논문 16-41-03-05 The Journal of Korean Institute of Communications and Information Sciences '16-03 Vol.41 No.03
http://dx.doi.org/10.7840/kics.2016.41.3.307

암호화된 영상의 데이터 은닉 기법의 오류 개선을 위한 섭동 함수 설계

김 영 훈◆, 임 대 운*, 김 영 식°

Design of Fluctuation Function to Improve BER Performance of Data Hiding in Encrypted Image

Young-Hun Kim◆, Dae-Woon Lim*, Young-Sik Kim°

요 약

가역적 데이터 은닉은 원본 이미지에 미치는 영향 없이 임의의 데이터를 숨길 수 있는 기술이다. Zhang은 원본 영상을 암호화하고 암호화된 영상에 데이터를 은닉하는 방법을 제안하였다. 이 때 은닉된 데이터를 추출하기 위해서 먼저 암호화된 영상을 복호화하고, 복호화된 영상의 공간 상관 특성을 나타내는 섭동 함수(Fluctuation Function)를 이용한다. 본 논문에서는 은닉된 데이터를 추출 과정에서 발생하는 오류를 감소시키기 위한 섭동 함수를 제안하고 모의실험을 통해 성능을 검증하였다.

Key Words : encrypted image, image recovery, reversible data hiding, fluctuation function

ABSTRACT

Reversible data hiding is a technique to hide any data without affecting the original image. Zhang proposed the encryption of original image and a data hiding scheme in encrypted image. First, the encrypted image is decrypted and uses the fluctuation function which exploits the spatial correlation property of decrypted image to extract hidden data. In this paper, the new fluctuation function is proposed to reduce errors which arise from the process extracting hidden data and the performance is verified by simulation.

Ⅰ. 서 론

오늘날 개인정보 보호 및 컨텐츠 보호를 위해서 데이터 은닉 기술이 많은 관심을 받고 있다. 이를 위해 암호학적 데이터를 통해 데이터를 암호화하는 방식이 많이 활용되고 있지만[1-3], 이 경우 데이터가 암호화되어 있다는 사실은 알려지게 되어 데이터 트래픽 분석을 통한 추론 공격이나 암호 알고리즘에 대한 해독 시도 등 공격의 주요 목표가 될 수 있다. 또 다른 방법으로 일반적인 커버 데이터에 또 다른 데이터를 은닉하는 방법을 사용할 수 있다. 이 경우 데이터가 은닉되어 있다는 사실 자체가 숨겨지게 되기 때문에 상대적으로 공격의 대상이 될 가능성을 줄일 수 있다[4,5]. 비인가자로부터 디지털 콘텐츠를 보호하는 것은 중요한 문제이며 앞서 언급한 비밀통신의 두 가지인 암호와 데이터 은닉을 동시에 수행하여 암호화된 영상에 데

※ 본 논문은 2013년 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구입니다.(NRF-2013S1A5A2A03044362)
◆ First Author : Dongguk University Department of Information Security Code and Cipher laboratory, seoulkyh7@naver.com, 학생회원
° Corresponding Author : Chosun University, Department of Information and Communication Engineering, iamyskim@chosun.ac.kr, 종신회원
* Dongguk University Department of Information and Communication Engineering, daewoonlim@gmail.com, 종신회원
논문번호 : KICS2015-12-389, Received December 10, 2015; Revised February 22, 2016; Accepted February 23, 2016

이터를 은닉함으로써 디지털 콘텐츠를 보호하고 은닉된 데이터의 존재를 숨길 수 있다.

의료 영상이나 군의 기밀 영상과 같은 응용 분야에서 데이터 은닉은 원본 이미지를 손상시키지 않고 보존하는 가역성이 매우 중요하다. 최근 몇 년간 많은 가역적 데이터 은닉 기술이 제안되었다. 차분 확장(difference expansion)을 사용하는 가역적 데이터 은닉 기법[6], 데이터 은닉을 위한 여분의 공간을 생성하고 무손실 압축을 수행하는 기법[7], 히스토그램의 최소점을 이용하고 은닉된 데이터에 대한 화소의 그레이스케일 값을 변경하여 가역적으로 데이터를 은닉하는 기법[8], 보간법을 이용한 가역적 이미지 워터마킹 기술[9] 등이다. 암호화된 영상에 데이터를 은닉하는 것과 관련된 기법으로는 암호화된 영상의 가역적 데이터 은닉 기법[10], 사이드 매치를 이용한 향상된 가역적 데이터 은닉 기법[11] 등이 있으며, 그 외에도 비트 평면으로 나타낸 영상의 화소 값을 LSB에 대해 비트 정보를 검사하면서 무손실 압축 기법을 사용하여 은닉할 공간을 찾은 후에 데이터를 삽입하는 기법[12], 인접 화소들 간의 유사도에 기반 한 데이터 은닉[13], 예측 부호화와 히스토그램의 쉬프팅을 사용하는 가역적 데이터 은닉[14], 픽셀 차분의 히스토그램 수정에 기반하여 이진트리를 이용하는 가역적인 데이터 은닉 방법[15], 예측 부호화를 통해 생성된 하이딩 트리를 이용하는 가역적 정보 은닉 기법[16] 등도 있다. 국내에서도 동적 비트 선택을 적용하여 가역적으로 데이터를 은닉하는 기법[20], 격자 기반의 가역적 데이터 은닉 기법[21], 인접하는 화소간의 차이 값을 이용하는 개선된 가역적 데이터 은닉 기법[22], RS(Reed-Solomon) 부호를 활용한 이미지 공간상관 관계 향상을 위한 전송 기법[23] 등 많은 연구가 진행되었다. 또한, 가역적 데이터 은닉 기법의 성능을 향상시키기 위한 다양한 기술도 제안되었다[17-19].

