오차 확산법을 이용한 기밀 데이터 합성법

박영란[†] · 이혜주[††] · 박지환[†††]

요 약

암호화(encryption)된 정보는 랜덤한 형태이기 때문에 공격자에 의해 기밀 정보가 누출될 위협이 있다. 한편, 화상 심층암호(image steganography)는 화상 내에 기밀 정보를 몰래 숨겨서 전송하는 것으로 제3자는 기밀 정보의 존재 사실을 알 수 없기 때문에 공격의 위협을 줄일 수 있게 된다. 화상 심층암호에서 기밀 정보는 잡음의 형태로 화상의 화소값을 변경하여 숨기게 된다. 이와 같이 농담화상(gray image)에 기밀 정보를 숨기는 경우에는 잡음으로 인한 화질 열화를 초래한다. 따라서, 농담화상에 디더링(dithering)을 수행하는 과정에서 기밀 정보를 숨기는 방식이 고안되었다. 오차 확산법을 이용한 기존의 방식은 고정된 간격마다 기밀 정보를 합성함에 따라 일정한 패턴이 생기는 문제점이 있다. 이러한 문제를 해결하고 기존의 방법을 향상시키기 위하여 본 논문에서는 런 길이(run length)를 이용하여 변환점에 기밀 정보를 합성하거나 원래의 디더값과 오차가 가장 적은 위치에 기밀 정보를 합성하는 새로운 방법을 제안하고, 그 성능을 컴퓨터 시뮬레이션을 통하여 평가하였다.

Embedding Method of Secret Data using Error-Diffusion

Young-Ran Park[†], Hye-Joo Lee[††] and Ji-Hwan Park[†††]

ABSTRACT

Because the encrypted data is random, there is a possibility of threat that attacker reveals the secret data. On the other hand, as the image steganography is to embed the secret data into cover image and to transmit the embedded image to receiver, an attacker could not know the existence of secret data even though he/she sees the embedded image, therefore the sender may reduce the threat of attack. In the image steganography, the secret data is embedded by modifying value of pixels as a form of noise. If the secret data is embedded into gray image, the degradation of image quality results from the modifications of image due to noise. Therefore many methods have been proposed to embed the secret data while dithering the gray image, but the existing method using error-diffusion has a problem that any patterns such as a diagonal lines or vertical take place due to embedding the secret data at the fixed interval.

To solve this problem and to improve the existing method, we proposed the new method that embeds the secret data at changed point with respect to 1's run-length or at the position where has the minimum difference with the original dithered value. We evaluated the performance of the proposed method by computer simulation.

1. 서 론

컴퓨터 네트워크의 발달로 인하여 정보를 빠르게 전달할 수 있게 되었다. 그러나, 이에 따라 제3자에게 정보를 누설하지 않고 안전하게 상대에게 정보를 전송해야 하는 정보보호의 중요성도 높아지고 있다. 현재 정보를 보호하기 위하여 가장 널리 사용되는 방법은 암호(cryptography)이다. 즉, 정당한 키를 획득할 수 있는 수신자만이 암호화된 정보를 복호할 수 있도록 하는 방법이다. 그러나, 이 방법은 암호화된 정보가 어떠한 의미인지 알 수 없는 랜덤한 형태로 변환

본 연구는 1998년도 눌원문화재단지원에 의해 수행되었음.
† 부경대학교 대학원 전산정보학과 (석사)
†† 부경대학교 대학원 전자계산학과 (박사과정)
††† 부경대학교 컴퓨터 멀티미디어 공학부

되기 때문에 무엇인지는 모르지만, 기밀 정보가 존재한다는 사실은 누구나 알 수 있으므로 공격의 가능성이 더욱 증가하게 된다.

이와는 달리 정보가 존재한다는 사실조차도 제3자가 알아차릴 수 없도록 하여 기밀 정보를 보호하고자 하는 심층암호(steganography)가 최근 연구되고 있다[1,2]. 심층암호는 기밀 정보를 숨기기 위하여 화상, 오디오, 비디오와 같은 원 데이터를 변조시킨 후, 그 데이터를 전송하여 정보를 보호하는 방법이다. 이때 기밀 정보를 숨기기 위해 이용되는 원 데이터를 cover-data, 기밀 정보가 숨겨져 있는 데이터를 stego-data라 한다[3].

cover-data의 형태는 화상, 오디오, 비디오 등 어떠한 형태의 데이터도 가능하나 본 논문에서는 화상 데이터만을 대상으로 하는 화상 심층암호(image steganography)의 한 방법을 제안한다. 화상 심층암호에서는 기밀 정보를 잡음의 형태로 원 화상 데이터 내에 숨겨 화상을 전송하는 것으로, 특히 농담화상을 이용한 화상심층암호에 대하여 많은 연구가 이루어져 왔다[4-7]. 그러나, 농담화상은 잡음에 의한 화상의 열화가 심하기 때문에 기밀 정보를 숨기는 경우 많은 주의가 요구된다. 이러한 어려움을 극복하기 위한 방법으로 화상의 계조를 낮추어 의사(pseudo)적으로 표현하는 디더 화상을 이용하여 기밀정보를 숨기는 방법이 제안되어 있다[8,9]. 즉, 디더링 기법에 의해 출력된 화상은 원래의 화상보다 많은 잡음을 가지게 된다. 따라서, 많은 잡음을 지닌 디더 화상은 화상 심층암호의 관점에서 볼 때 기밀정보를 숨기기에 적합한 성질을 갖는다.

