디지털산업정보학회 논문지 제14권 제2호-2018년 6월
http://dx.doi.org/10.17662/ksdim.2018.14.2.049

웨이브렛 패킷 변환의 특성을 이용한 영상 암호화 알고리즘

신 종 홍*

Image Cryptographic Algorithm Based on the Property of Wavelet Packet Transform

Shin Jonghong

〈Abstract〉

Encryption of digital images has been requested various fields. In the meantime, many algorithms based on a text - based encryption algorithm have been proposed. In this paper, we propose a method of encryption in wavelet transform domain to utilize the characteristics of digital image. In particular, wavelet transform is used to reduce the association between the encrypted image and the original image. Wavelet packet transformations can be decomposed into more subband images than wavelet transform, and various position permutation, numerical transformation, and visual transformation are performed on the coefficients of this subband image. As a result, this paper proposes a method that satisfies the characteristics of high encryption strength than the conventional wavelet transform and reversibility . This method also satisfies the lossless symmetric key encryption and decryption algorithm. The performance of the proposed method is confirmed by visual and quantitative. Experimental results show that the visually encrypted image is seen as a completely different signal from the original image. We also confirmed that the proposed method shows lower values of cross correlation than conventional wavelet transform. And PSNR has a sufficiently high value in terms of decoding performance of the proposed method. In this paper, we also proposed that the degree of correlation of the encrypted image can be controlled by adjusting the number of wavelet transform steps according to the characteristics of the image.

Key Words : Wavelet Packet, Image Encryption, Image Decryption, Degree Correlation

Ⅰ. 서론

암호화 기법은 보안이 보장되지 않는 네트워크를 경유해서 전송이 되거나 저장매체로 저장되는 데이터를 보호하는 효과적인 기술이다. 그래서 암호화의 목적은 인가되지 않은 사용자들로부터 정보를 은닉하는 것이다. 암호화 기술은 많은 발전을 했지만 충

* 숭실사이버대학교 전기공학과 부교수

분한 목적 동기와 많은 시간 그리고 풍부한 자원이 있으며, 비인가자나 비인가 단체에 의해서 해독될 수 있다. 결과적으로 암호화 기술이 발전함에 따라 암호 해독 기술도 동반해서 발전을 하고 있다.

디지털 영상의 암호화는 최근 다양한 분야에서 많이 응용이 되고 있다. 그런데 대부분의 디지털 영상 암호화알고리즘은 기존 텍스트 기반 암호화 알고리즘 시스템을 그대로 사용하고 있다. 그러나 디지털 영상 데이터의 특성은 텍스트 데이터의 특성과는 차이가 크며, 또한 디지털 영상의 데이터의 양은 일반적으로 텍스트 데이터의 양보다 훨씬 크다. 따라서 전통적인 텍스트 기반 암호화 알고리즘 방법들은 디지털 영상 암호화에 효과적으로 적용되어 사용하기가 어렵다. 이러한 이유로 인해서 효율적인 디지털 영상 암호화 알고리즘에 대한 개발이 요구되고 있다.

디지털 영상 암호화 방법은 압축 기술과 동일하게 손실과 무손실의 암호화 방법으로 분류가 된다. 손실 암호화 방법은 디지털 영상의 상세부분이 어느 정도 왜곡되는 것이 허용된다. 그래서 복호화된 디지털 영상은 원본의 디지털 영상과는 동일하지 않고 어느 정도의 차이가 존재한다. 물론, 암호화 수행 과정에서 발생한 작은 왜곡은 인간의 시각적 특성을 고려하였기 때문에, 사용되는 분야에 따라서 무시되고 수용할 수 있다. 무손실의 암호화 방법은 암호화 과정에서 어떠한 왜곡도 허용하지 않는 방법이다. 따라서 복호화 영상은 원본 영상과 동일한 영상을 유지한다. 이 방법은 의료 영상, 항공우주산업 영상, 개인정보 영상들과 같이 고품질 영상들을 필요로 하는 분야에서 사용된다.

또한 디지털 영상 암호화 알고리즘들은 순서나 위치를 변경하는 위치 순열, 화소의 값을 변경하는 수치 변환 그리고 시각적 변환 등의 세 개로 분류될 수 있다. 위치 순열과 수치 변환은 기존의 텍스트 암호화 알고리즘에서 사용되는 공통된 방법이지만 시각적 변환은 영상 암호화 알고리즘에서만 고유하게 사용되는 방법이다. 이산 코사인 변환(Discrete Cosine Transform: DCT)은 디지털 영상 변환 기술의 대표적인 방법이다. 그리고 다른 방법으로 이산 웨이브렛 변환(Discrete Wavelet Transform: DWT)이 있다.

