논문 2004-41SP-4-2

카오스 시스템을 이용한 JPEG2000-기반 영상의 적응적 정보 은닉 기술

(An Adaptive Information Hiding Technique of JPEG2000-based Image using Chaotic System)

김 수 민*, 서 영 호**, 김 동 욱**

(Su-Min Kim, Young-Ho Seo, and Dong-Wook Kim)

요 약

본 논문에서는 JPEG2000 표준에서 주파수 변환기법으로 채택된 이산 웨이블릿 변환과 선형양자화 방법을 채택하여 영상 전체가 아닌 영상의 부분 데이터만을 암호화하여 암호화를 위한 계산양을 줄이는 방법을 제안하였다. 또한 계산양이 많은 암호화 알고리즘 대신 비교적 계산양이 적은 카오스 시스템을 이용함으로써 계산양을 더욱 감소시켰다. 이 방법은 영상의 압축비를 유지하기 위해서 양자화와 엔트로피 코딩 사이에서 암호화를 수행하며, 부대역의 선택과 카오스 시스템을 이용한 무작위 변환방법을 사용한다. 영상에 대한 실험방법은 우선 암호화할 부대역을 선택한 후 영상데이터를 일정한 블록으로 만든 후 랜덤하게 좌/우로 시프트 하는 방법과 두 가지 양자화 할당 방식(Top-down/Reflection code)을 사용하여 암호화한 데이터를 압축 시 데이터양의 변화를 최소화 하였다. 또한, JPEG2000의 점진적 전송(Progressive transmission)에 적합한 암호화 방법을 제안하였다. 제안한 방법을 소프트웨어로 구현하여 약 500개의 영상을 대상으로 실험한 결과 원 영상 데이터를 부분적으로 암호화함으로써 원 영상을 인식할 수 없을 정도의 암호화효과를 얻을 수 있음을 알 수 있었다. 따라서 제안한 방법은 작은 양의 암호화로 효과적으로 영상을 숨기는 방법임을 확인할 수 있었다. 본 논문에서는 여러 방식을 제안하였으며, 이들의 암호화 수행시간과 암호화효과 사이에 상보적인 관계가 있음을 보여, 적용분야에 따라 선택적으로 사용할 수 있음을 보였다. 또한 본 논문의 방식들은 응용계층에서 수행되는 것으로, 현재 유·무선 통합 네트워크의 중요한 문제로 대두되고 있는 끝과 끝(end-to-end)의 보안에 대한 좋은 해결방법으로 사용될 수 있으리라 기대된다.

Abstract

In this paper, we proposed the image hiding method which decreases calculation amount by encrypt partial data using discrete wavelet transform and linear scale quantization which were adopted as the main technique for frequency transform in JPEG2000 standard. Also we used the chaotic system which has smaller calculation amount than other encryption algorithms and then dramatically decreased calculation amount. This method operates encryption process between quantization and entropy coding for preserving compression ratio of images and uses the subband selection method and the random changing method using the chaotic system. For ciphering the quantization index we use a novel image encryption algorithm of cyclically shifted in the right or left direction and encrypts two quantization assignment method (Top-down/Reflection code), made change of data less. Also, suggested encryption method to JPEG2000 progressive transmission. The experiments have been performed with the proposed methods implemented in software for about 500 images. Consequently, we are sure that the proposed are efficient image encryption methods to acquire the high encryption effect with small amount of encryption. It has been shown that there exits a relation of trade-off between the execution time and the effect of the encryption. It means that the proposed methods can be selectively used according to the application areas. Also, because the proposed methods are performed in the application layer, they are expected to be a good solution for the end-to-end security problem, which is appearing as one of the important problems in the networks with both wired and wireless sections.

Keywords : Image Encryption, Chaotic System, JPEG2000, DWT

* 학생회원, ** 평생회원, 광운대학교 전자재료공학과
(Dept. of Electronic Materials Eng., Kwangwoon University)

※ 본 논문은 정보통신부 정보통신연구진흥원에서 지원하고 있는 정보통신기초연구지원사업의 연구결과임. (과제번호 : 03-기초-0025)

접수일자: 2004년1월5일, 수정완료일: 2004년5월3일

I. 서 론

멀티미디어 시대를 맞이하여 현대의 생활에서 정보의 비중이 기하급수적으로 증가하고 있으며, 특히 영상/비디오 컨텐츠에 대한 선호도는 그 속도가 더욱 증가되고

있다[1]. 이들 컨텐츠들을 대상으로 하는 사업모델들은 지적재산권이나 개인적인 정보를 담고 있는 것들이 대부분이어서 이들 컨텐츠들의 보안문제가 최근 크게 대두되고 있다[2]. 이 보안문제의 해결방안으로 최근 네트워크의 보안에 더하여 컨텐츠 자체를 암호화하는 방법이 널리 연구되고 있다[3]. 본 논문 또한 영상/비디오 컨텐츠의 암호화를 다룬다.

영상/비디오 컨텐츠들은 함축적인 정보를 내포할 수 있다는 장점 이면에 데이터양이 매우 많아 네트워크의 용량이 수용하기 힘들다는 단점을 갖고 있다. 따라서 최근 20여 년 동안 이들 컨텐츠의 데이터양을 줄이는 연구가 매우 활발하게 이루어져 JPEG, MPEG[2], JPEG2000[4], H.26X[5] 등의 국제표준들이 제정되어, 현재 널리 상용화되고 있다. 이들 압축기술들은 손실압축과 무손실압축을 병행하여 데이터양을 줄이고 있다. JPEG, MPEG, 그리고 H.26X 기술은 특정 크기의 화소블록(기본적으로 8×8)을 단위로 하는 DCT(Discrete Cosine Transform)를 사용하기 때문에 압축률이 증가할수록 이들 블록 경계에 화질의 열화가 심해지는 블록효과(Block effect)가 발생하는 단점을 갖고 있다. 이 단점을 보완하고 압축률 대비 화질이 우수한 DWT(Dis-crete Wavelet Transform)-기반 영상압축 방법이 개발되었으며, JPEG2000으로 표준화되면서 그 사용분야가 급격히 증가하고 있다. DWT-기반 압축기술은 영상 전체를 대상으로 변환을 수행하므로 주파수 대역에 따른 다해상도(multi-resolution) 특성 뿐 아니라 변환된 각 부대역이 원 영상의 위치정보를 그대로 갖고 있어 데이터 압축 이외의 연구 분야에 대해서도 DCT에 비해 많은 장점을 갖고 있다. 본 논문에서는 DWT-기반 영상압축, 특히 JPEG2000 기술에 의해 압축되는 영상/비디오 데이터를 대상으로 한다.

영상/비디오 컨텐츠에 대한 암호화는 암호화의 특성, 즉 암호화된 데이터의 한 비트라도 소실되면 복원된 데이터는 원 데이터와 완전히 다른 데이터가 된다는 특성 때문에, 압축이 수행되는 영상/비디오의 경우 압축과정 내부에 포함될 수밖에 없고, 압축과정 중 손실압축에 의해 암호화된 데이터가 소실되지 않도록 하여야 한다. 따라서 암호화과정은 압축과정과 밀접한 관계를 가지며, 데이터 변환방법 및 내부 압축기술 등에 따라 암호화 방법 및 대상 데이터가 달라진다. 영상/비디오 암호화 연구는 암호화할 대상을 최소화하고 암호화효과를 최대화하는 방향에 초점을 맞추고 있는데, 그 이유는 암호화 자체가 많은 연산을 수행하여야 하므로 암호화에 소요되는 시간과 비용을 최소화하여야 하기 때문이다. [6]에서는 원 영상을 압축 없이 암호화하는 방법을 제안하였는데, 이 방법은 영상의 특정 비트평면을 암호화하여 영상 데이터를 숨기는 방법이다. 원 영상의 각 화소가 8비트로 표현되고 한 개의 비트평면만을 암호화한다고 해도 이 방법은 1/8에 해당하는 데이터를 암호화하여야 하므로 암호화에 의한 시간과 비용이 과다하다.

영상/비디오 데이터에 대한 암호화 기술은 선행 개발·발전된 DCT-기반 압축기술들을 대상으로 먼저 연구되었으며, DWT-기반 기술에 대해서는 상대적으로 늦은 1990년대 중반부터 연구가 시작되었다. 이 기술에 대한 연구는 아직 초기단계에 있다고 볼 수 있으며, 대부분 암호화의 특성 때문에 양자화 과정을 끝낸 데이터를 암호화하는 방법을 취하고 있다[7][8]. 이들은 특정 양자화 방법을 겨냥하고 있는데, [7]에서는 quadtree-기반의 SPHIT[9]를 겨냥하여 두 번의 iteration 결과 데이터를 암호화는 방법을 제안하였으며, [8]에서는 EZW 방법[10]에 대해 ATM 패킷 단위로 암호화를 적용하는 방법을 제안하였다. 암호화에 소요되는 시간과 경비를 줄이는 또 하나의 방법으로 기존의 암호화 알고리즘 대신 계산양이 적은 특정 방법을 사용하는 연구 또한 진행되고 있다. [11]에서는 베이커 맵(Baker map)을 이용한 위치교환 방식으로 암호화 방법을, [12]에서는 베이커 맵을 이용한 위치교환 방법에 암호화키를 이용한 암호화 방법을 각각 제안하였는데, 이 방법들은 암호화 전과 후의 데이터의 분포의 변화가 많아서 암호화 후 엔트로피 코딩 시 압축률 손실이 매우 크다. [13]에서는 카오스 맵(Chaos map)을 이용한 위치 교환 방식을 이용한 암호화를 수행하였고, [14]에서는 RNS(Residue Number System)을 발생시켜 암호화하는 방법을 제안하였으며, [15][16]에서는 스캔 패턴을 조절하여 암호화하는 방법을 제안하였으나, 암호화 정도에 따라 압축률 손실이 과다하여 압축과정에서 사용하기에는 적합하지 않다.

