비트 플레인별 적응적 가중치를 이용한 대용량 데이터 은닉에 관한 연구

이신주*, 정성환
창원대학교 컴퓨터공학과
e-mail : sinjoo@changwon.ac.kr, sjung@changwon.ac.kr

A Study on the Large Capacity Data Hiding Using Adaptive Weight on Bit Planes

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

요 약

본 논문은 비트 플레인의 위치에 따라 정보 삽입량에 대한 주관적이고 고정적인 임계치가 아니라 비트 플레인의 가중치를 고려하여 각 영상의 비트 플레인별 적응적인 임계값에 따라 최대 정보량을 삽입하고 추출하는 알고리즘을 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

통신망에 개방되어 있는 디지털 데이터를 보호하고 전송 중에 정보의 보호 및 은닉에 대한 필요성이 전자지불 및 전자화폐, 전자우편, 저작권 보호, 인증 등 다양한 형태로 요구되고 있다.

비밀 통신 기술은 크게 암호화와 스테가노그라피 방법으로 나눌 수 있다. 암호화는 메시지의 내용에 상관없이 비밀 키를 이용하여 비밀 메시지 그 자체를 해독할 수 없도록 구조를 의미없는 형태로 변화시켜 전달한다. 그러나 부호화된 메시지를 숨기거나 속이지는 못하는 단점이 있다.

스테가노그라피는 비밀 메시지 자체의 구조를 변경하지는 않고, 커버(cover)라 불리는 의미없는 미디어에 비밀 메시지를 숨겨서 전송하는 비밀 통신 방법이다.

일반적으로 비밀 메시지를 삽입하는 방법은 커버의 구조와 매우 밀접한 관계를 가진다. 따라서 정보를 삽입할 커버 이미지는 복잡한 자연영상을 사용한다. 그러나 많은 양의 정보 삽입은 커버에 심각한 변형을 가져올 수 있으며, 이런 형태의 변형은 비밀 정보가 삽입되어 있는다는 것을 의미할 수 있다. 따라서 삽입 정보의 존재 유무에 대한 의심은 스테가노그라피의 기본적인 목적에 상반되는 것이다.

스테가노그라피는 삽입 용량(capacity)과 삽입 정보의 비인지성(imperceptibility), 그리고 제거 공격에 대한 저항성(removal resistance) 등을 만족하여야 하며, 이러한 3 가지 요구 조건은 서로 밀접한 상관성을 가지고 있다.

최근에 삽입용량을 증가시키기 위한 스테가노그라피 시스템에 대한 많은 연구가 이루어지고 있다. 4 비트 고정 LSB 삽입 방법의 경우는, 삽입 용량은 커버의 50%가 일정하지만 이미지의 부드러운 부분에 대해 거짓 윤곽선이 나타난다. 이러한 단점을 보완하기 위하여 가변크기 방법을 사용하는 Kawaguchi[1]의 경우 비트 플레인의 중요도와 관계없이 동일한 복잡도를 모든 비트 플레인에 일괄적으로 적용하였다.

본 논문은 Eiji Kawauchi 의 방법을 기반으로 하여 이미지의 화질을 크게 감소시키지 않으면서, 인간 시각 시스템(Human Visual System : HVS)을 기초로 각 비트 플레인별 적응적인 임계값을 산출하여 대용량의 정보를 삽입하는 스테가노그라피 방법을 연구하였다.

2. 스테가노그라피

스테가노그라피는 정보 은닉 기술 중에 대표적인 기술의 하나로 정보를 숨기는 커버보다 숨겨진 비밀 메시지에 중점을 둔다. 따라서 비밀 통신을 위해 커버트 채널(covert channel)이라 부르는 의식되지 않는 채널을 이용하여 제 3 자에게 비밀 메시지의 존재유무를 알리지 않고 전송하는 일종의 비밀 통신 기술이다.

2.1 스테가노그라피의 특징

다음은 스테가노그라피의 일반적인 성질이며, 사용환경에 따라서 요구조건이 다를 수 있다. 일반적으로 커버의 조작에 민감하기 때문에 강인성(robusteness)을 요구하지만 삽입 용량과 서로 밀접한 상관관계를 가진다[2].

