JPEG2000의 보안을 위한 카오스 시스템의 하드웨어 구현

정회원 서 영 호*

Hardware Implementation of Chaotic System for Security of JPEG2000

Young-Ho Seo* ***Regular Member***

요 약

본 논문에서는 JPEG2000 표준에서 주파수 변환기법으로 채택된 이산 웨이블릿 변환과 선형양자화 방법을 사용하여 영상 전체가 아닌 영상의 부분 데이터만을 암호화하여 계산양을 줄이는 부분 암호화 방법을 제안하고 하드웨어로 구현하였다. 또한 계산양이 많은 암호화 알고리즘 대신 비교적 계산양이 적은 카오스 시스템을 이용함으로써 계산양을 더욱 감소시켰다. 영상 데이터의 변환 방법은 암호화할 부대역을 선택하여 영상데이터를 일정한 블록으로 만든 후 무작위로 좌/우 쉬프트 하는 방법과 두 가지 양자화 할당 방식(하향식-코드 할당방식/반향-코드 할당방식)에 따라 데이터를 교환하는 방식을 사용한다. 제안한 암호화 방법을 소프트웨어로 구현하여 약 500개의 영상을 대상으로 실험한 결과 원 영상 데이터를 부분적으로 암호화함으로써 원 영상을 인식할 수 없을 정도의 암호화 효과를 얻을 수 있음을 알 수 있었다. 구현한 하드웨어 암호화 시스템은 삼성 0.35㎛ 팬텀-셀 라이브러리를 사용하여 합성함으로써 게이트 수준 회로를 구성하였고 타이밍 시뮬레이션을 수행한 결과 100MHz 이상의 동작 주파수에서 안정적으로 동작함을 확인하였다.

Key Words : Image Encryption, Chaotic System, JPEG2000, DWT, Hardware.

ABSTRACT

In this paper, we proposed an image hiding method which decreases the amount of calculation encrypting partial data rather than the whole image data using a discrete wavelet transform and a linear scalar quantization which have been adopted as the main technique in JPEG2000 standard and then implemented the proposed algorithm to hardware. A chaotic system was used instead of encryption algorithms to reduce further amount of calculation. It uses a method of random changing method using the chaotic system of the data in a selected subband. For ciphering the quantization index it uses a novel image encryption algorithm of cyclical shifting to the right or left direction and encrypts two quantization assignment method(Top-down coding and Reflection coding), made change of data less. The experiments have been performed with the proposed methods implemented in software for about 500 images. The hardware encryption system was synthesized to find the gate-level circuit with the Samsung 0.35㎛ Phantom-cell library and timing simulation was performed, which resulted in the stable operation in the frequency above 100MHz.

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 하

※ 본 연구는 2005년도 한성대학교 교내연구비 지원과제임
* 한성대학교 정보통신공학과 (www.hansung.ac.kr, yhseo@hansung.ac.kr)
논문번호 : KICS2005-03-093, 접수일자 : 2005년 3월 8일

는 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].

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 이루어졌다. 이들 중 현재 상용화되어 사용 중인 표준은 ITU-T에서 제정한 H.263, ISO/IEC JPEG 계열의 JPEG 및 JPEG2000[4]과 MPEG계열 중 MPEG-2와 MPEG-4이다. 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(Discrete Wavelet Transform)[5]-기반 영상압축 방법이 개발되었으며, JPEG2000으로 표준화되면서 그 사용분야가 급격히 증가하고 있다.