본 논문에서는 암호화하는 양을 줄여 암호화에 소요되는 비용과 시간을 줄이기 위해 기존의 암호화 알고리즘 대신 카오스 시스템을 이용한 영상 컨텐츠 암호화 방법을 제안한다. 본 논문에서 대상으로 하는 영상압축 기술은 정규적인 리프팅(lifting) 방법과 선형양자화기를 사용하는 JPEG2000의 표준 압축기술이다. 리프팅을 통해 원 영상을 각 주파수대역으로 재편성(decomposition)하고 재구성된 영상을 [17]에서 제시되었던 방법으로 일정 부대역을 선택하여 암호화를 수행한다. LL4 영역에서는 좌/우 쉬프트 방법에 의해 암호화를 수행하고 다

른 부대역에서는 Top-down/Reflection code 방법으로 나누어서 영상에 대한 암호화를 수행한다. 이 암호화 방식의 목적은 최소의 암호화양으로 최대의 암호화 효과와 암호화 결과 압축률의 변화를 줄이는 것이며, 암호화를 수행하여 암호화 된 영상에 대한 전체 영상에 대한 암호화비율과 암호화효과에 있어서 상보적인 관계를 밝히는 것 또한 본 논문의 목적 중 하나이다. 또한, 영상 데이터를 화소 단위로 암호화하지 않고 영상을 비트평면(Bit-plain)단위로 암호화하여 JPEG2000 표준 방법에서 사용되는 점진적 전송(Progressive transmission)에서의 암호화된 데이터 복원 시 나타나는 문제점과 ROI (Regions of Interest) 영역에서의 암호화하기 위한 방법을 제시한다.

본 논문의 다음 장에서는 웨이블릿을 이용한 JPEG2000에서의 영상 압축/복원과 암호화 시 부대역의 선택에 관해 설명하고, Ⅲ장에서는 본 논문에서 영상을 암호화시 사용되는 카오스 시스템, 암호화 알고리즘, 전체적인 암호화 및 복호화 과정에 대해 설명한다. Ⅳ장에서는 제안한 방법에 대한 실험 및 그 결과를 보이고, 마지막으로 Ⅴ장에서는 본 논문의 결론을 맺는다.

Ⅱ. JPEG2000에서의 영상 압축/복원과 부대역의 선택

본 장에서는 본 논문에서 사용될 리프팅 변환을 이용한 JPEG2000 영상 압축/복원 방법과 리프팅 변환된 영상 데이터 중 암호화할 대상 부대역을 선택하는 것에 대해 설명한다.

1. 웨이블릿 변환을 이용한 JPEG2000에서의 영상 압축/복원

본 논문에서 대상으로 하는 영상압축 방법은 JPEG2000에서 표준으로 채택된 웨이블릿 변환방법 중 리프팅을 사용하였다. 그림 1에서는 리프팅을 이용한 영상의 압축 및 복원과정을 간단히 나타내었다. JPEG2000은 JPEG과 달리 원 영상의 타이링(Tiling) 크기를 조절할 수 있다. JPEG은 원 영상을 8×8 화소 단위로 DCT를 수행하기 때문에 높은 압축비율에서는 정사각형 모양의 블록효과가 발생한다. JPEG2000에서는 영상의 타이링하는 크기를 임의로 조절하여 영상의 화질을 향상하거나 메모리의 사용을 줄여줄 수 있는 장점이 있다. 즉, 타이링의 크기를 작게 할수록 압축을 수행하는 하드웨어의 메모리 사용을 감소시켜주는 장점이 있으나 영상의 화질을 떨어뜨린다. 본 논문에서는 타이링을 수행하지 않고 압축을 실행하여 영상의 화질을 최상으로 하였다.

JPEG에서 사용하는 DCT는 영상을 주파수의 특성대로 변환하지만 JPEG2000에서 사용하는 리프팅은 영상을 크기(Scale) 또는 해상도(Resolution)로 분해하기 때문에 상세한 정보를 가지면서도 낮은 해상도의 영상으로 분해할 수 있다. 여기서 JPEG2000은 손실압축과 무손실 압축을 위해 각각 9/7-필터와 5/3-필터 두 종류의 필터를 사용하는데, 리프팅 수행 시 저주파-필터(Low-pass filter)를 통과한 영상은 낮은 해상도의 영상을 가지게 되고, 고주파-필터(High-pass filter)를 통과한 영상은 나머지의 상세정보를 가짐으로써 이 두 정보를 종합하여 원 영상으로 완벽하게 복원하게 된다.이렇게 리프팅된 영상정보들을 양자화(Quantization)하는데, JPEG2000은 스칼라 양자화(Scalar quantization)방법을 사용한다. 여기서는 양자화 스탭 크기(Quantization step size)라는 특정한 상수로($\triangle_b$) 리프팅된 계수값들을 나누는데 이 값은 각 부대역의 특성에 따라 달리 적용됨으로써 최적의 압축된 영상을 구현할 수 있다.

부대역별로 양자화한 계수값은 ROI(Region of Interest) 과정을 통해 중요한 영상 부분을 화소의 비트만큼 쉬프트(Max-shift)한다. 그 결과 전체 영상은 화소당 비트수가 2배로 증가한다. 데이터를 코드블록단위로 나누어서 EBCOT(Embedded Block Coding with Optimal Truncation)의 Tier 1을 수행하여 코드블록의 각 비트평면 데이터에 대한 컨텍스트(Context)값과 결정(Decision)값을 추출한다. 그 값을 패스별로 묶고 이진 산술부호화(Arithmetic binary coding)로 무손실 압축을 하여 Tier 2에서는 압축된 데이터를 JPEG2000 표준에 맞추어서 전송 및 저장하게 된다.

영상이 2차원 데이터이기 때문에 리프팅 또한 2차원으로 수행되는데, 가장 대표적인 수행방식이 Mallattree 형식[3]이다. 리프팅에 의해서 원 영상은 주파수 대역에 따라 3n+1(n : 리프팅 레벨 수)개의 부대역으로 재편성되며, 레벨수가 증가할수록 주파수대역이 낮아진다. 그림 2에서 L은 저주파대역 통과, H는 고주파대역 통과를 각각 의미하며, XYj(X와 Y는 H 또는 L) 부대역은 j번째 레벨에서 수평방향으로 X주파대역을 통과하고 수직방향으로 Y주파수대역을 통과한 부대역을 의미한다. 그림 2에서 볼 수 있듯이, 모든 부대역은 전체영상에 대한 특정 주파수 대역의 정보를 가지게 된다. 이 중 가장 저주파 성분에 해당하는(그림 2의 경우 LL4) 부대역이

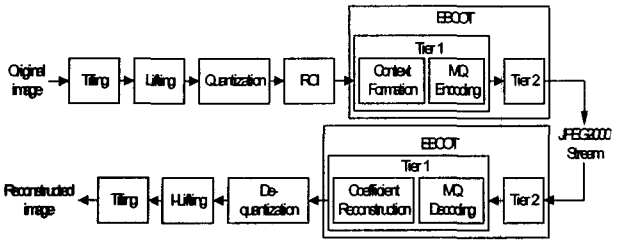


그림 1. JPEG2000 기반의 영상압축/복원 과정
Fig. 1. Image compression/Reconstruction procedure ba-sed on JPEG2000.

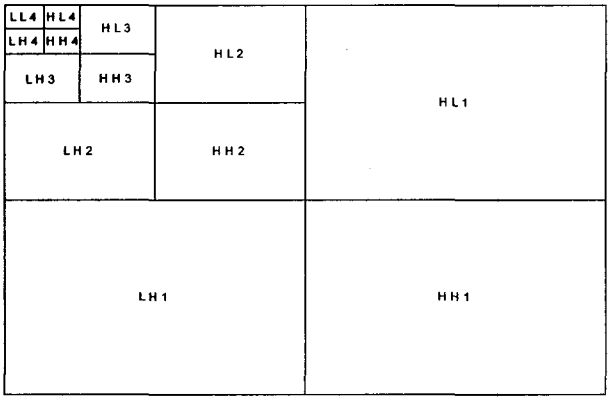


그림 2. 리프팅 결과 재편성된 부대역
Fig. 2. Decomposed subbands resulting from lifting.