- **삽입 용량(Capacity)** : 삽입 용량은 커버의 크기와 관련되어지며, 숨길 수 있는 정보의 크기이다. 많은 정보를 커버 이미지 안에 삽입해야 하므로 삽입 용량은 스테가노그라피 시스템에 있어 중요한 요소이다.
- **비인지성(imperceptibility)** : 비밀 통신이 이루어질 때 가장 중요한 것은 비밀 통신여부에 관한 사실 자체가 인지되어서는 안된다. 따라서 커버의 왜곡 혹은 잡음과 같은 변조로 인해 시각적 품질의 손실이나 혹은 중요한 부분의 화질 저하없이 삽입하는 것이 중요하다.
- **강인성(Robustness)** : 삽입된 정보는 의도적 또는 비의도적인 이미지 변형에 의해 삭제가 불가능해야 한다. 즉, 선형 혹은 비선형 필터링, 노이즈 추가 등 이미지 처리에도 삽입된 데이터가 손상되지 않고 남아있어야 한다.
- **검출성(Undetection)** : 제 3 자의 공격에 대하여 삽입한 비밀 정보가 검출되지 않아야 한다. 오직 비밀키 소유자만이 검출 혹은 추출할 수 있어야 하고 숨기진 비밀 정보의 존재를 증명할 수 있어야 한다. 그 밖의 경우에는 삽입된 비밀 정보의 존재에 대한 어떤 통계적인 증명도 발견할 수 없어야 한다.

2.2 스테기노그라피 삽입 방법

스테가노그라피 삽입 방법은 이미지가 변형되어도 사람이 인지할 수 없는 부분에 정보를 삽입한다. 이와 같이 비밀 정보 삽입시 커버를 변형하는 방법에 따라 다음과 같이 분류할 수 있다[3].

치환 방법(substitution method)은 정보 은닉을 위한 방법 중에서 가장 많이 사용된다. 이 방법은 비밀 메시지를 커버의 상대적으로 중요하지 않는 부분에 대치하는 방법이다. 대표적인 치환 방법은 LSB(Least Significant Bit), 팔레트기반 이미지(palette-based image), 이미지 다운그레이딩(image downgrading) 그리고 양자화 및 디더링(dithering) 등이 있다.

변환 방법은 최근에는 삽입된 정보를 더욱 강건하게 삽입하기 위해 신호의 주파수 영역에 삽입하는 방법이 이용되고 있다. 변환 영역 삽입 방법은 커버를 주파수 영역으로 변환하고 중요한 영역에 정보를 삽입하는 방법이다. 변환 영역 방법이 공간적 영역 방법보다 다양한 이미지 처리에 대한 공격에 강하다. 대표적인 변환 방법으로 DFT(Discrete Fourier Transform), DCT(Discrete Cosine Transform), DWT(Discrete Wavelet Transform) 등이 있다.

통계적 방법은 커버를 일정영역의 어떤 통계적인 특성을 이용하여 정보를 삽입하는 방법이다. 예로서, 만일 통계적인 특성이 크게 바뀌었을 경우 1 이 삽입되었으며, 바뀌지 않았다면 0 이 삽입되었다고 보는 방식이다. 통계적인 함수는 주로 평균이나 분산 등이 이용된다. 그러나 이런 통계적 스테가노그라피 기술은 다양하게 적용되기가 어렵다.

3. 제안한 알고리즘

스테가노그라피 시스템의 가장 중요한 전제 조건은 비인지성(imperceptibility)이다. 즉, 커버에 비밀 정보가 삽입되었다는 것을 제 3 자는 알 수 없어야 한다. 이미지를 이용한 스테가노그라피 시스템에서 삽입된 정보의 비인지성을 만족하기 위해 인간의 시각 시스템 즉, HVS(Human Visual System) 특성을 이용하여 정보를 삽입하는 방법들이 연구되고 있다.

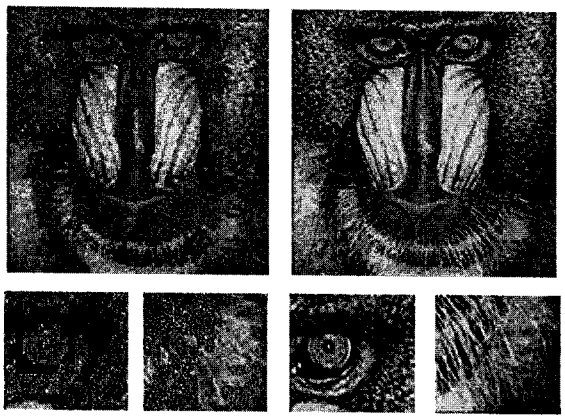
그러나 비인지성은 삽입되는 정보의 양에 크게 좌우되므로 일반적으로 삽입되는 정보의 양이 많을 수록 이미지에 대한 변형은 증가된다.

