차분 영상의 히스토그램 특성을 이용한 무손실 정보은닉 알고리즘

이상광, 호요성

광주과학기술원 정보통신공학과

Lossless Information Hiding Based on the Histogram of the Difference Image

Sang-Kwang Lee and Yo-Sung Ho
Kwangju Institute of Science and Technology (K-JIST)
E-mail: {sklee, hoyo}@kjist.ac.kr

요약

본 논문에서는 숨겨진 정보를 검출한 후, 정보가 삽입된 영상으로부터 왜곡없이 원본 영상을 복원할 수 있는 무손실 정보은닉(lossless information hiding) 알고리즘을 제안한다. 제안된 알고리즘은 차분 영상(difference image)의 히스토그램 특성을 기반으로 화소값을 수정하여 데이터를 삽입한다. 이 알고리즘은 기존의 무손실 정보은닉 알고리즘들에 비해 정보 삽입으로 인한 왜곡이 적고, 많은 양의 정보를 삽입할 수 있다. 이론적인 증명과 실험 결과를 통해 제안된 알고리즘에 의해 정보가 삽입된 영상의 PSNR(peak singal-to-noise ratio) 값은 대략 51 dB 이상의 값을 나타내며, 이 값은 다른 무손실 정보은닉 알고리즘들 보다 훨씬 높다. 또한, 제안된 알고리즘은 여러 형태로 변형되어 다양한 응용에 적절히 적용될 수 있다.

1. 서론

멀티미디어 컨텐츠의 디지털 표현은 원본 컨텐츠와 동일한 여러 복사본을 쉽고 널리 배포할 수 있다는 장점을 가지고 있다. 하지만, 원본과 동일한 형태의 수많은 복사본이 불법적으로 생산될 수 있다는 사실은 음반, 영화, 도서, 그리고 소프트웨어 출판 산업에 심각한 위협이 된다. 이러한 저작권(copyright) 보호에 대한 문제를 해결하기 위해 디지털 미디어 자체에 저작권 정보와 일련 번호(serial number)를 숨기는 연구가 시작되었다.

삽입된 일련 번호는 저작권 위반자를 가려내는데 도움을 주고, 저작권 정보는 그들을 기소하는데 이용될 수 있다. 동시에, 암호 서비스의 이용을 제한하는 정부 기관들의 움직임으로, 겉으로 구별되지 않도록 개인 정보를 삽입하는 방법의 연구가 진행되고 있다. 이러한 정보 은닉은 컨텐츠 안에 메시지를 삽입하는 문제를 넘어 폭넓은 범위를 포함하는 일반적인 개념이다. 여기서 은닉의 개념은 정보를 감지할 수 없도록 만드는 것, 또는 정보의 존재를 은밀히 하는 것이라고 말할 수 있다.

컨텐츠 내에 정보를 삽입하는 정보은닉 기술은 암호화 서명처럼 따로 저장할 필요가 없고, 삽입된 정보가 컨텐츠에 적용되는 동일한 변환을 겪는다는 장점을 가지고 있다. 하지만, 정보은닉 시스템은 정보삽입 과정에서 발생되는 왜곡을 피할 수 없다는 단점을 가지고 있다. 일반적으로 이러한 왜곡은 양자화, 비트 교환(bit-replacement), 화소값 0과 255에서의 잘림(truncation) 등으로 인해 완전히 제거될 수 없다. 비록 왜곡이 매우 작을지라도, 의료 영상이나 전략상 중요성을 갖는 군사 영상에서는 중요한 문제가 될 수 있다. 따라서, 삽입된 정보를 검출한 후, 원본 컨텐츠를 복원할 수 있는 기술이 요구되며, 이러한 요구를 만족하는 기술을 무손실 정보은닉 기술이라고 한다.

최근 무손실 정보 은닉에 관한 많은 연구들이 발표되고 있다. Honsinger[1]는 공간 영역에서의 무손실 정보은닉 방법을 제안하였다. 이 방법은 원본 영상에 해쉬 값을 삽입하기 위해 모듈로 256 덧셈을 이용하였다. 또 하나의 공간 영역에서의 방법으로 Fridrich[2]는 데이터 삽입을 위해 적당한 비트 화면(bit-plane)을 선택하여 무손실 압축한 후, 압축한 비트 화면과 해쉬 값을 삽입하였다.

