Journal of Korea Multimedia Society Vol. 11, No. 5, May 2008(pp. 588-596)

의료 영상을 위한 관심영역 기반 선택적 암호 기법

이원영[†], Yang Ou[††], 이경현[†††]

요 약

환자의 신변보호를 위하여 의료 영상에 비인가 된 사용자의 접근을 제한하는 것은 필수적이다. 본 논문에서는 의료 영상의 접근 제어를 위한 관심 영역(ROI, Region of Interest) 기반의 선택적 암호 기법들을 제안한다. 첫 번째 제안 기법은 웨이블릿 서브밴드들 중 관심영역에 속한 계수의 비트를 랜덤하게 변경하여 암호화를 수행하며, 이미지의 압축과 암호화가 동시에 수행되고 암호화로 인한 압축률에 대한 손실이 적은 특징을 가진다. 두 번째 제안 기법은 안전성의 향상을 위하여 압축된 코드스트림의 관심 영역에 대칭키 기반 암호 알고리즘을 적용하며, 암호화 과정에서 압축률에 영향을 미치지 않는 특징이 있다. 또한 제안 기법들은 JPEG2000의 코드스트림 표준 디코더와 호환성을 제공한다.

Selective Encryption Scheme Based on Region of Interest for Medical Images

Won-Young Lee[†], Yang Ou[††], Kyung Hyune Rhee[†††]

ABSTRACT

For the patients' privacy, secure access control of medical images is essentially necessary. In this paper, two types of Region of Interest (ROI)-based selective encryption schemes are proposed, which concentrate on the security of crucial parts in medical images. The first scheme randomly inverts the most significant bits of ROI coefficients in several high frequency subbands in the transform domain, which only incurs little loss on compression efficiency. The second scheme employs a symmetric key encryption to encrypt selectively the ROI data in the final code-stream, which provides sufficient confidentiality. Both of two schemes are backward compatible so as to ensure a standard bitstream compliant decoder so the encrypted images can be reconstructed without any crash.

Key words: Medical Imaging(의료영상), Selective Encryption(선택적 암호화), Region of Interest(관심영역), Random Bit Flipping(랜덤 비트 변경)

1. 서 론

최근 의료영상저장전송시스템(Picture Archiving and Communications Systems, PACS)의 개발로 의료영상은 기존 필름 판독을 통한 진단 방법에서 디지털화 된 데이터를 이용하는 방법으로의 변화가 가능해졌으며, 디지털화 된 데이터를 컴퓨터와 네트워크를 통하여 전송 및 처리가 가능하게 되었다. 하지만 디지털 의료 영상은 해상도가 크고 픽셀당 비트수가 높아 데이터의 양이 많기 때문에 저장과 전송 시에 부하를 줄이기 위한 방법으로 영상 압축 기술을 사용하며 의료 영상 장치들 사이에서 의료 영상 및 정보를

※ 교신저자(Corresponding Author) : 이경현, 주소 : 부산광역시 남구 대연 3동 부경대학교 (608-737), 전화 : 051)626-4887, FAX : 051)626-4887, E-mail : gwanghci@pknu.ac.kr
접수일 : 2007년 10월 11일, 완료일 : 2008년 3월 13일
[†] 준회원, 부경대학교 정보보호학과
(E-mail : gwangchi@pknu.ac.kr)
[††] 준회원, 부경대학교 정보보호학과
(E-mail : ouyang@pknu.ac.kr)
[†††] 종신회원, 부경대학교 전자컴퓨터정보통신공학부
※ 이 논문은 2006년도 정부(과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(No. R01-2006-00-10260-0)

저장하고 전송하기 위해 만들어진 표준인 DICOM (Digital Imaging and Communications in Medicine)에서는 영상의 압축을 위해 JPEG2000이 사용되고 있다[1,2].

영상 압축 기술의 표준인 JPEG2000은 일반적으로 자연영상의 경우 압축 효율이 높은 손실 압축 방식을 사용하지만 환자의 질병을 판단하기 위하여 사용되는 의료 영상은 진단의 정확성을 위해 무손실 압축 방식을 병행 사용하여 압축의 사용으로 인한 화질 저하를 최소화 한다. 하지만 무손실 압축 방식은 원 영상과 동일한 화질로의 복원이 가능하나 손실 압축에 비해 압축 효율이 낮다는 문제점이 있다. 그리고 CT(Computed Tomography), CR(Computed Radiography), US(Ultarsonography), MRI(Magnetic Resonance Imaging)와 같은 의료 영상들은 진단에 필요한 주요 정보는 전체 영상 중 특정 영역에만 존재한다는 특징을 가진다. 이러한 영상의 특징을 이용하여 압축의 효율을 높이고 주요 정보를 포함하는 영역은 고화질로 유지하기 위한 방법으로 JPEG2000의 관심영역(ROI, Region of Interest) 코딩이 있다[3,4]. 관심영역 코딩은 사용자 임의로 선택한 특정 영역을 무손실 압축 방식을 사용하여 고화질로 유지하고 그 이외의 영역은 손실압축을 사용하여 데이터의 양을 줄일 수 있다.

