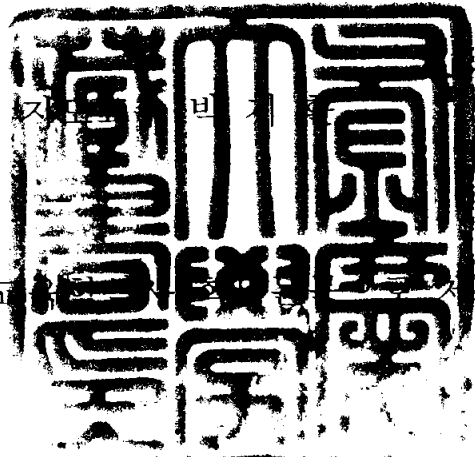


교육학 석사 학위 논문

카툰 영상을 이용한 스테가노그래피에
관한 연구



이 논문을 교

2004년 8월

부경대학교 교육대학원

전산교육전공

하 순 혜

하순혜의 교육학석사 학위논문을 인준함

2004 년 8 월 31 일

주 심 공학박사 김 창 수



위 원 이학박사 윤 성 대



위 원 공학박사 박 지 환



차 례

표차례	ii
그림차례	iii
Abstract	iv
I. 서 론	1
II. 관련 연구	3
1. CPT 방식	3
2. TP 방식	6
3. WTL 방식	10
III. 제안 방식	12
1. 이진 영상에서의 데이터 은닉	12
2. 다치 컬러 영상에서의 데이터 은닉	18
IV. 실험 및 결과	24
1. 이진 영상에서의 데이터 은닉 방식 비교	24
2. 다치 컬러 영상에서의 데이터 은닉 방식 비교	27
V. 결 론	30
참고 문헌	31

표 차 례

<표 1> 카툰 영상에서의 삽입 비트 수	25
<표 2> 텍스트 영상에서의 삽입 비트 수	25
<표 3> 기존 방식과 제안 방식의 삽입 비트 수 비교	27
<표 4> 기존 방식과 제안 방식의 화질 비교(PSNR)	28

그림 차례

그림 1. CPT 데이터 은닉 방식의 블록도	4
그림 2. CPT 방식의 데이터 은닉 예시	5
그림 3. 변경 가능한 픽셀	11
그림 4. 픽셀 재정렬 후 변경 가능한 픽셀	11
그림 5. 가시적인 픽셀의 변경	12
그림 6. 다른 순위를 가지는 3×3 블록의 두 패턴	13
그림 7. 제안 방식1에서의 데이터 은닉 예시	16
그림 8. (a) 변경 가능 픽셀, (b) 재정렬된 영상	16
그림 9. 변경된 영상 PF'	17
그림 10. 변경된 영상 PF' 를 원래 위치로 복귀	17
그림 11. (a) 변경 불가능한 패턴, (b) 변경 가능한 패턴	19
그림 12. 제안 방식2에서의 데이터 은닉 예시	21
그림 13. (a) F 의 이진화된 영상 GF , (b) $GF \oplus K$ 의 계산 결과	22
그림 14. 원영상과 삽입영상	26
그림 15. 원영상과 삽입영상	26
그림 16. 원영상과 삽입영상	28
그림 17. 원영상과 삽입영상	29

A STUDY ON STEGANOGRAPHY USING CARTOON IMAGE

Soon Hye Ha

Graduate School of Education

Pukyong National University

Abstract

A manufacture of digital media and information exchange are consisting vigorously by development of computer and Internet. Accordingly, study on data hiding technology is required. Usually, data hiding scheme is classed by Watermaking and Steganography greatly.

Usually, steganography is used in color or gray image to reduce visual effect. As cartoon image, binary image or few color image is used much, but it is difficult hiding secret information because color number is limited.

In this paper we propose data hiding scheme using weight matrix in binary or few color image. In our scheme using binary image, for each $m \times n$ block of the host image, we will hide as many as $\lfloor \log_2(mn+1) - 2 \rfloor$ bits of secret data by changing at most 2 bits in the block. And new scheme using few color image can hide as many as $\lfloor \log_2(mn+1) - 1 \rfloor$ bit of secret data in the block. The new scheme can still offer a good data hiding ratio and the hiding effect is quite invisible.

I. 서 론

컴퓨터 기술의 발달과 인터넷의 급속한 보급으로 정보 전달 효과가 뛰어난 디지털 미디어의 제작 및 정보 교환이 활발하게 이루어지고 있다. 이러한 디지털 미디어들은 접근이 용이하며, 편집 및 복사가 가능하고, 편리하게 전송할 수 있다는 장점으로 디지털 비밀 정보를 전자 메일 등으로 송수신하는 비율이 급증하고 있다. 따라서 이러한 비밀 정보를 네트워크를 통해 안전하게 전달하기 위한 정보보호의 필요성이 요구된다[1,6]. 이러한 문제를 해결하기 위한 방법으로 데이터 은닉 기술에 관한 연구가 활발히 진행되고 있으며, 데이터 은닉 기법은 크게 워터마킹(watermarking)과 스테가노그래피(steganography)로 분류된다.

워터마킹이란 디지털 콘텐츠에 사용자의 ID(Identification)나 자신만의 정보를 넣음으로써 불법적인 복제를 막고, 데이터의 소유자의 저작권과 소유권을 효율적으로 보호하기 위한 방법으로써 데이터에 일정한 암호를 숨겨서 부호화 하는 과정으로 이러한 부호를 워터마크라 한다. 이는 디지털 매체의 저작권 인증을 위한 기술로 워터마크의 삽입량은 중요하지 않으며, 추출 역시 완전하게 추출되지 않고 특정 기준 값 이상이면 저작권을 인정하기도 한다.

한편, 스테가노그래피는 송신자와 수신자간 비밀 정보 전달을 목적으로 비밀 정보를 이미지나 오디오, 비디오 또는 텍스트 등 커버(cover) 라고 불리는 다른 미디어에 숨겨서 전송하며 제 3자는 정보가 숨겨져 있다는 사실 자체를 알지 못하도록 통신하는 기술이다. 스테가노그래피는 삽입 용량(capacity), 숨겨진 정보의 비인지성(imperceptibility) 등을 만족하여야 하

고, 대부분 영상 데이터를 사용하며 일반적으로 시각적인 손상을 줄이기 위해 컬러 또는 그레이 영상에서 많이 응용되어지고 있다. 반면, 카툰 영상과 같이 표현 가능한 컬러 수가 제한된 이진 영상 및 다치 컬러 영상들도 그 활용도가 여전히 높음에도 불구하고 그 특성상 비밀 정보를 비가시적으로 숨기는 것이 쉽지 않다.

본 논문에서는 이진 영상 및 다치 컬러 영상에서 비밀 정보를 은닉하는 방법으로 가중치 테이블을 사용하여 정보의 삽입량을 증가시키는 방법을 제안한다.

첫 번째 제안 방식은 이진 영상을 이용한 데이터 은닉 방식으로 비가시적인 패턴을 가진 픽셀을 변경하여 기존의 방식에 비해 화질의 열화를 감소시키고, 영상의 모든 픽셀을 랜덤하게 재정렬함으로써 삽입량도 우수한 방식이다.

두 번째 제안 방식에서는 이진 영상에서 이용한 데이터 은닉 방식 중 높은 비밀 데이터의 삽입률을 보이는 TP 방식[3]을 다치 컬러 영상에 적용한다. 이 제안 방식은 기존의 다치 컬러 영상을 이용한 은닉 방식에 비해 2배 이상의 많은 비밀 데이터를 삽입하면서 화질 또한 우수하다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 방식에 대해 간략하게 소개하고, 3장에서는 이진 영상 및 다치 컬러 영상을 이용한 새로운 제안 방식을 기술하며, 4장에서는 실험을 통하여 기존 방식과 제안 방식을 비교, 분석한다. 그리고 마지막 5장에서 결론을 제시한다.

