특이값 분해를 이용한 다양한 이미지 변화에 강인한 정보 은닉 알고리즘

이동훈, 허준
고려대학교
bitterend@korea.ac.kr, junheo@korea.ac.kr

Robust Algorithm using SVD for Data Hiding in the Color Image against Various Attacks

Donghoon Lee, Jun Heo
Korea University

요 약

본 논문에서는 특이값 분해(Singular Value Decomposition)을 이용하여 이미지의 주파수 영역 내에 정보를 은닉하는 방법을 제시한다. 이미지를 주파수 영역으로 변환하기 위하여 블록 단위로 이산 코사인 변환(Discrete Cosine Transform)을 수행한다. 이후 인접한 네 블록의 DC 값들로 구성된 행렬의 특이값을 은닉하고자 하는 정보에 따라 변환한다. 원래의 DC 값은 정보에 따라 변환된 DC 값으로 대체되고 역 이산 코사인 변환(Inverse Discrete Cosine Transform)을 수행하여 정보가 은닉된 이미지를 얻는다. 제안하는 알고리즘의 성능을 분석하기 위해 JPEG(Joint Photographic Coding Experts Group), 선명화(Sharpening), 히스토그램 등화(Histogram Equalization)와 같이 다양한 이미지 변화를 거친 후, 은닉된 정보의 신뢰도를 비교한다.

1. 서론

최근 들어 통신 기술의 발전 및 디지털 기기의 사용 확대로 인하여 음성, 이미지를 포함한 다양한 디지털 컨텐츠의 생산 및 보급이 활성화 되고 있다. 기존의 아날로그 컨텐츠와 달리 복제 및 배포가 간단한 디지털 컨텐츠의 속성에 따라 저작권을 지키기 위한 방법의 강구가 시급한 실정이다. 워터마킹을 포함한 정보 은닉 기법은 불법 복제를 막기 위한 저작권 보호 기술로써 중요성이 증대되어 가고 있는 실정이다.

정보 은닉 기법은 크게 공간 영역과 주파수 영역에서 이루어진다. 최근에는 DCT(Discrete Cosine Transform)[1], DWT(Discrete Wavelet Transform)[2]와 같은 변환을 이용한 주파수 영역에서의 은닉 기법이 주로 이용되고 있다. 이는 주파수 영역에서의 정보 은닉이 공간영역에서의 정보 은닉에 비하여 다양한 이미지 변화에 대해 강인하기 때문이다. 정보 은닉 기술로써는 LSB(Least Significant Bit)[3], Spread Spectrum[4]을 이용하는 방법부터 최근에는 QIM(Quantized Index Modulation)[5], SVD(Singular Value Decomposition)[6]등이 이용되고 있다.

디지털 컨텐츠가 확산 및 배포되는 단계에서 사용자에 의한 수정이나 웹의 표준에 따라 포맷 변화가 발생한다. 따라서 부가적으로 컨텐츠에 은닉되어 있는 정보도 왜곡될 수 있는 가능성이 높아진다. 따라서 컨텐츠의 변화에 견딜 수 있는 정보은닉 알고리즘의 개발이 필요하다.

본 논문에서는 이미지를 기준으로 이상의 문제점에 견딜 수 있는 알고리즘을 제안한다. 구체적으로 블록 기반의 DCT 를 통하여 이미지를 주파수 영역으로 이전하고, 인접한 네 블록의 DC 값으로 이루어진 행렬의 특이값 분해(SVD)를 통하여 정보를 은닉하는 방법을 제시한다..

본 논문의 구성은 다음과 같다. 2 절에서는 특이값 분해에 대해 살펴본 후, 3 절과 4 절에서는 본 논문에서 제안하는 정보 은닉 및 추출 알고리즘을 설명한다. 5 절에서는 제안한 알고리즘의 성능을 실험을 통해서 확인하고, 마지막으로 6 절에서는 본 논문의 결론을 맺는다.

2. 특이값 분해

특이값 분해(Singular Value Decomposition)는 임의의 행렬의 본질적인 특성을 알 수 있는 수치해석 방법이다. 예를 들어 임의의 $m \times n$ 행렬 A는 특이값 분해를 통해 다음과 같이 세 개의 행렬로 분해된다.

$$A = U \times \Sigma \times V^T \quad (1)$$

U 는 $m \times m$, V 는 $n \times n$ 유니터리 행렬이고 S 는 $m \times n$ 대각선행렬이다. Σ 의 대각선 원소 σ 를 특이값(Singular Value)라고 부르고 아래와 같은 성질을 갖는다.

