Journal of Korea Multimedia Society Vol. 9, No. 2, February 2006(pp. 215-225)

이진영상을 위한 심층암호 기법에 관한 연구

박영란[†], 하순혜[††], 강현호[†††], 이혜주[††††], 신상욱[†††††]

요 약

흑백 두 가지의 값으로만 구성된 이진영상(만화 영상, 문서 영상 및 서명 영상 등)은 컬러 영상에 비해 적은 양의 잉여부분으로 인해 비가시적인 비밀 데이터의 삽입이 어렵다. 따라서 이진 엄폐영상을 이용한 심층암호에서는 많은 양의 비밀 데이터를 삽입하면서, 동시에 은닉영상의 비가시성을 만족시킬 수 있는 기술이 요구된다. 본 논문에서는 이에 대한 기존 연구들의 장점을 보완하여 은닉영상의 열화를 최소화 하고, 동시에 충분한 용량의 비밀 데이터를 삽입할 수 있는 방식을 제안한다. 제안 방식은 비가시적인 위치의 화소만을 변경시키며, $m \times n$ 크기의 한 블록에 대해서 $\lfloor \log_2(mn+1)-2 \rfloor$ 비트의 비밀 데이터를 숨길 수 있다.

A Study on Steganographic Method for Binary Images

Young-Ran Park[†], Soon-Hye Ha[††], Hyun-Ho Kang[†††], Hye-Joo Lee[††††], Sang-Uk Shin[†††††]

ABSTRACT

Binary images, such as cartoon character images, text images and signature images, which consist of two values with black and white have more difficulties inserting imperceptible secret data than color images. Steganography using binary cover images is not easy to satisfy requirements for both the imperceptibility of stego images and a high embedding rate of secret data at the same time. In this paper, we propose a scheme that can get both the high quality of stego images and a high embedding rate by supplementing the advantages of previous research. In addition, the insertion of the proposed method changes only existing pixels of the imperceptible position and can embed the secret data of $\lfloor \log_2(mn+1)-2 \rfloor$ bits in a block with size of $m \times n$.

Key words: Steganography(심층암호), Data Hiding(데이터 은닉), Binary Image(이진영상), Image Processing(이미지 처리)

1. 서 론

초고속 데이터 통신망의 발달로 인한 인터넷의 성장은 사용자에게 시간과 공간의 제약 없이 많은 유용한 정보의 수집과 전달이 가능하게 하였으며, 다양한 형태로 디지털화 된 멀티미디어 데이터가 여러 응용분야로 널리 확대될 수 있도록 하였다. 디지털 미디어들은 접근이 용이하며, 편집 및 복사가 가능하고, 편리하게 전송할 수 있다는 장점들을 가지고 있다. 이러한 장점들로 인해 발생할 수 있는 여러 가지 역기능 중 정보보호에 관한 문제는 우리가 배제할 수 없는 실정이다.

※ 교신저자(Corresponding Author) : 박영란, 주소 : 부산광역시 남구 대연 3동 599-1(608-737), 전화 : 051)620-6493, FAX : 051)620-6390, E-mail : young@shannon.pknu.ac.kr
접수일 : 2005년 3월 4일, 완료일 : 2005년 10월 5일
[†] 준회원, 부경대학교 정보보호학과
[††] 준회원, 부경대학교 전산교육학과
(E-mail : fbhome@empal.com)
[†††] 준회원, 일본 전기통신대학(電気通信大学) 정보시스템학연구과
(E-mail : kang@ice.uec.ac.jp)
[††††] 준회원, 경성대학교 컴퓨터과학과
(E-mail : iamhj@paran.com)
[†††††] 정회원, 부경대학교 전자컴퓨터정보통신공학부
(E-mail : sushin@pknu.ac.kr)

정보보호를 위한 방법의 일환으로 정보은닉(information hiding) 기술에 관한 연구가 널리 수행되고 있으며, 다양한 방법의 메커니즘들이 개발되어지고 있다. 정보은닉 기술 중 심층암호(steganography)는 디지털화 된 콘텐츠에 비밀 정보를 비가시적으로 숨겨 송신자 및 수신자간의 비밀 통신을 할 수 있는 기법이다. 이 기술은 오랜 역사를 가지고 있으며, 그동안 다양한 형태로 많은 연구들이 진행되어 왔다[1-3].

영상 심층암호(image steganography)는 송신자가 일반적인 엄폐영상(cover image)에 비밀 메시지를 은닉시켜 은닉영상(stego image)을 생성한다. 생성된 은닉영상을 수신자에게 보내면, 수신자는 은닉영상에서 비밀 메시지를 추출할 수 있다. 영상 심층암호에서 주로 이용되는 영상의 종류는 색의 구성에 따라 자연 영상, 컬러 영상, 그레이 영상, 이진영상 등으로 구분할 수 있다. 영상 심층암호 응용에서는 다수의 컬러 표현이 가능한 컬러 영상 및 그레이 영상을 주로 이용되고 있다[4-5]. 그러나 일상생활 및 인터넷상에 이용되고 있는 영상들 중에서 그 표현 색상 값이 흑과 백의 두 가지로 구성된 문서 영상(text image), 만화 영상(cartoon image), 스캔된 디지털 영상(scanned digital image), 팩스 영상(facsimile image) 등의 이진영상(binary image)들의 활용 또한 컬러 및 그레이 영상 못지않게 그 이용도가 높다고 판단되었으며 꾸준한 연구가 진행되어 왔다[6-12]. 그러나 두 가지 값만으로 구성된 이진영상은 그 특성상 데이터를 비시각적으로 은닉시키는 것이 쉽지 않다.

본 논문에서는 만화 또는 문서 영상과 같은 이진영상에 비밀 데이터를 비가시적으로 숨기는 방법을 제안한다. 제안 방식은 기존 방식들의 장점을 서로 보완 및 개선하여 데이터 삽입용량과 시각적인 측면에서 우수한 결과를 얻을 수 있었다.

논문의 구성은 2장에서는 기존의 관련 연구들의 특징과 데이터 삽입 과정을 기술하고, 3장에서는 기존 방식들의 문제점을 보완한 제안 방식을 소개한다. 4장에서는 실험을 통하여 기존 방식과 제안 방식을 비교 분석하며, 마지막 5장에서는 결론을 맺는다.

2. 관련 연구

2.1 가중치 행렬을 이용한 방식

데이터 은닉 기법 중 Chen 방식[9]은 가중치 행렬을 이용하여 삽입 처리로 인해 변경되는 화소의 수는 감소시키면서 삽입되는 비밀 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.

[비밀 데이터 은닉 과정]

엄폐영상을 F라 두고, F를 $m \times n$ 크기의 블록으로 나눈다. 한 블록에 삽입할 수 있는 데이터의 양은 r 비트($r \le \lfloor \log_2(mn+1) \rfloor$)이며, 송신자와 수신자간 공유하는 비밀 키는 다음과 같이 K와 W이다.