II. 관련 연구

이진 영상을 이용하여 비밀 데이터를 은닉하는 방법 중 가중치 테이블을 사용한 기법으로 CPT 방식[2]과 이를 개선한 TP 방식[3]이 있다. 가중치 테이블은 비밀키의 역할뿐 아니라 1 비트의 변경으로 여러 비트를 삽입한 효과를 가져온다.

또한 WTL 방식[4]은 영상의 모든 픽셀을 재정렬하여 각 블록에 변경 가능한 픽셀을 고르게 분포시킴으로써 모든 블록에 비밀 데이터가 삽입되도록 하는 방식이다.

1. CPT 방식

데이터 은닉 기법 중 CPT 방식은 가중치 테이블을 이용하여 변경되는 비트 수를 줄이면서 삽입되는 데이터의 양을 증가시키는 방법이다. 이 방법은 원 영상을 $m \times n$ 블록으로 분할한 후, 각 블록의 최대 2비트만을 변화시켜 한 블록에 $\lfloor \log_2(mn+1) \rfloor$ 비트만큼 숨길 수 있다. 그림 1은 CPT 방식의 블록도이다.

비밀 데이터를 삽입하기 위해, 원 영상을 F 라 두고, F 를 $m \times n$ 크기의 블록으로 나눈다. CPT 방식의 한 블록에는 r 비트($r \leq \lfloor \log_2(mn+1) \rfloor$)의 데이터를 삽입할 수 있으며, 송신자와 수신자간 공유하는 비밀키는 다음 두 가지로 구성된다.

- K : 랜덤한 $m \times n$ 크기의 이진 행렬

- W : $m \times n$ 크기의 가중치 정수 행렬

$$\{[W]_{i,j} | i=1 \dots m, j=1 \dots n\} = \{1, 2, \dots, 2^r - 1\}$$

여기서 구성될 수 있는 W 의 수는 $C_{2^r-1}^{mn} * (2^r - 1)! * (w^r - 1)^{mn - (2^r - 1)}$ 이고, 이는 보안을 유지하는 데 충분히 큰 수이다.

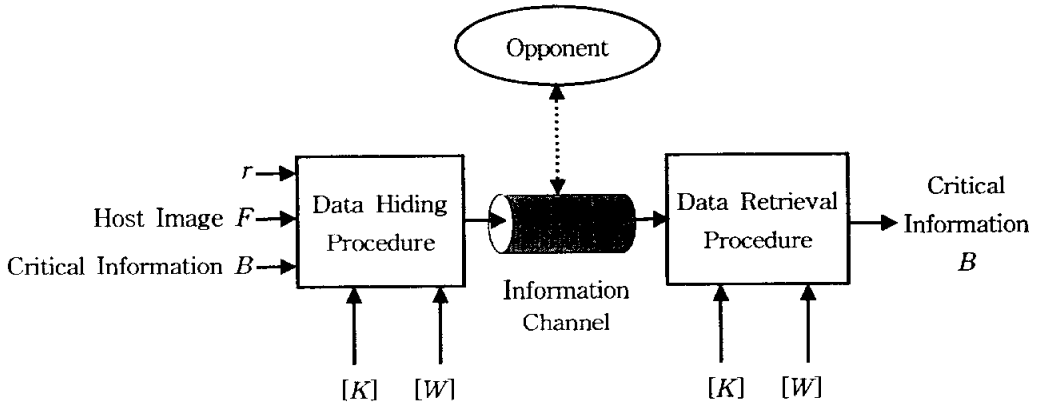


그림 1. CPT 데이터 은닉 방식의 블록도

원 영상 F 의 i 번째 블록을 F_i 라 두고, 삽입 비트열을 $b_1 b_2 \dots b_r$ 라 할 때, CPT 방식에서의 비밀 데이터 삽입과정은 다음과 같다.

compute $F_i \oplus K$;

compute $SUM((F_i \oplus K) \otimes W)$;

/*define S_w

$$S_w = \{(j, k) | [W]_{j,k} = w \wedge [(F_i \oplus K)_{j,k} = 0] \vee$$

$$([w]_{j,k} = 2^r - w \wedge [(F_i \oplus K)_{j,k} = 1])\}. \quad (w = 1, \dots, 2^r - 1)*/$$

$$d \equiv [(b_1 b_2 \dots b_r) - SUM((F_i \oplus K) \otimes W)] \pmod{2^r};$$

if $d=0$ then keep F_i intact;

else /*transform F_i to F'_i */

if there exists an h such that $S_{hd} \neq \emptyset$ and $S_{-(h-1)d} \neq \emptyset$

then

randomly pick an h which satisfies the above condition;

randomly pick a $(j, k) \in S_{hd}$ and complement the bit $[F_i]_{j, k}$;

randomly pick a $(j, k) \in S_{-(h-1)d}$ and complement the bit $[F_i]_{j, k}$;

예를 들어, 그림 2(a)와 같이 F (원 영상), K (비밀키 행렬), W (가중치 행렬)가 주어지고, 삽입할 비밀 데이터가 '1 0 1 0'이라 할 때, 삽입 과정은 다음과 같다.

$$F = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad K = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad W = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 1 \end{bmatrix}$$

(a) 원 영상 F , 비밀키 행렬 K , 가중치 행렬 W

$$F \oplus K = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad (F \oplus K) \otimes W = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 9 & 10 & 11 & 0 \\ 0 & 14 & 0 & 1 \end{bmatrix}$$

(b) $F \oplus K$ 와 $(F \oplus K) \otimes W$ 의 결과

그림 2. CPT 방식의 데이터 은닉 예시

$$r=4, \text{SUM}((F \oplus K) \otimes W) = 52,$$

$$d \equiv [(1010)_2 - 52] \bmod 2^4 = -42 \bmod 16 = 6,$$

$S_6 = \{(3, 2)\}$ 이므로 F 의 $(3, 2)$ 를 변경한다.

$$F = \begin{array}{|c|c|c|c|} \hline 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 0 & 1 \\ \hline 0 & \mathbf{1} & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ \hline \end{array}$$

비밀 데이터의 추출 시, 변경된 영상 F' 에 대하여 다음과 같이 계산하여 비밀 데이터를 얻을 수 있다.

$$\text{SUM}((F' \oplus K) \otimes W) \pmod{2^r} = 42 \bmod 16 = 10 = (1010)_2$$

\therefore 삽입된 비트열 $b_0 b_1 b_2 b_3 = 1010$

2. TP 방식

TP 방식은 CPT 방식의 변형으로 비밀 데이터 은닉 후, 화질을 개선하는데 목적이 있다. 앞에서 기술한 CPT 방식은 변경된 새로운 픽셀의 값이 이웃한 픽셀의 값과 동일하다면, 변화가 눈에 잘 띄지 않지만, 앞의 예처럼 변경된 픽셀 값이 1이고, 이웃한 8개의 픽셀 값이 모두 0이라면 데이터 삽입 후 변경된 부분을 쉽게 확인 할 수 있다.

