지각적으로 고화질을 보장하는 심층암층기술

장기식*, 정창호**, 이상진**, 양일우**
정보통신연구소*
고려대학교 정보보호기술연구센터**

High Quality perceptual Steganographic Techiques

Kisik Chang*, Changho Jung, Sangjin Lee**, Wooil Yang****
Service & Applications, Institute for Infocomm Research*
Korea University, Center for Information Security Technologies**
e-mail : *stusck@i2r.a-star.edu.sg, zangho@cist.korea.ac.kr*
sangjin@korea.ac.kr, doitnow@hananet.net

Abstract

Recently, several steganographic algorithms for two-color binary images have been proposed[7, 1, 5, 2]. In this paper, we propose a steganographic algorithm which embeds a secret message into bitmap images and palette-based images. To embed a message, the suggested algorithm divides a bitmap image into bit-plane images from LSB-plane to MSB-plane for each pixel, and considers each bit-plane image as a binary one. The algorithm splits each bit-plane image into $m \times n$ blocks, and embeds a r-bit($r = \lfloor \log_2 (mn+1) \rfloor - 1$) message into the block. And our schemes embed a message to every bit-plane from LSB to MSB to maximize the amount of embedded message and to minimize the degradation. The schemes change at most two pixels in each block. Therefore, the maximal color changes of the new algorithm are much smaller than other bit-plane embedding schemes' such as the sequential substitution schemes.

Ⅰ. 서론

심층암호기술은 점차 정교해지며, 널리 사용되고 있다. 심층암호의 목적은 송신자와 수신자가 감시자의 의심을 피하여 비밀 통신의 존재를 숨기는데 있다. 그러므로 심층암호는 엄폐물과 은닉물을 구별할 수 없어야 하고, 뿐만 아니라 엄폐물에 실용적으로 충분히 큰 비밀 메시지를 숨기는 기능을 제공해야 한다. 공개된 심층암호 도구들이 많이 존재하지만 이 두 가지 특징을 만족하는 도구를 찾기는 어렵다. 만약 심층암호 알고리즘이 안전하다면, 반대로 충분한 용량을 제공하지 못하고 있다.

1998년 Wu와 Lee는 팩시밀리 영상과 같이 두 가지의 단색인 검정색과 흰색으로 구성된 이진영상(binary image)을 이용하는 심층암호 기법을 처음으로 제안했다[7]. WL 기법은 삽입용량이 적은 단점 때문에 Chen과 Pan, Tseng은 가중치 행렬(weight matrix)을 사용한 CPT 기법을 제안했다[1]. 그러나 두 알고리즘은 삽입과정에서 변경할 화소의 위치를 무작위로 선택하기 때문에 메시지 삽입 후에 화질이 저하되는 결점을 가지고 있다. Tseng과 Pan은 거리 행렬(distance matrix)을 도입하여 CPT 기법을 개량했다[5]. TP 기법은 화질은 유지하지만, 삽입되지 않는 블록을 갖는다. 그래서 Chang과 Wu, Hwang이 반전된 블록의 거리행렬을 도입하여 삽입할 수 있는 블록을 증가시켰다[2]. 반면에 블록마다 삽입되는 비트수가 한 비트 감소하여 삽입용량의 증가효과를 거의 얻지 못하였다.

제안할 심층암호알고리즘은 비트맵(bitmap)과 같은 컬러영상과 팔레트기반의 영상에 확장된 TP 기법으로 비밀메시지를 삽입하는 것이다. 부가적으로 이 알고리즘은 오디오와 비디오 형식에도 일반화하여 적용할 수 있다. 메시지를 삽입하기 위해서는 먼저 비트맵 영상에서 컬러평면들을 나누고, 각 컬러평면을 비트평면으로 나눈다. 각각의 비트평면은 이진영상으로 고려하여, TP 기법을 적용하게 된다.