- K : 비밀 키는 $m \times n$ 크기의 랜덤 값 0과 1로 구성된 이진 행렬이다.
- W: $m \times n$크기의 가중치 행렬로, 구성 값은 식(1)에서처럼 $1 \sim 2^r - 1$ 의 정수이며, 각 위치에 할당되는 구성 값은 사용자가 임의로 선택한다.

$$\{[W]_{i,j} \mid i = 1...m, j = 1...n\} = \{1, 2, ..., 2^r - 1\} \quad (1)$$

엄폐영상 F의 i번째 블록을 F_i라 했을 때, 식(2)와 같이 해당 블록과 비밀 키 K와 각각 XOR 연산을 수행한다. 그 결과를 가중치 행렬 W와 대응되는 위치의 값으로 각각 곱해서 합을 계산한다.

$$SUM((F_i \oplus K) \otimes W) \quad (2)$$

삽입 비트열 $(b_1 b_2 ... b_r)$과 식(2)의 계산 결과를 토대로 차분 d를 식(3)을 이용하여 구한다. 식(3)의 계산에서, 만약 $d = 0$이라면 F_i는 변경하지 않는다. 그렇지 않으면 d를 0으로 만들기 위해 F_i 내의 어떤 화소의 값을 변경한다. 기호 $\otimes$ 은 행렬 P와 Q가 있다고 가정했을 때, $P \otimes Q$는 $P_{i,j} \times Q_{i,j}$를 의미한다.

$$d \equiv (b_1 b_2 ... b_r)_2 - SUM((F_i \oplus K) \otimes W) \pmod{2^r} \quad (3)$$

d를 0으로 만들 비트를 선택하기 위해 행렬 $F_i \oplus K$로부터 각 $w = 1, \cdots, 2^r - 1$에 대해 식(4)와 같이 계산한다. 식(4)에서, $S_d \neq \varnothing$ 이면, $(j,k) \in S_d$인 $F_{j,k}$를 변경한다. $S_d = \varnothing$이면, $S_{hd} \neq \varnothing$이면서 동시에 $S_{-(h-1)d} \neq \varnothing$를 만족하는 $h \in \{0, 1, \cdots, 2^r - 1\}$를 랜덤하게 선택하고, 두 집합에서 각각 한 화소를 선택한다. 즉, 블록 내에 두개의 화소 값을 변경하여 비밀 데이터를 삽입한다. 여기서 w는 가중치 행렬 W의 구성 값들이다.

$$S_w = \{(j,k) | [w]_{j,k} = w \wedge [F_i \oplus K]_{j,k} = 0) \vee ([w]_{j,k} = 2^r - w \wedge [F_i \oplus K]_{j,k} = 1)\} \quad (4)$$

예를 들어, (그림 1)의 (a), (b), (c)와 같이 엄폐영상 F, 비밀 키 행렬 K, 가중치 행렬 W가 주어지고, 삽입할 비밀 데이터 $b=1010$, 그리고 $r=4$ 라고 가정했을 때, 삽입 결과인 은닉영상이 (그림 1)의 (f)이다.

(그림 1)의 예에 대해서 계산 순서를 살펴보면, 우선 $(F \oplus K)$의 계산 결과는 (그림 1)의 (d)가 되고, (그림 1)의 (d)와 대응되는 위치의 가중치 W를 각각 곱하면 $SUM((F \oplus K) \otimes W) = 52$가 된다. 이것을 식(3)에 적용하여 d를 계산하면 $d \equiv (1010)_2 - 52 \bmod 2^4 = 10 - 52 \bmod 16 = 6$이다. 따라서 식(4)의 조건을 만족하는 $S_0 = \{(3,2)\}$가 되므로, F의 (3,2)의 값을 역으로 변경하면 은닉영상 F'이 (그림 1)의 (f)와 같이 생성된다.

[비밀 데이터의 추출 과정]

은닉영상 F'에 대하여 $SUM((F' \oplus K) \otimes W) (\bmod 2^r)$를 계산 하여 비밀 데이터를 획득할 수 있다. (그림 1)의 삽입 과정에서 얻은 은닉영상에 대해 식(5)를 적용하여 정확한 비밀 데이터 $b_0 b_1 b_2 b_3 = 1010$을 추출할 수 있다.

$$SUM((F' \oplus K) \otimes W) (\bmod 2^r) = 10 = (1010)_2 \quad (5)$$

Chen 방식은 변경된 새로운 화소의 값이 이웃한 화소의 값과 동일하다면, 변화가 눈에 잘 띄지 않지만, 위의 예처럼 변경된 화소 값이 1이고, 이웃한 8개의 화소 값이 모두 0이라면 데이터 삽입 후 변경된 부분을 쉽게 확이 가능하다. 따라서 서로 다른 값을 가지는 화소간의 거리를 계산하는 과정을 추가하여 은닉영상의 화질을 개선한 방식이 Tseng 방식[10]이다.

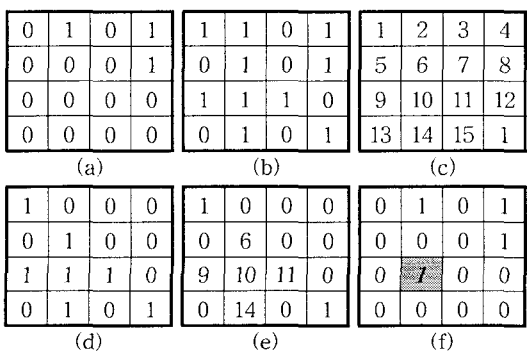


그림 1. Chen 방식의 삽입 예 : (a) F, (b) K, (c) W, (d) $F \oplus K$, (e) $(F \oplus K) \otimes W$, (f) F'

Tseng 방식에서는 한 블록 내에 삽입할 수 있는 비트 수 r ($r \le \lfloor \log_2(mn+1) - 1 \rfloor$)은 Chen 방식에 비해 1비트가 감소한다. 가중치 행렬의 구성하는 정수의 값의 최대 범위도 식(6)처럼 변경된다. 그러므로 Chen의 방식의 식(1)이 식(6)처럼 바뀌고, 식(3)은 식(7)과 같이 변경된다. 그리고 가중치 행렬 W를 구성할 때 W내의 각 2×2 서브 블록에는 적어도 하나의 홀수가 존재하도록 구성하는데, 그 이유는 식(7)에서 보면, 삽입할 비밀 비트의 마지막에 항상 '0'을 붙여서 계산이 되므로 d는 항상 짝수가 된다. 즉 정상적으로 비밀 데이터가 삽입된 블록에 대해서는 식(7)로 계산했을 때, d의 값이 짝수가 되어야 하고, 삽입되지 않은 블록에 대해서는 d의 값을 홀수가 되도록 처리를 해 주어야 된다. 그러나 식(7)에 의해서 계산했을 때, 그 결과가 홀수일 경우는 무관하지만, 만약 짝수의 값이 계산된다면, 삽입하지도 않은 블록이 삽입된 블록으로 처리되게 된다. 이러한 경우를 방지하기 위해 가중치 행렬 W에서 홀수 값을 가진 위치와 대응되는 엄폐영상의 값을 강제로 변경을 해야 된다. 그래서 좀 더 비가시적인 위치를 변경하기 위해 W의 서브 블록 내에 적어도 하나의 홀수가 존재하도록 구성시킨다.

