JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 12 : 2933~2942 Dec. 2015

쿼드트리 방식의 프레넬릿 변환을 이용한 영상의 암호화 기법

서영호[1*] · 이윤혁[2] · 김동욱[2]

A New Image Encryption Method using Quad-tree based Fresnelet Transform

Young-ho Seo[1*] · Yoon-hyuk Lee[2] · Dong-wook Kim[2]

[1*]School of Liberal Arts, Kwangwoon University, Seoul 139-701, Korea
[2]Department of Electronic Materials Engineering, Kwangwoon University, Seoul 139-701, Korea

요 약

본 논문에서는 이산 프레넬릿 변환(Fresnelet transform, FRNLT)을 이용하여 2차원 자연 영상의 중요 성분을 추적하고 암호화하는 방법을 제안한다. FRNLT을 통해서 얻어진 부대역의 특성을 분석하여 영상을 암호화하기 위한 정보를 추출한다. FRNLT 레벨, 부대역의 에너지, 그리고 시각적인 효과를 고려하여 암호화를 위한 최적화된 지점을 도축한다. 다양한 레벨과 암호화 영역을 선택함으로써 다양한 강도로 암호화가 가능하다. 암호화 효과는 정량적인 PSNR 결과, 암호화를 위한 CPU 시간, 암호화 영역의 크기, 그리고 시각적인 영향 등의 항으로 분석하여 경향성을 제시한다. 따라서 별도의 분석과정 없이 본 논문에서 제시된 파라미터를 이용하여 응용분야에 따라서 효율적으로 암호화를 수행할 수 있다. 실험결과를 살펴보면 $L_{TH}=4$이고 $E_{TH}=60$인 경우에 전체 데이터 중에서 0.42%만을 암호화하여도 원래의 영향을 분간할 수 없을 만큼 암호화 효과를 얻을 수 있었다.

ABSTRACT

This paper proposes a new method which traces significant element of 2-dimensional natural images and encrypts them by using Fresnelet transform (FRNLT). After analyzing property of the subbands obtained by the FRNLT, we estimated the information for ciphering 2D images. Considering FRNLT levels, energy of subbands, and visual effect, we estimated the optimized point for encryption. By selecting various levels and encrypting region, we can encrypt 2D image with various robustness. Encryption effectiveness was showed by analyzing numerical result, executing time for encryption, area of encrypted region, and visual observation. Therefore encryption for various application can be applied by using the suggested parameters without additional analysis. Identifying the experimental result, in the case of $L_{TH}=4$ and $L_{TH}=4$, an image was not recognized through encrypting only 0.42% among the entire data.

키워드 : 암호화, 이산 프레넬릿 변환, 쿼드트리, 부대역 에너지

Key word : Encryption, Discrete Fresnelet Transform, Quad Tree, Subband Energy

Received 19 August 2015, **Revised** 14 September 2015, **Accepted** 25 September 2015

*** Corresponding Author** Young-ho Seo(E-mail:yhseo@kw.ac.kr Tel:+82-2-940-5531)
School of Libral Arts, Kwangwoon university, Seoul 139-701, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2015.19.12.2933 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

영상/비디오 처리기술과 보안 및 보호 기술에 대한 연구는 여러 분야에서 다양한 접근방법으로 이루어지고 있으나, 각각의 솔루션들이 활발히 연구되고 있는 현재의 추세로 보면 앞으로는 프로토콜화된 통합 솔루션의 연구개발이 이루어질 것이며, 영상 및 비디오의 처리와 정보보안 및 보호의 통합 솔루션은 영상/비디오 응용분야의 핵심 기능이 될 것이라 전망할 수 있다.

최근에 다양한 네트워크 환경 기반의 안전한 멀티미디어 통신기술을 위한 멀티미디어 데이터의 암호화 방법이 제안되고 있다. 가장 많이 사용하는 멀티미디어 표준화 포맷인 MPEG[1-5]기반에 대한 연구는 오래 전부터 다양하게 진행되어 오고 있고, 이와 함께 웨이블릿 기반의 영상 암호화 방법도 지속적으로 발전되어 왔다[6-12]. 본 논문은 프레넬 변환과 웨이블릿 변환을 기반으로 하는 프레넬릿 변환을 기반으로 하는 영상 암호화 기법에 대해 논의하기 때문에 웨이블릿 변환 기반의 기법 위주로 설명하고자 한다. [6]에서는 퀴드트리를 기반으로 하는 SPHIT를 겨냥하여 암호화는 방법을 제안하였다. [7]과 [8]에서는 웨이블릿 변환 방식인 NSMRA (non-stationary multi-resolution analysis) 방법으로 각각 필터와 트리구조 변환을 통해 암호화를 수행하였는데 이러한 방법은 엔트로피 코딩의 하나인 산술 코딩을 목표로 하였다. [9]에서는 확률적인 암호화방법을 제안하였고, [10]에서는 [9]의 방법을 개선시켰다. [11]에서는 EZW 방법을 제안하였는데 ATM 패킷 방법을 적용하여 암호화를 수행하였다. [12]에서는 데이터를 변형하지 않고 데이터 자체를 암호화하는 방법을 시도하였는데, 영상의 중요한 비트 평면을 암호화하여 원 영상에서 1/8에 해당하는 적은 양의 데이터를 암호화였다.

