오차 확산법을 이용한 기밀 정보 합성법

박 영 란, 이 혜 주, 박 지 환
부경대학교 전산정보학과

Embedding Secret Information into Dithered Image Using Error Diffusion

Young Ran Park, Hye Joo Lee, Ji Hwan Park
Dept. of Computer Information Pukyoung Nat'l Univ

요 약

암호 통신의 한 방법으로 표면상은 의미 있는 형태를 유지하지만 실은 그 속에 중요한 기밀 정보를 숨겨놓은 심층암호(steganography)가 주목되고 있으며, 특히 디지털 화상을 이용하는 화상 심층암호는 저작권 보호 수단으로 활용되고 있다. 본 논문은 농담화상을 오차 확산법을 이용하여 흑·백의 2치로 의사적으로 표시하면서 기밀 정보를 합성하는 새로운 방식을 제안한다.

1. 서론

최근 컴퓨터 네트워크가 널리 보급되어 제3자에게 중요한 정보를 누설되지 않으면서 상대에게 전달해야 할 필요성이 높아지고 있다. 이와 같은 통신을 수행하기 위한 방법으로 중요한 정보를 다른 의미가 있는 데이터 내에 몰래 집어넣어서 제3자가 중요한 정보가 있음을 알아차릴 수 없도록 하는 수법이 연구되고 있다. 이와같은 형태를 심층암호라 하고, 기밀 정보가 합성된 화상을 전송하는 형태를 화상 심층암호(image steganography)라 한다[1].

한편, 디더링(dithering)이란 다계조 출력을 할 수 없는 출력장치에 농담화상을 의사적으로 표현하는 방법으로 다양한 방법들이 제안되어져 널리 이용되고 있다[2]. 디더링이 수행된 화상은 원래의 화상보다 많은 잡음을 가지게 되며, 많은 잡음을 지닌 디더링에 의한 화상은 화상 심층암호의 관점에서 기밀 정보의 합성에 적합한 성질을 가지게 된다.

본 논문에서는 오차 확산법을 이용하여 2치로 디더링한 후 기밀 정보를 몰래 합성하는 새로운 방식을 제안한다. 먼저, 2장에서는 오차 확산법을 이용한 디더링 방식을 소개하고, 3장에서는 기밀 정보 합성법의 기존 방식과 제안방식을 각각 설명한다. 그리고, 4장에서는 실험을 통하여 제안방식을 유효성을 보이고, 마지막으로 5장은 제안방식에 대한 향후의 연구 과제를 제시한다.

2. 오차 확산법을 이용한 2치 디더링

최근 OA기기 등의 급속한 보급으로 문서화상뿐만 아니라 농담화상의 이용이 증가하고 있다. 그러나, 프린터와 같이 출력장치가 표시할 수 있는 계조의 수는 한정적이기 때문에 계조수를 낮추어

이 연구는 1998년도 한국과학재단 연구비 지원에 의한 결과의 일부임. 과제번호 981-0928-152-2

화상의 계조를 의사(pseudo)적으로 표현하는 디더링(dithering)기법이 요구된다.

화상의 디더법 중에서 오차 확산법은 디더된 화소값과 원화상의 화소값의 오차를 주변화소에 확산시키는 방법으로 화질이 양호하여 흑백 2치의 화소에 의해 의사적으로 농담을 표현할 수 있는 수단으로 널리 이용되고 있으며, 다음과 같이 수행되어진다.

그림1과 같이 원화상의 위치 (i, j)에 있어서의 주목 화소값을 $p(i, j)$라 할 때, $p(i, j)$를 임계값 L에 의해서 새로운 화소값을 식(1)과 같이 구할 수 있다. 이때, $p(i, j)$와 디더된 새로운 화소값 $p'(i, j)$ 사이에 오차 $e(i, j)$가 생기게 된다. 이 오차를 표1의 확산계수를 이용하여 주변화소에 확산을 시키기 된다. 이 때, 확산계수 α를 이용하여 주목화소와 주변화소들의 상관관계를 고려하여 분배하고, 식(2)와 같이 오차 $e(i, j)$와 주변화소에 대응하는 확산 계수 α를 곱한 결과를 주변화소의 원화소의 값과 가산하여 새로운 주변 화소값으로 한다.

$$p'(i,j)=\begin{cases}1 & p(i,j)\geq L\\ 0 & p(i,j)<L\end{cases} \qquad (1)$$

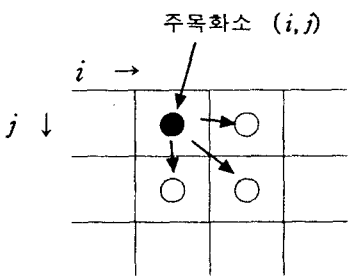
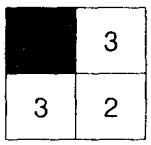