$$\{[W]_{i,j} \mid i = 1...m, j = 1...n\} = \{1,2,...,2^{r+1} - 1\} \quad (6)$$

$$d \equiv (b_1 b_2 ... b_r 0) - SUM((F_i \oplus K) \otimes W) \ (\bmod 2^{r+1}) \quad (7)$$

한편, 최소거리 행렬 $distF$의 계산은 식(8)에 의해 계산하여 행렬을 구성한다.

$$[distF]_{i,j} = \min_{\forall x,y} \sqrt{|i-x|^2 + |j-y|^2} \ | [F]_{i,j} \neq [F]_{x,y} \quad (8)$$

삽입을 할 때 최소거리 행렬에 값이 $\sqrt{2}$ 이하인 위치의 값을 변경해야 하므로 Chen 방식에서 식(4)는 식(9)처럼 변경이 된다.

$$S_w = \{(j,k) | [([w]_{j,k} = w \wedge [F_i \oplus K]_{j,k} = 0) \wedge (dist[F]_{j,k} \le \sqrt{2})] \vee [([w]_{j,k} = 2^{r+1} - w \wedge [F_i \oplus K]_{j,k} = 1) \wedge (dist[F]_{j,k} \le \sqrt{2})]\} \quad (9)$$

앞에서 살펴본 (그림 1)의 엄폐영상 F에서 서로 다른 값을 가지는 화소 사이의 최소 거리를 계산한 행렬 $distF$ (그림 2)의 (b)와 같다.

F

0	1	0	1
0	0	0	1
0	0	0	0
0	0	0	0

(a)

$distF$

1	1	1	1
$\sqrt{2}$	1	1	1
$\sqrt{10}$	$\sqrt{5}$	$\sqrt{2}$	1
$\sqrt{13}$	$\sqrt{8}$	$\sqrt{5}$	2

(b)

그림 2. 변경 가능한 화소를 선택하기 위한 Tseng 방식의 최소거리 계산의 예 : (a) 엄폐영상의 화소 값, (b) 엄폐영상에 대한 최소거리 행렬

최소거리 행렬의 값이 $\sqrt{2}$ 보다 큰 화소들은 변경하지 않으므로 은닉영상의 화질이 개선될 수 있다. 즉, (그림 2)의 (b)에 $distF$의 (3,2)의 값이 $\sqrt{5}$ 가 되면, 이것은 $\sqrt{2}$ 보다 큰 값이기 때문에 변경 하지 못한다. 따라서 이럴 경우 d와 같은 값이 되도록 하기 위해 2개의 비트를 변경해야 한다. $h=2$일 때, $S_{12}=\{(3,4)\}$, $S_{-6}=\{(2,2)\}$이고, 두 화소의 해당 $distF$의 값도 둘 다 $\sqrt{2}$ 를 넘지 않으므로 F의 (3,4)와 (2,2) 두 화소를 변경하여 화질을 개선한다. 블록의 모든 화소 값이 1 또는 0인 경우(블록 전체가 흑 또는 백인 경우)에는 그 블록은 삽입 처리를 하지 않는다. 해당 블록이 변경 조건에 맞는 화소가 존재하지 않을 경우에는 삽입 처리가 된 블록과 그렇지 않는 블록을 구별하기 위해 $SUM((F_i'\oplus K)\otimes W)$의 값이 홀수가 되도록 F_i의 값을 수정하는 작업이 필요하다.

삽입된 비밀 데이터의 추출은 우선 은닉영상의 해당 블록의 모든 화소 값이 1 또는 0인 경우와 $SUM((F_i'\oplus K)\otimes W)$가 홀수인 경우는 비밀 데이터가 삽입되지 않은 블록이므로 추출 과정에서 제외시키고, $SUM((F_i'\oplus K)\otimes W)$가 짝수인 블록에 대해서만 아래의 식(10)처럼 계산하여 삽입된 비밀 데이터를 추출하여 그 내용을 확인한다.

$$[SUM((F_i'\oplus K)\otimes W)(\mathrm{mod}\ 2^{r+1})]/2 \qquad (10)$$

한편, Tseng 방식보다 삽입용량은 작지만 비가시성을 높이기 위해 Tseng 방법을 수정한 방법이 Chang 등[8]에 의해서 제안되었다. 즉, Tseng 방법과 Chang 방법[8]과 다른 점은 Chang 방식은 블록 당 삽입용량이 Tseng 방식보다 1비트 작게 삽입되지만, 지정한 조건에 만족하지 않아 삽입하지 못하는 블록에 대한 낭비를 줄이기 위해, 원 영상에서 각 블록 F의 화소 값들을 역으로 (0은 1로, 1은 0으로 변환) 변환한 IF에 대해서도 Tseng 알고리즘을 수행하기 때문에 어느 정도의 삽입용량을 유지하게 된다. 또한, 비가시성이 Tseng의 방법보다 우수한 이유는 $SUM((F_i\oplus K)\otimes W)$을 물론 $SUM((IF_i\oplus K)\otimes W)$을 추가로 계산한 다음, 해당 블록에 대해 정상적인 Tseng 삽입 처리(블록의 원 화소 값을 이용)와 역으로 변환해서 처리한 것 중 좀 더 화질을 영향을 미치지 않는 쪽을 사용한다. 즉, 데이터의 삽입을 위해 블록내의 화소를 변경해야한다면, 정상적인 블록과 역으로 취한 블록 중 변경될 화소의 거리계산의 결과 값을 비교하여 더 작은 쪽을 선택하므로 Tseng 방법보다 비가시성이 높아진다. 그러나 Chang 알고리즘은 Tseng 방식과 비교했을 때 각 블록에 대해 이중(정상/역 변환)으로 계산한 다음 둘 중 하나를 선택하기 때문에 수행시간이 2배 이상 길어진다는 것이 단점이다. 물론, 수행시간을 희생하여 비가시성을 만족할 수 있었기 때문에 알고리즘의 유효성은 충분하다고 생각되지만, Chang의 방식은 추출이 정확하게 되지 않는다. 왜냐하면, 만약 비밀 데이터를 F_i에 삽입이 이루어졌다면 $SUM((F_i'\oplus K)\otimes W)$ 결과는 짝수가 되고, $SUM((IF_i'\oplus K)\otimes W)$ 결과 값이 홀수가 된다. 이와 반대로, IF_i에 데이터가 삽입되었다면 $SUM((F_i'\oplus K)\otimes W)$ 결과는 홀수, $SUM((IF_i'\oplus K)\otimes W)$ 결과는 짝수가 된다. 그러나 문제는 비밀 데이터 삽입으로 인해 F_i와 IF_i에서 어떤 화소를 변경해야 할 경우, 조건에 만족하는 화소가 양쪽 모두 존재하지 않을 경우에는 Chang 논문에서는 $SUM((F_i\oplus K)\otimes W)$ 결과는 홀수가 되도록, $SUM((IF_i\oplus K)\otimes W)$ 결과는 짝수가 되도록 강제로 변경시킨다. 따라서 수신자가 추출을 위해 $SUM((F_i'\oplus K)\otimes W)$을 계산했을 때, 그 결과가 홀수가 나오고, $SUM((IF_i'\oplus K)\otimes W)$의 계산은 짝수가 나왔다면, 삽입 처리에서 제외된 블록인지, IF_i에 데이터가 삽입되었는지를 구분을 할 수가 없다. 물론 논문에서는 추출에 대한 구체적인 설명이 없으므로 추출에서 어떤 처리로 정확하게 추출할 수 있는 방법이 존재하는지는 알 수가 없다. 또한 $w=1,2,\ldots,2^{r+2}-1$이면, S_w'의 구성에서 $[W]_{j,k}=2^{r+1}-w$로 정의하는지 의문이다. 결론적으로 Chang 논문은 Tseng 방법을 개선했다고 하나, 수식적으로 명확하지가 않고, 정확한 추출이 불가능할 것으로 추정된다.

