情報保護學會論文誌
第16卷 第2號, 2006. 4

모듈러 특성을 이용한 공간영역 기반의 심층암호

박 영 란†, 신 상 욱‡
부경대학교

Steganographic Method on Spatial Domain Using Modular Characteristic

Young-Ran Park†, Sang-Uk Shin‡
Pukyong National University

요 약

화상을 이용한 심층암호는 화상에 숨긴 비밀 메시지를 전송하기 위한 비밀 통신의 한 방법이다. 디지털 화상에 비밀 메시지를 은닉시키기 위해서 엄폐화상은 은닉 알고리즘에 의해 변경이 되며, 그 결과 은닉화상이 생성된다. 송신자는 의미 없는 일반적인 엄폐화상에 비밀 메시지를 숨긴 은닉화상을 수신자에게 전송한다. 본 논문에서는 화상의 연속 두 화소간의 차분과 비밀 양자화 범위를 이용하여 비밀 메시지를 은닉하는 공간 영역 기반의 심층암호 기법을 제안한다. 특히, 제안 방식은 삽입용량을 증가시키기 위해 모듈러 연산을 이용한다. 제안 방식은 모듈러 연산을 수행함으로써 기존의 관련 방식[6]보다 비밀 메시지의 삽입용량을 평균 60% 정도 더 증가시킬 수 있었다.

ABSTRACT

Image steganography is a secret communication method used to transmit secret messages that have been embedded into an image. To accommodate a secret message in a digital image, the original cover image is modified by the embedding algorithm. As a result, a stego image is obtained. The sender hides the secret message in a cover image that has no meaning, and then transmits the stego image to the receiver. In this paper, we propose a steganographic method based on spatial domain to embed a secret message using a difference value of two consecutive pixels and a secret quantization range. Especially, we use the modular operation for increasing of insertion information. Through experiments, we have shown that the proposed method has much more payload capacity, average 60 percent, than some existing methods by using modular operation.

Keywords : *Data Hiding, Steganography, Image Processing, Information Security*

Ⅰ. 서 론

컴퓨터 보급 및 인터넷 사용자의 증가로 인해 대부분의 정보 획득은 네트워크를 통해서 이루어지고, 텍스트, 이미지, 오디오 및 비디오 등은 디지털 데이터로 표현이 가능하다. 그러므로 정보화 사회에서 많은 사람들은 디지털 데이터를 이용한 통신이 빈번해졌다. 그러나 이러한 발달의 역기능으로 발생하고 있는 문제는 정보보호에 관한 것이다. 따라서 새로운 문제로 떠오르는 것이 디지털 통신에서의 데이터 보안, 디지털화 된 콘텐츠의 소유권에 관한 저작권 보호, 디지털 콘텐츠를 이용한 비가시적인 통신 등이 활발히 연구되고 있다[1].

접수일: 2006년 2월 3일; 채택일: 2006년 3월 21일
† 주저자 : rani@mail1.pknu.ac.kr
‡ 교신저자 : shinsu@pknu.ac.kr

심층암호(steganography)는 비가시적인 통신 기법으로 그리스어로 "덮어 쓴다"는 의미를 가진다. 이것은 많은 정보의 존재를 몰래 숨기는 방법으로 통신 채널에서 기밀 정보를 암호화하는 기술이다. 컴퓨터 기반의 화상을 이용한 심층암호는 디지털 화상에서 데이터 보안을 제공하는 데이터 은닉의 한 방법이다. 목적은 제3자가 인지하지 못하도록 디지털 화상에 비밀 메시지를 숨겨서 전달하기 위한 것이다[2],[3].

한편, 화상에서 심층암호를 수행할 경우, 화상의 공간 영역(spatial domain)에서 화소의 값을 변경하여 비밀정보를 삽입하거나 또는 화상을 주파수 영역(frequency domain)으로 변환한 다음 계수의 조작으로 삽입한다.