[13]에서는 영상 암호화에 대한 기존의 연구들을 분석하였고, [14]에서는 다차원 부분 푸리에 변환(Factional Fourier Transform, FRFT)을 이용한 암호화 기법을 제안하였다. 입력된 영상을 몇 개의 영역으로 나눈 후에 각각을 특정 차원의 FRFT를 적용하여 암호화를 수행한다. 만일 동일한 조건과 키가 없다면 역 FRFT를 수행할 수 없어서 복원을 할 수 없도록 하였다. [15]에서는 입력된 영상을 베이커지도를 이용하여 무작위로 섞은 후에 이중 무작위 위상 코딩 기법(double random phase encoding, DRPE)을 이용하여 암호화하는 방식을 제안하였다.

본 논문에서는 광학신호처리를 위한 프레넬릿 변환(Fresnelet transform, FRNLT)을 2차원 영상에 적용하여 영상을 다해상도의 영역으로 구분한 후에 이 영역을 암호화하는 기법을 제안하였다. 제안하는 방법은 암호화하는 데이터의 양과 계산양의 서로 상보적인 관계가 있고 안전한 영상 전송을 하기 위해 암호화하는 데이터의 양을 적응적으로 조절하여 다양한 환경에서 적용하는 것이 가능하다[16]. 2장에서는 FRNLT 변환과 특성에 대해서 먼저 소개하고, 3장에서는 암호화 기법을 제안한다. 다음으로 4장에서 실험결과를 보이고, 5장에서 본 논문의 결론을 맺는다.

Ⅱ. 이산 프레넬릿 변환과 특성

프레넬 변환(Fresnel transform, FLT)은 식 (1)과 같이 입력으로부터 거리 z에 회절현상을 나타낼 수 있다. $f(x)$는 입력이고 $g(s)$는 출력이다. λ는 광원의 파장이고 Δx와 Δs는 입력과 출력의 화소의 크기이다.

$$g(s) = Ff(x), \quad F = \frac{\Delta s}{\sqrt{\lambda z}} UWV \tag{1}$$

$$U = diag[u_x] \quad u_x = \exp\left[\frac{j\pi}{\lambda z}(x\Delta x)^2\right]$$

$$V = diag[v_s] \quad v_s = \exp\left[\frac{j\pi}{\lambda z}(s\Delta s)^2\right]$$

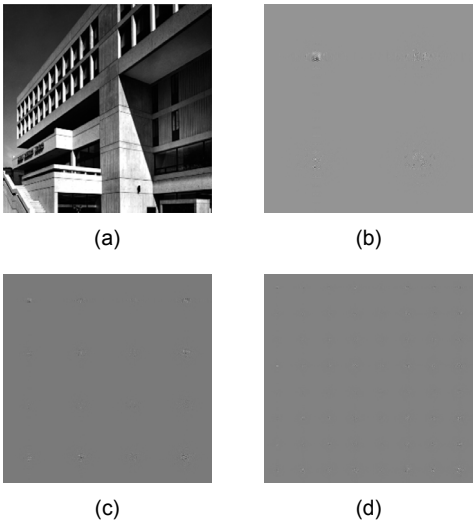
$$W = [w_{xs}] \quad w_{xs} = \exp\left[-\frac{j2\pi}{\lambda z}(x\Delta x)(s\Delta s)\right]$$

식 (1)의 프레넬 변환 필터 F을 식 2와 같이 각각 저대역 필터(F_0)와 고대역 필터(F_1)를 만들어 프레넬릿 변환(Fresnelet transform, FRNLT)을 수행할 수 있다. 식 (3)은 역 FRNLT을 위한 필터이다. L과 H는 웨이블릿 변환의 각각 저대역 필터와 고대역 필터이다. FRNLT 필터를 이용하여 변환을 하면 프레넬 도메인으로 출력되므로 1 레벨만 FLT 필터를 이용하고 이후 L과 H을 이용하여 웨이블릿 변환을 수행한다[17].

$$F_0 = \frac{\Delta s}{\sqrt{\lambda z}} LUWV, \quad F_1 = \frac{\Delta s}{\sqrt{\lambda z}} HUWV \tag{2}$$

$$F_0^* = \frac{\Delta x}{\sqrt{\lambda z}} V^* W^* U^* L^t, \quad F_1^* = \frac{\Delta x}{\sqrt{\lambda z}} V^* W^* U^* H^t \quad (3)$$

식 (2)를 이용하여 FRNLT를 통하여 나오는 부대역은 그림 1과 같이 확인 할 수 있다. 그림 2에 나타낸 FRNLT의 에너지 분포를 살펴보면 2차원 영상의 주파수 분해를 위한 변환과 다르다는 것을 확인할 수 있다. 이산 코사인 변환이나 이산 웨이블릿 변환을 자연영상에 적용할 경우에 일반적으로 저주파영역에 가장 많은 에너지가 분포하게 되는데 FRNLT를 적용할 경우에는 최고주파영역에 가장 많은 에너지가 분포하는 경향을 보인다.