TP 방식에서는 변경된 픽셀의 값과 이웃한 값이 동일한 값이 되도록 한 픽셀에 대해 서로 다른 값을 가지는 픽셀간의 거리를 계산하는 과정을 추가한다. 원 영상 F 에 대해 서로 다른 값을 가지는 픽셀 사이의 최소거리를 계산한 거리 행렬 $distF$ 를 다음과 같이 정의한다.

$$[dist(F)]_{i,j} = \min_{\forall x,y} \{ \sqrt{|i-x|^2 + |j-y|^2} \mid [F]_{i,j} \neq [F]_{x,y} \}$$

따라서 그림 2의 예시에서 살펴본 영상 F 의 거리행렬 $distF$ 는 다음과 같다. 거리 행렬 $distF$ 의 값이 $\sqrt{2}$ 보다 큰 비트의 값은 변경하지 않음으로서 데이터 삽입 후 화질을 개선할 수 있으며, CPT 방식의 예시에서 변경한 (3,2)의 해당 거리행렬 값은 $\sqrt{5}$ 이므로 TP 방식에서는 이 픽셀을 변경하지 않는다.

$$distF = \begin{array}{|c|c|c|c|} \hline 1 & 1 & 1 & 1 \\ \hline \sqrt{2} & 1 & 1 & 1 \\ \hline \sqrt{10} & \sqrt{5} & \sqrt{2} & 1 \\ \hline \sqrt{13} & \sqrt{8} & \sqrt{5} & 2 \\ \hline \end{array}$$

TP 방식에서는 화질을 위해 한 블록당 삽입할 수 있는 비트 수 r 은 CPT 방식에 비해 1비트 적게 삽입된다. ($r \leq \lfloor \log_2(mn+1) - 1 \rfloor$)

원 영상을 F 라 두고, F 를 $m \times n$ 크기의 블록으로 나눈다. 한 블록에는 r 비트 ($r \leq \lfloor \log_2(mn+1) - 1 \rfloor$)의 데이터를 삽입하며, 비밀키는 다음 두 가지로 구성된다.

- K : 랜덤한 $m \times n$ 크기의 이진 행렬
- W : $m \times n$ 크기의 가중치 정수 행렬

$$\{[W]_{i,j} | i=1 \dots m, j=1 \dots n\} = \{1, 2, \dots, 2^{r+1}-1\}$$

W 의 각 2×2 서브 블록에는 적어도 하나의 홀수가 존재하도록 구성하는데 이는 데이터 삽입 후 화질의 열화를 감소시키는 효과가 있다.

우선, 원 영상 블록의 모든 픽셀 값을 조사하여, 모두 1 또는 0인 경우 (블록 전체가 흑 또는 백인 경우)는 비밀 데이터를 삽입하지 않고, 그렇지 않은 블록에 대해 다음 단계에 따라 데이터를 삽입한다.

compute $F_i \oplus K$;

compute $SUM((F_i \oplus K) \otimes W)$;

/*define S_w

$$S_w = \{ (j, k) | [([W]_{j,k} = w \wedge [F_i \oplus K]_{j,k} = 0) \wedge (dist[F]_{j,k} \leq \sqrt{2})] \vee [([w]_{j,k} = 2^{r+1} - w \wedge [F_i \oplus K]_{j,k} = 1) \wedge (dist[F]_{j,k} \leq \sqrt{2})] \}.$$

$$(w = 1, \dots, 2^{r+1} - 1)*/$$

$$d \equiv [(b_1 b_2 \dots b_r 0) - SUM((F_i \oplus K) \otimes W)] \pmod{2^{r+1}};$$

if $d=0$ then keep F_i intact;

else /*transform F_i to F_i' */

if there exists an h such that $S_{hd} \neq \emptyset$ and $S_{-(h-1)d} \neq \emptyset$

then

randomly pick an h which satisfies the above condition;

randomly pick a $(j, k) \in S_{hd}$ and complement the bit $[F_i]_{j,k}$;

randomly pick a $(j, k) \in S_{-(h-1)d}$ and complement the bit $[F_i]_{j,k}$;

else /*no data will be hidden*/

if $SUM((F_i \oplus K) \otimes W) \pmod{2} = 1$ then keep F_i intact;

else

select a (j, k) such that $[W]_{j, k}$ is odd and
its corresponding $[dist(F)]_{j, k}$ is the smallest;
complement the bit $[F_i]_{j, k}$;

위의 과정 중 d 의 계산에서 삽입 비트열 마지막에 0을 추가하여 계산함을 유의한다. 또한 비밀 데이터가 삽입된 블록과의 구분을 위해 삽입되지 않은 블록의 경우, $SUM((F_i \oplus K) \otimes W)$ 의 값을 홀수로 만드는 과정을 추가한다.

비밀 데이터의 추출 시, 변경된 영상 F' 에 대하여 블록의 모든 비트가 1 또는 0인 경우와 $SUM((F_i' \oplus K) \otimes W)$ 가 홀수인 경우는 비밀 데이터가 삽입되지 않은 것으로 간주하고, $SUM((F_i' \oplus K) \otimes W)$ 가 짝수일 때, $[SUM((F_i' \oplus K) \otimes W) \pmod{2^{r+1}}] / 2$ 을 계산하여 삽입된 비밀 데이터를 얻는다.

그림 2의 CPT 방식의 예시에서 살펴본 영상 F (원 영상)와 K (비밀키 행렬)가 동일하게 주어질 경우, W (가중치 행렬)도 그림 2와 동일하게 구성할 수 있다. 단, 여기서 삽입할 비트수 r 은 CPT 방식보다 1비트 적은 3이 되며, 삽입할 비트열을 '1 0 1'이라 할 때의 삽입과정을 살펴보자.

$$r=3, SUM((F \oplus K) \otimes W) = 52,$$

$$d \equiv [(1010)_2 - 52] \pmod{2^4} = -42 \pmod{16} = 6,$$

$S_6 = \{(3, 2)\}$, $distF$ 의 $(3, 2)$ 는 $\sqrt{2}$ 보다 크기 때문에 변경 대상에서 제외되며, d 와 같은 값이 되도록 2개의 비트를 변경한다.

$h=2$ 일 때, $S_{12} = \{(3, 4)\}$, $S_{-6} = \{(2, 2)\}$ 이고, 두 픽셀의 해당 $distF$ 의

값도 둘 다 $\sqrt{2}$ 를 넘지 않으므로 F 의 (3,4), (2,2) 두 비트를 변경한다.

$$F' = \begin{array}{|c|c|c|c|} \hline 0 & 1 & 0 & 1 \\ \hline 0 & \mathbf{1} & 0 & 1 \\ \hline 0 & 0 & 0 & \mathbf{1} \\ \hline 0 & 0 & 0 & 0 \\ \hline \end{array}$$

비밀 데이터의 추출 시, 변경된 영상 F' 에 대하여 다음을 계산하여 비밀 데이터를 얻을 수 있다.

$$[SUM((F' \oplus K) \otimes W) \pmod{2^{r+1}}] / 2 = (42 \pmod{16}) / 2 = 10 / 2 = 5 = (101)_2$$

$$\therefore \text{삽입된 비트열 } b_0 b_1 b_2 = 101$$

3. WTL 방식

이진 영상에 기밀 데이터를 삽입하는 다른 방식 중 WTL의 방식은 변경 가능한 픽셀들을 계산하여 찾은 후, 이를 랜덤하게 섞는 과정(Shuffle)을 통해 보안뿐 아니라 데이터의 삽입률도 향상됨을 보였다. 변경 가능한 픽셀들이 서로 섞임으로써 변경 가능한 픽셀들이 각 블록에 분포되어 낭비되는 블록이 발생하지 않도록 하는 방식이다.

그림 3에서 점으로 표시된 부분은 변경 가능한 픽셀이며, 블록마다 변경 가능한 픽셀의 수가 현저하게 다르다.(사각형은 하나의 블록을 의미한다.)