Ⅱ. 정의

이 논문에서 사용되는 용어와 기호들을 정의하도록 한다. 우리는 비트맵 영상을 정수의 행렬로 다룬다. 따라서 비트맵과 행렬은 같은 의미를 가진다. 같은 크기의 두 개의 비트맵 영상 B_1과 B_2가 주어졌을 때 $B_1 \wedge B_2$는 B_1과 B_2 원소들끼리의 AND 연산을 의미한다. 이와 마찬가지로 $B_1 \oplus B_2$는 B_1과 B_2 원소들끼리의 XOR 연산이며, $B_1 \otimes B_2$는 B_1과 B_2 원소들끼리의 곱 연산이다. 행렬 B가 주어졌을 때, B의 i번째 행과 j번째 열의 원소를 $[B]_{ij}$로, B의 모든 원소들의 합을 $SUM(B)$로 나타낸다.

- B : 원본 이진영상으로 $m\times n$ 크기의 블록으로 나뉘게 된다. 간단하게 설명하기 위해서 B는 $m\times n$의 배수라고 가정한다.
- K : 송신자와 수신자가 공유하는 비밀키이다. 무작위로 선택된 $m\times n$ 크기의 이진 행렬이다.
- W : 송신자와 수신자가 공유하는 비밀 가중치 행렬로서 어떤 조건을 가지는 $m\times n$ 크기의 정수 행렬이다.
- r : $m\times n$ 크기의 한 블록에 삽입될 수 있는 비밀 메시지의 비트수이다.

Tseng과 Pan은 영상의 화질을 보존하기 위해 거리 행렬과 가중치 행렬을 사용했다. 우선 주어진 엄폐 영상 B을 아래 그림에서와 같이 B_1과 B_2로 수정한다고 하자.

$$B=\begin{bmatrix}1&1&0&0&0\\1&1&0&0&0\\1&0&0&0&0\\1&0&0&0&0\\1&0&0&0&0\end{bmatrix},\ B_1=\begin{bmatrix}1&1&0&0&0\\1&1&0&0&0\\1&1&0&0&0\\1&0&0&0&0\\1&0&0&0&0\end{bmatrix},\ B_2=\begin{bmatrix}1&1&0&0&0\\1&1&0&0&0\\1&0&0&0&0\\1&0&0&1&0\\1&0&0&0&0\end{bmatrix}$$

B_1과 B_2로는 B와 한 화소만 다르다. 이때 B_1이 B_2보다 B에 더 비슷하다고 볼 수 있다. B_1에서 수정된 위치가 B에서 1의 값을 갖는 원소 옆에 있기 때문이다. B_2에서 수정된 화소는 더 눈에 띄게 된다. 여기서 다음과 같이 거리 행렬을 정의한다.

정의 1. *B와 같은 크기이면서 다음을 만족하는 정수 행렬을 거리행렬(distance matrix)라 한다.*

$$dist([B]_{i,j})=\min_{\forall x,y\{\sqrt{|i-x|^2+|j-y|^2}\ |\ [B]_{ij}\neq[b]x,y\}}. \quad (1)$$

$dist([B]_{i,j})$는 $[B]_{i,j}$의 보수를 취했을 때 $[B]_{x,y}$와 같으면서 $[B]_{x,y}$에 가장 가까운 거리에 있는 $[B]_{i,j}$이다. 이 행렬이 삽입알고리즘에서 변형될 위치를 선택하는데 사용된다. 위의 행렬 B의 거리 행렬은 다음과 같다.

$$\mathrm{dist}(B)=\begin{bmatrix}2&1&1&2&3\\\sqrt{2}&1&1&2&3\\1&1&\sqrt{2}&\sqrt{5}&\sqrt{10}\\1&1&2&\sqrt{8}&\sqrt{13}\\1&1&2&3&4\end{bmatrix}.$$

정의 2. *$m\times n$ 가중치 행렬 W의 $\{1,2,\cdots,2^{r-1}\}$의 각 원소가 W에 적어도 한번 사용될 때, 행렬 W를 가중치 행렬(weight matrix)라고 한다. 즉, $\{W_{i,j}\ |\ i=1,\cdots,m;\ j=1,\cdots,n\}=\{1,2,\cdots,2^{r-1}\}$이다.*

