# 인접 화소들을 이용한 무손실 정보은닉 알고리즘

오 관 정, 이 상 광, 호 요 성 광주과학기술원 정보통신공학과

전화: 062-970-2258 / 핸드폰: 019-645-0603

## Lossless Information Hiding Algorithm Using Neighboring Pixels

Kwan-Jung Oh, Sang-Kwang Lee, Yo-Sung Ho Gwangju Institute of Science and Technology (GIST) E-mail: {kjoh81, sklee, hoyo}@gist.ac.kr

#### Abstract

In this paper, we present a lossless information hiding algorithm based on correlation of neighboring pixels. Reversible information hiding has drawn lots of interest recently. Being reversible, the original digital content can be completely restored after extracting the data. In this paper, we embed data to certain bit-plane and extract the embedded data and reconstruct to original pixel value by using the correlation of neighboring pixels.

#### I. 서론

정보은닉 기술은 고대로부터 인간사와 밀접한 관계를 가져온 기술로 최근에는 다양한 디지털 미디어 데이터 들에 대한 정보은닉 기술 및 응용에 관한 연구가 활발 히 진행되고 있다. 워터마킹(watermarking)과 스테가 노그래피(steganography)는 정보은닉 기술의 대표적인 분야들이다. 이러한 정보은닉 기술에서 중요시되는 관 점은 비인지성(imperceptibility)과 정보량(capacity)이 다. 비인지성이란 정보가 삽입된 컨텐츠가 사람의 지 각 능력의 범위 내에서 정보 삽입에 의한 변화의 정도 가 감지되지 않아야 한다는 것이다. 정보량은 삽입 가 능한 전체 비트수를 말한다. 디지털 영상의 경우 PSNR과 정보량을 이용하여 알고리즘의 비인지성과 정보량을 비교한다. 이와 같이 기존의 정보은닉 기술 의 주된 목적은 사람의 지각 능력이 허용하는 범위 내 에서 가능한 많은 정보를 삽입하는 것이었다[1]. 하지 만 최근에는 의료 영상이나 군사 영상과 같이 작은 왜 곡에도 민감한 분야에 적합한 무손실 정보은닉 기술들

이 관심을 받고 있다[2]. 무손실 정보은닉기술이란 정보검출 과정에서 원본 데이터로의 복원이 가능한 기술들을 말한다. 이러한 무손실 정보은닉 기술들은 삽입알고리즘의 복원성에 따라 크게 부가정보가 필요한 방식과 필요치 않는 방식으로 구분될 수 있다. 본 논문은 후자의 경우이며, 컨텐츠의 완전 복원을 위해 복원이 불가능한 화소에 대한 맵정보와 원본비트를 부가정보로 사용한다[3].

본 논문에서는 디지털 영상에서 인접한 화소들이 높은 상관관계를 갖는다는 점을 이용하다. 높은 상관관계를 갖는 인접 화소들을 이용하면 정보가 삽입된 화소를 원본 화소로 복원할 수 있다. 인접 화소들의 표준편차의 범위를 제한하면 그 복원성은 더욱 향상된다. 이에 기반하여 높은 상관관계를 갖는 블록들에 대해 정보를 삽입하고 인접 화소를 이용하여 원본 영상으로 복원한다.

#### Ⅱ. 정보삽입 알고리즘

디지털 영상에서 인접한 화소들은 상대적으로 높은 상 관관계를 갖으며, 비트평면을 기준으로 상위 비트평면으로 갈수록 그 상관도는 높아진다. 이를 이용하여 특정 비트평면까지의 복원이 가능하다. 그림 1과 같이 3×3 블록에서 중앙에 위치한 화소는 상하좌우 인접한 4개의 화소의 평균값에 의해 특정 비트평면까지 어느정도 복원이 가능하다. 본 논문에서는 인접 화소들의 표준편차를 이용하여 상관관계를 나타낸다. 즉, 표준편차의 범위를 제한함으로써 원본 비트로의 복원율을 향상시킬 수 있다. 향상된 복원율을 이용하여 주어진 영상에 대해 각 비트평면에 대한 최대 정보 수용량을 가지는 표준편차의 범위와 그 정보량을 구할 수 있다.

