논문 2005-42SP-5-20

3차원 카오스 캣맵을 이용한 JPEG2000 영상의 암호화 기술

(A Encryption Technique of JPEG2000 Image Using 3-Dimensional Chaotic Cat Map)

최 현 준*, 김 수 민*, 서 영 호**, 김 동 욱***

(Hyun-Jun Choi, Young-Ho Seo, and Dong-Wook Kim)

요 약

본 논문에서는 JPEG2000 표준에서 주파수 변환기법으로 채택된 이산 웨이블릿 변환을 기반으로 영상의 부분 데이터만을 암호화하여 계산량을 줄이는 방법을 제안하였다. 또한 계산량이 많은 암호화 알고리즘 대신 비교적 계산량이 적은 캣맵(cat map)과 카오스 시스템을 이용함으로써 계산량을 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 선택하여 영상데이터를 3차원 블록으로 만든 후 캣맵에 의해 3차원으로 영상의 픽셀값을 교환 하는 방법과 캣맵에 의해 암호화된 부대역을 카오스 시스템을 이용하여 모듈러 연산에 의해 암호화하였다. 또한, JPEG2000의 점진적 전송(Progressive transmission)에 적합하게 암호화하기 위해서 비트 평면을 선택하여 암호화하였다. 제안한 방법을 소프트웨어로 구현하여 500개의 영상을 대상으로 실험한 결과 원 영상 데이터를 부분적으로 암호화함으로써 원 영상을 인식할 수 없을 정도의 암호화효과를 얻을 수 있었다. 본 논문에서는 여러 방식을 제안하였으며, 이들의 암호화 수행시간과 암호화 효율 사이에는 상보적인 관계가 있음을 보여, 적용분야에 따라 선택적으로 사용할 수 있음을 보였다.

Abstract

In this paper, we proposed the image hiding method which decreases calculation amount by encrypt partial data using discrete wavelet transform(DWT) and linear scale quantization which were adopted as the main technique for frequency transform in JPEG2000 standard. Also we used the chaotic system and cat map 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. 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 is 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.

Keywords: DWT, Chaotic System, Cat Map, Image Encryption, Lifting.

I. 서 론

멀티미디어 시대를 맞이하여 영상과 비디오 컨텐츠에 대한 선호도가 급속히 증가하고 있다[1]. 데이터의 안전한 전송을 위해 여러 암호화 알고리즘이 개발되었으며 몇몇 알고리즘들은 국내 및 국제 표준으로 선정되어 여러 분야에서 사용되고 있다[2]. 특히, 영상/비디오 같은 매체는 데이터양이 매우 많아서 영상/비디오 전체를 암호화 하는데 많은 비용과 시간이 소요됨으로 암호화하는 양을 줄이는 연구가 이루어지고 있다. 영상/비디오의 데이터양을 줄이는 연구는 지금까지 두 주류를 형성하고 있다. 현재 가장 널리 사용되고 있는 분야는 JPEG 및 MPEG 분야로, 지금까지 상당부분이 국제표

* 학생회원, *** 평생회원 광운대학교 전자재료공학과
(Dept. of Electronic Materials Eng., Kwangwoon University)
** 평생회원, 한성대학교 정보통신공학과
(Dept. of Information and Communication Engineering, Hansung University)
※ 본 논문은 서울특별시 서울과학장학생 (Seoul Science Fellowship) 지원 사업의 결과입니다.
접수일자: 2005년4월4일, 수정완료일; 2005년6월9일

준으로 채택되었으며, 현재 대부분의 응용분야에 사용되고 있다.

영상/비디오 컨텐츠에 대한 암호화는 암호화된 데이터의 한 비트라도 소실되면 복원된 데이터는 원 데이터와 완전히 다른 데이터가 된다는 특성 때문에 압축이 수행되는 영상/비디오의 경우 압축과정에 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.