정의 3. *$m\times n$ 가중치 행렬 W의 2×2 부분행렬마다 적어도 하나의 홀수 원소를 포함한다면 이 가중치 행렬을 교정된 가중치 행렬(revised weight matrix)이라 한다.*

TP 기법은 삽입 후 은닉영상의 화질을 증진시키기 위해 교정된 가중치 행렬을 사용한다. 교정된 가중치 행렬의 모든 경우의 수는 다음과 같다.

$$\left({}_{\frac{mn}{2}}C_{2^{r-1}}\times(2^r-1)!\times(2^r-1)^{\frac{mn}{2}-(2^{r-1})}\right)\times\left({}_{\frac{mn}{2}}C_{2^{r-1}}\times(2^{r-1}-1)!\times(2^{r-1}-1)^{\frac{mn}{2}-(2^{r-1}-1)}\right). \quad (2)$$

아래는 교정된 가중치 행렬의 가능한 3가지 예이다.

$$\begin{bmatrix}o&o&o&o&o&o\\e&e&e&e&e&e\\o&o&o&o&o&o\\e&e&e&e&e&e\\o&o&o&o&o&o\\e&e&e&e&e&e\end{bmatrix},\ \begin{bmatrix}o&e&o&e&o&e\\e&o&e&o&e&o\\o&e&o&e&o&e\\e&o&e&o&e&o\\o&e&o&e&o&e\\e&o&e&o&e&o\end{bmatrix},\ \begin{bmatrix}e&o&e&o&e&o\\o&e&o&e&o&e\\e&o&e&o&e&o\\o&e&o&e&o&e\\e&o&e&o&e&o\\o&e&o&e&o&r\end{bmatrix}$$

Ⅲ. TP 기법

3.1 TP 삽입 과정

$r\le\lfloor log_2(mn+1)\rfloor-1$. TP 기법은 $m\times n$ 크기의 블록 B_i에 r 비트를 삽입한다. r 비트를 삽입하기 위해서 많아야 두 화소를 수정하게 된다. (3)

삽입 알고리즘은 메시지 $b_1b_2\cdots b_r$을 이진영상 B_i에 삽입해 식(4), (5)를 만족하도록 하면서 B'_i을 생성한다.

$$SUM((B'_i\oplus K)\otimes W)\equiv 0 \mod 2 \rightarrow SUM((B'_i\oplus K)\otimes W)/2\equiv b_1b_2\cdots b_r \mod 2^{r+1} \quad (4)$$

$$SUM((B'_i\oplus K)\otimes W)\equiv 1 \mod 2 \rightarrow \textit{there is no message in } B' \quad (5)$$

알고리즘은 다음과 같이 4단계로 구성된다.

1단계 B를 각각 $m\times n$ 크기의 블록으로 나눈다.

2단계 1단계에서 얻어진 각 블록 B_i가 전부 흰색이거나 검정색일 경우에는 아무런 변형을 가하지 않고 다음 블록으로 건너뛴다. 즉, 아무런 메시지도 삽입하지 않는다. 그렇지 않으면 다음 단계를 수행한다.

3단계 $B_i\oplus K$와 각 $w=1,2,\cdots,2^{r-1}$에 대하여 다음의 집합을 구한다.

$$S_w=\{(j,k)\ |\ [([W]_{j,k}=w)\cap([B_i\oplus K]_{k,j}=0)\cap((dist([B_i]_{j,k})\le\sqrt{2}))] \cup[([W]_{j,k}=2^{r+1}-w)\cap([B_i\oplus K]_{k,j}=1)\cap((dist([B_i]_{j,k})\le\sqrt{2}))]\}$$

즉, S_w의 원소인 (j,k)위치의 원소에 보수를 취했을 때의 w만큼 가중치의 차를 조정하게 된다.

