

# 차분 영상의 히스토그램 조작을 통한 무손실 정보은닉 기술

이상광, 서영호, 호요성\*

한국전자통신연구원, 광주과학기술원\*

전화 : 042-860-1833 / 핸드폰 : 010-3000-2406

## Lossless Data Hiding Based on Histogram Modification of Difference Images

Sang-Kwang Lee, Young-Ho Suh, Yo-Sung Ho\*

Electronics and Telecommunications Research Institute (ETRI)

Gwangju Institute of Science and Technology (GIST)\*

E-mail : {sklee, syh}@etri.re.kr, hoyo@gist.ac.kr

### Abstract

In this paper, we propose a lossless data hiding method where distortion due to data embedding can be completely removed from the watermarked image after the watermark has been extracted. In the proposed method, we utilize characteristics of the difference image and modify pixel values slightly to embed the data. We show that the lower bound of the PSNR (peak-signal-to-noise-ratio) values for typical images are about 51.14 dB. Moreover, the proposed method is quite simple and fast. Experimental results demonstrate that the proposed scheme can embed a large amount of data while keeping high visual quality of test images.

### 1. 서론

멀티미디어 콘텐츠의 디지털 표현은 원본 콘텐츠와 동일한 여러 복사본을 쉽고 널리 배포할 수 있다는 장점을 가지고 있다. 하지만, 원본과 동일한 형태의 수많은 복사본이 불법적으로 생산될 수 있으므로 음반, 영화, 도서, 그리고 소프트웨어 출판 산업에 심각한 위협이 된다. 이러한 저작권(copyright) 보호에 대한 문제

를 해결하기 위해 디지털 콘텐츠 자체에 저작권 정보와 일련 번호(serial number)를 숨기는 연구가 시작되었다[1].

콘텐츠 내에 정보를 삽입하는 정보은닉 기술은 암호화 서명처럼 따로 저장할 필요가 없고, 삽입된 정보가 콘텐츠에 적용되는 동일한 변환 과정을 겪는다는 장점이 있다. 하지만, 정보은닉 시스템은 정보삽입 과정에서 발생하는 왜곡을 피할 수 없다는 단점을 가지고 있다. 일반적으로 이러한 왜곡은 양자화, 비트 교환(bit-replacement), 화소값 0과 255에서의 잘림(truncation) 등으로 인해 정보 신호를 검출한 뒤에도 완전히 제거될 수 없다. 비록 왜곡이 매우 작을지라도, 의료 영상이나 전략상 중요성을 갖는 군사 영상에서는 중요한 문제가 될 수 있다. 따라서, 삽입된 정보를 검출한 뒤에도 원본 콘텐츠를 왜곡없이 복원할 수 있는 기술이 요구되며, 이러한 요구를 만족시키는 기술을 무손실 정보은닉 기술이라고 한다[2].

본 논문에서는 차분 영상의 히스토그램 특성을 기반으로 하는 무손실 정보은닉 방법을 제안한다. 제안한 방법은 전체 영상 크기의 절반에 해당되는 화소들의 값이 소량 변형되므로 정보 삽입으로 인한 왜곡이 적다. 차분 영상의 확률 분포는 라플라스안 분포에 가깝다. 이러한 차분 영상의 특성을 기반으로 히스토그램 이동과 히스토그램 조작을 통해 기존의 무손실 정보은닉 기술들보다 많은 양의 정보를 삽입할 수 있다[3, 4].

## II. 제안한 무손실 정보은닉 알고리즘

### 2.1 정보삽입 알고리즘

본 논문에서 제안한 알고리즘의 삽입 과정은 그림 1과 같다. 정보삽입 알고리즘은 워터마크 생성, 차분영상 생성, 히스토그램 이동, 히스토그램 조작의 주요 함수 블록들로 구성되며, 입력 신호는 원본 영상, 이진 로고 영상, 비밀키 (secret key) 값이다.

