블록기반의 적응적 임계값을 이용한 스테가노그라피

이신주, 정성환
창원대학교 컴퓨터공학과

Steganography using Block-based Adaptive Threshold

Sin-Joo Lee, Sung-Hwan Jung
Dept. of Computer Enginnering, Changwon Nat'l University

요 약

본 논문은 비트 플레인의 위치에 따라 블록별 적응적인 임계값를 이용하여 정보를 삽입하는 스테가노그라피 방법을 연구하였다. 다양한 이미지를 대상으로 고정 임계값을 적용하는 기존의 방법과 영상의 특징에 따라 비트 플레인별 임계값이 적응적으로 산출되는 제안한 방법에 대해서 최대용량을 측정하고, 같은 양의 정보를 삽입한 후 화질을 비교 분석하였다. 그 결과 기존의 방법보다 용량면이나 화질면에서 나은 결과를 얻을 수 있었다.

1. 서론

스테가노그라피(steganography)는 비밀 메시지의 구조를 변경하지 않고, 커버(cover)라 불리는 의미없는 미디어에 비밀 메시지를 숨겨서 전송하는 비밀 통신 방법이다. 이러한 정보 은닉을 위한 스테가노그라피의 가장 중요한 요구조건은 비인지성과 삽입용량이다. 일반적으로 삽입 용량이 증가할수록 삽입된 정보는 통계적으로 검출될 위험성이 커지며, 동시에 이미지의 일그러짐과 같은 품질 저하가 발생한다[1].

또한 정보가 삽입된 스테고 이미지는 스테그어날리시스(Steganalysis) 방법을 이용하여 숨겨진 메시지 존재에 대한 통계적인 정보를 찾아 내는 공격을 받을 수 있다. 따라서 스테가노그라피 방법에서는 이러한 스테그어날리스에 의한 공격을 고려하여야 한다.

일반적으로 대용량의 정보를 삽입하기 위해서는 비트 플레인을 많이 이용한다. 그러나 4비트 고정 LSB 삽입 방법은 커버의 50%정도 용량을 일정하게 삽입하지만, 이미지의 부드러운 부분에 거짓 윤곽선이 나타난다. 이러한 단점을 보완하기 위하여 가변크기 방법을 사용하는 Kawaguchi[2]의 경우 동일한 임계값을 모든 비트 플레인에 일괄적으로 적용하였다. 따라서 상위 비트 플레인에 정보가 삽입되어 화질의 열화가 생기기 쉽다. 또한 Y. K. Lee방법은 커버 이미지에 따라서 1~4(5)비트 플레인까지 정보가 삽입되므로 정보 삽입량은 증가할 수 있으나, 삽입량이 증가할수록 전체 영상에 걸쳐 노이즈와 같은 화질의 열화가 발생하였다[3].

따라서 본 연구에서는 비인지성과 삽입 용량에 따른 기존 연구들의 문제점을 해결하고 확장하기 위하여, 블록기반의 적응적 임계값를 산출하고 이를 적용한 스테가노그라피 방법을 제안하였다. 또한 정보가 삽입된 스테고 이미지에 일반적인 공격형태인 통계적인 정보 추출방법인 히스토그램 스테그어날리스를 적용하여 분석해 보았다.

2. 스테그어날리시스

스테가노그라피의 목적은 비밀 메시지를 제3자가 알아채지 못하게 안전하게 상대방에게 전송하는 것이다. 일반적으로 스테가노그라피 시스템에서는 정보 삽입시 커버 이미지의 어떤 특징을 변형하거나 규칙적인 패턴 등을 수반하게 된다. 만일 전송된 메시지에 어떤 의심이 간다면 스테가노그라피의 목적에 실패한

것이다. 따라서 스테그어날리스에서는 이런 변형이나 규칙적인 패턴 등을 이용하여 정보가 삽입되었다는 것을 검출하는 공격이라 할 수 있다.

일반적으로 통계적인 접근 방법으로 영상 또는 영역의 명암도 히스토그램의 모멘트들을 사용하여 영역을 표현할 수 있다. 그러나 스테가노그라피는 원래의 통계적 특성을 일부 잃게 하기 때문에 공격을 당하기 쉽다. 따라서 1차 모멘트나 2차 모멘트 등의 특성을 유지하면서 정보를 은닉하는 방법도 있지만 이는 삽입 정보량이 줄어드는 단점이 있다.

이처럼 스테그어날리스는 커버트 메시지나 스테가노그라피 메시지와 같은 숨겨진 비밀 정보들을 여러 가지 수단을 동원하여 발견하고자 하는 기술이다. 따라서 제안한 블록기반 적응적 임계값을 적용한 스테가노그라피 방법의 단점을 찾아내고, 더욱 강인성 있는 스테가노그라피 방법을 연구하고자 한다.

