Journal of Korea Multimedia Society Vol. 8, No. 3, March 2005(pp. 379-388)

비밀 양자화 범위를 이용한 화상 심층암호 응용

박영란[†], 신상욱[††]

요 약

화상 심층암호(image steganography)는 비밀 정보를 화상에 몰래 숨겨 송/수신자간에 주고받는 비밀 통신의 한 방법이다. 송신자는 특별한 의미를 갖지 않는 커버 화상(cover image)에 비밀 정보를 삽입한 스테고 화상을 수신자에게 전달한다. 수신자는 송신자에게 받은 스테고 화상(stego image)에서 숨겨진 비밀 정보를 추출하여 그 내용을 확인한다. 본 논문에서는 알고리즘이 간단하면서, 심층암호의 필수 조건인 비밀 정보의 삽입용량, 스테고 화상의 비가시성, 그리고 송/수신자간의 기밀성을 모두 만족할 수 있는 기법들을 제안한다. 제안 방식은 커버 화상의 연속 두 화소간의 차분 값과 양자화 범위를 이용하여 비밀 정보를 은닉시킨다. 특별히, 스테고 화상의 비가시성을 위해 커버 화상의 두 화소간의 차분 값에 따라 삽입 비트수를 다르게 한다. 또한, 기밀성을 위해서는 비밀 양자화 범위를 사용하여 제3자에 의해 비밀 정보가 해독되는 것을 방지할 수 있다. 제안 방식은 기존의 방식보다 화질을 개선시키기 위하여 범위의 상한값을 이용하였고, 삽입용량을 증가시키기 위해 특정 화소에 대해서는 삽입 처리를 중복으로 수행하였다. 실험을 통하여 기존의 방식과 제안 방식을 비교하였고, 그 결과 제안 방식의 유효성을 확인할 수 있었다.

Applications of Image Steganography Using Secret Quantization Ranges

Young-Ran Park[†], Sang-Uk Shin[††]

ABSTRACT

Image steganography is a secret communication scheme to transmit a secret message, which is embedded into an image. The original image and the embedded image are called the cover image and the stego image, respectively. In other words, a sender embeds a secret message into a cover image and transmits a stego image to a receiver, while the receiver takes the stego image, extracts the message from it, and reads the message. General requirements for steganography are great capacity of secret messages, imperceptibility of stego images, and confidentiality between a sender and a receiver. In this paper, we propose a method for being satisfied with three requirements. In order to hide a secret message into a cover image safely, we use a difference value of two consecutive pixels and a secret quantization range. The former is used for the imperceptibility and the latter for the confidentiality. Furthermore, the number of insertion bits is changed according to the difference value for the imperceptibility. Through experiments, we have shown that our method is more good quality of stego images than many other related methods and increases the amount of message insertion by performing dual insertion processing for some pixels.

Key words: Information Hiding(정보은닉), Steganography(심층암호), Information Security(정보보호), Image Processing(화상처리)

※ 교신저자(Corresponding Author) : 박영란, 주소 : 부산광역시 남구 대연3동 599-1번지(608-737), 전화 : 051)620-6392, E-mail : podosongei@hanmail.net
접수일 : 2004년 6월 14일, 완료일 : 2004년 9월 13일

[†] 준회원, 부경대학교 정보보호학과 박사수료
[††] 정회원, 부경대학교 전자컴퓨터정보통신공학부 전임강사
(E-mail : sushin@pknu.ac.kr)

1. 서 론

텍스트, 이미지, 오디오 및 비디오 등은 디지털 데이터로 표현이 가능하다. 인터넷 응용들의 급격한 증가는 사람들을 디지털 세계로 이끌어가고, 디지털 데이터를 통해 통신이 빈번해졌다. 그러므로 새로운 문제로 떠오르는 디지털 통신에서의 데이터 보안, 디지털화된 컨텐츠의 소유권에 관한 저작권 보호, 디지털 컨텐츠를 이용한 비가시적인 통신 등이 활발히 연구되고 있다.

스테가노그라피(steganography)라는 용어는 그리스어에서 유래되었으며 덮어쓴다는 의미이다.

이것은 많은 정보의 존재를 몰래 숨기는 방법으로 통신 채널에서 기밀 정보를 암호화하는 기술이다[1,2].

화상 심층암호(image steganography)는 제3자가 인지하지 못하도록 디지털 화상에 비밀 정보를 비가시적으로 숨겨서 전달하기 위한 것이다. 주로 비밀 정보는 자막, 설명문, 또 다른 이미지, 제어신호 또는 비트 스트림 형태로 표현할 수 있는 것들이어야 한다. 비밀 정보는 은닉 처리를 하기 전에 압축이나 암호화가 될 수도 있다[3-5].

한편, 화상 심층암호에서는 원 화상을 커버 화상(cover image), 비밀 정보가 삽입된 화상을 스테고 화상(stego image)이라는 용어를 사용하며, 다음과 같은 일반적인 조건을 만족해야 한다[6].

- **비가시성(invisible)**

비밀 정보를 삽입한 스테고 화상과 원 화상을 비교했을 때 시각적인 이질감을 주지 않아야 한다. 즉, 화질의 열화가 발생하지 않도록 비밀 정보를 은닉시켜야 한다.