공간 영역에서 삽입을 하는 대표적인 방법이 LSB(Least Significant Bit) 치환 방법이다[3]. 이 방법은 은닉화상의 화질이 좋고 삽입용량이 많으며, 알고리즘이 간단하다는 장점을 가진다. 그러나 모든 화소에 삽입되는 데이터의 양이 동일하므로 많은 양의 데이터를 삽입하면 화질이 부자연스러워 비밀정보의 존재를 쉽게 파악할 수 있게 된다. 따라서 이는 제3자로부터 의심을 받아 공격의 대상이 되기 쉽다[2]. 최근 발표된 공간영역 기반의 심층암호 기법들은 단순한 LSB 치환 방법의 단점을 보완하는데 많은 노력을 기울이고 있다. 엄폐화상의 어떤 화소가 윤곽 영역(edge area)에 속해 있는지 평탄영역(smooth area)에 포함하는지에 따라 화소마다 삽입의 양을 달리하는 방법들이 많이 발표되고 있다[4-6].

본 논문에서는 256 회색조 엄폐화상에 비밀 메시지를 삽입하는 방법이다. 엄폐화상에 대해서 연속된 2개의 화소 단위로 블록을 나누고, 한 블록 내의 두 화소간의 차분을 계산한다. 비밀 메시지의 은닉은 계산된 차분에 따라 비밀 양자화 범위를 참조하여 두 화소의 값을 조정함으로써 수행이 된다. 특히, 제안 방식은 모듈러 연산을 이용하여 비밀 메시지의 삽입용량을 증가시킬 수 있다. 제안 방식의 우수함을 평가하기 위해 다양한 화상을 대상으로 실험을 했으며, 그 결과 기존의 관련 연구에 비해 월등히 많은 양을 삽입함에도 불구하고 화상의 화질이 저하되지 않는 결과를 얻을 수 있었다.

본 논문의 구성은 2장에서 관련 연구를 소개하고, 3장에서는 제안 방식의 구체적인 내용을 기술하며, 4장은 기존의 방식과 제안 방식에 대해서 실험한 결과를 보이고, 마지막 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

일반적으로 화상의 구성은 전경(fore ground)인 윤곽영역(edge area)과 배경(back ground)이 되는 평탄영역(smooth area)으로 이루어져 있다. 따라서 윤곽영역의 화소 값은 그 주변의 화소 값들과 차이가 크지만, 평탄영역의 화소 값은 대체로 그 이웃 화소들과 유사한 값을 가진다.

화상에서 어떤 화소가 윤곽영역의 화소인지, 평탄영역의 화소인지를 구분하는 화상처리 기법들이 많지만, 아주 간단한 방법은 특정 화소를 중심으로 근접해 있는 화소들과의 차분을 계산해서 윤곽영역 또는 평탄영역으로 판단할 수도 있다. Wu의 방식[6]은 연속된 두 화소간의 차분을 이용하여 비밀정보를 은닉하는 방법으로써, 이들은 암호에서 비밀 키의 역할에 해당하는 양자화 범위를 이용한다.

2.1. 비밀 양자화 범위의 생성

양자화 범위는 그 간격에 따라 삽입용량과 비가시성이 달라진다. 즉, 구간을 나눌 때 범위의 간격을 넓게 하면 삽입용량을 많지만 은닉화상의 화질의 열화가 크게 되는 반면 범위의 간격을 좁게 하면 은닉화상의 화질은 좋지만 삽입용량이 적어지므로 적절한 간격의 조절이 필요하다.

양자화 범위의 생성을 구체적으로 살펴보면, 우선 엄폐화상을 겹치지 않도록 연속된 두 개의 화소 단위로 블록을 나눈다. 두 화소 값 g_i와 g_{i+1}에 대하여 차분 d를 식(1)과 같이 계산한다.

$$d = g_{i+1} - g_i \tag{1}$$

256 계조의 회색조 화상에서 차분 d의 범위는 -255에서 +255 사이가 될 것이며, 차분 d가 0에 가까운 값이라면 두 화소는 평탄 영역에 포함되는 화소를 뜻하고, -255 또는 +255에 근접한 값이라면 윤곽 영역에 포함되는 화소를 의미한다.