변환 영역에서의 무손실 정보은닉 방법으로 Macq[3]는 무손실 다해상도(multiresolution) 변환과 패치워크(patchwork) 개념을 이용하였다. Goldjan[4]은 많은 양의 데이터를 삽입하기 위한 방법을 제안하였다. 이 방법의 삽입 용량은 512x512x8 그레이 스케일(gray scale) 영상에 대해 3-24 kbits로 여전히 충분하지 않다. 또한, 삽입 용량이 늘어나면 심각한 화질 저하를 초래한다. Xuan[5]은 정수 웨이브렛 변환을 이용한 방법을 제안하였다. 이 방법은 19-54 kbits의 상당히 많은 양의 정보를 삽입할 수 있지만, 선처리(preprocessing) 과정으로 수행되는 히스토그램의 수정으로 정보가 삽입된 영상과 원본 영상 사이의 PSNR 값이 낮다.

Ni[6]는 원본 영상의 히스토그램이 0이 되는 점과 최대가 되는 점을 이용한 방법을 제안하였다. 512x512x8 그레이 스케일 영상에 대해 5-60 kbits의 비교적 많은 양을 삽입할 수 있으며, 모든 영상에 대해 48 dB 이상의 높은 PSNR 값을 보장한다. 하지만, 검출 과정에 필요한 부가 정보를 전송해야 하며, 한 개 이상의 0이 되는 점과 최대가 되는 점이 존재할 경우를 고려하여 알고리즘을 적용해야 하는 단점이 있다.

본 논문에서 차분 영상의 히스토그램 특성을 이용한 무손실 정보은닉 방법을 제안한다. 주어진 영상을 홀수 행과 짝수 행으로 구성된 영상으로 나눈 후, 두

영상으로부터 차분 영상을 생성한다. 차분 영상으로부터 히스토그램을 구한 후, 그 특성을 이용하여 정보를 삽입한다. 제안한 알고리즘은 Ni의 알고리즘[6]에 비해 1-24배 정도의 정보를 삽입할 수 있으며, 512x512x8 그레이 스케일 영상에 대해 51 dB 이상의 높은 PSNR 값을 보장한다. 또한, 알고리즘이 매우 간단하고 삽입 및 검출 시간이 매우 짧으므로 실시간 정보은닉 시스템에 적합하다.

2. 히스토그램을 이용한 기존의 알고리즘

이 절에서는 Ni[6]가 제안한 히스토그램 기반의 무손실 정보은닉 알고리즘을 살펴본다. 삽입 과정은 다음과 같다. 우선, 주어진 영상으로부터 히스토그램을 구한다. 히스토그램으로부터 0이 되는 점을 찾는다. 예를 들면, 그레이 레벨(gray level) 255 값을 갖는 화소가 없는 경우, 255가 0이 되는 점이 된다. 그런 후, 최대가 되는 점을 찾는다. 가령, 그레이 레벨 154 값을 갖는 화소가 가장 많을 경우, 154가 최대가 되는 점이 된다. 전체 영상에 대해, 그레이 레벨 155에서 254 사이의 값을 갖는 화소의 그레이 레벨을 1씩 증가시킨다. 즉, 히스토그램 범위 [155,254]를 1씩 이동시켜 그레이 레벨 155 값이 비워지도록 만든다.

전체 영상을 스캔하면서 그레이 레벨 154 값을 만나면 정보를 삽입할 것인지 결정한다. 만약 삽입될 정보 비트가 1이면 화소값을 1 증가시켜 155 값으로 만들고, 삽입될 정보 비트가 0이면 건너뛴다. 이 알고리즘의 정보 수용량은 최대가 되는 점의 히스토그램 값이 된다.

아주 드문 경우, 히스토그램에서 0이 되는 점이 발견되지 않을 수 있다. 이런 경우, 0이 되는 점 대신 최소가 되는 점을 이용할 수 있다. 예를 들면, 그레이 레벨 7 값의 화소 개수가 23이고 최소의 개수인 경우, 다른 그레이 레벨 값을 갖는 화소의 개수가 23 이상이라고 가정하여 0이 되는 점 대신 사용한다. 이 때, 그레이 레벨 7 값과 화소 개수 23이 부가 정보로 따로 송신되어야 한다. 또한, 0이 되는 점과 최대가 되는 점도 수신측에서 정보를 검출하는데 필요한 부가 정보로서 정보가 삽입된 영상과는 별도로 송신되어야 한다.