- **삽입량(capacity)**

송신자와 수신자 사이에 보다 많은 정보들을 교환하기 위하여 가능하면 하나의 화상 컨텐츠에 비밀 정보를 많이 삽입할 수 있는 방법을 생각해야 한다.

- **기밀성(confidential)**

가령 제3자가 비밀 정보의 은닉을 알아차렸다 하더라도 그 내용을 확인할 수 없도록 비밀 키(secret key)를 이용하여 비밀 정보의 내용을 복호하지 못하도록 해야 한다.

본 논문의 제안 방식은 256 레벨을 갖는 그레이 커버 화상에 비밀 정보를 삽입하는 방법으로써, 커버 화상에 대해서 연속된 2개 또는 3개의 화소를 한 단위 블록으로 분할한다. 블록 내의 화소간의 차분 값을 계산하고, 그 차분 값에 따라 비밀 양자화 범위를 참조하여 비밀 정보를 숨기는 방식이다. 차분 값을 이용하는 이유는 어떤 블록이 평탄 영역(smooth area)인지 윤곽 영역(edge area)인지에 따라 삽입용량을 달리하기 때문이다. 즉, 평탄 영역에는 작은 양을, 윤곽 영역에는 많은 양의 기밀 데이터를 삽입한다.

제안 방식의 우수함을 평가하기 위해 다양한 화상을 대상으로 실험을 했으며, 그 결과 기존의 관련 연구에 비해 비가사성 및 삽입용량의 측면에서 특히 유효성을 확인할 수 있었다.

본 논문의 구성은 2장에서 기존의 관련 연구에 대해서 소개하고, 3장에서는 두 가지 제안 방식을 구체적으로 기술하며, 4장은 기존 방식과 제안 방식에 대해서 실험 및 분석 결과를 보이고, 마지막 5장에서 결론을 제시한다.

2. 관련 연구

그레이 값을 가지는 화상에서의 심층암호 기법들은 일반적으로 화소 값의 LSB에 기밀 데이터를 숨기는 경우가 많다[7,8]. 그 이유는 계산 및 알고리즘이 간단하고, 많은 양의 데이터를 비가시적으로 삽입할 수 있다는 장점을 가지기 때문이다. 또한, LSB 삽입 방법은 화상의 특징을 고려하지 않고 모든 화소에 동일한 양의 데이터를 삽입한다. 하지만, 대부분의 화상은 윤곽 영역(edge area)과 평탄 영역(smooth area)으로 구분되어지며, 윤곽 영역의 화소 변화는 시각적으로 둔감하지만 평탄 영역은 아주 민감하다. 따라서, 기존의 관련 연구인 WT 방식[9]에서는 화상의 한 화소가 윤곽 또는 평탄 영역인지에 따라 삽입 데이터의 양을 달리 하는 기법을 제안하였다. WT 방식이란 2003년 Wu와 Tsai가 제안한 것으로 이하에서는 WT 방식으로 칭한다.

2.1 화소의 차분에 대한 비밀 양자화 범위 분할

WT 방식은 주어진 커버 화상을 겹치지 않도록 연속된 두 개의 화소 단위로 블록을 나누고, 블록내의 두 화소 값 g_i와 g_{i+1}을 이용해서 차분 값 d를 식(1)과 같이 계산한다.

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

따라서, 256 그레이 화상에서 차분 값 d의 범위는 -255~+255의 값을 가질 것이며, 차분 값 d가 0에 근접하면 두 화소의 값이 거의 비슷하므로 평탄 영역의 화소를 의미하고, -255 또는 +255에 근접한 값이면 두 화소 값의 차이가 크므로 윤곽 영역의 화소를 의미한다.

한편, d의 절대 값(0~255)을 이용하여 다수의 연속된 범위 $R_k(k=1, 2, \cdots, n)$로 분할을 한다. 이러한 범위는 인덱스 1 에서 n까지 할당되며, R_k 범위의 하한값과 상한값을 각각 l_k와 u_k로 표기한다. 그러므로 l_1은 0이고, u_n은 255가 되며, 특정 범위 R_k의 간격은 $u_k - l_k + 1$ 이 된다. 범위 분할의 예를 그림 1에 나타내었다. 그림 1의 범위 분할 예를 살펴보면, 0에 가까운 값들은 범위의 간격을 좁게 설정하고, 255에 가까운 값들은 범위의 간격을 넓게 설정하고 있다. 즉, 해당 블록에서 두 화소의 차분 값이 작으면 기밀 데이터도 적게 삽입하고, 두 화소의 차분 값이 크면 그 블록에는 기밀 데이터를 많이 삽입하기 위해서 간격의 차이를 두는 것이다. 결국 블록내의 두 화소의 차분 값을 이용하여 비밀 양자화 범위에서 해당 범위를 찾은 후 해당 블록에 삽입할 비트 개수를 선택하는 것이다. 구체적인 삽입 및 추출 방법을 다음 절에서 기술한다.

2.2 비밀 정보 삽입과 추출 방법

화상의 블록에서 두 화소간의 차분 값에 따라 블록마다 삽입되는 데이터의 양은 각각 다르다. 즉, 두 화소 간 차분의 절대 값이 비밀 양자화 범위에서 어느 범위에 해당하느냐에 따라 삽입 비트 수는 달라진다. 한 블록의 삽입 비트 수 m은 해당 k번째 범위내의 하한 값 l_k와 상한값 u_k에 의해 식(2)와 같이 계산된다.