식(1)에서 구해진 d의 절대 값(0 ~ 255)을 이용하여 연속된 양자화 범위 $R_k(k=1,2,...,n)$로 분할을 한다. 양자화 범위 R_k는 1에서 n까지 인덱스로 할당되며, R_k의 상한과 하한의 경계 값을 각각 u_k

와 l_k로 표기한다. 첫 번째 인덱스의 하한 값 l_1은 0이 되고, 마지막 인덱스의 상한 값 u_n은 255가 될 것이다.

R_k의 양자화 범위는 $u_k - l_k + 1$이 되며, 각 범위는 2의 누승을 취한다. [그림 1]은 양자화 범위의 일예를 나타낸 것이다.

상한/하한 값	l_1 u_1	l_2 u_2	⋯	l_n u_n
차분의 절대 값	0~3	4~11	⋯	192~255
범위간격	← 4 →	← 8 →	⋯	← 64 →

그림 1. 양자화 범위의 구간 간격 분할

2.2 비밀정보의 은닉

비밀정보를 삽입하기 위하여 앞 절에서 기술한 차분 d의 절대 값이 비밀 양자화 범위에서 어느 구간에 해당하는지 알아야 한다. 그리고 비밀정보의 비트 열 S에서 식(2)에서 계산된 m개의 비트를 선택하여 십진수로 변환시킨 b를 해당 k번째 범위의 하한 값 l_k을 이용하여 식(3)과 같이 계산한다. 이것이 새로운 차분 d'가 된다.

$$m = \log_2(u_k - l_k + 1) \tag{2}$$

$$d' = \begin{cases} l_k + b, & \text{if } d \geq 0 \\ -(l_k + b), & \text{if } d < 0 \end{cases} \tag{3}$$

결국, 엄폐화상의 두 화소 g_i와 g_{i+1}의 차분인 d를 새로운 차분 값 d'로 변경하여 은닉화상의 두 화소 g_i'와 g_{i+1}'를 식(5)에 의해서 얻는다. 식(5)에서 w는 식(4)의 계산 결과이다.

$$w = d' - d \tag{4}$$

$$(g_i', g_{i+1}') = \begin{cases} (g_i - \dfrac{w+1}{2},\ g_{i+1} + \dfrac{w-1}{2}), \\ \quad \text{if } d = odd \wedge w = odd \\ (g_i - \dfrac{w-1}{2},\ g_{i+1} + \dfrac{w+1}{2}), \\ \quad \text{if } d = even \wedge w = odd \\ (g_i - \dfrac{w}{2},\ g_{i+1} + \dfrac{w}{2}), \\ \quad \text{if } w = even \end{cases} \tag{5}$$

[그림 2]는 Wu 알고리즘의 비밀정보 은닉 절차를 표현한 것이다. [그림 2]의 예를 살펴보면, 어떤 블록의 두 화소 값이 97과 114이라면 차분 $d = +17$이 된다. 그런 다음 차분 d의 절대 값을 이용하여 비밀 양자화 범위에서 해당되는 범위를 찾는다. 그러면 16에서 31까지의 네 번째 범위로 삽입 비트수는 4비트가 된다. 비밀정보 비트열 중에서 4비트를 읽어 십진수로 변환하면 13이 되고, 이것을 해당 범위의 하한 값인 16과 더하면 새로운 차분 $d' = +29$가 된다. 이 새로운 차분과 원래의 차분과의 차이인 +12를 두 화소에 식(5)에 의해 배분을 시키면 각각 91과 120이 된다.