본 연구에서는 각 비트 플레인별 가중치를 기반으로 비트 플레인별 적응적인 복잡도를 산출하고 이를 이용하여 정보를 삽입하였다.

3.1 마스킹 임계값

마스킹(masking)은 큰신호에 의해 어떤 임계값 이하의 작은 신호가 가려진 것을 말하는 것으로, 인간 시각 시스템의 마스킹 성질은 사람의 눈에 감지되지 않는 곳을 의미하는 것이다. LSB 방법은 커버이미지의 최하위 비트 플레인안에 비밀 메시지를 직접적으로 치환하여 삽입한다. 따라서 최하위 비트의 조작은 상위의 비트보다 크기의 변화가 작기 때문에, 결국 인간의 시각으로는 그 차이를 감지하지 힘들다.

또한 각 비트 플레인위치에 따라 마스킹 되는 임계값이 달라야 한다. 그림 1 은 LSB 와 MSB 에 동일한 복잡도를 이용하여 같은 용량을 삽입한 후의 이미지 변화를 보여주고 있다. 실험은 복잡도 1.0, 삽입용량은 14,288 바이트를 삽입하였다. 그림 1(a)는 MSB 에 삽입한 결과로 PSNR 은 19.33dB 으로 화질의 열화가 매우 심하다. 그림 1(b)의 경우는 LSB 에 삽입한 결과로 PSNR 은 53.73dB 으로 원영상과 차이가 없었다.



(a) MSB 에 삽입한 경우 (b) LSB 에 삽입한 경우

그림 1. 동일한 복잡도에 대한 비트 플레인 삽입 결과

따라서 본 연구에서는 비트 플레인의 복잡도를 동일하게 적용시키는 것이 아니라 비트 플레인의 가중치를 고려하여 비트 플레인 별 적응적인 임계값에 따라 정보량을 삽입하고자 한다.

3.2 삽입 알고리즘

다음은 제안한 삽입 알고리즘에 대한 블록도과 절차를 서술한다. 그림 2 은 삽입 알고리즘의 블럭도이다.

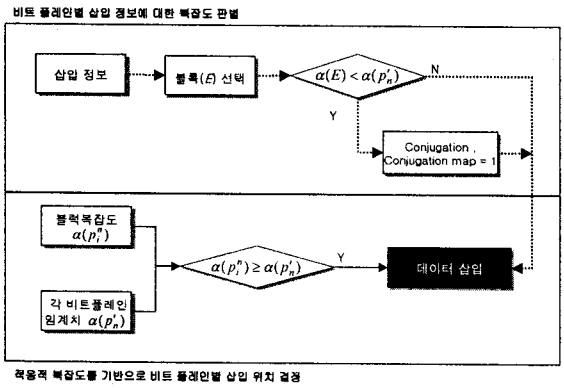


그림 2. 삽입 알고리즘 순서도

각 기호를 다음과 같이 정의한다.

$\alpha(p_n)$	n 번째 비트 플레인 복잡도
$diff_n$	$\alpha(p_n)-\alpha(p_{n-1})$ 비트플레인 복잡도의 차
W_n	n 번째 로그값과 크기 스케일을 이용한 가중치, $W_n=(\log_{10} n)*w,\ 0\le W_n\le 1$
$\alpha(p'_n)$	n 번째 비트 플레인의 적응적 임계값

(1) 이미지 데이터를 그레이 코드로 바꾼 후 n 개의 비트 플레인으로 나눈다.

(2) 각 비트 플레인을 $2^m x 2^m$ 크기의 블록으로 나누고 나누어진 블록은 $P_i, i=1,2,...4^{M-m}$ 으로 정의한다. 블록별 복잡도를 계산하여 비트 플레인($\alpha(p_n)$) 복잡도와 평균 복잡도(M)를 산출한다.