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

식(2)에서 계산된 m은 비밀 정보 비트열인 S 중에서 해당 블록에 삽입할 서브 비트열의 개수를 의미한다. 기밀 데이터를 삽입하기 위해서 해당 k번째

범 위	R_1		R_2		⋯	R_3	
범위의 간격	← 4 →		← 8 →		⋯	← 64 →	
차분의 절대 값	0	3	4	11	⋯	192	255
하한값/상한값	l_1	u_1	l_2	u_2	⋯	l_n	u_n

그림 1. 비밀 양자화 범위의 분할 예

범위의 하한값 l_k와 그 범위에 대응되는 m개의 서브 비트 열을 10진수로 변환한 b를 더하여 새로운 차분 값 d'를 식(3)과 같이 계산한다.

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

여기서, d는 앞에서 언급한 커버 화상에서 블록을 구성하는 두 화소간의 차분 값을 의미하며, 결국 기밀 데이터 삽입 방법은 커버 화상에서 원래의 차분 값 d를 새로운 차분 값 d'가 되도록 변경함으로써 스테고 화상을 획득한다. 그러므로 d와 d'간의 차이 값 w를 식(4)와 같이 계산하고, 이것을 이용하여 식(5)와 같이 커버 화상의 화소 값 g_i와 g_{i+1}를 새로운 화소 값 g'_i와 g'_{i+1}로 변경시킨다. 이러한 과정을 전체 블록에 대해 실행을 하면 비밀 정보가 삽입된 스테고 화상을 얻을 수 있다.

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

$$(g'_i, g'_{i+1}) = \begin{cases} (g_i - \frac{w+1}{2}, g_{i+1} + \frac{w-1}{2}), \\ \quad d = odd,\ w = odd \\ (g_i - \frac{w-1}{2}, g_{i+1} + \frac{w+1}{2}), \\ \quad d = even,\ w = odd \\ (g_i - \frac{w}{2}, g_{i+1} + \frac{w}{2}), \\ \quad w = even \end{cases} \tag{5}$$

한편, 삽입처리를 수행하기 전에 비밀 정보가 삽입된 스테고 화상의 경계값 문제를 예방하기 위하여 식(6)을 이용하여 해당 블록의 두 화소 값을 먼저 검사해야 한다. 만약 식(6)과 같이 수행한 결과, 블록의 두 화소 값이 0~255의 범위를 벗어나면 삽입처리에서 제외시킨다. 식(6)에서 $e = u_k - d$ 이다. 이 과정은 비밀 정보 추출과정에서도 확인해야 한다.

$$(g'_i, g'_{i+1}) = \begin{cases} (g_i - \frac{e+1}{2}, g_{i+1} + \frac{e-1}{2}), \\ \quad d = odd,\ e = odd \\ (g_i - \frac{e-1}{2}, g_{i+1} + \frac{e+1}{2}), \\ \quad d = even,\ e = odd \\ (g_i - \frac{e}{2}, g_{i+1} + \frac{e}{2}), \\ \quad e = even \end{cases} \tag{6}$$

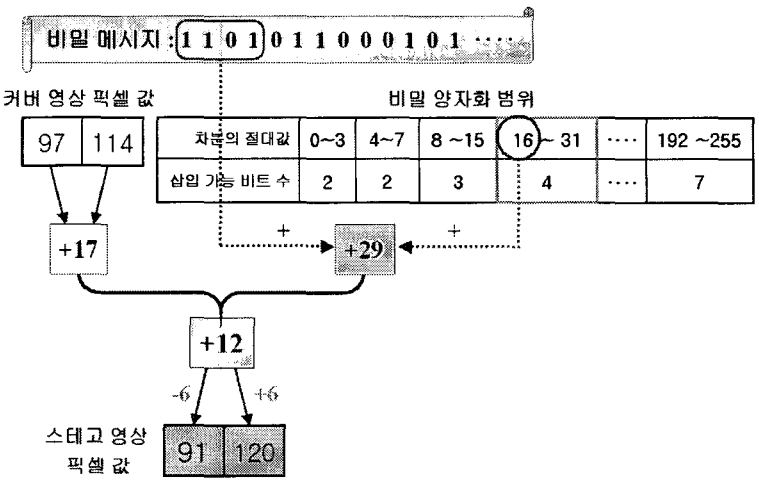


그림 2. WT 방식의 삽입 과정

WT 방식의 구체적인 삽입 예를 그림 2에 나타내었다.

그림 2에서 커버 화상의 두 화소 (97, 114)의 차분은 +17이 되고 차분의 절대 값을 이용하여 범위를 선택하면 4번째 범위인 하한값 16에서 상한값 31인 범위가 된다. 따라서 삽입가능 비트 수는 4비트가 되므로 비밀 정보 비트 열에서 4비트인 "1101"을 십진수로 변환한 13을 해당 범위의 하한값인 16과 더하여 새로운 차분 값 +29를 얻을 수 있다. 결국 스테고 화상의 화소 값은 커버 화상의 원래 차분 값 +17과 기밀 비트를 삽입한 새로운 차분 값 +29와의 차이인 +12를 두 화소에 각각 분배를 한다. 그러므로 그림 2의 경우, 스테고 화상의 두 화소 값은 (91, 120)이 된다.