그림1. 오차의 확산

$$\begin{aligned}p'(i+1,j)&=p(i+1,j)+e(i,j)\times\alpha_{i+1,j}\\ p'(i+1,j+1)&=p(i+1,j+1)+e(i,j)\times\alpha_{i+1,j+1}\\ p'(i,j+1)&=p(i,j+1)+e(i,j)\times\alpha_{i,j+1}\end{aligned} \qquad (2)$$

오차 확산법의 예로써 그림2(b)와 같이 주어진 화소값에 대하여 2치로 디더링 할 경우이다. 먼저, 임계값 $L=128$로 정하고, 그림2(a)와 같은 확산계수를 이용하면 디더된 화소값은 식(1)에 의해 그림2(c)와 같은 출력 화소값을 얻게 된다. 이와 같은 과정을 전체 화소에 대해서 실행하면 디더된 화상을 얻게 된다.



$\alpha_{i+1,j}=\frac{3}{8}$

$\alpha_{i,j+1}=\frac{3}{8}$, $\alpha_{i+1,j+1}=\frac{2}{8}$

(a) 확산계수

55	60	20
130	125	240
200	174	224

(b) 원 화소값

0	0	0
1	1	1
1	0	1

(b) 디더된 화소값

그림2. 오차 확산법의 예

3. 기밀 정보 합성법

3.1 기존의 합성법

2치 디더링에서의 기밀 정보 합성 방법[3-5]은 원 화상 G를 주사선 방향으로 오차 확산법을 이용하여 n만큼 2치화 하여 출력하고 이 비트 계열을 p라 한다. 이 때 p계열과 기밀 비트 b를 인수로 하면서 0 또는 1을 반환하는 함수 $F(b, p)$가 이용된다.

함수 F는 비트 계열 p와 b에 나타나는 '1'의 개수가 짝수이면 0을, 반대인 경우에는 1을 반환하게 된다. 즉, 그림3과 같이 길이 $n=4$로 설정하고 2치로 디더된 비트 계열 p와 합성 비트 $b=1$인 경우에 p와 b의 1의 개수는 홀수가 된다. 따라서 합성함수 F의 반환값은 1로써 이 값이 $n+1$번째 출력이 된다.

이 경우에 기밀 비트를 복호하기 위해서 $n+1$번째까지 1의 개수를 계산하여 홀수이면 '1'로

복호하고, 짝수인 경우에는 '0'으로 복호한다.

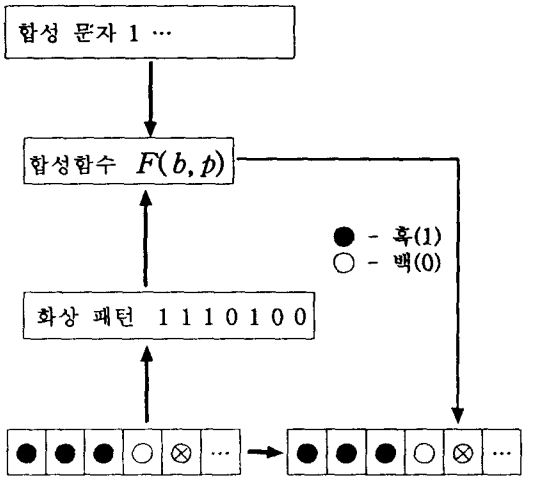


그림3. 문자 합성의 원리

이와 같이 기존의 방식으로 기밀 정보를 집어넣을 경우 항상 $n+1$번째의 화소값이 변하게 되어 화상 내에 일정한 패턴(수직선, 사선 모양)이 생기는 문제점이 발생하게 된다.

3.2 제안방식 I, II

기존의 방식은 n의 값에 의존하여 화상 내에 일정한 패턴이 발생되는 단점이 있다. 이러한 단점을 고려하여 기밀 정보를 합성하기 위한 새로운 방식을 제안한다.

제안방식I은 0 또는 1의 값이 k개 이상 연속하고 값이 변경되는 변환지점에 기밀 정보를 합성한다. 기밀 정보를 합성하기 위해 연속되는 런의 길이 k를 합성하고자 하는 비트 b의 값에 따라 홀수화/짝수화를 시키게 된다. 이때, 홀수화/짝수화를 위해 변경되는 부분은 변환 지점인 k의 다음 $k+1$번째인 화소가 된다. 합성하고자 하는 비트 b에 따라 식(3)과 같이 변환지점인 $k+1$의 화소값을 변경한다.

$$\begin{cases} \text{런의 길이를 짝수화}, & b=0\text{인 경우} \\ \text{런의 길이를 홀수화}, & b=1\text{인 경우} \end{cases} \quad (3)$$

예를 들어, 그림4와 같이 디더된 비트 계열은 5개의 변환지점이 발생된다. 이때 $k\geq 4$로 설정하는 경우 위치 5,12에서 기밀 정보를 합성하게 된다.