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

Fig. 1 FRNLT image results (a) oritinal (MIT), (b) 1-level, (c) 2-level, (d) 3-level

Table. 1 Energy compaction HH region for levels of FRLNT

Transform Level	Ratio of energy compaction (%)
1	28.92
2	29.36
3	16.71
4	11.20
5	5.02
6	5.66
7	5.02

표 1에서는 FRNLT의 레벨에 따른 HH 영역(최고주파 영역)의 집중도를 나타내었다. FRNLT를 적용할 경우에 레벨이 높아짐에 따라 HH 영역에 집중도가 줄어드는 것을 확인 할 수 있다. 반면에 크기, 위상 형태의 변환할 경우에 크기는 레벨이 높아짐에 따라 HH 영역의 집중도가 높아지는 것을 확인 할 수 있으며, 이는 일반 2D 영상에서 나타나는 특징과 다른 경향을 보이는 것이다.

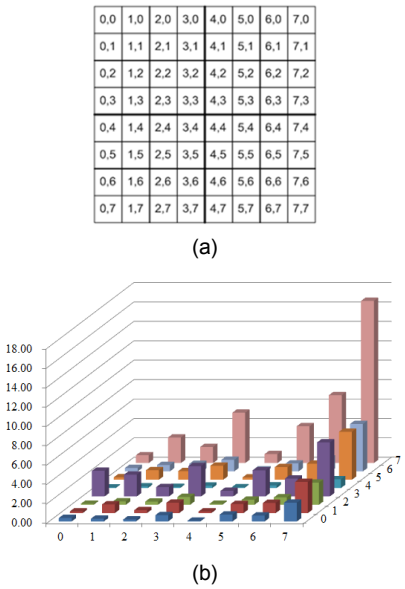


Fig. 2 Subband property (a) coordination of subband, (b) energy distribution in 3-level

Ⅲ. 제안한 암호화 기법

본 장에서는 영상을 위한 암호화 및 복호화 기법을 제안한다. 먼저 전체적인 과정을 소개하고, 다음으로 암호화 및 복호화 알고리즘을 설명한다. 그리고 암호화 과정을 위한 부대역 선택 알고리즘을 소개한다. 기본적인 암호화 방법은 [18]의 방식을 기반으로 한다.

영상을 암호화하기 위한 기존의 알고리즘들은 영상에 적응적이지 않다는 단점을 갖는다. 적응성이 없을 경우에는 알고리즘을 적용하는데 속도는 빠르지만 최적화는 되지 않는다. 속도와 최적화는 서로 상보적인 관계로 볼 수 있다. 영상의 어느 주파수 성분을 암호화

하였다면 역과정을 거친 후에 해당 주파수 성분을 공격할 여지가 있다. 이러한 취약성을 해결하기 위해서는 역과정의 추적은 어려워야 하고 암호화된 주파수 성분을 예측하기 어려워야 한다. [18]에서 제안된 기법은 이러한 조건을 충분히 만족하고 있어서 본 논문에서는 이를 기반으로 한 후에 여기에 FRNLT을 도입하고, 에너지분포를 통계화하여 암호화를 시도한다.

본 논문에서는 부대역을 쿼드트리 방식으로 주파수 대역을 분화시킨 후에 암호화를 수행하는데, 이러한 부대역 구조는 암호화된 주파수를 예측하기 어렵게 하고 역과정을 이용한 공격이 어렵다. 영상에 따라서 각각의 부대역에 대해 FRNLT를 수행하는데, 기준은 에너지의 중요도에 의존한다. 시각적인 인지도는 정보가 갖는 에너지의 량 및 부대역의 특성에 의존하기 때문에 가능하면 에너지가 높은 주파수 대역을 은닉하여 암호화 효과를 높이고자 한다.

3.1. 암호화 기법

제안한 암호화 알고리즘을 그림 3에 나타내었다. 영상을 4개의 부대역으로 변환하고, 4개의 부대역에 대해 각각 다시 FRNLT를 수행한다. 부대역들의 에너지 분포를 탐색하고, 다시 FRNLT를 수행할 부대역을 선정한다. 이러한 과정을 선택맵(selection map)과 우선순위맵(priority map)에 기록하여 탐색과정을 저장한다. 선택맵은 선택된 부대역에 대한 정보를 보유하고, 우선순위맵은 동일한 레벨에서 선택된 부대역들 중 어느 부대역이 암호화 우선순위가 높은지를 보유한다. 이러한 과정은 선택된 부대역들의 총 에너지값이 임계치(E_{TH})보다 클 때까지 계속 진행된다. FRNLT 레벨의 임계치(L_{TH})가 높아질수록 각 부대역의 크기와 에너지가 작아지기 때문에 에너지 임계치를 만족시키기 위해 선택되는 부대역의 개수는 증가하고 정밀하게 에너지 합계를 조절할 수 있다. 최종적으로 선택된 부대역들은 블록 암호화 알고리즘을 이용하여 암호화한 후에 역 FRNLT를 수행하여 암호화된 영상을 생성한다. 암호화 과정에서 생성된 선택맵, 우선순위맵, 그리고 블록 암호화 알고리즘의 암호키(cipher key)를 합쳐서 전체 보안키(secret key)가 된다. 이 보안키는 허가받은 사용자에게만 전달된다[18].

제안한 알고리즘으로부터 아래와 같이 디지털 영상의 암호화를 위한 다양한 정보화 솔루션을 제시한다.