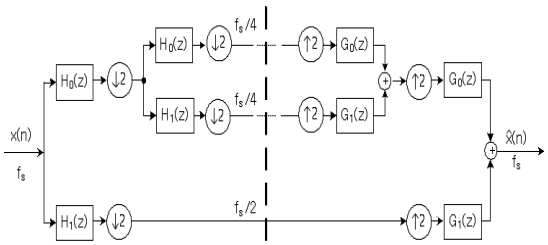
본 논문에서는 이산 웨이브렛 변환의 다른 실행 방법인 이산 웨이브렛 패킷 변환(Discrete Wavelet Packet Transform: DWPT)영역에서 전통적인 무손실 암호화 및 복호화 기술을 제안하였다. 이산 웨이브렛 패킷 변환은 디지털 입력 영상을 이산 웨이브렛 변환보다 더 많고 다양한 부대역 영상들로 분해할 수 있다. 이산 웨이브렛 패킷 변환으로 생성된 부대역 영상들의 계수는 위치 순열, 수치 변환 그리고 시각적 변환 알고리즘에 의해서 암호화 될 수 있다. 디지털 영상의 복호화 과정에서는 분해된 부대역 영상들의 계수에 암호화의 반대처리를 통해서 원 영상으로 복원을 한다. 그렇지만 제안된 복호화 알고리즘을 이용하지 않고 다른 복호화 방법 이용하는 경우 결코 원래의 영상으로 재생될 수 없다.

본 논문의 구성으로 2장에서는 웨이브렛 패킷 변환의 실행과 구성 그리고 웨이브렛 패킷 계수의 특징을 설명한다. 3장에서는 제안된 암호화 알고리즘과 복호화 알고리즘 수행 과정을 설명한다. 그리고 4장에서는 제안된 알고리즘의 성능을 기존의 이산 웨이브렛 암호화 방법과 비교 평가하는 실험과 그 결과를 제시하였다. 마지막으로 5장에서는 본 연구에 대한 결론과 향후 연구방향을 제시하였다.

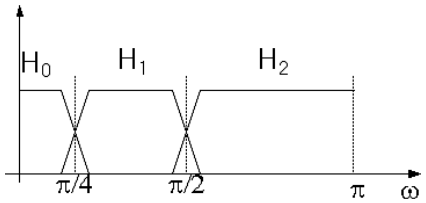
Ⅱ. 웨이브렛 패킷 변환

필터 뱅크(filter bank)는 실행 구조에 따라 등가

의 대역폭으로 분할되거나 비 등가 대역폭으로 분할된다[1]. <그림 1>의 dyadic tree구조 또는 octave band 구조는 저주파 대역만을 연속적으로 분할하는 방법으로, 결과적으로 이 과정이 이산 웨이브렛 변환을 수행한다. <그림 2>는 dyadic tree 구조의 주파수 응답으로 연속적으로 저주파 부분이 계속해서 분할되는 것을 확인할 수 있다. 저주파 신호의 특성을 더욱 정밀하게 분석할 수 있는 특성을 보여준다.

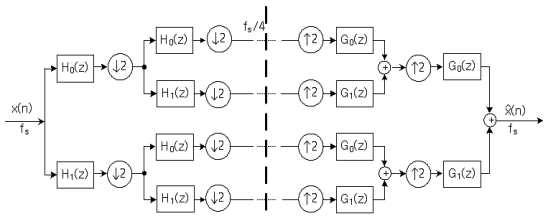


<그림 1> dyadic tree 구조

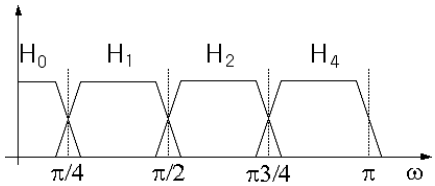


<그림 2> dyadic tree 구조의 주파수 응답

한편, <그림 3>과 같이 전 구간을 동일한 주파수 대역으로 분할하는 방법을 full binary tree구조 실행 방법이라고 한다. 이 방법은 고주파 대역에서도 저주파 대역에서와 마찬가지로 연속적인 주파수 분할을 진행하게 되는데, 이 과정을 이산 웨이브렛 패킷 변환이라고 한다. 따라서 웨이브렛 패킷 변환 시스템은 고주파 성분에서도 높은 정밀도를 갖는다. 그리고 가변적인 주파수 분해 능력을 가지고 있어서 적응적인 특별한 신호나 그룹에 가장 부합되는 대역 분할을 제공해 주는 것이 가능하다[2]. <그림 4>는 full binary tree구조의 주파수 응답을 나타낸 것으로 전 대역이 균일하게 분할이 진행되는 것을 확인할 수 있다. 따라서 고주파 성분도 정밀한 분석을 가능하게 한다.