본 논문에서는 디더링을 이용하여 기밀 정보를 숨기는 기존의 방식을 개선한 새로운 방식을 제안한다. 논문의 구성은 먼저, 2장에서 오차 확산법을 이용하여 기밀 정보를 숨기는 기존의 방법에 대해서 소개한다. 3장에서는 기존 방식보다 시각적으로 양호한 화질을 제공하는 제안방식에 대해서 기술한다. 제안방식에서는 2치 디더 화상에 대해서는 디더 화상에서의 1의 런의 길이를 이용하여 1과 0의 변환점에서 기밀 정보를 합성한다. 그리고, 다치 디더 화상에 대해서는 n번째 화소까지 디더링을 수행하고 합성 위치를 원래의 디더값과 오차가 가장 적은 디더값을 가진 화소로 결정함에 따라 고정된 간격인 n번째 화소마다 기밀 정보를 숨겨 일정한 패턴이 발생되는 기존의 방식을 개선하였다. 4장에서는 기존의 방식과 제안방식을 실험을 통하여 비교하여 결과로부터 제안방식의 유효성을 보이고, 마지막 5장에서는 결론으로써 제안방식에 연속되는 향후의 연구과제에 대하여 기술한다.

2. 디더 화상에 기밀 합성

2.1 오차 확산법

최근 OA기기 등의 급속한 보급으로 문서화상 뿐만 아니라 농담화상의 이용이 증가하고 있다. 그러나, 프린터와 같이 출력장치가 표시할 수 있는 계조의 수는 한정적이기 때문에 계조수를 낮추어 화상의 계조를 의사(pseudo)적으로 표현하는 디더링(dithering) 기법이 요구된다[10]. 화상 디더링 기법 중에서 오차 확산법은 디더된 화소값과 원 화상의 화소값 오차를 주변화소에 확산시키는 방법으로 화질이 양호하여 의사적으로 농담을 표현할 수 있는 수단으로 널리 이용되고 있다.

오차 확산법은 그림1과 같이 원 화상의 위치 (i, j)에서의 주목 화소값을 $p(i,j)$라 할 때,

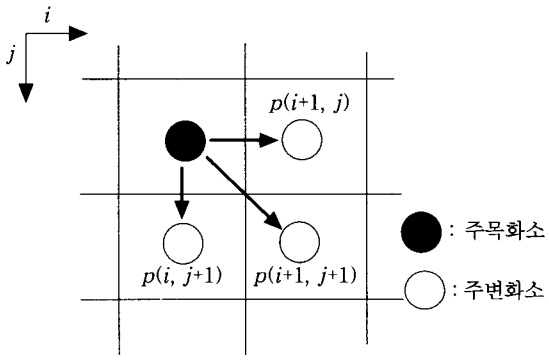


그림1. 오차의 확산

식(1)에 의해 $p(i,j)$는 임계값 T에 대하여 디더된 2치의 화소값 $p'(i,j)$로 변경된다.

$$p'(i,j)=\begin{cases}0(\text{ black}), & p(i,j)<T\\ 255(\text{ white}), & p(i,j)\geq T\end{cases} \quad (1)$$

이때, 원 화소값 $p(i,j)$와 디더된 $p'(i,j)$ 사이에는 오차 $e(i,j)=|p(i,j)-p'(i,j)|$가 생기게 된다. 이 오차를 식(2)와 같이 확산계수 $\alpha(i,j)$를 이용하여 주

변화소에 확산시키게 되고, 주변화소는 확산된 오차에 의해 원래의 화소값이 변경된다. 이때, 확산계수 $\alpha(i,j)$는 주목화소와 주변화소의 상관을 고려하여 주목화소로부터 멀어질수록 작은 값으로 설정한다.

$$\begin{aligned}\hat{p}(i+1,j) &= p(i+1,j)+e(i,j)\times\alpha(i+1,j)\\ \hat{p}(i+1,j+1) &= p(i+1,j+1)+e(i,j)\\ &\quad\times\alpha(i+1,j+1)\\ \hat{p}(i,j+1) &= p(i,j+1)+e(i,j)\times\alpha(i,j+1)\end{aligned} \tag{2}$$

오차 확산법의 일 예로써 확산계수 $\alpha(i+1,j)=\frac{3}{8}$, $\alpha(i,j+1)=\frac{3}{8}$, $\alpha(i+1,j+1)=\frac{2}{8}$에 대하여 그림2(a)의 원 화소값과 임계값 $T=128$이라 할 때, 그림2(b)의 디더 과정을 전 화소에 적용하면 그림2(c)와 같은 2치의 디더 화상을 얻게 된다.

다치 오차 확산법은 앞에서 설명한 2치 오차 확산법과 기본적으로 동일한 방법으로 수행되며, 출력 계조의 수가 2 이상으로 되는 차이점이 있다.

2.2 2치 디더 화상에 기밀 데이터 숨기기

2치 디더링에서의 기밀 데이터 합성법은 오차 확산법에 의해 2치화된 주사선(raster scan) 방향의 n개 출력값을 이용하여 기밀 데이터를 숨기는 방법이다. 여기서 간단히 흑과 백의 출력값을 각각 1과 0으로 표현하고 아래의 방법으로 기밀 데이터를 숨기게 된다.