[3]에서는 쿼드트리(quadtree) 기반의 SPHIT[5]를 겨냥하여 암호화하는 방법을 제안하였으며, [4]에서는 EZW 방법[6]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 연구가 진행되고 있다. [7]에서는 베이커 맵(Baker map)을 이용한 위치교환 방식의 암호화 방법을, [8]에서는 베이커 맵을 이용한 위치교환 방법에 암호화키를 이용한 암호화 방법을 각각 제안하였는데, 이 방법들은 암호화 전과 후의 데이터 분포의 변화가 많아서 암호화 후 엔트로피 코딩 시 압축률 손실이 매우 크다. [9]에서는 카오스 맵(Chaos map)을 이용한 위치 교환 방식을 이용한 암호화를 수행하였고, [10]에서는 RNS(Residue Number System)을 이용하여 암호화하는 방법을 제안하였으며, [11][12]에서는 스캔 패턴을 조절하여 암호화하는 방법을 제안하였으나, 암호화 정도에 따라 압축률 손실이 과다하여 압축과정에서 사용하기에는 적합하지 않다.

본 논문에서는 JPEG2000을 기반으로 영상 암호화를 수행하였다. 전체 영상을 암호화 하지 않고 [13]에서 제시되었던 방법으로 부대역을 선택하여 암호화하였다. 암호화 효율을 높이기 위해 선택된 부대역을 3차원 블록으로 만든 후 캣맵을 사용하여 암호화 하였고 카오스 시스템과 모듈러 연산을 이용하여 다시 한번 암호화하였다. 또한, 영상 데이터를 비트평면(Bit plain)단위로 암호화하여 JPEG2000 표준 방법에서 사용되는 점진적 전송에 적합하게 하였다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 3차원 캣맵과 암호화 알고리즘에 대해 설명하고, Ⅲ장에서는 3차원 캣맵과 카오스 시스템을 이용한 암호화 과정에 대해 설명한다. Ⅳ장에서는 제안한 방법에 대한 실험 및 결과를 보이고, 마지막으로 Ⅴ장에서는 본 논문의 결론을 맺는다.

Ⅱ. 3차원 캣맵과 암호화 알고리즘

1. 3차원 캣맵

본 논문에서는 [14][15][16]에서 사용된 2차원 캣맵(Arnold's cat map)을 확장해서 3차원으로 캣맵을 이용하여 영상을 암호화하였다. 식 (1)에 두개의 파라미터 a, b에 의한 2차원 캣맵을 나타내었고 암호화 되는 구조를 그림 1에 나타내었다. 그림 1은 원 영상이 (1,1) 좌표에서 (2,3)으로 길게 늘인 다음 다시 (1,1) 크기에 맞게 정렬하여 암호화 하는 그림이다.

식 (1)에서 z좌표를 고정시키고 x-y좌표 평면으로 변화하는 3차원 캣맵을 나타내면, 식 (2)와 같이 나타난다. 여기에서 x좌표를 고정시키고 y-z좌표 평면으로 변화하는 3차원 캣맵을 나타내면, 식 (3)의 결과를 얻는다. 또한 y좌표를 고정시키고 x-z좌표 평면으로 변화하는 3차원 캣맵을 나타내면, 식 (4)가 된다. 식 (2)(3)(4)을 결합하여 3차원 캣맵을 만들면, 식 (5)와 같다.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1 \tag{1}$$

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a_z & 0 \\ b_z & a_z b_z + 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} \bmod 1 \tag{2}$$

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & a_x \\ 0 & b_x & a_x b_x + 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} \bmod 1 \tag{3}$$

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & a_y \\ 0 & 1 & 0 \\ b_y & 0 & a_y b_y + 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} \bmod 1 \tag{4}$$

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} \bmod 1 \tag{5}$$

행렬 A를 식 (6)에서 나타내었다.