인간의 눈에 가장 민감한 성분이며, 영상에 대한 가장 함축적인 정보를 포함한다.

2. 부대역의 선택

앞에서 설명한 바와 같이 리프팅 결과의 각 부대역은 서로 다른 주파수 성분을 가지면서 전체 영상에 대한 정보를 포함하고 있다. 따라서 각 부대역은 복원 시 전체영상에 영향을 준다. 영상정보를 숨기는 작업은 영상정보가 전송되는 동안 허락되지 않은 사람이 영상정보를 포획하여 그 영상의 내용을 파악하거나 그 영상을 다시 사용하지 못하게 하는 것이 그 목적이다. 따라서 암호화 결과 영상을 인식하지 못하거나 영상을 다시 사용하지 못할 정도로 영상이 왜곡된다면 반드시 전체영상을 암호화할 필요는 없다. 더구나 암호화 알고리즘을 사용할 경우는 암호화를 위한 처리시간 때문에 전체 영상처리시간에 큰 영향을 줄 수 있으며, 특히 무선통신의 경우 암호화 및 복호화 과정으로 인한 지연시간(Laten-cy time)과 전력소모는 큰 장애요소가 되고 있다[18],[19]. 따라서 가능하면 암호화 양을 최소로 하는 것이 바람직하다. 본 논문에서는 4-레벨 DWT를 수행하는 것으로 가정하고 [17]에서 제시되었던 4가지 방법으로 부대역을 선택하여 암호화할 데이터양을 줄였다.

① LL4 : LL4만 암호화
② LL4-HH4 : LL4와 HH4 만 암호화
③ Level4 : 레벨-4의 모든 부대역 암호화
④ Level4-HH3 : 레벨-4의 모든 부대역과 HH3 암호화

첫 번째 LL4만을 암호화한 결과 영상은 다른 목적으로 사용할 수 없을 정도로 영상이 왜곡되나, 원 영상의 고주파 성분이 상당부분 남아있다. 이 고주파성분의 잔존은 대부분의 응용분야에서는 수용 가능하지만 특정 응용분야(예를 들어 군사적인 목적 등)에서는 수용할 수 없는 경우가 있다. 따라서 이 고주파 성분을 더욱 왜곡시키기 위해서는 LL4뿐 아니라 고주파 부대역에 대한 암호화를 수행하여야 한다. 그러나 암호화 양의 증가를 고려할 때 가장 적절한 첫 번째 선택은 HH4이다. LL4와 LL4-HH4 암호화 영상을 비교하면 PSNR(Peak Signal to Noise Ratio)은 큰 차이를 보이지 않지만 가시적인 암호화 효과는 후자가 훨씬 높음을 알 수 있다. 영상의 암호화를 다루는데 있어서 암호화 결과와 효율성이 PSNR에 절대적으로 비례한다고는 볼 수 없고 시각적이고 주관적인 인지가 많은 부분을 차지한다. 즉, LL4-HH4 암호화 결과는 원 영상을 거의 인식할 수 없을 정도의 충분한 효과를 얻을 수 있다. 세 번째 방법인 레벨-4의 네 부대역을 모두 암호화 대상에 포함시키는 경우(Level4) 두 번째 방법보다 더 고주파 성분을 정밀하게 왜곡시킨다. 영상에 따라 다소의 차이가 있으나, 레벨-4의 네 부대역을 모두 포함하는 세 번째 경우가 일반적으로는 두 번째 경우에 비해 더욱 암호화 효과가 두드러지는 것을 실험적으로 확인할 수 있다. 더욱더 영상을 왜곡시킬 필요가 있는 경우는 네 번째 방법인 레벨-4의 모든 부대역과 HH3 (Level4-HH3)을 암호화할 수 있다. 많은 부대역을 포함할수록 암호화 효과는 증가하겠으나, 상대적으로 암호화에 소요되는 시간과 비용은 증가한다.

Ⅲ. 카오스 시스템과 제안된 영상 암호화 알고리즘

본 장에서는 본 논문에서 사용되는 카오스 시스템과 이를 이용하여 본 논문에서 제안하는 영상 암호화 알고리즘에 대해서 설명한다.

1. 카오스 시스템

카오스 이론은 결정론적 비선형 동역학 시스템에서

나타나는 불규칙하고 예측 불가능한 양상을 정성적으로 연구하는 학문이다. 카오스란 말은 원래 무질서 또는 복잡함을 뜻하는 고대 그리스어로부터 유래 하였지만, 공학에서는 결정론적 비선형 동역학 시스템으로부터 생성되는 복잡하고 잡음과 유사한 신호의 현상을 말하고 있다.

카오스 알고리즘이 가지는 두 가지 특징은 위상공간상에 유한한 영역 내에서 주기성 없이 그려지는 이상한 끌개(Strange attractor)와 초기조건의 민감성(Sensiti -vity to initial condition)을 들 수 있다. 이상한 끌개는 이상한 끌개 위의 두 개의 초기점이 아무리 가깝다 하더라도 이들로부터 진화하는 궤도는 곧 기하급수적으로 멀어지며 판이하게 다른 진화 양상을 보여준다는 의미이다. 이러한 성질을 만족하기 위해서는 이상한 끌개의 기하학적 구조가 프랙털(Fractal) 구조를 가져야 한다. 프랙털 구조의 차원은 정수가 아니라는 특성 때문에 이상한 끌개라고 불린다. 초기 조건에 민감하다는 특성은 혼돈 끌개(Chaotic attractor) 안의 임의의 작은 영역을 고려할 때 이 영역 안의 모든 점들이 진화하는 과정을 살펴보면 알 수 있는데 처음에는 늘이고(Stretching) 다음에는 접는(Folding) 두 과정이 있으며, 혼돈 끌개 안에서는 이러한 늘임과 접힘의 과정이 무한히 반복된다. 카오스의 기하학적 성질의 결과는 가까이에 있던 두 점에서 출발하는 궤도가 처음에는 기하급수적으로 멀어지지만 접힘으로 인하여 혼돈 끌개라는 제한된 공간에 남아 있게 된다. 궤도가 혼돈 끌개라는 제한된 영역 안에 영원히 놓여 있기 위해서는 혼돈 끌개 안에서의 궤도운동은 근본적으로 회귀적(Recurrent)이어야 하고 끌개의 어느 한 점에서 출발하는 궤도는 어느 정도 불규칙한 시간이 지나면 다시 출발점 근처로 되돌아와야 한다. 따라서 카오스 시스템은 무한히 반복되는 접힘에 의해 언젠가 다시 처음에 있던 위치 근처로 되돌아오는 회귀적 성질을 갖는다[20].

본 논문에서 암호화에 사용되는 카오스 사상은 로지스틱 사상(Logistic map)이라는 식(1)에 나타낸 카오스 함수이다.

$$x(n+1) = rx(n)(1 - x(n)) \quad (1)$$

식(1)에서 $x(0)$는 초기값, r은 파라메타값을 각각 나타낸다. 그림 3을 식(1)을 초기조건 $x(0)$와 r값에 따라 반복시켰을 경우 각 초기값에 대한 수렴값을 그

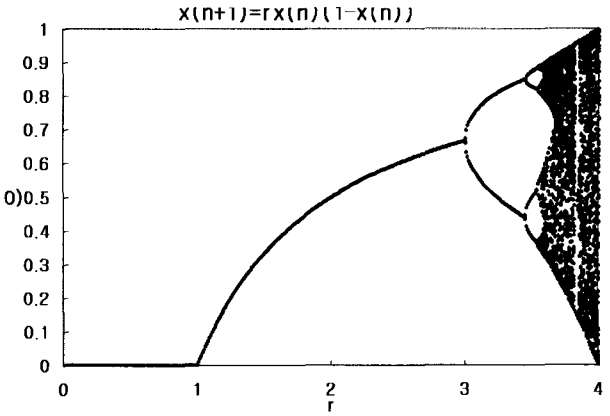


그림 3. $f(x) = rx(1-x)$함수의 분기 도형
Fig. 3. Bifurcation diagram of $f(x) = rx(1-x)$.

래프로 표시한 것이다. 그래프에서 r값이 1에서 하나의 수렴값을 가지다가 분기가 일어나면서 3.5이상의 어느 영역에서 이러한 수렴값을 알아볼 수 없는 카오스 영역이 됨을 알 수 있다. 수렴값을 알 수 없기 때문에 이 영역에서 식 (1)을 반복시키면 예측할 수 없는 카오스 값을 얻을 수 있다. 그림 4에서는 r값이 카오스 영역인 값인 3.99일 경우 $x(0)$값이 0.3 0.3000001값으로 변할 때 초기조건의 민감성을 나타내었다. 그림 4의 (a)는 1~24번, (b)는 25~100번 반복한 값을 산점도(Scatter plot)로 나타내었다. 24번 반복까지는 거의 같은 값을 나타내다가 그 후에는 전혀 다른 급격한 차이를 보이고 있다.