1994년, Sullivan와 Baker는 원 영상을 압축 없이 공간영역 데이터를 암호화하는 방법을 제안하였는데[6], 이 방법은 영상의 특정 비트평면을 암호화하여 영상 데이터를 숨기는 방법이다. 원 영상의 각 화소가 8 비트로 표현되고 한 개의 비트평면만을 암호화한다고 해도 이 방법은 1/8에 해당하는 데이터를 암호화하여야 하므로 암호화에 의한 시간과 비용이 과다하다. 2000년 Dang와 Chau는 quadtree-기반의 SPHIT[7]를 겨냥하여 두 번의 순환과정(iteration) 결과 데이터를 암호화는 방법[8]을 제안하였으며, 1996년 Said와 Pearlman는 EZW[9] 방법에 대해 ATM 패킷 단위로 암호화를 적용하는 방법[10]을 제안하였다. 암호화에 소요되는 시간과 경비를 줄이는 또 하나의 방법으로 기존의 암호화 알고리즘 대신 계산양이 적은 특정 방법을 사용하는 연구 또한 진행되고 있다. 1997년 Fridrich는 베이커 맵(Baker map)을 이용한 위치교환 방식의 암호화 방법[11]을, 2003년 Salleh는 베이커 맵을 이용한 위치교환 방법에 암호화키를 이용한 암호화 방법[12]을 각각 제안하였는데, 이 방법들은 암호화 전과 후의 데이터의 분포의 변화가 많아서 암호화 후 엔트로피 코딩 시 압축률 손실이 매우 크다. Belkhouche와 Qidwai는 카오스 맵을 이용한 위치 교환 방식[13]을 이용한 암호화를 수행하였고, 2001년 Ammar와 Al Kabbany는 RNS(Residue Number System)을 발생시켜 암호화하는 방법[14]을 제안하였으며, Maniccam[15]와 Bourbakis[16]는 스캔 패턴을 조절하여 암호화하는 방법을 1999년과 2003년에 각각 제안하였으나, 암호화 정도에 따라 압축률 손실이 과다하여 압축과정에서 사용하기에는 적합하지 않다.

Ⅱ. 제안한 암호화 알고리즘

2.1 암호화 알고리즘

본 논문에서 제시한 암호화 알고리즘은 영상전체가 아닌 영상의 일부분만 암호화하고 암호화 되는 부분 영상의 양을 환경에 따라 선택하는 선택적 부분 암호화 방법이다. 이 알고리즘에서 암호화되는 부분 영상은 리프팅 변환된 결과의 부대역 중 일부를 선택하여, 그 중 최저주파수 영역의 데이터는 좌/우 쉬프트 방법으로 암호화하고 다른 부대역에서는 카오스 값을 발생시켜 선형양자화 과정과 함께 코드 변환 방법으로 암호화한다. 리프팅 변환 결과의 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 경우는 암호화에 소요되는 처리시간 때문에 전체 영상처리시간에 큰 영향을 줄 수 있으며, 특히 무선통신 등의 제한적 환경에서는 암호화 및 복호화 과정으로 인한 지연시간과 전력소모는 큰 장애요소가 되고 있으므로, 가능하면 암호화 양을 최소로 하는 것이 바람직하다. 본 논문에서는 4-레벨 DWT를 수행하는 것으로 가정하고 4가지 방법[17]으로 부대역을 부분적으로 선택하여 암호화할 데이터양을 줄인다.

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

n 레벨 2DDWT를 수행하는 경우 레벨 k의 한 부대역(LLk, HLk, LHk, HHk)의 크기 Z_k는 식 (1)이고 이 때 Z_0은 원영상의 크기를 나타낸다. 그러므로 4-레벨의 2DDWT를 수행한 경우 레벨 4의 각 부대역은 원영상의 1/28=1/256의 크기에 해당하며, 원영상의 데이터양에 대비한 암호화양은 1/256, 1/128, 1/64, 1/32에 해당한다.

$$Z_k = \frac{1}{2^{2k}} Z_0,\ 1 \le k \le n \qquad (1)$$

본 논문에서 제안하는 최저주파수 대역의 암호화 방법은 다음과 같다. 먼저, 카오스값 $x(n)$을 식 (3)에 의해서 2z개의 $b(k), (0 \le k \le 2z-1)$ 값으로 나타낸다.