3. 제안한 블록기반 스테가노그라피 방법

본 절은 고정적 임계값 문제점과 삽입 용량을 증가하기 위하여 비트 플레인의 특성을 이용한 블록별 적응적 임계값 방법을 제안하였다.

3.1 적응적 임계값

그림1은 비트 플레인의 특징을 살펴보기 위하여 블록 복잡도를 나타내었다. LSB에 근접할수록 복잡도가 높은 영역이 많으며, MSB로 갈수록 상대적으로 복잡도가 낮은 영역이 급격하게 증가하고 복잡도의 분포가 전체적으로 퍼져 있음을 볼 수 있다. 따라서 MSB쪽으로 갈수록 작은 값의 변화에도 화질은 민감하게 변화함을 알 수 있다.

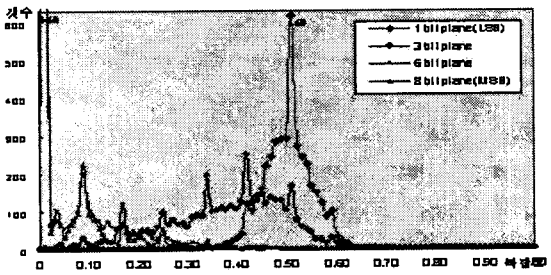


그림 1. 비트 플레인별 블록 복잡도(Lena의 예)

따라서 식 1과 같이 비트 플레인 위치에 따라 값의 크기를 나타내는 가중치를 정의하였다. 이는 비트 플레인의 특성을 고려한 것으로, 변화값이 큰 MSB 플레인은 큰 값을 갖고, 변화값이 작은 LSB 플레인들은 작은 값을 갖는다. k는 값의 크기를 나타내는 상수이며, i는 해당 비트 플레인의 위치를 나타낸다.

$$w(B_i) = k^* log_2^i, \quad 0 \leq k \leq 1, i \geq 1 \qquad \text{(식 1)}$$

따라서 비트 플레인의 가중치를 이용하여 각 블록이 가지는 복잡도의 크기값을 블록 임계값으로 나타내었다. 식 2는 블록별 적응적 임계값($\alpha'(B_i(x,y))$)을 나타낸 것이다. 해당 블록의 복잡도($c[B_i(x,y)]$)와 비트 플레인별 가중치($w(B_i)$)를 이용하여 산출된다.

$$\alpha'(B_i(x,y)) = w(B_i)^*(1 - c[B_i(x,y)]) \qquad \text{(식 2)}$$

블록별 적응적 임계값은 해당 블록에 정보를 삽입할 수 있는지 없는지를 판별할 때 사용된다.

3.2 제안한 삽입 알고리즘

그림 2는 제안한 적응적 임계값을 이용한 삽입 알고리즘의 블록도이다.

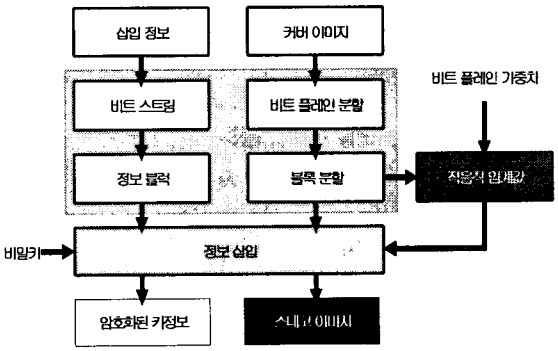


그림 2. 적응적 임계값을 이용한 삽입 알고리즘

다음은 $2^M \times 2^M$ 크기를 가진 커버 이미지에 블록별 적응적 임계값을 이용하여 정보를 삽입하는 방법이다.

(1) 삽입 정보(E)는 비트 스트림 형태의 정보 블록(E_n)으로 표현하고, 커버 이미지를 i개의 비트 플레인으로 나눈다.

(2) 각 비트 플레인을 $2^m \times 2^m$ 크기의 블록으로 나누고, 블록 복잡도($c[B_i(x,y)]$)를 계산한다.