그림 3. 변경 가능한 픽셀(점으로 표시된 부분)

영상의 모든 픽셀을 랜덤하게 섞는 과정을 통해 그림 4에서 보는 바와 같이 변경 가능한 픽셀이 블록마다 적어도 하나 이상 분포됨으로써 모든 블록에서의 데이터 삽입이 가능해 진다.

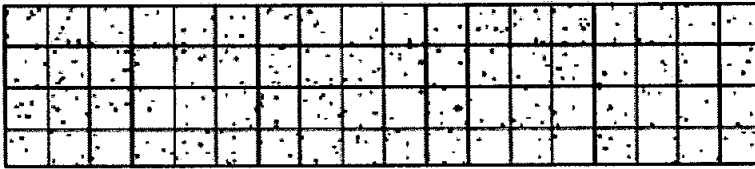


그림 4. 픽셀 재정렬 후 변경 가능한 픽셀

III. 제안 방식

제안 방식에서는 TP 방식의 화질을 개선하기 위해 변경시 비가시적인 패턴을 가진 픽셀을 선택하며, 삽입 과정에서 WTL 방식의 픽셀 재정렬을 이용한다. 또한 TP 방식을 다치 컬러 영상에 적용하여 기존의 방식에 비해 화질과 삽입량이 우수한 방식을 제안한다.

제안 방식은 이진 및 다치 컬러 영상과 텍스트 등에서 모두 적용 가능하지만 개선된 효과는 비교적 같은 값이 연속되어 구성되는 카툰 이미지에서 크게 느낄 수 있다.

1. 이진 영상에서의 데이터 은닉(제안 방식 1)

TP 방식은 화질을 고려하여 CPT 방식에서 거리 행렬($distF$)을 추가하였지만 여전히 데이터의 삽입 후 화질이 떨어진다.

예를 들면, 변경된 새로운 픽셀의 값과 같은 값이 하나라도 이웃해 있으면 변경이 가능하므로 그림 5의 (3,2)는 변경 조건에 만족하는 픽셀이지만 실제로 변경하면 가장자리에 점이 찍혀 변경을 쉽게 확인 할 수 있다.

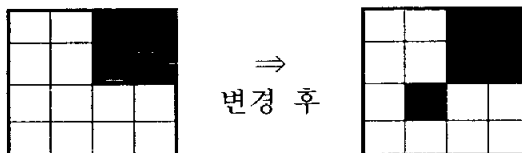


그림 5. 가시적인 픽셀의 변경

한편 WTL 방식은 픽셀들을 랜덤하게 재정렬하는 과정을 통해 모든 블록에 데이터를 삽입하는 것이 가능해 졌으나 한 블록에는 오직 1비트만이 삽입 가능하므로 TP 방식과 비교하면 WTL 방식은 삽입량이 매우 적은 단점이 있다.

제안 방식1에서의 변경 가능한 픽셀은 하나의 픽셀과 이웃한 8개의 픽셀과의 관계를 조사하여 픽셀의 우선 순위를 정한 후, 그 순위에 따라 변경될 픽셀이 선택된다. 그러므로 변경 후 눈에 잘 띄는 픽셀은 선택되지 않는다.

예를 들어, 그림 6(a)와 그림 6(b)의 패턴을 가진 두 블록에 대해 가운데 픽셀을 변경시킨다고 가정하면 그림 6(b)보다 그림 6(a)의 변화가 시각적으로 덜 민감하다. 그러므로 그림 6(a)의 패턴이 그림 6(b)보다 더 높은 우선 순위를 가지게 된다.

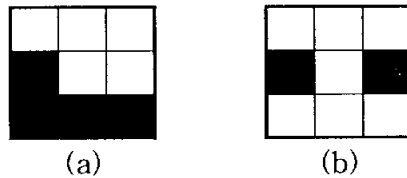


그림 6. 다른 순위를 가지는 3×3 블록의 두 패턴

픽셀들의 변경 우선 순위가 정해지면 영상을 일정한 블록으로 분할한 후, 블록 전체가 완전히 백이거나 흑인 블록을 제외한 모든 픽셀들을 랜덤하게 섞는다. 픽셀이 재정렬 된 영상을 다시 분할하고, 각 블록에 데이터를 삽입 할 때, 가중치 테이블을 이용한 TP 방식의 삽입 과정을 적용한다.

TP 방식에서 문제점으로 지적한 데이터 삽입 후 화질은 높은 순위를 가진 패턴의 픽셀을 선택함으로써 시각적인 영향을 줄일 수 있다. 그러나 패턴 조사를 통해 선택되는 변경 가능한 픽셀의 수는 TP 방식의 변경 가능

한 픽셀에 비해 그 수가 1/4 정도로 감소되어 삽입이 불가능한 블록이 증가하고, 데이터의 삽입량도 현저하게 감소한다.

가능한 모든 블록에 비밀 데이터의 삽입이 가능하도록, 한 블록에 삽입되는 데이터의 양은 $\lfloor \log_2(mn+1) - 2 \rfloor$ 비트로 TP 방식보다 1 감소시키고, 모든 픽셀들을 랜덤하게 재정렬하는 과정을 추가한다. WTL 방식에서 살펴본 바와 같이 픽셀을 랜덤하게 재정렬 과정은 각 블록에 변경 가능한 픽셀들이 고르게 분포되도록 한다. 따라서 한 블록당 삽입하는 데이터의 양은 TP 방식보다 적어지지만 삽입이 가능한 블록의 수는 증가되므로 TP 방식의 삽입량을 유지시킬 수 있다.

우선, 원 영상의 모든 픽셀에 대해 패턴의 우선 순위를 조사하여 변경 가능한 픽셀을 선택한다. (편의상 변경가능한 픽셀을 ‘음영’이라 표시한다.) 그리고 블록 전체가 완전히 흑 또는 백인 블록을 제외한 영상의 모든 픽셀을 랜덤하게 재정렬하며, 이 재정렬된 영상을 PF 라 한다. 이 때, 제안 방식1의 비밀 데이터 삽입 과정은 다음과 같다.

```

compute  $PF_i \oplus K$ ;
compute  $SUM((PF_i \oplus K) \otimes W)$ ;
/*define  $S_w$ 
 $S_w = \{ (j, k) \mid [ ([W]_{j,k} = w \wedge [PF_i \oplus K]_{j,k} = 0) \wedge (F_{j,k} = \text{'음영'}) ] \vee$ 
 $[ ([w]_{j,k} = 2^{r+1} - w \wedge [PF_i \oplus K]_{j,k} = 1) \wedge (F_{j,k} = \text{'음영'}) ] \}$ .
 $(w = 1, \dots, 2^{r+1} - 1)*/$ 
 $d \equiv [(b_1 b_2 \dots b_r 0) - SUM((PF_i \oplus K) \otimes W)] \pmod{2^{r+1}}$ ;
if  $d = 0$  then keep  $PF_i$  intact;
else /*transform  $PF_i$  to  $PF_i'$ */
```

```

if there exists an  $h$  such that  $S_{hd} \neq \emptyset$  and  $S_{-(h-1)d} \neq \emptyset$ 
then
    randomly pick an  $h$  which satisfies the above condition;
    randomly pick a  $(j, k) \in S_{hd}$  and complement the bit  $[PF_i]_{j, k}$ ;
    randomly pick a  $(j, k) \in S_{-(h-1)d}$  and complement the bit  $[PF_i]_{j, k}$ ;
else /*no data will be hidden*/
    if  $SUM((PF_i \oplus K) \otimes W) \bmod 2 = 1$  then keep  $PF_i$  intact;
    else
        select a  $(j, k)$  such that  $[W]_{j, k}$  is odd and
        its corresponding  $(j, k)$  is '음영';
        complement the bit  $[PF_i]_{j, k}$ ;

```

비밀 데이터의 삽입 후 영상 PF 의 모든 픽셀을 원 위치로 이동시킨 F' 를 전송한다.

