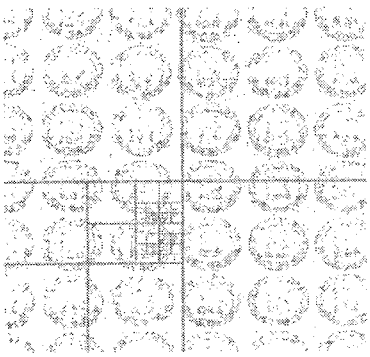


그림 8. 추출된 워터마크
Fig. 8 Extracted watermark from fabricated image

V. 결 론

최근 데이터의 디지털 화와 멀티미디어의 발달, 그리고 인터넷의 보급으로 인하여 디지털 데이터의 복제가 확산되고 있다 여러 가지 멀티미디어 데이터에 대한 소유권 문제와 이를 효율적으로 보호할 수 있는 기술이 요구되고 있다.

본 연구에서는 멀티미디어 데이터에 대한 소유권을 효과적으로 보호하고, 데이터의 불법 복제 및 배포를 제한할 수 있는 워터마크 기술을 의료영상보안 대책으로 적용해보았고 실험을 통해서 위/변조 사실을 구분하고자 했다.

특히, 이번 연구에서는 워터마킹 방법을 이용하여의료영상의 보안을 위해서 인증과 무결성을 보장하기 위한 새로운 방법을 규명해 보았다.

새로 제안된 알고리즘은 기존의 알고리즘에 비해서 이미지 화질 저하가 적고, 워터마크가 삽입되는 정확한 위치를 숨길 수 있었다.

그러나 제안한 방법의 경우 모든 공격유형에 대해서 안전한 방법이라고 할 수는 없다. 즉, 새로 제안한 알고리즘의 안전성과 이미지의 화질 사이에는 서로 trade off가 있음을 알 수 있었다.

향후 이 방법을 개선해서 다른 사람의 워터마크로 교체하는 것이 완전히 불가능하도록 해야 한다. 그렇게 되면 인터넷과 같은 공간상에 이미지를 배포해서 오랜 시간이 지나도 원래 이미지를 만든 저자가 누군가에 대한 인증을 수행할 수 있다.

참고문헌

[1] Wayne T. Dejarnette, "Web Technology and its Relevance to PACS and Teleradiology,"Applied Radiology, August 2000.

[2] DICOM (Digital Imaging and Communications in Medicine), Part 1~15(PS3.1-2001~PS3.15-2001), Published by National Electrical Manufacturers Association, 1300 N. 17th Street Rosslyn, Virginia 22209 USA, 2001 at http://medical.mena.org/dicom/2003.html

[3] J.J.Eggers,J.K. Su, and B. Girod, "Performance of a

practical blind watermarking scheme," *in Proc. of SPIE* Vol. 4314: Security and Watermarking of Multimedia Contents III, (San Jose, Ca, USA), January 2001.

[4] I.J Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Trans. Image Processing*, Vol. 6, pp. 1673-1687, 1997.

[5] E.T.Lin, C.I.Podilchuk, and E.J.Delp, "Detection of image alterations using semi-fragile watermarks," SPIe International Conf. on Security and Watermarking of Multimedia.

[6] International Journal of KIMICS, Vol. 1, No. 4, December 2003

[7] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "Copyright Protection of Digital Images by Embeded Unperceivable Marks", *Image and Vision Computing*, Vol. 16, pp. 897-906, 1998.

[8] A. Z. Tirkel, C. F. Osborne and T. E. Hall, "Image and Watermark Registration", Signal Processing, Vol. 66, pp. 373-384, 1998.

[9] J.Eggers and B. Girod, "Blind Watermarking Applied to Image Authentication", *in Proc. IEEE ICASSP*, Salt Lake City, UT. May 2001

[10] C.-S Lu and H. Liao, "Multipurpose watermarking for image authentication and protection", *in IEEE Trans. Image Processing, 2001*, vol. 10, pp. 1579-1592.

저자약력

오근탁(Keun-Tak Oh)

조선대학교 이학석사
조선대학교 박사수료
서린정보 시스템 대표

※ 관심분야 : 보안, 멀티미디어, 임베디드, 모바일, 유비쿼터스

김용호(Yong-Ho Kim)

1989년 광주대학교 전자계산학과 졸업(공학사)
1993년 경남대학교 전자계산학과 졸업(공학석사)
2005년 조선대학교 전자계산학과 졸업(이학박사)
2005년 현재 조선이공대학 인터넷정보과 교수

※ 관심분야 : 멀티미디어, 임베디드, 모바일, 유비쿼터스

이윤배(Yun-Bae Leeh)

광운대학교 이학석사
숭실대학교 공학박사
조선대학교 전자정보공과대학 컴퓨터공학부 교수
해양정보통신학회 이사

※ 관심분야 : 인공지능, 보안, 멀티미디어, 임베디드, 모바일, 유비쿼터스