- 암호화 효과의 판단을 위한 임계치 검출
- 영상을 구성하는 FRNLT 부대역 중에서 시각적으로 큰 영향을 미치는 성분의 검출
- 영상을 구성하는 FRNLT 부대역 중에서 에너지가 큰 성분의 검출
- 영상의 암호화를 위한 최적화된 암호화를 위한 부대역 및 동작시간의 제시
- 영상 암호화를 위한 FRNLT기반의 솔루션 제시

제안한 암호화 알고리즘에서 부대역을 선택하는 방법은 그림 4의 순서로 수행한다.

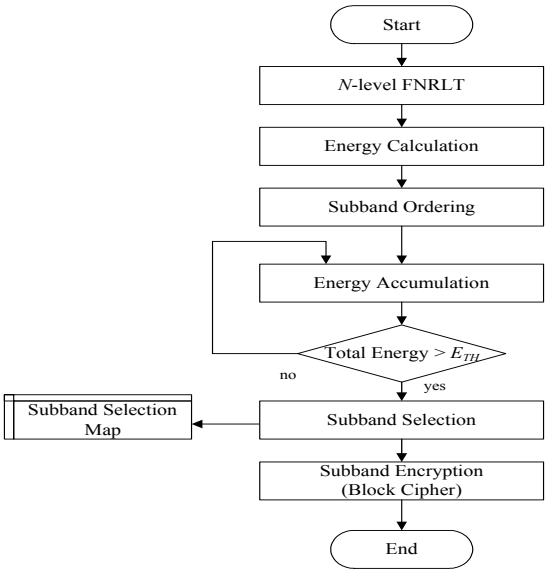


Fig. 3 Encryption procedure

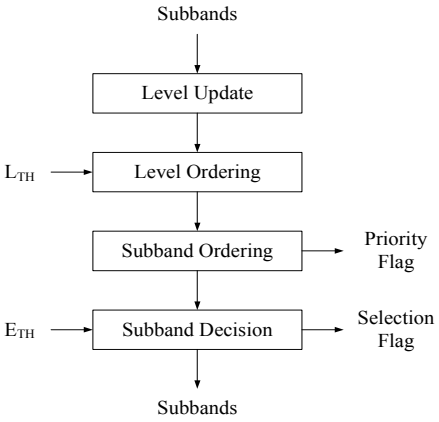


Fig. 4 Subband selection procedure

에너지 집중도가 높은 부대역을 추적하는 경우에 동일한 에너지를 갖는 부대역이 존재한다면 (LL, LH, HL, HH)의 순서로 우선 순위를 결정한다. L_{TH}에 의해 증가한 부대역에 대한 정보를 업데이트한 후에 L_{TH}에 따라서 생성되는 부대역들의 순서를 추적하여 Priority Map을 위한 Priority flag를 생성한다. 그리고 E_{TH}에 따라 부대역을 선택하고, Selection Map을 위해 Selection flag을 생성한다.

3.2. 복호화 기법

그림 5에는 영상을 복호화하는 절차를 나타내었다. 복호화 절차는 암호화 절차의 역과정이고 암호화 시 사용하였던 암호키를 그대로 사용하고, 암호화 과정에서 추출했던 선택맵과 우선순위맵을 이용한다[18].

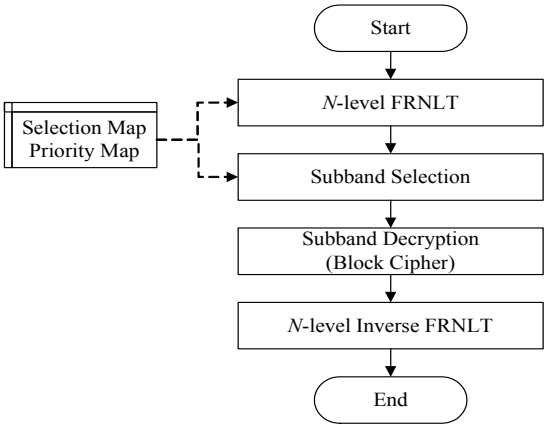


Fig. 5 Decryption procedure

Ⅳ. 실험 및 결과

4.1. 실험환경

제안한 암호화 기법을 다수의 영상에 적용하여 암호화 결과를 확인하였다. 먼저, 순방향 FRNLT를 이용하여 영상을 다양한 레벨의 부대역으로 변환하고, 앞 절에서 설명한 방법으로 부대역을 선택한다. 선택된 부대역의 계수들을 블록 암호화 알고리즘을 이용하여 암호화한다. 다음으로 역방향 FRNLT를 거쳐서 암호화된 영상이 생성된다. 암호화된 결과는 peak noise-to-signal ratio (PSNR)를 이용하여 정량적으로 확인하고, 시각적인 판단을 통해서 결과를 판단한다. PSNR은 식 (4)에 정의하였다.

$$PSNR(dB) = 10\log_{10}\frac{255^2}{\frac{1}{XY}\sum_{x,y}(I_{x,y} - I'_{x,y})^2} \quad (4)$$