[단계1] n개 화소의 2치 디더링의 수행

순차적으로 n개의 화소를 2치화하고, 그 출력 비트 계열을 B라 한다. 이때, 숨기고자 하는 기밀 비트 s와 B를 인자로 하는 합성 함수 $f(s,B)$를 이용한다.

[단계2] 함수 f의 출력 값 결정

합성 함수 f는 기밀 비트를 숨기기 위하여 계열 B와 s에 나타나는 1의 개수가 짝수일 때 0을, 홀수인 경우에는 1을 출력한다. 예를 들어, 그림3과 같이 $n=4$로 설정한 경우, 2치화된 비트 계열 $B=1110$이고 합성 비트 s가 1인 경우, B와 s에 포함된 1의 개수는 짝수가 된다. 따라서, 합성 함수 f는 0이 출력되어 $n+1$번째의 2치화된 출력값이 된다.

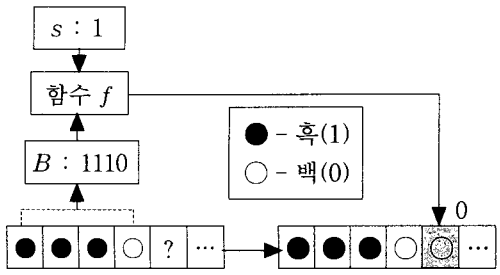


그림3. 기밀 비트의 합성

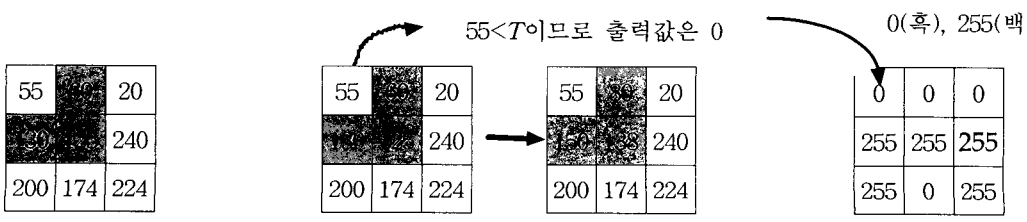
위의 방법은 간단하게 1의 개수를 이용하여 기밀 데이터를 숨기고 추출한다. 기밀 비트를 추출하기 위해서 2치화된 출력화상으로부터 $n+1$번째까지의 1의 개수가 홀수인 경우에는 추출된 기밀 비트 $\hat{s}$를 1로, 1의 개수가 짝수인 경우에는 $\hat{s}$는 0으로 간단히 결정함으로써 기밀 비트를 추출할 수 있다. 따라서, 위의 예에서 출력 값의 1의 개수는 홀수이므로 원래의 기밀 비트인 1이 정확하게 추출된다.

2.3 다치 디더 화상에 기밀 데이터 숨기기

기존의 방식[9]에서는 다치 오차 확산법을 이용하여 기밀 데이터를 다음과 같이 숨기고 있다. 먼저, l개의 계조값 $L_k(k=0,\cdots,l-1)$에 대해서 식(3)과 같이 2개의 그룹 G_1, G_2를 정의한다.

$$\begin{aligned}G_1 &= \{L_k | k=0,2,\cdots,l-2\}\\ G_2 &= \{L_k | k=1,3,\cdots,l-1\}\end{aligned} \tag{3}$$

단, $(L_0<L_1<\cdots<L_{l-1})$



(a) 원 화소값 (b) 디더 과정의 예(주목화소가 55인 경우) (c) 결과 디더 화상

그림2. 오차 확산법의 예

0과 1의 기밀 비트를 나타내기 위해서 G_1의 계조값은 0에, G_2의 계조값은 1에 각각 대응시킨 후, 길이가 m인 기밀 비트 계열 $S=\{s_i \mid i=0,1,\cdots,m-1\}$, $s_i \in \{0,1\}$의 1비트를 $n+1$번째 화소마다 숨기는 방식이다. 상세한 알고리즘은 다음과 같다.

[단계1] n번째 화소까지 다치 디더링 수행

오차 확산법을 이용하여 n개의 화소에 디더링을 수행한다. 이때, 기밀 비트를 숨기기 위하여 n개의 출력 계조값의 계열을 B라고 한다. 기밀 비트 s_i를 숨기기 위해서 계열 B의 계조값 L_k를 G_1과 G_2에 따라 0과 1로 구성된 계열 B'로 변환한다.

[단계2] 함수 f의 출력값 결정

합성 함수 f는 기밀 비트 s_i와 B'를 인수로 하는 함수 $f(s_i, B')$는 2치화 방식과 마찬가지로 1의 개수가 짝수가 되도록 0 또는 1을 조절하기 위한 함수이다. 따라서, 1의 개수가 짝수이면 함수 f는 0을 출력하게 되고, 반대의 경우에는 1의 값을 출력하게 된다.

[단계3] 계조값의 선택

2치화 방식과 달리 계조값의 선택은 $n+1$번째 원 화소값과 오차가 최소가 되는 계조값을 출력한다. 따라서, 함수 f의 출력값이 0이면 G_1 중에서 최소 오차의 값을 선택하여 $n+1$번째의 계조값으로 출력하게 된다. 반대로 함수 f의 출력값이 1이면 G_2 중에서 선택한다.