압축 통하여 저장 및 전송되는 데이터를 줄이는 문제 이외에도 의료 영상에 대한 보호도 함께 고려되어야 한다. 의료 영상은 환자의 개인정보를 포함하고 있으므로 허가받지 않은 사용자가 열람하거나 취득할 경우 환자의 신상정보가 유출될 가능성이 존재한다. 그러므로 비인가 사용자의 접근제한과 의료 영상의 기밀성 유지를 위하여 암호화 기술이 필요하다.

본 논문에서는 의료 영상을 위한 JPEG2000 관심영역 코딩 기반의 선택적 암호 기법을 제안한다. 첫 번째 기법은 DWT(Discrete Wavelet Transform) 이후 관심영역 내의 계수 중 특정 비트를 랜덤하게 변환하여 암호화를 수행하며, 알고리즘이 간단하여 쉽게 구현될 수 있으며 압축 효율의 저하가 적다. 두 번째 기법은 관심 영역에 대칭키 암호 알고리즘을 사용하여 암호화 과정을 수행한다. 본 논문에서는 AES(Advanced Encryption Standard) 암호 알고리즘[5]을 사용하여 충분한 안정성을 보장한다. 또한 제안하는 두 기법 모두 JPEG2000 표준의 코드스트림과 호환성을 가진다.

본 논문의 구성은 다음과 같다. 2장은 관련연구로 JPEG2000 표준의 특징과 관심영역 코딩과 기존에 제안되었던 일반적인 영상의 암호화 기법들에 대해서 소개하고, 3장에서는 의료영상을 위한 관심영역 기반의 선택적 암호 기법들을 제안한다. 그리고 4장에서 제안된 기법들을 실험을 통하여 그 결과를 보이고 분석한다. 그리고 제안하는 기법의 안전성과 효율성에 대해 평가한 후 마지막 5장에서 결론을 맺는다.

2. 관련연구

2.1 JPEG2000 표준

정지 영상의 압축 표준으로 DCT(Discrete Cosinte Transform) 기반의 JPEG이 널리 사용되고 있지만 저조한 압축 성능과 블록화 현상 등의 문제점으로 인해 DWT 기반의 JPEG2000이 디지털 영상 압축 표준으로 새롭게 제정되었다. JPEG2000은 네트워크 영상 전송이나 원격 인식 등에 이용하기 위하여, 저비트율 전송 환경에서도 향상된 압축 성능을 지원하고, 다양한 형태와 특징, 다양한 모델의 영상에 대처할 수 있는 통합된 압축 시스템을 지원하고 있다. 또한, 다양한 응용분야에 적용할 수 있도록 향상된 화소 정확도와 해상도에 의한 점진적 전송, 사용자가 원하는 화질의 코딩으로 전송하고 영역을 확보할 수 있는 관심영역 코딩, 비트 에러가 존재하는 통신환경에서의 견강성 유지등을 주요한 특징으로 갖는다.

JPEG2000의 기본 구조는 (그림 1)과 같이 전처리 과정(preprocessing), DWT, 양자화, 산술 부호화, 비트열 구성의 과정을 통하여 압축이 이루어지며, 그 역으로 진행되는 복호화 과정을 통해 재구성 된다. 먼저, 전처리 과정에서 영상은 사각형의 겹쳐지지 않은 크기가 같은 타일로 분할되는 타일링 과정 후 레벨 시프팅(level shifting), 색공간 변환(color space transform)을 하게 되고 이후 DWT를 수행하여 각 계층별로 분해된다. 웨이블릿 계수들은 양자화과정을 거치게 되며 분해된 계층은 서로 겹쳐지지 않는 작은 정사각형의 블록인 코드블록(code-block)으로 나누어지고 각 코드블록 단위로 독립적으로 엔트로피 코딩인 산술 부호화가 수행되어 코드스트림이 생성된다.