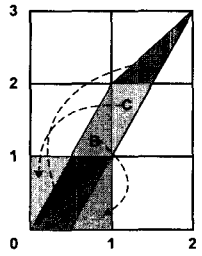


그림 1. 2차원 캣맵의 구조.
Fig. 1. Structure of 2D cat map.

$$A=\begin{bmatrix}1 & a_z & 0\\ b_z & a_z b_z+1 & 0\\ 0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & a_x\\ 0 & b_x & a_x b_x+1\end{bmatrix}\begin{bmatrix}1 & 0 & a_y\\ 0 & 1 & 0\\ b_y & 0 & a_y b_y+1\end{bmatrix}$$
$$=\begin{bmatrix}1+a_x a_z b_y & a_z & a_y+a_x a_z+a_x a_y a_z b_y\\ b_z+a_x b_y+a_x a_z b_y b_z & a_z b_z+1 & a_y a_z+a_x a_z a_z b_y b_z+a_x a_z b_z+a_x a_y b_y+a_x\\ a_x b_x b_y+b_y & b_x & a_x a_y b_x b_y+a_x b_x+a_y b_y+1\end{bmatrix} \quad (6)$$

행렬 A는 행렬식이 1(det A=1)이 되어서 초기의 파라미터값이 같다면 행렬 A^{-1}을 구해 암호화 된 영상을 복호화 하면 원래 영상을 얻을 수 있다.

2. 암호화 알고리즘

암호화하기 위해서 2차원 영상을 그림 2와 같이 3차원으로 전환시킨 후 영상을 암호화 한다. 이때 식 (7)과 같이 3차원 블록 i개와 R로 나누어서 암호화 한다. 여기서 $N_i \in \{2,3,\cdots,N\}$ 이고 $R \in \{0,1,2,\cdots,7\}$ 이다.

$$W\times H = N_1^3 + N_2^3 + \cdots + N_i^3 + R \quad (7)$$

3차원으로 재구성된 영상은 식 (5)에 의해 암호화되고 식 (9)의 모듈러 연산에 의해 다시 암호화된다. 식 (9)의 *C(k)*는 암호화된 픽셀값을 의미하는데 식에서 $\phi(k)$는 식 (8)에서의 *x(n+1)*값이고 *i(k)*는 현재 픽셀값 *C(k-1)*은 전 픽셀의 암호화된 픽셀값을 의미한다. 여기서 *r*, *x(0)*는 식 (8)에서의 초기화 파라미터 값이고, 식 (9)에서의 *C(0)*도 암호화시 암호화를 하기 위한 초기값을 나타낸다. 즉 영상 암호화에 필요한 키(Key)값은 식 (6)에서 A 행렬 원소 즉, $a_x, b_x, a_y, b_y, a_z, b_z$이고 식 (8)(9)에서 *r*, *x(0)*, *C(0)* 이다. 식 (10)은 암호화된 영상을 복원할 때 사용되는 식이다. 여기서 N은 3차원 영상의 크기를 나타낸다.

$$x(k+1) = rx(k)[1-x(k)] \quad (8)$$
$$C(k) = \phi(k)\oplus\{[i(k)+\phi(k)]\bmod N\}\oplus C(k-1) \quad (9)$$
$$I(k) = \{\phi(k)\oplus C(k)\oplus C(k-1)+N-\phi(k)\}\bmod N \quad (10)$$

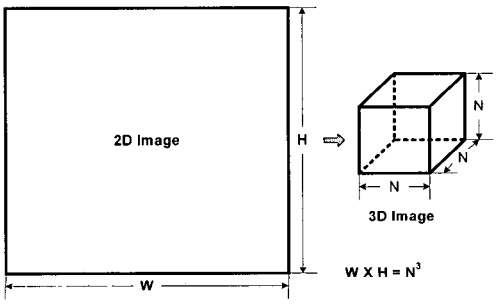


그림 2. 2차원 영상을 3차원으로 전환.
Fig. 2. Change of 2D to 3D image.

Ⅲ. 제안한 암호화 과정

본 장에서는 카오스 캣맵을 이용하여 본 논문에서 제안하는 선택적 부분 영상 암호화 알고리즘에 대해 설명한다.