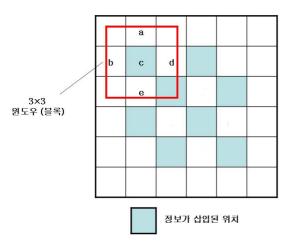


그림 1. 3×3 윈도우와 정보삽입 위치

#### 2.1 정보삽입

본 논문에서 정보 삽입의 기본 단위는 3×3 블록으로 한다. 그림 2와 같이 정보가 삽입될 비트평면에 대해 블록의 표준편차가 어떤 임계값 이하를 가질 때만 정보를 삽입한다. 정보삽입 방법은 화소의 특정 비트평면을 원하는 정보 비트로 대체하는 것이다. 복원이 불가능한 블록에 대해서는 해당 화소의 위치 정보를 나타내는 맵정보와 원본 비트값을 부가정보로 만들어 은닉할 데이터와 함께 삽입한다. 정보의 삽입 및 검출과정에서 임계값으로 사용되는 표준편차의 계산은 다음과 같다.

표준편차 = 
$$\sqrt{\frac{1}{4}\sum_{i=1}^{4}(n_i-m)^2}$$
 (1)

여기서 n는 a, b, d, e이고 m은 a, b, d, e의 평균을 나타낸다.

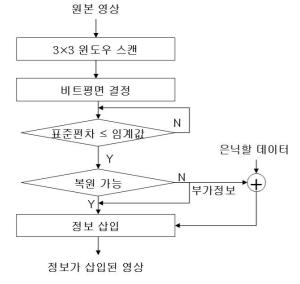


그림 2. 정보삽입 순서도

$$|m - c| < |m - c'|$$
 : 복원 가능  $|m - c| \ge |m - c'|$  : 복원 불가능 (2)

식 (2)는 복원성을 판단하는 식으로 c'는 특정 비트 평면의 비트가 원본 데이터와 다르게 조작된 값이다. 예를 들어, c의 값이  $16=00010000_{12}$ 이라면 2번째 비트 평면의 조작에 대한 복원성 판단을 위한 c'의 값은  $18=00010010_{12}$ 이 된다. m과 원본 화소값의 비교를 통해 검출 과정에서 복원이 불가능한 화소에 대한 맵정보와 원본 화소값 정보를 모아서 부가정보를 만든다. JBIG2를 이용하여 맵정보를 압축함으로써 부가정보를 크게 줄인다.

제안한 알고리즘에서 삽입 가능한 총 정보량은 복 원 가능한 비트수와 부가정보 비트수의 차로 나타내어 질 수 있다[3].

$$P \le B - Mc \tag{3}$$

여기서 P는 은닉될 데이터량을, B는 복원 가능한 비 트의 수를, 그리고 Mc는 압축된 맵정보를 나타낸다. 식 (3)에서 보듯이, 정보량은 압축된 맵정보에 영향을 받는다. m이 원본 화소값에 가까울수록 데이터의 복원 성이 좋아지고, 이는 맵의 중복성을 높여 맵의 압축효 율에 영향을 미친다. 따라서 원본 화소에 최대한 가까 운 m을 구하는 것이 중요하다. 본 논문에서는 인접한 화소들의 평균을 m으로 이용하였다. 3×3 윈도우에서 주변 8개의 화소를 이용하여 인접 화소들의 통계적 분 포 특성에 따른 가중치를 이용하면 더 높은 데이터 복 원율을 갖는 m값을 얻을 수 있다. 그러나 8개의 화소 를 이용하는 경우 정보 삽입에 이용 가능한 블록의 수 가 4개를 이용한 경우에 비해 절반 정도에 불과하다. 따라서 Baboon과 같이 복잡한 영상에서는 데이터의 복원율이 높아져 성능이 향상되었으나, 대부분의 영상 에서는 복원율의 향상이 미비하여 결과적으로 정보량 의 효율성이 떨어진다.