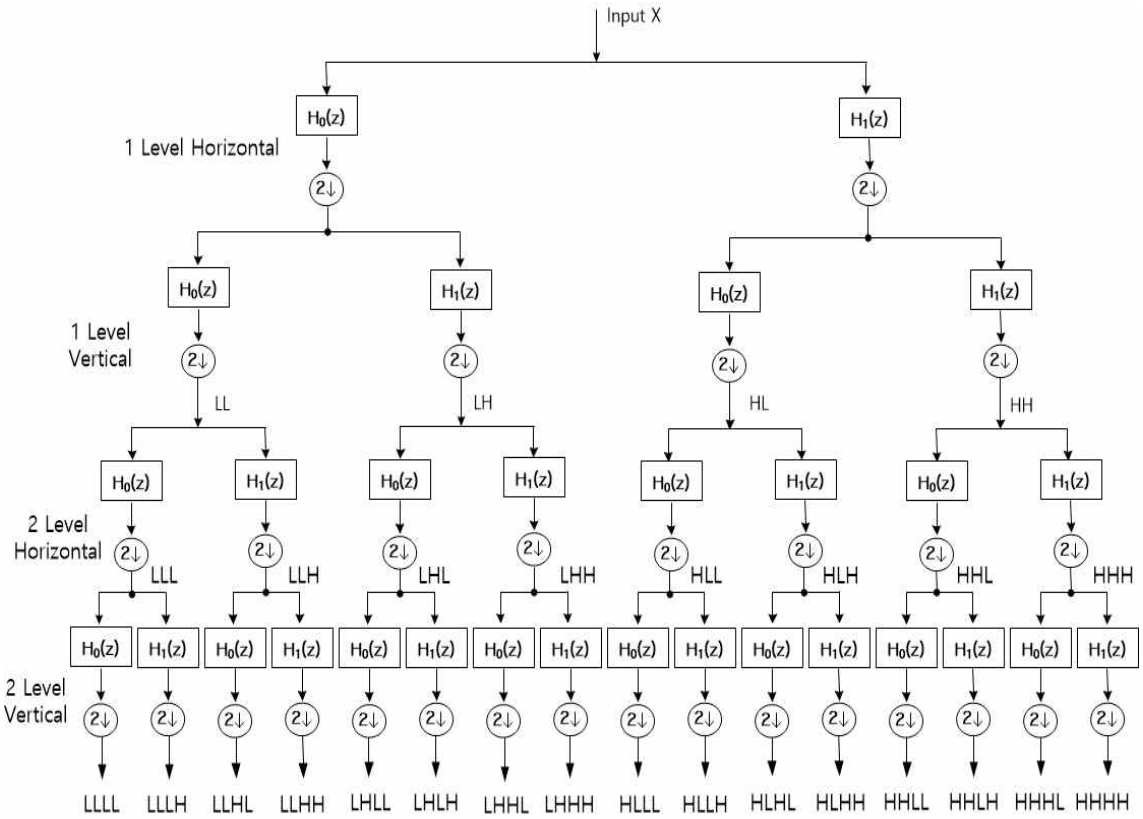


<그림 3> full binary tree 구조



<그림 4> full binary tree 구조의 주파수 응답

이산 웨이브렛 패킷 변환을 2차원의 디지털 영상에 적용하려면, 이산 웨이브렛 변환과 동일하게 디지털 영상을 수직 방향으로 필터 뱅크에 입력한 후, 그 출력이 연속해서 수평 방향으로 필터 뱅크에 입력되어 처리되는 분리 가능의 2차원 이산 웨이브렛 패킷 변환이 사용된다. 그러나 분리 가능 이산 웨이브렛 변환보다 고주파 영상에 대한 처리가 추가되므로 복잡도가 더 높다. <그림 5>는 2차원 이산 웨이브렛 패킷 변환을 2 단계(level)로 수행한 것을 나타낸다. 1 단계에서 총 4개의 부대역 영상이 생성되는 것은 웨이브렛 변환과 동일하며 각 주파수 성분도 동일하다. 그래서 LL은 가장 낮은 저주파 부대역 영상의 계수를 나타내며, LH, HL, HH는 순차적



<그림 5> 2단계 2차원 이산 웨이브렛 패킷 변환 실행

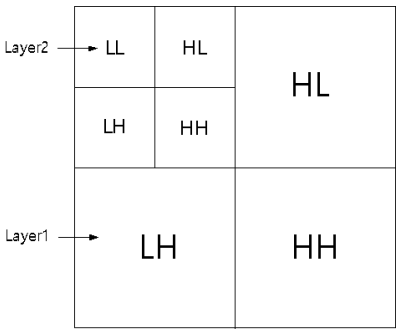
으로 높은 주파수 부대역 영상의 계수를 생성하게 된다. 따라서 4개의 부대역 영상들이 함께 조합되면 원 영상의 모든 주파수 정보를 구성되는 것이다. 최저 주파수 LL 계수 값의 특징은 디지털 영상의 가장 중요한 부분이 포함되어 있어, 가장 큰 에너지 값을 갖는다. 그래서 에너지 값이 작은 나머지 부대역 영상 LH, HL, HH의 계수 값들과의 구별이 충분히 가능하다.

그렇지만 고주파 성분을 포함하고 있는 LH, HL, HH 부대역 영상의 계수 값들은 아주 작은 에너지 값으로 분해되었기 때문에 서로간의 계수의 구별이 어렵다.