1. 부대역의 선택

리프팅 변환 결과 각 부대역은 서로 다른 주파수 성분을 가지면서 전체 영상에 대한 위치 정보를 포함하고 있어서 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 부분 암호화 결과 영상을 인식하지 못하거나 영상을 다시 사용하지 못할 정도로 영상을 왜곡시킬 수 있다면 반드시 전체영상을 암호화할 필요는 없다. 더구나 암호화 알고리즘을 사용할 경우 암호화에 소요되는 처리시간 때문에 전체 영상처리 시간에 큰 영향을 줄 수 있으며, 특히 무선통신 등의 제한적 환경에서는 암호화 및 복호화 과정으로 인한 지연시간(latency time)과 전력소모는 큰 장애요소가 되고 있으므로, 가능하면 암호화 양을 최소로 하는 것이 바람직하다. 본 논문에서는 4-레벨 DWT를 수행하는 것으로 가정하고 4가지 방법으로 부대역을 부분적으로 선택하여 암호화할 데이터양을 줄인다.

① LL4 : LL4만 암호화
② LL4-HH4 : LL4와 HH4만 암호화
③ Level4 : 레벨-4의 모든 부대역 암호화
④ Level4-HH3 : 레벨-4의 모든 부대역과 HH3 암호화

이 방식은 [13]에서 제안된 방식으로 암호화 목적과 적용분야에 따라 선택적으로 사용된다.

2. 영상 암호화 및 복호화

영상 암호화 과정을 그림 3에 나타내었다. 2차원 영상을 입력 받아서 리프팅 기반의 웨이블릿 변환을 수행한다. 그리고 [13]에서 제시된 방법으로 부대역을 선택하여 암호화 한다. 선택된 부대역을 3차원 영상으로 변환 후 식 (5)에 의한 캣맵과 식 (9)에 의한 모듈러 연산에 의해 암호화 한 후 다시 2차원 영상으로 복원 하여 암호화 된 영상을 얻게 된다. 암호화시 키 값은 a_x, b_x, a_y, b_y, a_z, b_z, *r*, *x(0)*, *C(0)* 이다.

a_x, b_x, a_y, b_y, a_z, b_z는 3차원 캣맵으로 암호화시 사용

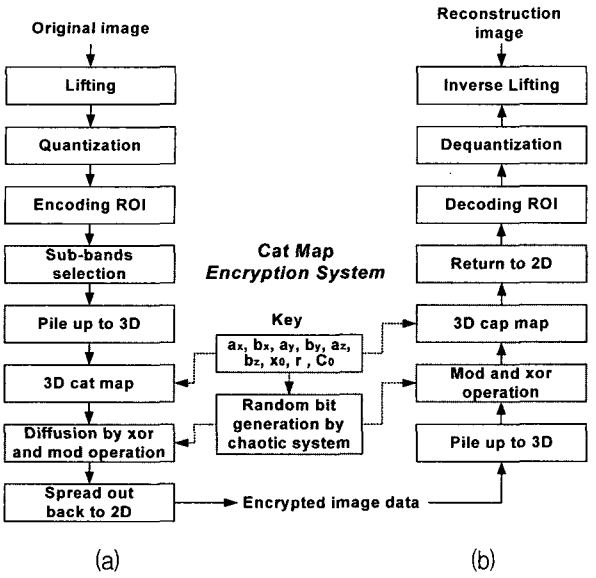


그림 3. 영상 암호화 및 복호화 과정; (a)암호화, (b)복호화.

Fig. 3. Image encryption and decryption procedure; (a)encryption, (b) decryption.

되고 r, $x(0)$, $C(0)$는 모듈러 연산 암호화 시 사용된다. 일반적인 암호화 알고리즘이 그렇듯이 본 논문에서도 암호화/복호화를 위한 암호화 키는 통신대상 양측에서 이미 보유하고 있다고 가정한다.