이 중에서 Zhang은 이미지에 은닉되는 데이터 및 원본 콘텐츠를 공격자 또는 제 3자에게서 보호받을 수 있도록 암호화된 이미지에 데이터를 은닉하고 추출하는 가역적인 데이터 은닉 기법을 제안하였다.

본 논문에서는 Zhang의 방식을 개선시킨 새로운 데이터 은닉 기법을 제안한다. 제안된 방식에서는 데이터 추출 시 원본 이미지에 대한 판정을 위해 공간상관 특성을 계산할 때 사용하는 섭동 함수를 개선하여 기존에 발생하는 오류를 감소시키기 위한 섭동함수를 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 Zhang이 제안한 기존의 암호화된 영상에 대한 데이터 은닉 기법을 자세히 설명한다. 그런 후에 3장에서는 제안하는 개선된 방법을 설명할 것이다. 4장에서는 제안한 방식의 모의실험을 통해 성능을 검증한 후에 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

그림 1과 같이 기존의 암호화된 영상을 이용한 가역적 데이터 은닉 기법은 영상 암호화(Image Encryption), 데이터 은닉(Data Embedding), 영상 복호화(Image Decryption), 데이터 추출 및 영상 복구(Data Extraction & Image Recovery)의 네 단계로 구성된다. 또한, 콘텐츠 소유자(Content Owner), 데이터 은닉자(Data Hider), 수신자(Receiver)의 세 명의 사용자가 존재한다.

콘텐츠 소유자는 원본 이미지를 소유한 자로서 암호화키를 사용하여 원본 이미지를 암호화하여 암호화된 이미지를 생성하고 데이터 은닉자에게 전송한다. 데이터 은닉자는 데이터 은닉키를 사용하여 암호화된 이미지에 데이터를 은닉한 후 수신자에게 데이터 은닉키와 함께 전송한다. 원본 이미지가 완전히 암호화되어있기 때문에 데이터 은닉자는 그 내용을 알지 못하며, 은닉되는 데이터에 따라 암호화된 이미지를 일부 수정하여 데이터를 은닉한다. 수신자는 콘텐츠 소유자로부터 받은 암호화키를 사용하여 먼저, 암호화된 이미지를 복호화하며 복호화 된 이미지는 원본 이미지와 유사하다. 다음으로 데이터 은닉키를 사용하여 복호화 된 이미지로부터 삽입된 데이터를 추출하고 원본 이미지를 복구한다. 화소 변경이 없는 이미지의 공간 상관 특성을 이용하여 일부 수정되었던 이미지의 데이터는 원래의 값으로 복구되고 은닉된 데이터가 추출된다. 이는 가역적인 방식으로 특정 데이터를 은닉하고 추출하는 기술로, 암호화 시 동기식 스트림 암호를 사용한다. 이미지를 암호화한 후에 데이터를 은닉시키고 데이터를 추출한 이후에 이미지를 복호화하는 일반적인 방법과는 달리 Zhang의 기법에서는 먼저 데이터가 은닉된 암호화된 이미지를 복호화한 후에 데이터를 추출하고 이미지를 복구하도록 제안되었다. 그림 2는 그림 1과 매핑 되어 가역적 데이터 은닉 기법의 각 단계별 영상을 보여준다. (a)는 원본 영상으로 사용된 512×512 크기의 흑백 Lena 영상이며, (b)는 암호화된 영상, (c)는 암호화된 영상에 데이터를 은닉한 영상, (d)는 (c)를 복호화한 후 데이터가 은닉된 영상, (e)는 (d)로부터 데이터를 추출하고 복구된 원본 영상을 보여준다. (b), (c)는 모두 노이즈처럼 보이고,

