패킷화 이산 웨이블릿 변환을 이용한 영상의 효율적인 암호화 기법

서영호* · 최의선** · 김동욱***

Efficient Encryption Technique of Image using Packetized Discrete Wavelet Transform

Youngho Seo* · Eui-Sun Choi** · Dong-Wook Kim***

이 논문은 2013년도 광운대학교 교내 학술연구비 지원에 의해 연구되었음

요 약

본 논문에서는 이산 웨이블릿 패킷 변환을 이용하여 디지털 시네마와 같은 영상의 중요 성분을 추적하고 암호화하는 새로운 방법을 제안한다. 공간과 주파수 영역에서 영상의 특성을 분석하여 영상을 다루는데 필요한 정보를 얻는다. 얻어진 정보들을 종합하여 웨이블릿 변환과 부대역의 패킷화를 이용한 암호화 방법을 제안한다. 웨이블릿 변환의 레벨과 에너지 값을 선택함으로써 다양한 강도로 암호화가 가능하다. 암호화 효과를 수치 및 시각적으로 분석하여 최적의 파라미터를 제시한다. 따라서 별도의 분석과정 없이 본 논문에서 제시된 파라미터를 이용하여 효율적으로 암호화를 수행할 수 있다. 실험결과를 살펴보면 전체 데이터 중에서 단지 0.18%의 데이터만을 암호화하더라도 객체를 분간할 수 없다. 부대역의 패킷화 정보와 암호화 시 이용한 키를 전체 암호키로 이용할 수 있다.

ABSTRACT

In this paper, we propose a new method which estimates and encrypts significant component of digital image such as digital cinema using discrete wavelet packet transform (DWPT). After analyzing the characteristics of images in spatial and frequency domain, the required information for ciphering an image was extracted. Based on this information an ciphering method was proposed with wavelet transform and packetization of subbands. The proposed algorithm can encrypt images in various robust from selecting transform-level and energy threshold. From analyzing the encryption effect numerically and visually, the optimized parameter for encryption is presented. Without additional analyzing process, one can encrypt efficiently digital image using the proposed parameter. Although only 0.18% among total data is encrypted, the reconstructed image dose not identified. The paketization information of subbands and the cipher key can be used for the entire secret key.

키워드

암호화, 영상, 이산 웨이블릿 변환, 부대역, 에너지

Key word

encryption, image, discrete wavelet transform, subband, energy

* 종신회원 : 광운대학교 교양학부
** 정회원 : 한국폴리텍 4대학
*** 종신회원 : 광운대학교 전자재료공학과(교신저자, dwkim@kw.ac.kr)

접수일자 : 2012. 10. 10
심사완료일자 : 2012. 10. 29

Open Access http://dx.doi.org/10.6109/jkiice.2013.17.3.603

Ⅰ. 서 론

디지털 시네마를 비롯하여 이산 웨이블릿에 기반을 둔 JPEG2000/MJPEG2000의 사용 확대에 따라 자연히 보안/보호 연구도 이들을 기반으로 하는 시스템을 겨냥하는 경우가 늘어나고 있고, 향후 이들 기술의 확대에 따라 이러한 경우는 더욱 늘어날 전망이다[1-3]. 아직 영상/비디오 처리기술과 보안 및 보호 기술을 하나의 시스템으로 구현하는 연구는 세계적으로 이루어지지 않고 있으나, 각각의 솔루션들이 활발히 연구되고 있는 현재의 추세로 보면 조만간 통합적 솔루션의 연구개발이 이루어질 것이며, 영상/비디오 처리 및 정보보안/보호의 통합 솔루션은 영상/비디오 응용분야의 기반 핵심부품의 선점이라는 의미에서 세계 굴지의 업체에서 이 분야에 대한 경쟁이 곧 시작될 것이라 전망할 수 있다.

