실시간 처리를 위한 쿼드트리 기반 무손실 영상압축 및 암호화

윤 정 오[†]·성 우 석[††]·황 찬 식[†††]

요 약

일반적으로 무손실 영상압축 및 암호화 방법에는 압축과 암호화 과정이 독립적으로 이루어진다. 압축 후 암호화를 수행하면 압축열이 암호에 대한 평문으로 사용되므로 압축에 따른 엔트로피가 감소하여 랜덤한 성질을 갖게된다. 그러나 압축열 전체에 대한 암호화는 수행시간이 길어져 실시간 처리를 저해하는 원인이 되기도 한다. 본 논문에서는 무손실 영상압축과 암호의 결합에서 전체 처리시간을 줄이는 방법을 제안한다. 이는 쿼드트리 압축 알고리즘으로 그레이 영상을 분해하여 구조부분만을 암호화하는 방법이다. 아울러 영상의 무상관성과 동질영역을 확보하기 위한 변환과정을 수행하여 무손실 압축성능을 개선하였고, 쿼드트리 분해시 암호화되지 않은 데이터를 레벨별로 재구성하여 안전성을 갖도록 하였다. 모의 실험을 통하여 제안한 방법이 영상 압축율의 개선과 암호화 방법의 안전성 확보 및 실시간 처리가 가능함을 확인하였다.

QuadTree-Based Lossless Image Compression and Encryption for Real-Time Processing

Jeong-oh Yoon[†] · Woo-seok Sung[††] · Chan-sik Hwang[†††]

ABSTRACT

Generally, compression and encryption procedures are performed independently in lossless image compression and encryption. When compression is followed by encryption, the compressed-stream should have the property of randomness because its entropy is decreased during the compression. However, when full data is compressed using image compression methods and then encrypted by encryption algorithms, real-time processing is unrealistic due to the time delay involved. In this paper, we propose to combine compression and encryption to reduce the overall processing time. It is method decomposing gray-scale image by means of quadtree compression algorithms and encrypting the structural part. Moreover, the lossless compression ratio can be increased using a transform that provides an decorrelated image and homogeneous region, and the encryption security can be improved using a reconstruction of the unencrypted quadtree data at each level. We confirmed the increased compression ratio, improved encryption security, and real-time processing by using computer simulations.

키워드 : 쿼드트리(quadtree), 무손실 영상압축(lossless image compression), 영상암호(image encryption)

1. 서 론

최근 인터넷 사용이 보편화되면서 방대한 양의 영상 데이터에 대한 통신시간의 단축과 통신비용의 절감이 요구되고 있으며 통신보안의 중요성이 점점 증대되고 있는 실정이다. 특히 의료영상, 군사용 영상, 위성영상 등과 같이 정밀성과 보안을 필요로 하는 데이터를 전송할 경우는 무손실(lossless) 영상압축과 암호화(encryption)가 이루어지게 된다. 영상압축 및 암호화 방법에는 압축과 암호화 과정을 독립적으로 수행하는 방법과 압축과 암호화 과정이 동시에 이루어지도록 하는 방법이 있다. 전자는 영상압축 과정을 거친 압축열 전체를 AES, RSA [1, 2]등의 암호 알고리즘을 사용하여 독립적으로 암호화하는 방법으로 안전성은 확보가 되지만 암호화 시간이 길어져 실시간 통신을 어렵게 하는 문제점이 있다. 후자는 영상압축 알고리즘에 초기 데이터 구조를 변화시키는 방법[3], 난수를 평문에 삽입하여 정돈된 평문을 흩트리는 방법[4], Space-Filling 곡선을 사용하여 각 프레임의 화소들을 스크램블 하는 방법[5], SCAN 패턴에 의해 조합하여 치환하는 방법[6, 7]등의 암호화 과정을 추가함으로써 영상압축과 암호화가 동시에 이루어지게 하는 방법이다. 그러나 후자의 경우 난수 삽입에 의한 방법은 영상압축 성능이 감소되며 스크램블과 치환과정을 이용한 방법은 영상의 히스토그램 공격 등에 취약성이 있다. 이

† 정 회 원 : 경운대학교 정보통신공학과 교수
†† 정 회 원 : 경북대학교 대학원 전자공학과
††† 정 회 원 : 경북대학교 전기전자공학부 교수
논문접수 : 2001년 8월 6일, 심사완료 : 2001년 10월 15일

와 같이 영상 압축과 암호의 결합에 관련된 기존의 방법들은 지연시간이 길어 실시간 통신이 불가능하거나 압축성능의 저하 및 공격자의 공격에 취약성이 노출되는 문제점들을 지니고 있다.

본 논문에서는 무손실 영상압축과 암호의 결합에서 원영상에 포함된 중복성을 감소시켜 암호적 성질이 향상되도록 무손실 압축성능을 개선하는 방법과 암호화 강도를 유지하면서 압축 데이터의 일부분만을 암호화하도록 하여 암호화 과정에서 소요되는 암호화 시간을 줄일 수 있는 방법에 대해 제안한다. 제안한 방법에서 암호적 성질을 향상시키기 위한 압축과정은 무손실(lossless)이 되도록 그레이 영상에 적용하여 무상관성(decorrelation)을 갖도록 예측오차를 구하고 동질영역들을 확보하기 위한 변환과정을 수행한 다음 쿼드트리 알고리즘을 기반으로 한 분해과정을 수행하였다. 또한 암호화를 위한 방법으로는 압축과정에서 쿼드트리 형태로 분해되어진 영상의 윤곽을 나타내는 구조(structure)부분만을 DES나 AES 등의 알고리즘으로 암호화하도록 하였다. 이는 분리된 쿼드트리 구조의 파일크기가 압축열 전체 크기보다 적으므로 암호화 시간이 감소되는 것을 의미하며 실험영상에 적용하여 이를 확인할 수 있다. 그리고 안전성 평가를 위해 필요한 요소들을 분석하고 특히, 쿼드트리 분해를 할 때 암호화가 되지 않는 쿼드트리 데이터를 안전성이 유지되도록 재구성하여 하였다.

본 논문의 구성은 다음과 같다. 2장에서는 쿼드트리 알고리즘에 대해 설명하고 3장에서는 무손실 영상압축 및 암호화에 대해 설명한다. 4장에서는 실험 결과 및 분석, 5장에서 결론을 맺는다.