예를 들어, 5치화를 수행하는 경우, 계조값 $L_k=\{0,64,128,192,255\}$에 대해서 다음과 같이 그룹화한다.

$$G_1=\{0,128,255\},\quad G_2=\{64,192\}$$

이와 같은 그룹에 대해서, 그림4와 같이 $n=4$라 하고 [단계1]에서 디더되어 출력된 계열 $B=G_1G_2G_2G_2$에 대해서 B'로 변환한 후, 숨기고자 하는 비트 s_i에 대해 함수 f의 출력값을 결정하고, $n+1$번째의 계조값을 선택함으로써 비트 s_i를 숨기게 된다.

숨겨진 비트의 추출은 디더된 화상으로부터 $n+1$번째까지의 계열 B'를 구하여 1의 개수가 짝수이면 0으로, 홀수이면 1로 복호한다. 따라서, 그림4의 예에서는 $B'=01110$이므로 1의 개수가 홀수로서 숨겨진 비트는 1임을 알 수 있다.

기존의 2치와 다치 디디링을 이용한 기밀 데이터의 합성법은 항상 $n+1$번째의 화소값이 변하게 되므로 화상 내에 일정한 패턴이 발생되는 단점이 있다. 따라서, 이 점을 개선하기 위한 새로운 방식을 3장에 기술한다.

3. 제안방식

3.1 2치 디더 화상을 위한 합성법

일정한 패턴이 발생되는 기존의 방식을 개선하기 위하여 두 가지의 개선방식을 제안한다. 먼저, 제안

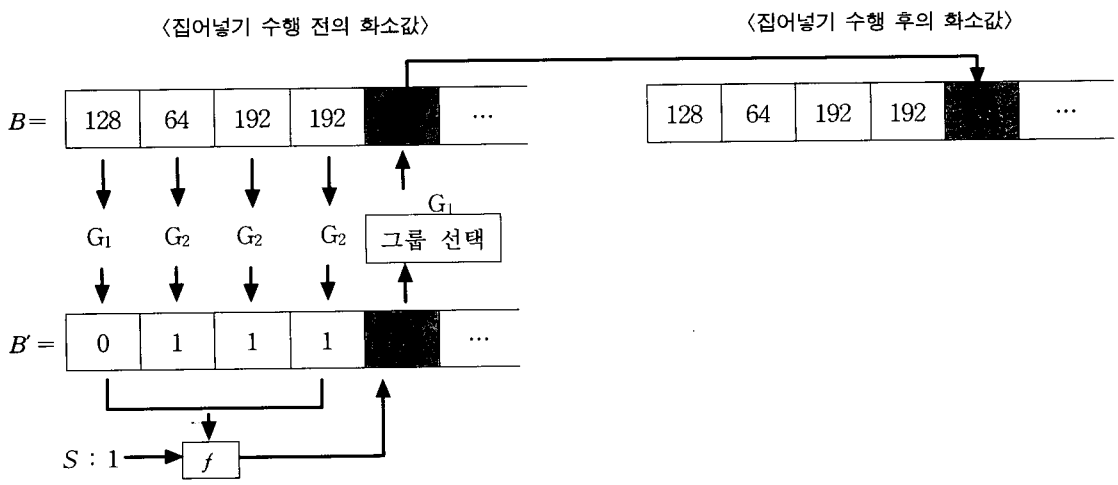


그림4. 기밀 비트 합성의 일 예

방식 I 은 0 또는 1의 값이 k개 이상 연속하고 값이 변경되는 변환지점에 기밀 정보를 숨기게 된다. 기밀 정보를 숨기기 위해 연속되는 런의 길이 k를 숨기고자 하는 비트 s의 값에 따라 홀수화/짝수화를 시키게 된다. 홀수화/짝수화를 위해 변경되는 부분은 변환 지점으로 $k+1$번째 화소가 된다. 즉, 숨기고자 하는 비트 s에 따라 식(4)와 같이 $k+1$번째 화소값을 변경한다.

$$\begin{cases} \text{런의 길이 } k\text{를 짝수화 , } s=0\text{인 경우} \\ \text{런의 길이 } k\text{를 홀수화 , } s=1\text{인 경우} \end{cases} \quad (4)$$

예를 들어, 그림5와 같이 디더된 계열은 5개의 변환 지점이 존재한다. 이때, $k=4$로 설정한 경우, 위치 5, 12에서 기밀 데이터를 숨기게 된다. 1의 런의 길이가 4이고 기밀 비트가 '0'인 경우 1의 개수가 짝수이므로 위치 5의 화소값은 기밀 비트와 같기 때문에 변경되지 않는다. 그러나, 위치 12에서의 기밀 비트는 '1'로 홀수화 되어야 함으로 위치 12의 화소값은 '1'로 변경된다.

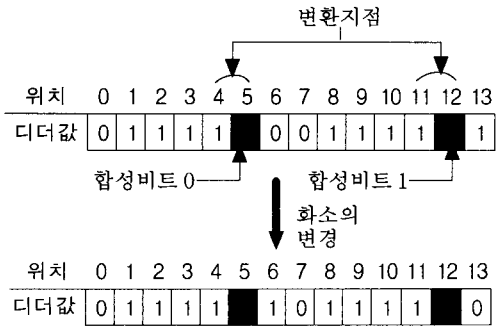


그림5. 제안방식I의 합성 원리

기밀 비트의 추출은 런의 길이 $k=4$이면 변환 지점을 포함하여 k의 값이 홀수인지 짝수인지를 판단하여 홀수이면 1, 짝수이면 0으로 복호하면 된다.