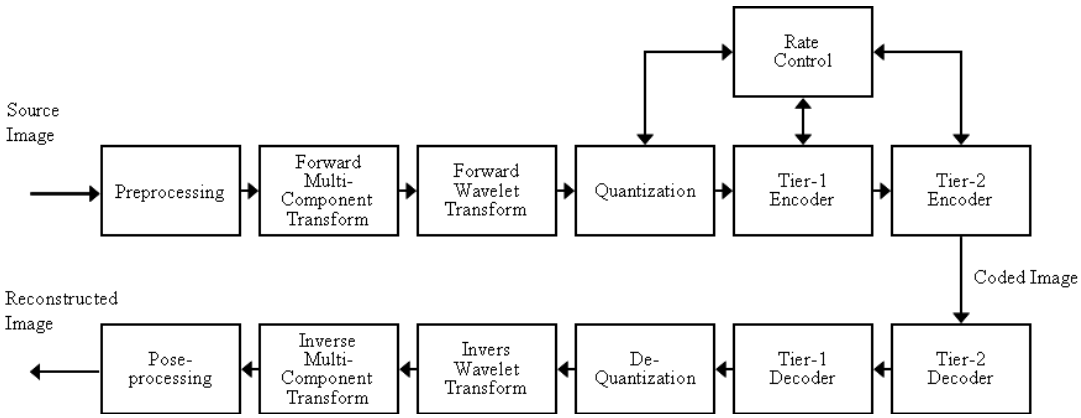


그림 1. JPEG 2000의 처리과정

2.2 JPEG2000의 관심영역 코딩

JPEG2000의 관심영역 코딩은 관심영역 마스크에 속한 웨이블릿 계수들을 배경영역(non-ROI)보다 높은 비트평면에 위치하도록 하여 우선순위를 가지게 하는 계수의 스케일링(scaling)에 기반을 하고 있다. 우선, 사용자의 임의의 선택에 의한 관심영역 마스크가 지정되면 DWT의 수행 이후 (그림 2)(a)와 같이 마스크 영역은 각 계층의 동일한 위치에 존재하게 된다. 모든 웨이블릿 계수들은 LSB(Least Significant Bit)에서부터 MSB(Most Significant Bit)까지를 나타내는 M_b 이내의 크기를 가지게 되는데 스케일링 과정은 관심영역의 우선순위를 높이기 위하여 각 계층의 마스크 영역에 속한 웨이블릿 계수들의 값을 항상 M_b 이상이 되도록 하여 배경영역의 웨이블릿 계수들보다 높은 비트평면에 위치하도록 하는 것이다. (그림 2)(b)는 스케일링 업 과정을 보이고 있다.

관심영역 코딩으로 높은 우선순위를 가지는 마스크 영역은 높은 비트평명에 위치하므로 영상의 재구성 과정에서 최우선적으로 복원되며 배경영역보다 높은 화질을 가진다. 만약, 영상의 전송 과정에서 코드스트림이 분할되거나 혹은 영상의 재구성 과정에서 전체 영상을 복원하기 이전에 수행이 종료된다고 하더라고 관심영역은 다른 배경영역보다 높은 질의 영상을 구성할 수 있다[6].

2.3 JPEG2000 기반의 영상 암호화 기술

일반적인 영상의 기밀성 유지와 접근제어를 위하여 JPEG2000 기반의 암호화 기술에 대한 많은 연구

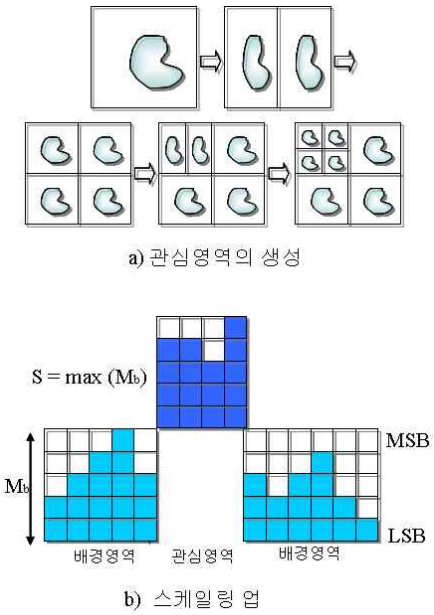


그림 2. 관심영역의 생성과 스케일링 업

가 진행되어왔다. JPEG2000 코드스트림을 변형하여 암호화하는 기법과 웨이블릿 계수를 치환하여 암호화하는 기법이 제안되었다[7-10]. 이와 같은 기법은 알고리즘이 간단하여 구현이 용이하고 암호화로 인한 부하가 적다는 장점을 가지지만 암호화 효과가 미미하여 높은 안전성을 기대할 수 없다. 또한 웨이블릿 계수를 이용한 기법의 경우 계수들의 치환으로 인해 계수들의 상관관계를 줄이므로 엔트로피 코딩의 효율을 떨어뜨려 압축 효율이 낮아진다는 단점을 지닌다. Norcen 등[11]은 JPEG2000의 비트스트림

중 일부 20%만을 선택하여 암호화하는 선택적 암호화 기법을 제안하였으며, Lian 등[12]은 주파수 서브밴드, bit-plane이나 부호화 패스 중 선택적으로 중요 데이터만을 암호화하는 기법을 제안하였다. 또 다른 기법으로는 Uhl 등[13-15]이 제안한 웨이블릿 필터나 웨이블릿 패킷의 구조만을 암호화하는 기법이 있다. 그러나 이들 기법들은 영상의 전체 데이터 중 극히 일부분만을 암호화하므로 암호화에 대한 부하가 적으나 실제 계수들은 암호화되지 않은 평문 상태로 존재하기 때문에 악의적인 사용자의 공격에 취약하다는 단점이 있다. 그러므로 상기 제안된 기법들은 의료 영상에 사용되기에 부적합하다.