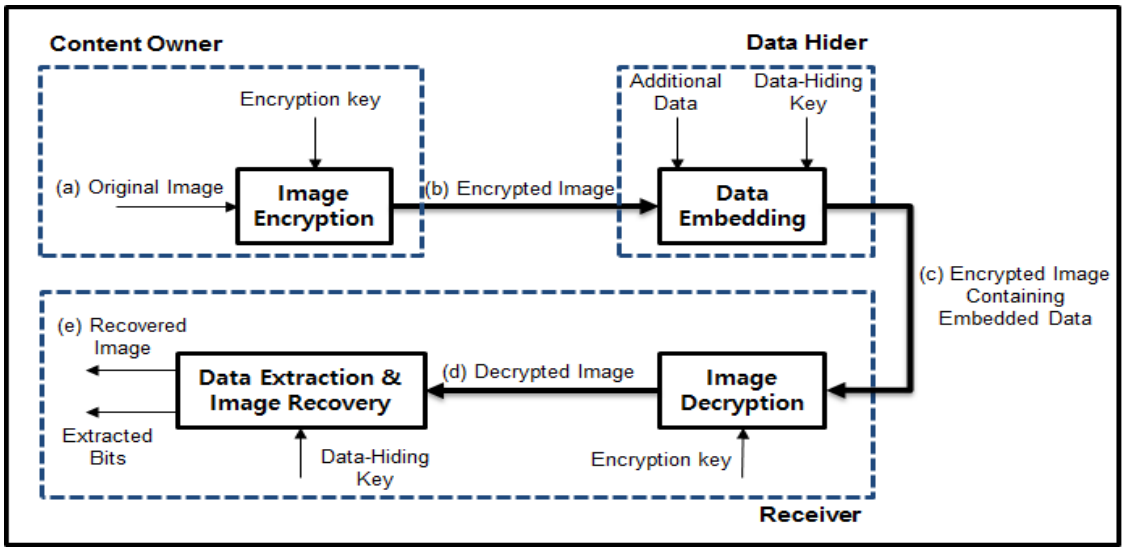
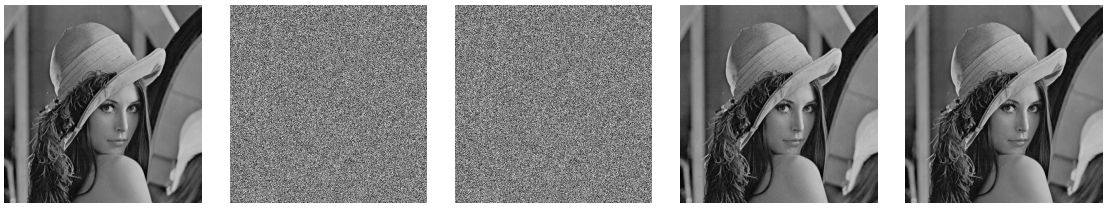


그림 1. Zhang이 제안한 암호화된 영상의 데이터 은닉 기법의 블록도
Fig. 1. Block diagram of data hiding in encrypted images proposed by Zhang



(a) 원본 영상 (original) (b) 암호화된 영상 (encrypted) (c) 은닉된 영상 (embedded) (d) 복호화된 영상 (decrypted) (e) 복구된 영상 (recovered)

그림 2. 암호화된 영상의 데이터 은닉 기법의 단계별 영상
Fig. 2. Images of data hiding in encrypted image

(a), (d), (e)는 육안으로는 영상의 차이가 거의 나지 않아 분간하기 매우 어렵다는 것을 알 수 있다.

이미지 암호화 단계에서는 원본 이미지 비트들과 의사 난수 비트들의 배타적 논리합으로 계산하며, 이를 통해 이미지를 암호화한다.

콘텐츠 소유자로부터 암호화된 이미지가 주어지면 데이터 은닉자는 원본 이미지의 내용을 알지 못하는 상태에서 데이터 은닉키를 사용하여 암호화된 데이터의 일부분을 수정함으로써 데이터를 은닉한다. 은닉을 위해 먼저, 임의의 정수 s에 대해 s^2개의 이미지 화소로 구성된 블록으로 암호화된 이미지를 분할하고 각각의 블록은 데이터 은닉키를 사용하여 두 개의 집합 S_0과 S_1로 랜덤하게 분리된다. 이때, 각 블록에는 하나의 비트가 은닉된다. 그림 3에서 좌측은 이미지를 블록으로 분할하는 것을 보여주며 우측은 그 중 한 블록이 임의의 두 집합 S_0과 S_1로 나누어지는 것을 보여준다. 우측 그림에서 회색으로 표시된 화소들의 집합을 S_0이라 가정하고, 흰색으로 표시된 화소들의 집합을 S_1이라 가정한다. 만약, s=8일 경우 총 64개의 화소가 하나의 블록이 되며 각 블록은 데이터 은닉키에 따라 S_0과 S_1로 32개씩 중복되지 않도록 나누어진다. 만약 은닉할 비트가 0이면 S_0집합에 속하는 암호화된 화소의 LSB(Least Significant Bit) 3bits를 반전시키고, 은닉할 비트가 1이면 S_1집합에 속한 암호화된 LSB 3bits를 반전시킨다. 은닉할 비트에 따라 블록마다 집합 S_0과 S_1중 하나에 속한 픽셀들만 변경되고 다른 하나의 집합에 속하는 암호화된 픽셀들은 변경되지 않는다.