그러나, 이 방법에는 예외적인 상황이 발생한다. 즉, 그림5와 같이 비트 계열을 변경한 후 기밀 비트를 추출하는 경우 위치 12의 변환지점에서 복호가 불가능하게 된다. 이것은 원 비트 계열의 '1'의 런의 길이가 4이고 기밀 비트가 '1'인 경우에는 위치 12의 값이 1로 변경되었지만, 13번째의 값이 '1'로써 추출시에는 원래의 변환 지점인 12를 확인하지 못하게 된다. 따라서, 이것을 방지하기 위해서 변경하고자 하는 위치인 $k+1$번째와 $k+2$번째의 화소값을 동시에 변경해야 한다. 즉, 위의 예에서 위치 12와 13의 값이 서로 동일하게 되지 않도록 $k+2$번째 화소값을 그림6과 같이 변경시켜 복호 오류를 해결한다.

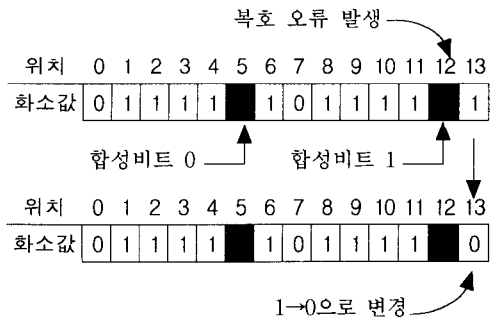


그림6. 복호 오류 방지책

제안방식 I 은 기존의 방식과 달리 고정된 n을 이용하지 않기 때문에 일정한 패턴은 발생하지 않게 된다. 그러나, 화상에 따라 숨길 수 있는 기밀 데이터의 길이가 달라지므로 기밀 데이터를 숨기기 위해서는 사전에 런의 길이를 확인해야 하는 단점이 있다. 그러므로, 주어진 화상에 고정된 길이의 기밀 데이터를 숨기기 위해 그림7과 같이 $3\times m$의 블록을 이용하는 방식 II를 제안한다.

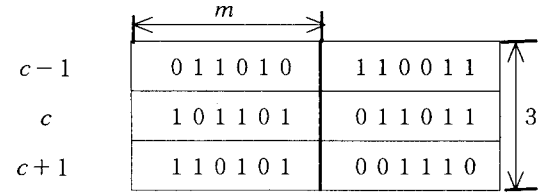


그림7. $3\times m$의 블록

제안방식 II는 중앙의 행 c를 중심으로 2비트의 기밀 정보에 따라 각각 상·하의 행 $c-1$, $c+1$에서의 '1'의 개수를 표1과 같이 짝수화/홀수화한다.

표1. 홀수화/짝수화에 의한 기밀 정보의 합성

기밀 비트		1의 개수	
		c과 $c-1$	c과 $c+1$
0	0	짝수화	짝수화
0	1	짝수화	홀수화
1	0	홀수화	짝수화
1	1	홀수화	홀수화

복호 시에는 c와 $c-1$, c와 $c+1$에 나타나는 1의 개수를 구하여 그 개수가 짝수인지 홀수인가에 따라서 표1에 대응되는 기밀 비트를 추출하게 된다. 여기서 홀수/짝수를 정확하게 판단하기 위해서 중앙의 행 c의 화소값은 변경하지 않아야 한다. 또한, 변경시킬 화소값을 설정하는데 있어서 블록의 가운데를 기준으로 그림8과 같이 $c-1$ 행은 왼쪽 방향의 화소, $c+1$ 행은 오른쪽 방향의 화소를 선택한다.

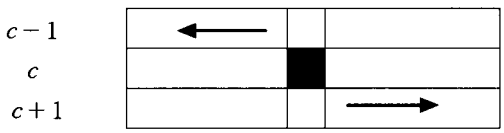


그림8. 합성 위치 선택 방법

3.2 다치 디더 화상을 위한 합성법

기존의 다치화상을 이용한 방법은 앞에서 기술한 단점 이외에도 화소값의 변경시에 주변화소간의 상관을 고려하지 않기 때문에 기밀 데이터의 합성에 의해 시각적으로 화질이 열화된다. 따라서, 일정한 패턴이 발생하지 않으면서 화질의 열화를 줄일 수 있는 새로운 방식을 제안한다.

제안 방식은 기존의 방식과 동일하게 n개의 화소까지 오차 확산법을 이용하여 디더링을 수행한다. 기존의 방식은 2개의 그룹으로 나누어 0과 1의 계열을 구성하여 기밀 비트를 숨기지만 제안 방식은 그룹을 정의하지 않고 출력된 계조값의 빈도수를 이용한다.

[단계1] 빈도의 계산

길이가 n인 출력 계조값 계열 B내에서 각 계조값 L_k의 빈도 C_k를 계산한다.