검출 과정은 다음과 같다. 전체 영상에 대해 최대가 되는 점의 그레이 레벨을 만났을 경우, 그 값이 변경없이 154이면 0을 검출하고, 그 값이 155로 변경되었으면 1을 검출한다. 다시 한 번 전체 영상을 스캔하면서 히스토그램 범위 [156,255]를 1씩 감소시킨다. 이런 방식으로 원본 영상을 왜곡없이 복원할 수 있다. 0이 되는 점이 한 개 이상일 경우, 삽입 과정에서 설명한 부분을 숙지하여 검출해야 한다.

이 알고리즘은 512x512x8 그레이 스케일 영상에 대해 5-6Kbits의 비교적 많은 양을 삽입할 수 있으며, 모든 영상에 대해 48 dB 이상의 높은 PSNR 값을 보장한다. 삽입 과정에서 0이 되는 점과 최대가 되는 점 사이의 그레이 레벨을 갖는 화소들은 1씩 더해지거나 빼지게 된다. 최악의 경우, 영상의 모든 화소가 1씩 더해지거나 빼지게 되면 MSE(mean square error) 값은 1이 되며, PSNR=$10\times\log_{10}(255\times255)$=48.13 dB가 된다.

본 절에서 설명한 알고리즘은 검출 과정에 필요한 부가 정보를 전송해야 하며, 한 개 이상의 0이 되는 점과 최대가 되는 점이 존재할 경우를 고려하여 알고리즘을 적용해야 하는 단점이 있다. 또한, 영상 히스토그램 자체의 특정 부분이 국부적으로 변경되므로 보안성(security) 문제가 발생된다.

3. 제안된 알고리즘

본 논문에서는 차분 영상의 히스토그램 특성을 이용한 무손실 정보은닉 방법을 제안한다. 삽입 과정은 다음과 같다. 우선, 주어진 영상을 홀수 행과 짝수 행으로 구성된 영상으로 나눈 후, 두 영상으로부터 차분 영상을 생성한다. 차분 영상으로부터 히스토그램을 구한 후, 히스토그램의 최대가 되는 점인 차이값 0을 중심으로 두 방향의 정보 삽입 과정을 수행한다. 즉, 두 번째와 세 번째 최대값을 갖는 차이값 -1과 1을 이용하여 정보를 삽입한다. 예를 들면, 차이값의 범위가 [-82,108]이고 차이값 -1을 이용하는 경우, 차이값 -2 비우기 위해 히스토그램 범위 [-82,-2]를 -1씩 이동시킨다. 마찬가지로 차이값 1을 이용하는 경우, 차이값 2를 비우기 위해 히스토그램 범위 [2,108]을 1씩 이동시킨다.

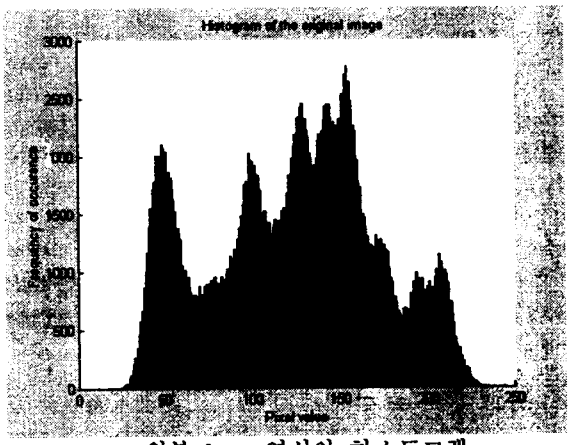
전체 영상을 스캔하면서 그레이 레벨의 차이값이 -1 또는 1 값을 만나면 정보를 삽입할 것인지 결정한다. 만약 삽입될 정보 비트가 1이면 차이값 -1을 만난 경우 차이값을 1 감소시키고 차이값 1을 만났을 경우 1을 증가시킨다. 삽입될 정보 비트가 0이면 건너뛴다. 그림 1은 원본 Lena 영상과 정보가 삽입된 영상을 보여주고 있으며, 화질 저하없이 정보가 삽입됨을 알 수 있다.