3. 의료 영상을 위한 관심영역 기반의 선택적 암호 기법

앞 절에서 소개 된 JPEG2000 기반의 암호화 기법들은 일반적인 자연 영상의 암호화를 위한 기법들이다. 이들 기법들을 일반적인 자연 영상에 비해 데이터의 양이 많고, 전체 영상에서 주요 데이터를 포함하고 있는 영역이 제한적인 의료 영상에 직접적으로 적용하는 것은 효과적이지 못하다. 이 절에서는 JPEG2000의 관심영역 코딩을 이용하여 의료 영상의 주요 데이터 부분을 선택하여 효과적으로 암호화할 수 있는 두 가지 암호화 기법을 제안한다.

영상의 암호화 과정에서 공간적 중복성의 파괴로 인한 압축 효율 저하가 발생할 수 있으므로 대부분의 멀티미디어 암호는 영상의 부호화 과정이나 부호화 이후 수행된다[16]. 제안하는 기법 역시 영상의 압축비 손실을 최소화하기 위해 영상의 부호화 과정에서 암호화가 동시에 이루어진다.

3.1 랜덤 비트 인버팅

랜덤 비트 인버팅 기법은 양자화 된 목표 영상의 웨이블릿 계수를 임의의 비트열과 XOR 연산을 통하여 암호화 한다. 암호화의 대상이 되는 영상은 DWT 이후 관심영역 코딩을 수행하고 관심영역에 속하는 코드블록들은 (그림 3)과 같이 암호화가 수행된다.

관심영역에 속하는 코드블록의 웨이블릿 계수들의 부호비트와 MSB부터 임의의 몇 비트가 암호화를 위해 선택되고, 선택된 비트들은 시드값에 의존적인 PRNG(Pseudo Random Number Generator)를 통해

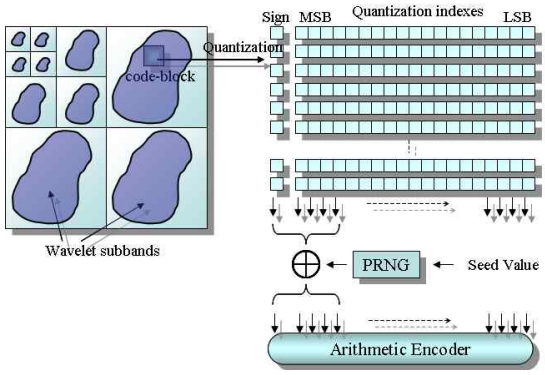


그림 3. 비트 인버팅 기법

생성된 비트열과의 XOR 연산으로 암호화를 수행한다. 예를들어, 어떤 코드블록의 비트평면에서 선택된 비트열의 값이 '0011'이고 PRNG를 통하여 생성된 비트열의 값이 '0101'이라면 XOR 연산으로 '0110'으로 암호화 된다. 이와 같은 암호화 과정이 끝나면 암호화 된 비트열과 나머지 암호화되지 않은 비트열은 다시 합쳐져서 산술 부호화 과정으로 이어진다.

암호화와 복호화의 동기를 위해서는 부호기와 복호기가 동일한 PRNG를 사용하여야하며 사용되는 시드값 역시 동일해야 한다. 만약, 서로 다른 PRNG를 사용하거나 시드값이 틀릴 경우 암호화 된 영상은 복호화 될 수 없다. 그리고 암호화를 위해 사용되는 비트열은 시드값에 의존적인 PRNG를 통해 생성되므로 시드값을 비밀로 유지하여야 한다.

3.2 대칭키 암호를 이용한 암호화

JPEG2000에서는 임의 접근, 관심영역 코딩, 확장성 등의 특징을 가능케 하기 위해 압축된 비트스트림의 체계화 된 구성으로 유연성을 제공한다. 특히, 비트스트림을 (그림 4)와 같이 여러 개의 화질 레이어(quality layer)로 나누어 다양한 비트 전송률에 유연하게 대응할 수 있다. 대칭키 암호 알고리즘을 이용한 암호화 기법은 이러한 화질 레이어의 특정 부분을 선택하여 암호화하며 특히, 화질 레이어의 첫 번째 레이어는 영상의 중요 정보를 포함하고 있어 영상의 재구성 과정에서 영상의 질을 결정하는 요소가 되므로 다른 레이어 보다 적은 양의 데이터로 높은 암호화 효과를 기대할 수 있다.