2. 제안된 암호화 알고리즘

본 논문에서 제시한 암호화 알고리즘은 선택된 부대역 중 LL4 영역에는 좌/우 쉬프트 방법으로 암호화를 적용시키고 다른 부대역에서는 카오스 값을 발생시켜 선형양자화 과정과 함께 암호화에 적용된다.

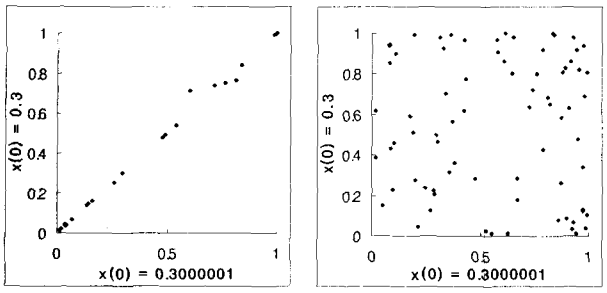
(1) LL4 영역에서의 암호화 방법

본 논문에서 제시하는 LL4 부대역에 대한 암호화 알고리즘을 그림 5에 나타내었다.

먼저, 식 (1)에서 생성된 카오스값 $x(n)$을 식 (2)에 의해서 2z개의 $b(k), (0 \leq k \leq 2z-1)$ 값으로 나타낸다.

$$x(n) = 0.b(0)b(1)\cdots b(2z-2)b(2z-1) \quad (2)$$

여기서 z는 임의의 자연수이며, x(n)의 소숫점 아래 2z자리까지 사용함을 의미한다. 이 b(k) 값들을 사용하여 웨이블릿 계수 Wj에 대해 pj(암호화 방향을 나타내는



(a) (b)

그림 4. 초기조건의 민감성에 대한 산점도;
(a) 1～24 사이클, (b) 25～100 사이클

Fig. 4. Scatter plot about sensitivity to initial condition;
(a) 1～24 cycles, (b) 25～100 cycles.

파라메터)와 qj(암호화 양을 나타내는 파라메터)를 식 (3)과 (4)로 계산한다.

$$p_j = b(2j) \tag{3}$$

$$q_j = (\alpha + \beta \cdot b(2j+1)) \bmod t \tag{4}$$

여기서 α, β 그리고 식 (1)의 초기값인 x(0)는 이 암호화시스템의 비밀키로 사용된다. 또한 g mod h는 g에 대한 modulo-h 연산을 뜻하며, t는 웨이블릿 계수의 비트 수를 나타낸다. 이 값들에 의한 Wj의 암호화는,

$$W'_j = \begin{cases} W_j << q_j, & p_j = 0 \\ W_j >> q_j, & p_j = 1 \end{cases} \tag{5}$$

로 수행된다. 여기서 W'j는 암호화된 Wj를 나타내며, <<와 >>는 왼쪽-쉬프트-회전(shift-left and rotation)과 오른쪽-쉬프트-회전(shift-right and rotation)을 각각 나타낸다. 즉, 본 논문에서 제시하는 LL4 부대역의 암호화 방법은 식 (1)로 생성되는 카오스 값에서 식 (2)와 같이 소수점 아래 2z개 비트 중 2개(b(2j)와 b(2j+1))를 사용하여 쉬프트-회전의 방향(pj)과 그 양(qj)을 결정하고 이에 따라 웨이블릿 계수(Wj)의 쉬프트-회전을 수행하는 것이다.

식 (2)에 나타낸 것과 같이 한 개의 카오스 값으로부터 2z개의 이진수를 얻으므로 한 개의 카오스 값은 z개의 웨이블릿 계수를 암호화하는데 사용된다. 따라서 카오스 값은 z개의 웨이블릿 계수마다 한 개씩 생성하면 된다. 또한 암호화 방법으로 쉬프트 동작을 사용함으로써 암호화에 필요한 계산양이 매우 적어 고속동작이 용이하다. 이 암호화 방식에서 α와 β, x(0), 그리고 r을 암호화 키로 사용하는데, 카오스 시스템의 특성상 이 값들을 모르면 pj값과 qj값을 유추하기가 매우 어렵다. 따라서 이 암호화 시스템은 충분한 보안성을 유지할 수 있다고 볼 수 있다[21].

(2) 양자화 계수 할당방법을 이용한 타 부대역의 암호화 방법

LL4 이 외 부대역의 웨이블릿 계수는 일반적으로 양자화에 의해 일부 데이터가 소실된다. 암호화의 특성상 이런 데이터의 소실은 영상의 복원과정에서 수행되는 복호화에 의해 원 데이터를 그대로 복원할 수 없다. 따라서 본 논문에서는 각 부대역에 대해 양자화가 진행된 결과, 즉 양자화 인덱스(Quantization Index, QX)를 암호화 대상 데이터로 하며, 암호화 또한 양자화 방법을 고려하여 수행한다.

일반적으로 암호화는 특정 단위의 데이터를 무작위로 썩는 효과를 발휘한다. 이 단위는 암호화 기술에 따라 다르며, 블록 암호화의 경우 일정양의 데이터를 단위로 하고 스트림 암호화는 소량의 데이터(1 비트에서 수 byte 정도)를 단위로 한다. 일반적으로 이 단위가 클수록 계산량이 많으며, 반면 암호화 알고리즘의 복잡성은 증가한다. 이 무작위성은 사용되는 암호화키에 의해서 결정되며, 이 키가 공개되지 않으면 암호화된 데이터를 복호화하는데 많은 시간과 비용이 소요된다는 것에 그 보안성의 근거를 두고 있다. 본 논문에서는 각 QX를 암호화 단위로 하여 스트림 암호화의 가능성을 부과하며, 앞 절에서와 같이 x(0), α, β, 그리고 r을 암호화키로 사용한다.

본 논문에서 사용하는 암호화 방법은 대상 QX 값을 다른 QX로 치환하는 것이다. 복호화시 치환된 것을 원 QX로 재치환할 수 있기 위해서는 치환패턴이 예측 가능하여야 한다. 이 방법을 사용하는 또 하나의 고려사항은 양자화 과정 다음의 엔트로피 코딩(entropy coding) 과정이다. 일반적으로 엔트로피 코딩은 높은 빈도수의 QX일수록 짧은 코드를, 낮은 빈도수의 QX일수록 긴 코드를 부여함으로써 데이터의 소실 없이 추가적인 압축을 꾀하는 것이다. 만약 양자화 과정 다음의 암호화 과정에 의해 QX의 분포를 과다하게 흩뜨려 압축률을 크게 손상한다면 좋은 암호화 방법이 될 수 없다. 따라서 본 논문에서는 이 점을 고려하여 양자화 과정과 함께 암호화 방법을 제안한다.

앞에서 언급한 바와 같이 본 논문에서는 JPEG2000 등에서 표준으로 채택하고 있는 선형 고정 양자화기를 고려하며, 그림 6에 한 예를 보이고 있다. 이 예는 특정 부대역의 웨이블릿 계수를 $\triangle_b$로 나눈 결과 3 비트만

```
procedure{ChaoticEncryption_LL4}
Size of LL4 subband = M XN;
Select parameter r;
Select a, β, x(0) as secret keys;.
c = 0, n = 0;
x(n) = x(n+1) by eq. (1);
for (i is 0 to M - 1){
    for (j is 0 to N - 1){
        pj = b(2c);
        qj = ( a+β×b(2c+1)) mod t;
        if (pj == 0) then
            f(i,j) = f(i,j)<<< qj;
        else
            f(i,j) = f(i,j)>>> qj;
        if ((c mod z)==0), then
            x(n) = x(n+1) by eq. (1);
            n = n + 1;
        c = c + 1; } }
```

그림 5. LL4 부대역의 암호화 방법
Fig. 5. Encryption method for LL4 subband.

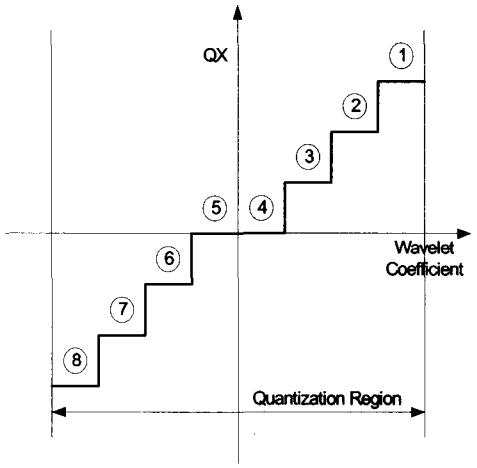
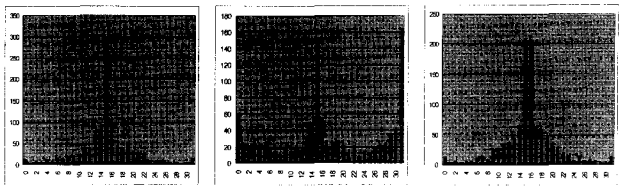


그림 6. 양자화기의 예
Fig. 6. Example of a quantizer.