(a) 원본 Lena 영상

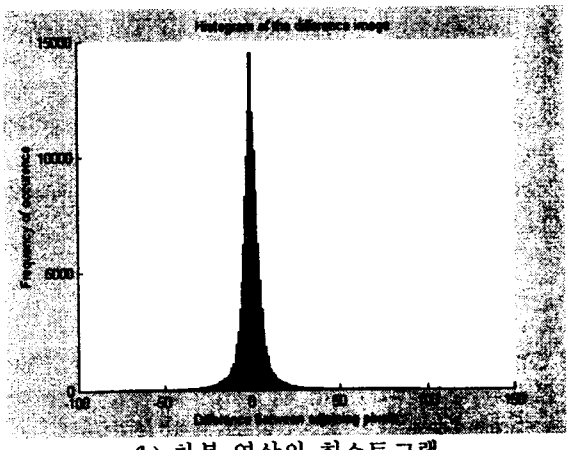
(b) 정보가 삽입된 영상(PSNR=53.2 dB)

그림 1. 정보가 삽입된 결과

이러한 방법으로 삽입할 수 있는 정보 용량은 차이값 -1과 1 점에서의 히스토그램 값들의 합이 된다. 차분 영상의 히스토그램은 영상 자체의 히스토그램에 비해 몇 개의 특정 점에서의 압축(compaction)이 잘되므로 삽입 용량을 증가시킬 수 있다. 그림 2는 이러한 압축 특성을 보여주고 있으며, 실험은 2절에서 설명한 알고리즘에 비해 1-24배 이상의 정보를 삽입할 수 있다는 것을 보여 준다.



(a) 원본 Lena 영상의 히스토그램



(b) 차분 영상의 히스토그램

그림 2. 차분 영상 히스토그램의 압축 특성

검출 과정은 다음과 같다. 정보가 삽입된 영상을 홀수 행과 짝수 행으로 구성된 영상으로 나눈 후, 두 영상으로부터 차분 영상을 생성한다. 차분 영상으로부터 히스토그램을 구한 후, 차이값이 -1과 1되는 점을 검사하여, 그 값이 변경없이 -1이거나 1이면 0을 검출하고, 그 값이 -2나 2로 변경되었으면 1을 검출한다. 다시 한 번 전체 영상을 스캔하면서 히스토그램 범위 [-83,3]을 1씩 증가시키고, [3,109]를 1씩 감소시킨다. 이런 방식으로 원본 영상을 왜곡없이 복원할 수 있다.

제안한 알고리즘은 모든 영상에 대해 51 dB 이상의 높은 PSNR 값을 보장한다. 최악의 경우, 차분 영상의 모든 화소가 1씩 더해지거나 빼지게 된다. 이런 경우, 차분 영상의 크기는 원본 영상의 반이 되므로 MSE 값은 1/2이 된다. 즉, PSNR=$10\times\log_{10}(255\times255\times2)$ =51.14 dB가 되어 2절에서 설명한 알고리즘 보다 약 3 dB 정도가 증가된다.

2절에서 설명한 알고리즘과 비교해 볼 때, 제안한 알고리즘은 수신측에 부가 정보를 전송할 필요가 없으며, 0이 되는 점과 최대가 되는 점의 개수를 고려할 필요가 없다. 또한, 차분 영상의 히스토그램이 수정되므로 영상 히스토그램 자체에서는 전체적으로 확산된 형태의 수정으로 나타난다. 하지만, 알고리즘이 공개되었을 경우, 정보가 삽입될 곳을 정확히 알 수 있으므로 보안성 문제가 발생한다. 이 문제를 해결하기 위해, 제안한 알고리즘은 보안성이 고려된 알고리즘으로 변형될 수 있다.

4. 실험 결과 및 분석

제안한 무손실 정보은닉 알고리즘의 성능을 평가하기 위해, 다양한 형태의 영상에 적용하여 정보 용량과 PSNR을 측정해 보았다. 그림 3은 실험에서 삽입된 280x70 크기의 이진 영상을 보여주고 있다. 즉, 삽입된 정보 용량은 19,600 bits이다.