최근에 무선 환경에서의 안전한 멀티미디어 통신기술을 위한 응용 계층에서의 방법이 제안되고 있으며 이미 MPEG-4 [4-6]기반에 대한 연구는 상당부분 진행되어 왔다. 상대적으로 웨이블릿 기반의 영상처리 방법이 더욱 최근에 발전되고 있으므로 이 방법들에[7]~[12] 대한 보안 알고리즘 또한 초기단계의 연구가 이루어지고 있다. [7]에서는 다른 2가지 방법으로 부분 암호화 방식을 제안하였고, [13]에서는 쿼드트리(quad-tree)를 기반으로 하는 SPHIT를 겨냥하여 암호화는 방법을 제안하였다. [8]과 [9]에서는 웨이블릿 변환 방식인 NSMRA (non-stationary multi-resolution analysis) 방법으로 각각 필터[8]와 트리구조 변환[9]을 통해 암호화를 수행하였는데 이러한 방법은 엔트로피 코딩의 하나인 산술 코딩을 목표로 하였다. [10]에서는 확률적인 암호화방법을 제안하고 [13]에서 그 방법을 개선시켰다. [11]에서는 EZW 방법을 제안하였는데 ATM 패킷 방법을 적용하여 암호화를 수행하였다. [12]에서는 데이터를 변형하지 않고 데이타 그 자체를 암호화하였다. 대신에 그것은 영상의 중요한 비트 평면을 암호화하여 원 영상에서 1/8에 해당하는 적은 양의 데이터를 암호화였다. 최근에는 MPEG 기반의 비디오를 위한 암호화 기법[14][15]도 연구되었다.

본 논문에서는 패킷화된 DWT를 사용하였는데 이 방법은 암호화하는 데이터의 양과 계산양의 서로 상보적인 관계가 있고 안전한 영상 전송을 하기 위해 암호화하는 데이터의 양을 적응적으로 조절하여 다양한 환경에서 적용하는 것이 가능하다. 다음 장에서는 DWT를 이용한 영상압축방법과 DWT 결과 영상 및 그 데이터 구조에 대해서 설명하고, 본 논문에서 제안하는 부분영상 암호화를 위한 데이터 선택 방법과 선택된 데이터를 암호화하는 방법을 3장에서 설명한다. 4장에서는 제한한 방법에 대한 실험 결과를 보이고 마지막으로 5장에서는 본 논문의 결론을 맺는다.

Ⅱ. 이산 웨이블릿 변환과 웨이블릿 계수의 특성

DWT는 DCT와 같이 시간영역의 신호를 주파수 영역의 계수로 변환한다. 그러나 푸리에 변환을 기반으로 하는 도구들과 달리 주파수 영역에서 신호가 갖는 주파수 성분뿐만 아니라 위치에 따른 주파수 성분의 정보까지 얻을 수 있다. 또한 영상을 블록으로 분할하지 않고 원 영상을 그대로 처리함으로서 블록효과를 제거할 수 있다. DWT를 기반으로 영상을 압축할 경우에 다양한 압축률을 얻기 쉬우며, 전체영상에 대해 주파수 대역별로 분리하므로 비트스트림이 잡음에 강인하다. 부대역의 구조를 활용하면 일부분 전송된 정보로 전체영상을 복원할 수 있는 장점을 갖는다. 현재 디지털 시네마를 위한 압축도구인 JPEG2000의 기본 주파수 변환도구로 사용되고 있다[2].

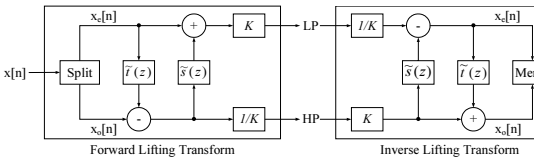


그림 1. 팩토링을 이용한 정방향/역방향 리프팅
Fig. 1 Forward/inverse lifting using factoring

DWT를 연산하는 방법은 크게 컨벌루션 필터링 방법과 리프팅 방법이 있다. 리프팅은 컨벌루션 필터링을 변형 및 개선하여 연산의 속도와 메모리의 사용효율을 높인 방법이다. 본 논문에서는 리프팅을 이용하여 DWT를 수행하고자 한다[2]. 리프팅 방식의 기본적인 원리는 웨이블릿 필터의 다상 행렬을 삼각 행렬과 대각 행렬로 인수분해하는 것이다.

그림 1에 일반적인 리프팅 과정을 나타내고 있는데, 리프팅을 이용한 웨이블릿 변환은 분할, 결합, 예측, 갱신, 및 조정의 네 단계로 구성된다[16].

2 dimensional(2D) DWT는 열과 행방향으로 1D DWT를 각각 독립적으로 연산하여 수행된다.