3. 점진적 전송에 따른 영상 암호화

JPEG2000에서는 EBCOT 코딩 중 Tier 2과정에서 점진적 전송으로 전송비율에 따른 압축률 및 영상의 화질을 조절할 수 있으며, 그 방식으로는 SNR(Signal to Noise Ratio) scalability, resolution scalability를 사용하는 방식이 있다. SNR scalability는 전송율를 높일수록 화질이 향상되고, resolution scalability는 부대역 별로 전송하여 전송되는 부대역이 많을수록 영상의 크기를 크게 한다. 영상 암호화 시 제안한 알고리즘이 부대역 별로 선택적으로 암호화하기 때문에 resolution scalability에는 아무런 문제가 없으나, SNR scalability에는 화소단위로 암호화를 수행하면 복원 시 원래 영상을 얻을 수 없는 문제는 화소단위로 암호화하지 않고 EBCOT의 코딩방법에 따라 비트평면 단위로 암호화하여 그 문제를 해결할 수 있다.

그림 4에 JPEG2000에서 점진적 전송방식에 따른 암호화 수행방법을 나타내었다. 여기서 i, j는 영상의 좌표를 나타내고, k는 계수의 비트 좌표를 나타낸다. ROI 영역이 설정이 되어 있는 경우 ROI 영역의 비트평면에서 일정한 블록의 데이터를 모아서 제안한 알고리즘에 의해 암호화한다. ROI 영역이 설정 되지 않을 경우는

```
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) {
                pj = b(2c);
                qj = ( a+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 (pj == 0) then block'(s) = block(s) <<< qj;
                    else block'(s) = block(s) >>> qj;
                    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 4. 점진적 전송에 따른 영역 암호화 방법.

Fig. 4. Encryption method by progressive transmission.

전체 비트평면에서 일정한 블록의 데이터를 모아서 암호화한다. 암호화된 데이터를 점진적 전송에 의해 일부 비트평면만을 전송하게 되는데, 이때 화소에 대해 암호화를 한 경우는 그 화소에 해당되면 모든 비트를 가지고 복호화를 수행하여야 하며 비트평면으로 암호화한 경우는 블록 크기만큼의 데이터만으로 복호화 한다.

Ⅳ. 구현 및 실험결과

제안한 영상암호화 알고리즘은 JPEG2000 기반 영상 압축기 중 양자화기와 엔트로피 코더 사이에 삽입하는 형태로 구현하였다. 사용된 암호화키로 a_x=0x0001, b_x=0x0002, a_y=0x0003, b_y=0x0004, a_z=0x0005, b_z=0x0006, $C(0)$=0x0007, $x(0)$=0.75, r=3.75를 사용하였다. 실험 영상은 Lena(512×512)를 이용하여 4-레벨 리프팅을 수행 하였다. 그 결과 LL4 부대역이 32×32 이므로 식 (7)에 의해 $32\times32=10^3+2^3+2^3+2^3=1024$로 분할한다. 즉, 10×10×10인 3차원 영상 1개, 2×2×2인 3차원 영상 3개이다. HH4, HL4, LH4 부대역 암호화 할 때도 같은 방법으로 분할하였다. HH3 부대역은 64×64 이므로 식 (7)에 의해 $64\times64=16^3=4096$로 분할한다.

제안한 방법에 대하여 500개의 영상을 대상으로 실험한 결과를 표 1에 나타내었다. 표 1에서 첫 번째 행은 선택된 부대역 조합, 두 번째 행은 전체 영상에 대한 암호화한 데이터의 비율, 세 번째 행은 암호화를 수행할 때 얻어지는 카오스값의 개수, 그리고 네 번째 행은 암호화

표 1. 제안한 암호화 방식에 따른 실험 결과.
Table 1. Experimental result by the proposed encryption schemes.