추출 방법은 스테고 화상의 블록 내 두 화소 g'_i와 g'_{i+1}에 대해서 차분 값 d^*를 계산하고, 이것을 삽입 과정에서처럼 송/수신자가 공유하고 있는 비밀 양자화 범위를 참조하여 식(7)에 의해 b를 복원한 후, m개의 서브 비트 열로 변환하면 된다. 이러한 추출 과정을 스테고 화상의 전체 블록에 대하여 수행하면 비밀 정보 S를 확인할 수 있다.

$$b = \begin{cases} d^* - l_k & \text{for } d^* \geq 0 \\ -d^* - l_k & \text{for } d^* < 0 \end{cases} \quad (7)$$

그림 2와 같이 스테고 화상의 두 화소 값이 (91, 120)일 때, 두 화소의 차분을 계산하면 +29가 되고, 차분의 절대 값을 이용하여 비밀 양자화 범위에서 해당 범위를 확인해 보면, 4번째 범위인 하한값 16에서 상한값 31인 범위를 찾게 되고, 이것을 차분 값 29에서 하한값 16을 뺀 13을 4비트의 이진 비트 열로 변환하면 최종적으로 기밀 비트 "1101"을 추출하게 된다.

3. 효율적인 화상 심층암호의 응용 기법

제안 방식은 2장에서 언급한 WT 방식의 비밀 양자화 범위를 적용하여 비가시성과 삽입용량을 증가시키는데 목적으로 접근하였고, 이에 효율적인 두 가지 기법을 제안한다.

한편, 다양한 그레이 화상들을 대상으로 연속된 두 화소간의 차분 값을 분석한 결과 차분 값의 범위는 그림 3에서처럼 -50에서 +50사이의 값들이 대부분을 차지하고 있다는 것을 알 수 있었다. 따라서

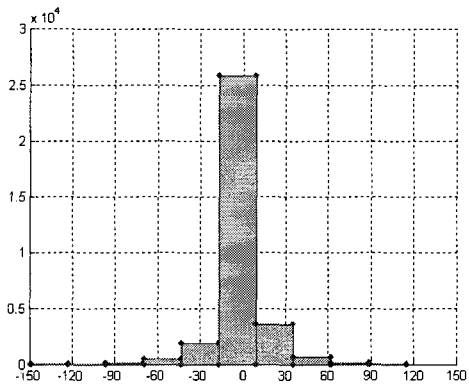


그림 3. 커버 화상의 차분 값 분포(Lena, 256×256)

제안 방식에서는 비밀 양자화 범위의 구간을 분할할 때, 이러한 점을 고려하여 설정하였다.

또한, 삽입과 추출과정에서 경계 값 문제에 대한 예외처리는 기존의 WT 방식을 따른다.

3.1 제안 방식 I

본 절에서는 기존의 WT 방식과 동일한 삽입용량을 은닉시키면서 스테고 화상의 화질이 보다 더 우수한 결과를 얻을 수 있는 방법을 제안한다.

WT 방식에서는 삽입 데이터의 값을 해당 범위의 하한값 l_k에 더하여 새로운 차분 d'을 구하고, 커버 화상의 두 화소 간 차분 값 d를 새로운 차분 값인 d'가 되도록 두 화소 값을 조정한다. 즉, d와 d'간의 차이만큼을 두 화소의 값에 가감함으로써 분배한다. 그러므로 WT 방식은 커버 화상의 화소 값과 스테고 화상의 화소 값과의 최대 오차가 $(u_k - l_k + 1)/2$ 가 된다. 따라서 범위의 간격이 좁은 경우에는 큰 문제가 되지 않지만, 범위 간격이 넓은 경우에는 최대 오차 또한 커지므로 화질의 열화가 발생한다.

제안 방식 I은 커버 화상의 화소 값과 스테고 화상의 화소 값과의 최대 오차를 WT 방식의 절반밖에 되지 않는 $(u_k - l_k + 1)/4$ 로 감소시킬 수 있는 방법이다.

◉ 제안 방식 I의 삽입 방법

제안 방식 I의 삽입 처리는 두 화소 g_i와 g_{i+1}에 대해서 차분 값 d을 계산하고, 차분의 절대 값으로 비밀 양자화 범위에서 해당 범위를 선택한다. 해당 범위의 삽입 비트 수 m만큼의 비밀 정보 비트 열을 십진 데이터 값 b로 변경한 후, 식(8) 및 식(9)에 의해서 d_{low}와 d_{upper}를 계산한다. 또 d_{low}와 d_{upper}의 값은 d의 절대 값인 d_a와의 차분을 식(10)과 같이 계산하여 d'을 구한다.

$$d_{low} = \begin{cases} l_k + b & \text{for } d \geq 0 \\ -(l_k + b) & \text{for } d < 0 \end{cases} \tag{8}$$

$$d_{upper} = \begin{cases} u_k - b & \text{for } d \geq 0 \\ -(u_k - b) & \text{for } d < 0 \end{cases} \tag{9}$$

$$d' = Min(|d_a - d_{low}|, |d_a - d_{upper}|) \tag{10}$$

위의 과정에서 얻어진 d'을 이용하여 새로운 화소 값 g'_i와 g'_{i+1}을 식(4) 및 식(5)에 의해 계산되며, 이러한 과정을 전체 커버 화상에 대해 주사선 방향으로 실행을 하면 스테고 화상이 생성된다.