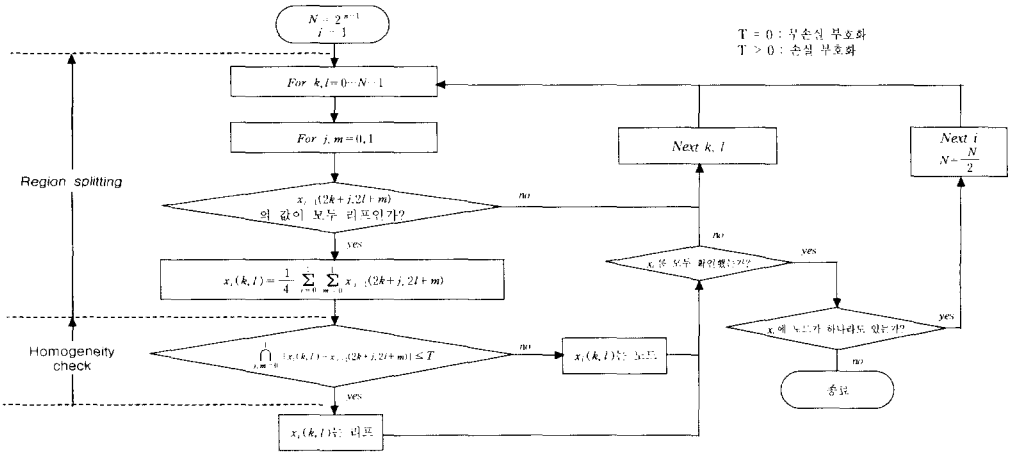
2. 쿼드트리 알고리즘

쿼드트리 생성은 크게 두 과정으로 나눌 수 있으며 영상을 4개의 쿼드런트(quadrant)로 분리하는 영역 분할 과정과 분할된 영역의 동질성(homogeneity)을 검사하는 과정이다. 영역 분할의 진행 방향은 하향식(top-down procedure)과 상향식(bottom-up procedure)이 있으며[8] 하향식은 전체의 영역이 하나의 값으로 표현될 수 있는지 먼저 판단하고, 그렇지 않으면 영역을 같은 크기가 되도록 네개의 부블록(sub-block)으로 나눈다. 나누어진 각 부블록들이 다시 하나의 값으로 표현될 수 있는지 판별하는 과정을 거쳐 더 작은 부블록으로 나누어 가는 과정을 반복한다. 상향식은 최소 블록 크기(1×1 블록)인 화소에 대해 이웃하는 화소들과 병합할 것인지를 판별해 나가는 방식으로 유효한 부블록이 동질 영역으로 판별되면, 다시 상위 영역의 블록으로 병합될 수 있는지를 판단하는 반복 과정이며 일반적으로 상향식 진행 절차가 쿼드트리 압축과정에서 효과적인 방법으로 알려져 있다.

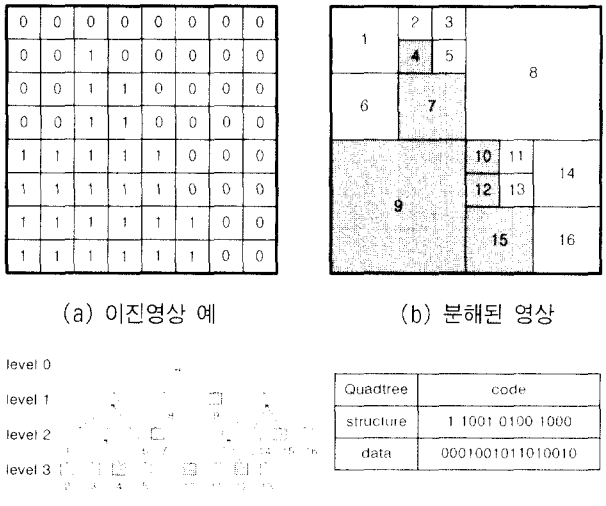
(그림 1)은 상향식 진행 절차로 영역분할 과정과 동질성 검사과정이 수행되는 쿼드트리 알고리즘을 흐름도로 표현하였다. 영상의 크기는 $2^n \times 2^n$으로 가정할 때 n은 레벨 수이며, N은 영상크기인 2^n이다. $x_i(k,l)$은 (k,l)위치에서의 레벨 i에 대한 쿼드트리 노드를 나타내고 있다. 또한 레벨 i의 노드에 대한 자식노드들은 NW-NE-SE-SW의 순서로 $x_{i-1}(2j,2k)$, $x_{i-1}(2j-1,2k)$, $x_{i-1}(2j+1,2k+1)$, $x_{i-1}(2j,2k+1)$이 된다. 이와 같이 정의된 (그림 1)의 쿼드트리 알고리즘은 임계값 T에 따라 손실 혹은 무손실 분해가 가능하다.

영상을 쿼드트리 알고리즘으로 분해하면 각 레벨에서 분리되는 정보를 갖는 쿼드트리 구조와 영상의 화소 값들인 쿼드트리 데이터가 만들어진다. 쿼드트리 구조는 0과 1의 값들로 구성되며 0은 리프(leaf)노드이고 1은 내부(internal)노드를 나타낸다. 리프노드는 현재의 레벨에서 분해가 종료되며 내부노드는 다음 레벨에서 4개의 쿼드런트로 분해가 이루어지는 것을 의미한다. 쿼드트리 데이터는 각 레벨의 리프노드에 대응되는 영상의 화소 값들이다.

(그림 2)는 $2^3 \times 2^3$크기와 트리 깊이(depth) 3을 갖는 간



(그림 1) QuadTree 알고리즘 흐름도

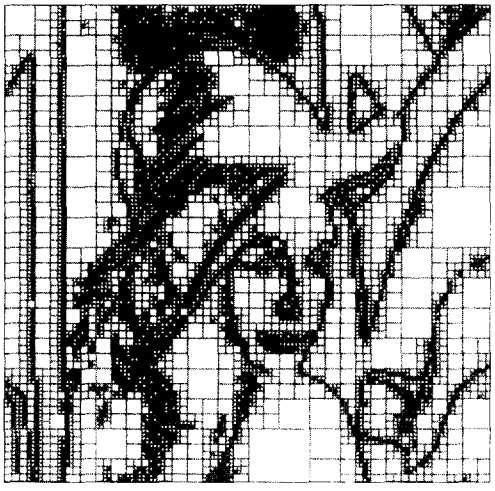


(a) 이진영상 예 (b) 분해된 영상

(c) 쿼드트리 표현 (d) 쿼드트리 부호화

(그림 2) 이진영상의 쿼드트리 부호화

(a) 이진 Lena 영상



(b) Lena 영상의 쿼드트리 구조

(그림 3) 이진 Lena 영상의 쿼드트리 구조

단한 이진영상을 무손실 쿼드트리 알고리즘에 적용할 때 쿼드트리 구조와 쿼드트리 데이터 값이 생성되는 과정을 나타낸 것이다. 분해된 영상에 표시된 숫자는 쿼드트리 데이터가 저장되는 순서를 나타낸다. (그림 2)의 쿼드트리 표현에서 원형의 노드는 4개의 부블록(sub-block)으로 분해가 더 이루어지는 것을 의미하는 내부노드이며 사각형의 노드는 더 이상의 분해가 이루어지지 않는 리프노드이다.