2차원 데이터, 즉 영상에 대해 2D DWT를 수행하면 각기 다른 주파수 특성을 갖는 4개의 영역이 생성된다. 이 영역을 부대역이라고 하고 일반적으로 주파수 특성에 따라서 LL, LH, HL, 및 HH 영역으로 표시한다. 4개의 부대역은 열과 행방향으로 다운 샘플링되었기 때문에 4개의 부대역을 합한 크기는 원영상의 크기와 동일하다. 1-레벨 DWT에 의해 생성된 부대역의 구조를 그림 2(a)에 표시하였다.

처음으로 생성된 4개의 부대역 중에서 가장 저주파 부대역인 LL 부대역에 대해 2D DWT를 적용한다. 이러한 방식으로 주파수를 분할하는 방식을 Mallat-tree 방식이라고 한다.

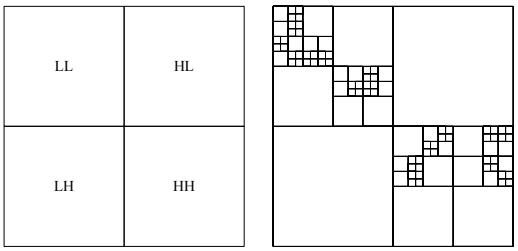


그림 2. DWPT에 의한 부대역의 생성
(a) 1 레벨 (b) 5 레벨의 예
Fig. 2 Subband structure example by DWPT
(a) 1 level (b) 5 level

Mallat-tree 방식으로 L-레벨만큼 2D DWT를 수행하면 (3L+1)개의 부대역이 생성된다[12]. 4개의 부대역 중에서 필요에 따라 임의의 부대역을 선택하여 DWT를 수행하는 방식을 이산 웨이블릿 패킷 변환(discrete wavelet packet transform, DWPT)이라 한다[15]. 패킷화된 DWT 부대역의 구조를 그림 2(b)에 표시하였다.

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.

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 역과정을 추적하기 어려워야 하고 주파수 성분을 예측하기 어려워야 한다. 제안하고자 하는 알고리즘은 이러한 문제들을 적절히 해결하고 효율적으로 암호화를 시도하고자 한다.

영상은 유사한 주파수 특성을 갖기 때문에 예측이 용이하여 mallot-tree 방식의 DWT가 적당하지 않다. 즉 부대역을 패킷화하여 영상에 특화된 부대역 구조로부터 추출된 주파수 성분을 암호화해야 한다. 이러한 부대역 구조는 암호화된 주파수를 예측하기 어렵게 하고 역과정을 이용한 공격이 어렵다. 영상에 따라서 각각의 부대역에 대해 적응적으로 DWT를 수행하고 그 기준은 에너지의 중요도에 의존한다. 시각적인 인지도는 정보가 갖는 에너지의 량에 비례하기 때문에 가능하면 에너지가 높은 주파수 대역을 은닉하여 암호화 효율을 높여야 한다.

3.1. 암호화 기법

제안한 암호화 알고리즘을 그림 3에 나타내었다. 영상을 4개의 부대역으로 변환하고, 4개의 부대역에 대해 각각 다시 DWT를 수행한다. 부대역들의 에너지 분포를 탐색하고, 다시 DWT를 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. DWT 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.

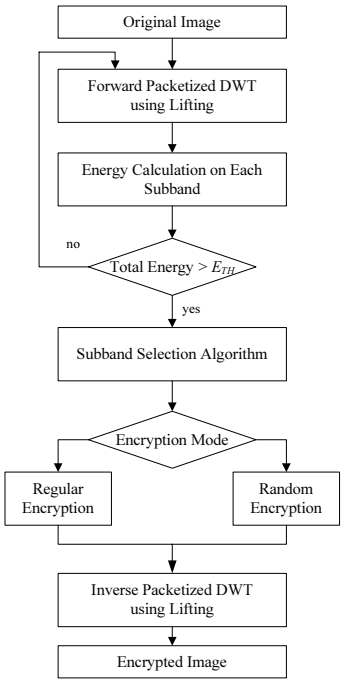


그림 3. 영상 암호화 절차
Fig. 3 Image encryption procedure

최종적으로 선택된 부대역들은 블록 암호화 알고리즘[18]을 이용하여 암호화한 후에 역 PDWT를 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.

3.2. 복호화 기법

그림 4에는 영상을 복호화하는 절차를 나타내었다. 복호화 절차는 암호화 절차의 역과정이고 암호화 시 사용하였던 암호키를 그대로 사용하고, 암호화 과정에서 추출했던 선택맵과 우선순위맵을 이용한다.