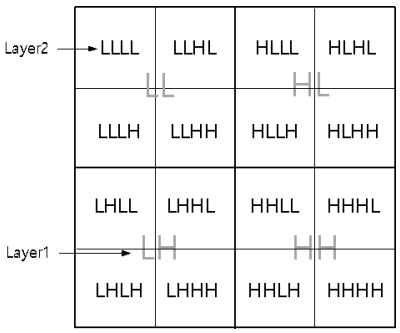
전통적인 이산 웨이브렛 변환에서는 <그림 1>과 같이 에너지 값이 큰 최저 주파수 LL만 연속적으로 분할하여 LL만의 정밀도를 높이지만, 이산 웨이브렛 패킷 변환에서는 고주파 성분들에 대해서도 정밀도를 높이기 위해서 LH, HL, HH에 대해서도 연속적인 분할을 진행하게 된다. 디지털 영상에 대한 2차원 이산 웨이브렛 패킷 변환을 2단계까지 진행하게 되면 <그림 5>과 같이 총 16개의 부대역 영상으로 분해가 된다. 생성된 16개의 부대역들은 1단계에서 생성된 부대역들의 주파수 특성을 상속하게 된다.

따라서 $LLLL$은 최저주파수가 되고 $HHHH$는 최고주파수가 된다.

<그림 6>은 2차원 이산 웨이브렛 변환을 2단계 수행하여 얻어진 디지털 영상의 대역 분할된 모습을 나타낸 것으로 이 구조를 octave tree구조라고 한다. 1차원 이산 웨이브렛 변환과 마찬가지로 저주파 대역만 계속적으로 분해되는 구조라는 것을 확인할 수 있다. <그림 7>은 2차원 이산 웨이브렛 패킷 변환을 2단계 수행을 통해서 얻어진 디지털 영상의 대역 분할된 모습을 나타낸 것이다. 1단계의 진행과정까지는 2차원 이산 웨이브렛 변환과 동일한 결과를 얻지만 2단계가 진행되는 동안 저주파 영역의 분해뿐만 아니라 고주파 전 영역까지 분해가 계속되어서 총 16개로 분할된 full binary tree구조가 형성되는 것을 확인할 수 있다.

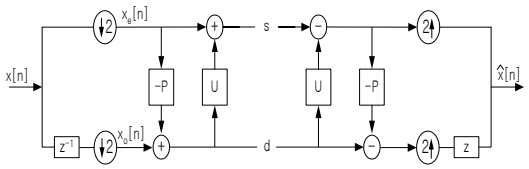


<그림 6> 2단계의 Octave Tree Band



<그림 7> 2단계의 full binary Tree Band

리프팅(lifting) 웨이브렛 이론은 웨이브렛 변환의 다위상(polyphase) 표현에서 다위상 행렬들을 Euclidean 알고리즘을 사용하여 인수분해를 통해 predict와 update단계로 나누어 실행하는 방법이다. 그래서 리프팅 웨이브렛 변환은 <그림 8>과 같이 곱셈과 과정 없이, 덧셈과 지연 연산만으로 간단하게 실행될 수 있다[3]. 본 논문에서는 디지털 영상에 대한 암호화를 고속으로 수행하기 위해서 리프팅 웨이브렛 변환을 사용하였다.



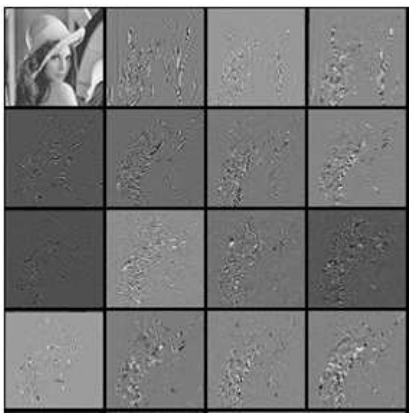
<그림 8> predict와 update의 리프팅 단계 블록도

Ⅲ. 제안 알고리즘

3.1 암호화 알고리즘

제안된 암호화 알고리즘을 수행하기 위한 첫 번째 수행 과정에서는 필터 길이 7탭의 분석 필터를 사용하여 2차원 이산 웨이브렛 패킷 변환을 수행 하여서 <그림 7>과 같이 입력 영상을 다양한 부대역 영상들로 분해한다. 2차원 이산 웨이브렛 패킷 변환 1 단계에서는 최저 주파수의 부대역 영상 LL_1과 상세 계수의 부대역 영상들 LH_1과 HL_1 그리고 HH_1으로 분해된다. 그리고 2차원 이산 웨이브렛 패킷 변환 2 단계를 진행하면 $LLLL$부터 $HHHH$까지 총 16개의 부대역 영상들이 생성된다. 2차원 이산 웨이브렛 패킷의 단계의 수는 성능을 위해서 가변적(K 레벌)으로 수행한다. 두 번째 수행 과정에

서는 필터 길이 8탭의 분석필터를 이용하여 2차원 이산 웨이브렛 패킷 변환을 수행한다. 필터의 길이를 다르게 한 것은 암호화 강도를 위해서 복잡도를 증가시킨 것이다. 이때 입력 부대역 영상은 첫 번째에서 분해된 최저주파수 부영상 LL_1의 집합이다.