[단계2] 기밀 데이터 숨기기

빈도 C_k가 최대인 L_k에 대하여 C_k가 짝수인지 홀수인지를 판단하여 기밀 비트를 숨긴다. 기밀 비트의 값이 '0'이고 C_k가 홀수이면, C_k를 짝수가 되도록 계열 B내에서 L_k와의 오차가 최소가 되는 계조값을 L_k로 변경한다. 반대로 기밀 비트의 값이 '1'이고 C_k가 짝수이면 C_k가 홀수가 되도록 계조값을 변경하여 기밀 비트를 숨긴다.

예를 들어, $n=4$이고 $l=5$인 경우 $L_k=\{0,64,128,192,255\}$, $k=0,\cdots,l-1$에 대해서 출력 계조값 계열 B가 {128, 64, 128, 128}이면 B내에의 L_k의 빈도 C_k는 표2와 같이 계산된다.

표2. 계조값의 빈도

k	L_k	C_k
0	0	0
1	64	1
2	128	3
3	192	0
4	255	0

이 예에서 $L_2=128$일 때 최대 빈도를 가지며 $C_2=3$으로 홀수가 된다. 여기에서 숨기고자 하는 비트가 '0'인 경우에는 C_2를 짝수가 되도록 128과 최소 오차를 갖는 계조값인 64를 128로 변경한다. 따라서, 변경된 계조값의 계열 B'는 {128, 128, 128, 128}이 된다. 반대로 비트가 '1'인 경우에는 이미 최대 빈도를 가지는 128의 빈도는 홀수이므로 계열 B가 그대로 출력되어진다.

숨겨진 기밀 비트는 최대 빈도를 갖는 계조값의 빈도가 홀수인지 짝수인지를 판단하여 간단하게 추출된다. 즉, 위의 예에서는 변경된 계조값이 {128, 128, 128, 128}로 최대 빈도 수는 짝수가 되므로 숨겨진 비트의 값은 '0'임을 알 수 있다. 반대로 '1'의 경우에도 홀수인지를 판단하여 비트 값을 알게 된다. 이때, 최대 빈도수를 가지는 계조값이 여러 개가 존재하는 경우에는 최대 빈도수를 가지는 계조값 중에서 임의로 하나를 선택하여 다른 계조값으로 변경하여 최대 빈도수를 조정한다. 단, 변경시 차가 최소가 되도록 계조값은 선택하여 변경한다.

제안방식은 원래의 긴 계열에 대해 하나 정도의 계조값이 변경되어도 인간의 시각으로는 인식할 수 없음을 이용한 것으로 n에 대해 변경되는 화소의 위치가 일정한 기존의 방식에 비해 변경되는 계조값의 위치가 계열 B의 구성에 따라 일정하지 않게 된다. 따라서, 일정한 패턴이 발생되지 않으며 기밀 정보를 알아내려는 제3자의 공격에 대해서도 견고하게 된다. 또한 제안방식은 주사선 방향으로 기밀 정보를 숨기지 않고 2차원 블록으로 화상을 분할하여 기밀

정보를 숨기도록 확장할 수 있다. 확장된 방식은 주변화소간의 상관을 고려할 수 있기 때문에 보다 양호한 화질을 얻을 수 있다.

4. 시뮬레이션 및 결과

각 제안방식의 유효성을 알아보기 위해 그림9의 원 화상 Lenna(크기 256×256, 256레벨)을 이용하여 기존의 방식[8]과 제안방식을 구현하여 그 성능을 비교하였다. 먼저, 기밀 데이터를 숨기지 않고 각각 2치와 다치 오차 확산법으로 디더링만 수행한 화상을 그림10에 나타내었다.

2치 화상에 대해 기존 방식, 제안방식 I 과 방식 II로 각각 800비트의 임의의 기밀 데이터를 합성한 결과를 그림11에 나타낸다.

그림11의 결과에서 800비트의 기밀 데이터를 숨기는 경우에는 기존방식과 제안방식들의 차이를 시각적으로 인식할 수 없다. 그러나, 보다 많은 기밀정보를 숨기는 경우, 기존의 방식은 앞에서 지적한 바와 같이 사선 모양의 패턴이 생김을 그림12로부터 알 수 있다.

위와 같은 사선 모양의 패턴이 발생하는 이유는 그림13(a)와 같이 고정된 간격 n에 따라 삽입위치가 랜덤하지 않기 때문이다. 그러나, 그림13(b),(c)와 같이 제안방식 I, II는 n 자체는 고정이지만 삽입되는 위치는 삽입할 때마다 달라지기 때문에 그 위치가 랜덤하게 된다. 따라서, 제안방식에 의한 기밀정보의 삽입시에 더욱 효과적인 방법이라고 할 수 있다.

제안방식 I 은 화상 내의 화소값이 변하는 지점에서 최대 두 개의 화소값을 변경하여 기밀 데이터를 숨기기 때문에 화상의 성질에 따라 숨길 수 있는 기밀 데이터의 양은 제한된다. 기밀 데이터의 양을 조절할 수 있는 적절한 런의 길이 k의 선택이 필요하다. 그러나, 제안방식 II는 블록에 항상 2비트의 기밀정보를 숨길 수 있으며, 블록 내에서 제안방식 I 을 적용하거나 또는 화상의 성질을 고려하여 상·하 행