2.2 화소 재편성(shuffle)을 이용한 방식

이진영상을 이용한 비밀 데이터를 삽입 방식 중 Wu 방식[11]은 변경 가능한 화소들을 계산하여 찾은 후, 이를 랜덤 재편성(shuffle)을 하여 보안뿐만 아니라 비밀 데이터의 삽입용량도 증가시킬 수 있는 방법이다. 이진 엄폐영상에서 비밀 데이터 삽입을 위해 비가시적인 위치의 화소 값을 변경한다. 이때, (그림 3)의 (c)처럼 하나의 블록 내에 비가시적인 위치가 2개 이상 존재할 경우, 변경 가능한 화소들이 서로 재편성함으로써 (그림 3)의 (d)처럼 변경 가능한 화소들이 각 블록에 골고루 분포되어 낭비되는 블록이 발생하지 않도록 하는 방식이다.

(그림 3)의 (b)에서 점으로 표시된 부분은 변경 가능한 화소이며, (그림 3)의 (c)는 (그림 3)의 (b)를 블록으로 분할한 것이다. 영상의 모든 화소를 랜덤 재편성을 통해 (그림 3)의 (d)에서처럼 변경 가능한 화소가 블록마다 적어도 하나 이상 분포되어야 모든 블록에서의 데이터 삽입이 가능해진다.

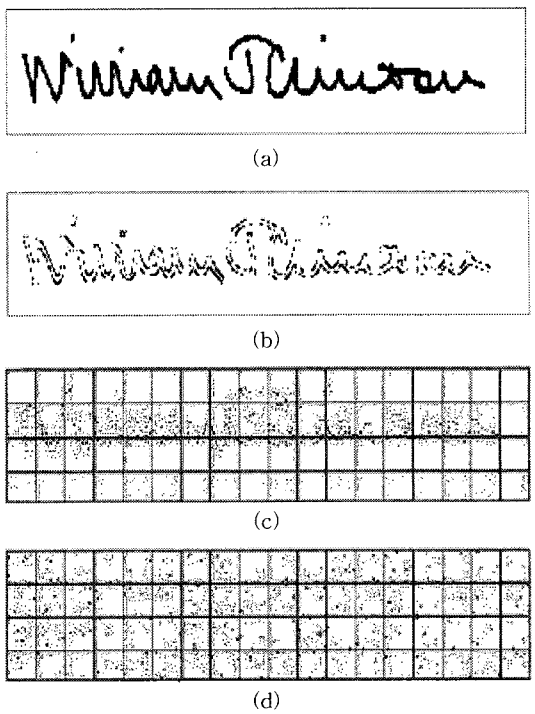


그림 3. Wu 방식의 재편성 과정 : (a) 이진 엄폐영상, (b) 변경 가능한 위치의 화소들, (c) 블록 분할, (d) 화소 재편성 후 변경 가능한 화소들

3. 제안 방식

가중치 테이블을 사용하여 많은 양의 데이터를 삽입하는 Tseng 방식은 화질을 고려하여 거리 행렬 $distF$를 추가하였지만 여전히 비밀 메시지 삽입 후 화질의 열화가 발생한다. 예를 들면, 변경된 새로운 화소 값과 동일한 값이 하나라도 이웃해 있으면 변경이 가능하므로 (그림 4)의 (3,2)는 변경 조건에 만족하는 화소이지만 실제로 변경하게 되면 윤곽부분의 가장자리에 잡음처럼 열화가 발생되어 제3자가 쉽게 변경을 확인 할 수 있다. 게다가, 변경 가능한 화소들이 주로 하나의 블록 내에 편중되어 있으므로, 블록 내의 두 화소가 한꺼번에 변경될 경우 은닉영상은 비가시성을 만족하지 못하게 된다. 또한, $distF$를 계산하는데 소요되는 시간이 길다는 단점을 가지고 있다.

한편, Wu 방식은 변경 화소 선택을 패턴의 우선순위로 결정하는데, 변경될 화소의 선택은 가장 비가시적인 화소부터 선택되므로 데이터의 삽입 후 영상의 변화가 눈에 잘 띄지 않는다. 그러나 한 블록에 최소한 하나 이상의 변경 가능한 화소가 있어야 하므로 블록의 크기는 충분히 커야 한다. 비록 랜덤 재편성(shuffle)을 통해 모든 블록에 데이터를 삽입하는 것이 가능해 졌으나 한 블록에는 오직 1비트만이 삽입 가능하므로 Tseng 방식과 비교하면 Wu 방식은 삽입용량이 매우 적다.

제안 방식에서는 영상 심층암호의 기본 조건인 삽입용량과 비가시성을 충분히 만족할 수 있는 방법을 제시한다. 제안 방식은 Tseng 방식의 가중치 테이블과 Wu 방식의 변경 가능 화소의 랜덤 재편성의 개념을 결합시켜 기존 두 방식의 단점을 보완한 효율적인 영상 심층암호 기법이다.

또한, 제안 방식에서의 변경 가능한 화소는 하나의 화소와 이웃한 8개의 화소와의 관계를 조사하여 화소의 값이 변경되더라도 비가시성을 만족할 수 있도록 Pan 방식[12]을 적용하여 우선순위를 정한 후, 그 순위에 따라 변경될 화소를 선택한다. 즉, 비밀 데이터를 삽입시킬 위치의 화소가 시각적으로 쉽게 확인할 수 있는 위치인 경우에는 해당 화소는 우선순위에서 제외된다. 예를 들어, (그림 5)에서처럼 (a) 및 (b)와 같은 패턴을 가진 두 블록에 대해 가운데 화소를 변경시킨다고 가정하면 (그림 5)의 (a)보다 (b)의 변경이 시각적으로 더 민감하므로, 화소의 변경 여부를

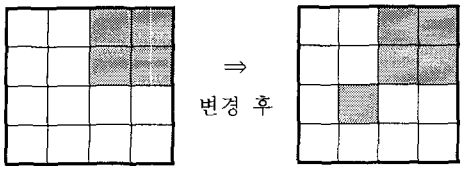


그림 4. 가시적으로 화소가 변경되는 경우

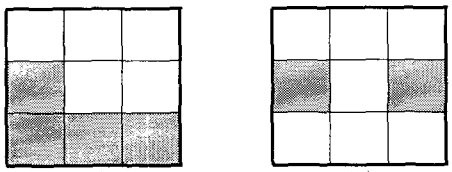


그림 5. 다른 순위를 가지는 3×3 블록의 두 패턴

쉽게 알 수 있다. 그러므로 (그림 5)의 (a)의 패턴이 (b)보다 더 높은 우선순위를 가지게 된다. 특별히, Pan 방식을 사용한 이유는 블록 단위의 패턴을 비교하여 비가시적인 화소를 검출하기 때문에 알고리즘이 간단하므로 처리시간을 단축시킬 수 있다.