<그림 9> 3단계 2차원 웨이브렛 패킷 변환으로 생성된 LL_1의 부대역 영상 집합

LL_1의 부대역 영상 집합은 첫 번째 과정에서 몇 단계로 수행되었는지 따라서 구성이 다르다. <그림 9>에서는 3단계로 진행했을 때의 Lenna 영상의 LL_1의 부대역 영상 집합을 나타낸 것이다.

두 번째 2차원 이산 웨이브렛 패킷 변환에서는 LL_2와 LH_2, HL_2, HH_2의 부대역 영상 집합이 생성된다. 실질적인 암호화 처리의 처리는 LL_2, LH_2, HL_2, HH_2의 부대역 영상 집합에서 적용이 된다. 암호화 처리의 첫 번째 과정은 부대역 영상 집합들 중에서 LL_2의 부대역 영상 집합들의 계수 값들을 다른 나머지 부대역 영상 집합의 계수 값들과 구별이 되지 않도록 LL_2의 부대역 영상 집합의 계수 값들을 설정하는 것이다. 그래서 LL_2 의 부대역 영상 집합의 계수 값을 $(m_2 \times n_2)$으로 나누는 것이다. 여기서, m_2과 n_2은 LL_2 부대역 영상 집합의 크기 행렬을 나타낸다. 따라서 LL_2의 부대역 영상 집합의 총합이 평균값으로 떨어지게 된다[4].

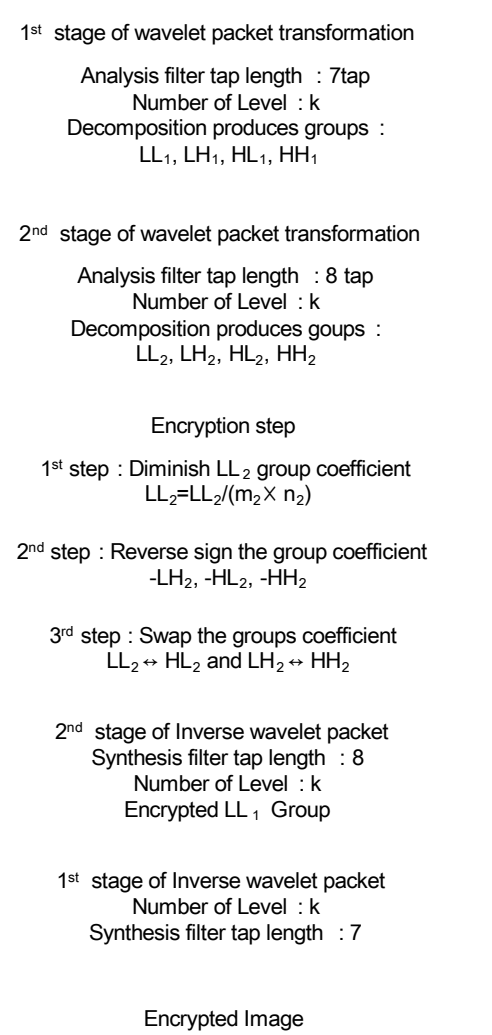
$$LL_2(i,j) \Rightarrow \frac{LL_2(i,j)}{(m_2 \times n_2)} \quad (1)$$

암호화 과정의 두 번째 과정에서는 LL_2의 부대역 영상 집합을 제외한 LH_2, HL_2, HH_2의 부대역 영상 집합들의 계수 값들에 (-1)을 곱하여 부호를 반전 시킨다. 이 과정은 부대역 영상 집합 내에서 가장 어두운 값과 가장 밝은 값을 반전시켜서 암호화의 강도를 높인 것이다. 암호화의 세 번째 과정에서는 LH_2의 부대역 영상 집합과 HH_2의 부대역 영상 집합을 서로 바꾸고 그리고 LL_2 부대역 영상 집합과 HL_2 부대역 영상 집합을 서로 바꾸는 전치과정이다[5].

마지막으로 분해되었던 부대역 영상의 집합을 역 2차원 이산 웨이브렛 패킷 변환을 통해서 다시 합성을 한다. 먼저 8탭의 합성 필터을 이용하여 역 이산 웨이브렛 패킷 변환을 수행하여 LL_1의 부대역 영상 집합을 재구성한다. 재구성한 LL_1은 암호화된 부대역 영상의 집합이다. 그리고 7탭의 합성 필터를 이용하여 역 이산 웨이브렛 패킷 변환을 수행하여 최종의 암호화된 영상을 생성하게 된다. <그림 10>은 제안된 영상의 암호화 알고리즘 처리 과정을 나타낸 것이다.