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

여기서 z는 임의의 자연수이며, $x(n)$의 소숫점 아래 2z자리까지 사용함을 의미한다. 이 $b(k)$값들을 사용하여 웨이블릿 계수 W_j에 대해 p_j(암호화 방향을 나타내는 파라메터)와 q_j(암호화 양을 나타내는 파라메터)를 식 (3)과 (4)로 각각 계산한다.

$$p_j = b(2j) \qquad (3)$$

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

여기서 α, β 그리고 초기값인 $x(0)$, r는 이 암호화 시스템의 비밀키로 사용된다. 또한 g mod h는 g에 대한 modulo-h 연산을 뜻하며, t는 웨이블릿 계수의 비트 수를 나타낸다. 이 값들에 의한 W_j의 암호화는 식 (5)로 수행된다.

$$W_j' = \begin{cases} W_j << q_j, & p_j = 0 \\ W_j >> q_j, & p_j = 1 \end{cases} \qquad (5)$$

여기서 W_j'는 W_j를 암호화한 결과를 나타내며, <<와 >>는 왼쪽-쉬프트-회전과 오른쪽-쉬프트-회전을 각각 나타낸다. 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. 이 암호화 방식에서 α, β, $x(0)$ 그리고 r을 암호화키로 사용하는데, 카오스 시스템의 특성상 이 값들을 모르면 p_j값과 q_j값의 유추가 거의 불가능하다.

최저주파수 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[17]. 선형 양자화를 이용한 암호화 방식을 그림 1에 나타내었다.

```
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 1. 최저주파수대역 외의 부대역에 대한 암호화 방법
Fig. 1. Encryption method for the subbands except the lowest frequency subband

2.2 영상 암호화 및 복호화

그림 2에서 4-레벨 DWT를 수행하는 것으로 가정하고 최저주파수 대역(LL4) 및 그 외의 부대역에 대한 암호화 및 복호화 과정을 흐름도로 나타내었다. 원 영상을 리프팅 변환한 후 양자화하여 각 부대역별로 QX 값을 구한다. 먼저 암호화를 수행하기 위해서는 암호화할 부대역을 선택하고, 부대역 LL4 영역과 다른 부대역을 구별해서 암호화를 수행한다. 암호화된 데이터는 EBCOT를 거쳐 암호화된 영상 압축 데이터의 형태로 전송된다. 복호화 과정은 암호화과정의 역순으로 진행된다.

2.3 점진적 전송에 따른 영상 암호화

JPEG2000에서는 EBCOT 코딩 중 Tier 2과정에

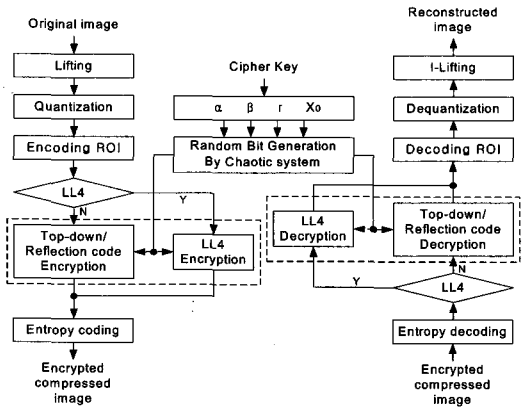


그림 2. 영상 암호화/복호화 과정; (a) 암호화, (b) 복호화
Fig. 2. Image encryption/decryption procedure; (a) encryption, (b) decryption

```
Progressive_Encrypt(){
 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 = (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 (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 3. 점진적 전송에 따른 영역 암호화 방법
Fig. 3. Regional encryption methods for progressive transmissions

서 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 3에 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 2-1절에서 제안한 알고리즘에 의해 암호화한다. ROI 영역이 설정 되지 않을 경우는 전체 비트평면에서 일정한 블록의 데이터를 모아서 암호화한다. 암호화 된 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 block size만큼의 데이터만으로 복호화를 수행한다.

Ⅲ. 제안한 알고리즘의 하드웨어 구조

그림 4에 암호화 시스템이 삽입된 JPEG2000 영상압축기의 구조를 나타내었다. 암호화기는 ROI와 EBCOT 사이에 삽입한다. 사용자에 의해 $x(0)$, r 값이 결정되면 카오스 시스템에 의해 $x(n)$이 얻어진다. 그리고 변수 결정 블록에서 α, β에 의해 p_j, q_j값이 정해지고 그 값에 따라 암호화 블록에서 암호화가 이루어진다. 카오스 시스템의 연산에서 소수점 이하 비트들이 미치는 영향을 그림 5에 나타내었다. 분기도형의 모양이 소수점 이하 비트가 증가할수록 카오스 성질을 만족하는 것을 알 수 있다. 카오스 성질에 만족하는 암호화키 r을 결정하게 되는데 그 값이 3.5이상을 선정하게 된다. 이때 그림 5에서 r이 3.5이상의 수렴 값의 분포가 소수점 이하 비트가 16bit 이상일 때 많이 분포한다. 이를 바탕으로 하드웨어 구현을 위한 수 체계를 확립하였다. 본 논문에서는 소수점 이하 비트를 16bit로 하여 암호화기를 설계하였다.