그림 3. 삽입된 이진 영상(280x70)

512x512x8 그레이 스케일 Lena 영상에 대해, 차분 영상의 히스토그램을 살펴보면, 차이값 -1에 해당되는 히스토그램 값이 11,944, 1에 해당되는 값은 11,903으로 정보 용량은 23,847 bits가 된다.

그림 4는 실험으로 사용된 8개의 512x512x8 그레이 스케일 영상을 보여주고 있다. 표 1과 표 2는 그림 4의 실험 영상들에 대해 PSNR 값과 정보 용량을 Ni의 알고리즘과 비교한 표이다. 표 1은 Ni의 알고리즘이 모든 영상에 대해 48.13 dB 이상의 PSNR을 제공하지만, 제안된 알고리즘은 51.14 dB 이상을 보장한다는 이론적 증명을 실험으로 보여주고 있다. 표 2는 Ni의 알고리즘이 1.6-21.9 kbits의 정보를 삽입할 수 있지만, 제안된 알고리즘은 7.4-39.7 kbits의 정보를 삽입할 수 있다는 것을 보여주고 있다. 즉, 1-24배 이상의 정보 용량을 갖는다.

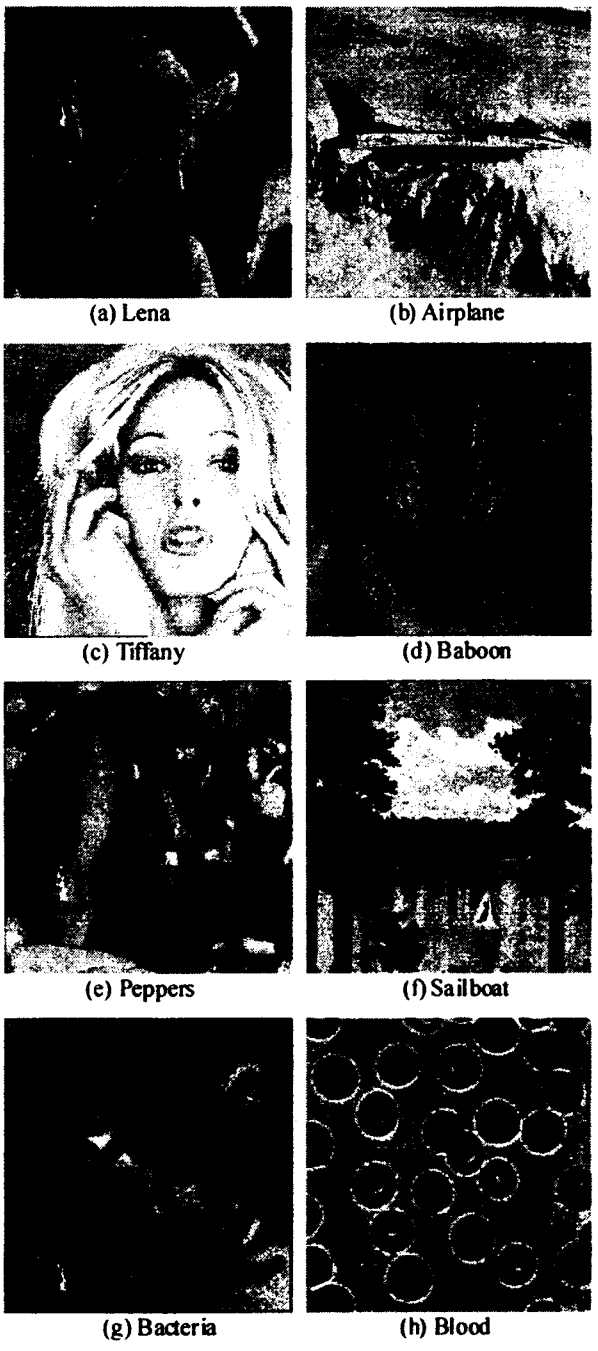
제안된 알고리즘은 Baboon 영상과 같이 인접하는 화소간의 변화의 차가 큰 복잡한 영상의 경우, 차분 영상 히스토그램의 압축 특성이 크게 줄어 정보 용량이 그만큼 감소하게 된다. 반대로, Bacteria 영상과 같이 화소의 변화가 적은 단조로운 영상의 경우, 차분 영상 히스토그램의 압축 특성이 뚜렷히 나타나 많은 양의 정보를 삽입할 수 있다. 실제로 두 영상의 정보 용량 차이는 약 5배 정도 차이가 난다는 것을 알 수 있다.