한편, 스테고 화상을 이용하여 수신자가 비밀 정보를 복원할 때 오류를 방지하기 위해 d'가 d_{low}와 d_{upper}중 어느 값을 선택했는지를 구분하기 위하여 d_{low}를 선택했을 경우는 g'_i의 값을 짝수로, d_{upper}를 선택했을 경우는 홀수가 되도록 처리를 해준다.

정리하면, 제안 방식 I은 차분의 절대 값에 따라 해당 k번째 범위를 선택하고, 삽입 비트열의 값에 대해서 선택한 범위의 하한값 l_k와 상한값 u_k를 기반으로 각각 계산, 비교한 후 커버 화상 원래의 화소 값과 오차가 작은 것을 기준으로 스테고 화상의 화소 값을 결정하여 삽입 처리를 수행한다. 삽입 방법의 일 예를 그림 4에 나타내었다.

그림 4에서 두 화소 값 (97, 114)에 대해서 식(1)을 이용하여 차분 값 +17을 구하고, 차분의 절대 값으로 비밀 양자화 범위에서 해당 범위를 찾아보면 4번째 범위의 하한값 16과 상한값 31 및 삽입 가능한 비트수가 4비트임 알 수 있다. 따라서, 비밀 정보에서 4비트를 선택해서 이것을 십진수 변환한 13을 식(8) 및 식(9)처럼 해당 범위의 하한값에는 가산을, 상한값에는 감산을 하면, 각각 +29와 +18이 된다. 이렇게 구해진 두 값과 식(10)과 같이 커버 화상의 차분인 +17과 비교해서 오차가 작은 값을 선택하면, 새로운 차분 값은 +18이 되고 이것을 원래의 차분 값과 비교해 보면 1만큼 차이가 나고, 두 화소에 분배하면 (97, 115)로서 스테고 화상의 화소 값을 얻을 수 있다.

◉ 제안 방식 I의 추출 방법

비밀 정보를 추출하는 방법은 우선, 비밀키의 역할을 하는 비밀 양자화 범위를 송신자와 수신자가 서로 공유함을 전제로 한다.

스테고 화상의 한 블록의 두 화소 값 g'_i와 g'_{i+1}을 이용하여 차분 값 d^*을 구하고, 그 차분의 절대 값을 이용하여 비밀 양자화 범위에서 해당 범위를 선택한 후, 식(11)에 의해 비밀 정보를 추출한다.

$$b = \begin{cases} d^* - l_k & \text{if } g'_i = even,\ d^* \geq 0 \\ -d^* - l_k & \text{if } g'_i = even,\ d^* < 0 \\ u_k - d^* & \text{if } g'_i = odd,\ d^* \geq 0 \\ -u_k - d^* & \text{if } g'_i = odd,\ d^* < 0 \end{cases} \tag{11}$$

그림 4를 예로 들면, 스테고 화상의 두 화소의 차분 값인 +18을 구한 다음, 두 화소 중 첫 번째 화소인 g'_i가 짝수인지 홀수인지 확인을 한다. 그림 4의 예에서는 스테고 화상의 g'_i 화소 값이 97로써 홀수이

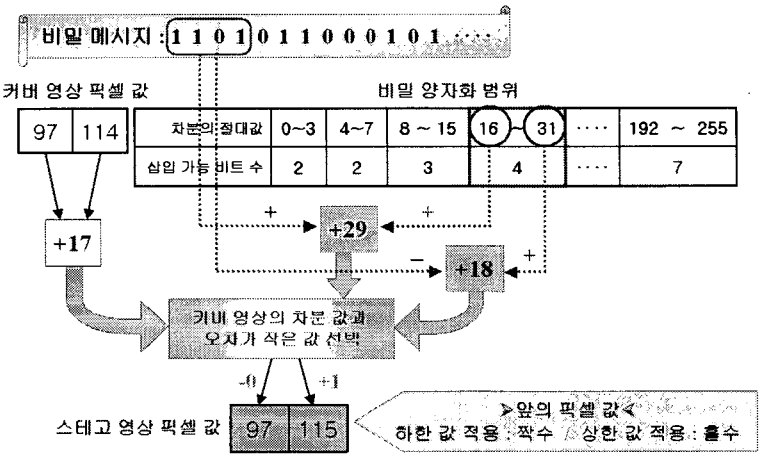


그림 4. 제안 방식 I의 삽입 과정

므로 삽입 시 기밀 데이터를 상한값에서 감산을 이용하여 삽입 처리를 했다는 것을 의미하므로 상한값 31에서 차분 18을 빼면 기밀 데이터 13을 얻게 되고 이것을 해당 범위의 삽입 가능 비트 수만큼 이진 비트 열로 변환하면 "1101"인 기밀 비트를 복호할 수 있게 된다.