본 실험에서는 FRNLT 과정 이후에 생성된 부대역 계수를 모두 암호화하지 않고 계수의 최상위 비트만을 암호화한다. 최상위 비트만을 암호화해도 전체 비트를 암호화한 것과 효과가 거의 유사하였다. 제안한 암호화 방법을 이용하여 암호화를 수행한 예를 그림 6에 나타내었다. 그림 6의 예는 $L_{TH} = 3$이고 $E_{TH} = 50$의 경우이다. $E_{TH} = 20$이지만 실제로 암호화된 에너지의 양은 49.4518%이고, PSNR은 2.43dB이다. 암호화된 부대역의 크기는 10.9375%이고, 최상위 비트 평면만을 암호화했기 때문에 암호화된 양은 0.48%이다. 그림 6(a)는 원본 영상을 나타내고, (b)는 선택된 부대역을 나타낸다. 그림 6(c)는 암호화 과정을 거친 부대역이고, 그림 6(d)는 암호화 후에 복원한 영상을 나타낸다. 전체 데이터에서 매우 소량의 데이터만을 암호화했음에도 불구하고 그림 6(d)와 같이 영상을 분간할 수 없을 정도로 암호화 효과가 뛰어나다. 또한 FRNLT 구조와 선택된 부대역에 대한 정보가 없다면 다시 복구할 수 없기 때문에 보안성이 매우 높다.

4.2. 정량적 결과분석

암호화 이후의 영상의 PSNR을 측정하여 그림 7에 그래프로 정리하였다. L_{TH}과 E_{TH}를 변화시키면서 100여장의 영상에 대해서 다양한 조건을 실험하였다. 결과를 살펴보면 PSNR 값이 L_{TH}과 E_{TH}에 대해 규칙성 있는 경향성을 갖는다는 것을 확인할 수 있다. E_{TH}가 증가하면 암호화 효과가 높다진다는 것을 확인할 수 있다. 즉, 많은 에너지를 암호화할수록 암호화 효과가 높다지는 경향성을 확인할 수 있고, 이는 모든 L_{TH}에 대해서 동일하게 적용된다는 것을 확인할 수 있다. 그러나 L_{TH}가 높다질수록 PSNR이 높아지는 것을 확인할 수 있는데 이는 암호화 효과가 낮아진다는 것을 의미한다. L_{TH}가 1과 2인 경우는 부대역을 세분화할 수 없어서 포함되는 에너지를 점층적으로 증가시킬 수 없다.

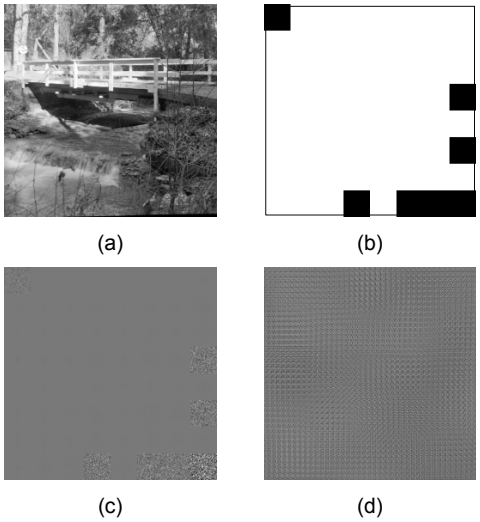


Fig. 6 Encryption procedure (a) original image (b) selected subbands (c) encrypted subbands (d) reconstructed image

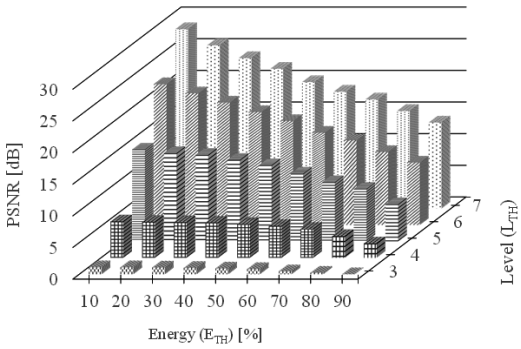


Fig. 7 Encryption PSNR result

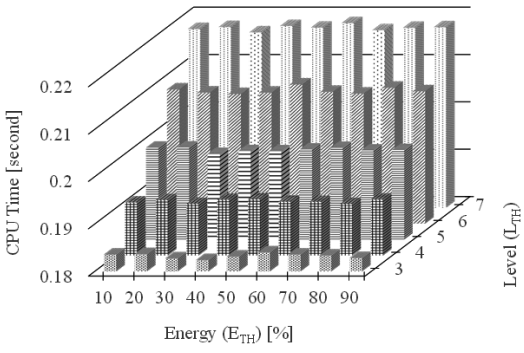


Fig. 8 Encryption time

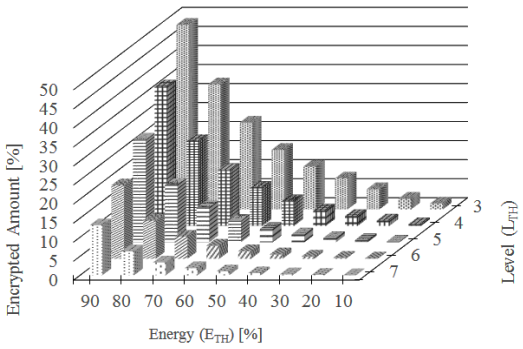


Fig. 9 Encrypted data

따라서 실험 결과에 포함시키지 않았다. L_{TH}가 3인 경우에는 PSNR이 매우 낮은 것을 확인할 수 있고, L_{TH}가 4인 경우에는 거의 PSNR이 일정하게 유지되다가 E_{TH}가 60일 때부터 낮아지는 것을 확인할 수 있다.