이 경우에 1의 런의 길이가 4이고 합성 비트가 0인 경우에는 런의 길이는 짝수이므로 위치 5의 화소값은 변경할 필요가 없게 되지만, 합성 비트가 1인 경우에는 홀수화가 요구되므로 위치 12의 화소값은 '1'로 변경해야 한다.

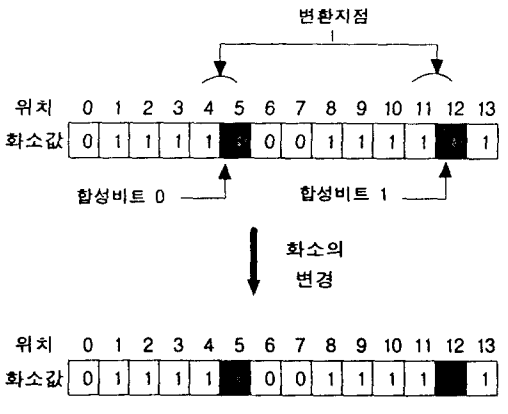


그림4. 제안방식I의 합성 원리

합성 비트를 복호하는 경우에는 런의 길이가 $k\geq 4$이면서 변화 지점을 포함하여 k가 홀수인지 짝수인지를 판단하여 1 또는 0을 복호하게 된다.

그러나, 이 방법에는 한가지의 예외적인 상황이 발생이 된다. 즉, 그림4와 같이 비트 계열을 변경하여 기밀 정보를 복호하는 경우에 위치 12의 변환지점에서 복호가 불가능하게 된다. 이것은 원 비트 계열의 1의 런의 길이가 4이고 합성 비트가 1인 경우에 위치 12의 화소값은 1로 변경된다. 이와 같은 경우 복호시에 1의 런의 길이가 합성시의 경우와 달라지게 되어 정확하게 복호되지 않는다. 따라서, 이것을 방지하기 위해서 변경하고

자 하는 비트인 $k+1$번째와 $k+2$번째 화소값을 동시에 변경한다. 즉, 위의 예에서 위치 12와 13의 값이 서로 동일하지 않도록 $k+2$번째 화소값을 변경하면 그림5와 같은 결과로 이러한 문제를 해결할 수 있다.

합성 전의 화상의 화소값과 제안방식I를 이용하여 기밀 비트 '01' 를 합성한 후의 각 화소값을 그림5에 나타낸다.

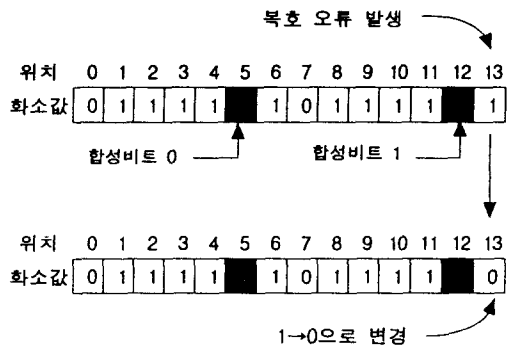


그림5. 제안방식I의 수정

제안방식I은 화상에 따라 넣을 수 있는 기밀 정보의 길이가 달라지게 되나, 제안방식II는 주어진 화상에 고정된 길이의 기밀 정보를 집어넣을 수 있는 방식이다. $3\times m$의 블록을 그림6과 같이 설정하여 기밀 정보를 합성하기 위해 중앙의 행 (l)을 중심으로 2비트의 기밀 정보에 따라 각각 상·하의 행 $l-1$, $l+1$과의 1의 개수를 표1과 같이 짝수화/홀수화 한다.