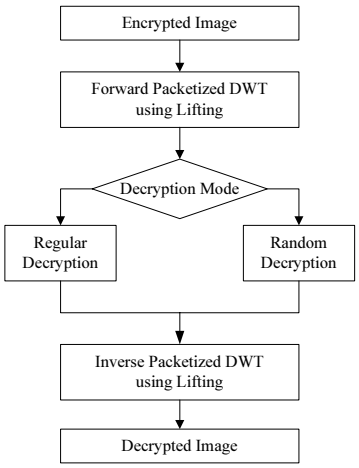


그림 4. 영상 복호화 절차
Fig. 4 Image decryption procedure

3.3. 부대역 선택

제안한 영상의 암호화 알고리즘에서 부대역을 선택하는 방법은 그림 5의 순서로 수행한다. 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 우선순위맵을 위한 우선순위 플래그를 생성한다. 그리고 E_{TH}에 따라 부대역을 선택하고, 선택맵을 위해 선택 플래그을 생성한다.

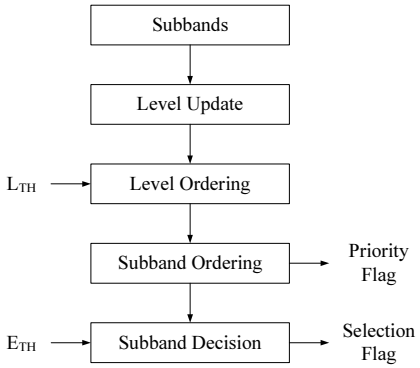


그림 5. 부대역 선택 절차
Fig. 5 Subband selection procedure

Ⅳ. 실험 및 결과

제안한 암호화 기법을 100여장의 영상에 적용하여 암호화 결과를 확인하였다. 먼저, 순방향 DWPT를 이용하여 생성된 영상을 주파수 영역의 계수로 변환하고, 앞 절에서 설명한 방법으로 부대역을 선택한다. 선택된 부대역의 계수들을 블록 암호화 알고리즘을 이용하여 암호화한다. 역방향 DWPT를 거쳐서 암호화된 영상이 생성된다. 암호화된 결과는 peak noise-to-signal ratio (PSNR)과 normalized correlation (NC)를 이용하여 수치적으로 확인한다. 또한 수치적인 통계와 함께 시각적인 판단을 통해서 결과를 판단한다. PSNR은 식 (1)에 정의하였다.

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

본 실험에서는 DWPT 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 $L_{TH}=4$이고 $E_{TH}=55$의 경우이다. $E_{TH}=20$이지만 실제로 암호화된 에너지의 양은 51.1%이고, PSNR은 9.07dB이다. 암호화된 부대역의 크기는 0.39%이고, 최상위 비트 평면만을 암호화했기 때문에 암호화된 양은 0.53%이다.

그림 6(a)는 원본 영상을 나타내고, (b)는 암호화된 부대역을 나타낸다. 그림 6(c)는 암호화에 선택된 부대역을 표시하고, 그림 6(d)는 복원한 암호화된 영상을 나타낸다. 전체 데이터에서 매우 소량의 데이터만을 암호화했음에도 불구하고 그림 6(d)와 같이 영상을 분간할 수 없을 정도로 암호화 효과가 뛰어나다. 또한 DWPT의 구조와 선택된 부대역에 대한 정보가 없다면 다시 복구할 수 없기 때문에 보안성이 매우 높다.

E_{TH}와 L_{TH}의 값을 조절하여 다양한 암호화 방법이 가능하다. 그림 7은 $E_{TH}=55$인 경우에 L_{TH}에 따라 선택된 부대역들을 나타낸다. 모든 경우에 대해서 최저 주파수 대역은 반드시 포함시킨다. 최저 주파수 대역은 에너지의 양에 상관없이 전체 영상의 평균 주파수를 나타내므로 암호화 시 포함시킨다. $E_{TH}=55$를 선택하여 나타낸 이유는 이 정도의 에너지 이상이면 모든 L_{TH}에 대해서 전체적인 영상을 분간할 수 없었기 때문이다.