한편, 제안 방식은 높은 순위를 가진 패턴의 화소를 선택함으로써 Tseng 방식의 문제점인 은닉영상의 화질의 열화를 줄일 수 있지만, 패턴 조사를 통해 선택되는 화소의 수는 Tseng 방식의 변경 가능한 화소에 비해 그 수가 1/4 정도로 감소되어 삽입이 불가능한 블록이 증가하고, 데이터의 삽입용량도 현저하게 감소하게 된다. 그러므로 제안 방식에서는 가능한 모든 블록에 비밀 데이터의 삽입이 가능하도록, 하나의 블록에 삽입되는 데이터의 양은 $\lfloor \log_2(mn+1)-2 \rfloor$ 비트로 Tseng 방식보다 1 비트 감소시키고, 모든 화소들을 랜덤 치환(random permutation)을 통해 각 블록에 변경 가능한 화소들이 골고루 분포되도록 한다. 따라서 한 블록 당 삽입하는 데이터의 양은 Tseng 방식보다 적어지지만 삽입이 가능한 블록의 수는 증가되므로 Tseng 방식의 삽입용량 만큼을 은닉시킬 수 있다.

제안 방식의 구체적인 삽입 과정을 살펴보면, 먼저 엄폐영상 F의 모든 화소에 대해 패턴의 우선순위를 조사하여 변경 가능한 화소를 선택한다. 그리고 블록 전체가 모두 흑 또는 백 화소로 구성된 블록을 제외한 영상의 모든 화소를 랜덤치환을 하며, 랜덤치환된 영상을 PF라 했을 때, 아래의 단계를 통해 은닉영상 F'가 생성된다.

[1단계] 엄폐영상의 PF의 i번째 블록인 PF_i와 이진행렬 형태인 비밀 키 K를 각각 대응되는 위치의 값과 XOR 연산을 수행한 후 가중치 행렬 W를 식 (11)과 같이 곱한다.

$$SUM((PF_i \oplus K) \otimes W) \tag{11}$$

[2단계] 삽입하고자 하는 비밀 데이터 r 비트에서 마지막 0을 추가한 $r+1$ 비트열을 십진수로 변경한다. 이때 십진수로 변경한 값은 마지막 비트에 0을 연접한 값이기 때문에 항상 짝수이다. 또한, [1단계]에서 계산된 결과 값에서 2^{r+1}을 나눈 나머지 값과의 차분 d를 식(12)과 같이 계산한다.

$$d \equiv (b_1 b_2 \cdots b_r 0) - SUM((PF_i \oplus K) \otimes W) \pmod{2^{r+1}} \tag{12}$$

[3단계] d의 값을 이용하여 삽입 처리를 수행한다. 즉, 차분 d가 0이면 PF_i 블록의 화소 값을 변경하지 않고 데이터를 은닉시키게 된다. 따라서 PF_i와 PF_i'의 값은 동일하다. 그러나 차분 d의 값이 0이 아닌 경우에는 아래의 순서(①~③)를 수행하여 데이터를 은닉시킨다.

① 우선, 식(13)과 같이 S_w를 미리 정의해 둔다.

$$\begin{aligned} S_w = \{(j,k) | [([W]_{j,k=w} \wedge [PF_i \oplus K]_{j,k} = 0) \\ \wedge (F_{j,k} = \text{'변경가능 화소'})] \\ \vee [([W]_{j,k} = 2^{r+1} - w \wedge [PF_i \oplus K]_{j,k} = 1) \\ \wedge (F_{j,k} = \text{'변경가능화소'})]\} \end{aligned} \tag{13}$$

여기서, $w = 1, \cdots, 2^{r+1}-1$이며, '변경가능 화소'라는 것은 거리 계산에서 패턴 우선순위에 의해 선택된 화소를 의미한다.

② $S_d \neq \varnothing$이면, 위의 ①에서 정의한 S가 $(j,k) \in S_d$인 $[PF_i]_{j,k}$의 값만 역(0→1, 1→0)으로 변경하고, $S_d = \varnothing$이면, $S_{h,d} \neq \varnothing \wedge S_{-(h-1)d} \neq \varnothing$인 $h \in 0, 1, \ldots, 2^r - 1$가 한 개 이상 존재한다면 h를 임의로 선택하여 위의 ①에서 정의한 S가 $(j,k) \in S_{h,d}$에 만족하는 $[PF_i]_{j,k}$ 화소의 값을 역으로 변경시키고 또한, $(j,k) \in S_{-(h-1)d}$인 $[PF_i]_{j,k}$ 화소의 값을 역으로 변경시킨다. 즉, $S_d \neq \varnothing$이면 하나의 화소만 변경하여 비밀 데이터를 은닉시키고, $S_d = \varnothing$이면 두 개의 화소를 변경하여 데이터를 은닉시킨다.

③ 차분 d가 정의한 S에 부합하지 못하여 삽입처리를 수행하지 못할 경우는 해당 i번째 블록의

$SUM((PF_i \oplus K) \otimes W)$ 계산 결과 값이 홀수이면, PF_i를 변경하지 않고 PF_i'를 생성($PF_i = PF_i'$)하고, 짝수이면 가중치 행렬의 $[W]_{j,k}$가 홀수이면서, '변경가능 화소'인 (j,k)의 화소를 선택 $[PF_i]_{j,k}$의 화소를 역으로 변경한다.

엄폐영상 F에서 블록의 모든 화소가 흑이거나 백인 블록을 제외시킨 모든 화소를 랜덤 치환을 수행하여 생성된 영상 PF의 모든 블록에 대하여 [1단계]에서 [3단계]까지를 반복 수행을 하게 되면 비밀 데이터가 삽입된 영상 PF'가 생성될 것이며, 이것을 원래의 화소 위치로 이동시키기 위해 역으로 랜덤 치환을 시키면 은닉영상 F'가 생성된다.

비밀 데이터의 추출은 변경된 영상 F'에 대하여 삽입할 때 랜덤 치환한 위치로 모든 화소를 이동한 영상 PF'후 블록으로 분할한다. i번째 블록 PF_i'에 대해 $SUM((PF_i' \oplus K) \otimes W)$가 짝수이면, $[SUM((PF_i' \oplus K) \otimes W) \pmod{2^{r+1}}]/2$을 계산하여 삽입된 비밀 데이터를 추출할 수 있다.