비밀 데이터의 추출 시, 변경된 영상 F' 에 대하여 삽입할 때 재정렬한 위치로 모든 픽셀을 이동한 후 블록으로 분할한다. 블록 PF'_i 에 대해 $SUM((PF'_i \oplus K) \otimes W)$ 가 짝수이면, $[SUM((PF'_i \oplus K) \otimes W) \bmod 2^{r+1}] / 2$ 을 계산하여 삽입된 비밀 데이터를 얻을 수 있다.

예를 들어, F (원 영상)의 4×4 크기의 첫 번째 블록 F_1 , 두 번째 블록 F_2 , K (비밀키 행렬)가 그림 7과 같이 주어졌을 때, 블록 당 삽입할 수 있는 비트 수는 2비트이다. ($r \leq \lfloor \log_2(mn+1) - 2 \rfloor = 2$) 따라서, w (가중치 행렬)가 다음과 같이 구성될 수 있으며, 여기서 삽입할 비밀 데이터가 '1 0 1 0'이라 할 때, 제안 방식1의 삽입 과정을 살펴본다.

$$F = \begin{matrix} \begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{matrix} \\ F_1 \quad F_2 \end{matrix} \quad K = \begin{matrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{matrix} \quad W = \begin{matrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 1 \\ 2 & 3 & 4 & 5 \\ 6 & 7 & 1 & 2 \end{matrix}$$

그림 7. 제안 방식1에서의 데이터 은닉 예시

원 영상 F 의 모든 픽셀에 대해 패턴의 우선 순위를 조사하여 변경 가능한 픽셀을 그림 8(a)의 음영 부분으로 표시하였다. 그림 8(b)는 영상의 모든 픽셀들을 랜덤하게 재정렬한 것으로 변경 가능한 픽셀이 각 블록에 고르게 분포됨을 알 수 있다.

$$F = \begin{matrix} \begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \text{shaded} & \text{shaded} & \text{shaded} & \text{shaded} & \text{shaded} & \text{shaded} & 1 \\ 0 & 0 & 0 & 1 & \text{shaded} & \text{shaded} & \text{shaded} & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{matrix} \\ F_1 \quad F_2 \end{matrix} \quad PF = \begin{matrix} \begin{matrix} 0 & 1 & \text{shaded} & 1 & 0 & 1 & 1 & \text{shaded} \\ 1 & 0 & 1 & \text{shaded} & 1 & 1 & 0 & 1 \\ \text{shaded} & 1 & \text{shaded} & 1 & \text{shaded} & 1 & 1 & \text{shaded} \\ 1 & \text{shaded} & 1 & 1 & 0 & 1 & \text{shaded} & 0 \end{matrix} \\ PF_1 \quad PF_2 \end{matrix}$$

(a) (b)

그림 8. (a) 변경 가능 픽셀(음영 부분), (b) 재정렬된 영상

재정렬된 영상 PF 를 다시 블록으로 분할한 후, i 번째 블록 PF_i 에 대해 $PF_i \oplus K$ 및 $SUM((PF_i \oplus K) \otimes W)$ 를 계산한다. ($i=1,2$)

$$SUM((PF_1 \oplus K) \otimes W) = 45,$$

$$SUM((PF_2 \oplus K) \otimes W) = 17.$$

각 블록에 대해 d_i 를 계산한다.

$$d_1 \equiv [(100)_2 - 45](\text{mod } 2^{2+1}) = -41 \text{ mod } 2^3 = 7,$$

$$d_2 \equiv [(100)_2 - 17](\text{mod } 2^{2+1}) = -13 \text{ mod } 2^3 = 3.$$

첫 번째 블록의 경우 $d_1 = 7$ 이고, $S_7 = \{(2,4)\}$ 이므로, PF_1 의 (2,4)를 변경한다. 두 번째 블록의 경우 $d_2 = 3$ 이고, $S_3 = \emptyset$ 이므로 두 픽셀을 변경한다. 따라서 $S_5 = \{(3,4)\}$, $S_{-2} = \{(3,1)\}$ 이므로, 그림 9와 같이 PF_2 의 (3,4)와 (3,1)을 변경한다.

$$PF' = \begin{array}{|c|c|c|c|c|c|c|c|} \hline 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ \hline 1 & 0 & 1 & \mathbf{1} & 1 & 1 & 0 & 1 \\ \hline 0 & 1 & 0 & 1 & \mathbf{1} & 1 & 1 & \mathbf{1} \\ \hline 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ \hline \end{array}$$

PF_1' PF_2'

그림 9. 변경된 영상 PF' (이탤릭체-변경된 픽셀)

삽입 과정의 마지막으로 영상의 모든 픽셀을 재정렬하기 이전의 위치로 이동시킨다. 그림 10은 변경된 영상 PF' 의 각 픽셀을 원 위치로 복귀시킨 것이다.

$$F' = \begin{array}{|c|c|c|c|c|c|c|c|} \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & \mathbf{1} & \mathbf{1} & 0 & 0 & 0 & \mathbf{1} & 1 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ \hline \end{array}$$

F_1' F_2'

그림 10. 변경된 영상 PF' 를 원래 위치로 복귀(이탤릭체-변경된 픽셀)

비밀 데이터의 추출 시, 변경된 영상 F' 에 대하여 삽입할 때 재정렬한 위치로 모든 픽셀을 이동한 후 블록으로 분할한다. 각 블록 PF_i' 에 대해 $[SUM((PF_i' \oplus K) \otimes W) \pmod{2^{r+1}}] / 2$ 을 계산하여 삽입된 비밀 데이터를 얻을 수 있다.

$$[SUM((PF_1' \oplus K) \otimes W) \pmod{2^{r+1}}] / 2 = (44 \pmod{8}) / 2 = 4 / 2 = 2 = (10)_2$$

\therefore 첫 번째 블록에 삽입된 비트열 $b_0b_1 = 10$

$$[SUM((PF_2' \oplus K) \otimes W) \pmod{2^{r+1}}] / 2 = (20 \pmod{8}) / 2 = 4 / 2 = 2 = (10)_2$$

\therefore 두 번째 블록에 삽입된 비트열 $b_0b_1 = 10$

2. 다치 컬러 영상에서의 데이터 은닉(제안 방식 2)

CPT 방식과 TP 방식, WTL 방식 및 제안 방식1은 모두 이진 영상을 이용하여 비밀 데이터를 은닉하는 기법이였다. 2절에서는 다치 컬러 영상에 TP 방식의 삽입 과정을 적용하여, 기존의 다치 컬러 영상을 이용한 은닉 기법에 비해 삽입량과 화질 모두 우수한 방식을 제안한다.

이진 및 다치 컬러 영상에서 비밀 정보를 삽입하는 기존 방식 중 화질과 삽입량이 우수한 PWP 방식[5]은 한 픽셀과 그 이웃 픽셀과의 의존성에 따라 우선순위를 부여하는 방식이다. 높은 우선순위를 가지는 패턴의 중앙 픽셀은 삽입할 비트 값에 따라, 변경 없이 그대로 두거나, 패턴 컬러와 동

일한 값으로 변경된다.

그러나 PWP 방식은 원 영상의 중앙 픽셀과 변경할 패턴과의 컬러 값 차이를 전혀 고려하지 않음으로써 시각적으로 다소 자연스럽지 못함을 느낄 수 있으며, 영상의 한 블록에는 오직 한 비트만이 삽입 가능하다.