대칭키 암호를 이용한 암호 기법은 JPEG2000 표

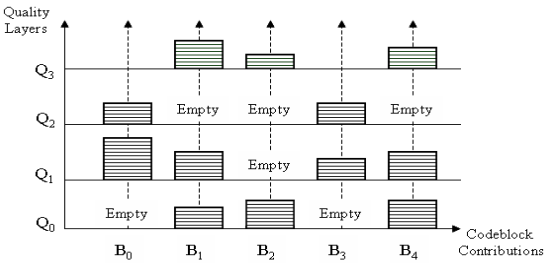


그림 4. JPEG2000의 화질 레이어

준과의 호환성 유지를 위하여 표준에서 사용되는 마커정보나 구문정보는 암호화하지 않는다. 하지만 영상의 압축 이후 수행되는 암호화의 경우 전체 코드스트림 중 암호화가 수행될 데이터 부분을 추출해야하므로 암호화를 수행하기 위한 연산 이외에도 탐색에 대한 연산이 더 필요하다. 이러한 부하를 줄이기 위하여 각 코드블록의 율 왜곡 최적화(rate-distortion optimization) 직후 암호화를 수행함으로써 암호화될 영상 데이터의 탐색에 필요한 부하를 줄일 수가 있다.

의료 영상은 그 특성상 영상의 해상도가 크고 픽셀당 비트수가 높아 데이터의 양이 많기 때문에 본 논문의 실험에서는 암호화 과정에서 처리 속도가 빠르고 안전성이 검증된 AES 암호 알고리즘을 사용하였으며 임의의 크기의 비트스트림의 데이터를 암호화하기 위하여 CFB(Cipher Feed Back) 모드가 사용되었다.

4. 실험결과

4.1 실험환경

기 제안된 두 가지의 기법은 JJ2000(Version 5.1)[17]을 사용하여 구현하였다. 그리고 실험에는 (표 1)과 같이 8bpp(bit per pixel) 흑백의 US, CR, CT, MRI 이미지가 사용되었으며 인코딩과 디코딩 과정에서 5-레벨의 DWT, 64×64 크기의 코드-블럭, 20개의 화질 레이어가 사용되었다. 그리고 화질의 왜곡 정도를 표현하기 위한 방법으로 PSNR(peak signal to noise ratio)이 사용되었다.

표 1. 각 영상의 PSNR 비교

Image and Size	Whole PSNR(dB)	ROI PSNR(dB)	Encrypted data raito
MRI (1024×1024)	12.793	10.002	1.258%
US (1215×948)	12.396	9.812	0.960%
CT (1134×1133)	12.814	7.780	0.727%
CR (1275×1067)	11.353	6.347	1.393%

비트 심도(bit depth) n에 따른 PSNR은 아래와 같이 정의된다.

$$PSNR = 10\log_{10}\frac{(2^n-1)^2}{MSE}$$

또한, MSE는 다음과 같이 정의된다.

$$MSE = \frac{\sum(\hat{x}-x)^2}{A}$$

여기서 x는 원 이미지의 픽셀 값을 나타내며, $\hat{x}$는 재구성된 픽셀 값을 나타내고 A는 관심영역을 나타낸다. PSNR을 통한 율 왜곡 표현에서 높은 값의 PSNR은 비교 영상이 원 영상과 유사한 화질을 가진다는 것을 의미한다. 반대로 낮은 PSNR값을 가지는 영상은 영상의 왜곡이 심하다는 것을 나타내며, 이것은 암호화 강도가 높다는 것을 의미한다.

4.2 실험결과 및 분석

첫 번째 실험은 랜덤 비트 인버팅이다. 각 해상도 레벨의 관심영역은 독립적으로 암호화 되며, 실험에서는 각 해상도 레벨의 고주파수 서브밴드에 존재하는 웨이블릿 계수의 MSB(MSB-0에서부터 MSB-8까지)를 각각 암호화 하였다. 예를 들어, 레벨-1은 HL1, LH1, 그리고 HH1 서브밴드에 존재하는 계수들을 의미한다.

(그림 5)의 실험결과와 같이 MSB-1과 높은 해상도 레벨을 선택하여 암호화하였을 때 그 강도가 가장 높다는 것을 알 수 있다. 그러나 부호비트인 MSB-0에서의 암호화 효과는 높지 않으며 다른 비트들과는 달리 낮은 해상도 레벨일수록 암호화 효과가 높은 것을 알 수 있다.