표 1. Ni의 알고리즘과 PSNR 비교

실험 영상 (512x512x8)	PSNR (dB)	
	Ni의 방법	제안된 방법
Lena	48.2	53.2
Airplane	48.3	54.5
Tiffany	48.2	53.6
Baboon	48.2	52.7
Peppers	48.2	53.3
Sailboat	48.2	54.4
Bacteria	48.2	55.2
Blood	48.2	58.1

표 2. Ni의 알고리즘과 정보 용량 비교

실험 영상 (512x512x8)	정보 용량 (bits)	
	Ni의 방법	제안된 방법
Lena	5,460	23,847
Airplane	16,171	30,487
Tiffany	8,782	26,059
Baboon	5,421	7,399
Peppers	5,449	17,280
Sailboat	7,301	14,391
Bacteria	1,642	39,665
Blood	21,890	22,009



(a) Lena (b) Airplane

(c) Tiffany (d) Baboon

(e) Peppers (f) Sailboat

(g) Bacteria (h) Blood

그림 4. 512x512x8 실험 영상들

Fridrich[2]의 알고리즘은 LSB(least significant bit)가 일반적으로 무작위 분포를 하고 있으므로 압축 효율이 높지 않고, 압축되는 데이터의 양이 많지 않아 충분한 정보 용량을 보장하지 못한다. 또한, 비트 화면의 압축으로 화질 저하가 심하다. 따라서, 제안된 알고리즘의 결과가 모든 영상에 대해 기존의 무손실 정보은닉 알고리즘들에 비해 높은 PSNR 값을 갖는 동시에, 높은 정보 용량을 제공하고 있다.

5. 결론

본 논문에서는 차분 영상의 히스토그램 특성을 이용한 무손실 정보은닉 알고리즘을 제안하였다. 제안된 알고리즘은 512x512x8의 그레이 스케일 영상에 대해 기존의 알고리즘들에 비교하여 많은 양의 정보를 삽입할 수 있으며, 동시에 51 dB 이상의 PSNR 값을 유지한다. 특히, 화소간의 변화가 적은 단조로운 영상의 경우, 차분 영상 히스토그램의 압축 특성이 뚜렷하여 많은 양의 정보를 삽입할 수 있었다. 또한, 알고리즘이 매우 간단하여 컬러 영상에 쉽게 확장되어 적용될수 있으며, 삽입 및 검출 시간이 매우 짧으므로 실시간 정보 은닉 시스템에 적합하다. 차분 영상의 히스토그램을 이론적으로 분석하여 알고리즘을 적용한다면 보안성 문제도 해결될 수 있다.

감사의 글

본 연구는 광주과학기술원(K-JIST)과 광주과학기술원 실감방송연구센터를 통한 대학IT연구센터(ITRC), 그리고 교육부 두뇌한국21(BK21) 정보기술사업단의 지원에 의한 것입니다.

참고 문헌

[1] C.W. Honsinger, P. Jone, M. Rabbani, and J.C. Stoffel, "Lossless recovery of an original image containing embedded data," US Patent: 6,278,791 B1, 2001.

[2] J. Fridrich, M. Goldjan, and R. Du, "Invertible authentication," *Proc. SPIE, Security and Watermarking of Multimedia Contents*, pp. 197-208, Jan. 2001.

[3] B. Macq and F. Deweyand, "Trusted headers for medical images," *DFG VIII-D II Watermarking Workshop*, Oct. 1999.

[4] M. Goldjan, J. Fridrich, and R. Du, "Distortion-free data embedding," *Proceedings of 4th Information Hiding Workshop*, pp. 27-41, April 2001.

[5] G. Xuan, J. Zhu, J. Chen, Y.Q. Shi, Z. Ni, and W. Su, "Distortionless data hiding based on integer wavelet transform," *IEE Electronics Letters*, vol. 38, no. 25, pp. 1646-1648, December 2002.

[6] Z. Ni, Y.Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *Proc. ISCAS 2003*, vol. 2, pp. 912-915, May 2003.