$$\Sigma = \begin{pmatrix} \sigma_1 & 0 & 0 \\ 0 & \sigma_{\cdots} & 0 \\ 0 & 0 & \sigma_p \end{pmatrix} \quad (2)$$

$$\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_p \geq 0, \quad p = \min(m, n)$$

3. 정보 은닉 알고리즘

디지털 컨텐츠에 은닉하고자 하는 정보, w 는 바이너리 시퀀스로 표현이 가능하다. 본 논문에서는 이미지에 비트 단위로 정보를 은닉한다.

$$w = (w_1 w_2 w_3 \cdots w_i \cdots w_n) = 010 \cdots 0, \quad 0 \le i \le n \tag{4}$$

컬러 이미지는 R, G, B 세 개의 채널로 분해가 가능하다. 정보 은닉 이후에도 이미지의 품질을 유지하기 위해 인간의 눈에 둔감한 B 채널의 이미지를 사용한다. 8×8 블록단위의 2 차원 DCT 를 이용하여 B 채널의 이미지를 주파수 영역으로 확장한다. 한 비트의 정보를 숨기기 위해 총 네 개의 인접한 블록을 한 단위로 이용한다. 먼저 그림 1 과 같이 인접한 네 개 블록의 DC 값으로 구성된 2x2행렬 A_i를 구한다.

$$A_i = \begin{bmatrix} A_i^{11} & A_i^{12} \\ A_i^{21} & A_i^{22} \end{bmatrix} \tag{5}$$

행렬 A_i에 대하여 특이값 분해를 수행하여 행렬 Σ_i를 구한다.

$$\Sigma_i = \begin{bmatrix} \sigma_1^i & 0 \\ 0 & \sigma_2^i \end{bmatrix} \tag{6}$$

0 또는 1 로 구성된 정보를 은닉하기 위하여 Σ_i행렬의 특이값 σ_2^i를 수정한다. σ_2^i는 σ_1^i에 비하여 행렬 Σ_i에 대한 기여도가 적기 때문에 이를 통한 정보은닉은 이미지 품질의 저하를 줄일 수 있다.

$$w_i = 1, \quad \sigma_2^i = \alpha, \qquad \alpha > 0 \tag{7}$$

$$w_i = 0, \quad \sigma_2^i = 0 \tag{8}$$

정보에 따라 수정된 특이값에 대하여 $U \times \Sigma \times V^T$ 를 통해 수정된 DC 값들로 이루어진 행렬 A_i^* 를 얻을 수 있다. 은닉하고자 하는 정보의 모든 비트에 대하여 위의 과정을 반복한다. 이를 수행한 이미지에 대해 8×8 블록단위의 2 차원 역 DCT 를 수행하여 정보가 은닉된 이미지를 얻을 수 있다.

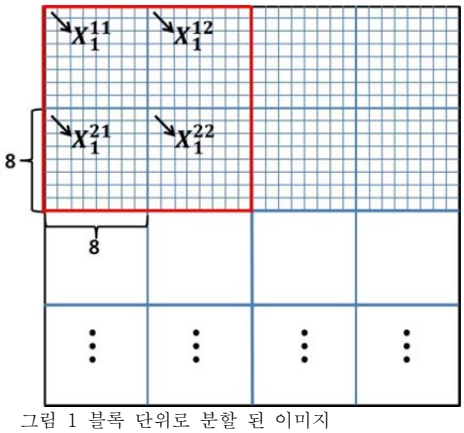


그림 1 블록 단위로 분할 된 이미지

4. 정보 추출 알고리즘

정보 추출 시에는 정보 은닉 시와 같이 원본 이미지에 대하여 8×8 블록단위의 2 차원 DCT 수행한다. 이를 통해 얻어진 블록 A_i^*에 대하여 특이값 분해를 수행하여 행렬 Σ_i^*를 구한다.

$$\Sigma_i^* = \begin{bmatrix} \sigma_1^{*i} & 0 \\ 0 & \sigma_2^{*i} \end{bmatrix} \tag{9}$$

정보를 추출하기 위하여 σ_2^{*i} 의 α 와 0 까지의 유클리드 거리를 비교한다. 복잡도를 줄이기 위해 α 와 0 의 중간값 β 를 비교 기준으로 설정한다.

$$\beta = \frac{0+\alpha}{2} \tag{10}$$

원본 이미지의 왜곡 또는 이미지 압축에 대해 특이값의 변화를 고려하여 β에 가중치를 준다.

$$\beta^* = c * \beta, \qquad 0 < c \le 1 \tag{11}$$

따라서 이미지에 은닉된 정보는 다음과 같이 추출된다.