(그림 6)은 암호화로 인한 압축 효율의 손실을 알아보기 위하여 무손실 압축을 사용한 이미지의 압축 이후 암호화를 수행하였을 때의 파일 크기를 나타내고 있다. 실험결과를 통하여, 비트 인버팅을 통한 이미지의 암호화는 압축률에 큰 영향을 미치지 않는다는 것을 알 수 있으며 특히, 레벨 1부터 레벨 3까지의

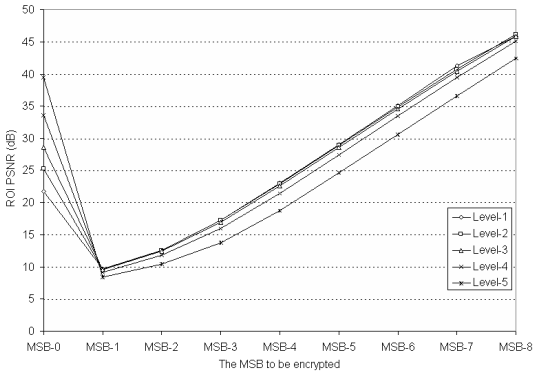


그림 5. 각 해상도 레벨의 MSB에서 PSNR 비교

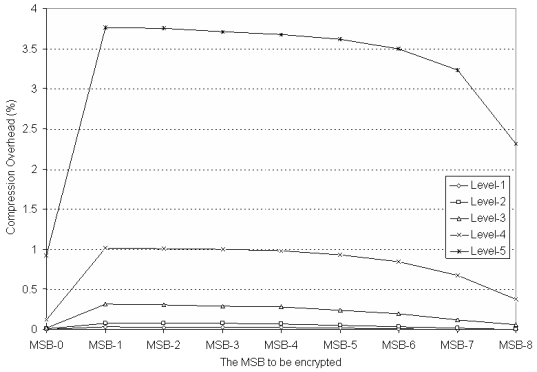


그림 6. 각 해상도 레벨의 MSB에서 파일크기 변화

낮은 해상도 레벨에서의 압축 손실은 0.5%이하로 0에 가까운 것을 확인할 수 있다.

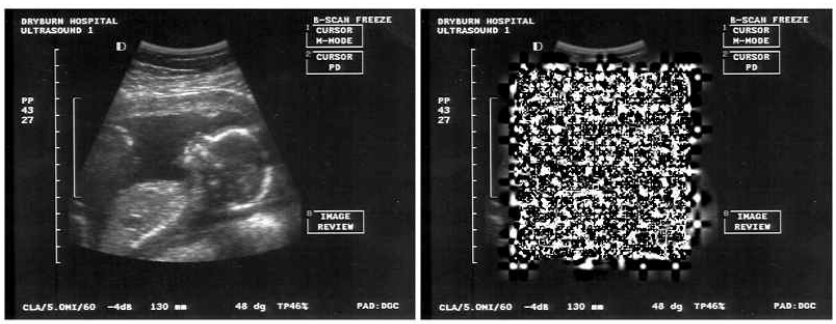
실험을 통하여 전체 영상에서 암호화 효과가 가장 큰 MSB-0와 MSB-1, 압축 효율의 손실이 적은 해상도 레벨 1에서 3까지를 선택하여 암호화하는 것이 가장 효율적이라는 것을 알 수 있다. (그림 7)은 MSB-0와 MSB-1, 그리고 해상도 레벨 1부터 3까지의 데이터를 암호화한 영상을 보이고 있다.

두 번째 실험은 관심영역의 첫 번째 화질 레이어 데이터를 AES 암호 알고리즘으로 암호화 한 것이다. 전체 이미지 중 20%의 영역이 관심영역으로 선택되었으며 (표 1)에서 관심영역의 PSNR, 전체 영상의 PSNR 그리고 암호화된 데이터의 비율을 보이고 있다. 암호화되는 데이터의 양은 전체 데이터에 비해 적지만 영상의 PSNR이 10dB 정도로 탁월한 암호화 효과가 있다. (그림 8)은 대칭키를 이용한 암호화 기법을 이용하여 영상을 암호화한 것이다.

4.3 안전성과 효율성

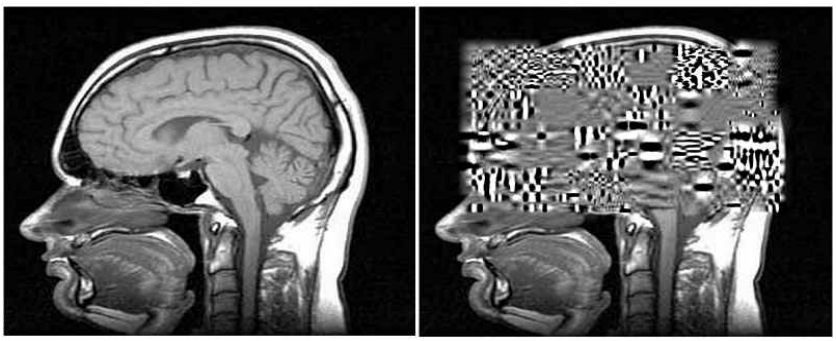
멀티미디어 암호 기법은 두 가지의 측면에서 안전성을 판단할 수 있다. 첫 번째 측면은 인간의 눈으로 보이는 시각적인 효과를 통하여 판단하는 것이다. 원 영상과 암호화 된 영상이 인간의 시각으로 얼마나 많은 차이를 보이는가 하는 것이 그 기준이 된다. 두 번째 측면은 암호학적인 측면에서의 접근으로써 멀티미디어에 적용된 암호 알고리즘의 암호학적 강도가 판단 기준이 된다. 의료 영상의 경우 육안으로 쉽게 인지할 수 있거나 낮은 안전성을 지니는 암호 알고리즘의 사용으로 인해 환자의 정보가 유출될 경우 환자 개인에게 심각한 영향을 끼칠 수 있으므로 의료 영상에 사용되는 암호 기법은 원 영상을 유추할 수 없게 함은 물론, 암호학적 안전성도 보장되어야 한다.