(그림 2)의 쿼드트리 부호화는 쿼드트리 구조의 부호화와 쿼드트리 데이터의 부호화로 분리되어 이루어지며 구조는 쿼드트리 표현에서 상위 레벨부터 순서대로 0과 1로 표현되고 쿼드트리 데이터는 저장되는 순서에 따라 리프노드에 대응되는 이진영상의 화소 값들로 이루어진다.

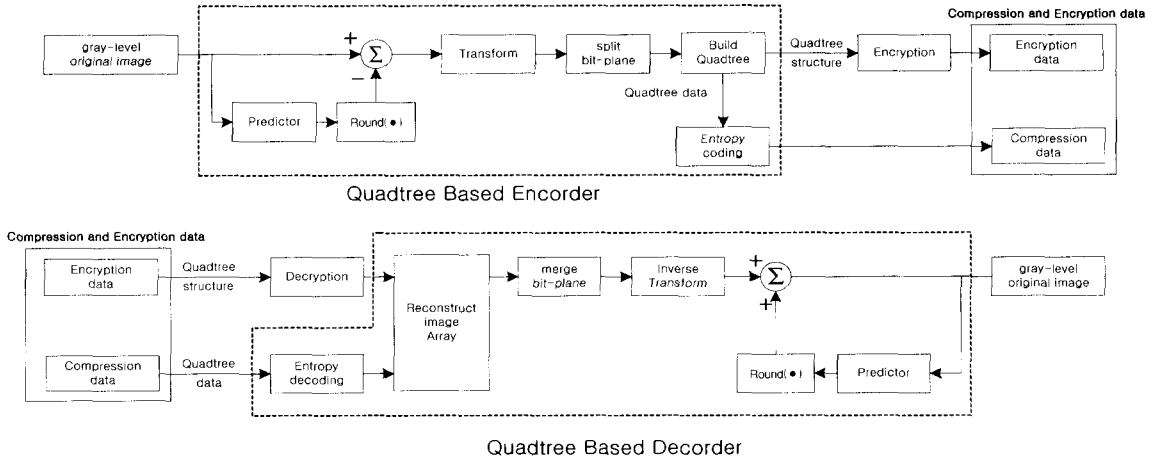
(그림 3)은 영상 크기가 $2^9 \times 2^9$인 이진 lena 영상에 쿼드트리 알고리즘을 적용하여 분해한 영상의 쿼드트리 구조를 나타내었다. 분해된 쿼드트리 구조는 원 영상의 윤곽(outline)을 나타내는 에지 성분들이며 동질영역의 위치와 크기 정보를 포함하고 있다.

3. 무손실 영상압축 및 암호화

압축과 암호의 결합시스템을 이용하는 것은 통신망에서 효율성과 기밀성을 동시에 만족시킬 수 있다는 것을 의미한다. 이러한 효과를 달성하기 위해 압축과 암호를 결합하며 Shannon과 Hellman에 의해 압축 알고리즘이 정보 이론적 차원에서 암호에 좋은 영향을 미칠 것이라는 가능성이 제시되었다[9, 10]. 이는 압축 수행후 암호화를 수행하면 압축열을 암호에 대한 평문으로 사용함으로서 평문을 암호화하는 것보다 암호 강도가 더욱 증가하기 때문이다. 또한 압축은 중복성(redundancy)을 감소시키는 방법의 일종으로 원 데이터에 포함된 통계적 성질이 압축열에서는 감소되어 압축열 자체가 암호적 성질을 지니게 되므로 압축 알고리즘이 공개되지 않으면 공격자는 압축열 해독이 불가능하다. 그러나 압축 알고리즘과 암호 알고리즘을 모듈화하여 압축 후 암호화를 수행하면 압축열 전체에 대해서 암호화를 수행하므로 처리시간이 느린 단점이 있다.

본 논문에서는 쿼드트리 알고리즘을 기반한 무손실 압축 성능을 개선하여 암호적 성질이 향상되도록 하였으며, 암호화 과정의 소요시간을 줄이기 위해 압축열 전부를 암호화하는 대신에 압축과정에서 분리된 정보의 일부분만 암호화하여 실시간 통신에 적합하도록 (그림 4)와 같이 구성하였다.

(그림 4)에서 무손실 쿼드트리 알고리즘은 동질영역들을 분해(decomposition)하여 쿼드트리 구조를 만들고 동질영역의 대표값들로 쿼드트리 데이터를 구성하여 공간적인 중복



(그림 4) 제안한 무손실 영상 압축방법 및 암호의 결합방법

성을 제거하는 압축방법이다. 그러나 쿼드트리 알고리즘을 그레이 영상에 직접 적용하면 동질 영역들이 거의 존재하지 않는 복잡성을 가지고 있어 압축성능의 개선을 기대할 수 없다. 따라서 압축성능을 개선하기 위해 전처리 과정을 거쳐 무상관성과 동질영역이 형성되도록 하였다. 영상내 화소들의 상관성을 제거하기 위해 예측자로 예측오차를 구하였으며, F-변환[11]을 수행하여 분산된 예측오차들의 분포를 최대값 주위에 집중되도록 재구성하였다. 이는 비트 평면(bit-plane)으로 분리할 경우 동질영역들이 MSB(most significant bits)측의 비트 평면에서 많은 분포가 이루어지며, 아울러 비트 평면간의 상관성이 제거된다는 것을 의미한다. 이와 같은 전처리 과정은 쿼드트리 알고리즘으로 무손실 영상압축을 수행할때 훨씬 효율적인 압축성능을 얻을 수 있게 된다.