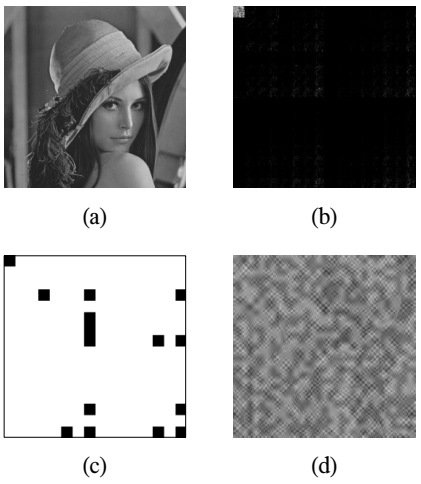


그림 6. 암호화 실험 과정 (a) 원영상 (b) 암호화된 부대역 (c) 선택된 부대역 (d) 복원된 영상
Fig. 6 Encryption procedure (a) original image (b) encrypted subbands (c) selected subbands (d) reconstructed image

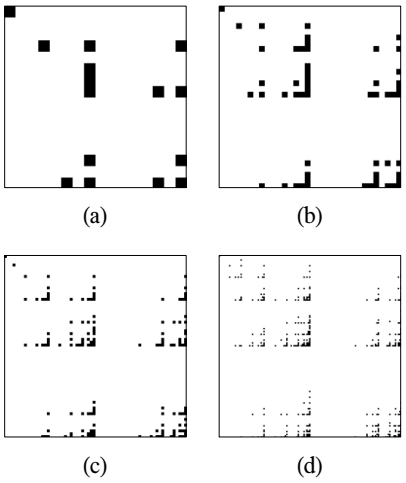


그림 7. $E_{TH}=55$인 경우에 선택된 부대역
(a) $L_{TH}=4$ (b) $L_{TH}=5$ (c) $L_{TH}=6$ (d) $L_{TH}=7$
Fig. 7 the selected subbands in case of $E_{TH}=55$
(a) $L_{TH}=4$ (b) $L_{TH}=5$ (c) $L_{TH}=6$ (d) $L_{TH}=7$

L_{TH}가 높아질수록 더욱 에너지를 정밀하게 분해하고 중요한 주파수 성분을 골라낼 수 있기 때문에 암호화 효과는 더욱 높일 수 있다. 이에 따라 DWPT로 인한 연산량은 증가할 수 있지만 L_{TH}가 높은 경우에 DWPT의 연산은 매우 소량이므로 전체적인 비용을 고려하면 거의 비슷한 효과라고 할 수 있다. 그림 8에는 E_{TH}와 L_{TH}에 따라서 선택된 부대역의 개수를 나타내었다.

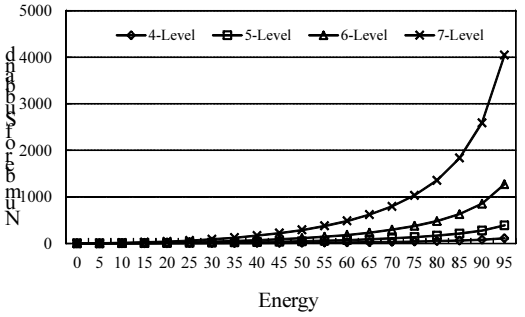


그림 8. 암호화를 위해 선택된 부대역의 개수
Fig. 8 The number of the selected subband for encryption

암호화 이후의 영상의 PSNR을 측정하여 그림 9에 그래프로 정리하였다. L_{TH}과 E_{TH}를 변화시키면서 100여 장의 영상에 대해서 다양한 조건을 실험하였다. 결과를 살펴보면 PSNR 값이 L_{TH}과 E_{TH}에 대해 규칙성 있는 경향성을 갖지 않는다는 것을 확인할 수 있다. PSNR은 10dB 전후의 값을 갖기 때문에 이미 경향성을 갖는 범위를 벗어난 것으로 볼 수 있다.