그림 6은 카오스 시스템의 하드웨어 구조를 나타내고 있다. 암호화에 사용될 쉬프트 방향(p_j)와 그 정도(q_j)는 그림 8에 나타낸 것과 같아 그림 7에서 생성된 $x(n+1)$을 α와 β값으로 결정한다. 이렇게 생성된 p_j와 q_j값에 따라 쉬프트 레지스터에서 데이터가 암호화되며, 이것을 그림 8에 나타내었다.

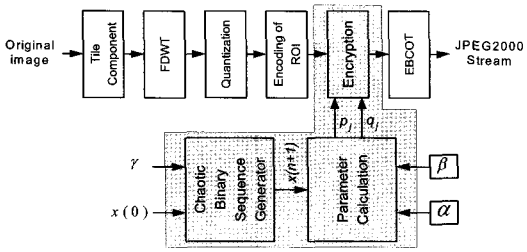


그림 4. 제안한 암호화 시스템이 삽입된 JPEG2000의 구조
Fig. 4. The structure of JPEG2000 including the proposed encryption system

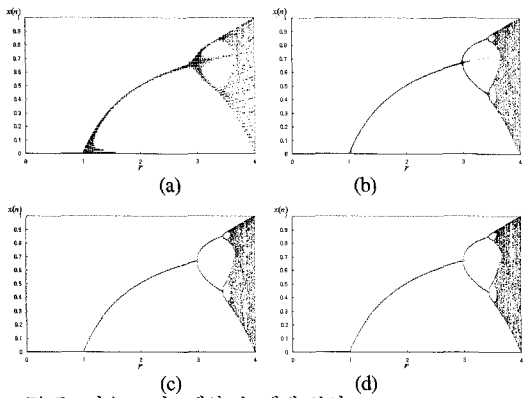


그림 5. 카오스 시스템의 수 체계 분석
Fig. 5. Precision analysis of chaotic system.

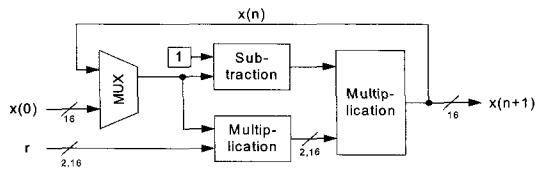


그림 6. 카오스 시스템의 구조
Fig. 6. The structure of chaotic system

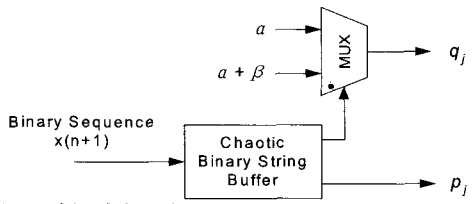


그림 7. 변수 결정 모듈
Fig. 7. variable decision module

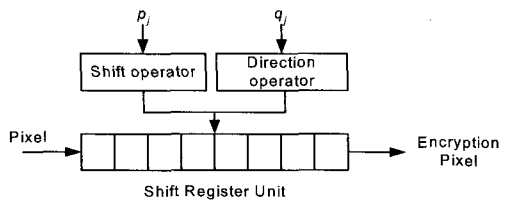


그림 8. 암호화기 내부 블록도
Fig. 8. Internal structure of encryptor

Ⅳ. 실험 및 하드웨어 구현 결과

본 논문에서 영상의 선택적 부분 암호화 방법은 그 동작과 성능을 분석하기 위해 C++언어로 구현하였으며, 실험환경은 Pentium IV 2GHz의 CPU이었다. 암호화 키는 $\alpha = 6$, $\beta = 12$, $x(0) = 0.75$, $r = 3.75$를 사용하였다.