삽입 및 추출 과정을 예를 들어 설명한다. 먼저, 엄폐영상 F의 4×4 크기의 첫 번째 블록 F_1, 두 번째 블록 F_2가 (그림 6)의 (a)와 같이 주어지고, 비밀 키 행렬 K가 (그림 6)의 (b)와 같이 주어졌다고 가정하면, 블록 당 삽입할 수 있는 비트 수는 2비트 ($r \le \lfloor \log_2(mn+1) - 2 \rfloor = 2$)이다. 따라서 가중치 행렬 W는 (그림 6)의 (c)처럼 구성될 수 있으며, 여기서 삽입할 비밀 데이터가 '1010'이라 할 때, 제안 방식의 삽입 과정을 기술하면 다음과 같다.

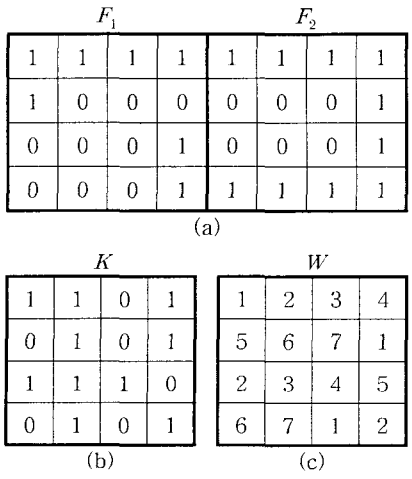


그림 6. 엄폐영상, 비밀 키 행렬 및 가중치 행렬 : (a) 엄폐영상의 두 블록, (b) 비밀 키 행렬, (c) 가중치 행렬

먼저, 엄폐영상 F의 모든 화소에 대해 패턴의 우선순위를 조사하여 변경 가능한 화소를 (그림 7)의 (a)에 음영 부분으로 표시하였다. (그림 7)의 (b)는 영상의 모든 화소들을 랜덤하게 치환한 것으로 변경 가능한 화소가 각 블록에 골고루 분포되었음을 알 수 있다.

랜덤 치환된 영상 PF를 다시 블록으로 분할한 후, i번째 블록 PF_i에 대해 $PF_i \oplus K$ 및 $SUM(PF_i \oplus K) \otimes W)$을 계산한다. (그림 7)의 예에서는 $i = 1, 2$ 이다. 두 블록에 대해 비밀 키 K와 가중치 행렬 W를 이용하여 계산한 각각의 합은 $SUM(PF_1 \oplus K) \otimes W)$의 계산 결과는 45가 되고, $SUM(PF_2 \oplus K) \otimes W)$은 17이 된다. 각각의 블록에 대해 d_i를 계산하면, $d_1 \equiv (100)_2 - [45 \pmod{2^{2+1}}] = -1$와 $d_2 \equiv (100)_2 - [17 \pmod{2^{2+1}}] = 3$이 된다. 첫 번째 블록의 경우 $d_1 = -1$이므로, PF_1의 (2, 4)를 역으로 변경하면 1을 뺀 결과가 되어 (그림 8)의 PF'_1 결과를 얻게 된다. 두 번째 블록의 경우 $d_2 = 3$이지만, 하나의 화소 변경으로 만족하는 결과를 얻지 못한다. 따라서 $PF_2 \oplus K$의 결과와 가중치 행렬 W를 이용하여 PF_2의 (3, 4)의 화소 값을 역으로 변경하면 5를 더하는 것이고 (3, 1)의 화소를 역으로 변경하면 2를 빼는 것이기 때문에 결과적으로 3을 더한 결과가 될 수 있다.

마지막으로 영상의 모든 화소를 랜덤 치환하기 이전의 위치로 이동시킨다. [그림 9]는 변경된 영상 PF'의 각 화소를 원 위치로 복귀시킨 결과이다.

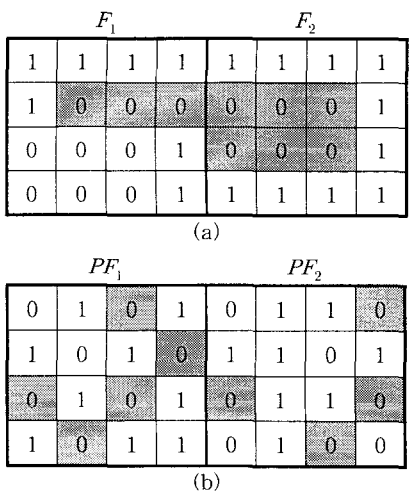


그림 7. 엄폐영상의 원 블록과 랜덤 치환을 수행한 블록 : (a) 변경 가능 화소(음영 부분), (b) 랜덤 치환된 영상

PF_1'				PF_2'			
0	1	0	1	0	1	1	0
1	0	1	1	1	1	0	1
0	1	0	1	1	1	1	1
1	0	1	1	0	1	0	0

그림 8. 변경된 영상 PF'(이탤릭체-변경된 화소)

F_1'				F_2'			
1	1	1	1	1	1	1	1
1	1	1	0	0	0	1	1
0	0	0	1	0	0	0	1
0	0	0	1	1	1	1	1

그림 9. 변경된 영상 PF'를 원래 위치로 복귀 (이탤릭체-변경된 화소)

비밀 데이터의 추출은 변경된 영상 F'에 대하여 삽입할 때 랜덤 치환한 위치로 모든 화소를 이동한 후 블록으로 분할한다. 각 블록 PF_i'에 대해 $[SUM(PF_i' \oplus K) \otimes W) \pmod{2^{r+1}}]/2$ 를 계산하여 그 결과가 짝수이면 비밀 메시지가 삽입된 블록이므로 데이터를 추출하고, 홀수이면 추출하지 않는다. 앞에서 기술한 삽입 예에 대한 추출 과정은 살펴보면, 첫 번째 블록과 두 번째 블록에 삽입된 비트열은

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

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

각각의 숨겨진 비밀 데이터를 추출할 수 있다.

4. 실험 및 결과

기존의 방식들과 제안 방식의 성능을 평가하기 위해 실험을 해 보았다. 실험에 사용된 영상은 흑/백의 두 값으로만 구성된 이진 만화 영상 및 문서 영상들 중 240×360 크기의 Lucy 영상과 300×300 크기의 문서 영상에 대해 블록의 크기를 다양하게 변경하여 실험한 결과를 제시한다.

먼저, 만화 영상과 문서 영상에 삽입된 비밀 데이터의 양은 표 1 및 표 2와 같다. 표 1과 표 2를 살펴보면, 비밀 데이터의 삽입용량은 Tseng 방식이 가장 많고, 다음이 제안 방식이며, Wu 방식은 다른 두 방식에 비해 매우 적다. 하지만 Tseng 방식은 은닉영상의 비가시성 측면에서 문제가 있음을 이후에 제시할 것이다. Wu 방식은 한 블록에 변경 가능한 화소가 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 감소됨을 알 수 있었다

표 1. 이진 만화 영상에 삽입된 비밀 정보의 양

블록 크기	삽입 비트 수		
	Tseng	Wu	제안 방식
6×6	1704	×	1450
15×15	660	384	545
30×30	296	96	217

표 2. 이진 문서 영상에 삽입된 비밀 정보의 양

블록 크기	삽입 비트 수		
	Tseng	Wu	제안 방식
6×6	3136	×	2022
15×15	1140	400	910
30×30	472	100	329

결국, 제안방법과 Chang 방법의 기반이 된 알고리즘은 Tseng 방법이며, 제안방법의 목적은 Tseng 기법보다 삽입용량은 다소 작지만, 비가시성이 월등히 높다는 것과 거리계산에서 소요되는 시간을 단축시킨다. 그러나 Chang 방법은 Tseng 방식에 비해 비가시성은 높였지만, 삽입용량이 작고, 이중 처리로 인해 수행시간 더 길어지는 단점을 가진다. Chang 방법은 추출이 명확하게 되지 않아 본 논문의 비교에서 생략하였다.