남은 것을 보이고 있다. 본 논문에서 택한 치환방법은 대칭적 치환이다. 즉, 영역 ①의 QX를 암호화하기 위해서는 이 QX값을 영역 ⑧의 QX로 치환하고, 영역 ②는 영역 ⑦의 QX로, 영역 ③은 영역 ⑥, 영역 ④는 ⑤로 각각 치환한다. 일반적으로 그림 6의 각 영역에 QX를 할당하는 방법은 ①부터 ⑧까지 3-비트 이진수를 차례로 할당하는 것이다. 여기서 이 방법은 Top-down방식이라 부르기로 한다. 또 다른 QX할당방법은 ①부터 ⑧까지 3-비트 Reflection-code를 할당하는 방법이다. 이



(a) (b) (c)

그림 7. 암호화에 의한 양자화 계수분포의 변화; (a) 암호화 전, (b) Top-down방식에 의한 암호화 후, (c) Reflection-code방식에 의한 암호화 후
Fig. 7. Change in QX distribution by encryption; (a) beforeen cryption, (b) after encryption with top-down scheme, (c) after encryption with Reflection-code scheme.

방법을 Reflection-code방식이라 한다.

일반적으로 LL4를 제외한 부대역들에서의 웨이블릿 계수 분포는 Gaussian분포를 보이며, 양자화 후에도 불연속성을 가질 뿐 이 분포특성에는 변함이 없다. 앞에서 언급한 치환에 의한 암호화를 가정할 때 Top-down방식에 의한 QX할당방법은 Reflection-code방식에 비해 Gaussian 분포를 상대적으로 많이 변화시킨다. 그림 7에 한 예를 나타내었는데, (a)의 양자화된 QX들을 Top-down방식(b)과 Reflection-code방식(c)으로 암호화를 했을 때 분포의 변화를 보이고 있다. (b)는 상당한 무작위성 치환의 결과를 보이는 반면, (c)는 Gaussian 분포를 흩트리지 않고 그 빈도수만 조절된 것을 볼 수 있다. 그러나 뒤에서 기술하겠지만, 두 방법은 암호화 효과면에서 약간의 차이를 보이므로 본 논문에서는 두 방식 모두를 같이 기술하여 비교할 수 있도록 한다.

결론적으로 본 논문의 LL4를 제외한 부대역의 암호화 방식은 다음과 같다. 특정 부대역의 QX에 대해 식 (1)의 카오스 값으로 식 (2)에서 구한 해당 $b(k)$값이 1일 때는 암호화를 수행하고 $b(k)$값이 0일 때는 암호화하지 않는다. 이 때 QX의 할당방식은 Top-down방식과 Reflection-code방식 모두를 고려한다. 이 암호화 방식을 그림 8에 나타내었다. 식 (2)에서 구한 $b(k)$값이 1과 0이 될 확률이 약 1/2 이므로 선택된 부대역에서 암호화 하는 비율은 약 1/2이 된다. 이 암호화 방법을 적용한 결과 Top-down방식은 4.23%, Reflection-code방식은 1.17%의 평균 압축률이 감소하였으며, 이로써 Reflection-code방식이 압축률 측면에서는 우수한 성능을 보임을 알 수 있다.

일반적으로 LL4를 제외한 부대역들에서의 웨이블릿 계수 분포는 Gaussian분포를 보이며, 양자화 후에도 불연속성을 가질 뿐 이 분포특성에는 변함이 없다. 앞에서

```
M=MSB(msb value is the selected subband)
chaotic_Encrypt(){
    switch (mode) {
        case Top_down        : Topdown(); //Fig. 7 (b)
        case Reflection code : Reflect();   //Fig. 7 (c)
    } }
Topdown(){
for (i is 0 to x){
    for (j is 0 to y){
        if( b(k) == 1 ){
            if ( f(i,j) ≧ M ) then
                f'(i,j) = f(i,j) - M;
            else f'(i,j) = f(i,j) + M; }
        else f'(i,j) = f(i,j);
        k = k + 1; } } }
Reflect(){
for (i is 0 to x){
    for (j is 0 to y){
        if( b(k) == 1 ) then f'(i,j) = f(i,j)1's complement;
        else                f'(i,j) = f(i,j);
        k = k + 1; } } }
```

그림 8. LL4 이 외의 부대역에 대한 암호화 방법
Fig. 8. Encryption method for the subbands except LL4.

언급한 치환에 의한 암호화를 가정할 때 Top-down방식에 의한 QX할당방법은 Reflection-code방식에 비해 Gaussian 분포를 상대적으로 많이 변화시킨다. 그림 7에 한 예를 나타내었는데, (a)의 양자화된 QX들을 Top-down방식(b)과 Reflection-code방식(c)으로 암호화를 했을 때 분포의 변화를 보이고 있다. (b)는 상당한 무작위성 치환의 결과를 보이는 반면, (c)는 Gaussian 분포를 흩트리지 않고 그 빈도수만 조절된 것을 볼 수 있다. 그러나 뒤에서 기술하겠지만, 두 방법은 암호화 효과면에서 약간의 차이를 보이므로 본 논문에서는 두 방식 모두를 같이 기술하여 비교할 수 있도록 한다.

결론적으로 본 논문의 LL4를 제외한 부대역의 암호화 방식은 다음과 같다. 특정 부대역의 QX에 대해 식 (1)의 카오스 값으로 식 (2)에서 구한 해당 $b(k)$값이 1일 때는 암호화를 수행하고 $b(k)$값이 0일 때는 암호화하지 않는다. 이 때 QX의 할당방식은 Top-down방식과 Reflection-code방식 모두를 고려한다. 이 암호화 방식을 그림 8에 나타내었다. 식 (2)에서 구한 $b(k)$값이 1과 0이 될 확률이 약 1/2 이므로 선택된 부대역에서 암호화 하는 비율은 약 1/2이 된다. 이 암호화 방법을 적용한 결과 Top-down방식은 4.23%, Reflection-code방식은 1.17%의 평균 압축률이 감소하였으며, 이로써

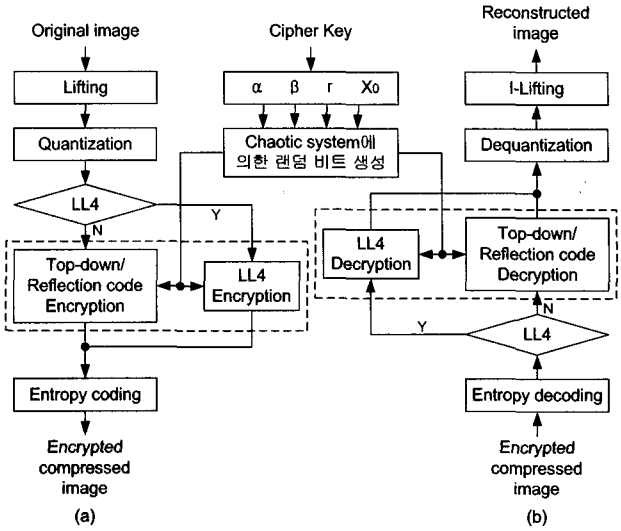


그림 9. 영상 암호화/복호화 과정; (a) 암호화, (b) 복호화
Fig. 9. Image encryption/decryption procedure; a) encryp -tion, (b) decryption.

Reflection-code방식이 압축률 측면에서는 우수한 성능을 보임을 알 수 있다.

3. 영상 암호화 및 복호화

그림 9에서 LL4 및 그 외의 부대역에 대한 암호화 및 복호화 과정을 흐름도로 나타내었다. 원 영상을 리프팅 수행 후 양자화하여 각 부대역별로 QX 값을 구한다. 먼저 암호화를 수행하기 위해서는 사용자가 2장에서 논의된 것 같이 4가지 방법에 의해 암호화할 부대역을 선택한다. 그리고 부대역 LL4영역과 다른 부대역을 구별해서 암호화를 수행하게 되는데 LL4(즉, 저주파 성분이 모여 있는 영상)는 좌/우로 쉬프트하고, 다른 부대역에서는 치환방법(Top-down방식 또는 Reflection-code방식)에 의해 암호화가 각각 수행된다. 암호화된 데이터는 EBCOT를 거쳐 암호화된 영상 압축 데이터의 형태로 전송된다. 복호화 과정은 암호화과정의 역순으로 진행된다. 그림 9에서 점선으로 표시된 블록이 암호화/복호화를 수행하는 부분이다. 일반적인 암호화 알고리즘이 그렇듯이 본 논문에서도 암호화/복호화를 위한 암호화키는 통신대상 양측에서 이미 보유하고 있다고 가정한다.