3.2 복호화 알고리즘

암호화된 영상에 대한 복호화 알고리즘은 암호화 알고리즘의 반대로 처리가 진행된다. 그래서 암호화된 영상으로부터 영상 원본이 갖고 있는 상세 부분을 드러나게 한다. 이 목적을 위해서 첫 번째 과정에서는 길이 7탭의 분석필터를 이용하여 2차원 이산 웨이브렛 패킷 변환을 수행한다. 암호화 과정



<그림 10> 제안된 영상 암호화 알고리즘의 처리 과정

과 마찬가지로 최저 주파수의 부대역 영상 집합 LL_1과 상세 계수의 부대역 영상 집합들 LH_1, HL_1, HH_1을 생성한다. 그리고 부대역 영상의 집합 LL_1에 대해서 길이 8탭의 분석필터를 이용하여 두 번째 과정의 2차원 이산 웨이브렛 패킷 분해를 수행하여 LL_2와 그리고 LH_2, HL_2, HH_2의 부대역 영상 집합들을 생성한다. 이 때, 실행되는 단계의 수는 암호화 과정과 동일한 수로 진행된다. 부대역 영상 집합들의 이산 웨이브렛 계수에 대한 복호화 과정은 암호화 과정의 반대로 진행된다. 첫 번째 단계에서 LH_2와 HH_2의 부대역 영상 집합을 서로 교환하고 LL_2와 HL_2의 부대역 영상 집합을 서로 교환한다. 두 번째 단계에서는 LH_2, HL_2, HH_2의 부대역 영상 집합의 계수 값들의 부호를 반전시키기 위해서 각 계수 값들에 (-1)을 곱한다. 마지막 단계는 암호화 단계에서 사용한 동일한 가중치 인자를 다음과 같이 LL_2에 곱하여 원래의 에너지 크기 값으로 복원한다[4].

$$LL_2(i,j) \Rightarrow LL_2(i,j)(m_2 \times n_2) \qquad (2)$$

마지막 과정에서는 필터 길이 8탭의 합성 필터를 이용하여 역 2차원 이산 웨이브렛 패킷 변환을 수행하여 LL_1의 부대역 영상 집합을 복원한다. 그리고 길이 7탭의 합성 필터를 이용하여 역 2차원 이산 웨이브렛 패킷 변환을 수행하여 복호화된 영상을 생성한다. 제안된 암호화 알고리즘은 무손실 암호화 기법을 만족해야 하므로 복호화된 영상의 화소들은 원래의 영상의 화소와 동일한 값을 갖는다. <그림 11>은 제안된 복호화 알고리즘 처리 과정을 나타낸 것이다.

Encrypted Image

1st stage of wavelet packet transformation

Analysis filter tap length : 7tap
Number of Level : k
Decomposition produces groups :
LL_1, LH_1, HL_1, HH_1

2nd stage of wavelet packet transformation

Analysis filter tap length : 8 tap
Number of Level : k
Decomposition produces goups :
LL_2, LH_2, HL_2, HH_2

Decryption step

1st step : Swap the groups coefficient
$LL_2 \leftrightarrow HL_2$ and $LH_2 \leftrightarrow HH_2$

2nd step : Reverse sign the group coefficient
$-LH_2$, $-HL_2$, $-HH_2$

3rd step : Grow LL_2 group coefficient
$LL_2 = LL_2 \times (m_2 \times n_2)$

2nd stage of Inverse wavelet packet
Synthesis filter tap length : 8
Number of Level : k
Decrypted LL_1 Group

1st stage of Inverse wavelet packet
Number of Level : k
Synthesis filter tap length : 7

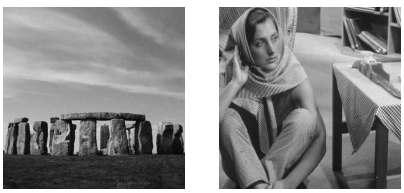
Decrypted Image

<그림 11> 제안된 복호화 알고리즘의 처리 과정

Ⅳ. 성능 실험 결과

본 논문에서는 제안된 방법의 성능을 분석하기 위해서 시각적인 확인 실험과 정량적인 해석 실험을 수행하였다. 제안된 방법을 위한 실험에 사용된 실험 디지털 영상은 통계적인 특성이 잘 알려진 8비트 그레이 영상을 사용하였다. 그리고 영상의 크기는 256×256 화소를 사용하였다. <그림 12>는 실험 영상을 나타낸 것이다.

(a) Lenna (b) Peppers



(c) Stone (d) Barbara

<그림 12> 실험 영상

실험 성능을 정량적으로 평가하기 위해서 상호 상관 함수(cross-correlation function) 값과 첨두 신호대 잡음비(Peak Signal to Noise Ratio) 값을 사용하였다. 상호 상관 함수는 두 신호 사이에 얼마나 유사성이 있는지를 나타낸 것으로, 암호화된 영상 신호가 원래의 영상 신호와 얼마나 유사한지를 측정한다. 따라서 정량화된 성능판단을 수행하게 된다. 식(3)은 두 신호 x(t)와 y(t)에 대해서 상호 상관 함수를 정의한 것이다.

$$R_{xy}(\tau)=\int_{-\infty}^{\infty} x(\tau)y(t+\tau)dt \qquad (3)$$

첨두 신호대 잡음비는 복호화된 영상이 원본 영상과 얼마나 동일한 정도를 측정하기 위해서 사용된다. 식(4)는 두 영상 신호에 대한 첨두 신호대 잡음비를 정의한 것이다.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \qquad (4)$$