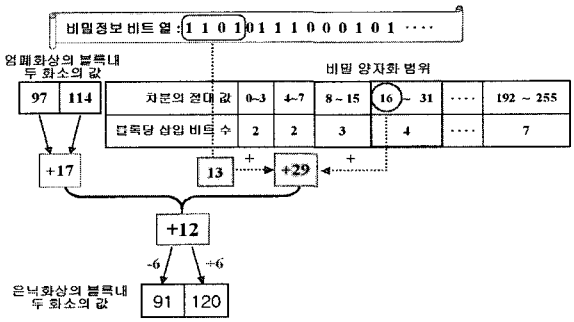

그림 2. Wu 알고리즘을 이용한 은닉 절차

2.3 비밀정보의 추출

엄폐화상에 비밀정보를 삽입하여 생성된 은닉화상을 전달받은 수신자는 은닉화상의 한 블록인 두 화소 값 g_i'와 g_{i+1}'간에 차분 d^* 식(6)에 의해 계산한다. 그런 다음, 비밀 양자화 범위를 참조하여 해당 k번째 범위를 찾고, 그 범위의 하한 값인 l_k를 이용하여 식(7)에서처럼 b를 계산하고, 이것을 m개 이진 비트 열로 변환하면 비밀정보를 추출할 수 있다.

$$d^* = g_{i+1}' - g_i' \tag{6}$$

$$b = \begin{cases} d^* - l_k, & \text{if } d^* \geq 0 \\ -d^* - l_k, & \text{if } d^* < 0 \end{cases} \tag{7}$$

[그림 2]를 예로 설명하면, 은닉화상의 블록 내 두 화소 값은 91과 120이다. 두 화소 값에 대해 차분 d^*을 계산하면 +29가 된다. 이 차분 d^*가 비밀 양자화 범위에서 어느 범위에 속하는가를 찾아 하한 값을 확

인하면 16이라는 것을 알 것이고, 그런 다음 차분 +29에서 하한 값 16을 빼면 13이라는 것을 알 수 있다. 이렇게 계산된 13을 해당 범위의 삽입 비트 수인 4비트로 이진수로 변경하면 '1101'을 추출할 수 있다.

Ⅲ. 제안 방식

제안 방식은 비밀 메시지의 삽입용량을 증가시키기 위하여 모듈러 연산(modular operation)을 이용하였다. 그 결과, 기존의 Wu 방식과 비교했을 때, 양자화 범위의 구성에 따라 최대는 약 두 배정도의 비밀정보를 삽입할 수 있었다. 즉, 블록 당 삽입 가능 비트 수가 식(8)과 같다.

$$m = \lfloor \log_2(u_k - l_k +) \rfloor + 1 \tag{8}$$

3.1 양자화 범위의 구간 간격 분할시 개선점 제시

다양한 종류의 회색조 화상들을 대상으로 연속 두 화소간의 차분을 분석한 결과, 차분의 범위가 [그림 3]과 같이 분포하는 것을 실험으로 알 수 있었다.

[그림 3]에서 보면, -50에서 +40 사이의 값들이 거의 대부분을 차지하고 있다는 것을 실험으로 알 수 있었다. 따라서 비밀 양자화 범위의 구간 간격을 나눌 때, 이러한 특징을 고려해야 할 것이다. 엄폐화상에 대하여 연속된 두 화소간의 차분을 계산하여 그 값의 범위를 히스토그램으로 확인한 후, 이를 참조하여 비밀 양자화 범위를 나누면 보다 효과적일 것이다. 양자화 범위는 송신자와 수신자가 서로 공유하며, 수신자는 비밀 메시지를 복원할 때 키(key)로 이용된다. 즉, 양자화 범위 분할의 간격을 알아야만 비밀 메시지를 정확하게 복원할 수 있다. 따라서 비밀 양자화 범위는 암호 기법에서의 비밀키(secret key)로 취급될 수 있다.

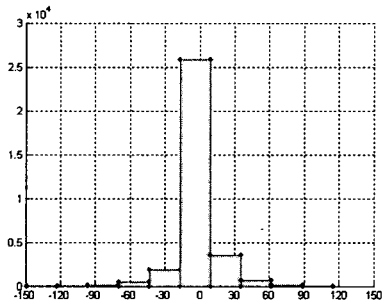

그림 3. 두 화소의 차분 값 분포 (Lena,256*256)

비밀 양자화 범위의 간격 분할은 은닉화상의 화질을 고려하여 차분의 출현 빈도가 높은 것에 대해서는 간격을 좁도록 분할하고, 빈도가 낮은 것은 간격을 넓도록 분할하면 보다 우수한 결과를 얻을 것이라 생각된다.