3.2 제안 방식 II

제안 방식 II는 삽입용량을 증가시키기 위하여 커버 화상을 겹치지 않게 연속된 3개의 화소 단위로 블록을 나누고, 가운데 화소를 중심으로 좌·우 화소와의 차분을 각각 계산하여 비밀 정보를 은닉한다. 따라서 WT 방식은 6개의 화소로 세 번의 삽입 처리가 수행되지만, 제안 방식은 네 번의 삽입 처리를 수행하므로 삽입 데이터의 양이 WT 방식에 비해 1/4 만큼 더 증가하게 된다.

◉ 제안 방식 II의 삽입 방법

제안 방식 II의 삽입 처리 과정을 살펴보면, 먼저 커버 화상을 겹치지 않게 연속된 세 개의 화소를 하나의 블록으로 하여 전체 화상을 분할한다. 처리 순서는 주사선 방향으로 한 블록씩 수행한다.

한 블록내의 연속된 세 개의 화소 값을 각각 v_i, v_{i+1}, v_{i+2}라고 가정하면, 식(12)과 식(13)에 의해서 차분 값 d_L과 d_R을 각각 계산하고, 식(14)과 식(15)에 의해 d'_L 과 d'_R을 구한다.

$$d_L = v_{i+1} - v_i \tag{12}$$

$$d_R = v_{i+1} - v_{i+2} \tag{13}$$

$$d'_L = \begin{cases} l_{kL} + b_j & \text{if } d_L \geq 0 \\ -(l_{kL} + b_j) & \text{if } d_L < 0 \end{cases} \tag{14}$$

$$d'_R = \begin{cases} l_{kR} + b_{j+1} & \text{if } d_R \geq 0 \\ -(l_{kR} + b_{j+1}) & \text{if } d_R < 0 \end{cases} \tag{15}$$

식(14)와 식(15)에서 b_j와 b_{j+1}은 식(2)의 계산에서 얻어진 블록 내 삽입 가능한 비트 수 m개의 서브 비트 열을 십진수로 변환한 값이다. 즉, 비밀 정보 S 중에서 해당 블록에 삽입시키고자 하는 서브 비트 열의 두 값을 각각 의미한다.

원래의 차분 값 d_L과 d_R, 그리고 새로운 차분 값 d'_L과 d'_R을 이용하여 식(16)과 식(17)에서처럼 각각의 차이인 w_L과 w_R을 계산한다. 결과적으로 스테고 화상의 화소 값들의 차분 값이 d'_L, d'_R가 되도록 하기 위해서 식(18) 및 식(19)을 이용하여 r_1, r_2, r_3, r_4을 계산한다.

$$w_L = d'_L - d_L \tag{16}$$

$$w_R = d'_R - d_R \tag{17}$$

$$(r_1, r_2) = \begin{cases} v_i - \dfrac{w_L+1}{2},\ v_{i+1} + \dfrac{w_L-1}{2}, \\ \quad \text{if } w_L = odd,\ d_L = odd \\ v_i - \dfrac{w_L-1}{2},\ v_{i+1} + \dfrac{w_L+1}{2}, \\ \quad \text{if } w_L = odd,\ d_L = even \\ v_i - \dfrac{w_L}{2},\ v_{i+1} + \dfrac{w_L}{2}, \\ \quad \text{if } w_L = even \end{cases} \tag{18}$$

$$(r_4, r_3)=\begin{cases} v_{i+2}-\frac{w_R+1}{2},\ v_{i+1}+\frac{w_R-1}{2}, \\ \quad \text{if } w_R=odd,\ d_R=odd \\ v_{i+2}-\frac{w_R-1}{2},\ v_{i+1}+\frac{w_R+1}{2}, \\ \quad \text{if } w_R=odd,\ d_R=even \\ v_{i+2}-\frac{w_R}{2},\ v_{i+1}+\frac{w_R}{2}, \\ \quad \text{if } w_R=even \end{cases} \quad (19)$$

위의 식에서 계산된 값들 중 r_2와 r_3는 동일한 위치인 가운데 화소를 의미한다. 그러므로 새로운 가운데 화소 값을 얻기 위하여 r_2와 r_3의 평균값을 계산하여 새로운 가운데 화소의 값 v'_{i+1}을 먼저 결정하고, 나머지 왼쪽과 오른쪽 화소 값은 v'_{i+1}을 기준으로 각각의 차분 값이 d'_L과 d'_R가 되도록 v'_i와 v'_{i+2}의 값을 조절하면 된다. 삽입 처리의 일 예를 그림 5에 나타내었다.

그림 5에서 삽입 과정을 보면, 우선 한 블록의 세 개의 화소 값 (74, 99, 113)에서 가운데 화소 값 99를 기준으로 좌·우 화소간의 차분 값을 식(12)과 식(13)과 같이 계산하면 왼쪽의 차분 값 +25와 오른쪽의 차분 값 -14를 각각 얻을 수 있다. 그런 다음 차분의 절대 값을 이용하여 각각의 해당 범위를 찾아서 삽입 가능한 비트 수를 참조하여 왼쪽 및 오른쪽에 삽입할 비트 수만큼을 십진수로 변환한 b_j와 b_{j+1}을 식(14)과 식(15)에 의해 새로운 좌·우의 차분 값 +26과 -11을 구할 수 있다. 삽입에 따른 화소 값의 변경은 식(16), 식(17), 식(18) 및 식(19)에 의해 왼쪽을 기준으로 한다면 왼쪽 화소 값은 73을 가운데 화소 값은 99를 얻을 것이고, 오른쪽을 기준으로 한다면 가운데 화소 값은 101을 오른쪽 화소 값은 112를 얻을 것이다. 따라서 가운데 화소 값은 동일한 위치의 화소이므로 하나의 화소 값으로 표현을 하기 위해 두 값인 99와 101을 평균을 취한 값 100을 가운데 화소 값으로 결정하고, 나머지 좌·우 화소는 그 차이만큼을 조정하면 스테고 화상의 세 개의 화소 값 (74, 100, 111)을 생성할 수 있다.