(3) 비트 플레인 복잡도의 차($diff_n$)를 이용하여 잡음 혹은 정보가 있는 비트 플레인인지 구별한다. 그림 3 와 같이 각 비트 플레인의 적응적인 임계값을 계산한다.

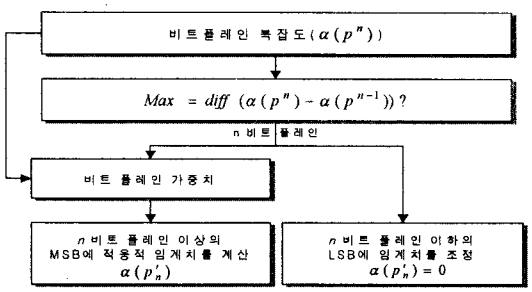


그림 3. 적응적 임계값 산출 및
비트 플레인 적용 블럭도

(4) 각 블록에 대한 컨주게이션 적용 유무를 저장하기 위해 컨주게이션 맵을 정의한다[1,5]. 컨주게이션 맵은 블록의 개수와 같으므로 $C_n=C'_1,C'_2,...C'_{4^{M-m}}$ 로 표현된다.

(5) 적응적인 복잡도 $\alpha(p'_n)$ 은 식(1)과 같이 비트 플레인의 복잡도 $\alpha(p_n)$ 와 비트 플레인 가중치(W_n)를 이용하여 산출한다. 그림 4 는 Baboon 의 예로서 각 비트 플레인별 적응적인 임계값이다.

$$value=((W_n-\alpha(p'_{n-1}))\times\alpha(p_n))/M \qquad \text{식(1)}$$

$$\alpha(p'_n)=W_n-value$$

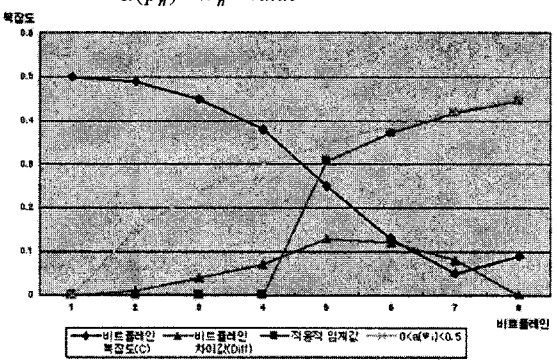


그림 4. 복잡도와 로그가중치를 이용하여
조정된 적응적 임계값

(6) LSB 에서 MSB 순으로 삽입하며, 삽입하기 전에 컨주게이션 맵의 모든 Q 값은 0 으로 초기화 된다. 삽입할 블록의 복잡도가 임계값 $\alpha(p'_n)$ 이상이면 P_i 가 E_i 로 치환하여 비밀 정보를 삽입한다. 이때 E_i 의 복잡도가 $\alpha(p'_n)$ 보다 작다면 E_i 를 컨주게

이션 후 삽입한다.

(7) 각 비트 플레인을 취합한 후, 그레이코드를 다시 원래의 이미지 코드로 바꾼다.

3.3. 추출 알고리즘

비밀 정보를 추출하기 위해서는 비트 플레인 가중치와 컨주게이션 맵이 필요하다. 먼저 블록의 복잡도가 임계값 보다 크면, 비트 플레인 전체에 비밀정보가 삽입되었다고 볼 수 있다. 그리고 블록의 컨주게이션 맵 값이 1 이면 컨주게이션을 하여 삽입된 정보를 추출하게 된다. 그림 5 는 적응적 복잡도를 이용한 추출 알고리즘의 블럭도이다.

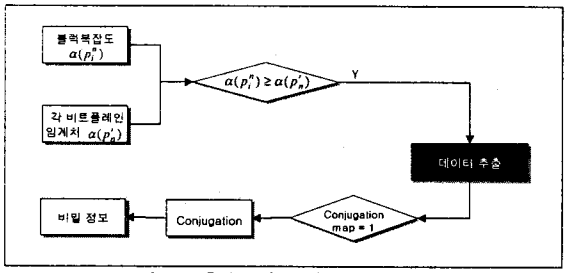


그림 5. 추출 알고리즘의 블럭도

4. 실험 결과

실험에서 사용된 그레이 이미지는 8bit/pixel 의 512×512 크기이며, 각 비트 플레인을 8×8 (m=3) 크기를 가지는 블록으로 나누었다.