제안 방식2에서의 변경 가능한 픽셀은 한 픽셀의 값을 조사하여 이웃한 8개의 픽셀의 값 중 4개 이상이 그 값과 다를 경우 선택한다. 예를 들면 그림11(a)의 중앙 픽셀 값 4와 다른 값이, 이웃한 8개의 픽셀 중 3개만 있으므로 중앙 픽셀을 변경할 수 없다. 반면 그림11(b)의 패턴은 중앙 픽셀과 다른 값이, 이웃에 6개 있으므로 변경이 가능하다.

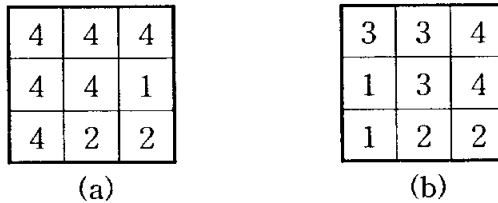


그림 11. (a) 변경 불가능한 패턴, (b) 변경 가능한 패턴

그리고 패턴의 중앙 픽셀 값을 변경시킬 경우 원 영상의 중앙 픽셀 값을 최대한 고려하여 원 영상의 픽셀 값과 근접한 값으로 변경하기 위해 픽셀 값들을 2개의 그룹으로 분류하는 방식을 사용한다.

예를 들어 다치 컬러 $G=\{0,1,2,3,4\}$ 라 가정했을 때, G 를 그룹 $G_0=\{0,2,4\}$ 과 그룹 $G_1=\{1,3\}$ 으로 분류한다. 만일, 그림 11(b)의 중앙 픽셀의 값 3($3 \in G_1$)이 변경된다고 가정하면, 변경되는 값은 G_0 의 값 중 원래의 값과 오차가 가장 작은 2 또는 4로 변경된다.

이렇게 변경된 한 비트는 가중치 테이블을 사용함으로써 여러 비트를 삽입한 효과를 가져올 수 있다. 이를 위해 그룹 G_0 에 속한 픽셀 값은 "0"으

로, G_1 에 속한 픽셀 값은 “1”로 분류하여 원 영상을 이진 영상으로 간주한 후, TP 방식의 삽입 과정을 적용한다.

우선, 원 영상 F 의 모든 픽셀의 패턴을 조사하여 변경 가능한 픽셀을 찾는다. (편의상 변경 가능한 픽셀을 ‘음영’이라 표시한다.) 그리고 영상 F 의 컬러 그룹 $G=\{0,1,2,3,4,5,\dots\}$ 를 $G_0=\{0,2,4,\dots\}$, $G_1=\{1,3,5,\dots\}$ 로 분류, 그룹 G_0 을 “0”, G_1 을 “1”로 두고 F 를 이진화된 영상으로 간주한다. 이 이진화된 영상을 GF 라 할 때, 제안 방식2의 삽입 과정은 다음과 같다.

compute $GF_i \oplus K$;

compute $SUM((GF_i \oplus K) \otimes W)$;

/*define S_w

$$S_w = \{ (j, k) \mid [([W]_{j,k} = w \wedge [GF_i \oplus K]_{j,k} = 0) \wedge (F_{j,k} = \text{'음영'})] \vee [([w]_{j,k} = 2^{r+1} - w \wedge [GF_i \oplus K]_{j,k} = 1) \wedge (F_{j,k} = \text{'음영'})] \}.$$

$$(w = 1, \dots, 2^{r+1} - 1)*/$$

$$d \equiv [(b_1 b_2 \dots b_r) - SUM((GF_i \oplus K) \otimes W)] \pmod{2^{r+1}};$$

if $d=0$ then keep GF_i intact;

else /*transform GF_i to GF_i' */

if there exists an h such that $S_{hd} \neq \emptyset$ and $S_{-(h-1)d} \neq \emptyset$

then

randomly pick an h which satisfies the above condition;

randomly pick a $(j, k) \in S_{hd}$ and complement the bit $[GF_i]_{j,k}$;

randomly pick a $(j, k) \in S_{-(h-1)d}$ and complement the bit $[GF_i]_{j,k}$;

else /*no data will be hidden*/

if $SUM((GF_i \oplus K) \otimes W) \bmod 2 = 1$ then keep GF_i intact;

else

select a (j, k) such that $[W]_{j, k}$ is odd and

its corresponding (j, k) is '음영';

complement the bit $[GF_i]_{j, k}$;

비밀 데이터의 삽입 후 이진화 영상 GF 의 모든 픽셀을 다치 컬러 영상으로 변경한 F 를 전송한다.

비밀 데이터의 추출 시, F 을 삽입할 때와 같이 컬러 값이 두 그룹으로 분류하여 이진화된 GF 로 변환한 후, $SUM((GF \oplus K) \otimes W)$ 의 결과가 짝수이면 $[SUM((GF \oplus K) \otimes W) \bmod 2^{r+1}] / 2$ 를 계산하여 삽입된 데이터를 얻을 수 있다.

삽입 과정을 예를 들어 살펴보면 다음과 같다. 원 영상(5치 컬러 영상) F , 비밀키 행렬 K , 가중치 행렬 W 가 그림 12와 같이 주어지고, 삽입할 비트 수 r 이 $3 (r \leq \lfloor \log_2(mn+1) \rfloor - 1 = 3)$, 비트열이 '1 0 1' 일 때의 삽입 과정이다.

$$F = \begin{bmatrix} 0 & 2 & 3 & 3 \\ 1 & & & 3 \\ 1 & & & 4 \\ 3 & 3 & 4 & 3 \end{bmatrix} \quad K = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \quad W = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 1 \end{bmatrix}$$

그림 12. 제안 방식2에서의 데이터 은닉 예시

원 영상 F 의 모든 픽셀의 패턴을 조사하여 변경 가능한 픽셀을 찾는다. 그림 12의 F 에서 음영으로 표시된 부분이 변경 가능한 픽셀이다.

영상 F 의 컬러 그룹을 $G=\{0,1,2,3,4\}$ 라 할 때, $G_0=\{0,2,4\}$, $G_1=\{1,3\}$ 로 분류하고, 그룹 G_0 을 “0”, G_1 을 “1”로 두면, F 를 그림 13(a)와 같이 이진화된 GF 로 표시할 수 있다. 그림 13(b)는 $GF \oplus K$ 를 계산한 결과이다.

$$GF = \begin{array}{|c|c|c|c|} \hline 0 & 0 & 1 & 1 \\ \hline 1 & 1 & 0 & 1 \\ \hline 1 & 0 & 1 & 0 \\ \hline 1 & 1 & 0 & 1 \\ \hline \end{array} \quad GF \oplus K = \begin{array}{|c|c|c|c|} \hline 1 & 0 & 1 & 1 \\ \hline 1 & 0 & 1 & 1 \\ \hline 1 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 \\ \hline \end{array}$$

(a) (b)

그림 13. (a) F 의 이진화된 영상 GF , (b) $GF \oplus K$ 의 계산 결과

$$SUM((GF \oplus K) \otimes W) = 48 ,$$

$$d \equiv [(1010)_2 - 48] \bmod 2^{r+1} = -38 \bmod 2^{3+1} = 10 .$$

$S_{10} = \{(3, 2)\}$ 이므로, GF 의 (3, 2)를 변경한다. 따라서 원 영상 F 의 (3, 2)의 값을 G_1 의 값으로 변경하며 이때 가장 오차가 적은 1 또는 3으로 변경한다. 변경된 영상 F' 는 다음과 같다.

$$F' = \begin{array}{|c|c|c|c|} \hline 0 & 2 & 3 & 3 \\ \hline 1 & 1 & 2 & 3 \\ \hline 1 & \mathbf{1} & 3 & 4 \\ \hline 3 & 3 & 4 & 3 \\ \hline \end{array}$$

비밀 데이터의 추출 시, F 을 삽입할 때와 같이 이진화된 GF 로 변환한 후, $[SUM((GF \oplus K) \otimes W)(\text{mod } 2^{r+1})] / 2$ 를 계산하여 삽입된 데이터를 얻을 수 있다.

$$[SUM((GF \oplus K) \otimes W)(\text{mod } 2^{r+1})] / 2 = (58 \text{ mod } 16) / 2 = 10 / 2 = 5 = (101)_2$$

$$\therefore \text{삽입된 비트열 } b_0 b_1 b_2 = 101$$

IV. 실험 및 결과

앞에서 살펴본 이진 영상을 이용한 데이터 은닉 방식으로는 CPT 방식, TP 방식, WTL 방식 그리고 제안 방식 1(3장 1절)이 있었다. 실험에서는 CPT 방식을 제외한 나머지 방식의 화질과 삽입량을 비교하였다.