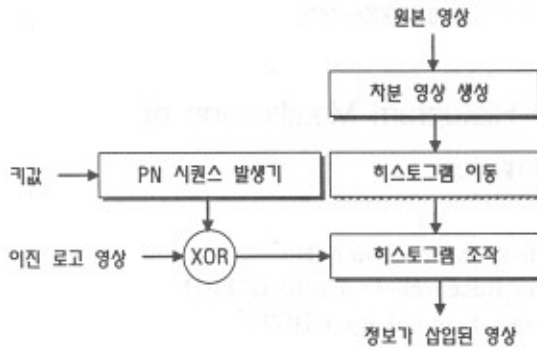


그림 1. 정보삽입 알고리즘

$P \times Q$  크기의 이진 워터마크 시퀀스  $W(m,n)$ 을 생성하기 위해, 사용자 키를 이용하여 만든 이진 랜덤 시퀀스  $A(m,n)$ 과 이진 로고 영상  $B(m,n)$ 을 비트단위 XOR을 이용하여 조합한다.

$$W(m,n) = A(m,n) \oplus B(m,n) \quad (1)$$

여기서  $\oplus$ 는 비트단위 XOR 연산이다.

$M \times N$  크기의 그레이스케일 영상  $I(i,j)$ 에 대해,  $M \times N/2$  크기의 차분 영상  $D(i,j)$ 를 생성한다.

$$D(i,j) = I(i,2j+1) - I(i,2j) \quad (2)$$

여기서  $I(i,2j+1)$ 과  $I(i,2j)$ 는 홀수라인 필드와 짝수라인 필드이다.

워터마크를 삽입하기 위해, 다음과 같이 히스토그램 이동을 통해 차분값 -2와 2를 비운다. 히스토그램 이동된 차분 영상  $\bar{D}(i,j)$ 는 다음과 같다.

$$\bar{D}(i,j) = \bar{I}(i,2j+1) - I(i,2j) \quad (3)$$

여기서

$$\bar{I}(i,2j+1) = \begin{cases} I(i,2j+1) + 1, & D(i,j) \geq 2 \\ I(i,2j+1) - 1, & D(i,j) \leq -2 \\ I(i,2j+1), & \text{otherwise} \end{cases} \quad (4)$$

히스토그램 조작 과정에서, 워터마크 시퀀스

$W(m,n)$ 은 히스토그램이 이동된 차분 영상  $\bar{D}(i,j)$ 에 다음과 같이 삽입된다.

$$I_c(i,2j+1) = \begin{cases} \bar{I}(i,2j+1) + 1, & \bar{D}(i,j) = 1, W(m,n) = 1 \\ \bar{I}(i,2j+1) - 1, & \bar{D}(i,j) = -1, W(m,n) = 1 \\ \bar{I}(i,2j+1), & \text{otherwise} \end{cases} \quad (5)$$

제안한 방법의 정보 수용량은 차분 영상에서 차분값이 -1과 1인 화소들의 개수와 같다. 차분 영상의 차분값들은 대부분 0값 주위에 분포하기 때문에, 제안한 방법을 통하여 많은 양의 정보를 삽입할 수 있다. 또한, 화소값 0과 255를 갖지 않는 대부분의 영상들에 대해, 최악의 경우 정보삽입 과정에서 전체 영상의 절반인 홀수라인 필드의 모든 화소값들이 1만큼 변형되므로  $PSNR(dB) = 10 \log_{10}(255 \times 255 \times 2) = 51.14$ 이 된다. 따라서, 정보가 삽입된 영상의 PSNR 하한값은 51.14 dB가 되며, 이는 기존의 무손실 정보은닉 기술들보다 훨씬 높은 값이다.

### 2.2 정보검출 및 복원 알고리즘

본 논문에서 제안한 알고리즘의 검출 및 복원 과정은 그림 2와 같다. 이 과정에서는 삽입된 이진 로고 영상을 검출하고 정보가 삽입된 영상을 원본 영상으로 복원한다.

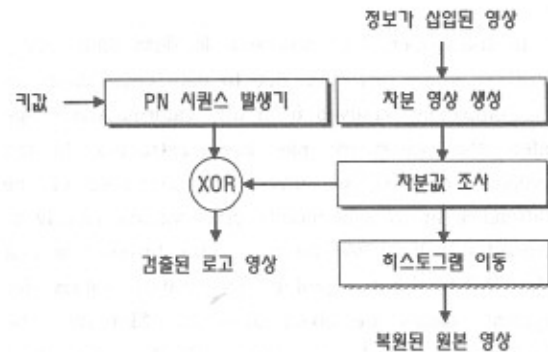


그림 2. 정보검출 및 복원 알고리즘

먼저 정보가 삽입된 영상  $I_c(i,j)$ 로부터 차분 영상  $D_c(i,j)$ 를 생성한다. 차분 영상을 스캔하여 차분값을 조사하면서 워터마크 시퀀스  $W_c(m,n)$ 를 검출한다.

