

# 이미지 포맷변환에 강인한 양자화 인덱스 변조 기반의 정보은닉 알고리즘

백중현, 신정환, 허준  
고려대학교

[bell211@korea.ac.kr](mailto:bell211@korea.ac.kr), [jhsh@korea.ac.kr](mailto:jhsh@korea.ac.kr), [junheo@korea.ac.kr](mailto:junheo@korea.ac.kr)

## Quantization Index Modulation Data Hiding Algorithm robust against Image Format Variation

Jong Hyun Baik, Jeong Hwan Shin, Jun Heo  
Korea University

### 요 약

본 논문에서는 이미지 블록의 평균 픽셀 값 특성을 양자화 인덱스 변조 기법에 적용하여 이미지 포맷변환에 강인한 정보은닉 기법을 제안한다. 포맷변환에 강인한 이미지 속성은 정규화된 픽셀 히스토그램에 기반하여 분석되며, 그 중 평균 픽셀 값을 통해 정보은닉 알고리즘이 구성된다. 평균 픽셀 값을 양자화 인덱스 변조기법에 적용하기 위한 방안으로 DCT 계수를 정규화 하는 방법이 선택되며, 추출 성공률을 높이기 위해 오류정정부호가 사용된다. 따라서 본 논문의 알고리즘을 통해 결합 이미지가 압축, 사이즈 변화 등의 과정을 거치게 될 경우 발생하는 문제점을 극복할 수 있다.

### 1. 서론

최근 들어 개인 사용자의 멀티미디어 데이터 제작이 자유로워지고, 그 유용성이 급격히 증가함에 따라 관련된 서비스 창출에 대한 수요가 증가하고 있다. 이러한 동향에 따라 정보은닉 기법에 대한 응용범위가 확대되고 있으며, 다양한 목적에 부합하는 정보은닉 기법에 대한 연구가 활발히 진행되고 있다. 또한 전문적인 도구의 도움 없이 이미지 데이터의 변화 및 수정이 쉬워지고 있기 때문에 크기변화, 압축 등의 다양한 포맷변환을 함께 고려한 정보은닉 기법이 요구된다. 특히 이미지 크기가 급격히 감소하는 경우에 대해서 효과적으로 정보를 은닉할 수 있는 알고리즘이 매우 부족한 실정이다.

정규화된 픽셀 히스토그램은 픽셀 히스토그램을 이미지 블록의 픽셀 사이즈로 정규화한 이산 분포함수로 픽셀 값의 분포 비율을 효과적으로 표현할 수 있는 도구이다. 또한 [그림 1]에서 확인 할 수 있듯이, 크기에 관계없이 같은 장면을 표현하는 블록에 대해서는 매우 유사한 분포를 갖는다. 정규화된 픽셀 히스토그램을 픽셀 값에 대한 이산 확률 분포함수라고 표현해도 무방하므로, 이를 바탕으로 계산 가능한 평균 픽셀 값도 이미지 크기에 독립적인 속성을 가진다는 것을 알 수 있다. 본 논문에서는 이러한 평균 픽셀 값을 이용하여 정보를 숨기는 알고리즘을 구성하고자 한다.

DCT(Discrete Cosine Transform)는 주어진 이미지의 주파수 특성을 분석하기 위해 보편적으로 사용되는 도구로써 JPEG 등의 다양한 이미지 포맷에 사용되고 있다. 2 차원 DCT 에 의해 주파수 영역에서 이미지 성분의 중요도를 구분할

수 있는데, 이 중 가장 낮은 주파수에 대한 DCT 계수, 즉 DC 값이 압축에 가장 강인한 속성을 갖는다. 앞서 언급한 평균 픽셀 값은 DC 계수를 정규화 함으로써 얻을 수 있으므로 주파수 영역에서 픽셀 분포의 속성을 다룰 수 있다.

