다치 디더링 화상을 이용한 정보 은닉 기법

박영란, 이혜란, 박지환
부경대학교 대학원 전자계산학과

Information Hiding Using Multi-Level Dithering Image

Young-Ran Park, Hye-Ran Lee, Ji-Hwan Park
Dept. of Computer Science, PuKyong Nat'l University

요 약

암호 통신의 한 방법인 화상 심층암호(image steganography)는 화상 내에 기밀정보를 몰래 숨겨서 전송하는 것으로 표면상은 의미 있는 형태를 유지하지만, 실제로는 그 속에 기밀 정보를 몰래 은닉하는 형태로서 제3자는 기밀 정보의 존재 여부를 확인할 수 없기 때문에 공격의 위협을 감소시킬 수 있다. 특히 디지털 화상을 이용하는 화상 심층암호는 저작권 보호 수단으로 활용되고 있다. 본 논문은 256레벨의 그레이 화상에 다치 오차확산법을 이용하여 디더링을 수행하는 단계에서 기밀 정보를 은닉하는 새로운 방법을 제안한다

1. 서론

최근 컴퓨터 네트워크가 널리 보급되어 제3자에게 중요한 정보가 누설되지 않으면서 상대에게 정보를 안전하게 전달해야 할 필요성이 높아지고 있다. 이와 같은 통신을 수행하기 위한 방법으로 중요한 정보를 다른 의미가 있는 데이터 내에 몰래 집어넣어 제3자에게는 그 정보가 있음을 알아차릴 수 없도록 하는 방법이 연구되고 있다. 이와 같은 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 출력장치에서 그레이화상을 계조수를 낮추어 의사(pseudo)적으로 표현하는 방법으로 다양한 방법들이 제안되어 널리 이용되고 있다[2]. 디더링이 수행된 화상은 원래의 화상보다 많은 잡음을 가지게 되며, 많은 잡음을 지닌 디더링에 의한 화상은 화상 심층암호의 관점에서 기밀 정보의 은닉에 적합한 성질을 가지게 된다.

본 논문에서는 오차 확산법을 이용하여 다치로 디더링한 후 정보를 은닉하는 새로운 방식을 제안한다. 먼저, 2장에서는 오차 확산법을 이용한 디더링 방식을 소개하고, 3장에서는 기밀 정보 은닉 방법의 기존 방식과 제안방식을 각각 설명한다. 그리고, 4장에서는 실험을 통하여 제안방식의 유효성을 보이고, 마지막으로 5장은 결론 및 제안방식에 대한 향후의 연구 과제를 제시한다.

2. 오차 확산법을 이용한 다치 디더링

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 있다. 2치화 방식을 확장시킨 3치, 5치 등의 다치 화상으로의 디더링 방법은 다음과 같이 수행된다.

그림1과 같이 원화상의 위치 (i,j)의 주목 화소값을 $p(i,j)$ 라 하고 표현 가능한 다치 화상의 계조수를 g라 한다. 이때 출력 화상의 계조값 $L_k(k=0,\cdots,g-1)$를 결정하기 위해 화소값 $p(i,j)$ 와 출력 화상의 계조값 L_k와의 차가 $\min(|p(i,j)-L_k|)$ 일 때의 L_k를 $p(i,j)$ 의 디더된 화소값 $p'(i,j)$라 한다. 이와 같이 계산된 출력 화소값 $p'(i,j)$ 와 원화상의 화소값 $p(i,j)$ 와의 오차값 $e=p(i,j)-p'(i,j)$를

구하여 (i,j)의 주변화소에 확산 분배를 한다.

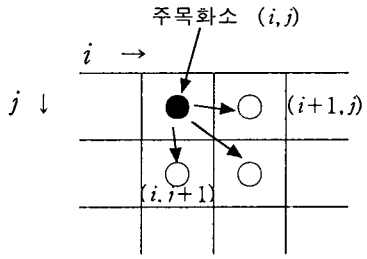

그림1. 오차의 확산

이 때, 오차는 확산계수 α를 이용하여 주목화소와 주변화소들의 상관관계를 고려하여 분배된다.

$$p'(i+1,j)=p(i+1,j)+e(i,j)\times\alpha_{i+1,j}$$
$$p'(i+1,j+1)=p(i+1,j+1)+e(i,j)\times\alpha_{i+1,j+1} \quad (1)$$
$$p'(i,j+1)=p(i,j+1)+e(i,j)\times\alpha_{i,j+1}$$

식(1)과 같이 오차 e와 주변화소에 대응하는 확산계수 α를 곱한 결과를 주변화소의 원 화소값에 가산하여 새로운 주변화소값, 즉 오차가 확산된 화소값으로 변경하는 과정을 모든 화소에 대하여 수행하면 원화상은 g치화 되어진다.