Item case	Encryption ratio	# of random bit	PSNR (dB)
LL4 only	1:256	2048	9.7568
LL4-HH4	1:170.67	3072	9.4321
Level 4	1:102.4	5120	9.2547
Level 4-HH3	1:56.89	9216	9.2354

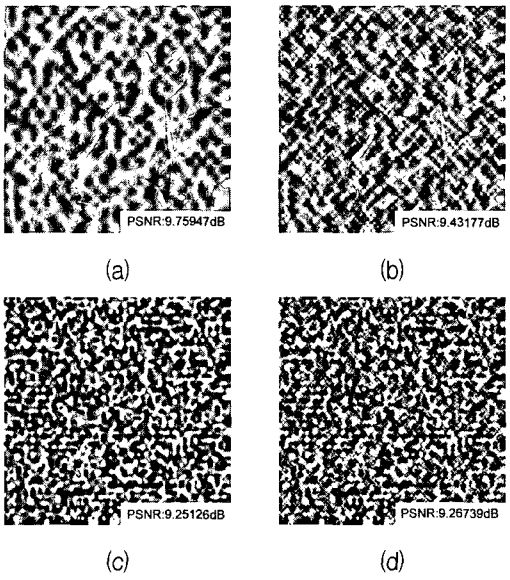


그림 5. Lena 영상의 암호화 결과; (a) LL4 (b) LL4-HH4 (c) Level 4 (d) Level 4-HH3
Fig. 5. Encryption result of lena image; (a) LL4 (b) LL4-HH4 (c) Level 4 (d) Level 4-HH3.

수행 후의 PSNR 평균값을 각각 나타낸다. 영상과 PSNR을 비교할 때 암호화하는 양이 많을수록 그에 따른 암호화 효과가 좋아지는 것을 알 수 있다.

그림 5의 (a)에서 LL4만을 암호화한 결과 영상의 PSNR(Peak Signal to Noise Ratio)은 9.75947dB이었으며, 예상한 바와 같이 영상의 고주파성분이 상당부분 인식할 수 있을 정도였다. 그러나 알려지지 않은 영상을 대상으로 LL4만 암호화한 결과에 대해 인식정도를 실험한 결과 대부분의 영상을 인식하지 못하였다. 그림 5의 (b)는 LL4와 HH4 부대역, (c)는 Level 4 부대역, (d)는 Level 4와 HH4 부대역을 선택하여 암호화 한 영상과 PSNR을 나타내었다. 그림 6은 JPEG2000의 점진적 전송에 대한 실험결과를 나타내었다. 화소당 비트수를 16비트로 설정해서 (a)는 2비트 전송된 영상, (b)는 4비트 전송된 영상, (c)는 6비트 전송된 영상, (d)는 9비트 전송한 영상이다. 그림에서 볼 수 있듯이 전송 비트수에 무관하게 암호화 효과는 거의 일정하며, 오히려 적은 비트 전송률의 경우 가시적인 암호화

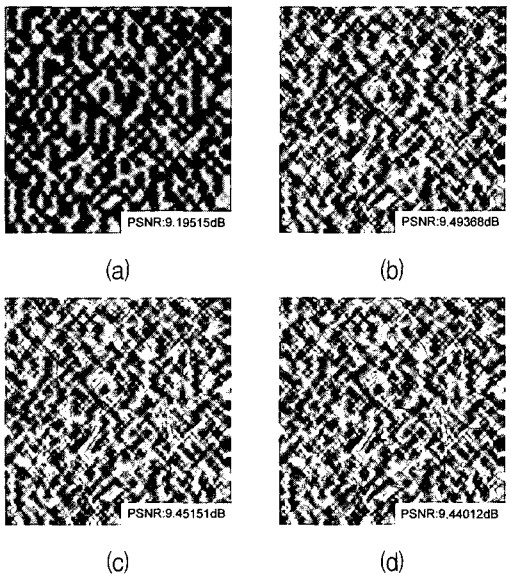


그림 6. SNR scalability의 점진적 전송을 위한 암호화 영상(LL4-HH4); (a) 2-비트 전송 (b) 4-비트 전송 (c) 6-비트 전송 (d) 9-비트 전송
Fig. 6. Encrypted image for progressive transmission with SNR scalability; (a) 2-bit transmission, (b) 4-bit transmission, (c) 6-bit transmission, (d) 9-bit transmission.

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 7은 resolution scalability의 결과를 나타낸 것이다. LL4를 전송할 경우에는 LL4만 암호화하고, LL3를 전송할 때에는 LL4와 HH3를 암호화하거나 레벨-4를 암호화 한다. LL2, LL1, LL0를 전송할 때는 레벨-4와 HH3를 암호화하여 전송에 따른 암호화 비율을 조절 할 수 있다. 따라서 이 방법은 점진적 전송방식에서 효과적으로 사용될 수 있을 것으로 사료되며, 특히 무선통신 등에서 네트워크의 상태에 따른 적응적 전송

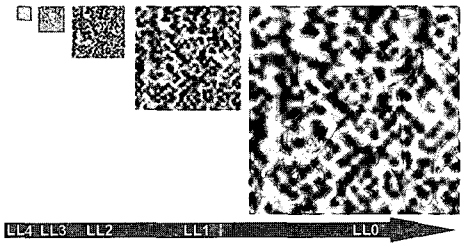
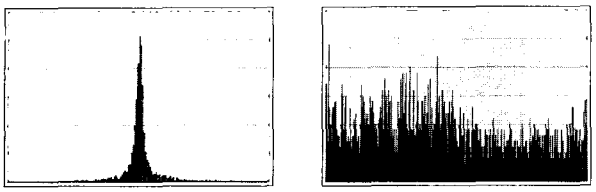


그림 7. Resolution scalability의 점진적 전송을 위한 암호화 영상.
Fig. 7. Encrypted images by progressive transmission with resolution scalability.



(a) (b)

그림 8. 암호화에 의한 데이터 분포의 변화(HH3); (a) 암호화 전 (b) 암호화 후

Fig. 8. Change in data distribution by encryption; (a) before encryption, (b) after encryption.

방식에서 매우 유용한 암호화 방식이라 판단된다.