그림9. 원 화상 Lenna

(a) 2치 디더 화상

(b) 다치 디더 화상

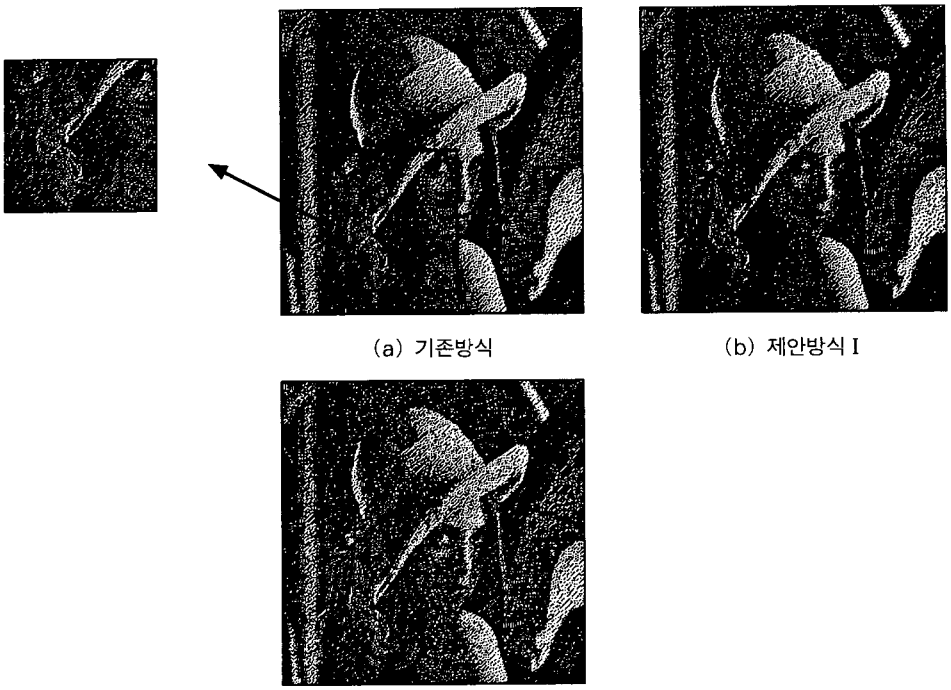
그림10. 디더된 화상

(a) 기존방식

(b) 제안방식 I

(c) 제안방식 II

그림11. 2치 디더 화상에 800 비트 합성



(a) 기존방식 (b) 제안방식 I

(c) 제안방식 II

그림12. 2치 디더 화상에 2,400 비트 합성

(a) 기존 방식 (b) 제안방식 I (c) 제안방식 II

그림13. 기밀정보 삽입 위치의 표시(2치)

에서 은닉 위치를 선택한다면 더 좋은 결과를 얻을 수 있을 것으로 기대된다.

다치 화상을 위한 제안방식은 각각 800비트, 4,000 비트의 임의의 기밀 데이터를 숨긴 화상과의 SNR을 표3에 나타내었다.

표3에서 제안방식은 주사선 방향으로 기밀 정보를 숨기는 방법이다. 기존의 방식과 제안방식은 숨기는 기밀 정보의 길이에 따라 n의 값이 변하게 된다. 여기에서 기밀 정보의 길이로 화상의 크기를 나누어서 n의 값을 구하게 된다. 확장방식은 주사선 방향이 아니라 블록으로 화상을 분할하는 경우로 블록의 크기도 역시 화상의 크기와 기밀 정보의 길이에 따라 결정된다. 2치 화상과 마찬가지로 적은 양의 기밀 정보를 숨기는 경우에는 그림14과 같이 일정한 패턴이 생기지 않는다.

그러나, 기밀 정보의 양이 증가할수록 그림15에

표3. 합성후의 SNR

(a) 800 비트 합성

방식 \ 화상	Lenna	Girl
디더링 화상	18.216	17.647
기존방식	18.154	17.595
제안방식	18.097	17.626
확장방식(블록)	18.224	17.688

(b) 4,000 비트 합성

방식 \ 화상	Lenna	Girl
디더링 화상	18.216	17.647
기존방식	17.650	17.196
제안방식	18.054	17.764
확장 방식(블록)	18.216	17.858

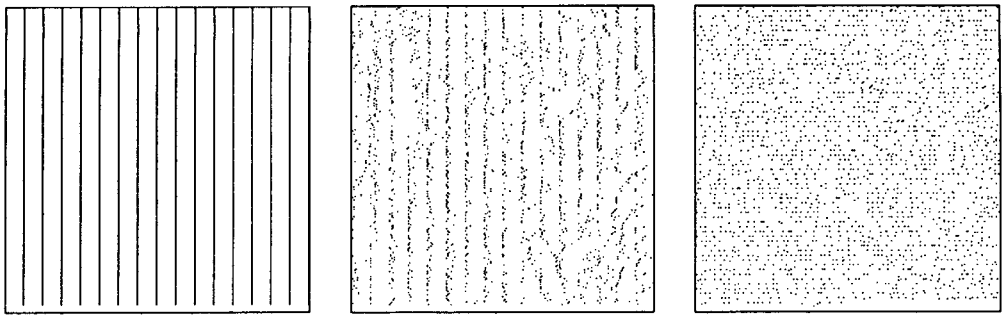
(a) 기존방식 (b) 제안방식Ⅱ (c) 제안방식Ⅱ

그림14. 다치 디더 화상에 800 비트 합성

(a) 기존방식 (b) 제안방식Ⅰ

(c) 제안방식Ⅱ

그림15. 다치 디더 화상에 4,000 비트 합성



(a) 기존방식 (b) 제안방식 I (c) 제안방식 II

그림16. 기밀정보의 삽입 위치의 표시(다치)

나타난 바와 같이 수직선 모양의 일정한 패턴이 발생하지만, 제안방식에서는 그러한 패턴이 발생되지 않으며 또는 2차원 블록으로 화상을 분할하여 적용하는 경우가 시각적으로 더 양호한 화질을 제공한다.