4단계 $d\equiv b_1b_2\cdots b_t\ \|\ 0_{(2)}-SUM((B_i\oplus K)\otimes W)$ 다음과 같이 가중치의 차(weight difference)를 구한다. (6)

식(4)을 만족하도록 4단계에서 구한 합을 d만큼 증가시켜야 한다. 이제 d=0이면 B_i를 수정하지 않아도 식(4)을 만족한다. $d\neq0$일 때는, $S_{hd}\neq\varnothing$이고 $S_{-(h-1)d}\neq\varnothing$인 임의의 h를 선택하여 $(j,k)\in S_{hd}$와 $(j',k')\in S_{-(h-1)d}$의 화소를 보수를 취하면 식(4)을 만족한다. 만약 h가 존재하지 않으면 식(5)을 만족하도록 임의의 한 화소를 보수를 취한다..

3.2 TP 추출 과정

주어진 영상 B를 B'로 나눈다. B'가 전부 흰색이나 검정색이거나 SUM((B'i⊕K)⊗W)이 홀수이면 메시지를 추출하지 않는다. 그 외에는 다음 식을 통해 메시지를 추출한다.

$$\frac{SUM((B'_i \oplus K) \otimes W)}{2} \equiv b_1 b_2 \cdots b_r \mod 2^r \quad (7)$$

Ⅳ. 제안 기법

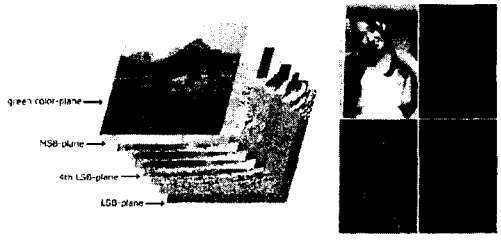
4.1 비트맵 영상에 대한 삽입 알고리즘

비트맵 영상의 화소값은 red, green, blue의 밝기 값으로 표현된다. RGB 영상인 비트맵 영상은 3개의 컬러평면으로 구성되어 있다고 볼 수 있다. 각 컬러는 8비트로 구성되어 있고 최상위 비트에서 최하위 비트까지 8개의 비트평면으로 나누어질 수 있다.

표 1. 제안된 알고리즘과 LSB-치환의 삽입량 비교
$M \times N$: 전체 영상의 크기, $m \times n$: 블록의 크기
k : 삽입과정에서 사용된 비트평면의 개수

	제안된 알고리즘	LSB-치환
블록당 삽입량 (bits/block)	$\lfloor log_2 mn+1 \rfloor - 1$	mn
블록당 삽입률 (bits/pixel)	$\frac{\lfloor log_2 mn+1 \rfloor - 1}{mn}$	1
블록당 변화되는 평균 비트수 (bits/block)	1.5	$\frac{mn}{2}$
전체삽입용량 (bits)	$\lfloor \frac{M}{m} \rfloor \times \lfloor \frac{N}{n} \rfloor \times r \times k$	MN
전체 수정된 화소의 평균 개수	$1.5k \times \lfloor \frac{M}{m} \rfloor \times \lfloor \frac{N}{n} \rfloor$	$\frac{MN}{2}$

그림 1. 비트맵 영상의 분할



Human Visual System(HVS)은 색상이나 채도보다 밝기 변화에 가장 민감하다. 밝기 Y는 RGB 컬러로부터 다음과 같이 계산된다[8].

$$Y = 0.299R + 0.587G + 0.114B$$

따라서 blue, red, green 순으로 삽입하는 것이 시각적으로 덜 민감하다.

삽입 알고리즘은 다음과 같다.

1단계 비트맵 엄폐영상 I를 3가지 컬러평면 B, G, R로 나눈다.

2단계 컬러 평면 C를 8개 비트 평면으로 나눈다.

3단계 비트 평면 $C^i \in \{C^0, C^1, \cdots, C^7\}$를 $m \times n$ 크기의 행렬이 되도록 나눈다.

4단계 나누어진 행렬 C_i^j는 TP 기법을 통해 삽입한다.