쿼드트리를 기반으로 한 무손실 영상압축은 쿼드트리 구조와 쿼드트리 데이터라는 두 개의 압축열이 생성된다. 특히, 쿼드트리 구조는 동질영역의 크기와 위치정보들로 구성된 영상의 윤곽 정보들로써 이를 알지 못하면 영상복원이 힘든 중요한 부분이다. 따라서 암호화를 위한 방법은 압축열 전체를 암호화하지 않고 구조부분만을 DES나 AES등의 알고리즘으로 암호화함으로써 압축열 전체를 암호화하는것보다 암호화 과정의 처리시간이 단축되도록 하였다. 일반적으로 압축과 암호의 결합 구조에서는 압축과정에서 소요되는 처리시간 보다는 암호화 과정에서 소요되는 처리시간이 훨씬 길어지게 된다[1, 2, 7]. 그러므로 실시간 처리가 가능하기 위해서는 암호화 과정의 처리시간 단축이 중요한 관건이 된다.

제시한 암호의 결합 방법은 압축열의 구조부분만을 암호화하므로 영상전체를 압축하고 암호화하는 방법 보다 처리속도가 훨씬 빠른 특징을 가지고 있다. 따라서 처리시간의 단축정도는 동일한 암호알고리즘을 적용하는 경우 암호화되는 압축열 전체의 파일크기와 쿼드트리 구조부분의 파일크기를 서로 비교함으로써 구할 수 있다.

3.1 무손실 영상압축 방법

무손실 영상압축은 무상관성 과정과 부호화 과정으로 이루어진다. 본 논문에서는 쿼드트리 알고리즘을 이용하여 무손실 압축성능을 개선하기 위한 방법으로 3단계의 무상관성과 동질영역을 만드는 전처리 과정을 거쳐 압축하도록 하였다.

예측자는 무손실 JPEG 표준안[12]에서 제시한 선형 예측자들 중에서 모드 "6" 과 화소 근처의 기울기 강도를 적응적으로 처리하는 비선형 예측자인 GAP[13]의 두가지 경우에 대해 독립적으로 예측오차를 구하여 제안한 방법에 적용하였다.

구해진 예측 오차값들은 최소, 최대값에 가까운 값들로 많이 분포되어 있어 동질영역들이 거의 존재하지 않으며 동질영역들의 생성이 이루어지도록 비트 평면으로 분리하였다. 그러나 비트 평면으로 분리할 경우, 비트 평면간 상관성 제거와 MSB(most significant bits) 영역의 값들로 구성된 비트 평면들이 LSB(least significants bits) 영역의 비트 평면들 보다 동질영역이 많이 형성되므로 모든 영역의 비트 평면에서 효율적인 동질영역이 분포되도록 고려해야 한다. 따라서 비트 평면을 구성하기 전에 MSB 영역의 비트 평면들에 대해 더욱 많은 동질 영역이 생성되도록 식 (1), 식 (2)와 같은 가역의 F-변환 과정을 거쳤다. $d'(i,j)$는 예측 오차값이고 q는 화소를 표현하는 비트 수이다.

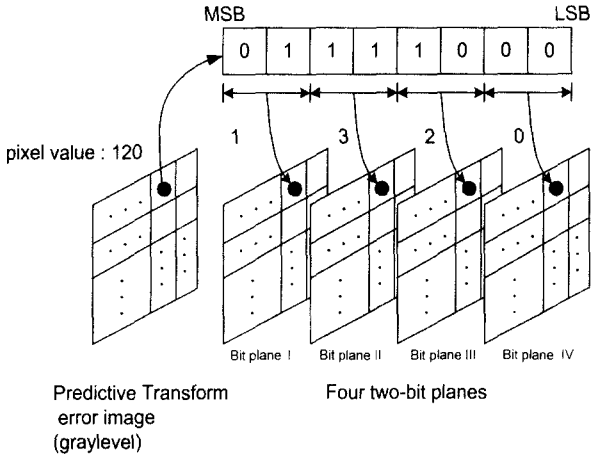
$$d_1(i,j) = F[d'(i,j)] = \begin{cases} 0 & \text{if } d'(i,j)=0 \\ d'(i,j)-1 & \text{if } d'(i,j) \le 2^q - m \\ 2(2^q - d'(i,j)) & \text{if } d'(i,j) > n \end{cases} \quad (1)$$

단, $m = 1 \cdots 2^{q-1}-1$, $n = 1 \cdots 2^{q-1}$

$$d'(i,j) = F^{-1}[d_1(i,j)] = \begin{cases} 0 & \text{if } d_1(i,j)=0 \\ 2^q - m & \text{if } d_1(i,j)=2m \\ n & \text{if } d_1(i,j)=2n-1 \end{cases} \quad (2)$$

단, $m = 1 \cdots 2^{q-1}-1$, $n = 1 \cdots 2^{q-1}$

변환된 예측오차 영상을 비트 평면으로 구성하기 위해 영상의 각 화소를 비트 단위로 표현한 다음 2비트씩 묶어 4개의 4진 비트 평면으로 나누었다. 즉, 그레이 레벨을 갖는 변환 예측오차 영상에 대해 각 화소들을 비트 단위로 표현하고 상위 비트부터 차례로 2비트씩 묶어 4진 영상을 갖도록 (그림 5)와 같이 비트 평면을 구성하였다. (그림 5)와 같이 구성된 비트 평면은 F-변환으로 동질영역이 최적으로 생성되며 비트 평면간 상관성 제거[14]도 가장 효율적으로 이루어진다.

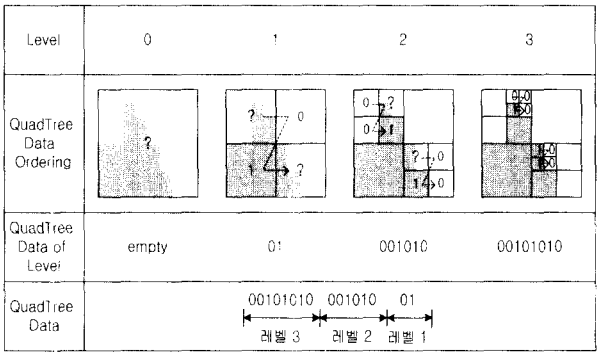


(그림 5) 비트 평면 구성방법

이와 같이 구성된 각 비트 평면에 대해 무손실 쿼드트리 알고리즘을 적용하여 영상압축을 수행하였다. 생성된 압축열은 쿼드트리 구조부분과 쿼드트리 데이터 부분으로 구성되어 있으며, 제시된 방법으로 모의실험을 한 결과 기존의 무손실 JPEG 표준안과 GAP 방법 보다 압축율(bpp) 측면에서 평균적으로 압축성능이 개선되었고 일부 영상들에서만 거의 유사한 압축성능이 있음을 확인할 수 있었다. 이는 제안한 압축방법이 동질영역을 많이 포함하고 있는 영상에 대해서 특히 압축성능이 뛰어나다는 것을 의미한다.