4. 점진적 전송에 따른 영상 암호화

JPEG2000에서는 EBCOT 코딩 중 Tier 2과정에서 점진적 전송(Progressive transmission)으로 전송비율에 따른 압축률 및 영상의 화질을 조절할 수 있다. 이 때 화소당 암호화를 수행하면 복원 시 원래 영상을 얻을

```
Progressive_Encrypt(){                    /* mask(i,j)is a map of the ROI */
    bs = block size
    for (k is 0 to t-1){
        for (i is 0 to x-1){
            for (j is 0 to y-1){
                p_j = b(2c);
                q_j = ( α+β×b(2c+1) ) mod t;
                switch (ROI) {
                    case 0 : block(s) = bit-plain(i,j,k);
                             s = s + 1;
                    case 1 : if ( mask(i,j) == 1 ) then
                             block(s) = bit-plain(i,j,k);
                             s = s + 1;
                }
                if ( s == block size ) then
                    if (p_j == 0) then block'(s) = block(s) <<< q_j;
                    else block'(s) = block(s) >>> q_j;
                    for (t is 0 to bs-1) bit-plain(i,j-bs-1+t,k) = block(t)
                    c = c + 1;
                    l = 0;
                if ( (c mod z) == 0 ) then
                    x(n) = x(n+1) by eq. (1);
                    n = n + 1;
    } } }
```

그림 10. 점진적 전송에 따른 영역 암호화 방법
Fig. 10. Encryption method by progressive transmission.

수 없다. 이 문제는 화소단위로 암호화하지 않고 EBCOT의 코딩방법에 따라 비트평면 단위로 암호화하여 해결할 수 있다.

그림 10에 JPEG2000에서 점진적 전송방식에 맞추어 암호화 수행방법을 나타내었다. 여기서 i, j는 영상의 좌표를 나타내고, k는 계수의 비트 좌표를 나타낸다. 우선 ROI 영역이 설정이 되어있으면 ROI 영역의 비트평면을 일정한 블록(그림 10에서 block size)의 데이터를 모아서 3-2-1절에서 제안한 알고리즘에 의해 암호화한다. 즉, 중요한 부분만을 암호화하여 암호화 하는 양을 줄일 수 있다. ROI 영역이 설정 되지 않을 경우는 전체 비트평면을 일정한 블록의 데이터를 모아서 암호화한다. 암호화 된 데이터를 점진적 전송에 의해 일부 비트평면만을 전송하게 되는데 이때 화소에 대해 암호화를 했을 경우에는 그 화소에 해당되면 모든 비트를 가지고 복호화를 하는데 비트평면으로 암호화하면 복원 시 일정한 크기(block size)만큼의 데이터만을 가지고 복호가 가능하다.

Ⅳ. 구현 및 실험결과

2장, 3장에서 설명한 영상의 선택적 부분 암호화 방법은 C언어로 구현하였으며, 실험환경은 Pentium Ⅳ 2GHz의 CPU이다. 본 논문의 영상암호화 알고리즘은 본 연구실에서 연구한 JPEG2000 기반 영상압축기 중 양자화기와 엔트로피 코더 사이에 삽입하는 형태로 구현하였다. 사용된 암호화 키는 α=6, β=12, x(0)=0.75, r=3.75를 사용하였다.

Ⅱ장에서 언급한 각 부대역 조합에 대해 Ⅲ장의 LL4 및 기타 부대역의 암호화방식을 적용한 Lena영상들을 그림 11에 나타내었다. 그림 11 (b)의 LL4만을 암호화한 결과 영상의 PSNR은 9.44161dB이었으며, 예상한 바와 같이 영상의 고주파성분이 상당부분 인식할 수 있을 정도였다. 그러나 알려지지 않은 영상을 대상으로 LL4만 암호화한 결과에 대해 인시정도를 실험한 결과 대부분의 영상을 인식하지 못하였다. 따라서 일반적으로 영상의 재사용을 막기 위한 용도로는 LL4만을 암호화하여도 충분함을 알 수 있었다.

그림 11 (c), (d) (e)는 LL4-HH4, Level4, Level4-HH3의 부대역 조합에 대해 LL4를 제외한 나머지 부대역들에 Top-down방식에 의한 암호화를 수행한 결과를 각각 나타내고 있으며, PSNR값은 각각 9.43591dB, 9.39624dB, 9.39388dB을 나타내었다. 암호화 대상 데이터의 양이 증가할수록 암호화 비용은 증가하나 암호화 효과 또한 증가함을 알 수 있다. 그러나 PSNR값은 암호화효과에 비해 감소하는 양이 충분치 못하다. 따라서 PSNR값만으로 암호화효과를 충분히 나타내지 못함을 알 수 있다. 그러나 본 논문에서는 정량적으로 암호화효과를 나탤 수 있는 방법이 없어 여전히 PSNR값을 사용한다.

그림 11 (f), (g), (h)는 Reflection code 방식으로 LL4-HH, Level4, Level4-HH3 부대역 조합을 각각 암호화한 결과이며, 이들의 PSNR 값들은 9.44006dB, 9.39411dB, 9.40163dB이었다. 이 PSNR값들과 가시적인 효과를 고려하면 Top-down 방법으로 암호화한 영상이 Reflection code 방법으로 암호화한 영상보다 암호화 효과가 좋음을 알 수 있다. 그러나 앞에서도 언급한 바와 같이 Top-down방식은 Reflection-code방식보다 압축률을 많이 떨어뜨리기 때문에 통신매체 또는 통신 단말기의 상태, 암호화 비용 등을 감안하여 적응적으로 암호화 방법을 선택할 수 있다.

제안한 방법에 대하여 500여개의 테스트 영상을 실험한 결과를 표 1에 나타내었다. 표 1에서 첫 번째 행은 선택된 부대역 조합과 QX 할당방식, 두 번째 행은 전체

표 1. 제안된 암호화 방식에 따른 실험 결과
Table 1. Experimental results by the proposed encryption schemes.

Item case	Encryption ratio	# of random bit	PSNR (dB)	Compressing ratio	Damage rate(%)
LL4 only	1:256	2048	8.86671	24.1695	0
LL4-HH4 Reflection code	1:170.67	3072	8.33751	23.8868	1.17
LL4-HH4 Top-Bottom	1:170.67	3072	8.33678	23.1471	4.23
Level 4 Reflection code	1:102.4	5120	8.33751	23.6166	2.29
Level 4 Top-Bottom	1:102.4	5120	8.27562	21.6875	10.27
Level 4-HH3 Reflection code	1:56.89	9216	8.30058	22.6843	6.14
Level 4-HH3 Top-Bottom	1:56.891	9216	8.27257	19.05	21.18

영상에 대한 암호화한 데이터의 비율, 세 번째 행은 암호화를 수행할 때 식 (2)에서 얻어진 카오스값의 개수, 그리고 네 번째 행은 암호화 수행 후의 PSNR 평균값을 각각 나타낸다. 다섯 번째 행은 엔트로피 코딩 결과의 압축률을 나타내며, 여섯 번째 행은 암호화하지 않을 때의 압축률에 대한 압축률 손실비율을 각각 나타내고 있다. 영상과 PSNR을 비교 할 때 암호화하는 양이 많을수록 그에 따른 암호화 효과가 좋아지는 것을 알 수 있고, Top-down과 Reflection code을 비교할 때 Top-down 방법이 더욱 암호화 효과가 좋다는 것을 알 수 있으나, 압축률을 비교할 때는 Reflection code 방법이 암호화 후 데이터의 분포에서 알 수 있듯이 압축률이 높다는 것을 알 수 있다.

그림 12에서는 3-4절에서 제안한 방법으로 JPEG2000의 점진적 전송에 대한 실험결과를 나타내고 있다. 화소당 비트수를 14비트로 설정해서 (a)는 3비트 전송된 영상, (b)는 6비트 전송된 영상, (c)는 9비트 전송된 영상, 그리고 (d)는 전체비트인 14비트를 전송한 영상이다. 여기서는 8비트 단위로 묶어서 제안한 알고리즘에 의해 암호화하였다. 그림에서 볼 수 있듯이 전송 비트수에 무관하게 암호화효과는 거의 일정하며, 오히려 적은 비트 전송률의 경우 가시적인 암호화 효과는 더욱 뚜렷함을 알 수 있다. 따라서 이 방법은 점진적 전송방식에서 효과적으로 사용될 수 있을 것으로 사료되며, 특히 무선통신 등에서 네트워크의 상태에 따른 적응적 전송방식에서 매우 유용한 암호화 방식이라 판단된다.

그림 13에서는 영상 가운데를 ROI 설정 후 ROI 영역을 암호화한 영상을 점진적 전송한 영상들을 나타내고 있다. 여기서는 최대-쉬프트(Max-shift) 방법으로 13비트를 쉬프트하는 것을 가정하였다. 즉 실험에 사용된 화소당 비트수는 14비트이고 이 영상을 최대-쉬프트 하면 ROI 설정된 영상의 화소당 비트수는 27비트가 된다. 그림 13 (a)에서는 이 중 5 비트가 전송된 영상, (b)는 13비트, (c)는 17 비트, (d)는 27 비트전체를 전송하여 복원된 영상을 각각 나타내고 있다. 이 영상에서 (a)영상은 ROI 영상 중 일부 비트만 전송되었고 (b)영상은 ROI 설정된 부분이만 전송 되었다. 이 영상들에 의하면 13비트 이상의 전송율에서 전송 비트율이 증가할수록 ROI가 설정되지 않은 영역(Background)의 화질이 좋아지나 ROI 영역의 암호화 정도는 변화가 없는 것을 알 수 있다. 따라서 ROI가 설정된 영상의 경우 ROI 설정부분은 전송초기부터 암호화의 효과로 내용을 판별할 수 없으므로 ROI 설정에 의한 영상전송에서도 ROI 설정 목적에 부합하는 암호화 효과를 얻을 수 있다.