$$\sigma_2^{*i} > \beta^*, \quad w_i^* = 1 \quad , 1 \le i \le n \tag{12}$$

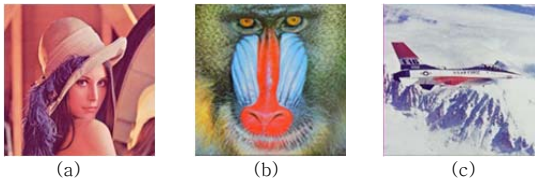
$$\sigma_2^{*i} < \beta^*, \quad w_i^* = 0 \quad , 1 \le i \le n \tag{13}$$

n 개의 비트에 대해서 위의 추출과정을 수행하면 은닉된 정보 w^*을 얻을 수 있다.

$$w^* = (w_1^* w_2^* w_3^* \cdots w_n^*) \tag{14}$$

5. 실험 결과 및 성능 분석

본 실험에서는 제안된 알고리즘의 성능을 확인하기 위하여 임의의 비트 시퀀스가 은닉된 이미지에 다양한 변화를 가한 후 원 정보를 추출하는 실험을 전개하였다. 성능 비교를 위해 BER(Bit Error Rate)를 이용하였고, α 는 70, c = 0.6 을 이용하였다. 또한 이미지 압축과 변화는 포토샵을 이용하였다.



(a) (b) (c)

그림 2 정보은닉에 이용된 이미지 (a) Lena (b) Baboon (c) F-16

(a) (b) (c)

그림 3 제안한 알고리즘을 적용하여 정보가 은닉된 이미지
(a) Lena (b) Baboon (c) F-16

Sample Image (Size)	Lena (512x512)	Baboon (512x512)	F-16 (512x512)
Total Bits	1000 bits		
Attack	BER = Error Bits / Total Bits		
JPEG QF 100	0	0	0
JPEG QF 80	0	0	0
JPEG QF 60	0	0.001	0.001
JPEG QF 40	0.099	0.15	0.073
Sharpening	0.033	0.034	0.014
Equalization	0.065	0.062	0.25
Median Filter 3 pixel	0.119	0.239	0.096

표 1 다양한 이미지 변화에 대한 제안된 알고리즘의 성능 비교

표 1 에 따라 제안된 알고리즘이 JPEG QF 80 까지는 정보를 완벽하게 복원할 수 있음을 확인할 수 있었다. 또한 JPEG QF60,40, 선명화 및 히스토그램 등화에도 정보 복원에 높은 신뢰도를 보였다. 반면에 중간값 필터에서는 상대적으로 낮은 복원률을 보였다.

6. 결론

본 논문에서는 SVD 를 이용하여 다양한 이미지 변화에 강인한 정보은닉 알고리즘을 제시하였다. 실험 결과를 통해서 이미지 품질을 유지하면서 JPEG 압축 시 QF 60 까지 정보의 높은 신뢰도를 유지하였고, 등화, 선명화와 같은 다양한 이미지 변화에도 강인한 성능을 보였다. 또한 정보 추출 시의 원본 이미지가 불필요하기 때문에 알고리즘 이용의 제약을 줄였다. 제안된 알고리즘에 오류정정부호를 적용한다면 등화, 선명화뿐만 아니라 JPEG 압축의 경우는 QF40 까지 정보가 견딜 수 있을 수 있을 것으로 예상된다.

ACKNOWLEDGEMENT

본 연구는 삼성 전자 산학 연구결과로 수행되었음

참고문헌

[1] F.M. Boland, J.J.K. O'Ruanaidh, C. Dautzenberg, "Watermarking digital images for copyright Protection", in *Proc. IEE Int. Conf. on Image Processing and Its Applications*, pp. 326-330, Edinburgh, U.K., July 1995.

[2] J.J. Chae and B.S. Manjunath, "A Robust Embedded Data from Wavelet Coefficients", in *SPIE'98, Proceedings of the SPIE International Conference on Storage and Retrieval for Image and Video Databases VI*, San Jose, CA, 1998.

[3] I. Cox, J. Kilian , F. T. Leighton and T. Shamoon "Secure spread spectrum watermarking for multimedia", *IEEE Trans. Image Process.*, vol.6, pp. 1673 1997

[4] Chi-Kwong Chan and L.M. Cheng, "*Hiding Data in Images by Simple LSB substitution", Pattern Recognition*, Vol. 37, pp. 469-474, 2004

[5] B. Chen and G. W. Wornell "*Quantization index modulation: A class of provably good methods for digital watermarking and information embedding", IEEE Trans. Inf. Theory*, vol. 47, pp.1423 2001

[6] Chi-Kwong Chan and L.M. Cheng, "*Hiding Data in Images by Simple LSB substitution", Pattern Recognition*, Vol. 37, pp. 469-474, 2004