3.2 암호화 방법

압축과정에서 쿼드트리 알고리즘에 의해 분해되어진 구조부분은 영상의 윤곽(outline)을 재구성할 수 있는 동질영역의 위치와 크기를 나타내는 중요한 정보를 지니고 있으며, 데이터 부분은 단순히 동질영역의 화소값들 만으로 이루어진다. 따라서 암호화 시간을 단축하기 위해 영상의 중요한 정보가 포함된 구조부분만을 AES나 RSA등의 알고리즘으로 암호화하도록 하였다. 그러나 무손실인 경우 쿼드트리 데이터들은 동일한 비트 할당을 하여 표현하고 좌에서 우로 횡단(traversal)하는 순서[15]로 구성되어 화소값의 정보가 노출되어 있다. 즉, 쿼드트리 데이터의 처음 값은 영상의 좌측 상단에 위치하는 화소값이고 마지막 데이터는 영상의 우측 하단에 위치하는 화소값이 되리라는 예측을 할 수 있다. 이는 영상의 경우 배경부분 같은 것은 일부분의 데이터만으로도 넓은 영역들의 복원이 가능함을 의미한다. 따라서 본 논문에서는 쿼드트리 알고리즘으로 분해하는 과정에서 쿼드트리 데이터의 구성순서를 (그림 6)의 방법으로 재구성하여 영상의 외각부분 노출 가능성을 제거하였다. 이는 쿼드트리 데이터부분의 구성순서를 은닉하는 방법이다.



(그림 6) 쿼드트리 데이터의 구성방법

(그림 6)은 흰색과 검은색의 블록이 각각 "0"과 "1"의 화소값을 가지는 8×8 크기의 이진영상에 대해 쿼드트리 데이터를 구성하는 방법이다. 구성 방법은 레벨별로 분해가 더 이상 되지 않는 블록의 화소값을 비월 주사(raster scan) 방식의 순서로 탐색하면서 쿼드트리 데이터를 구성하였으며, 최하위 레벨에서 최상위 레벨로 서로 결합하여 쿼드트리 데이터가 되도록 하였다. 그리고 각 레벨을 분리하기 위한 별도의 부호화 과정은 쿼드트리 분해가 이루어진 다음의 과정이므로 필요가 없다.

3.3. 쿼드트리 특성에 따른 안전성 분석 방법

제시된 암호화 방법의 안전성을 분석하기 위해 우선 쿼드트리 알고리즘이 갖는 특성[16]을 정리하였다.

정리 1. 내부노드 수 r이 "0"이상의 정수일 때 완전한 쿼드트리는 4r+1개의 노드를 가 지며 리프 노드는 3r+1개를 가진다.

정리 2. 4r+1개의 노드와 h+1의 깊이(depth)를 가지는 쿼드트리들과 r개의 노드와 h의 깊이를 가지는 4-ary

tree 들은 일대일 대응관계이다.

정리 3. 최대 깊이가 h+1이고 3r+1개의 리프 노드를 가지는 쿼드트리 개수는 최대 깊이 가 h이고 r개의 노드를 가지는 4-ary 트리 수와 같다.

정리 4. 생성 가능한 쿼드트리의 수 $a_{r,h}$는 식 (3), 식 (4)와 같다.

$$g_h(z) = \sum_r a_{r,h} z^r \tag{3}$$

$$g_h(z) = \begin{cases} 1+z & ,If\ h=0 \\ 1+z(g_{h-1}(z))^4 & ,If\ h>0 \end{cases} \tag{4}$$

쿼드트리 구조의 크기와 데이터의 크기는 정리 1에 의해 이론적인 근사값을 구할 수 있다. 쿼드트리의 각 노드는 내부 노드와 리프 노드뿐이므로 "1"과 "0"의 한 비트로 표현되어 구조 크기는 4r+1 비트를 가지고 화소값이 B 비트로 표현되는 영상인 경우 쿼드트리 데이터의 크기는 B(3r+1) 비트이다. 따라서 전체 쿼드트리 크기에서 쿼드트리 구조가 차지하는 크기는 식 (5)로 나타낼 수 있다. <표 1>은 B 값에 따른 쿼드트리 구조의 크기를 식 (5)에 의해 구한 근사값이다.

$$\frac{4r+1}{B(3r+1)+4r+1} \tag{5}$$

〈표 1〉 B 값에 따른 쿼드트리 구조 크기의 백분율

B	1	2	3	4	5	6	7	8
쿼드트리 구조크기(%)	57.1	40.0	30.8	25.0	21.1	18.2	16.0	14.3

본 논문에서 제시한 암호화 구조는 압축과정에서 중요한 데이터의 일부분에 대해 안전성이 입증된 암호알고리즘으로 암호화를 시키는 구조이다. 따라서 안전성분석 측면에서 살펴보면, 암호화가 이루어지는 부분의 데이터 양이 암호화가 되지 않는 데이터 양에 비해 상대적으로 아주 작아 임의로 구성 가능한지에 대한 고려가 있어야 한다. 아울러 상당한 크기의 암호화되지 않은 쿼드트리 데이터를 가지고 영상 복원이 가능한지에 대한 분석도 아울러 이루어져야 한다. 그러므로 제시된 암호화 방법의 안전성 분석은 쿼드트리 알고리즘의 특성을 이용하여 암호화가 이루어지는 구조부분과 암호화가 되지 않는 데이터부분에 대해 3가지 측면을 고려하였다.

첫째는 암호화 과정의 처리시간이 단축되는 것을 확인하기 위해 구조 부분의 크기를 구하여 압축된 전체 데이터 크기와 비교하는 방법이다. 둘째는 발생 가능한 쿼드트리를 모두 구하여 각 쿼드트리에서 분리된 구조부분으로 영상의 윤곽을 구성하고 암호화되지 않은 데이터 부분을 대입하여 복원을 시도하는 방법이다. 즉, 쿼드트리 발생 개수에 의한 전수공격 방법의 형태로써 쿼드트리 발생 개수가 많을 경우 영상복원이 불가능하다고 할 수 있다. 셋째는 쿼드트리 알고리즘의 특성을 분석하여 구조부분을 모르더라도 암호화되지 않은 쿼드트리 데이터의 구성순서와 비트 할당 등의 성질을 파악하여 영상복원 가능성을 분석해 보는 방법이다. 이와 같이 제시한 안전성 분석의 요소들은 쿼드트리 압축 알고리즘의 특성에 기반하고 있다.