4.2 팔레트 기반 영상에 대한 삽입 알고리즘

먼저 팔레트 기반 영상을 이진영상으로 다루는 방법을 보자. 팔레트 기반 영상은 색인 값을 통해 영상을 구성하게 된다. 256 색상이 사용된 영상은 8비트의 색인 값으로 표현되는데 이 8비트를 비트평면으로 나누어 이진영상으로 생각할 수 있다. 각 비트평면은 비트맵 영상에 대한 알고리즘처럼 삽입할 수 있게 된다.

팔레트를 수정하지 않고 위와 같은 방법으로 삽입을 하게 되면 화질은 심한 손상을 받게 된다. 따라서 화질을 유지하기 위한 팔레트 조작이 필요하다. 이 목적을 위해 팔레트 색상들의 색인 값이 가까울수록 비슷한 색상이 배열되도록 정렬한다. 가장 간단한 정렬방식은 EzStego에서 사용되었는데, 첫 번째 팔레트 색상을 기준으로 유클리드 거리가 가까운 것부터 먼 것으로 정렬한다[3].

삽입과정은 세 단계로 구성된다. 먼저 팔레트의 색상들을 정렬하고, 색인 값의 비트 평면에 삽입한 후, 팔레트를 원래대로 돌려놓아야한다. 팔레트가 정렬되어 있는 것은 의심을 받게 되기 때문이다.

Ⅴ. 실험과 분석

5.1 삽입 용량

제안된 알고리즘은 LSB-치환 기법에 비해 최대 삽입량은 적다. 하지만 삽입된 비트 수에 대한 수정된 비트 수의 비율이 더 작다. 따라서 화질을 보존하는데 강점을 가지며, 삽입될 비트의 위치도 화질을 고려하게 된다.

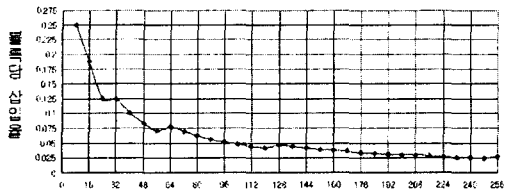
표 2. 189개의 비트맵 영상의 평균 삽입량

k	평균 삽입량	
비트평면	4×4 블록	8×8 블록
1	20,705.41(1.9379%)	9,627.14(0.9005%)
2	40,796.01(3.8186%)	19,121.79(1.7889%)
3	59,355.86(5.5571%)	28,174.91(2.6373%)
4	75,539.40(7.0755%)	36,414.28(3.4105%)
5	88,820.53(8.3258%)	43,531.58(4.0806%)
6	98,085.31(9.2725%)	49,252.93(4.6230%)
7	105,370.40(9.8980%)	53,388.35(5.0184%)
8	108,592.93(9.9671%)	55,608.58(5.2338%)

표 3. 800×600 크기의 팔레트 기반 영상 153개의 평균 삽입량

k	평균 삽입량	
비트평면	4×4 블록	8×8 블록
1	8,989.31(1.8728%)	4,357.28(0.9078%)
2	17,509.12(3.6477%)	8,577.26(1.7869%)
3	25,342.06(5.2796%)	12,544.75(2.6156%)

그림 2. 블록크기와 블록당 삽입률의 관계



5.2 실제 삽입 용량

제안된 알고리즘은 비트맵 영상과 팔레트 기반 영상으로 실험하였다. 448×336에서 1500×1124까지 다양한 크기의 비트맵 영상 189개와 800×600 크기의 팔레트 기반 영상 153개로 테스트하였다. 블록의 크기는 4×4(m=n=4, r=3)과 8×8(m=n=8, r=5)로 진행되었다. 4×4블록은 8×8블록보다 4×⅝(=2.4)배 더 삽입될 것으로 예상된다. 실험결과를 살펴보면 대략 2배 이상 더 삽입되는 것을 확인할 수 있다.

5.3 은닉영상의 화질

테스트 영상을 관찰한 결과, 비트맵 영상에서 4×4블록으로 삽입한 경우는 5번째 비트평면에 삽입할 때부터, 8×8블록으로 삽입한 경우는 6번째 비트평면에 삽입할 때부터 화질의 변화를 확인할 수 있었다. 팔레트 기반 영상은 4×4블록의 경우는 4번째 비트평면, 8×8블록의 경우는 5번째 비트평면에서부터 화질 변화를 확인할 수 있었다.