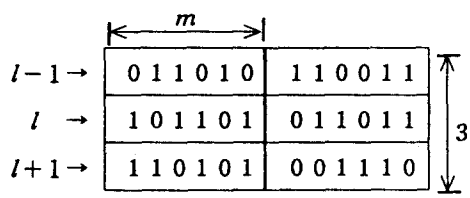


그림6. $3\times m$의 블록

표1. 홀수화/짝수화에 의한 기밀 정보의 합성

기밀 정보		1의 개수	
		l과 $l-1$	l과 $l+1$
0	0	짝수화	짝수화
0	1	짝수화	홀수화
1	0	홀수화	짝수화
1	1	홀수화	홀수화

복호시에는 l과 $l-1$, l과 $l+1$에 나타나는 1의 개수를 구하여 그 개수가 짝수인지 홀수인가에 따라 표1에 각각 대응되는 기밀 정보를 추출하게 된다. 여기에서, 홀수/짝수를 정확하게 판단하기 위해서 중앙의 행 l의 화소값을 변경하면 안되므로 행 $l-1$, $l+1$의 화소값만을 변경시켜야 한다. 이때, 변경시킬 화소값을 설정하는데 있어서 그림7의 방법과 같이 $l-1$과 $l+1$의 화소를 임의로 선택하여 변경한다.

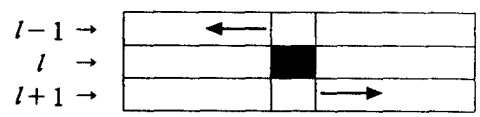


그림7. 합성 위치 선택 방법

4. 실험 및 결과

그림8의 원화상 Lenna(size: 256×256화소, 256레벨)를 이용하여 기존의 합성 방식 및 제안방식I과 제안방식II를 각각 동일한 기밀 정보량을 합성한 결과를 시각적으로 비교하여 그 성능을 평가하였다.

그림8. 원화상 "Lenna"

먼저, 집어넣기를 수행하지 않고 오차확산법을 이용하여 2치 화상으로 디더를 수행한 화상을 그림9에 나타낸다.

그림9. 더더 화상

제안방식의 유효성을 확인하기 위해 기존의 방식과 제안방식I, II에 대해 각각 800 bits, 2400 bits의 임의의 기밀 정보를 합성한 결과를 그림10에 나타낸다.

그림10(a). 기존 방식

그림10(b). 제안방식 I

그림10(c) 제안 방식II

그림10. 디더 화상에 800 bits 합성

그림10의 결과에서 800 bits의 기밀 데이터를 집어넣는 경우에는 기존의 방식과 제안방식들의 차이는 시각적으로 그다지 인식할 수 없다.

그러나, 보다 많은 기밀 정보를 집어넣은 그림11의 결과에서 기존의 방식은 앞에서 지적한 바와 같이 사선 모양의 패턴이 생김을 알 수 있다.

그림11(a). 기존 방식

그림11(b). 제안 방식I

그림11(c) 제안 방식II

<그림11. 더더 화상에 300bytes 합성>

제안방식I은 화상내에서 화소값이 변하는 지점에서 최대 두 개의 화소값을 변경하여 기밀 정보를 집어넣기 때문에 화상의 성질에 따라 집어넣을 수 있는 기밀 정보의 양은 제한되어진다. 런의 길이 k를 가변적으로 하여 기밀 정보의 양은 조절할 수 있으므로 적절한 k의 선택이 요구된다.

제안방식II는 블록에 항상 2비트의 기밀 정보를 넣을 수 있으며, 블록 내에서 제안방식I의 방법을 적용하거나 또는 화상의 성질을 고려하여 상·하의 행의 합성 위치를 선택한다면 보다 좋은 결과를 얻을 수 있을 것으로 기대된다.

5. 결론

본 논문에서는 농담화상을 오차 확산법을 이용하여 2치화 한 후 기밀 정보를 집어넣는 방법을 제안하고 그 유효성을 확인하였다. 기존의 방식은 많은 기밀 정보를 집어넣는 경우 일정한 패턴이 생기는 단점이 있다. 제안방식I은 화소값이 변하는 지점의 화소값을 변경하였으며, 제안방식II는 블록을 설정하여 상·하 행의 상관을 고려하여 화소값을 변경하였다.

향후 과제로써 다치 화상에의 제안방식의 적용과 평가, 화상의 왜곡을 보다 최소화 하면서 대량의 기밀 정보를 집어넣을 수 있도록 개선하는 것이다.

[참고문헌]

[1] K. Matsui, "Video Steganography", Morikita Publishing Co, Ltd, 1993(in Japanese)

[2] R. Crane, "A Simplified Approach to Image Processing", pp.153-171, Prentice Hall PTR(1997)

[3] 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, pp.7-14(1996-02) (in Japanese)

[4] K. Matsui, K. Tanaka, "Video-Steganography : How to Secretly Embed a Signature in a Picture", IMA Intellectual Property Project Proceedings, Vol.1, pp.187-206, 1994

[5] K. Oka, K. Matsui, "Embeding Signature into a Hardcopy of Dithered Image", Trans. of IEICE, D-II, Vol.J80-D-11, No.3, pp.820-823 (1997.3) (in Japanese)