그리고, 다치 컬러 영상을 이용한 데이터 은닉 방식인 제안 방식2(3장 2절)를 기존의 PWP 방식과 비교하여 화질 및 삽입량의 어느정도 우수한지 알아본다.

1. 이진 영상에서의 데이터 은닉 방식 비교

실험은 카툰 영상(Lucy 240×360)과 텍스트 영상(300×300)에 대해 블록의 크기를 달리 하며 기존 방식들(TP 방식, WTL 방식)과 제안 방식1로 각각 실험하였다.

카툰 영상에서 세 가지 방식으로 삽입된 비트 수를 비교하면 표 1과 같다. 표 1에서 TP 방식과 제안 방식1이 삽입량에 있어 우수함을 알 수 있다. 반면, WTL 방식은 한 블록에 변경 가능한 픽셀이 적어도 하나 이상은 있어야 하므로 블록의 크기가 작은 경우는 삽입 자체가 불가능하다. 그러므로 블록의 크기는 어느 정도 커야 하고 블록의 크기가 커짐에 따라 삽입되는 비트 수는 다른 두 방식에 비해 크게 감소한다.

상대적으로 공백이 적은 텍스트 영상의 경우 변경 가능한 픽셀의 수가 카툰 영상보다 더 많다. 표 2의 텍스트 영상에서의 삽입 비트 수를 비교해

보면 TP 방식이 데이터 삽입량이 가장 우수하고, 다음이 제안 방식1이며, WTL 방식은 다른 두 방식에 비해 삽입량이 매우 적다.

<표 1> 카툰 영상에서의 삽입 비트 수

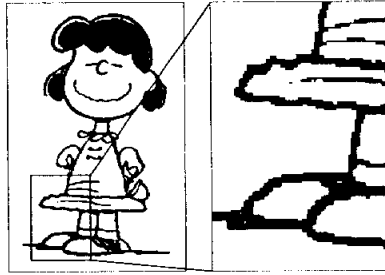
블록크기	삽입 비트 수		
	TP	WTL	제안 방식1
6×6	1704 bit	×	1450 bit
15×15	660 bit	384 bit	545 bit
30×30	296 bit	96 bit	217 bit

<표 2> 텍스트 영상에서의 삽입 비트 수

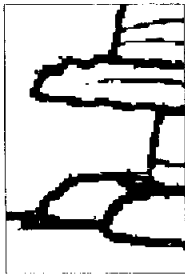
블록크기	삽입 비트 수		
	TP	WTL	제안 방식1
6×6	3136 bit	×	2022 bit
15×15	1140 bit	400 bit	910 bit
30×30	472 bit	100 bit	329 bit

그림 14과 그림 15는 각각 카툰 영상과 텍스트 영상에서 블록 크기가 15×15일 때 원 영상과 삽입 영상들을 확대하여 비교한 것이다.

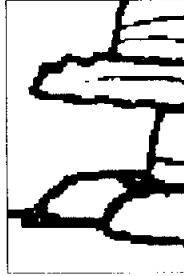
WTL 방식과 제안 방식1의 삽입 영상은 원 영상과 비교해 볼 때 별 차이를 느끼기 어렵다. 그러나 그림 14(b)와 그림15(b)의 TP 방식으로 삽입한 영상을 살펴보면 가장자리에 점이 찍혀있다. 이러한 점은 영상 전반에 걸쳐 찍혀 있으며, 이로 인해 비밀 데이터 삽입 후 영상은 시각적으로 두드러져 보인다.



(a) 원 영상



(b) TP

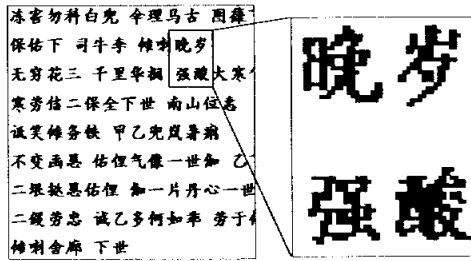


(c) WTL

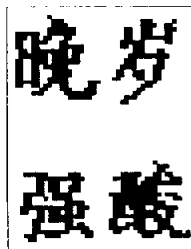


(d) 제안 방식1

그림 14. 원 영상과 삽입영상(15×15 블록)



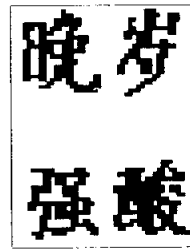
(a) 원 영상



(b) TP



(c) WTL



(d) 제안방식1

그림 15. 원 영상과 삽입영상(15×15 블록)

실험 결과를 통해 TP 방식은 삽입량은 우수하나 데이터의 삽입 후 픽셀의 변경이 가시적이며, WTL 방식은 화질은 우수하나 데이터의 삽입량이 적음을 알 수 있다. 반면, 제안 방식1은 많은 양의 비밀 데이터를 삽입하면서 시각적인 측면에 있어서도 우수함을 확인 할 수 있다.

2. 다치 컬러 영상에서의 데이터 은닉 방식 비교

이 절의 실험에서는 기존의 PWP 방식과 3장 2절의 제안 방식2를 다치 컬러 영상에 적용하여 데이터의 삽입량을 비교하고, PSNR을 이용하여 화질을 평가하였다. 표 3은 각 영상에 삽입된 데이터의 비트수를 비교한 것이다. 기존 방식에 비해 제안 방식2는 훨씬 많은 양의 데이터를 삽입할 수 있다.

<표 3> 기존 방식과 제안 방식의 삽입 비트 수 비교

영상 \ 방식	페이지(5치)	페이지(9치)	도널드(9치)
기존 방식	790 bit	733 bit	587 bit
제안 방식2	1,716 bit	2,140 bit	1,900 bit

기존 방식과 제안 방식2에 대해 각각 PSNR을 계산한 결과를 표 4와 같이 얻을 수 있다. 5치 컬러 영상에서는 기존의 방식과 제안 방식2의 화질이 거의 차이가 없으나, 9치 컬러 영상에서는 제안 방식의 화질이 매우 우수함을 알 수 있다.

<표 4> 기존 방식과 제안 방식의 화질 비교(PSNR)

영상 방식	영상		
	페이지(5치)	페이지(9치)	도날드(9치)
기존 방식	30.36 db	34.12 db	32.80 db
제안 방식2	30.57 db	35.75 db	35.89 db

그림16(a)는 174×270 크기의 5치 컬러로 구성된 원 영상이고, 그림16(b)는 기존 방식, (c)는 제안 방식2를 이용하여 데이터가 삽입된 영상이다. 제안 방식2를 통해 삽입된 영상은 많은 양의 데이터가 삽입되었음에도 화질이 우수하다.