4. 실험 결과 및 분석

4.1 압축 성능

제안한 무손실 압축 방법의 성능 평가를 위해 컴퓨터 모의실험을 수행하였다. 분석에 있어서 PC 펜티엄Ⅲ(800MHz)를 사용하였으며, 실험에 사용된 영상은 크기가 512 × 512이고 8비트 그레이 레벨을 갖는 CT, MRI, US, Lena, Sailboat,

(a) CT영상 (b) MRI 영상

(c) US 영상 (d) Lena 영상

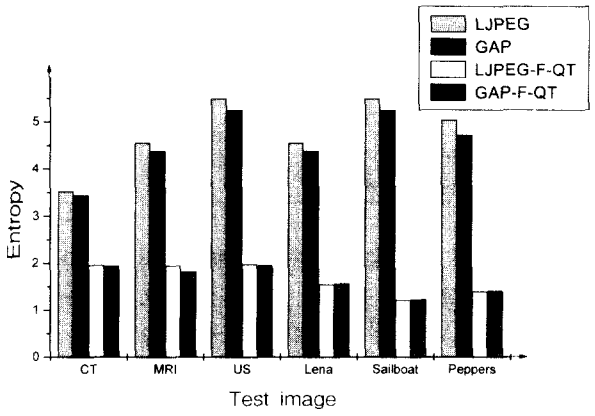
(e)Sailboat 영상 (f) Peppers 영상

(그림 7) 실험 영상들

Peppers 영상으로 (그림 7)과 같다. 일반적으로 영상의 무손실 압축성능을 평가하기 위한 척도로는 엔트로피와 압축율을 구하여 비교한다. 식 (6)은 엔트로피를 계산하기 위한 것으로 엔트로피가 적을수록 화소간의 상관성이 줄어들어 압축 효율이 개선됨을 나타낸다. 식 (7)는 각 화소를 표현하는 평균 비트수를 bpp(bit per pixel)로 나타낸 것으로 압축율이다.

$$H = -\sum_{i=1}^{L} P_i \log_2 P_i \tag{6}$$

$$bpp = \frac{8 \times compressed\ file\ size}{original\ file\ size} \tag{7}$$



(그림 8) 기존의 방법과 제안한 방법의 엔트로피

(그림 8)은 기존의 무손실 압축 방법들인 JPEG 표준안, GAP 방법과 제안한 방법들인 예측, F변환, 쿼드트리를 결합한 방법(LJPEG-F-QT, GAP-F-QT)을 식 (6)을 가지고 실험 영상에 적용하여 구한 엔트로피이다. 이는 제안한 방법이 기존의 방법들보다 엔트로피가 적어 화소간의 상관성이 많이 줄어들었다는 것을 의미하며 부호화 할 경우 압축율이 개선되리라는 것을 추측할 수 있다.

<표 2>는 실험 영상들에 대해 기존의 방법과 제안한 방법의 압축율을 식 (7)을 이용하여 구한 것이다. <표 2>에 의하면 제안한 방법이 무손실 JPEG 표준안 보다 평균 약 0.27 bpp 정도 압축율이 개선되었음을 알 수 있으며, 특히 의료영상인 CT, MRI, US 영상은 다른 실험 영상들에 비해 동질영역을 많이 포함하고 있어 쿼드트리 알고리즘을 기반한 제안한 방법이 기존의 방법보다 우수한 압축 결과를 얻을 수 있었다.

〈표 2〉 실험 영상들에 대한 압축율 비교

(단위 : bpp)

Images	기존의 방법		제안한 방법	
	L-JPEG (mod 6)	GAP	LJPEG-F-QT	GAP-F-QT
CT	3.419	3.336	2.991	2.917
MRI	3.396	3.324	3.229	2.996
US	3.442	3.259	2.971	2.842
Lena	4.564	4.401	4.666	4.496
Sailboat	5.500	5.251	5.478	5.413
Peppers	5.064	4.745	5.031	4.939
평 균	4.231	4.052	4.061	3.933

4.2. 안전성 분석

본 절에서는 3.3절에서 제시한 방법에 의해 안전성을 분석한다. <표 3>은 압축부분에 대한 수행시간을 각 루틴별로 측정하여 분석한 것으로 512×512 크기의 그레이 영상인 CT영상에 대해 적용하였다. 그러나 제안한 방법이 기존의 무손실 압축방법들에 비해 처리시간이 다소 늦어짐을 알 수 있다. 왜냐하면 제안한 방법이 F-변환, 비트평면 분해 후 쿼드트리 적용 등의 과정추가로 인한 오버헤드 시간이 부과되기 때문이며 압축성능과는 상반되는 결과를 보이고 있다. 그러나 암호 알고리즘과의 결합에 있어서 암호화되는 파일 크기를 감안하면 오히려 처리시간이 단축될 것으로 판단된다.

〈표 3〉 CT 영상에 대한 압축부분의 수행시간 비교(sec)

수행 시간	기존의 방법		제안한 방법	
	L JPEG (mode 6)	GAP	LJPEG-F-QT	GAP-F-QT
압 축	0.61	0.90	2.21	2.66
복 호	0.53	0.74	2.01	2.52

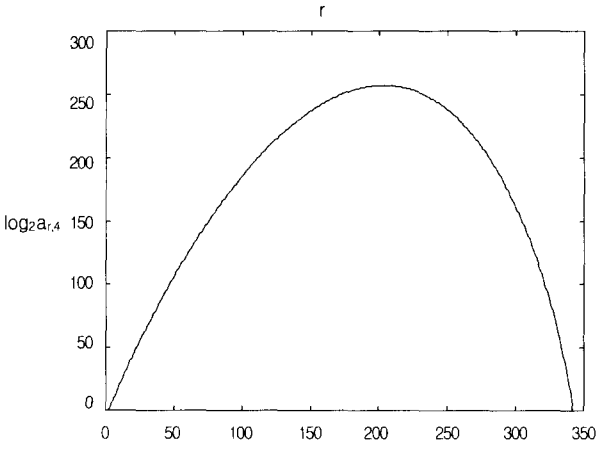
일반적으로 DES와 같은 암호알고리즘은 압축알고리즘에 비해 파일 크기에 따라 매우 큰 수행시간을 필요로 하게 된다. <표 4>는 동일한 암호알고리즘의 사용환경에서 암호알고리즘에 적용되는 파일 크기를 구한 것이다. 제시된 기존의 영상 압축알고리즘은 알고리즘 특성상 압축 데이터에서 영상의 윤곽 등의 정보를 갖는 일부분만을 추출하여 암호화에 적용하기가 어렵다. 이는 안전성의 측면도 함께 고려되어야 하기 때문이다. 그러나 제안한 방법에서는 분리된 각 비트 평면의 쿼드트리 구조 부분에 대해 암호화가 가능하다. 따라서 암호화에 필요한 파일 크기는 기존의 방법에 비해 약 20% 이하만 암호화하므로 암호화 시간이 약 80% 정도 빠른 처리가 가능하다는 것을 보여준다. 그리고 복원