역시 그림16과 같이 삽입 위치가 제안방식이 기존의 방식에 비하여 랜덤함을 알 수 있다.

5. 결 론

본 논문에서는 농담화상에 오차 확산법을 적용시켜 각각 2치화상과 다치화상에 기밀 정보를 숨기는 화상 심층암호를 제안하고 그 유효성을 확인하였다. 제안방식은 기본적으로 0과 1의 기밀 데이터에 대해서 계조값의 홀수화/짝수화를 수행하여 기밀 정보를 숨기는 방법이다. 2치화상에 기밀 데이터를 숨기기 위한 제안방식 I 은 연속되는 런의 길이를 이용하여 화소값이 변하는 지점의 화소값을 변경하고, 방식 II 는 블록을 설정하여 상·하 행의 상관을 고려하여 화소값을 변경한다.

다치 화상을 위한 방식은 상대적으로 빈도가 높은 계조값을 갖는 계조의 빈도를 홀수화/짝수화 함으로써 기밀 데이터를 숨긴다. 이 방법은 기존의 방식에 비해 화상의 성질을 고려하기 때문에 양호한 화질을 제공할 뿐만 아니라, 기밀 데이터의 양이 많아짐에 따라 일정한 패턴이 발생하는 문제점을 개선할 수 있었다.

최근 멀티미디어 데이터의 저작권 보호를 위한 하나의 해법으로써 많은 연구가 이루어지고 있는 디지털 워터마킹(digital watermarking) 기법은 심층암호의 개념에서 출발한다. 따라서, 본 논문에서 제안한 방식에 대해서 암호의 개념을 이용하여 더욱 안전하게 기밀 데이터를 숨기는 방법을 고려한다면 저작권 보호를 위한 방법으로도 이용 가능하다. 이러한 점에서 본 논문의 향후 연구과제는 컬러화상에 대하여 기밀 데이터를 숨길 수 있는 방법에 대한 연구와 이것을 디지털 워터마킹에 적용하는 것을 들 수 있다.

참 고 문 헌

[1] R.Andersion and F.A.P.Peticolas, "On the Limits of Steganograpy", IEEE JSAC, Vol.41, No.7, pp.474-481, 1998

[2] P.Wayer, Disappearing Cryptography, AP professional, 1996

[3] B.Pfitzmann, "Information Hiding Terminology", in Information Hiding, Springer Lecture Notes in Computer Science, Vol.1147, pp.347-350, 1996

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

[5] L.M.Marvel et al., "Reliable Blind Information Hiding for Images", in Information Hiding, Springer Lecture Notes in Computer Science, Vol.1525, pp.48-61, 1998

[6] C.Cachin, "An Information-Theoretic Model for Steganograpy", in Information Hiding, Springer Lecture Notes in Computer Science,

Vol.1525, pp.306-318, 1998

[7] S. Craver, "On Public-Key Steganography in the Presence of an Active Warden", in Information Hiding, Springer Lecture Notes in Computer Science, Vol.1525, pp.355-368, 1998

[8] S.Koide, T.Ogihara, Y.Kaneda, "A Data Embedding Method and the Mean Density Approximation Method", Tech. Report of IEICE, IE95-122, pp.7-14, 1992(in Japanese)

[9] K.Oka, K.Matsui, "Embedding Signature into a Hardcopy of Dithered Image", Trans. of IEICE, D-II, Vol.J80-D-II, No.3, pp.820-823, 1997(in Japanese)

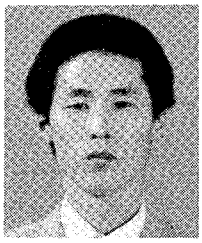
[10] R.Crane, A Simplified Approach to Image Processing, pp.153-171, Prentice Hall PTR, 1997

박 영 란

1996년 한국방송통신대학교 전자계산학과 졸업(이학사)
1998년 부경대학교 대학원 전산정보학과 (이학석사)
메일 주소 : <parkyr@unicorn.pknu.ac.kr>
관심분야 : 정보보안

이 혜 주

1994년 부산수산대학교 전자계산학과 졸업(이학사)
1997년 부경대학교 전자계산학과 (이학석사)
1997년~현재 부경대학교 전자계산학과 박사과정 재학 중
관심분야 : 멀티미디어 압축, 암호학 응용, 화상 처리 등



박 지 환

1984년 경희대학교 전자공학과 졸업(공학사)
1987년 일본국립전기통신대학 정보공학과(공학석사)
1990년 일본요코하마국립대학 전자정보공학과(공학박사)
1990년~1996년 부산수산대학교 전자계산학과 전강, 조교수, 부교수
1994년~1996년 일본동경대학 생산기술연구소 객원연구원
1996년~현재 일본동경대학 생산기술연구소 협력연구원
현재 부경대학교 전자계산학과 부교수
관심분야 : 멀티미디어 압축, 암호학 응용, 오류제어부호 등