오차 확산법의 예로써 그림2(b)와 같이 주어진 화소값에 대하여 계조수 $g=5$로 디더링 할 경우, 우선 동일한 간격으로 양자화 하면 계조값 L_k의 범위는 {0,64,128,192,255}가 된다. 그림2(a)와 같은 확산계수를 이용하면 식(1)에 의해 디더된 화소값은 그림2(c)와 같은 출력 화소값을 얻게 된다.

	3
3	2

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

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

(a) 확산계수

140	100	90
130	120	110
200	170	150

(b) 원화소값

128	128	64
128	128	128
192	192	128

(c) 디더된 화소값

그림 2. 오차 확산법의 예

3. 기밀 정보의 은닉 방법

3.1 기존 방법

다치 오차 확산법을 이용하여 화상을 디더링 하면서 은닉 정보를 잡음의 형태로 집어넣는 기존의 방식[3]은 g개의 계조값 $L_k(k=0,1,\cdots,g-1)$에 대해서 식(2)와 같이 2개의 그룹 G_1, G_2를 먼저 정의한다.

$$G_1=\{L_k|k=0,2,\ldots,g-2\}$$
$$G_2=\{L_k|k=1,3,\ldots,g-1\} \quad (2)$$
$$\text{단, } (L_0<L_1<\ldots<L_{g-1})$$

첫 번째 단계는 길이가 m인 은닉 정보 계열 $B=\{b_l|b_l=0,1 \ ; l=0,1,\cdots,m-1\}$의 한 비트를 원화상의 $n+1$번째의 화소마다 집어넣는 방식으로 먼저, 오차 확산법을 이용해서 주사선 방향으로 n화소 만큼 g치화를 수행한다. 이때, 디더한 계조값 L_k로 구성되는 길이 n의 계열을 D라고 한다. 기밀 정보 b_l을 합성하기 위해 계조값 L_k가 속하는 그룹 G_1과 G_2에 각각 0과 1을 대응시켜 D'를 구한다. 즉, D'는 0과 1로 구성되는 계열이다.

두 번째 단계는 함수 F의 출력값을 결정하는 것으로 집어넣고자 하는 기밀 정보 b_l과 D'를 인수로 하는 함수 $F(b_l,D')$는 D'와 b_l에 포함된 1의 개수가 짝수가 되도록 0 또는 1을 조절하는 역할을 한다. 즉, b_l을 포함하여 1의 수가 짝수이면 함수 F는 0으로, 반대의 경우에는 1로 출력하게 된다.

함수 F의 출력값이 0이면 G_1의 값 중에서 $n+1$번째의 원 화소값과 오차가 최소가 되는 계조값을 출력하고, 1인 경우에는 그룹 G_2에서 선택하여 출력하게 된다. 이 과정을 주사선 방향으로 $n+1$번째마다 수행하면 결과적으로 기밀 정보를 집어넣을 수 있다.

이와 같은 기존의 방식으로 기밀 정보를 집어넣을 경우 항상 $n+1$번째의 화소값이 변하게 되어 화상내에 일정한 패턴이 생기는 문제점이 있다.

3.2 제안방식

기존의 방식에서는 0과 1에 대응되는 2개의 그룹을 정의하여 1의 개수를 짝수가 되도록 $n+1$번째의 화소값을 변경하게 된다. 이 방식은 화소값을 변경할 때 주변화소간의 상관을 고려하지 않기 때문에 기밀

정보의 은닉에 의해 화질이 열화 된다. 따라서, 일정한 패턴이 발생하지 않고 화질의 열화를 줄일 수 있는 새로운 방식을 제안한다.

제안 방식은 주어진 화상에 고정된 길이의 기밀 정보를 집어넣을 수 있는 방식이다. 수행 과정을 살펴보면 먼저, 기존의 방식과 동일하게 주사선 방향으로 n개 화소까지 오차 확산법을 이용하여 디더를 수행하고, 2개의 그룹으로 나누어 0과 1의 계열을 구성한다. 그런 다음 $3\times m$의 블록을 그림3과 같이 설정하여 기밀 정보를 은닉한다. 중앙의 행(l)을 중심으로 2비트의 기밀 정보에 따라 각각 상·하의 행 $l-1$, $l+1$과의 계조값 L_k가 속하는 그룹 G_1과 G_2에 각각 0과 1에 대응되는 D'에 대해서 1의 개수를 표1과 같이 짝수 또는 홀수화 한다.