은닉된 데이터를 복구하기 위해서 먼저 암호화된 이미지의 암호를 해제하며, 여기에 은닉된 데이터를 추출하기 위해서 암호가 풀린 이미지를 데이터 은닉키에 따라 데이터 은닉 시와 같은 방법으로 다시 s^2개

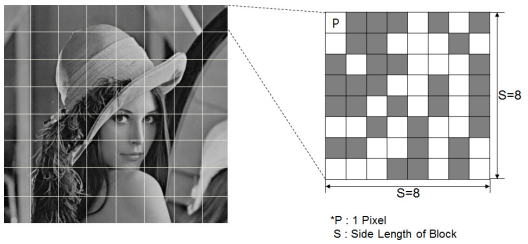


그림 3. 블록 분할과 집합 나누기 예시
Fig. 3. Block segmentation and set division

의 화소로 구성된 블록으로 분할하고 각각의 블록을 두 개의 집합 S_0과 S_1로 동일하게 나눈다. 각각의 복호화 된 블록에 대해 수신자는 S_0집합에 속하는 화소의 LSB 3bits를 반전시키고 이렇게 생성된 새로운 블록을 H_0라 가정한다. 마찬가지로 S_1집합에 속하는 화소의 LSB 3bits를 반전시킨 블록을 H_1이라 가정한다. 은닉을 위해 S_0 또는 S_1집합에 속하는 화소들의 LSB 3bits를 반전시켰을 것이므로 H_0과 H_1 중 하나의 블록만이 원본 이미지의 블록과 같아지고 다른 하나는 모든 LSB 3bits가 반전된 상태가 된다. 다시 말해 H_0과 H_1 중 하나의 블록은 왜곡이 최소화된 상태인 원본 이미지로 복구되고 또 다른 하나의 블록은 왜곡이 최대화된 이미지가 된다. 일반적으로 영상 이미지는 주변 화소와의 유사한 영상 값을 갖는 연속성을 갖고 있는데 왜곡이 일어나면 주변 화소들 간 값의 변화가 커진다. 이러한 왜곡은 이미지의 공간 상관 특성을 계산하여 측정할 수 있으며 왜곡의 정도를 측정함으로써 H_0와 H_1 중 어느 쪽이 원본 이미지인지 판정할 수 있다. $s \times s$ 의 크기를 갖는 두 개의 블록 H_0과 H_1에 대해 블록의 주변 화소들 간 변화 값을 측정하기 위해서 다음의 섭동 함수(Fluctuation Function)를 사용해서 H_0와 H_1에 대한 공간 상관 특성 값을 계산하여 f_0과 f_1라 한다.

$$f = \sum_{u=2}^{s-1}\sum_{v=2}^{s-1}\left| p_{u,v} - \frac{p_{u-1,v} + p_{u,v-1} + p_{u+1,v} + p_{u,v+1}}{4} \right| \quad (1)$$

수식 (1)은 중심 화소와 주변 네 개의 인접한 화소의 평균값을 뺀 절대 값들을 누적시킨다. 이후 수신자는 구해진 f_0과 f_1을 비교함으로써 데이터 추출과 이미지 복구를 수행한다. 원본이미지가 주변 필셀 간의 상관관계가 더 높을 것이고 이것은 더 적은 섭동(fluctuation) 값으로 나타나게 된다. 그러므로 f_0과 f_1을 비교하여 만약 $f_0 \leq f_1$이라면 H_0을 원본 블록으로 판정하고 은닉된 비트인 0을 추출한다. 반면에 $f_0 > f_1$이라면 H_1을 원본 블록으로 판정하고 은닉된 비트인 1을 추출한다. 마지막으로 은닉 메시지를 얻기 위해 추출된 비트들을 결합하고 복구된 블록들을 모아 하나의 원본 이미지로 복구한다.