영상의 암호화에 대한 암호화 효과는 기존의 연구들([6-8],[11-16]의 연구들)과 비교할 때 본 논문에서 제안한 방법과 많은 차이를 나타내고 있다. 일부 연구들 [11-16] 에서는 영상을 주파수 영역이 아닌 공간영역에서의 암호화 방법을 제안하여 영상의 일부분이 아닌 영상전체를 암호화했기 때문에 그 비교가 객관적이지 않을 수 있다. 영상에 대해서 원래의 영상과의 왜곡 정도를 PSNR로 판단하는 것이 보통이지만 PSNR이 15dB이하일 경우는 영상과 PSNR간의 상관도가 매우 작아지는 것이 보통이기 때문에 암호화 효과에 대해서는 주관적인 판단을 내릴 수밖에 없다. 공간 영역에서 특정 주파수 변환 방식을 고려하지 않고 영상에 대한 암호화를 수행한 [6]의 연구에서는 원 영상에 대해 최소 1/8의 데이터를 암호화한다. 쿼트트리(Quad-tree)를 이용한 [7]의 연구는 원래의 영상에 대해서 13%에서 27%의 암호화 율을 나타내고 있고 쿼드트리에 SPHIT를 적용한 방식에서는 두 번의 코딩 패스에 대한 암호화를 수행하였는데 이 경우에는 2~5%의 암호화 율에 해당한다. 또한 [8]의 연구와 같이 DWT 부대역의 제로트리를 이용한 암호화 방식은 제로트리 기반의 양자화 과정이 내포하는 코딩 패스의 반복수, 즉 압축률에 따른 암호화 율을 고려하여야 본 논문의 결과와 비교가 가능하다. 그러나 논문들에서 이러한 결과들에 대한 수치적, 혹은 그래프적인 결과 및 경향성 제시를 하지 않고 있기 때문에 비교가 어렵지만 제로트리 기반의 양자화 방식에 의해 일반적인 30dB의 PSNR을 가질 수 있는 압축률에서는 약

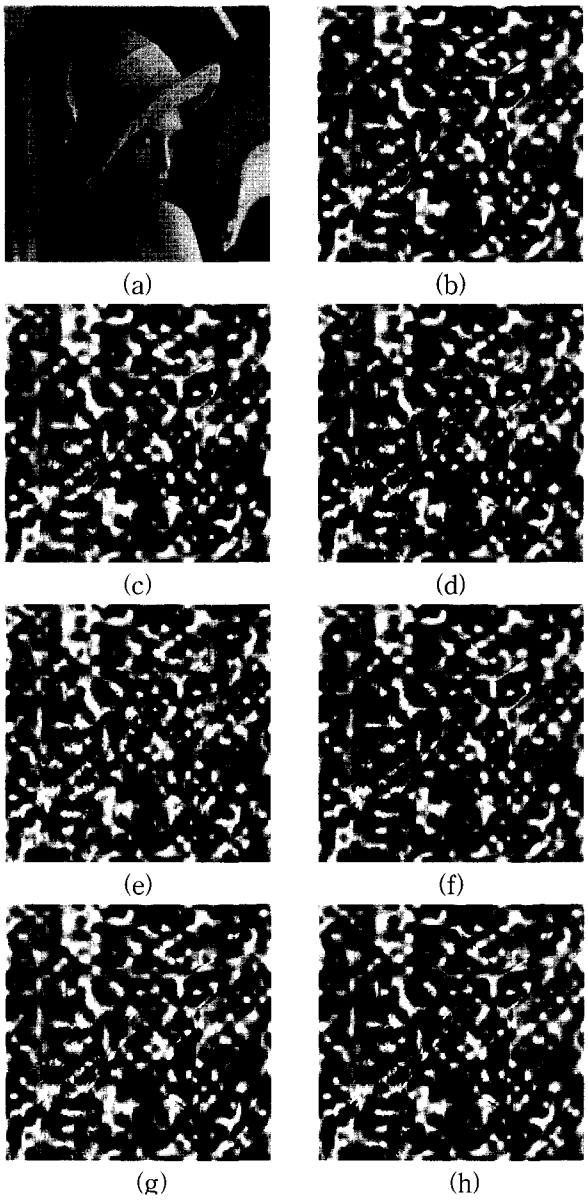


그림 11. 부대역별로 암호화한 영상; (a) 원 영상, (b) LL4만 암호화된 영상, (c) Top-down 방식에 의해 LL4-HH4를 암호화 영상, (d) Top-down방식에 의해 Level4를 암호화한 영상, (e) Top-down방식에 의해 Level4-HH3을 암호화한 영상, (f) Reflection code방식에 의해 LL4-HH4를 암호화한 영상, (g) Reflection-code방식에 의해 Level4를 암호화한 영상, (h) eflection-code방식에 의해 level 4-HH3을 암호화한 영상.

Fig. 11. Lena example by the proposed schemes; (a) original image, (b) image encrypted only for LL4, (c) image encrypted for LL4-HH4 with Top-down method, (d) image encrypted for Level4 with Top-down method, (e) image encrypted for Level4 -HH3 with Top-down method, (f) image encrypted for LL4-HH4 with Reflection-code method, (g) image encrypted for Level4 with Reflection-code method, (h) image encrypted for Level4-HH3 with Reflection-code method.

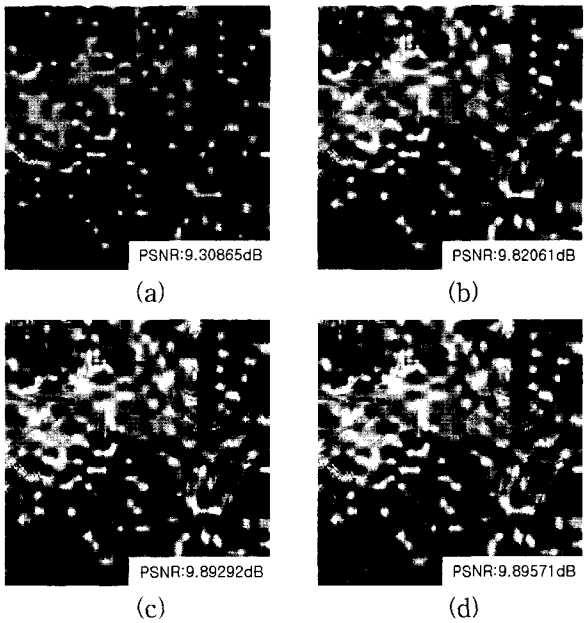


그림 12. 점진적 전송을 위한 암호화 영상; (a) 3비트 전송, (b) 6비트 전송, (c) 9비트 전송, (d) 14비트 전송.

Fig. 12. Encrypted image by progressive transmission; (a) 3 bits transmission, (b) 6 bits transmission, (c) 9 bits transmission, (d) 16 bits transmission.

1:30 이상의 암호화 율을 가져야 한다. 그러나 표 1에 나타낸 바와 같이 본 논문에서 제시한 알고리즘이 암호화 율은 최저 1:256에서 최고 1:56.89이어서 암호화 비용 대비 암호화 효과가 우수하다는 것을 알 수 있다.

V. 결 론

본 논문에서는 JPEG2000을 기반으로 하는 영상압축을 가정하고 기존의 암호화 알고리즘이 아닌 계산양이 상대적으로 적으면서 실시간 동작이 가능한 카오스 시스템의 카오스 값을 이용하여 암호화하는 영상데이터 은닉 방법을 제시하였다. 이 방법은 웨이블릿 변환 및 양자화 과정을 거친 영상데이터를 대상으로 하며 영상 전체가 아닌 일부분을 암호화하는 부분 암호화방식을 선택하였다. 영상의 부분 데이터를 선택함에 있어서 리프팅에 의해 재편성된 부대역들을 대상으로 4 가지의 조합을 구성하였는데, 이 조합들은 암호화 양과 암호화 효과에 대한 상보적인 관계를 갖는다. 따라서 통신 네트워크의 상태, 통신단말기의 상태 등을 고려하여 선택적으로 사용할 수 있도록 하였다.