◉ 제안 방식 Ⅱ의 추출 방법

추출 방법은 삽입과정을 역으로 수행하면 된다. 비밀 양자화 범위를 비밀키로 하여 스테고 화상에서 블록의 화소 값에 대해 가운데 화소를 중심으로 좌·우 화소간의 차분 값 d^*_L와 d^*_R을 각각 계산하여 식(6)을 이용하여 왼쪽을 기준으로 한번 추출하고, 또 오른쪽을 기준으로 한번 추출하면 한 블록에 삽입했던 기밀 비트를 얻을 수 있다.

그림 5를 예로 들면, 스테고 화상의 한 블록의 세 화소 값 (74, 100, 111)에 대해 가운데 화소를 중심으로 좌·우 화소간의 차분 값의 절대 값을 계산하면 왼쪽은 26을, 오른쪽 11을 얻게 되고, 이것을 이용하여 해당 범위를 각각 찾은 후, 해당 범위의 하한값을 빼주면 왼쪽은 10을 오른쪽은 3을 구하게 된다. 따라서 10과 3을 삽입 가능 비트 수만큼의 이진수로 변환하면 "1010"과 "011"로 비밀 정보를 추출할 수 있다.

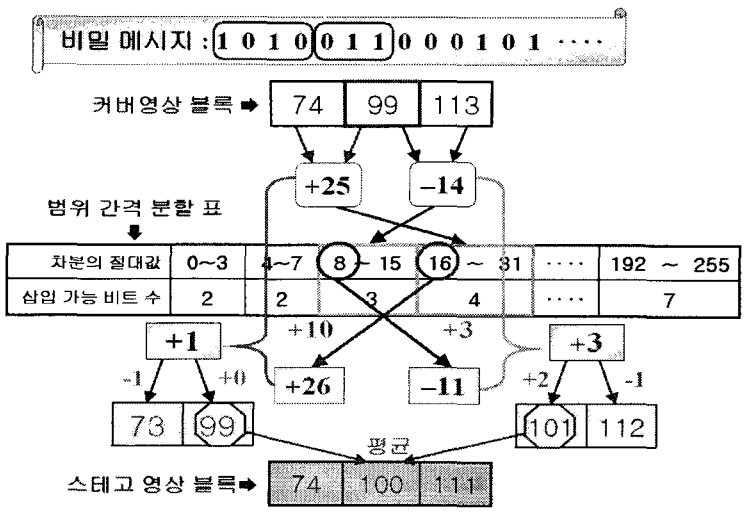


그림 5. 제안 방식Ⅱ의 삽입 과정

4. 실험 및 비교

앞에서 기술한 WT 방식과 제안 방식 I 및 제안 방식 II에 대하여 각각 실험한 결과를 보이고, 각각의 방식에 대하여 PSNR을 이용한 비가시성 평가와 삽입용량을 비교하였다.

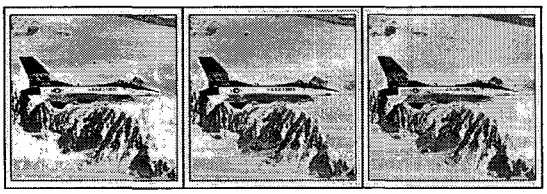
4.1 WT 방식과 제안 방식 I의 비교

실험 화상은 모두 256 그레이 화상이며, 크기는 256×256, 양자화 범위 분할 레벨은 6(8, 8, 16, 32, 64, 128) 및 레벨 13(2, 2, 4, 4, 4, 8, 8, 16, 16, 32, 32, 64, 64)으로 나누어 각각 실험한 결과를 그림 6과 그림 7에 나타내었다.

표 1은 WT 방식과 제안 방식 I의 실험 결과에 대해서 정량적인 평가를 나타낸 것이다. 여기서 알 수 있듯이, WT 방식과 제안 방식 I의 비밀 정보 삽입용량은 동일하지만, PSNR과 최대 오차를 측정한 결과 본 제안 방식 I이 우수하다는 것을 확인할 수 있다.