Ⅲ. 문제 분석 및 개선된 기법 제안

3.1 기존 기법의 문제점

기존 기법에서 블록을 두 개의 집합 S_0과 S_1로 나눌 때 사용되는 화소의 범위로 블록 내 전체 화소인 s^2개를 사용하고, 섭동 함수를 계산 할 때 사용되는 화소의 범위로는 $(s-2)\times(s-2)$개의 화소를 사용하였다. 기존의 섭동 함수는 계산하려는 화소를 기준으로 상, 하, 좌, 우로 네 개가 인접하는 화소 값들을 사용하며 블록의 최외곽 화소들은 공간 상관 특성 값을 직접 계산하지 않고 참조만 하게 된다. 다시 말해, 블록으로 분류할 때 사용되는 화소의 범위와 섭동 함수를 계산 할 때 사용되는 화소의 범위가 다르기 때문에 원본 이미지 블록 판정에 대한 정확성이 떨어지고 섭동 값을 기준으로 한 복구 오류 확률이 0이 아닌 문제를 갖고 있다. 그림 4(a)는 512×512의 흑백 lena 영상이고, (b)는 (a)를 대상으로 데이터 추출 시 s=8인 경우에 비트 오류가 발생한 블록을 검은색 점으로 시각화한 그림이다. 또한 그림 4(c)는 512×512의 흑백 baboon 영상이고, (d)는 (b)와 마찬가지로 (c)를 대상으로 s=8인 경우에 비트 오류가 발생한 블록을 검은색으로 시각화한 그림이다. 그림을 통해 lena영상은 머리카락 부분에서, baboon영상은 얼굴의 털 부분에서 오류가 많이 발생했음을 알 수 있다. 이러한 복구 오류는 기존 기법에서 암호화된 영상에 데이터를 은닉한 후 영상에서 데이터를 추출할 때, 섭동 함수로 계산된 공간 상관 특성 값으로 은닉된 데이터를 판정하기 때문에 오류가 발생할 수 있다. 이는 가역성이라는 특성을 알고리즘이 특정 값에서 만족시키지 못한다는 것을 의미한다.

기존 섭동 함수의 한계로 인한 잘못된 판정으로 발생하는 오류율을 낮추는 방법으로 임의의 화소 개수인 s를 크게 하는 방법이 있다. 그림 5는 s의 변화량에 따른 BER(Bit Error Rate)을 도식화 한 것으로 임의의 화소 개수 s가 커질수록 BER이 감소함을 알 수 있다. 그러나 s가 커질수록 하나의 이미지에 은닉할

(a) 레나(Lena)

(c) 바분(Baboon)

(b) 레나 영상에서 오류가 발생한 블록 (Incorrect bit-extraction with Lena)

(d) 바분 영상에서 오류가 발생한 블록 (Incorrect bit-extraction with Baboon)

그림 4. s=8인 경우 오류가 발생한 블록
Fig. 4. Blocks of incorrect bit-extraction with the cover Lena, Baboon and s=8

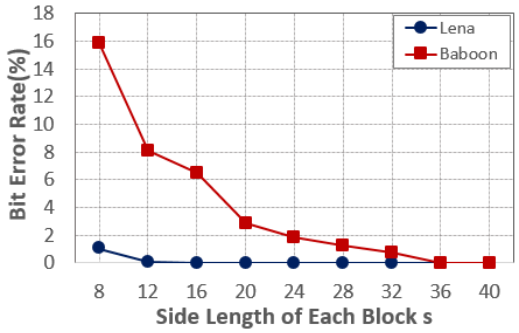


그림 5. s의 변화에 따른 비트 오류율
Fig. 5. BER(Bit Error Rate) according to change of s

수 있는 데이터의 양은 줄어든다. 만약 512×512 크기의 영상을 8×8 크기의 블록으로 나눈다면 총 4,096개의 블록이 생기며 하나의 블록에 하나의 비트를 은닉할 수 있으므로 총 4,096 bits(512 Bytes)의 데이터를 은닉할 수 있다. 표 1은 s의 변화량에 따라 은닉할 수 있는 데이터의 수를 영상 크기별로 수치화 한 것이다. 결과적으로 s가 작을수록 은닉할 수 있는 데이터의 수는 많지만 BER이 높아지고, s가 커질수록 BER은 감소하지만, 은닉할 수 있는 데이터의 수는 작아진다. 그러므로 임의의 화소 개수 s를 낮춰서 은닉할 수 있는 데이터의 양도 증가시키고 BER 또한 낮출 수 있는 최적의 방법이 필요하다.

표 1. 영상의 크기와 s의 변화에 따른 은닉할 수 있는 데이터의 수
Table 1. The number of data being able to hide according to size of image and change of s

size of image	side length of block								
	8	12	16	20	24	28	32	36	40
256 x 256	1024	455	334	256	113	83	64	50	41
512 x 512	4096	1820	1024	655	455	334	256	202	164
1024 x 1024	16384	7281	4096	2621	1820	1337	1024	809	655

또한, 데이터 은닉자가 데이터가 은닉된 암호화된 영상을 수신자에게 전송할 때 제 3자에게 공격을 받아 비트가 변경된다면 데이터 추출 시 오류율이 증가할 수 있으며, 변경된 비트의 분포에 따라 오류율에 큰 영향을 미칠 수 있다. 예를 들어, 변경된 비트가 MSB(Most Significant Bit)에 위치해 있다면 섭동함수의 결과 값이 크게 변경되기 때문에 오류가 발생할 확률이 높다. 반대로 LSB에 위치해 있다면 결과 값에 미치는 영향이 작기 때문에 오류 발생 확률이 낮아진다.