〈표 4〉 암호화 되는 파일크기 비교(bits)

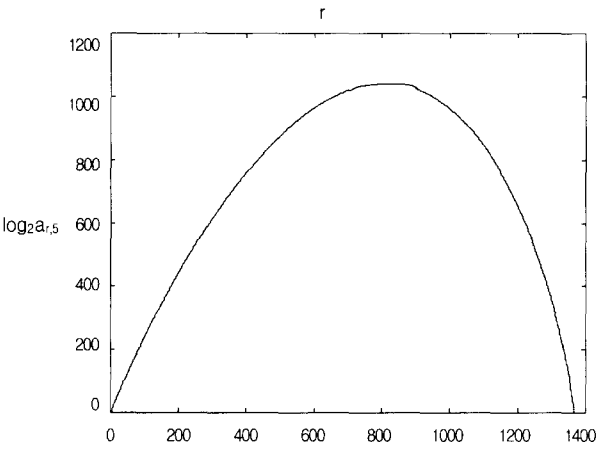
실험 기법 \ 실험영상		CT	MRI	US	Lena	Sailboat	Peppers
기존의 방 법	L-JPEG (mode 6)	896,168	890,312	902,424	1,196,544	1,398,536	1,327,488
	GAP	917,504	871,464	854,304	1,153,776	1,376,568	1,243,888
제안한 방 법	LJPEG -F-QT	149,192	161,232	146,932	230,752	271,672	254,128
	GAP -F-QT	148,860	153,264	144,428	224,936	269,480	250,648

에 있어서는 각 비트 평면들의 암호화 된 구조부분이 먼저 전송이 이루어 진 다음 쿼드트리 데이터 전송이 이루어져야 할 것이다.

제안한 구조의 안전성 분석은 우선, 쿼드트리 발생 개수에 의한 전수공격 방법의 형태로써 발생 가능한 쿼드트리를 모두 구하여 각 쿼드트리에서 분리된 구조부분으로 영상의 윤곽을 구성하고 암호화되지 않은 데이터 부분을 대입하여 복원을 시도하는 방법이다. 이런 경우 발생 가능한 쿼드트리 개수가 많으면 복원이 불가능하다. 따라서 식 (3)과 식 (4)에 의해 쿼드트리 개수 $a_{r,h}$를 구하여 이산대수 값으로 (그림 9)에 나타내었다. h는 쿼드트리 레벨 n-1인 깊이(depth)이고 r은 내부 노드 개수이다.



(a) Number of quadtree of Maximun depth 5



(b) Number of quadtree of Maximun depth 6

(그림 9) h 값에 따른 쿼드트리 발생 개수

(그림 9)를 분석해 보면 h가 4이고 r이 200인 경우 쿼드트리 발생 경우의 수는 약 2^{250}개 정도가 생성되고, h가 5이고 r이 800인 경우는 약 2^{1000}개정도 생성된다. 따라서 내부 노드수 r이 아주 작거나 크지 않다면 쿼드트리 구조를 모르고서는 완전한 영상복원이 불가능하다는 것을 알 수 있다. <표 5>는 실험 영상에 대해 제안한 방법을 적용할 경우 각 그레이 비트 평면에서 발생하는 내부 노드 개수를 구한 것이다.

〈표 5〉 분리된 그레이 비트 평면의 내부노드 개수

제안한 방법	실험영상	비트평면 I	비트평면 II	비트평면 III	비트평면 IV
LJPEG -F-QT	CT	47,364	47,598	28,856	2,248
	MRI	57,380	53,466	18,927	1,961
	US	45,227	45,073	31,174	3,156
	Lena	85351	82073	31699	3633
	Sailboat	80036	77891	58945	10567
	Peppers	86328	84892	45232	4767
GAP -F-QT	CT	48,113	47,731	27,096	2,157
	MRI	57,850	51,842	13,306	1,694
	US	45,128	45,163	28,322	2,559
	Lena	86,008	81,383	28,183	2,215
	Sailboat	86,423	83,882	58,998	8,746
	Peppers	86,681	84,799	44,496	2,859

<표 5>를 분석해 보면 h가 8인 경우 분리된 그레이 비트 평면에 대한 내부 노드수 r을 구한 것으로 쿼드트리가 발생되는 경우의 수는 무수히 많아 실제 영상들에 있어서 구조부분을 모르면 완전한 영상 복원이 불가능하다는 것을 의미한다.

암호화되지 않은 쿼드트리 데이터만을 가지고 영상복원을 시도하는 형태의 방법에서는 일반적인 무손실 쿼드트리 알고리즘의 수행 과정을 분석하여 데이터 부분이 어떤 구성순서와 비트 할당 등으로 되어 있는지를 파악하여 데이터 부분만으로는 영상복원이 어렵다는 것을 제시해야 한다. 일반적으로 쿼드트리 데이터는 완전한 쿼드트리 분해가 이루어 진 다음 리프 노드에 대응되는 동질영역의 화소값을 왼쪽에서 오른쪽으로 횡단하면서 순서대로 구성되어 진다. 이런 경우 공격자는 다음과 같은 정보를 획득할 수 있다. 첫째는 무손실 압축에서 각 쿼드트리 데이터값의 비트 수가 일정하게 고정되어 할당되므로 데이터 값들의 분리가 쉽게 이루어지고, 둘째는 형제 노드의 데이터값이 서로 인접해 있으며, 셋째는 데이터의 시작과 마지막 값은 항상 영상의 좌측 상단과 우측 하단에 위치하고 있다는 점이다. 공격자는 이런 정보를 가지고 영상의 일부분들에 대한 복원이 가능할 것이고 특히, 일반적인 정지 영상은 모서리 부분을 포함하는 배경 부분에서 동일한 모양을 가지는 경우가 많아 물체의 외각이 노출될 가능성이 많다.