그림 8은 HH3 부대역을 암호화 시 암호화 전과 후의 데이터 분포의 변화를 나타내었다. 암호화 전과 후의 데이터 분포가 틀려서 암호화 효율이 높다는 것을 알 수 있다.

영상 암호화에 대한 암호화 효과는 기존의 연구들[3][4][8]~[12]과 비교를 통해 표 2에 나타내었는데, 본 논문에서 제안한 방법과 많은 차이를 보이고 있다. 일부 연구들에서는 영상을 주파수 영역이 아닌 공간영역에서 암호화하는 방법을 제안[8]~[12]하였는데, 이 방법들은 영상의 일부분이 아닌 영상전체를 암호화했기 때문에 비교가 객관적이지 않을 수 있다. 영상에 대해서 원래의 영상과의 왜곡 정도를 PSNR로 판단하는 것이 보통이지만 PSNR이 15dB이하일 경우는 영상과 PSNR 간의 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 연구[8]에서는 원 영상에 대해 최소 1/8의 데이터를 암호화한다. 쿼트 트리(Quad tree)를 이용한 연구[3]는 원래의 영상에 대해서 13%에서 27%의 암호화율을 나타내고 있고, 쿼드트리에 SPHIT를 적용한 방식에서는 두 번의 코딩 패스에 대한 암호화를 수행하였는데 이 경우에는 2~5%의 암호화율을 나타낸다. 또한 DWT 부대역의 제로트리를 이용한 암호화 방식[4]은 제로트리 기반의 양자화 과정이 내포하는 코딩 패스의 반복수, 즉 압축률에 따른 암호화율을 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 1:30 이상의 암호화율을 가져야 한다. 그러나 표 2에 나타낸 바와 같이 제안한 알고리즘이 암호화율은 최저 1:256에서 최고 1:56.89이어서 암호화 비용 대비 암호화 효과가 우수하다는 것을 알 수 있다.

표 2. 제안한 영상암호화 시스템과 기존 연구와의 비교.

Table 2. Performance comparison between the proposed image encryption system and the previous researches.

Proposed Algorithm	Transform domain	Encryption ratio
[8]	Spacial domain	1:1
[9]		
[10]		
[11]		
[12]		
[3]	Frequency domain	1:3.7 ~ 1:7.69
[4]		1:30
Ours		1:256 ~ 1:56.89

V. 결 론

본 논문에서는 JPEG2000을 기반으로 하는 영상압축을 가정하고 암호화 알고리즘이 아닌 계산양이 상대적으로 적은 3차원 캣맵과 카오스 시스템을 이용한 모듈러 연산을 사용하여 영상을 암호화하여 영상데이터를 감추는 방법을 제시하였다. 이 방법은 웨이블릿 변환 및 양자화 과정을 거친 영상데이터를 대상으로 하며 영상 전체가 아닌 일부분을 암호화하는 부분 암호화방식을 택하였다. 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 값과 캣맵을 구성하기 위한 암호화키를 사용함으로써 보안성을 강화시켰다.

본 논문에서 제안한 방법은 통신프로토콜의 응용수준에서 이루어지므로 유/무선 복합 통신매체를 사용하는 경우 유/선무선구간 사이에서의 복호화를 필요로 하지 않아 통신의 끝과 끝(end-to-end) 보안을 위한 좋은 해결책으로 사용 가능할 것으로 전망된다.

참 고 문 헌

[1] I. Chisalita, N. Shahmehri, "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] G. J. Sullivan and R. L. Baker, "Efficient Quadtree coding of images and videos", IEEE Trans. on Signal Processing, Vol. 3, pp. 327-331, May 1994.

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

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