그림 8에는 암호화되는 동안 걸린 시간을 측정하여 정리하였다. L_{TH}가 높아질 경우에 FRNLT를 수행하는데 시간이 길어져서 CPU 시간이 증가하는 것을 볼 수 있다. E_{TH}에 따라서는 CPU 시간이 크게 변화하지 않는 것을 보면 암호화 시간보다 FRNLT를 수행하는 시간이 훨씬 큰 영향을 미친다는 것을 확인할 수 있다. 뿐만 아니라 그림 7과 8을 종합적으로 살펴보면 동일한 E_{TH}을 경우에 L_{TH}가 6 및 7과 같이 클 경우에 PSNR도 높고, 즉 암호화 효과도 낮으면서 CPU 시간도 많이 걸린다는 것을 알 수 있다.

그림 9를 살펴보면 암호화되는 데이터양은 L_{TH}가 작아질수록 늘어난다는 것을 확인할 수 있다. 그러나 그림 8에서 확인한 것과 같이 암호화시간보다 FRNLT에 소요되는 시간이 크기 때문에 암호화되는 데이터양은 크게 중요하지 않다는 것을 확인할 수 있다.

4.3. 시각적 결과분석

영상과 같은 시각적인 데이터에 대한 암호화 효과는 정량적인 결과만으로 판단하기 어렵다. 정량적으로 결과가 나쁘다 할지라도 시각적으로 구분이 된다면 알고리즘이 효과적으로 적용되었다고 볼 수 없기 때문이다.

그림 10을 살펴보면 E_{TH}가 동일하다 할지라도 L_{TH}에 따른 암호화 효과는 다르다는 것을 확인할 수 있다. 암호화 영상 결과를 살펴보면 동일한 E_{TH}이라면 L_{TH}

가 낮을수록 암호화 효과가 높다는 것을 확인할 수 있다. 즉 적절한 정도의 L_{TH}에서 적절한 크기의 부대역이 선택될 경우에 암호화 효과가 높다고 해석할 수 있다. 여기에서 적절한 L_{TH}는 4에 해당하는 것으로 판단할 수 있다.

4.4. 부대역의 선택

E_{TH}와 L_{TH}의 값을 조절하여 다양한 암호화 방법이 가능하다. 그림 11은 $E_{TH}=60$이고 $L_{TH}=4$ 인 경우에 선택된 부대역들을 나타낸다. 모든 경우에 대해서 최저 주파수 대역은 포함시켰다. 최저 주파수 대역은 에너지의 양에 상관없이 전체 영상의 평균 주파수를 나타내므로 암호화 시 포함시킨다. $E_{TH}=60$는 앞 절에서 선택된 에너지 값으로 이유는 이 정도의 에너지 이상이면 모든 L_{TH}에 대해서 전체적인 영상을 분간할 수 없었기 때문이다. L_{TH}는 4일 경우에 가장 효율적으로 암호화 효과가 나타났기 때문에 선택하였다.

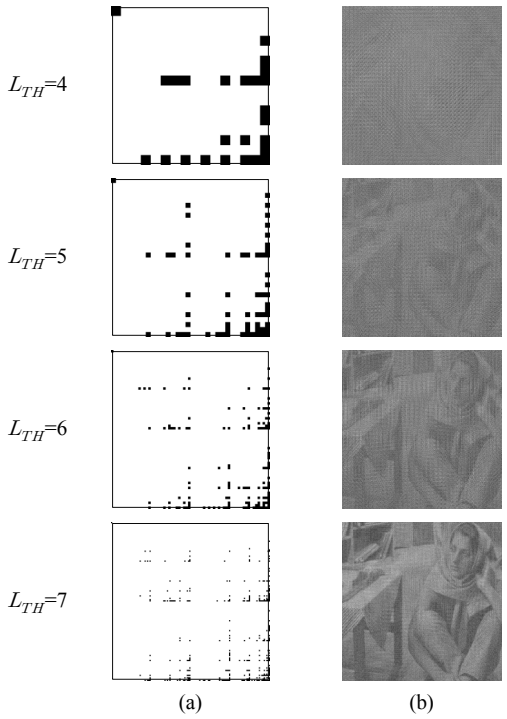


Fig. 10 Ciphering effect for L_{TH} in the case of E_{TH}=60 (a) selected subbands, (b) encrypted images

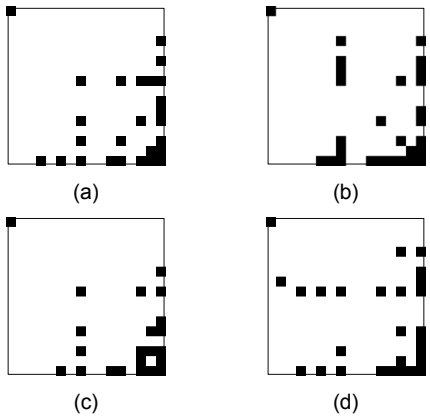


Fig. 11 the selected subbands in the case of $E_{TH}=60$ and $L_{TH}=4$ (a) Bridge (b) Lena (c) Map (d) MIT

그림 12에는 모든 경우에 대해서 선택된 부대역의 영역을 나타냈다. E_{TH}의 증가에 따라서 선택되는 부대역 영역은 당연히 증가한다. 또한 L_{TH}가 증가할수록 선택되는 부대역 영역은 감소한다. 다시 말하면 부대역을 세세하게 분해할수록 에너지를 더욱 세밀하게 나누고 에너지를 더욱 소수의 부대역으로 집중시킬 수 있다는 것을 의미한다. 그러나 앞서 살펴본 실험결과에 따르면 에너지를 세밀하게 나누었다고 해서 암호화 효과가 높아지지 않는다.