3.2 개선된 기법 제안

본 논문에서 제안하는 기법은 데이터 추출 및 원본 이미지 복원 시 임의의 블록 크기 s를 줄여 은닉할 수 있는 데이터의 양을 증가시키면서도 동시에 BER을 낮출 수 있는 개선된 섭동 함수이다. 제안하는 기법에서 데이터 은닉 과정은 기존과 동일하며 복구 과정에서 사용하는 섭동 함수를 새롭게 설계하였다.

은닉된 데이터를 복원하기 위해 수신자는 콘텐츠 소유자와 동일한 데이터 은닉키를 사용해서 각 블록마다 S_0과 S_1 집합을 다시 생성하고 각 집합마다 해당하는 화소의 LSB 3bits를 반전시켜서 H_0과 H_1을 생성한다. 제안하는 기법에서 S_0과 S_1 집합을 분류하는 블록 내 화소 개수는 기존 기법과 동일한 s^2이며 섭동함수를 계산할 때 블록 내 화소의 범위를 그림 6에 나타낸 것처럼 다르게 설정하였다. 기존 기법에서 섭동함수를 계산할 때 계산하려는 화소를 기준으로 상, 하, 좌, 우 네 개가 인접하는 화소 값들만을 사용하고 블록의 최외곽 화소들은 계산 시에 참조하기만 하였다. 즉, 기존 기법의 섭동 함수에 사용되는 화소의 범위(그림 6의 좌측)는 $(s-2)\times(s-2)$ 이다. 그러나 최외각 화소에도 원본 이미지에 대한 추가적인

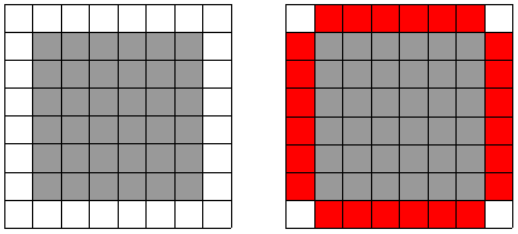


그림 6. 기존 및 제안하는 섭동 함수의 블록 내 계산범위
Fig. 6. The calculation range of conventional and proposed fluctuation function in block

정보가 더 들어 있기 때문에, 이를 활용하기 위해 제안하는 기법의 섭동 함수에 사용되는 화소의 범위는 그림 6의 우측에 나타낸 것처럼 s^2-4개로 확대되었다. 기존의 방법 대비 $4s-8$개의 픽셀을 더 활용함으로써, 원본 이미지 블록 판정 시 기존 기법보다 더 정밀하게 판정할 수 있다.

앞서 생성한 H_0과 H_1의 공간 상관 특성을 측정하기 위해 새롭게 제안하는 섭동 함수의 보다 구체적인 계산식은 수식 (2)에 나타나 있다.

$$\begin{aligned} f = & \sum_{u=2}^{s-1}\sum_{v=2}^{s-1}\left|p_{u,v}-\frac{p_{u-1,v}+p_{u,v-1}+p_{u+1,v}+p_{u,v+1}}{4}\right| \\ & +\frac{3}{4}\sum_{v=2}^{s-1}\left|p_{1,v}-\frac{p_{1,v-1}+p_{2,v}+p_{1,v+1}}{3}\right| \\ & +\frac{3}{4}\sum_{v=2}^{s-1}\left|p_{s,v}-\frac{p_{s-1,v}+p_{s,v-1}+p_{s,v+1}}{3}\right| \\ & +\frac{3}{4}\sum_{u=2}^{s-1}\left|p_{u,1}-\frac{p_{u-1,1}+p_{u+1,1}+p_{u,2}}{3}\right| \\ & +\frac{3}{4}\sum_{u=2}^{s-1}\left|p_{u,s}-\frac{p_{u-1,s}+p_{u,s-1}+p_{u+1,s}}{3}\right| \end{aligned} \quad (2)$$

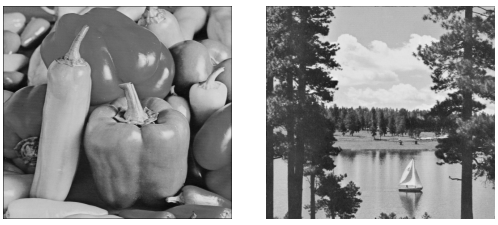
즉, 기존의 원본 이미지 판정 방식에 포함시키지 않았던 인접하는 화소 수가 세 개인 경우의 화소 값들이 판정식에 추가함으로써 검출되는 비트 오류 확률을 줄일 수 있다.