본 논문에서 제안된 랜덤 비트 인버팅의 안전성을 확인하기 위하여 에러 은닉 공격을 사용하였으며, 에러 은닉 공격은 암호화 된 데이터 부분을 0이나 1과 같은 고정된 값으로 교체하는 방법이다. (그림 9)(a)



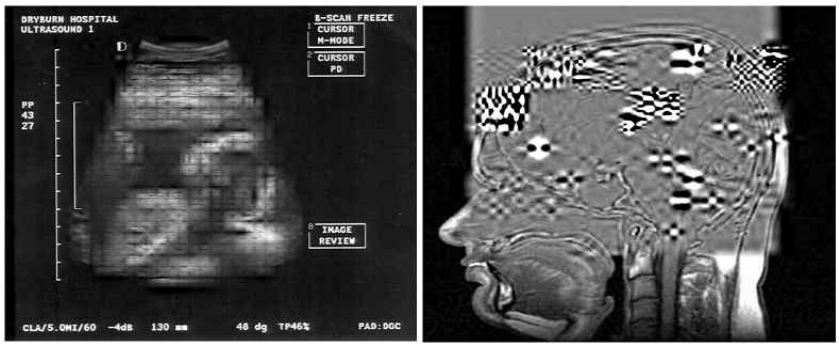
(a) 원 영상 (b) 암호화된 영상

그림 7. US 영상의 암호화(랜덤 비트 인버팅)



(a) 원 영상 (b) 암호화된 영상

그림 8. MRI 영상의 암호화(대칭키 암호를 이용한 암호화)



(a) 복원된 US 영상 (b) 복원된 MIR 영상

그림 9. 공격으로 복원된 이미지

는 암호화 된 (그림 7)(b)의 영상을 에러 은닉 공격을 통하여 복원한 영상이다. 원 영상인 (그림 7)(a)와 복원된 영상은 PSNR이 20.22dB로 동일 영상임을 유추할 수 있지만 복원된 영상으로 환자의 상태를 판단할 수 있을 정도의 정확성은 보이지 않는다. 그리고 랜덤 비트 인버팅 기법은 PRNG를 통한 랜덤 비트의 생성이후 XOR 연산을 통하여 암호화가 이루어지므로 연산양이 적어 쉽게 구현이 가능하며 영상 데이터의 상호연관성을 파괴시켜 암호화로 인한 압축률의 손실이 있지만 0.5% 이내로 무시할 정도이다.

대칭키 암호를 이용한 암호화 기법의 안전성은 대칭키 암호 알고리즘의 암호학적 강도에 기반하고 있다. AES와 같은 대칭키 암호 알고리즘의 경우에는 확산(diffusion)과 혼돈(confusion)을 통한 쇄도효과(Avalanche Effect)로 인해 에러 은닉 공격으로는 영상을 복원 할 수 없다. JPEG2000의 에러 강인 코딩[18]을 사용하여 공격이 가능하지만 효과적이지 못하다. (그림 9)(b)는 (그림 8)(b)를 에러 강인 코딩을 이용하여 복원한 영상을 보이고 있다.

5. 결 론

일반적인 자연 영상과 달리 의료 영상은 환자의 개인정보를 포함하고 있어 비인가 사용자가 임의로 접근하거나 열람할 수 없도록 접근제어 및 기밀성 유지가 필요하다. 본 논문에서는 의료영상의 기밀성 유지와 접근제어를 위한 JPEG2000의 관심영역 기반의 선택적 암호 기법을 제안하였다. 랜덤 비트 인버팅은 웨이블릿 변환 후 관심영역 내에 존재하는 계수들의 부호 비트와 MSB에서부터 임의의 몇 비트를 PRNG를 통해 생성된 임의의 비트열과 XOR 연산을 통하여 암호화한다. 실험을 통하여 낮은 해상도 레벨(1~3)과 MSB-0, MSB-1을 암호화 하였을 경우 암호화 효과가 가장 높다는 사실을 확인하였고 암호화

로 인한 압축률의 저하는 0.5%정도로 매우 낮다. 그리고 암호화에 복잡한 연산이 필요치 않고 구현이 간단하다는 특징을 가지므로 기존의 의료영상장치들에 쉽게 적용될 수 있을 것으로 기대한다. 그리고 대칭키 암호를 이용한 암호화는 보다 뛰어난 안정성을 제공하기 위하여 압축된 관심영역의 영상 데이터에 AES와 같은 암호 알고리즘을 사용하는 기법으로, 안전성은 사용되는 암호 알고리즘의 안전성에 기반하며, JPEG 2000 코드스트림 구조의 첫 번째 화질 레이어만을 사용하므로 적은 양의 데이터 암호화로 높은 효율을 보인다.