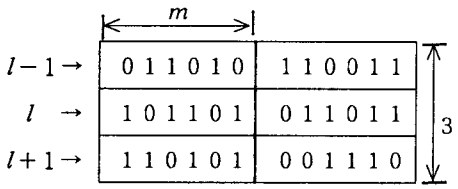

그림3. $3\times m$의 블록

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

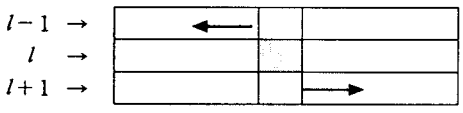

그림4. 합성 위치 선택 방법

복호시에는 l과 $l-1$, l과 $l+1$에 나타나는 1의 개수를 구하여 그 개수가 짝수인지 홀수인지에 따라 표1에 각각 대응되는 기밀 정보를 추출하게 된다. 여기에서, 홀수 또는 짝수를 정확하게 판단하기 위해서 중앙의 행 l의 화소값을 변경하면 정확한 추출이 불가능하므로 행 $l-1$, $l+1$의 화소값만을 변경시켜야 한다. 이때, 변경시킬 화소값을 설정하는데 있어서 그림4의 방법과 같이 $l-1$과 $l+1$의 화소를 임의로 선택하여 변경한다.

4. 실험 및 결과

그림5의 원화상 Lena(size: 256×256 화소, 256레벨) 화상 기존의 방식과 제안방식을 동일한 기밀 정보량으로 각각 은닉한 후 그 결과를 시각적으로 비교하여 성능을 평가하였다.

그림5. 원화상 "Lena"

먼저, 집어넣기를 수행하지 않고 오차 확산법을 이용하여 다치 화상으로 디더를 수행한 화상을 그림6에 나타낸다.

그림 6. 디더링 화상

제안방식의 유효성을 확인하기 위해 기존의 방식과 제안방식에 대해 각각 800 bits, 2400 bits, 4000 bits의 임의의 기밀 정보를 은닉한 결과를 그림7~8에 나타낸다.

그림7(a)의 결과에서 800 bits의 기밀 데이터를 집어넣은 경우에는 기존의 방식과 제안방식들의 차이는 시각적으로 그다지 인식할 수 없다.

그러나, 보다 많은 기밀 정보를 집어넣은 그림7(b)의 결과에서 기존의 방식은 앞에서 지적한 바와 같이 사선 모양의 패턴이 그림7(c)에서는 수직선 모양의 패턴이 생김을 알 수 있다. 기존의 방식과 제안 방식에 대해 SNR을 표2~3에서 각각 비교하였다. 또한, 제안방식은 블록에 항상 2비트의 기밀 정보를 넣을 수

있으며, 블록 내에서 화상의 성질을 고려하여 상·하의 행의 합성 위치를 선택한다면 보다 좋은 결과를 얻을 수 있을 것으로 기대된다.

(a) 800 비트 은닉

(b) 2400 비트 은닉

(c) 4000 비트 은닉

그림 7. 기존의 방식

(a) 800 비트 은닉

(b) 2400 비트 은닉

(c) 4000 비트 은닉

그림 8. 제안 방식

표 2. 원화상과의 SNR

방식 / 은닉 비트	기존방식[3]	기존방식[4]	제안방식
800 비트	18.144	18.223	18.052
2400 비트	17.940	18.229	17.685
4000 비트	17.650	18.216	17.389

표 3. 디더링 화상과의 SNR

방식 / 은닉 비트	기존방식[3]	기존방식[4]	제안방식
800 비트	15.365	34.909	35.138
2400 비트	15.021	29.179	29.075
4000 비트	14.796	26.466	26.523

5. 결론

본 논문에서는 그레이화상을 오차 확산법을 이용하여 다치화 한 후 기밀 정보를 집어넣는 방법을 제안하고 그 유효성을 확인하였다. 기존의 방식은 많은 기밀 정보를 집어넣는 경우 일정한 패턴이 생기는 단점이 있다. 이러한 문제점을 해결하기 위한 방안으로 본 제안방식에서는 블록을 설정하여 상·하 행의 상관을 고려하여 화소값을 변경하였다.

향후 과제로써 대량의 기밀 정보 은닉에 따른 화상의 왜곡을 보다 최소화할 수 있는 방법의 연구가 필요하다.

[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] 박영란, 이혜주, 박지환, "오차 확산법을 이용한 기밀 데이터 합성법", 멀티미디어학회 논문지 제2권 제 2호 pp.155~165(1999. 6)