[6] J. M. Shapiro, "Embedded image coding using zerotrees of wavelet coefficients", Signal Processing, IEEE Trans. on [see also Acoustics, Speech, and Signal Processing, IEEE Transactions on], Vol. 41 Issue: 12, pp. 3445-3462, Dec. 1993.

[7] M. Podesser, H. P. Schmidt, and A. Uhl, "Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments", Proc. 5th Nordic Signal Processing Symposium, 2002.

[8] M. Salleh, S. Ibrahim, I.. F. Isnin, "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.

[9] J. Fridrich, "Image encryption based on chaotic maps", 1997 IEEE International Conference on , Vol 2, pp. 1105-1110, 12-15 Oct. 1997.

[10] A. Ammar, A. Kabbany, A. Youssef, M. Amam, "A secure image coding scheme using residue number system", Radio Science Conference, 2001. NRSC 2001. Proceedings of the Eighteenth National, Vol. 2, pp. 399-405, 27-29 March 2001.

[11] 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.

[12] N. Bourbakis, A. Dollas, "SCAN-based compression-encryption-hiding for video on demand", Multimedia, IEEE , Vol. 10Issue: 3, pp. 79-87, July-Sept. 2003.

[13] 서영호, S. Det, 김동욱, "웨이블릿 영역에서의 선택적 부분 영상 암호화", 한국통신학회 논문지 Vol. 28 No. 6C, pp. 648-658, 2003. 6.

[14] http://online.redwoods.cc.ca.us/instruct/darnold/laproj/Fall97/Gabe/catmap.pdf

[15] http://mathworld.wolfram.com/ArnoldsCatMap.html

[16] http://online.redwoods.cc.ca.us/instruct/darnold/maw/catmap4.htm

저 자 소 개

최 현 준(학생회원)
2003년 2월 광운대학교 전자재료 공학과 졸업(공학사).
2005년 2월 광운대학교 대학원 졸업(공학석사).
2005년 3월~현재 광운대학교 전자재료공학과 박사과정.
<주관심분야 : Image Processing, 암호학, FPGA /ASIC 설계>

서 영 호(평생회원)
1999년 2월 광운대학교 전자재료 공학과 졸업(공학사).
2001년 2월 광운대학교 대학원 졸업(공학석사).
2000년 3월~2001년 12월 인티스닷컴(주) 연구원.
2003년 6월~2004년 6월 한국전기연구원 연구원.
2004년 8월 광운대학교 대학원 졸업(공학박사).
2004년 9월~2004년 11월 유한대학 겸임교수.
2004년12월~2005년 유한대학 연구교수.
2005년 9월~현재 한성대학교 교수
<주관심분야 : Image Processing/Compression, 워터마킹, 암호학, FPGA/ASIC 설계>

김 수 민(학생회원)
2002년 8월 전주대학교 전기전자 공학과 졸업(공학사).
2005년 2월 광운대학교 대학원 졸업(공학석사).
<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>