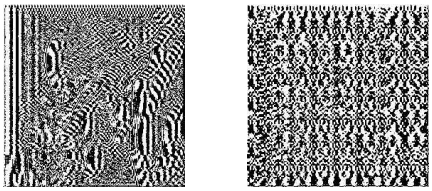
255는 화소의 첨두 값을 나타내며, MSE(mean square error)는 평균 제곱 오차로 식(5)와 같다.

$$MSE=\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \| I(i,j)-k(i,j) \|^2 (5)$$

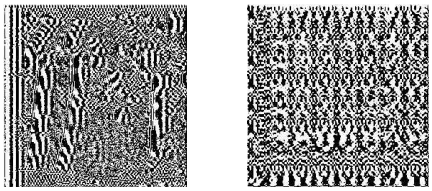
여기서, $I(i,j)$는 원 영상, $k(i,j)$는 복원 영상을 나타낸다.

2차원 이산 웨이브렛 패킷 변환은 5단계를 수행하여 LL_1 부대역 영상 집합을 조밀하게 분해하였다. 단계 수가 증가하면 연산의 복잡도가 증가하지만 많은 부대역 영상들로 분해가 되어서 암호화의 강도를 증가할 수 있다. 암호화가 되기를 원하는 디지털 영상의 여러 가지 특성에 따라서 단계의 수를 조정할 수 있고 암호화된 영상은 원 영상을 유추하기 어렵게 할 수 있다.

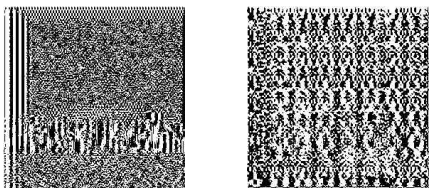
<그림 13>은 일반 2차원 이산 웨이브렛 변환을 수행하고 암호화한 영상(WT 암호)과 2차원 이산 웨이브렛 패킷 변환을 수행하고 암호화한 영상(WP 암호)을 시각적으로 비교한 것이다[6]. 2차원 이산 웨이브렛 변환으로 암호화한 영상은 동일한 암호화 방법을 적용했음에도 불구하고 원래의 영상을 유추할 수 있도록 어느 정도 윤곽이 살아있는 것을 확인할 수 있다. 그러나 2차원 이산 웨이브렛 패킷 변환으로 암호화된 영상들은 원본의 영상을 전혀 유추할 수 없도록 확실하게 암호화된 것을 확인할 수 있다.



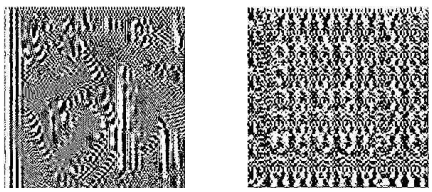
(a) Lenna WT 암호 (b) Lenna WP 영상



(c) Pepper WT 암호 (d) Pepper WP 암호



(e) Stone WT 암호 (f) Stone WP 영상



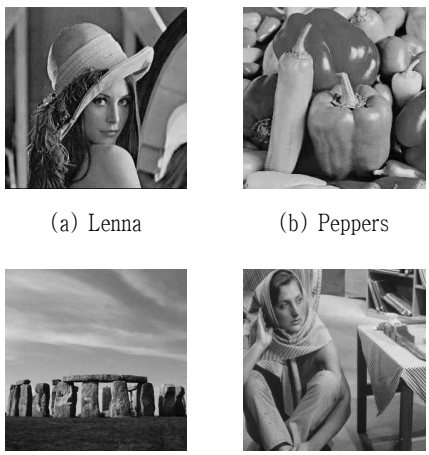
(g) Barbara WT 암호 (h) Barbara WP 암호

<그림 13> 실험 결과 영상

<그림 14>는 2차원 이산 웨이브렛 패킷 변환을 통해서 암호화 되었던 영상을 다시 복호화한 영상이

다. <그림 12>의 원본 영상과 비교 했을 때, 복호화된 영상들이 시각적으로 특별한 왜곡이 없다 것을 확인할 수 있다.

<표 1>은 제안된 방식의 정량적 평가를 위해 상호 상관(corr)과 첨두 신호대 잡음비(PSNR)를 계산한 것이다. 암호화 영상이 원래의 영상과 상호 상관이 작을수록 암호화 영상에서 원래 영상의 해독을 어렵게 한다. 따라서 상호 상관이 작은 값일수록 암호화 성능이 우수하다.



(a) Lenna (b) Peppers

(c) Stone (d) Barbara

<그림 14> 복호화된 실험 영상

<표 1>의 결과로부터 웨이브렛 패킷 변환[7]을 이용한 암호화 더 우수하다고 할 수 있다. Barbara 영상의 경우 영상의 복잡도가 높은 영상으로 5단계의 웨이브렛 패킷 변환의 상호 상관이 웨이브렛 변환 방법 보다 더 높지만 7단계로 수행 했을 경우에는 corr은 0.0041이고 PSNR은 214.3382로 더 좋은 결과를 얻을 수 있다.