4.1 실험 결과

2장에서 언급한 각 부대역 조합에 대해 III장의 최저주파수 영역 및 기타 부대역의 암호화방식을 적용한 Lena영상들을 그림 9에 나타내었다. 그림 9(a)의 원 영상에 대해서 그림 9(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 인지정도를 실험한 결과 대부분의 영상을 인식하지 못하였다. 따라서 일반적으로 영상의 재사용을 막기 위한 용도로는 LL4만을 암호화하여도 충분함을 알 수 있었다. 그림 9(c) 및 (d)는 각각 9.39388dB 및 9.40163dB의 PSNR값들을 가지는데 가시적인 효과를 고려하면 하향식-코드 할당방식으로 암호화한 영상이 반향-코드 할당방식으로 암호화한 영상보다 암호화 효과가 좋음을 알 수 있다. 500여개의 테스트 영상을 실험한 결과를 표 1에 나타내었다. 영상과 PSNR을 비교할 때 암호화하는 양이 많을수록 그에 따른 암호화 효과가 좋아지는 것을 알 수 있고, 하향식-코드 할당방식과 반향-코드 할당방식을 비교할 때 하향식-코드 할당방식이 더욱 암호화 효과가 좋다는 것을 알 수 있으나, 반향-코드 할당방식이 암호화 후 데이터의 분포에서 알 수 있듯이 압축률이 높다는 것을 알 수 있다.

그림 10에서는 3.3절에서 제안한 방법으로 JPEG 2000의 SNR scalability에 대한 실험결과를 나타내

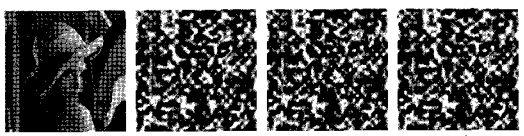
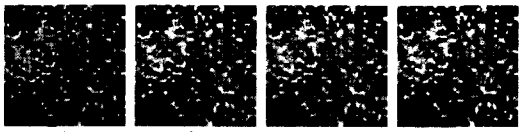


그림 9. a부대역별로 암호화한 영상; (a) 원 영상, (b) LL4, (c) Level4-HH3(하향식-코드 할당방식) (d) Level4-HH3(하향식-코드 할당방식)을 암호화한 영상
Fig. 9. Lena example by the proposed schemes; (a) original image, image encrypted (b) only for LL4, (c) for Level4-HH3 by Top-down method, (d) for Level4-HH3 by Reflection-code method



(a) (b) (c) (d)

그림 10. SNR scalability의 점진적 전송을 위한 암호화 영상; (a) 3비트 전송(9,39dB), (b) 6비트 전송(9.82dB), (c) 9비트 전송(9.89dB), (d) 16비트 전송(9.90dB)

Fig. 10. Encrypted images for progressive transmission with SNR scalability; (a) 3bits transmission(9,39dB), (b) 6bits transmission(9.82dB), (c) 9bits transmission(9.89dB), (d) 16bits transmission(9.90dB)

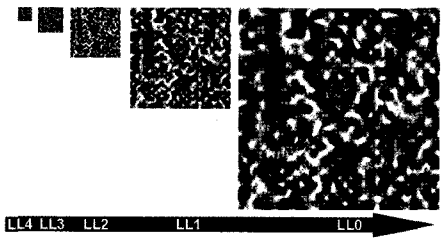
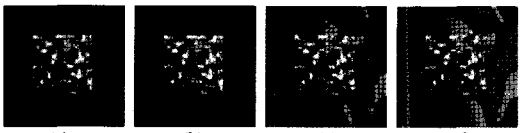


그림 11. Resolution scalability의 점진적 전송을 위한 암호화 영상

Fig. 11. Encrypted images by progressive transmission with resolution scalability



(a) (b) (c) (d)

그림 12. SROI 영역을 암호화한 영상에서의 점진적 전송; (a) 5비트 전송, (b) 13비트 전송, (c) 17비트 전송, (d) 27비트 전송

Fig. 12. Progressive transmission in image that encrypt ROI area (a) 5bits transmission, (b) 13bits transmission, (c) 17bits transmission, (d) 27bits transmission