표 1 은 Lena 이미지를 대상으로 기존의 방법과 제안한 방법에 대해서 최대용량을 측정하고, 같은 양의 정보를 삽입한 후 화질에 대한 변화를 비교한 것이다. 제안한 방법는 영상의 특징에 따라 비트 플레인별 적응적 임계치가 측정되어 적용된 것이다. 실험을 위해 기존방법에서 사용되는 고정 임계값으로 $\alpha = 0.4$, 삽입용량은 100,635 byte 로 삽입한 결과이다.

표 1. 최대 용량 비교

삽입 방법	최대용량 (byte)	비율	100,635 byte 삽입		보안성	임계값
			RMS	PSNR		
4 비트 고정 LSB	131,072	50.0%	5.78	32.88	No	고정
Lee	130,144	49.7%	5.51	33.30	No	고정
Kawaguchi	112,800	43.0%	5.17	33.85	Yes	고정
제한한 방법	138,512	53.8%	3.6	37.00	Yes	가변

표 2 은 동일한 메시지를 삽입한 후 커버의 화질을 동일한 화질일 경우, 기존방법과 제안한 방법에 대한 삽입한 용량을 측정한 결과이다. 4LSB 경우는 기본적으로 50%정도의 용량을 삽입할 수 있다. 그러나 부드러운 부분에 거짓 윤곽선이 나타나며, 비트 플레인의 급격한 변화로 인해 비밀 메시지가 삽입되었음을 쉽게 알아차릴 수 있다. 따라서 제안한 방법은 전체 비트 플레인에 데이터가 삽입되어지므로 심각한 화질의 변화없이 대용량의 데이터를 삽입할 수 있었다.

표 2. 동일한 화질의 경우 삽입 용량 비교

실험이미지		4LSB	Lee	Kawaguchi	제안방법
Baboon (31db)	용량 [byte]	131,072 [50%]	90,000 [34.3%]	112,800 [43.6%]	136,000 [51.5%]
Lena (32.4db)	용량 [byte]	131,072 [50%]	130,144 [49.6%]	104,000 [39.7%]	122,500 [46.7%]
Girl (32.1db)	용량 [byte]	131,072 [50%]	50,000 [19.1%]	102,000 [38.9%]	122,000 [46.5%]
Couple (32.1db)	용량 [byte]	131,072 [50%]	72,500 [27.7%]	105,850 [40.4%]	126,500 [48.3%]

5. 결론

본 논문에서는 Kawaguchi 의 방법을 기반으로 이미지의 각 비트 플레인에 지역적인 복잡도를 측정하였다. 기존의 방법은 정보 삽입시에 주관적이고 고정적인 임계치를 동일하게 적용한다. 그러나 본 연구에서는 비트 플레인의 가중치를 고려하여 비트 플레인별 적응적인 임계값에 따른 스테가노그라피의 삽입 용량을 연구하였다.

다양한 이미지를 대상으로 고정 임계값을 적용하는 기존의 방법과 영상의 특징에 따라 비트 플레인별 적응적 임계값을 사용하는 제안한 방법에 대해서 같은 양의 정보를 삽입한 후, 화질에 대해 비교 분석을 하였다. 또한 동일한 화질에 대한 최대용량을 측정하였다. 그 결과 기존의 방법보다 화질면이나 용량면에서 나은 결과를 얻을 수 있었다.

스테그어날리스 기법을 연구하여, 이를 바탕으로 LSB 삽입 방법의 취약점을 개선하는 연구가 필요하다.

참고문헌

[1] 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.

[2] N. F. Johnson, Z. Duric, S. Jajodia, Information hiding: Steganography and Watermarking- Attacks and Countermeasures, Kluwer Academic Publishers, 2001.

[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.

[4] Y. K. Lee, L. H. Chen, "High Capacity Image Steganographic Model," IEEE Processings-Vision, Images & Signal Processing(UK), vol.147, no.3, pp.288-294, 2000.

[5] 배재민, 정성환, " 비트 플래인 복잡도를 기반으로 한 스테가노그라피의 삽입 용량 비교," 한국멀티미디어 추계학술대회, pp.699-702, 2001.