5.4 통계 분석

Westfeld와 Provos가 소개한 χ^2-test를 사용하여 통계분석을 시행하였다[6, 4]. 원본 영상은 탐지되지 않는 것들로만 테스트되었기 때문에 false positive error는 제거되었다. 실험 결과는 4×4블록이 8×8블록보다 더 잘 탐지되는 것을 확인했다.

표 4. 189개 비트맵 영상의 통계 분석 결과
Original : Wesfeld가 제안한 χ^2-test
Extended : Provos가 제안한 χ^2-test

k	4×4 블록		8×8 블록	
비트평면	Original	Extended	Original	Extended
1	11(5.82%)	31(16.40%)	0(0.00%)	5(2.65%)
2	15(7.94%)	45(23.81%)	0(0.00%)	7(3.70%)
3	21(11.11%)	55(29.10%)	0(0.00%)	7(3.70%)
4	26(13.76%)	75(39.68%)	2(1.06%)	9(4.76%)
5	38(20.11%)	77(40.74%)	3(1.59%)	9(4.76%)
6	42(22.22%)	102(53.97%)	4(2.12%)	11(5.82%)
7	51(26.98%)	102(53.97%)	5(2.65%)	13(6.88%)
8	49(25.93%)	103(54.50%)	6(3.17%)	20(10.58%)

표 5. 153개 팔레트 기반 영상의 통계 분석 결과

k	4×4 블록		8×8 블록	
비트평면	Original	Extended	Original	Extended
1	0(0.00%)	0(0.00%)	0(0.00%)	0(0.00%)
2	0(0.00%)	1(0.65%)	0(0.00%)	0(0.00%)
3	0(0.00%)	1(0.65%)	0(0.00%)	0(0.00%)

VI. 결론

화질을 보장하면서 충분한 용량을 제공하는 심층암호기술을 제안하였다. 제안된 알고리즘은 블록당 $\lfloor log_2(mn+1) \rfloor - 1$ 비트를 삽입하면서 평균적으로 1.5 비트만 수정한다. 또한 수정되는 비트는 영상의 윤곽선을 유지해 주기 때문에 영상은 매우 잘 보존된다. 최대 삽입량은 상대적으로 적은 편이지만, 상위 비트평면까지 삽입하므로서 삽입량을 증가시켜주었기 때문에 충분한 삽입량을 제공해준다.

참고문헌

[1] Y.Y. Chen, H.K. Pan, and T.C. Tseng, "A Secure Data Hiding Scheme for Two-Color Images", *Proceedings of the Fifth IEEE Symposiumon Computers and Communications*, 2000, pp.750-755.

[2] C.C. Chang, M.N. Wu, and K.F. Hwang, "High Quality Perceptual Data Hiding Technique for Two-Color Images", *Proceedings of Pacific Rim Workshop on Digital Steganography*, 2002, Kitakyushu, Japan, July 11-13, 2002, pp.65-70.

[3] R. Machado, "EzStego", http://www.stego.com/

[4] N. Provos, "Defending Against Statistical Steganalysis", *Proceedings of the 10th USENIX Security Symposium*, August 2001, pp.323-335.

[5] T.C. Tseng and H.K. Pan, "Secure and Invisible Data Hiding in 2-color Images", *Proceedings of INFOCOM*, 2001, IEEE, Vol.2, pp.887-896, 2001.

[6] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems", *Information Hiding - Third International Workshop*, IH'99, vol.1768 of Lecture Notes in Computer Science, Springer-Verlag, pp.61-76, 1999.

[7] M.Y. Wu and J.H. Lee, "A Novel Data Embedding Method for Two-Color Facsimile Images", *Proceedings of International Symposium on Multimedia Information Processing*, Chung-Li, Taiwan, R.O.C, December 1998.

[8] R.C. Gonzalez and R.E. "Woods, Digital Image Processing" , *Addison-Wesley Publishing Company, Inc.*, 1992, pp.225-237.