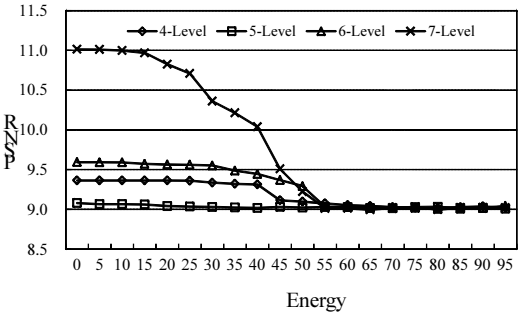


그림 9. 영상의 암호화 PSNR 결과
Fig. 9 Encryption PSNR result of image

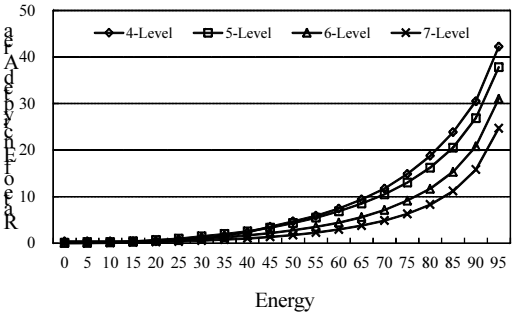


그림 10. 암호화 영역의 비율에 대한 그래프
Fig. 10 Graph for ratio of encrypted region

레벨 L_{TH}과 에너지 E_{TH}에 따른 암호화 영역의 비율을 그림 10에 보였다. 동일한 E_{TH}라면 L_{TH}가 클수록 암호화 영역은 작다. 즉, 작은 부대역만을 암호화할지라도 유사한 에너지를 만족시킬 수 있다는 의미이다. DWPT의 레벨이 증가하면 주파수를 더욱 세분화할 수 있고, 중요 주파수 영역을 찾는 것이 더욱 정밀해진다. L_{TH}에 따른 최상위 비트 위치를 표 1에 나타냈다. 즉, 암호화된 데이터의 값은 그림 10의 결과를 표 1로 나누어야 한다.

표 1. 레벨에 따른 MSB의 위치
Table. 1 position of MSB for level

L_{TH}	MSB
2	9
3	10
4	11
5	12
6	12
7	13

선택된 E_{TH}에서 암호화 영역의 비율을 표 2에 정리하였다. 표 2의 값들은 그림 9 및 10의 실험 결과로부터 추출한 값이다. 표 2는 수치적인 암호화 결과를 비교 분석한 결과에 해당한다. 표 2를 살펴보면 동일한 E_{TH}에서 L_{TH}이 증가하면 암호화된 영역의 비율은 감소한다. 즉, 주파수를 세분화시키면 작은 영역만을 암호화한다 할지라도 더 많은 에너지가 암호화되어 암호화 효율은 높아진다는 것을 확인할 수 있다. 표 2의 암호화 효율은 식 (2)으로 정의하였다. 레벨 7의 결과를 살펴보면 전체 데이터의 0.18%만을 암호화하여도 객체가 완전히 은닉

된다. 레벨 6의 경우는 0.29%를 암호화 하였을 때 객체가 분간할 수 없게 된다.

표 2. 암호화 효율의 분석 및 비교
Table. 2 Analysis and comparison of encryption efficiency

Item	L_{TH}			
	4	5	6	7
E_{TH}	55			
Ratio of Encrypted Region(%)	5.86	5.45	3.49	2.28
Ratio of Encrypted Data(%)	0.53	0.46	0.29	0.18
Efficiency	9.39	10.06	15.75	24.16
Efficiency Ratio(%)	38.85	41.63	65.21	100

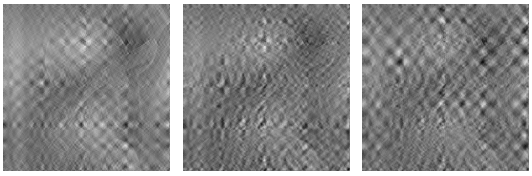
표 2에서는 E_{TH}를 55로 고정하였지만 영상이 분간하기 어려운 지점은 각 L_{TH}별로 차이가 있다. 모든 L_{TH}에 대해서 영상이 확실히 분간하기 어려운 지점을 선택한 것이 $E_{TH}=55$이다. 그림 11에는 E_{TH}가 증가함에 따라서 영상이 어떻게 훼손되어 가는지를 나타내었다. 그림 11(a)에는 아직까지 약간의 윤곽선 정보가 남아 있고, 그림 11(b)부터는 원래 영상을 알고 있지 않았다면 어떤 영상인지 분간하기 어려워진다. 그림 11(c)는 확연히 원래 영상을 구별하기 어렵다.

$$Efficiency = \frac{E_{TH}}{Ratio\ of\ Encrypted\ Data} \quad (2)$$

표 2에서는 E_{TH}를 55로 고정하였지만 영상이 분간하기 어려운 지점은 각 L_{TH}별로 차이가 있다. 모든 L_{TH}에 대해서 영상이 확실히 분간하기 어려운 지점을 선택한 것이 $E_{TH}=55$이다.