3.2 은닉화상 생성 방법

제안 방식은 삽입 데이터의 용량을 보다 더 증가시킬 수 있도록 개선하였으며, 그 결과 비밀 양자화 범위의 분할에 따라 Wu의 기법보다 최대 약 두 배의 데이터를 삽입할 수 있었다.

자세한 은닉 과정을 살펴보면, 먼저 엄폐화상을 겹치지 않게 연속된 두 개의 화소 단위로 블록을 나눈다. 처리 순서는 주사선 방향으로 한 블록씩 수행한다. 한 블록내의 두 화소 g_i와 g_{i+1}사이의 차분 값 d를 식(1)과 같이 계산하고, 해당 k번째 범위를 선택한 후, 삽입 가능한 비트 수 m을 확인한 다음 비밀 메시지 S 중에서 $m+1$비트를 읽어서 십진수 변환한 값 b를 구한다.

$$b' = b \bmod (u_k - l_k + 1) \tag{9}$$

$$c = \lfloor b/(u_k - l_k + 1) \rfloor \tag{10}$$

구해진 b를 식(9)와 같이 모듈러 연산을 이용하여 나머지인 b'을 계산하고 또, 식(10)을 적용하여 몫인 c를 각각 계산한다. 여기서, $(u_k - l_k + 1)$은 2^m과 동일한 값이다.

$$d' = \begin{cases} l_k + b', & \text{if } d \geq 0 \\ -(l_k + b'), & \text{if } d < 0 \end{cases} \tag{11}$$

은닉화상을 구성할 새로운 차분 값 d'는 식(11)을 이용하여 계산한 후, 삽입 처리는 식(4)와 식(5)를 수행하여 은닉화상의 화소 값 g_i' 와 g_{i+1}'을 얻는다. 이렇게 삽입 처리를 수행한 뒤, 복호 시 오류가 발생하지 않도록 하기 위해 식(10)의 c값에 따라 식(12)과 같이 되도록 g_i' 와 g_{i+1}'을 조절하여 최종적으로 은닉화상의 화소 값을 얻는다.

$$g_i' = \begin{cases} even, & \text{if } c = 0 \\ odd, & \text{if } c = 1 \end{cases} \tag{12}$$

이와 같은 과정을 엄폐화상의 전체 블록에 대하여 수행하면 은닉화상이 생성된다. 제안 방식의 삽입 예를 [그림 4]에서 표시하였다.

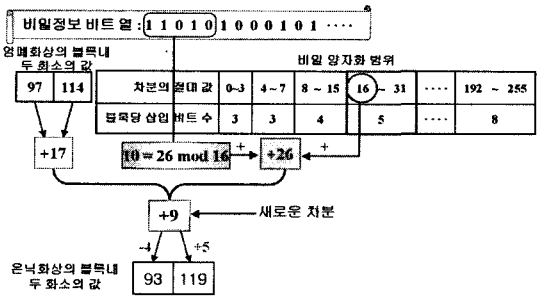

그림 4. 제안 방식의 은닉 절차

[그림 4]를 살펴보면, 두 화소의 차분 값 d의 절대 값 17은 4번째 범위인 하한 값 16에서 상한 값 31의 범위이다. 따라서 삽입 가능 비트 수 m이 4비트이지만, 제안 방식에서는 $m+1$인 5비트를 읽어 십진수로 변환하면 26이 된다. 삽입 데이터 26을 식(9)와 식(10)을 이용하면 $b^{'}=10$과 $c=1$로 각각 계산된다. 새로운 차분 값 $d^{'}$을 구하기 위하여 식(11)을 적용하면 +26이 되고, 최종적으로 원래의 차분 d와 새로운 차분 $d^{'}$의 차이만큼을 두 화소에 고루 배분한다. 그러나 제안 방식은 추출 시 오류의 발생을 방지하기 위해 식(12)를 적용하면 은닉화상의 블록 내 두 화소 값 93과 119를 얻을 수 있다.