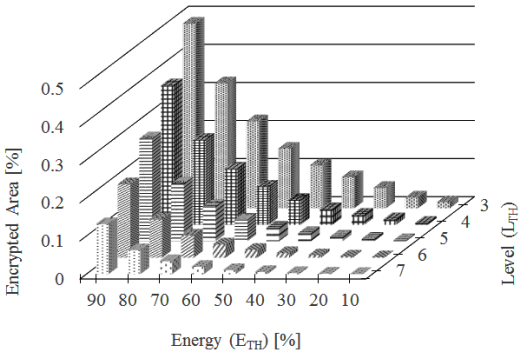


Fig. 12 The number of the selected subband for encryption

4.5. 암호화 효율

L_{TH}와 E_{TH}에 따른 암호화 영역과 PSNR간의 관계를 그래프로 그림 13에 정리하여 암호화 효율에 대한 설명을 하였다. E_{TH}가 증가함에 따라서 PSNR은 감소

한다. 즉, 암호화 효과가 높아진다. 그러나 암호화 영역이 증가하면서 CPU 시간이 커지게 될 것이다. 그림 13의 그래프를 이용하여 응용 분야에 따라서 적절한 지점을 선택하여 암호화를 적용할 수 있을 것이다.

L_{TH}에 따른 최상위 비트 위치를 표 2에 나타냈다. 즉, 암호화된 데이터의 값은 그림 9의 결과를 표 1로 나누어야 한다.

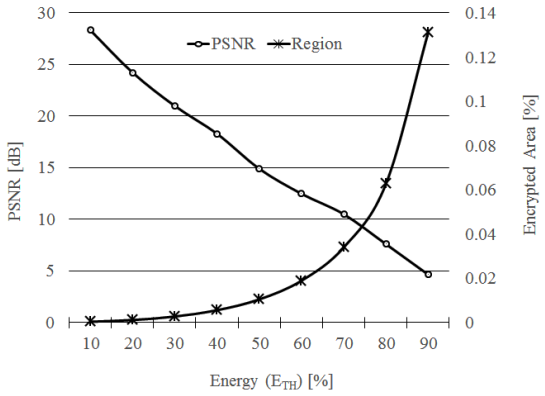


Fig. 13 Comparing graph between encrypted region and PSNR

Table. 2 position of MSB for level

L_{TH}	MSB
2	23
3	23
4	24
5	24
6	25
7	25

선택된 $L_{TH}=4$에서 암호화 영역의 비율을 표 3에 정리하였다. 표 3의 값들은 앞서 보인 실험결과들로부터 추출한 값이다. 표 3은 수치적인 암호화 결과를 비교 분석한 결과에 해당한다. 표 3을 살펴보면 동일한 L_{TH}에서 E_{TH}이 증가하면 암호화된 영역의 비율은 증가한다. 즉, 주파수를 세분화시키면 작은 영역만을 암호화한다 할지라도 더 많은 에너지가 암호화되어 암호화 효율은 높아진다는 것을 확인할 수 있다. 전체 데이터의 0.42%만을 암호화하여도 객체가 완전히 은닉된다.

Table. 3 Analysis and comparison of encryption efficiency

Item	L_{TH}=4			
E_{TH}	60	70	80	90
Ratio of Encrypted Region (%)	10.00	14.69	22.27	36.56
Ratio of Encrypted Data (%)	0.42	0.61	0.89	1.46

Ⅴ. 결 론

본 논문에서는 FRNLT을 이용하여 2차원 자연 영상을 암호화하는 새로운 방법을 제안하였다. FRNLT의 레벨, 쿼드트리 형태의 부대역들에 대한 에너지, 그리고 시각적인 효과를 관찰함으로써 암호화를 위한 최적화된 지점을 추출하였다. 암호화 효과는 PSNR 결과를 통해 관찰하였는데 L_{TH}가 커질수록 나빠지는 것을 확인하였다. 예상한 것과 같이 E_{TH}가 증가할수록 암호화 효과는 높아졌다. CPU 동작시간에 영향을 미치는 주요요인은 L_{TH}의 레벨이었고, 에너지를 세부적으로 분해하여 잘 집중시킨 후에 암호화시킨다 할지라도 암호화 효과가 좋아지지 않았다. 또한 레벨에 대한 것보다 암호화에 대한 동작시간이 훨씬 작기 때문에 암호화 데이터량은 크게 중요하지 않은 요인이었다. 실험결과를 살펴보면 최적화된 지점은 $L_{TH}=4$이고 $E_{TH}=60$인 경우로써 이때 0.42%만을 암호화하여도 원래의 영향을 분간할 수 없을 만큼 암호화를 효과를 얻을 수 있었다.