그림 11에는 E_{TH}가 증가함에 따라서 영상이 어떻게 훼손되어 가는지를 나타내었다. 그림 11(a)에는 아직까지 약간의 윤곽선 정보가 남아 있고, 그림 11(b)부터는 원래 영상을 알고 있지 않았다면 어떤 영상인지 분간하기 어려워진다. 그림 11(c)는 확연히 원래 영상을 구별하기 어렵다.

그림 8, 9, 및 10에서 주어진 정보를 바탕으로 응용 분야에 따라 암호화 강도를 변화시키면서 다양한 형태로 영상 정보를 보호할 수 있다.



(a) (b) (c)

그림 11. L_{TH}=7의 경우에 E_{TH}에 따른 암호화 효과 (a) E_{TH}=50, (b) E_{TH}=55, (c) E_{TH}=60
Fig. 11 Encryption effect according to E_{TH} in case of L_{TH}=7 (a) E_{TH}=50, (b) E_{TH}=55, (c) E_{TH}=60

V. 결 론

본 논문에서는 웨이블릿 영역에서 암호화를 통해 영상정보를 효율적으로 은닉하는 방법을 제시하였다. 이산 웨이블릿 변환을 패킷화하여 영상의 주파수 성분을 분해하고, 이들 주파수에서 중요한 주파수 성분을 추적하였다. 중요한 주파수, 즉 많은 에너지를 갖는 주파수 성분을 선택하고 암호화하여 영상을 암호화하였다. 암호화 효과는 수치 및 시각적으로 확인하였다. 복원된 영상의 PSNR을 수치적으로 확인했을 경우에 상관성을 정의하기 어려웠다. 그러나 시각적인 특성과 암호화량을 분석하여 DWPT 레벨과 에너지 량 사이의 관계를 규명할 수 있었다. DWPT 레벨이 증가할수록 암호화량에 대한 암호화 효율은 높아진다. 그러나 연산량이 증가하므로 응용분야에 따라서 레벨과 에너지량, 그리고 암호화 강도를 적절하게 선택해서 사용해야 한다. 7-레벨의 경우에 전체 데이터 중에서 0.18%의 데이터만을 암호화한다 할지라도 복원된 객체를 시각적으로 확인하기 어려웠다.

감사의 글

이 논문은 2013년도 광운대학교 교내 학술연구비 지원에 의해 연구되었음

참고문헌

[1] W. Staliings, Cryptography and Network Security, Principles and Practice, Prentice-Hall, Upper Saddle River, NJ, 1999.

[2] R. M. Rao and A. S. Bopardikar, Wavelet Transforms, Introduction to Theory and Application, Addison-Wesley, Reading, 1998.

[3] Edited by Martin Boliek, JPEG 2000 Final Draft International Standard, ISO/IEC JTC 1/SC 29/WG 1, 2000.

[4] 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.

[5] A. M. Alattar, et al., "Improved Selective Encryption Techniques for Secure Transmission of MPEG Video Bit-streams", ICIP'99, pp. --, 1999.

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

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

[14] 박성호, 최현준, 서영호, 김동욱, "DCT-기반 영상/비디오 보안을 위한 암호화 기법 및 하드웨어 구현", 대한전자공학회, 전자공학회논문지-SP 302, pp. 27-36, 2005. 3.

[15] 이호준, 이형준, "디지털 영상 감시 시스템의 영상 데이터 암호화", 한국통신학회, 한국통신학회논문지 32(12), pp. 457-462, 2007. 12.

[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.

[18] 한국정보보호센터, 128비트 블록 암호알고리즘(SEED) 개발 및 분석 보고서, 12. 1998.

저자소개

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

최의선(Eui-Sun Choi)

2000년 2월 광운대학교 일반대학원 졸업(공학석사)
2004년 8월 광운대학교 일반대학원 졸업(공학박사)
2013년 3월 ~ 현재 한국폴리텍 4대학 아산캠퍼스 정보통신시스템과 초빙교수
※관심분야 : 마이크로웨이브, RFID, LTCC, 안테나, 세라믹

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