(3) 각 블록에 따라 적응적 임계값을 산출한다. 식 3과 같이 LSB에서 MSB순으로 비밀키에 의해 선택된 블록의 복잡도($c[B_i(x,y)]$)가 임계값($\alpha'[B_i(x,y)]$) 이상이면 정보(E_n)를 삽입한다. 이때 정보 블록의 복잡도($c(E_n)$)가 블록 복잡도($c[B_i(x,y)]$)도 보다 낮으면 위치맵($L(x,y)$)을 설정한다. 생성된 위치맵은 정보 추출시 미검출되는 정보 블록을 위해 사용된다.

$$B_i(x,y) = E_n, \text{ if } c[B_i(x,y)] \geq \alpha'[B_i(x,y)]$$
$$L(x,y) = \begin{cases} 1, & \text{if } c(E_n) < c[B_i(x,y)], \\ 0, & otherwise \end{cases} \quad (식3)$$

(4) 정보 삽입후, 비트 플레인을 취합하면 스테고 이미지가 생성과 정보 삽입시 사용한 키정보는 암호화하여 전송한다.

3.3 추출 알고리즘

비밀 정보를 추출하기 위해서는 정보삽입시 사용한 키정보가 필요하다. 그림 3은 추출 알고리즘의 블록도이다.

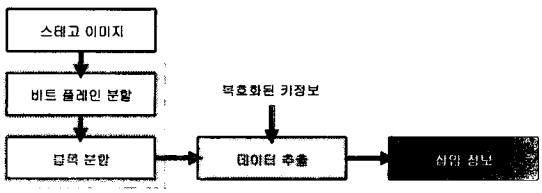


그림 3. 적응적 임계값을 이용한 추출 알고리즘

(1) 스테고 이미지를 i개의 비트 플레인으로 분할한다. 각 비트 플레인을 $2^m \times 2^m$크기의 블록($B_i(x,y)$)으로 나누고, 블록 복잡도($c[B_i(x,y)]$)를 산출한다.

(2) 복호화된 키정보는 정보 삽입시 적용된 비트 플레인별 최소 적응적 임계값($\alpha'(B_i)_{\min}$)과 위치맵($L(x,y)$) 그리고 비밀키(K_{seed})이다.

(3) 비트 플레인별 검출 블록의 순서는 비밀키를 이용한 난수 생성기에 의해서 위치를 알아낸다.

$$E_n = B_i(x,y), \quad \text{if } c[B_i(x,y)] \geq \alpha'(B_i) \text{ or } L(x,y) = 1 \quad (식 5)$$

식 5와 같이 해당 블록이 마스킹 임계값 이상이거나 스킹 임계값보단 낮지만 위치맵에 의해서 설정되었다면 이는 정보 블록으로 검출한다.

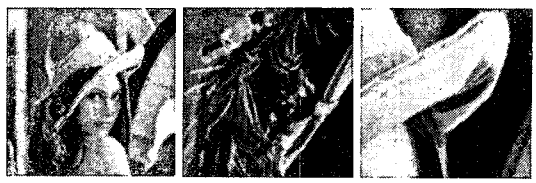
4. 실험 결과

실험에서 사용된 그레이 이미지들은 8bit/pixel의 512×512크기이며, 각 비트 플레인은 $2^3 \times 2^3$크기 블록으로 나누었다.

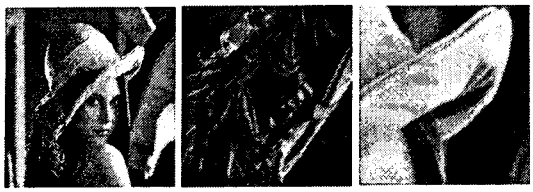
표1. 같은 용량을 삽입한 후의 화질비교

	삽입용량 (Byte)	Proposed Method PSNR(dB)	Kawaguchi PSNR(dB)
Baboon	130,144	30.64	29.27
Lena	117,000	32.53	29.98
Peppers	130,203	30.75	29.28
F16	116,072	31.38	29.07
Couple	130,270	30.79	30.60
Girl	103,200	34.45	33.32
Fishboat	130,382	30.88	28.74
평균	122,467	31.63	30.04

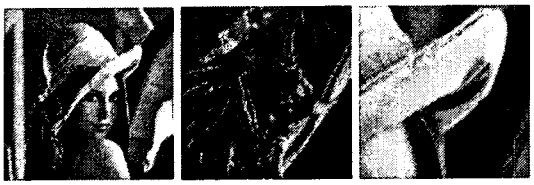
그림2는 Lena 이미지에 기존 방법와 제안한 방법을 적용하여 동일한 정보량(117,000 byte)을 삽입한 스테고 이미지이다. (a)는 정보가 삽입되지 않은 Lena의 커버 이미지이다. (b)는 제안한 방법으로 비트 플레인의 갖 o치와 블록별 적응적 임계값을 이용하여 정보를 삽입한 결과이다. 전체 비트 플레인에 걸쳐 정보가 삽입되므로, 상대적으로 심각한 화질의 변화는 없었다. (c)는 Kawaguchi방법으로 임의의 임계값을 전체 비트 플레인에 적용하는 삽입 방법이다. 그러나 임계값이 최상위비트 플레인까지 일괄적으로 적용되어 화질 열화가 많이 발생하였다.