$$W_c(m,n) = \begin{cases} 0, & D_c(i,j) = -1, 1 \\ 1, & D_c(i,j) = -2, 2 \end{cases} \quad (6)$$

이진 로고 영상  $B_c(m,n)$ 을 복원하기 위해 사용자 키를 이용하여 만든 이진 랜덤 시퀀스  $A_c(m,n)$ 과 검출된 이진 워터마크 시퀀스  $W_c(m,n)$ 을 비트단위

XOR을 이용하여 조합한다.

$$B_e(m, n) = A_e(m, n) \oplus W_e(m, n) \quad (7)$$

마지막으로, 히스토그램 이동을 통해 정보 삽입된 홀수라인 필드  $I_e(i, j)$ 를 복원한다.

$$I_r(i, 2j+1) = \begin{cases} I_e(i, 2j+1) - 1, & D_e(i, j) \geq 2 \\ I_e(i, 2j+1) + 1, & D_e(i, j) \leq -2 \\ I_e(i, 2j+1), & \text{otherwise} \end{cases} \quad (8)$$

짝수라인 필드는 삽입 과정에서 조작을 가하지 않았기 때문에 그대로 이용하면 된다. 즉,

$$I_r(i, 2j) = I_e(i, 2j) \quad (9)$$

### 2.3 무손실 영상 복원

제안한 알고리즘은 삽입 과정에서 화소의 경계값인 0과 255의 조작으로 인해 정보 손실이 발생한다. 따라서, 복원 과정을 통해 원본 영상으로 완전하게 되돌아갈 수 없다. 이러한 문제를 해결하기 위해, 히스토그램 조작시 모듈로 연산(modulo arithmetic)을 이용한다. 홀수라인 필드  $I(i, 2j+1)$ 에 대해 덧셈 모듈로  $+_c$ 와 뺄셈 모듈로  $-_c$ 를 다음과 같이 정의한다.

$$\begin{aligned} I(i, 2j+1) +_c 1 &= (I(i, 2j+1) + 1) \bmod c \\ I(i, 2j+1) -_c 1 &= (I(i, 2j+1) - 1) \bmod c \end{aligned} \quad (10)$$

여기서  $c$ 는 모듈로 주기이다. 복원 문제는 경계값에서의 오버플로우(overflow)나 언더플로우(underflow)로 인한 화소값의 잘림 현상이 발생할 때 생긴다. 따라서, 제안한 알고리즘에서의 모듈로 연산은  $255 +_c 1$ 과  $0 -_c 1$ 만 고려하면 된다.

정보검출 과정에서 홀수라인 필드의 화소값이 255인 경우, 그 값이  $254 + 1$ 에 의해 조작된 것인지  $0 -_{256} 1$ 에 의한 것인지 구별해야 한다. 이웃하는 화소간에 급격한 변화가 없다고 가정하면,  $I_e(i, 2j+1)$ 과  $I_e(i, 2j)$  사이에 큰 차이가 나는 경우 정보삽입 과정에서 모듈로 연산으로 인해 조작된 것이라고 예측할 수 있다. 즉,  $I_e(i, 2j+1) = 255$ 는 다음과 같이 예측된다.

$$\begin{cases} I(i, 2j+1) + 1, & |I_e(i, 2j+1) - I_e(i, 2j)| \leq \tau \\ I(i, 2j+1) -_{256} 1, & \text{otherwise} \end{cases} \quad (11)$$

여기서  $\tau$ 는 임계값이다. 즉, 인접하는 화소들간의 차이가  $\tau$ 보다 크면 255는 0로부터 조작된 것으로, 그렇지 않으면 254로부터 조작된 것으로 예측한다. 마찬가지로,

0에 대해 다음과 같이 예측한다.

$$\begin{cases} I(i, 2j+1) - 1, & |I_e(i, 2j+1) - I_e(i, 2j)| \leq \tau \\ I(i, 2j+1) +_{256} 1, & \text{otherwise} \end{cases} \quad (12)$$

### III. 실험 결과 및 분석

본 논문에서 제안한 무손실 정보오버 알고리즘의 성능을 평가하기 위해,  $512 \times 512 \times 8$  그레이스케일의 영상에 적용한 후 워터마크가 삽입된 영상의 PSNR 값과 정보 수용량을 측정하였다. 그림 3은 실험을 통해 삽입된  $128 \times 56$  크기의 이진 로고영상을 보여주고 있으며, 이는 7,168 bits의 이진 비트 시퀀스와 동일한 크기이다.