본 논문에서 제안하는 섭동 함수는 인접하는 화소의 수가 네 개인 화소의 경우는 계산하려는 화소와 상, 하, 좌, 우 화소의 평균값을 뺀 절대 값을 사용하고, 인접하는 화소의 수가 세 개인 화소의 경우는 계산하려는 화소와 인접한 세 개 화소의 평균값을 뺀 절대 값의 합으로 계산한다. 세 개가 인접하는 화소를 계산할 때 최상단의 화소들은 하, 좌, 우 화소를, 최하단의 화소들은 상, 좌, 우 화소를, 최좌측의 화소들은 상, 하, 우 화소를, 최우측의 화소들은 상, 하, 좌 화소를 각각 인접하는 화소에 맞게 계산한다. 또한, 인접하는 화소 수에 따라 가중치를 다르게 주어 네 개가 인접하는 화소에 대해서는 가중치를 1로, 세 개가 인접하는 화소에 대해서는 가중치를 $\frac{3}{4}$ 로 하여 판정의 신뢰도를 높였다. 이는 기존 기법보다 연산이 많아지기는 하지만 공간 상관 특성 값을 더욱 정확하게 계산하여 원본 이미지에 대해 더 세밀한 판정을 할 수 있게 된다.

Ⅳ. 성능 검증

제안된 기법의 성능 검증을 위해 그림 7과 같은 512×512 크기의 흑백 영상인 Lena, Baboon, Peppers, Sailboat 영상을 샘플 입력 영상으로 사용하였다. 그리고 데이터 추출 시의 기존 기법과 제안하는 기법을 BER을 기준으로 비교하여 그래프와 표로 나타내어 제안하는 기법의 성능 증가를 입증한다. 그림 8, 그림 9, 그림 10, 그림 11은 각각 Lena, Baboon, Peppers, Sailboat 영상에 대해 기존 기법과 제안하는 기법의 섭동 함수를 사용하여 도출된 BER을 그래프로 도식화 한 것이다. 그리고 자세한 결과는 표 2, 표 3, 표 4, 표 5에 수치화하였다. 성능 검증의 결과는 대부분 기존 기법보다 제안 기법의 BER이 감소하였으며, 특히 s=8일 때 그림 8의 lena는 1.07%에서 0.46%로 BER이 감소했으며, 그림 9의 Baboon은 15.83에서 13.5%로, 그림 10의 Peppers는 1.49에서 0.88로,

(a) 레나(Lena) (b) 바분(Baboon)



(c) 피망(Peppers) (d) 요트(Sailboat)

그림 7. 모의실험을 위해 사용된 샘플 영상
Fig. 7. Sample image used for simulation

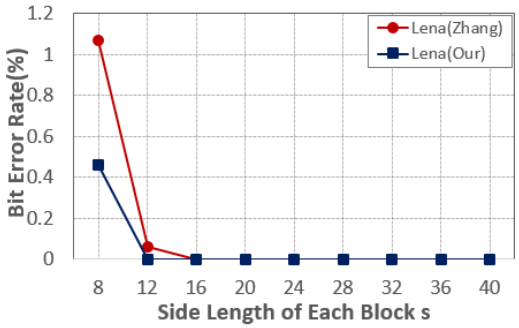


그림 8. Lena 영상에 대한 기존/제안 기법의 BER 비교
Fig. 8. BER Comparison of method between conventional and proposed for Lena image

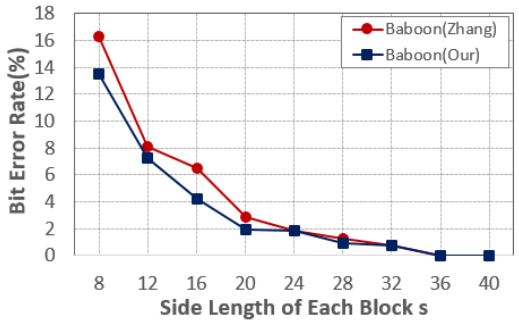


그림 9. Baboon 영상에 대한 기존/제안 기법의 BER 비교
Fig. 9. BER Comparison of method between conventional and proposed for Baboon image

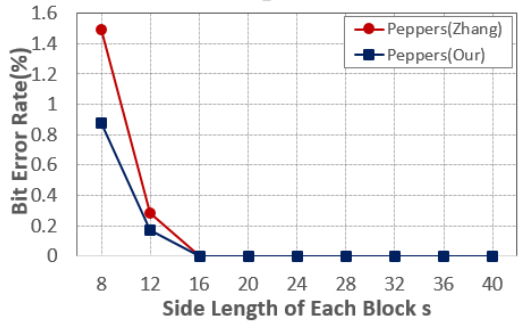


그림 10. Peppers 영상에 대한 기존/제안 기법의 BER 비교
Fig. 10. BER Comparison of method between conventional and proposed for Peppers image