3.3 비밀정보의 추출 방법

추출 방법은 은닉화상의 블록내의 두 화소 값 g_i^*와 g_{i+1}^*에 대해서 차분 값 d^*를 계산한 후, 식(13)과 식(14)를 이용하여 삽입된 서브 비트 열 b를 추출해낸다.

$$b^{'}=\begin{cases} d^*-l_k, & \text{if } d^*\geq 0 \\ -d^*-l_k, & \text{if } d^*<0 \end{cases} \tag{13}$$

$$b=\begin{cases} b^{'}+2^m, & \text{if } g_i^*=even \\ b^{'}, & \text{if } g_i^*=odd \end{cases} \tag{14}$$

[그림 4]를 예로 들면, 은닉화상에서 블록의 화소 값 93과 119에 대한 차분 값 d^*는 +26이 되고, 이것의 절대 값을 계산하여 해당 범위를 찾는다. 그럼 4번째 범위인 하한의 값 16에서 상한의 값 31인 범위임을 알 수 있고, 삽입 가능 비트 수가 5비트라는 것도 확인할 수 있다. 따라서 식(13)을 이용하면 $b^{'}=10$이 계산되고, 식(14)를 이용하면 $b=26$이 된다. 계산된 b를 5비트의 이진수로 표현하면 기밀 비트를 추출할 수 있다.

Ⅳ. 실험 및 결과

앞에서 기술한 Wu 방식과 제안 방식에 대하여 각각 실험한 결과를 보인다. 실험 화상은 모두 256 회색조 화상이며, 크기는 256×256, 범위 분할의 레벨 수는 6개, 13개, 22개로 나누어 실험을 하였다. 그 결과 은닉화상의 시각적인 확인과 엄폐화상과 은닉화상과의 정량적인 계산 PSNR을 계산해 본 결과 Wu 방식과 제안 방식 모두 우수함을 확인할 수 있었다. 하지만, 삽입 비트 양은 제안 방식이 Wu 방식보다 훨씬 많이 삽입되었다.

[그림 5]와 [그림 6]은 Wu 방식과 제안 방식을 범위 분할의 레벨 수 13과 22일 경우에 대해 각각 실험한 결과를 나타낸 것이다. [그림 5]와 [그림 6]에서 알 수 있듯이 엄폐화상과 은닉화상들은 시각적으로 구별하기 어렵다.

(a) 엄폐화상

(b) 은닉화상 (Wu 방식)

(c) 은닉화상 (제안 방식)

그림 5. 실험 화상(Lena, 13 분할)

(a) 엄폐화상

(b) 은닉화상 (Wu 방식)

(c) 은닉화상 (제안 방식)

그림 6. 실험 화상(Baboon, 22 분할)

표 1은 Wu의 방식과 제안 방식에 대해서 삽입용량과 시각적인 평가(PSNR)를 비교한 것이며, [그림 7]은 두 방식의 삽입용량을 그래프로 표현한 것이다.

표 1. Wu 방식과 제안 방식의 비교

구분	분할 레벨 수	삽입용량(bytes)		PSNR(dB)	
		Wu	제안	Wu	제안
Lena	6	13,274	17,367	38.3	38.2
	13	7,198	11,294	44.8	44.1
	22	5,322	9,418	49.9	47.6
Baboon	6	14,389	18,483	36.3	36.1
	13	9,453	13,549	42.7	42.3
	22	6,618	10,714	48.2	46.6

엄폐화상 Lena를 이용했을 때 비밀 메시지의 삽입용량을 보면 레벨 수가 6, 13, 22인 경우 에 제안 방식이 Wu 방식보다 각각 31%, 57%, 77%정도 더 삽입되었다. 따라서 제안 방식은 레벨 수가 많을수록 Wu 방식과 삽입용량의 차이는 더욱 커진다. 왜냐하면, 레벨 수가 많다는 것은 한 블록에 삽입 가능한 비트 수 m이 작아진다는 것을 의미한다. 그러므로 Wu 방식이 블록 당 m비트가 삽입 된다면, 제안 방식은 항상 1비트가 더 많은 $m+1$ 비트를 삽입할 수 있기 때문이다.