암호화 방법에 있어서 카오스 값의 무작위성을 사용하였으며, 카오스 시스템의 초기값 뿐 만 아니라 카오스 시스템을 사용하기 위한 세 개의 파라메타 값을 암호화

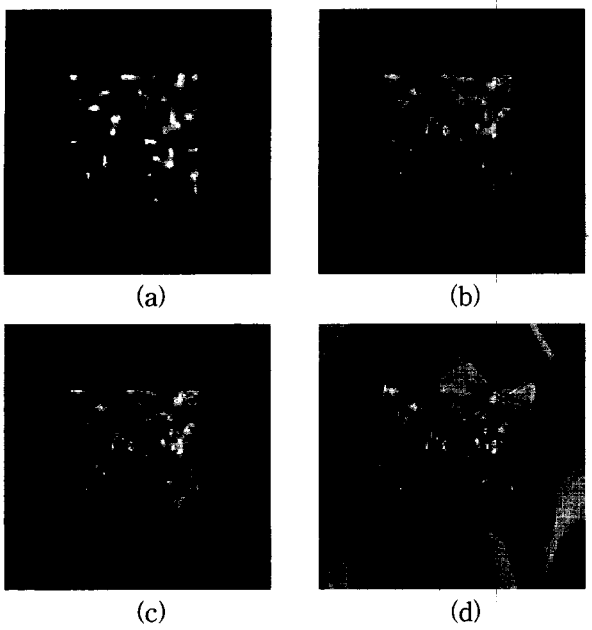


그림 13. ROI 영역을 암호화한 영상에서의 점진적 전송; (a) 5비트 전송, (b) 13비트 전송, (c) 17비트 전송, (d) 27비트 전송.

Fig. 13. Progressive transmission in image that encrypt ROI area; (a) 5 bits transmission, (b) 13 bits transmission, (c) 17 bits transmission, (d) 27 bits transmission.

키로 사용함으로써 보안성을 강화시켰다. 암호화 방식은 최저주파수 대역의 양자화에 의한 영향이 매우 작다고 가정하고 그 데이터를 계수단위로 쉬프트하는 방식을 사용하며, 그 외의 부대역에 대해서는 양자화 과정에서 Top-down방식과 Reflection-code방식의 두 양자화 계수 할당방식을 대상으로 양자화 계수를 대칭적으로 치환하는 방법을 사용하였다. Top-down방식은 Reflec-tion-code방식에 비해 동일한 암호화 양에 대한 암호화효과가 우수한 반면, 엔트로피 코딩 시 나타나는 압축률 저하양이 크다. 따라서 이 두 방식 또한 네트워크의 상태 등에 따라 선택적으로 사용할 수 있다.

본 논문이 JPEG2000 영상압축과정을 타겟으로 하고 있으므로, EBCOT의 점진적 전송방식에 적합한 암호화 방식 또한 제한하였다. 이 방식은 웨이블릿 계수 또는 양자화 인덱스를 암호화 단위로 하지 않고 비트평면의 데이터를 특정비트수로 나누어 암호화 단위로 설정한 방식이다. 이 방식으로 인해 점진적 전송의 경우도 데이터의 소실을 최소로 하여 원 데이터를 복원할 수 있으며, 저 비트율의 전송 시부터 충분한 암호화 효과가 나타남을 알 수 있었다. 또한 JPEG2000에서 표준으로 채택된 ROI 설정에 대하여 이 방식을 적용한 결과 ROI로 설정된 영역의 데이터는 충분한 암호화 효과를 나타냄과 동시에 ROI 특성을 그대로 유지하여 ROI 설정 후 점진적 전송에도 유용하게 사용될 수 있으리라 사료된다.

제안한 방법을 테스트 한 결과, 본 논문에서 나타난 부대역 조합의 선택에 따른 암호화 양과 암호화 효과의 상보적인 관계와 양자화 계수 할당방식에 따른 암호화 효과와 압축률 손실의 상보적인 관계는 통신환경의 변화에 따른 적응적 암호화에 충분하다고 판단된다. 또한 점진적 전송방식 및 ROI 설정에의 적용가능성으로 무선통신 등과 같이 네트워크 상황이 크게 변화하는 응용분야에서도 적용 가능할 것으로 사료되어, 본 논문에서 제안한 방법은 향후 그 응용가능성이 매우 높다고 판단된다.

참 고 문 헌

[1] Chisalita, I. and Shahmehri, N, "Issues in image utilization within mobile e-services" Proceedings of WET ICE 2001. Proceedings. pp. 62-67, 2001.

[2] J. D. Gibson, et al., Digital Compression for Multimedia, Principles and Standards, Morgan Kaufmann Pub., San Francisco CA, 1998.

[3] R. M. Rao, and A, S. Bopardikar, Wavelet Trans-forms, Introduction to Theory and Applications, Addison-Wesley, Readings MA, 1998.

[4] Martin Boliek, et al., JPEG 2000 Part I Final Draft International Standard, ISO/IEC JTC1/SC29 WG1, 24 Aug. 2000.

[5] Ianin E. G. Richardson, Video codec design developing image and video compression system, Wiley, pp. 79-92, 2002.

[6] G. J. Sullivan and R. L. Baker, "Efficient Quad-tree coding of images and videos", IEEE Trans. on Signal Processing, Vol. 3, pp. 327-331, May 1994.

[7] P. P. Dang and P. M. Chau, "Image Encryption for Secure Internet Multimedia Applications", IEEE Trans. on Consumer Electronics, Vol. 46, No. 3, pp. 395-403, Aug. 2000.

[8] Said, A., Pearlman, W.A., "A new, fast, and efficient image codec based on set partitioning in hierarchical trees", Circuits and Systems for Video Technology, IEEE Transactions on , Volume: 6Issue: 3, June 1996, pp. 243-250.

[9] Shapiro, J.M., "Embedded image coding using zerotrees of wavelet coefficients", Signal Proce-ssing, IEEE Transactions on [see also Acous-tics, Speech, and Signal Processing, IEEE Transactions on], Volume: 41 Issue: 12, pp. 3445-3462, Dec. 1993.

[10] M. Podesser, H. P. Schmidt, and A. Uhl, "Selective Bitplane Encryption for Secure Trans -mission of Image Data in Mobile Environmen -ts", Proc. 5th Nordic Signal Processing Sympo -sium, 2002.
[11] Fridrich, J, "Image encryption based on chaotic maps", 1997 IEEE International Conference on , Vol 2, pp. 1105-1110, 12-15 Oct. 1997.
[12] Salleh, M., Ibrahim, S., Isnin, I.F., "Enhanced chaotic image encryption algorithm based on baker's map", Circuits and Systems, 2003. ISCAS '03. Proceedings of the 2003 International Symposium on , Vol. 2, pp. 508-511, May 25-28, 2003.
[13] Belkhouche, F., Qidwai, U., "Binary image encoding using 1D chaotic maps", IEEE Region 5, 2003 Annual Technical Conference, pp. 39-43, 11 April 2003.
[14] Ammar, A., Al Kabbany, A., Youssef, M., Amam, A., "A secure image coding scheme us -ing residue number system", Radio Science Conference, 2001. NRSC 2001. Proceedings of the Eighteenth National , Volume: 2, pp. 399-405, 27-29 March 2001.
[15] 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.
[16] Bourbakis, N.; Dollas, A., "SCAN-based com -pression-encryption-hiding for video on dema -nd", Multimedia, IEEE , Volume: 10Issue: 3, pp. 79-87, July-Sept. 2003.
[17] 서영호, Sujit Det, 김동욱, "웨이블릿 영역에서의 선택적 부분 영상 암호화", 한국통신학회 논문지 Vol. 28 No. 6C, pp. 648-658, 2003. 6.
[18] Sandra K. Miller, "Facing the Challenge of Wireless Security", IEEE Computer Magazine, pp. 16-18, July 2001.
[19] S. R. Ravi, et al., "Securing Wireless Data: System Architecture Challenges", ISSS'02, pp. 195-200, Oct. 2002.
[20] 문희태, 카오스와 비선형동역학, 서울대학교출판부, pp. 136-139, 2002.
[21] Jui-Cheng Yen, Jiun-In Guo, "A new chaotic key-based design for image encryption and de -cryption", Circuits and Systems, 2000. Procee -dings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on, vol. 4, pp. 49-52, 28-31 May 2000.

저 자 소 개

김 수 민(학생회원)
2002년 8월 전주대학교 전기전자 공학과 졸업 (공학사)
2003년 3월 ~ 현재 광운대학교 전자재료공학과 석사과정.
<주관심분야: Image Processing, 암호학, FPGA/ASIC 설계>

김 동 욱(평생회원)
1983년 2월 한양대학교 전자공학과 졸업(공학사).
1985년 2월 한양대학교 대학원 졸업(공학석사).
1991년 9월 Georgia공과대학 전기 공학과 졸업(공학박사).
1992년 3월~현재 광운대학교 전자재료공학과 정교수.
광운대학교 신기술 연구소 연구원.
2000년 3월~2001년 12월 인티스닷컴(주) 연구원.
<주관심분야: 디지털 VLSI Testability, VLSI CAD, DSP 설계, Wireless Communication>

서 영 호(평생회원)
1999년 2월 광운대학교 전자재료 공학과 졸업(공학사).
2001년 2월 광운대학교 대학원 졸업(공학석사).
2000년 3월~2001년 12월 인티스닷컴(주) 연구원.
2001년 3월~현재 광운대학교 전자재료공학과 박사과정.
2003년 6월~현재 한국전기연구원 연구원
<주관심분야: Image Processing/Compression, 워터마킹, 암호학, FPGA/ASIC 설계>