따라서 (그림 6)에서 제시한 방법으로 쿼드트리 데이터를 재구성하면 물체의 외곽 부분이 노출되는 것을 방지할 수 있다. 이 방법은 일반적인 무손실 쿼드트리 알고리즘에서 노출되는 데이터부분 구성순서를 은닉한 것이다. 즉, 레벨별로 비월 주사 방식에 의해 데이터를 생성하고 결합하는

방법이므로 데이터들이 서로 치환되는 효과를 가진다. 이는 쿼드트리 데이터의 시작과 마지막 값의 위치를 알 수 없게 하며 형제노드의 데이터 값들도 서로 떨어져 분포하게 되어 영상의 일부분이 노출되어 있다고 하더라도 확장은 불가능하다.

5. 결 론

본 논문은 쿼드트리 알고리즘을 그레이 레벨 영상에 적용하여 무손실 압축성능을 개선하는 방법을 제시하였고, 암호화 강도를 유지하면서 암호화 시간을 줄여 실시간 처리가 가능한 방법에 대해 제안하였다. 무손실 압축성능 평가를 위해 모의 실험을 한 결과 무상관성과 동질영역을 확보하기 위한 변환 과정을 수행한 제안한 방법이 무손실 JPEG 표준안 보다 0.27bpp정도 개선됨을 확인할 수 있었고, 우수한 압축성능을 가지는 GAP 방법과 비교하여도 거의 유사하거나 우수한 압축율을 얻을 수 있었다. 특히 CT, MRI, US 영상은 다른 실험 영상들에 비해 동질영역을 많이 포함하고 있어 가장 우수한 압축성능을 얻었다. 또한 암호화 과정의 처리시간은 기존의 압축된 비트열 전체를 암호화하는 방법에 비해 약 80% 정도 단축될 수 있음을 확인하였다. 이는 압축과정에서 소요되는 지연시간을 고려하더라도 압축과 암호의 수행시간이 단축된다고 할 수 있다. 그리고 제안한 부분암호 구조의 안전성 평가를 위한 필요한 요소를 아울러 분석하였고, 암호 강도 측면에서는 쿼드트리 데이터가 치환의 효과를 갖도록 재구성하여 기존의 압축된 비트열 전체를 암호화하는 방법과 유사한 수준이 되도록 하였다.

향후 연구 과제는 일반적인 여러 영상 압축 알고리즘들을 분석하여 압축 성능이 개선되거나 영향을 미치지 않는 범위 내에서 압축 데이터의 일부분만 암호화하여도 전체를 암호화한 효과를 얻을 수 있는 방법들에 대한 연구가 계속 필요하며, 안전성을 확보하는 방법과 안전성 평가 방법에 대한 연구가 계속 진행되어야 할 것이다. 이는 안전한 실시간 영상통신 등에서 지연시간 감소에 큰 도움을 줄 것으로 예상된다.

참 고 문 헌

[1] "Data Encryption Standard(DES)," National Bureau of Standards FIPS Publication 46, 1977.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Comm. of the ACM, 21 pp.120-126, 1978.

[3] D. Jones, "Applications of Splay Trees to Data Compression," comm. ACM, pp.996-1007, Aug. 1988.

[4] X. Liu, P. G. Farrell, and C. A. Boyd, "Resisting the Bergen-Hogan Attack on Adaptive Arithematic Coding," Proc. 6th IBM Int., Conf., Cryptography Coding, pp.199-208, 1997.

[5] Y. Matias and A. Shamir, "A Video Scrambling Technique Based on Space Filling Curves," Proc., CRYPTO., pp.398-417, 1988.

[6] H. K. C. Chang and J. L. Liu, "A Linear Quadtree Compression Scheme for Image Encryption," Signal Proc. Image comm., Vol.10, No.4, pp.279-290, Sept. 1997.

[7] S. S. Maniccam, N. G. Bourbakis, "SCAN Based Lossless Image Compression and Encryption," IEEE Trans., Image Processing, Vol.3, No.5, pp.490-499, Sept. 1999.

[8] E. Shusterman and M. Feder, "Image Compression via Improved Quadtree Decomposition Algorithms," IEEE Trans., Image Proc., Vol.3, No.2, pp.207-215, Mar. 1994.

[9] C. E. Shannon, "Communication Theory of Secrecy System," Bell Syst. Tech. Journal, Vol.28, pp.656-715, Oct. 1949.

[10] M. E. Hellman, "An Extension of the Shannon Theory Approach to Cryptography," IEEE Trans., Info. Theory, IT-23, No.3, pp.289-294, May, 1977.

[11 Y. Wang, "A Set of Transformations for Lossless Image Compression," IEEE Trans. Image Processing, Vol.4, No.5, pp.677-679, May, 1995.

[12] ISO/IEC JTC 1/SC 29/WG 1(1994) "Call for Contributions-Lossless Compression of Continuous-Tone Still Picture," ISO Working Document ISO/ IEC/ JTC 1/SC29/ WG 1/N41.

[13] X. Wu, "Lossless Compression of Continuous-Tone Images via Context Selection, Quantization, and Modelling," IEEE Trans. Image Processing, Vol.6, pp.656-664, May, 1997.

[14] L. Shen and R.M.Rangayyan, "Improved Joint Bi-Level Image Experts Group Data Compression of Continuous-Tone Image," SPIE, Vol.2727, pp.54-65, Mar, 1996.

[15] H. Cheng and X. Li, "Partial Encryption of Compressed Images and Videos," IEEE Trans. Signal Processing, Vol. 48, No.8, pp.2439-2451, Aug., 2000.

[16] D. E. Knuth, 'The Art of Computer Programming : Fundamental Algorithms,' Vol.1, Addison-Wesley, 3rd Edition, 1997.

윤 정 오

e-mail : joyun@kyungwoon.ac.kr

1989년 경북대학교 전자공학과 졸업

1991년 경북대학교 전자공학과 석사

1998년 경북대학교 전자공학과 박사수료

1997년~현재 경운대학교 정보통신공학과 교수

관심분야 : 영상압축, 영상통신, 정보보호

성 우 석

e-mail : sosshy97@palgong.knu.ac.kr

2000년 경북대학교 전자공학과 졸업

2000년~현재 경북대학교 전자공학과 석사 과정

관심분야 : 영상처리, 암호통신, 통신시스템설계

황 찬 식

e-mail : cshwang@ee.knu.ac.kr

1977년 서강대학교 전자공학과 졸업

1978년 한국과학기술원 전기전자공학과 석사

1996년 한국과학기술원 전기전자공학과 박사

1991년~1992년 UTA 방문교수

1979년~현재 경북대학교 전기전자공학부 교수

관심분야 : 영상통신, 암호통신, 초고속망