표 3은 기존 방식들과 제안 방식의 객관적인 화질을 비교하기 위해 식(13)과 같이 NC를 이용하여 평가한 결과이다. 식(13)에서 W는 엄폐영상, W_r는 비밀 데이터가 삽입된 은닉영상을 의미한다.

$$NC = \frac{\sum_i \sum_j W(i,j) \cdot W_r(i,j)}{\sum_i \sum_j [W(i,j)]^2} \qquad (13)$$

표 3. NC를 이용한 화질 비교 (블록 크기 15×15)

실험 영상	NC		
	Tseng 방식	Wu 방식	제안 방식
Lucy	0.9992	0.9989	0.9998
문서	0.9986	0.9986	0.9988

표 3에서 알 수 있듯이 정량적인 평가에서는 NC 값이 모두 비슷하지만, 제안 방식이 조금 더 높음을 알 수 있었다. 실험에서, 엄폐영상의 화소 값과 은닉영상의 화소 값이 서로 다른 경우의 개수, 즉 변경 화소 수는 Wu 방식이 제일 많고, 그 다음이 Tseng의 방식이며, 제안 방식이 제일 작게 변경되었다. 그러나 Wu 방식과 제안 방식은 비가시적인 위치에만 변경되었기 때문에 인간의 시각적인 측면에서 그 변경을 쉽게 인지할 수 없음을 알 수 있었다.

(그림 10)과 (그림 11)은 이진 만화 영상과 문서 영상에 대해 기존 방식들과 제안 방식을 실험한 결과들을 각각 보이며, 블록의 크기는 15×15이다.

(그림 10)과 (그림 11)을 살펴보면, Wu 방식과 제안 방식의 은닉영상은 엄폐영상과 시각적인 차이를 인지하기 힘들다. 반면, Tseng 방식은 은닉영상의 윤곽 부분 주위에 많은 잡음들이 모여 있음을 볼 수 있다. 특히, (그림 10)의 (b)와 (그림 11)의 (b)에 확대한 그림을 보면 쉽게 확인이 가능하다.

제안 방식을 Tseng 방식과 비교하면, 비밀 데이터의 삽입용량은 다소 작지만, 큰 차이는 아니라 생각되며, 은닉영상의 비가시성을 보면 제안 방식이 월등히 우수함을 알 수 있다. Tseng 방식은 객관적인 평가(NC 측정)에서는 크게 떨어지지 않지만, 시각적인 평가(주관적인 평가)에서는 은닉영상의 열화가 많이 발생한다는 것을 알 수 있다. 또한 제안 방식과 Wu 방식과 비교하면, Wu 방식은 정량적인 평가는 조금 낮지만, 화소의 변경이 시각적으로 아주 둔한 위치에서 일어났기 때문에 비가시성은 뛰어났다. 하지만, Wu 방식은 삽입용량이 매우 적다는 단점을 가지고 있다.

결과적으로, 제안 방식은 비밀 데이터를 충분히 은닉시킬 수 있으며, 은닉영상의 비가시성도 매우 뛰어나다. 따라서 제안 방식은 Tseng 방식과 Wu 방식을 장점들을 접목시켜 삽입용량과 비가시성이 서로 보완될 수 있는 보다 효율적인 알고리즘이라 여겨진다.

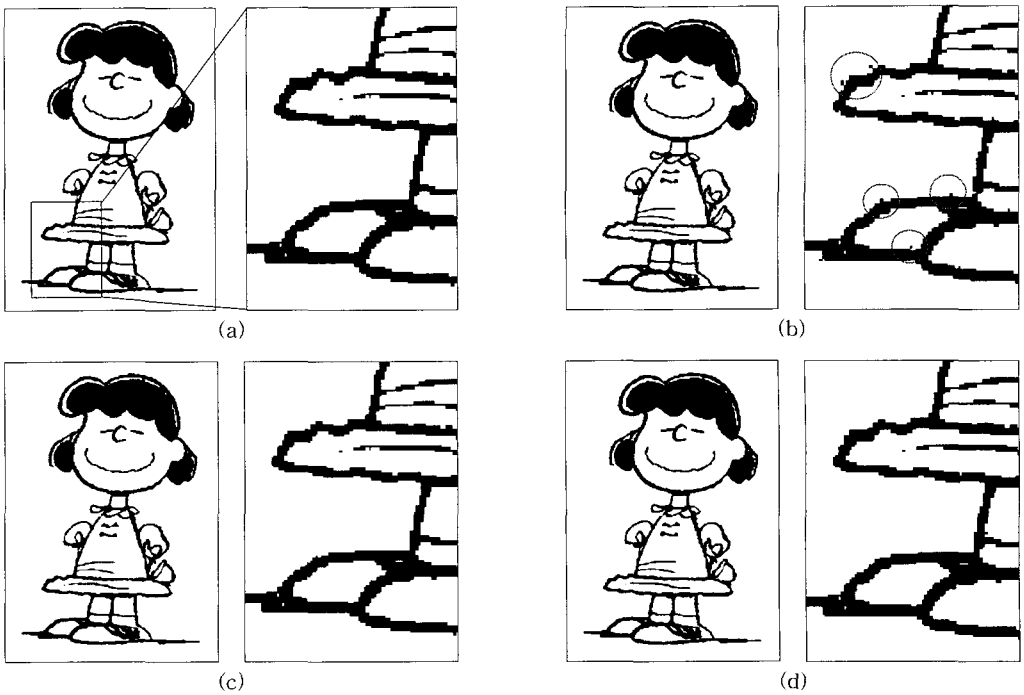


그림 10. 만화 엄폐영상과 은닉영상 (블록 크기 : 15×15 화소) : (a) 엄폐영상 (Lucy, 240×360), (b) 은닉영상 (Tseng 방식), (c) 은닉영상 (Wu 방식), (d) 은닉영상 (제안 방식)