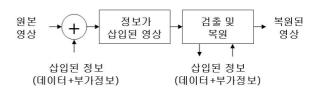


그림 3. 정보삽입 및 검출 과정

실제 응용에서는 표준 편차의 범위를 조절함으로써 원하는 정보량이나 PSNR 값에 맞춘 정보 삽입이 가 능하다. 또한 삽입 및 검출 과정에서 사용되는 표준편 차의 임계값과 정보 삽입에 사용된 비트평면의 정보를 키값으로 활용하여 보안성을 제공할 수 있다. 그림 3 은 알고리즘의 정보삽입 및 검출 과정을 보여준다.

#### III. 정보검출 및 복원 알고리즘

정보검출 과정은 정보가 삽입된 비트평면에서 삽입된 전체 정보를 검출한 후 부가정보와 은닉된 데이터를 분리하여 은닉된 데이터를 얻어내는 과정을 말한다. 정보복원 과정은 검출과정에서 얻어진 부가정보와 알 고리즘의 복원성을 이용하여 원본 영상으로의 복원을 말한다. 위 과정은 정보검출 과정이 복원 과정보다 선 행된다.

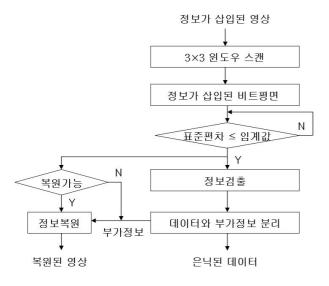


그림 4. 정보검출 순서도

그림 4와 같이 정보가 삽입된 비트평면에 대해 인접 화소의 표준편차가 정보 삽입에 이용된 임계값의 범위를 만족한다면, 해당 비트평면의 비트를 읽어서 삽입된 전체 정보를 검출한다. 삽입된 전체 정보를 은 닉하고자 한 데이터와 복원 과정에 필요한 부가정보로 분리한다.

정보검출 과정이 끝나면, 부가정보와 삽입 알고리 즉의 복원성을 이용하여 원본 영상으로 되돌리는 정보 복원 과정을 수행한다. 먼저 인접 화소들의 표준편차의 범위를 이용하여 정보가 삽입됐던 부분과 삽입되지 않았던 부분을 구분한다. 정보가 삽입됐던 부분은 맵정보를 이용하여 다시 원본 데이터로의 복원 가능한경우와 그렇지 않은 경우로 구분된다. 복원이 가능한경우는 정보가 검출된 비트평면에 대해 인접화소의 평균값인 m을 이용하여 조작된 비트를 원본 비트로 되돌린다. 이 과정에는 삽입 과정에 이용되었던 식 (2)가역으로 이용된다. 복원이 불가능한 경우는, 부가정보인 맵정보와 원본 비트값을 이용하여 해당 위치의 원본 비트값을 복원한다. 이러한 과정을 통해 복원된 영상은 정보가 삽입되기 전의 원본 영상과 정확히 일치하게 된다.

## Ⅳ. 실험 결과 및 분석

본 논문에서 제안한 무손실 정보은닉 알고리즘의 성능을 실험하기 위해 512×512×8 실험 영상을 사용하였다. 각 영상에 대해 임계값 제한 전후의 복원율을 비교하였다. 또한, 이를 기반으로 한 비트평면의 최대 정보량과 랜덤 신호 삽입에 대한 영상의 PSNR을 조사하였다. 표 1은 실험 영상의 비트평면에 대한 데이터 복원율을 보여주고 있다.

표 1. 각 비트평면에 대한 복원율(%)

비트평면 영상	비트평면2	비트평면3	비트평면4	비트평면5
Lena	64.75	76.59	89.91	96.87
Baboon	54.79	59.42	66.77	76.51
Airplane	67.02	79.17	89.62	95.53
Tiffany	62.53	72.86	85.05	93.42
Sailboat	57.32	63.76	74.15	87.94
Blood	77.89	89.90	98.21	99.91
Peppers	58.18	66.43	79.24	93.11

표 1에 보인 것처럼 Baboon과 같이 인접 화소들간의 상관관계가 낮은 복잡한 영상의 경우는 다른 영상과 비교하여 복원율이 현저히 낮은 것을 알 수 있다. 반면에 Blood 영상은 비트평면 2에서도 상대적으로 높은 복원율을 갖는다. 이와 같은 복원율의 차이는 결국정보량의 차이로 나타난다.