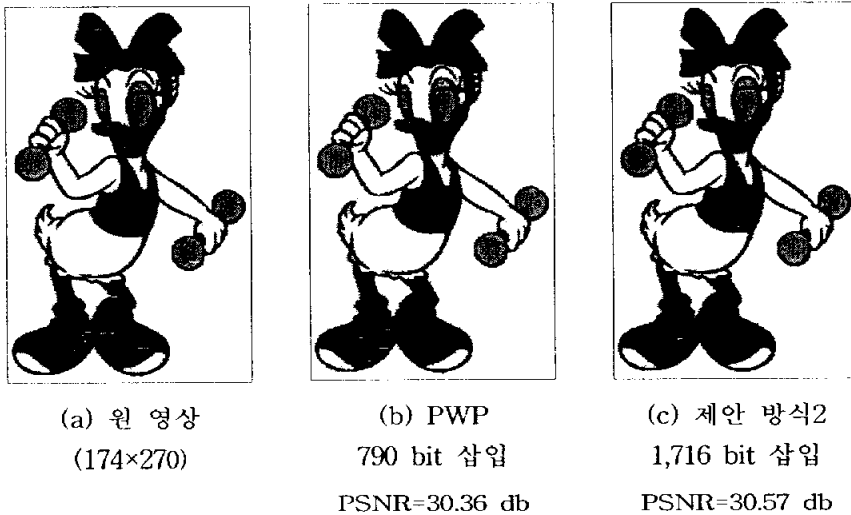


그림16. 원 영상과 삽입 영상(5치 컬러, 페이지)

그림17은 150×276 크기의 9치 컬러로 구성된 도날드 영상을 PWP 방식

과 제안 방식2로 실험한 결과이다.



(a) 원 영상
(150×276)



(b) PWP
587 bit 삽입
PSNR=32.80 db



(c) 제안 방식2
1,900 bit 삽입
PSNR=35.89 db

그림17. 원 영상과 삽입 영상(9치 컬러, 도날드)

기존의 PWP 방식은 한 블록에 한 비트를 삽입하는데 비해, 제안 방식2는 가중치 테이블을 사용함으로써 1 픽셀의 변경으로 여러 비트를 삽입할 수 있었다. 또한 제안 방식에서 변경될 픽셀은 원 영상의 픽셀과 오차가 적은 값으로 대체 되도록 하여 화질 또한 우수하다.

실험을 통한 시각적인 평가 및 수치적인 평가에서 제안 방식2는 PWP 방식과 비교해서 두 배 이상의 기밀 데이터가 삽입되었음에도 불구하고 화질이 더욱 우수함을 확인할 수 있었다.

V. 결 론

본 논문에서는 카툰 영상과 같은 이진 및 다치 컬러 영상을 이용하여 기밀 데이터를 삽입하는 스테가노그래피의 방식을 제안하였다.

이진 영상을 이용한 데이터 은닉 방식 중 기존 TP 방식은 데이터의 삽입량은 매우 우수하나 가시적인 픽셀이 변경되는 단점이 있다. 또한 WTL 방식은 화질은 우수하지만 데이터의 삽입량이 TP 방식에 비해 매우 적다. 제안 방식1에서는 각 픽셀의 패턴을 조사하여 비시각적인 픽셀을 찾은 후 비가시적인 픽셀을 변경함으로써 화질의 열화를 감소시켰으며, TP 방식의 가중치 테이블을 제안 방식에 적용하면서 WTL 방식의 픽셀 재정렬을 통해 삽입량도 우수하게 유지시킬 수 있었다.

또한 TP 방식을 다치 컬러 영상에 적용한 제안 방식2는 기존의 PWP 방식에 비해 삽입량을 2배 이상 증가시킬 수 있었다. 그리고 PWP 방식의 경우 원 영상의 중앙 픽셀과 변경할 패턴과의 컬러 값 차이를 전혀 고려하지 않음으로써 시각적으로 다소 자연스럽지 못함을 느낄 수 있었으나 제안 방식2에서는 변경될 픽셀이 원 영상의 픽셀과 오차가 적은 값으로 대체 되도록 하여 화질 또한 우수하다는 것을 알 수 있었다.

향 후 연구에서는, 이진 영상 및 다치 컬러 영상 모두에 적용하여 많은 데이터를 삽입하는 동시에 더욱 우수한 화질을 유지할 수 있는 방안이 계속 연구되어야 할 것이다.

참 고 문 헌

- [1] S. Koide, T. Ogihara, Y. Kaneda, "A Data Embedding Method for Bilevel Images Based on the Error Diffusion Method and the Mean Density Approximation Method", Technical Report of IEICE, IE95-122, p.7-14, 1996. 2
- [2] Yu-Yuan Chen, Hsiang-Kuang Pan and Yu-Chee Tseng "A Secure Data Hiding Scheme for Two-Color Images," in IEEE Sym. on Comp. and Commu. 2000.
- [3] Yu-Chee Tseng and Hsiang-Kuang Pan "Secure and Invisible data Hiding in 2-Color Images", Proc. of IEEE INFOCOM 2001.
- [4] Min Wu, Edward Tang and Bede Liu " Data Hiding in Digital Binary Image", IEEE Int. Conf. on Multimedia & Expo(ICME) 2000.
- [5] Gang Pan, Zhaohui Wu, Yunhe Pan "A Data Hiding Method for Few-Color Image", IEEE International Conference on Acoustics, Speech, and Signal Processing(ICASSP'02), vol.4, May 2002
- [6] 박영란, 이혜주, 박지환 "오차 확산법을 이용한 기밀 데이터 합성법", 한국멀티미디어학회 논문지, 제2권 2호 p.155-165, 1999. 6

감사의 글

대학 졸업을 앞두고 아르바이트 삼아 초등학교 방과 후 강사를 시작한 것이 2년 후 교육대학원 입학에 결심하게 된 계기가 되었습니다. 그 때는 일단 입학만 하면 정말 열심히 하리라 나름대로 자신감도 있었고, 각오도 단단히 했던 것 같습니다. 막상 입학 후 초등학교 일과 아르바이트 그리고, 대학원 생활까지 병행하면서 바쁘고 정신없이 하루하루를 그냥 대충 보내 버렸습니다. 그런 와중에 입학 때의 마음가짐은 온데간데없이 과연 졸업이나 할 수 있을까 고민해야만 했습니다. 다행히도 주위 여러 사람들의 도움과 지도 덕분에 이 논문을 마칠 수 있었습니다.

항상 따뜻하게 챙겨준 현화 언니, 입학할 때부터 챙겨준 민정이 언니, 너무 친근해서 초면부터 말을 놓아버린 소진이, 그리고 현호 선배, 진홍이 선배, 착하고 이쁜 후배인 지혜와 수완이 그리고 영희, 연구실 모임 때마다 전화해 주던 병만씨와 승우씨 등 연구실 선후배, 동기 모두에게 감사드립니다. 특히, 부족함이 많은 저에게 논문뿐 아니라 여러모로 큰 도움이 되어준 영란이 언니에게도 고마운 마음을 전합니다. 그리고 이제 고인이 되시고 박지환 지도 교수님... 돌이켜 생각해보니 교수님께 좋은 모습을 보여드리지 못한 것이 그저 송구스럽기만 합니다. 교수님께 고개 숙여 깊이 감사드립니다. 또한 부족한 제 논문의 심사를 맡아주신 김창수 교수님과 윤성대 교수님께 감사드립니다.

힘들 때나 기쁠 때 항상 의지가 되어준 엄마, 이 누나의 끝없는 잔소리와 짜증도 다 받아준 천사표 동생, 그리고 내 일이라면 굶은일도 마다않던 오빠에게 한없는 고마움과 애정을 느끼며 이 논문을 바칩니다.

2004년 8월 하순혜