고 있다. 전송 비트수에 무관하게 암호화 효과는 거의 일정하며, 오히려 적은 비트 전송률의 경우 가시적인 암호화 효과는 더욱 뚜렷함을 알 수 있다. 그림 11은 resolution scalability의 결과를 나타낸 것이다. LL4 전송할 경우에는 LL4만 암호화하고, LL3를 전송할 때에는 LL4와 HH3를 암호화하거나 Level 4를 암호화한다. LL2, LL1, LL0를 전송할 때는 Level4와 HH3를 암호화하여 전송에 따른 암호화 비율을 조절할 수 있다.

그림 12에서는 영상 가운데를 ROI로 설정한 후 ROI 영역을 암호화한 영상을 점진적 전송한 영상들을 나타내고 있다. 여기서는 max-shift방법[4]으로 13비트를 쉬프트하는 것을 가정하였다. 즉, 실험에 사용된 화소당 비트수는 14비트이고 이 영상을 max-shift하면 ROI 설정된 영상의 화소당 비트수는 27비트가 된다. 그림 12(a)는 이 중 5, (b)는 13, (c)는 17, (d)는 27 비트를 전송하여 복원한 영상을 각각 나타내고 있다.

영상 암호화에 대한 암호화 효과는 기존의 연구들과 비교한 결과를 표 2에 나타내었다. 영상에 대해서 원래의 영상과의 왜곡 정도를 PSNR로 판단하는 것이 보통이지만 PSNR이 15dB이하일 경우는 영상의 시각적 판단과 PSNR간의 상관도가 매우 작다. 공간 영역에서 암호화를 수행한 연구[6]에서는 원 영상에 대해 최소 1/8의 데이터를 암호화한다. 쿼트트리(quad-tree)를 이용한 연구[9]는 13~27%의 암호화 율을 나타내고, 쿼드트리에 SPHIT를 적용한 방식은 두 번의 코딩 패스에 대한 암호화를 수행할 경우에 2~5%의 암호화율을 나타낸다. 또한 DWT의 부대역간 제로트리를 이용한 방식[8]은 30dB의 PSNR을 가질 수 있는 압축률에서 약 1:30 이상의 암호화율을 가진다. 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.

표 1. 제안된 암호화 방식에 따른 실험 결과

Table 1. Experimental results by the proposed encryption schemes

Item case	Encryption ratio	random bit	PSNR (dB)	Compression ratio	Error 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	1:56.89	9216	8.27257	19.05	21.18

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
Fridrich[11]	Spacial domain	1:1
Salleh[12]		
Belkhouche[13]		
Ammar[14]		
Maniccam[15]		
Bourbakis[16]		
Sullivan[6]		1:8
Said[10]	Frequency domain	1:3.7 ~ 1:7.69
Dang[8]		1:30
Ours		1:256 ~ 1:56.89

표 3. 구현한 암호화 시스템의 하드에어 사용량
Table 3. Amount of hardware use in the implemented encryption system

Part	Number of gates
Chaotic System	4,870
Parameter Calculation	221
Encryption	1,138
Total	6,229

표 4. 제안한 암호화 알고리즘과 다른 암호화 알고리즘과의 하드웨어 사용량 비교
Table 4. Comparison the amount of the used hardware of the proposed encryption algorithm

Encryption Algorithm	Target Technology	Number of gates
AES	Hynix 0.25um	40,521
SEED		23,333
Triple-DES		23,425
Chaotic System	Samsung 0.35um	6,229