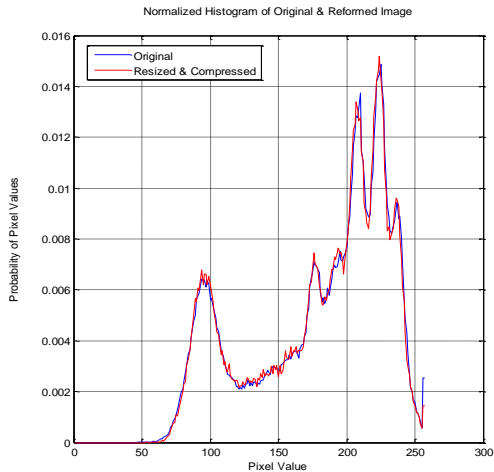
양자화 인덱스 변조 방식은 숨기고자 하는 정보에 따라 원본 데이터를 정해진 양자화 구간에 의해 변조하는 기법이다. 근본적으로 원본 이미지의 화질 열화와 추출 성공률 사이에 존재하는 상충관계를 극복하기 위해 적절한 양자화 구간을 선택하는 것이 중요하다. 그러나 상대적으로 복잡도가 낮은 방식이므로 쉽게 구현될 수 있다는 장점을 가진다. 본 논문에서는 정규화된 DC 계수를 양자화 인덱스 변조 방법에 적용하여 JPEG 압축과 크기 변화에 모두 강인한 알고리즘을 제안하고자 한다.

### 2. 정보은닉기법과 추출기법

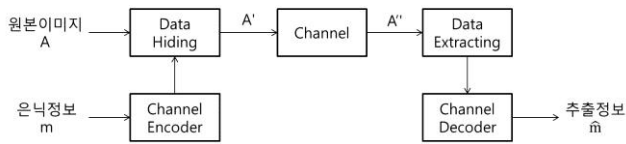
본 논문에서 다루고자 하는 시스템 모형은 [그림 2]와 같다. [그림 2]에서의 채널블록은 JPEG 압축 또는 이미지 크기의 변화에 의한 포맷변환을 의미한다. 본 연구에서 제안하는 알고리즘은 이미지에 숨겨지는 정보를 비트단위로 은닉하는 방법을 사용한다. 또한 이미지의 정보 은닉 수용력을 최대화 하기 위하여 1 블록당 1 비트를 은닉하도록 하며, (15,7)BCH 부호를 적용하여 숨겨지는 정보를 보호한다.

정보가 숨겨지는  $W \times H$  크기의 원본이미지를  $A$  라고 하며, 다수의 비트정보를 숨기기 위해서 원본이미지  $A$  를 숨기고자 하는 비트의 수만큼 세부 블록으로 분할한다. 숨기고자 하는 비트의 수를  $u \times v$  라고 할 때, 세부블록  $a_{ij}$  ( $i = 1, \dots, u, j =$

$1, \dots, v$  는 크기는  $k \times k$  의 정사각형 블록이다. 또한 컬러 이미지에 대해 B(blue) 성분만을 대상으로 알고리즘을 적용함으로써 원본의 화질열화를 최소화한다.



[그림 1] 사이즈 및 압축률 변화에 따른 정규화된 픽셀 히스토그램



[그림 2] 정보은닉 시스템 블록도

2 차원 DCT 는 식(1)에 의해 수행된다. (0,0) 위치의 계수  $F_{(0,0)}$  를 정 사각 블록의 가로 혹은 세로길이  $k$  로 정규화하면 식(2)와 같이 블록의 평균 픽셀 값  $m_{ij}$  와 같도록 할 수 있다. DCT 기법은 직접적으로 픽셀 값을 수정하지 않아도 주파수 영역에서 평균 픽셀 값을 다루는 방법을 제공하며, 알고리즘을 체계적으로 구성하는데 도움이 된다.

$$F_{(p,q)} = \frac{\Lambda(p)\Lambda(q)}{k/2} \sum_{x=0}^{k-1} \sum_{y=0}^{k-1} \cos\left(\frac{(2x+1)p\pi}{2k}\right) \cos\left(\frac{(2y+1)q\pi}{2k}\right) f_{(x,y)} \quad (1)$$

$$m_{ij} = \frac{F_{ij(0,0)}}{k} \quad (i = 1, \dots, u, j = 1, \dots, v) \quad (2)$$

정보은닉 알고리즘은 다음과 같다.