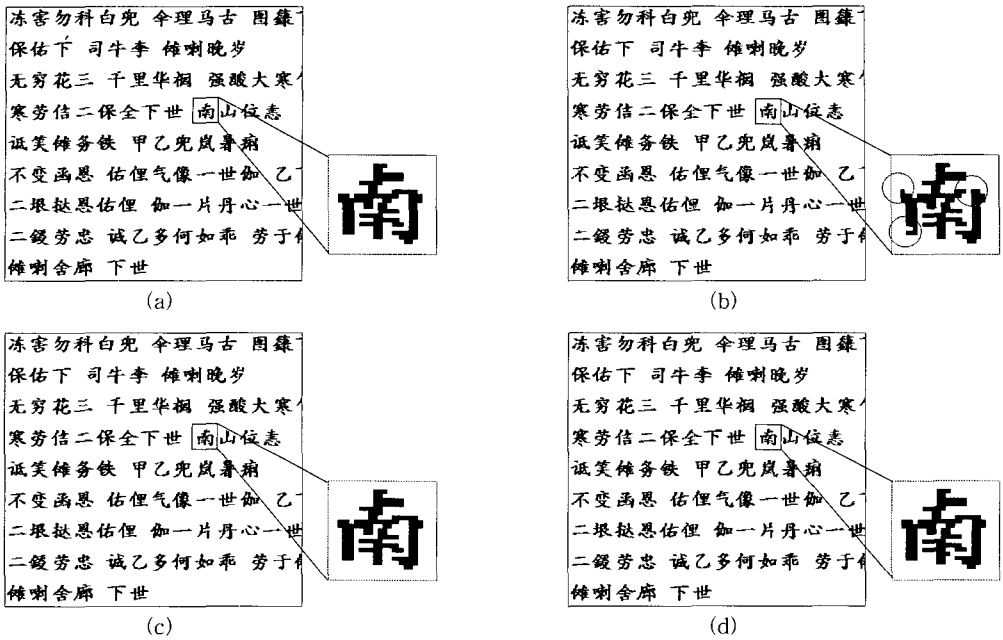


그림 11. 문서 엄폐영상과 은닉영상 (블록 크기 : 15×15 화소) : (a) 엄폐영상 (300×300), (b) 은닉영상 (Tseng 방식), .(c) 은닉영상 (Wu 방식), (d) 은닉영상 (제안 방식)

5. 결 론

본 논문에서는 이진영상을 이용하여 비밀 데이터를 삽입하는 영상 스테가노그라피의 한 방법을 제시하였다. 제안 방식은 은닉영상의 비가시성을 높이기 위해 패턴을 이용해 비시각적인 위치의 화소를 선택하여 삽입 처리를 수행하였다. 즉, 비밀 데이터의 삽입으로 인해 화소가 변경되더라도 시각적으로 인지가 둔한 위치의 화소들을 변경시켜 은닉영상의 화질을 개선시켰다. 또한, 랜덤 치환을 통해 한 블록 내에 비가시적인 화소들이 편중되는 현상을 억제하였으며, 가중치 행렬을 이용하여 비밀 데이터의 삽입용량을 증가시킬 수 있는 방식을 제안하였다.

참 고 문 헌

[1] N.F. Johnson, Z. Duric, and S. Jajodia, *Information Hiding*, Kluwer Academic Publishers, London, 2001.

[2] E. Kawaguchi, H. Noda, and M. Niimi, "Image Data Based Steganography," *Information Processing Society of Japan(IPSJ MAGAZINE)* Vol. 44, No. 3, pp. 236-241, 2003.

[3] K. Nozaki, M. Maeda, K. Tsuda, and E. Kawaguchi, "A Model of Anonymous Covert Internet Mailing System Using Steganography," *Proceedings of Pacific Rim Workshop on Digital Steganography(STEG)*, pp. 7-10, 2002.

[4] C.C. Chang, T.S Chen, and L.Z. Chung, "A Steganographic Method Based upon JPEG and Quantization Table Modification," *Information Sciences Journal 141, ELSEVIER*, pp. 123-138, 2002.

[5] C.C. Thien and J.C. Lin, "A Simple and High-hiding Capacity Method for Hiding Digit-by-digit in Images Based on Modulus Function," *Pattern Recognition Journal 36*, PERGAMON, pp. 2875-2881, 2003.

[6] M.Y. Wu and J.H. Lee "A Novel Data Embedding Method for Two-Color Facsimile Images." *In Proc. of International Symposium on Multimedia Information Processing (ISMIP98)*, 1998.

[7] Y. Abe, K. Inoue and K. Ejiri "Digital Watermarking for Bi-Level Image," *Proc. of*

Symposium on Crypotography and Information Security 2000, C05, 2000.

[8] 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*, pp. 65-70, 2002.

[9] Y.Y. Chen, H.K. Pan, and Y.C. Tseng, "A Secure Data Hiding Scheme for Two-Color Image," *Proc. IEEE Symposium on Computer and Communication(ISCC 2000)*, p. 750-755, 2000.

[10] Y.C. Tseng and H.K. Pan, "Secure and Invisible Data Hiding in 2-Color Images," *Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2001)*, Vol. 2, pp. 887-896, 2001.

[11] M. Wu, E. Tang, and B. Liu, "Data Hiding in Digital Binary Image," *IEEE Int. Conf. on Multimedia and Expo(ICME 2000)*, p. 393-396, 2000.

[12] G. Pan, Y. Wu, and Z. Wu, "A Novel Data Hiding Method for Two-Color Image," *International Conference on Information and Communications Security(ICICS2001)*, LNCS 2229, pp. 261-270, 2001.

박 영 란

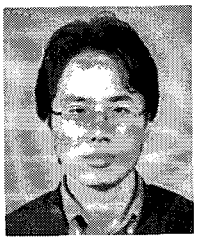
1996년 2월 방송통신대학 전자계산학과 졸업(이학사)
1998년 8월 부경대학교 전산정보학과 졸업(이학석사)
2005년 2월 부경대학교 정보보호학과 박사수료

관심분야 : 심층암호, 정보보호, 영상처리, 영상인증, 디지털 워터마킹

하 순 혜

2000년 2월 부경대학교 전자계산학과 졸업(이학사)
2004년 8월 부경대학교 교육대학원 전산교육학과 졸업(교육학석사)

관심분야 : 심층암호, 디지털 워터마킹, 디지털 영상처리



강 현 호

1999년 2월 동의대학교 컴퓨터공학과 졸업(공학사)
2001년 2월 부경대학교 대학원 전자계산학과 졸업(이학석사)
2004년 2월 부경대학교 대학원 전자계산학과 박사 수료
2005년 4월~현재 일본 전기통신대학(電気通信大学) 정보시스템학연구과 박사 과정
관심분야 : 멀티미디어 컴텐츠 보호 및 응용, 신호처리, 오류정정부호

이 혜 주

1994년 2월 부경대학교 전자계산학과 졸업(이학사)
1997년 2월 부경대학교 대학원 전자계산학과 졸업(이학석사)
2000년 2월 부경대학교 대학원 전자계산학과 졸업(이학박사)
2000년 6월~2001년 2월 한국정보통신대학원대학교 박사후연구과정생
2001년 3월~2005년 1월 한국전자통신연구원 방송미디어연구그룹 선임연구원
2005년 3월~2006년 2월 경성대학교 초빙교수
관심분야 : 디지털 비디오 신호처리 및 부호화, 디지털 워터마킹

신 상 욱

1995년 2월 부경대학교 전자계산학과(이학사)
1997년 2월 부경대학교 대학원 전자계산학과(이학석사)
2000년 2월 부경대학교 대학원 전자계산학과(이학박사)
2000년 4월~2003년 8월 : 한국전자통신연구원 선임연구원
2003년 9월~현재 : 부경대학교 전자컴퓨터정보통신공학부 조교수
관심분야 : 암호 이론, 정보보호, 이동통신 정보보호