PSNR은 복호화된 영상이 원래 영상과의 차이점을 정량적으로 비교한 것이다. 일반적으로 PSNR 30dB이상이면 시각적으로 차이를 구별하기 어렵다. 실험 결과 전부 200dB이상으로 계산과정에서 발생할 수 있는 오차를 제외하고 원래의 영상과 동일하게 복호화된 것을 확인할 수 있다. 따라서 제안한 영상의 암호화 알고리즘이 정량적으로 가역적 암호화 방식이라는 것을 확인할 수 있다.

<표 1> 암호 영상의 상관값과 복호 영상의 PSNR값

	image	Lenna	Peppers	Stone	Barbara
WT	corr	0.0071	0.0329	0.0577	0.0066
	PSNR	256.23	253.99	253.35	256.06
WPT	corr	0.0054	0.0215	0.0212	0.0158
	PSNR	233.03	226.16	229.30	229.97

Ⅴ. 결론

디지털 영상에 대한 암호화는 다양하게 요구되고 있다. 그 동안 텍스트 기반의 암호화 알고리즘을 기반으로한 다양한 방법들이 제안되었다. 본 연구에서는 디지털 영상의 특성을 활용하기 위해서 이산 웨이브렛 변환 영역에서 암호화하는 방법을 제안하였다. 특히, 암호화된 영상이 원래의 영상과의 유사성을 제거하기 위해서 2차원 이산 웨이브렛 패킷 변환을 사용하였다. 이산 웨이브렛 패킷 변환은 이산 웨이브렛 변환보다 더 많은 부대역 영상들로 분해할 수 있고 이 부대역 영상의 계수에 다양한 위치 순열, 수치변환, 그리고 시각 변환을 수행할 수 있다. 결과적으로 본 논문에서는 기존의 이산 웨이브렛 변환보다 암호화 강도가 높으면서 가역적인 특성을 그대로 유지할 수 있는 무손실의 대칭키 암호화와 복호화 알고리즘을 제안하였다. 제안된 방법의 성능은 시각적인 방법과 정량적인 방법을 통해서 증명하였다. 실험결과를 통해서 시각적으로 암호화된 영상이 원래 영상과는 전혀 다른 독립적인 신호로 보여지는

것으로 확인할 수 있었으며, 상호 상관도를 이용하여서도 기존의 이산 웨이브렛 변환을 이용한 것보다 더 낮은 수치를 보이는 것도 확인 하였다. 그리고 복호화 성능에서도 복화화 된 영상이 충분히 높은 PSNR 값을 갖는 것을 확인하였다. 또한 영상의 특성에 따라서 이산 웨이브렛 패킷 변환의 단계를 조정하여서 암호화된 영상의 상호 상관도를 적절하게 조절할 수 있다는 것도 제안하였다. 향후 연구 과제로 각 디지털 영상의 특성에 맞는 2차원 이산 웨이브렛 패킷 분할과 암호화를 통해서 연산의 복잡도를 줄이면서 암호화 강도를 높이는 연구가 더 필요하다.

참고문헌

[1] M. Y. Gokhale, DaIjeet Kaur Khanduja, “Time Domain Signal Analysis Using Wavelet Packet Decomposition Approach,” Int. J. communication, Network and System Science, 3, 2010, pp. 321-329.

[2] K. Ramchanandran, M. Vetterli, "Best wavelet packet bases in a rate-distortion sense," IEEE Trans. on Image Processing, Vol. 2, No. 2, April, 1993, pp. 160-175.

[3] Daubechies, I., W. Sweldens, "Factoring Wavelet transforms into lifting steps," Asilomar Conference on Signals, Systems, and Computers, 1997.

[4] Sara Tedmori, Nijad Al-Najdawi , “Image Cryptographic Algorithm Based on the Haar Wavelet Transform,” Information Sciences, Vol. 269, 2014, pp.21-34.

[5] Y. Chen “Cheating Prevention in Visual Cryptography,“ IEEE Trans. Image Process., Vol 21, No 7, 2012, pp.3319-3323.

[6] Park Byeonghoon, Lim Joonghee, Shin Jonghong, “Imaged Cryptographic Algorithm Based on the Lifting Wavelet Transform,“ 2015 The Korea Society of Digital Industry & Information Management Falling Proceeding, 21th Nov. 2015, pp.47-51.

[7] 신종홍, “웨이브렛 변환 계수의 특성을 이용한 생체 영상 암호화 알고리즘,“ 디지털산업정보학회논문집, 제12권,ㅁ 제2호, 2016, pp.41-49.

■ 저자소개 ■

신 종 홍
(Shin Jonghong)

2003년 3월~현재
숭실사이버대학교 전기공학과 교수

2002년 8월 홍익대학교 전기공학과 (공학박사)
1999년 2월 홍익대학교 전기공학과 (공학석사)
1997년 2월 홍익대학교 전기공학과 (공학사)

관심분야 : 멀티미디어 신호처리, 보안영상처리
E-mail : sigs@mail.kcu.ac

논문접수일 : 2018년 05월 30일
수 정 일 : 2018년 06월 04일
게재확정일 : 2018년 06월 05일