- (1) 원본이미지의 모든 블록  $a_{ij}$  에 대하여  $\frac{M}{u} \times \frac{N}{v}$  2 차원 DCT 를 수행하여 DCT 블록  $X_{ij}$  을 얻는다.
- (2) 식(2)와 같이 각 DCT 블록  $X_{ij}$  의 DC 계수  $F_{ij(0,0)}$  에 대해 블록의 가로 혹은 세로길이  $k$  로 정규화한다.
- (3) 양자화 구간 간격  $\Delta$  에 의해 정규화된 DC 계수를 양자화 한다.
- (4) 해당하는 정규화된 DC 계수가 어떤 양자화구간에 존재하는지 관찰한다.
- (5) (15,7)BCH 부호에 의해 부호화된 은닉정보를  $c$ , 수정된 후의 정규화된 DC 계수를  $m'_{ij}$  라고 하자.  $c$  의 값에 따라 정규화된 DC 계수를  $\Delta$  만큼 변경하여 식 (3)의 조건을 만족하도록 변조한다.

$$\begin{cases} i \cdot \Delta \leq m'_{ij} < (i+1) \cdot \Delta, i \text{ is even} & \text{if } c = 0 \\ i \cdot \Delta \leq m'_{ij} < (i+1) \cdot \Delta, i \text{ is odd} & \text{if } c = 1 \end{cases} \quad (3)$$

(6) 변조된 DC 계수에 대해 정규화의 역 연산을 하고, IDCT(Inverse Discrete Cosine Transform)을 수행한다.

위와 같은 방식으로 만들어진 결합이미지  $A'$  는 [그림 2]의 채널을 겪게 되는데, 본 논문에서는 채널을 이미지에 JPEG 압축이 가해지거나 크기가 감소하는 상황으로 모호화하고 있다. 따라서 은닉정보는 채널을 통과한 크기  $W' \times H'$  의 이미지  $A''$  를 대상으로 식(3)의 양자화 구간 분석에 의해 추출된다.

### 3. 실험결과



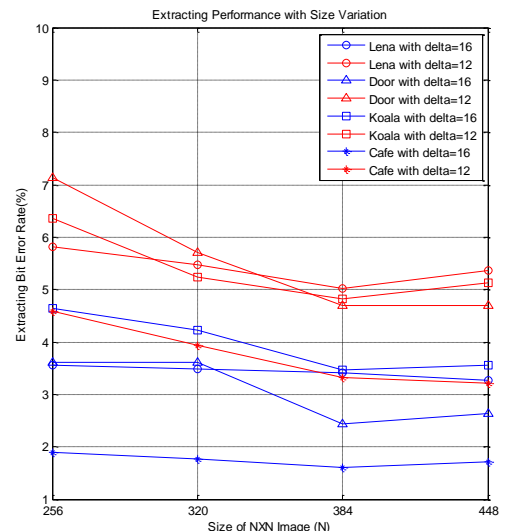
(a)Lena (b)Koala (c)Cafe (d)Door

[그림 3] 샘플이미지

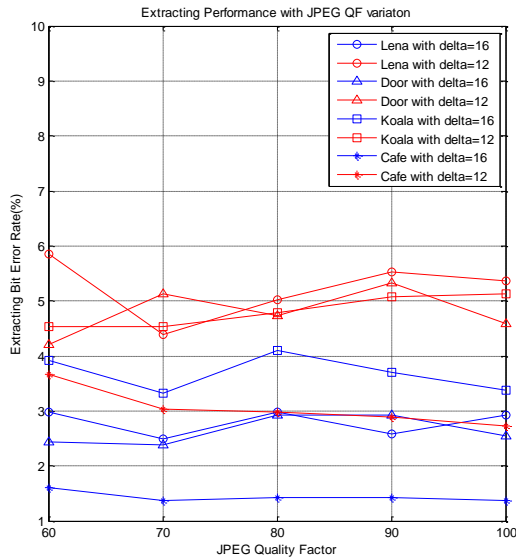


[그림 4] 결합이미지

대부분의 정보은닉 기법에서 화질 열화 정도와 은닉효율은 서로 상충관계에 있다. 양자화 인덱스 변조기법의 경우에는 양자화 구간 간격에 따라 둘 사이의 상충관계가 조절된다. 양자화 구간 간격  $\Delta$  가 증가하면 원본 이미지의 변조 폭이 증가함에 따라 변조 심볼 간 최소거리도 증가하므로 추출 정확도를 높일 수 있다. 그러나 동시에 너무 큰 변조 폭은 원본의 화질 열화를 초래할 수 있다. 반대로  $\Delta$  를 너무 작게 선택하면 화질 열화를 최소화 할 수 있지만, 추출 오류를 증가시키는 결과를 초래한다.