(a) 정보가 삽입되지 않은 커버 이미지



(b) 제안한 방법으로 삽입한 결과



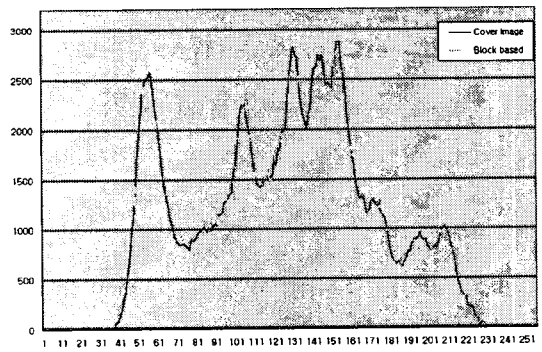
(c) E. Kawaguchi 방법으로 삽입한 결과

그림2. 정보량(117,000 byte)을 적용한 후의 실험 결과

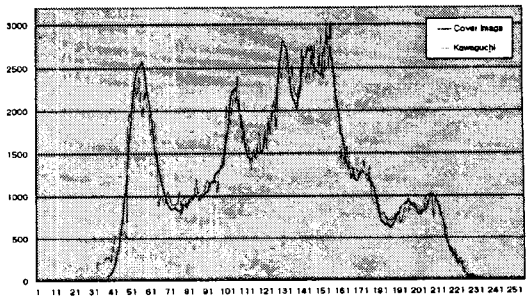
5. 통계적 특징을 이용한 스테그어날리시스

그림 3과 같이 동일한 정보(107,128 byte)가 삽입된 스테고 이미지에 대하여 정보 삽입 여부에 알아보았다. 이는 가장 간단한 공격의 한 방법으로, 기존 방법과 제안한 방법을 적용한 스테고 이미지와 커버 이미지의 상관관계를 히스토그램으로 분석해 보았다.

(a)는 제안한 방법을 적용한 결과화면이다. 스테고 이미지가 커버 이미지와의 거의 같은 분포를 가짐을 알 수 있었다. 화면상 차이점을 알 수 없어, 커버와의 면적의 차이를 계산 결과, 차이값이 96이었다. (b)는 고정 임계값을 적용한 후 결과화면이다. 커버 이미지와 거의 비슷한 분포를 따르고 있지만, 중간값이 변화의 가 많음을 볼 수 있었다. 커버와의 차이값은 106이었다.



(a) 커버 이미지와 제안한 방법의 히스토그램



(b) 커버 이미지와 고정 임계값을 적용한 히스토그램

6. 결론

본 연구에서는 비트 플레인의 가중치를 고려하여 블록별 적응적인 임계값을 이용한 스테가노그라피 방법을 연구하였다. 모든 비트 플레인에 고정 임계값을 적용하여 정보를 삽입한 결과, 비트 플레인에 따라 화질의 변화가 다름을 알 수 있었다.

제안한 스테가노그라피 방법은 Kawaguchi의 고정 임계값 문제를 해결하고 정보 삽입량을 적응적으로 증가하였다. 이를 위하여 비트 플레인별 위치 가중치와 블록별 복잡도에 따른 새로운 적응적 임계값을 제안하였다.

Baboon, Lena 등의 표준 이미지들을 이용하여 제안한 방법과 기존의 Kawaguchi방법에 대하여, 동일한 정보량을 삽입하고 이에 따른 화질을 비교하였다. 그 결과, 제안한 방법이 기존의 방법보다 화질면에서도 평균 약 2dB 향상되었다. 또한 제안한 방법에 대하여 통계적 특징을 이용한 스테그어날리스를 적용하였다. 그 결과 커버 이미지와 상대적으로 비슷한 분포를 가짐을 알 수 있었다.

[참고문헌]

[1] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, " Information Hiding-A Survey, " Proc. of the IEEE, special issue on protection of multimedia content, vol.87, no.7, pp.1062-1078, 1999.

[2] M. Mimi, H. Noda, E. Kawaguchi, "An Image Embedding in Image Complexity Based Region Segmentation Method," Proc. of ICIP, vol.3, pp.74-77, 1997.

[3] Sin-Joo Lee, Jae-Min Bae, Sung-Hwan Jung, "High Capacity Image Steganography Using Complexity Measure," Proc. of EALPIIT 2002, pp.349-352, 2002.