4.2 하드웨어 구현결과

제안된 카오스 시스템의 암호화 알고리즘은 HDL (Hardware Description Language)을 사용하여 설계하였고, 삼성 0.35㎛ 라이브러리를 이용하여 Synopsys™의 디자인 컴파일러로 합성하여 하드웨어를 구현하였다. 구현된 회로는 6,229개 게이트를 사용하였다. 적은 양의 하드웨어 자원을 이용하기 때문에 하드웨어적인 오버헤드가 거의 발생하지 않으면서 실시간으로 비디오 영상을 처리하는 실시간 코덱들에 이식이 가능한 솔루션이 될 수 있을 것으로 사료된다. 설계한 암호화 시스템의 하드웨어 양을 표 2에 보였는데, 이 암호화 시스템이 이식된 영상압축 프로세서[18]는 약 5만게이트를 사용하여 암호화시스템은 약 12%의 하드웨어를 사용하였다. 표 3에서는 다른 암호화 알고리즘과 게이트 수를 비교하였는데, 표에서 알 수 있듯이 본 논문에서 사용하는 암호화 알고리즘은 다른 알고리즘에 비해 5~10%의 작은 하드웨어를 사용한다는 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. 제안한 암호화 시스템은 HDL로 설계하였고 삼성 0.35㎛ 팬텀-셀 라이브러리를 이용하여 Synopsys™의 디자인 컴파일러로 합성하여 하드웨어로 구현하였다. Cadence™의 NC-Verilog를 이용하여 타이밍 시뮬레이션을 수행한 결과 동작주파수 200MHz 이상에서 안정적으로 동작함을 확인하였다. JPEG2000 Part 8에서 영상암호화를 적용한 JPSEC(Secure JPEG 2000) 기반 컨텐츠 보호 방식으로 사용될 수 있을 뿐만 아니라 다양한 분야에서 좋은 솔루션으로 제공될 수 있다.

참 고 문 헌

[1] Chisalita, I. and Shahmehri, N, "Issues in image utilization within mobile e-services", IEEE Workshop on Mobile Internet and e-Business Applications, Boston, USA, pp. 62-67, Jun. 2001.

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

[3] R. M. Rao, and A, S. Bopardikar, "Wavelet Transforms, 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] R. M. Rao and A. S. Bopardikar, "Wavelet

Transforms, Introduction to Theory and Application", Addison-Wesley, Reading, Sep. 1998.

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

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

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

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

[10] 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, Vol. 6, Issue 3, pp. 243-250, Jun. 1996.

[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, 25-28 May 2003.

[13] Belkhouche, F., Qidwai, U., "Binary image encoding using 1D chaotic maps", IEEE Region 5, 2003 Annual Technical Conference, pp. 39-43, 11 Apr. 2003.

[14] Ammar, A., Al Kabbany, A., Youssef, M., Amam, A., "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 Mar. 2001.

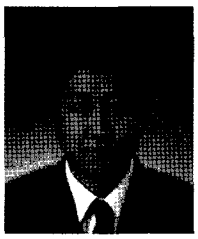
[15] S. S. Maniccam, N. G. Bourbakis., "SCAN Based Lossless Image Compression and Encryption.", IEEE Transactions, Image Processing, Vol. 3, No. 5, pp. 490-499, Sep. 1999.

[16] Bourbakis, N.; Dollas, A., "SCAN-based compression encryption hiding for video on demand", Multimedia, IEEE , Vol. 10, Issue 3, pp. 79-87, Jul.-Sep. 2003.

[17] 서영호, Sujit Det, 김동욱, "웨이블릿 영역에서의 선택적 부분 영상 암호화", 한국통신학회 논문지 Vol. 28, No. 6C, pp. 648-658, 2003. 06.

[18] Young-Ho Seo, Wang-Hyun Kim, Ji-Sang Yoo, Dai-Gyoung Kim and Dong-Wook Kim, "A real-time image compressor using 2-dimensional DWT and its FPGA implementation", Trans. of IEICE, VolE87-A, No. 8. Aug. 2004.

서 영 호(Young-Ho Seo) 정회원



1999년 2월 광운대학교 전자재료공학과 졸업(공학사)
2001년 2월 광운대학교 일반대학원 졸업(공학석사)
2000년 3월~2001년 12월 인티스닷컴(주) 연구원
2004년 8월 광운대학교 일반대학원졸업(공학박사)
2003년 6월~2004년 6월 한국전기연구원 연구원
2004년 12월~2005년 8월 유한대학 연구교수
2005년 9월~현재 한성대학교 전임강사
<관심분야> 2D/3D 영상 및 비디오 처리, 디지털 홀로그램, SoC 설계, 워터마킹/암호화
e-mail : yhseo@hansung.ac.kr