[그림 5] 이미지 크기변화에 따른 정보 추출 오류확률



[그림 6] JPEG 화질요소 변화에 따른 정보 추출 오류확률

실험은 두 가지 서로 다른 양자화 구간 간격  $\Delta$ 에 대해 JPEG 화질 요소와 크기변화에 따른 추출 오류 확률을 측정하는 방식으로 진행되었다. 숨겨진 정보는 총 2048 비트이다. [그림 3]의 샘플 이미지는 모두  $512 \times 512$  크기의 raw 이미지이다. [그림 5]와 관련된 실험에서는 이미지의 크기가  $448 \times 448$ ,  $384 \times 384$ ,  $320 \times 320$ ,  $256 \times 256$ 으로 감소하는 경우에 대해 관찰하였다. JPEG 압축의 경우 화질요소가 100, 90, 80, 70, 60인 경우에 대해 관찰하였고 [그림 6]에서 그 결과를 확인할 수 있다.

양자화 구간 간격  $\Delta$ 가 12인 경우와 16인 경우를 비교해본 결과 [그림 4]와 [그림 5]를 통해 알 수 있듯이 16인 경우에 더 낮은 오류 확률을 보였다. 주어진 양자 구간 간격에 대해서는 크기 감소폭이 클수록 오류 확률이 높아진다는 것을 확인할 수 있었다. 그러나 매 많은 양의 데이터 차이에도 불구하고 이미지 크기에 관계없이 정보추출이 비교적 성공적임을 알 수 있었다. 실험에서 가정한 최대 크기 변화는 가로, 세로가 각각  $1/2$ 씩 감소한 경우이다. 즉, 원본 데이터의  $3/4$ 를 잃어야 하는 상황에서도 높은 성공률로 은닉정보를 추출해낼 수 있음을 확인하였다. JPEG 압축의 경우 화질 요소에 따른 성능 변화 경향을 보이지는 않지만 대체로 6%이하의 낮은 오류 확률을 보임을 확인하였다. 따라서 실험을 통해 본 논문에서 제시하는 기법이 JPEG 압축과 급격한 크기변화에 강인한 알고리즘임을 보였다.

#### 4. 결론

본 논문에서는 정규화된 픽셀 히스토그램에 기반하여 분석한 이미지의 속성을 정보를 은닉에 응용하고자 하였다. 정규화된 픽셀 히스토그램은 포맷에 관계없이 지속되는 이미지의 특성이다. 따라서 이러한 특성은 다양한 변환과정에 강인한 알고리즘을 만드는데 매우 효과적으로 이용될 수 있다.

평균 픽셀 값은 일반적으로 공간영역에서 계산되지만, 주파수 영역에서도 계산된다는 것을 밝힘으로써 JPEG 압축에도

견딜 수 있는 속성을 동시에 갖추고 있다. 따라서 본 논문에서는 평균 픽셀 값을 주파수 영역에서 계산하고 그것을 양자화 인덱스 변조기법에 응용한 정보은닉 알고리즘을 제안하였다.

제안된 알고리즘을 통해 이미지의 포맷 변환이 잦은 상황에서 쉽게 발생할 수 있는 픽셀 값 변화, 데이터 손실 등의 문제점을 극복할 수 있었다. 또한 본 연구를 통해 제안되는 알고리즘은 양자화 구간 간격과 오류정정부호의 종류에 따라 다양한 목적에 의해 응용될 것으로 기대된다.

#### ACKNOWLEDGEMENT

본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음(NIPA-2011-C1090-1131-0009)

#### 참고문헌

- [1] F.A.P.Petitcolas, R.J.Anderson. and M.G.Kuhn, "Information Hiding-A Survey," Proc,IEEE,vol.87, no.7,1999,pp.1062-1078
- [2] B.Chen and G.W.Wornell, "Quantization Index Modulation : A Class of Provably Good Methods for Digital Watermarking and Information Embedding", IEEE Trans. Information Theory, vol.47, no.4, 2001, pp.1423-1443
- [3] Mei Jiansheng, Li Sukang and Tan Xiaomei. "A Digital Watermarking Algorithm Based On DCT and DWT", International Symposium on Web Information Systems and Applications (WISA '09), pp no-104-107,2009
- [4] Chee Sun Won, "Boosting robustness against composite attacks for quantization index-modulation algorithms", J.Electron.Imaging 19,023010(May 11, 2010);doi : 10.1117/1.3427158
- [5] Zhicheng Ni, Yun Q. Shi, Fellow, Nirwan Ansari, Wei Su, "Robust Lossless Image Data Hiding Designed for Semi-Fragile Image Authentication", IEEE Transactions on circuits and systems for video technology, Vol. 18, No. 4, April 2008, pp. 497-509.