ACKNOWLEDGMENTS

The present Research has been conducted by the Research Grant of Kwangwoon University in 2014.

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and future Planning (NRF-2014R1A2A1A11052433)

REFERENCE

[1] L. Qiao and K. Nahrstedt, “Comparison of MPEG Encryption Algorithms,” *International Journal on Computer and Graphics(Special Issue on Data Security in Image Communication and Networks)*, Vol. 22, No. 3, pp. 437-444, 1998.

[2] A. M. Alattar, et al., "Improved Selective Encryption Techniques for Secure Transmission of MPEG Video bit-Streams," *International Conference on Image Processing (ICIP)'99*, 1999.

[3] C. Shi and B. Bhargava, "A Fast MPEG Video Encryption Algorithm," *Proc. Of ACM Multimedia 1998*, pp. 81-88, 1998.

[4] Sung-Ho Park, Hyun-Jun Choi, Young-Ho Seo, and Dong-Wook Kim, “Ciphering Scheme and Hardware Implementation for MPEG-Based Image/Video Security,” *Journal of The Institute of Electronics and Information Engineers*, vol.42, no.2, pp. 27-36, March. 2005.

[5] Ho-Joon Lee, Hyung-Jun Lee, “Digital data Encryption on Digital Video Recorder System,” *Journal of the korean institute of communications and information sciences*, vol.32, no.12, pp. 457-462, December. 2007.

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

[7] A. Pommer and A. uhl, "Wavelet Packet Methods for Multimedia Compression and Encryption," *IEEE Pacific Rim Conf. On Communications, Computers, and Signal Processing*, pp. 1-4, 2001.

[8] A. Pommer and A. Uhl, "Selective Encryption of Wavelet Packet Subband Structures for Obscured Transmission of Visual Data," *IEEE Benerux Signal Processing Symposium*, pp. 25-28, 2002.

[9] X. Wu and P. W. Moo, "Joint Image/Video Compression and Encryption via High-Order Conditional Entropy Coding of Wavelet Coefficients," *Int'l Conference on Multimedia Computing and Systems*, pp. 908-912, 1999.

[10] T. Uehara and R. Safavi-Naini, "Attacking and Mending Arithmetic Coding Entropy Schemes," *Proc. Of Australian Science Conference*, pp. 408-419, Jan. 1999.

[11] 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.

[12] 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.

[13] Ran Tao, Xiang-Yi Meng, Wang Yue, "Image Encryption with Multiorders of Fractional Fourier Transforms," *IEEE Transactions on Information Forensics and Security*, vol.5, no.4, pp.734-738, Dec, 2010.

[14] A.S. Rajput, N. Mishra, S. Sharma, "Towards the Growth of Image Encryption and Authentication Schemes," *2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp.454-459, 22-25 Aug, 2013.

[15] A.M. Elshamy, A.N.Z. Rashed, A.E.A. Mohamed, O.S. Faragalla, Yi Mu, S.A. Alshebeili, F.E.A. El-Samie, “Optical Image Encryption Based on Chaotic Baker map and Double Random Phase Encoding,” *Journal of Lightwave Technology*, vol.31, no.15, pp.2533-2539, 2013.

[16] 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.

[17] Young-Ho Seo, Moon Seok Kim, Dong-Wook Kim, “Quad-tree Subband Quantizer Design for Digital Hologram Encoding Based on Fresenelet,” *Journal of the Korea Institute of Information and Communication Engineering*, Vol. 19, No. 5, pp. 1180-1188 May. 2015.

[18] Youngho Seo, Eui-Sun Choi, Dong-Wook Kim, “Efficient Encryption Technique of Image Using Packetized Discrete Wavelet Transform,” *Journal of the Korea Institute of Information and Communication Engineering*, Vol. 17, No. 3, pp. 603-611 March. 2013.

서영호(Young-Ho Seo)

1999년 2월 : 광운대학교 전자재료공학과 졸업(공학사)
2001년 2월 : 광운대학교 일반대학원 졸업(공학석사)
2004년 8월 : 광운대학교 일반대학원 졸업(공학박사)
2005년 9월 ~ 2008년 2월 : 한성대학교 조교수
2008년 3월 ~ 현재 : 광운대학교 교양학부 부교수
※관심분야 : 실감미디어, 2D/3D 영상 신호처리, 디지털 홀로그램, SoC 설계

이윤혁(Yoon-Hyuk Lee)

2012 2월 : 광운대학교 전자재료공학과 졸업(공학사)
2014 2월 : 광운대학교 일반대학원 졸업(공학석사)
2014 3월 ~ 현재: 광운대학교 일반대학원 박사과정
※관심분야 : 디지털 홀로그램, SoC 설계

김동욱(Dong-Wook Kim)

1983년 2월 : 한양대학교 전자공학과 졸업(공학사)
1985년 2월 : 한양대학교 공학석사
1991년 9월 : Georgia공과대학 전기공학과(공학박사)
1992년 3월 ~ 현재 : 광운대학교 전자재료공학과 정교수
2009년 3월 ~ 현재 : 광운대학교 실감미디어 연구소 연구소장
※관심분야 : 3D 영상처리, 디지털 홀로그램, 디지털 VLSI Testability, VLSI CAD, DSP설계, Wireless Communication