## GIST-ETRI

그림 3. 이진 로고 영상 ( $128 \times 56$ )

그림 4는 원본 Lena 영상과 워터마크가 삽입된 영상을 보여준다. Lena 영상은 오버플로우나 언더플로우에 인한 잘려진 화소를 포함하고 있지 않으며 워터마크 삽입으로 인한 시각적인 왜곡도 발생하지 않는다. 그림 5는 6개의 다른 실험 영상들에 대한 결과를 보여주고 있다.



(a) 원본 Lena 영상 (b) 정보가 삽입된 영상

그림 4. Lena 영상에 대한 결과

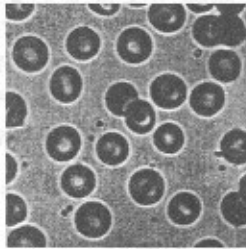
표 1은 실험 결과를 요약하고 있다. 실험 영상들에 대한 PSNR 값을 살펴보면, 제안한 알고리즘이 51.14 dB 이상의 PSNR 값을 보장해준다는 이론적 증명을 실험을 통해 보여주고 있다. 정보 수용량의 경우  $512 \times 512 \times 8$  그레이스케일의 실험 영상들에 대해 약 8 kbits에서 30 kbits로 대부분의 응용 분야에 충분히 적용될 수 있는 수치이다.



(a) Airplane



(b) Baboon



(c) Blood



(d) Peppers



(e) Sailboat



(e) Tiffany

그림 5. 정보가 삽입된 영상들

표 1. 실험 결과

실험 영상들 (512 × 512 × 8)	PSNR (dB)	정보 수용량 (bits)	경계값 화소 (화소 개수)
Airplane	58.78	30,487	0
Baboon	51.49	7,383	0
Blood	55.59	22,009	20
Lena	57.63	23,579	0
Peppers	55.74	17,280	2
Sailboat	55.55	14,391	0
Tiffany	52.50	26,004	83

표 1에서 볼 수 있듯이, Baboon 영상과 같이 인접한 화소간의 변화의 차가 큰 복잡한 영상의 경우, 차분 영상의 차분값들이 0에서 멀어지므로 정보 수용량이 그만큼 감소하게 된다. 이와는 달리, Airplane 영상과 같이 화소의 변화가 적은 단조로운 영상의 경우, 차분 영상의 히스토그램 압축 특성이 뚜렷하여 많은 양의 정보를 삽입할 수 있다. 실제로 두 영상의 정보 수용

량은 약 4배가량 차이가 난다는 것을 알 수 있다.

Blood, Peppers, Tiffany와 같은 영상들은 오버플로우나 언더플로우를 발생시키는 경계값 화소를 포함하고 있다. 하지만, 그러한 화소 개수가 상대적으로 적고 그림 5에서 보듯이, 오버플로우나 언더플로우로 인한 왜곡이 심각하지 않다는 것을 알 수 있다.

## V. 결론

본 논문에서는 차분 영상의 히스토그램 특성을 이용한 무손실 정보은닉 알고리즘을 제안하였다. 원본 영상에 대한 복원 문제를 해결하기 위해 일반적으로 사용하는 덧셈, 뺄셈 연산대신 모듈로 연산을 사용하였다. 실험 결과는 제안한 알고리즘이 가능한 한 삽입 과정에서 생기는 왜곡을 줄이면서 많은 양의 정보를 삽입할 수 있다는 것을 보여주었다. 워터마크를 검출한 후 원본 콘텐츠를 복원하는 기술은 군사 영상과 의료 영상과 같은 민감한 사한을 다루는 분야에 요구된다. 본 논문에서 제안한 무손실 정보은닉 방법은 이러한 응용들에 효과적으로 적용될 수 있다.

## 감사의 글

본 연구는 광주과학기술원 (GIST) 실감방송연구센터 (RBRC)를 통한 정보통신부 대학IT연구센터 (ITRC), 교육인적자원부 두뇌한국21 (BK21) 정보기술사업, 디지털콘텐츠협동연구센터 (DCRC), 그리고 한국전자통신연구원 (ETRI)의 지원에 의한 것입니다.

## 참고 문헌

- [1] I. Cox, M. Miller, and J. Bloom, Digital watermarking, Morgan Kaufmann Publishers, 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] 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, Dec. 2002.
- [4] Z. Ni, Y.Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," Proc. ISCAS 2003, vol. 2, pp. 912-915, May 2003.