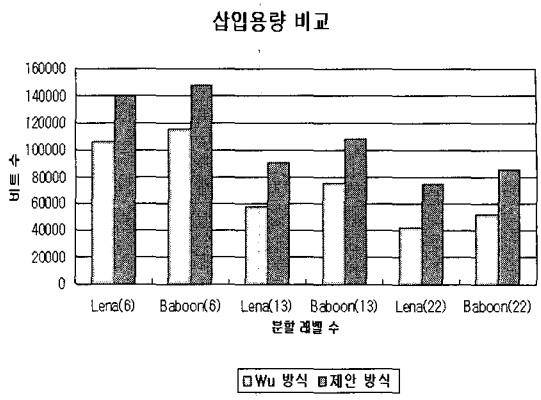

그림 7. Wu 방식과 제안 방식의 삽입용량 비교 차트

표 1에서 알 수 있듯이, 제안 방식의 삽입용량이 Wu 방식보다 훨씬 많음에도 불구하고, 분할 레벨 수가 6 또는 13일 때 두 은닉화상의 PSNR은 거의 동일하다. 그러나 레벨 수가 22인 경우, 제안 방식의 은닉화상이 2dB 정도 낮지만 PSNR이 아주 높기 때문에 특별히 단점이라 여겨지지 않는다.

V. 결 론

본 논문에서는 비밀 양자화 범위를 이용한 정보은닉의 한 방법을 제시하였다. 제안 방식은 모듈러 연산의 성질을 이용하였기 때문에 기존의 Wu 방식과 비교했을 때 화질은 비교적 동일하게 유지하면서 삽입용량을 증가시킬 수 있었다. 특히, 양자화 범위의 생성에 구간 간격을 어떻게 분할하느냐에 따라 기존의 Wu 기법보다 약 2배정도의 삽입용량을 은닉시킬 수 있다는 것을 실험을 통하여 알 수 있었다.

참 고 문 헌

[1] Neil F. Johnson, Zoran Duric and Sushil Jajodia, "Information Hiding", Kluwer Academic Publishers, 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] R.Z. Wang and C.F. Lin, "Image Hiding by Optimal LSB Substitution and Genetic Algorithm", Pattern Recogni-

tion Vol. 34, pp. 671-883, 2001.
[4] T. Zhang and X. Ping, "A New Approach to Reliable Detection of LSB Steganoraphy in Natural Image", Signal Processing Journal 83, ELSEVIER, pp. 2085-2093, 2003.
[5] X. Zhang and S. Wang, "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security", Pattern Recognition Letters, ELSEVIER, Vol. 25, pp. 331-339, 2004.
[6] D.C. Wu and W.H. Tsai, "A Steganographic Method for Images by Pixel-value Differencing", ELSEVIER Pattern Recognition Letters Vol. 24, pp. 1613-1626, 2003.

〈著者紹介〉

박 영 란 (Young-Ran Park) 준회원
1996년 2월 : 한국방송통신대학 전자계산학과 졸업
1998년 8월 : 부경대학교 전산정보학과 석사
2003년 3월~현재 : 부경대학교 정보보호학과 박사과정
관심분야 : 스테가노그라피, 디지털 영상처리, 디지털 영상인증, 디지털 워터마킹, 핑거프린팅

신 상 욱 (Sang-Uk Shin) 준회원
1995년 2월 부경대학교 전자계산학과 졸업
1997년 2월 부경대학교 대학원 전자계산학과 석사
2000년 2월 부경대학교 대학원 전자계산학과 박사
2000년 4월~2003년 8월 : 한국전자통신연구원 선임연구원
2003년 9월~현재 : 부경대학교 전자컴퓨터정보통신공학부 조교수
관심분야 : 암호이론, 정보보호, 이동통신 정보보호