(a) 커버 화상 (b) 스테고 화상 (WT 방식) (c) 스테고 화상 (제안 방식 I)

그림 6. 실험 화상(Lena image, 6-level)



(a) 커버 화상 (b) 스테고 화상 (WT 방식) (c) 스테고 화상 (제안 방식 I)

그림 7. 실험 화상(Airplane image, 13-level)

표 1. WT 방식과 제안 방식 I의 수치적인 비교 분석

화상	분할 레벨수	삽입량 (byte)	PSNR(dB)		최대오차	
			WT	제안 I	WT	제안 I
Lena	6	13,274	38.29	43.93	56	22
Sailboat		13,294	38.39	44.32	31	16
Lena	13	7,198	45.50	48.16	26	15
Airplane		6,711	44.50	47.78	28	16

4.2 WT 방식과 제안 방식 II의 비교

본 절에서는 WT 방식과 제안 방식 II에 대하여 실험한 결과를 그림 8과 그림 9에 나타내었다. 실험 화상은 모두 256 그레이 화상이며, 크기는 270×270이다. 범위 분할은 그림 8은 13개의 레벨로 나누었고, 그림 9는 22개의 레벨로 나누어 각각 실험을 하였다. 그 결과 화질은 WT 방식과 제안 방식 II 모두 우수한 결과를 얻을 수 있었다. 그 측정은 식(20)의 PSNR로 하였으며, 모두 40dB 이상이므로 화질이 우수함을 알 수 있다.

(a) 커버 화상 (b) 스테고 화상 (WT 방식) (c) 스테고 화상 (제안 방식II)

그림 8. 실험 화상(Sailboat image, 13-level)

(a) 커버 화상 (b) 스테고 화상 (WT 방식) (c) 스테고 화상 (제안 방식II)

그림 9. 실험 화상(Lena image, 22-level)

비밀 양자화 범위의 간격이 동일할 경우, 삽입 비트 양은 제안 방식 II가 WT 방식보다 많은 비트들이 삽입되었음을 확인할 수 있었다. 표 2는 WT 방식과 제안 방식 II의 삽입용량과 PSNR을 비교한 것이다. 표 2를 살펴보면, 삽입용량은 제안 방식 II이 더 많지만, PSNR은 약 2dB정도 떨어진다. 하지만, 삽입용량을 고려했을 때, PSNR이 40dB 이상이므로 그다지 문제가 되지 않는다고 생각된다.

표 2. WT 방식과 제안 방식Ⅱ의 비교

구분	분할 레벨 수	삽입량(byte)		PSNR(dB)	
		WT	제안Ⅱ	WT	제안Ⅱ
Lena	13	7,869	10,469	45.91	43.42
Sailboat		7,702	10,244	46.54	44.15
Lena	22	5,852	7,795	50.43	48.19
Sailboat		5,839	7,762	50.87	48.70

5. 결 론

본 논문에서는 화상 심층암호에 관한 두 가지 응용 기법을 제시하였다.

제안 방식Ⅰ은 스테고 화상의 화질을 기존의 WT 방식보다 더욱 더 향상시키기 위해 기밀 비트를 삽입할 때, 해당 범위의 하한값과 상한값을 이용하여 커버 화상의 화소 값과 오차가 작은 값을 스테고 화상의 화소 값으로 취하였다. 이로 인해 기존의 WT 방식에 비해 오차가 절반으로 줄일 수 있어, 전체적인 화질이 좋아졌음을 실험을 통해 확인할 수 있었다.

또한, 제안 방식Ⅱ는 비밀 정보의 삽입용량을 증가시키기 위해 연속 세 개의 화소를 한 블록으로 정하고, 가운데 화소를 중복으로 수행함으로써 기존의 WT 방식보다 약 1/4정도의 비밀 정보를 더 은닉할 수 있었다.

결과적으로, 본 논문에서는 삽입 및 추출 알고리즘이 복잡하지 않으면서 비가시성, 삽입용량, 그리고 기밀성을 모두 보장될 수 있는 화상 심층암호의 응용 방법들을 제시하였다.

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, ELSEVIER*, Vol. 141, pp. 123-138, 2002.

[5] H. Noda, J. Spaulding, M.N. Shirazi, M. Niimi and E. Kawaguchi, "BPCS Steganography Combined with JPEG2000 Compression", *Proceedings of Pacific Rim Workshop on Digital Steganography(STEG)*, pp. 98-107, 2002.

[6] 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, PERGAMON*, Vol.36, pp. 2875-2881, 2003.

[7] R. Z. Wang and C. F. Lin, "Image Hiding by Optimal LSB Substitution and Genetic Algorithm", *Pattern Recognition, ELSEVIER*, Vol. 34, pp. 671-883, 2001.

[8] T. Zhang and X. Ping, "A New Approach to Reliable Detection of LSB Steganoraphy in Natural Image", *Signal Processing Journal, ELSEVIER*, Vol.83, pp. 2085-2093, 2003

[9] D. C. Wu and W. H. Tsai, "A Steganographic Method for Images by Pixel-value Differencing", *Pattern Recognition Letters, ELSEVIER*, Vol. 24, pp. 1613-1626, 2003.

박 영 란

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

관심분야 : 정보보호, 심층암호, 디지털 영상처리, 디지털 워터마킹

신 상 욱

1995년 2월 부경대학교 전자계산학과(학사)
1997년 2월 부경대학교 전자계산학과(석사)
2000년 2월 부경대학교 전자계산학과(박사)
2000년 4월～2003년 8월 : 한국전자통신연구원 선임연구원
2003년 9월～현재 부경대학교 전자컴퓨터정보통신공학부 전임강사

관심분야 : 암호 이론, 정보보호, 이동통신 정보보호