표 2. 임계값(th) 제한 후 비트평면에 대한 복원율(%)

비트평면				
	비트평면2	비트평면3	비트평면4	비트평면5
영상				
Lena	th=0.5	th=3.0	th=10	th=15
	72.39	82.35	92.73	98.11
Baboon	th=0.5	th=2.0	th=4.0	th=10
	68.76	78.77	85.27	89.51
Airplane	th=1.0	th=3.0	th=10	th=15
	80.18	88.37	94.41	98.38
Tiffany	th=0.5	th=3.0	th=5.0	th=10
	85.93	81.82	91.82	96.69
Sailboat	th=0.5	th=1.0	th=3.0	th=10
	70.21	79.66	81.95	92.30
Blood	th=1.5	th=5.0	th=10	th=15
	90.80	93.65	99.18	99.95
Peppers	th=0.5	th=1.0	th=4.0	th=10
	61.46	72.47	82.81	95.00

표 2는 임계값을 제한한 후, 복원율이 향상되는 것을 보여준다. 복원율의 향상은 맵정보의 압축 효율을 증가시킴으로써 정보를 삽입할 여유 공간을 만들어 준다. 표 3은 표 2의 향상된 복원율을 바탕으로 하여 비트평면 당 최대의 정보량을 구하고, 랜덤 비트 정보를 직접 삽입했을 경우의 PSNR 값을 나타낸다. 그림 5는

Airplane의 원본 영상과 비트평면 4에 정보가 삽입된 영상을 보여준다. 그림 6은 6개의 다른 실험 영상에 대한 결과를 보여준다.



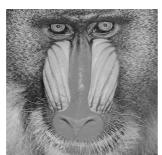


(a) 원본 영상

(b) 정보가 삽입된 영상

그림 5. Airplane 영상에 대한 결과





(a) Lena

(b) Baboon

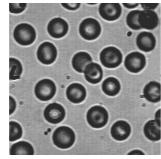




(c) Tiffany

(d) Sailboat





(e) Peppers

(f) Blood

그림 6. 정보가 삽입된 실험 영상들

표 3. 각 비트평면에 대한 정보량(bits)과 PSNR(dB)

	_ 0 _ 1	,, ,,		
비트평면 영상	비트평면2	비트평면3	비트평면4	비트평면5
Lena	0	7,072	68,721	102,098
		51.16	45.72	42.42
Baboon	0	0	4,257	22,756
			52.65	45.62
Airplane	42	25,428	68,920	100,342
	58.81	50.46	45.89	42.63
Tiffany	130	2,711	44,490	85,669
	65.10	51.20	46.63	42.69
Sailboat	0	0	5,791	51,159
			49.96	43.36
Blood	14,926	52,935	102,985	117,765
	56.72	49.62	45.77	42.53
Peppers	0	0	10,705	75,496
			47.14	42.61

## V. 결론

본 논문에서는 인접 화소들의 상관관계를 이용하여 비트평면에 정보를 은닉하는 방법을 제안하였다. 인접화소들의 표준편차를 이용하여 정보 삽입에 이용되는화소를 제한함으로써 복원율을 향상시켜서 정보량을최대화 할 수 있었다. 삽입하고자 하는 정보량이나 정보가 삽입된 영상의 PSNR에 맞추어 최소한의 조작으로 원하는 성능을 낼 수 있어서 알고리즘의 유연성면에서 커다란 장점을 갖는다.

#### 감사의 글

본 연구는 광주과학기술원(GIST)과 광주과학기술원 실감방송연구센터를 통한 대학IT연구센터(ITRC), 그리 고 교육부 두뇌한국21(BK21) 정보기술사업단의 지원 에 의한 것입니다.

## 참고 문헌

- [1] J. Fridrich, M. Goljan and R. Du, "Lossless data embedding new paradigm in digital watermarking," EURASIP Journal Applied Signal Processing, vol. 2002, no. 2, pp. 185–196, Feb. 2002.
- [2] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Reversible data hiding," Proc. ICIP, vol. II, pp. 157–160, Sept. 2002.
- [3] J. Tian, "Reversible data embedding and content authentication using difference expansion," IEEE Transaction on Circuits and Systems for Video Technology, 2003.