참 고 문 헌

[1] PS 3.1-2003, DICOM (Digital Imaging and Communications in Medicine) Part 1: Introduction and Overview, National Electrical Manufactures Association, 2003.

[2] PS 3.1-2003, DICOM (Digital Imaging and Communications in Medicine) Part 5: Data Structures and Encoding, National Electrical Manufactures Association, 2003.

[3] ISO/IEC 15444-1: Information Technology-JPEG2000 Image Coding System-Part 1: Core Coding System, 2000.

[4] A.P. Bradley and F.W.M. Stentiford, "JPEG2000 and Region of Interest Coding," *Digital Image Computing Techniques and Applications*, pp. 303-308, 2002.

[5] FIPS PUB 197: Advanced Encryption Standard(AES), http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf, Nov, 2001.

[6] D. Taubman and M. Marcellin, *JPEG2000: Image Compression Fundamentals, Standards and Practice*, Kluwer Academic Publishers, 2002.

[7] K. Ando, O. Watanabe, and H. Kiya, "Partial Scambling of Images Encoded by JPEG2000," *The Institute of Electronics Information and Communication Engineers Transactions*, Vol.11, No.2, pp. 282-290. 2002.

[8] R. Grosbois, P. Gerbolot, and T. Ebrahimi, "Authentication and Access Control in the JPEG2000 Compressed Domain," *Processing SPIE 46th annual Meeting, Applications of Digital Image Processing XXIV*, pp. 95-104, 2001.

[9] R. Norcen, and A. Uhl, "Encryption of Wavelet-Coded Imagery Using Random Permutations," *International Conference on Image Processing*, pp. 3431-3434, 2003.

[10] T. Uehara, R. Safavi-Naini, and P. Ogrunbona, "Securing Wavelet Compression with Random Permutations," *IEEE Pacific Rim Conference on Multimedia*, pp. 332-335, 2000.

[11] R. Norcen and A. Uhl, "Selective Encryption of the JPEG2000 Bitstream," *International Federation for Information Processing*, LNCS 2828, pp. 194-204, 2003.

[12] S. Lian, J. Sun, D. Zhang, and Z. Wang, "A Selective Image Encryption Scheme Based on JPEG2000 Codec," *Advances in Multimedia Information Processing*, LNCS 3332, pp. 65-72, 2004.

[13] A. Pommer and A. Uhl, "Selective Encryption of Wavelet-packet Encoded Image Data - Efficiency and Security," *ACM Multimedia Systems (Special issue on Multimedia Security)*, pp. 279-287, 2003.

[14] D. Engel and A. Uhl, "Lightweight JPEG2000 Encryption with Anisotropic Wavelet Packets," *International Conference on Multimedia & Expo*, pp. 2177-2180, 2006.

[15] J. Wen, M. Severa, and W. Zeng, "A Format-Compliant Configurable Encryption Framwork for Access Control of Video," *IEEE Transaction on Circuits and Systems for Video Technology*. Vol.12, No.6, pp. 545-557, 2002.

[16] W. Zeng, H. Yu, and C.Y. Lin, *Multimedia Security Technologies for Digital Rights Management,* Elsevier, Oxford, UK., 2006.

[17] JJ2000-Java Implementation of JPEG2000,

http://jpeg2000.epfl.ch/

[18] L. Moccagatta, S. Soudagar, J. Liang, and H. Chen, “Error-Resilient Coding in JPEG2000 and MPEG-4,” *IEEE Journal on Selected Areas in Communications*. Vol.18, No.6, pp. 899-914, 2000.

이 원 영

2007년 2월 부경대학교 컴퓨터 멀티미디어공학과 졸업
2007년 3월～현재 부경대학교 정보호호학과 석사과정
관심분야 : 정지영상 및 동영상 암호화, 디지털 서명.

Yang Ou

2004년 7월 중국 Liaoning 과학기술대학 컴퓨터과학과 학사
2006년 8월 경상대학교 정보시스템학과 석사
2006년 9월～현재 부경대학교 정보보호학과 박사과정
관심분야 : 정지영상 압축, 정지영상 및 동영상 암호화.

이 경 현

1982년 경북대학교 수학교육과 학사
1985년 한국과학기술원 응용수학과 석사
1992년 한국과학기술원 수학과 박사
1993년～현재 부경대학교 전자컴퓨터 정보통신공학부 교수
관심분야 : 정보보호론, 공개키 암호, 신원기반 암호, 멀티미디어 정보보호, 그룹 키 관리