그림 11의 Sailboat는 6.35%에서 3.47로 감소했음을 확인할 수 있다. 각 그림에서 볼 수 있듯이 제안하는 기법의 BER이 기존의 기법보다 감소했음을 확인할 수 있다. 다시 말해, BER 성능 측면에서 기존 기법에 비해 제안하는 기법이 더 우수하며 제안된 섭동 함수로 인해 이미지의 공간 상관 특성 값을 더욱 세밀하게

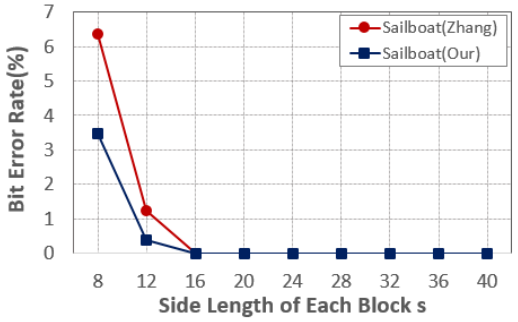


그림 11. Sailboat 영상에 대한 기존/제안 기법의 BER 비교
Fig. 11. BER Comparison of method between conventional and proposed for Sailboat image

표 2. Lena 영상에 대한 BER 수치
Table 2. BER figure for Lena image

method	side length of each block s								
	8	12	16	20	24	28	32	36	40
Zhang	1.07	0.06	0	0	0	0	0	0	0
Our	0.46	0	0	0	0	0	0	0	0

표 3. Baboon 영상에 대한 BER 수치
Table 3. BER figure for Baboon image

method	side length of each block s								
	8	12	16	20	24	28	32	36	40
Zhang	16.28	8.11	6.45	2.88	1.81	1.23	0.78	0	0
Our	13.5	7.26	4.2	1.92	1.81	0.93	0.78	0	0

표 4. Peppers 영상에 대한 BER 수치
Table 4. BER figure for Peppers image

method	side length of each block s								
	8	12	16	20	24	28	32	36	40
Zhang	1.49	0.28	0	0	0	0	0	0	0
Our	0.88	0.17	0	0	0	0	0	0	0

표 5. Sailboat 영상에 대한 BER 수치
Table 5. BER figure for Sailboat image

method	side length of each block s								
	8	12	16	20	24	28	32	36	40
Zhang	6.35	1.25	0	0	0	0	0	0	0
Our	3.47	0.40	0	0	0	0	0	0	0

계산함으로써 원본 이미지 판정에 대한 정확성과 신뢰성이 증가하였다.

표 6은 앞선 모의실험 결과 중 은닉할 수 있는 데

표 6. s=8인 경우 각 영상에 대한 기존/제안 기법의 BER 비교
Table 6. BER comparison of conventional and proposed method for each image and s=8

BER \ Image	Lena	Baboon	Peppers	Sailboat
Zhang's method (A)	1.07%	15.87%	1.49%	6.35%
Our's method (B)	0.46%	13.5%	0.88%	3.47%
reduction rate (1-(B/A))	57%	15%	41%	45%

이터의 수가 가장 많지만 비트 오류율 또한 가장 큰 경우인 하나의 블록 내의 화소의 개수인 s=8일 때 기존 기법과 제안하는 기법을 비교하여 수치화한 결과이다. 표에서는 모든 이미지에서 BER 수치가 감소했음을 확인할 수 있다. 특히, 이미지의 특성상 주변에 인접한 화소끼리의 흑백 대비가 큰 화소를 많이 갖고 있는 Baboon 영상을 제외하고, 나머지 영상에 대해서 기존 기법 대비 평균 BER 감소율은 46%로 본 논문에서 제안하는 섭동 함수의 성능이 크게 개선되었음을 확인하였다.

V. 결 론

본 논문에서는 은닉된 데이터를 추출 과정에서 발생하는 오류를 감소시키기 위한 섭동 함수를 제안하였다. 은닉할 수 있는 데이터양이 많지만 검출되는 비트 오류율이 큰 경우에 해당하는 임의의 화소 개수 s를 작게 하여 데이터 은닉 기법을 사용할 때에 대한 최적의 방법을 연구하였다. 데이터 추출 시에 블록내의 최외곽의 상, 하, 좌, 우 화소는 섭동함수에 사용되지 아니하고 계산 시에만 참조되었던 이전의 기법에서 원본 이미지에 대한 판정의 정확성을 높이기 위해 인접하는 화소의 수가 세 개인 화소까지도 계산될 수 있도록 섭동함수를 수정함으로써 비트 오류율을 감소시킬 수 있었다. 특히, 평균적으로 BER을 46%까지 감소시킴으로써 성능 측면에서 본 논문이 제안한 기법의 우수성을 입증할 수 있었다.

본 논문은 데이터 은닉자에게 원본 콘텐츠의 내용을 알지 못하게 하면서 데이터와 이미지를 전송하기 위해 이미지를 암호화시켜 보호하고 암호화된 이미지 내에 특정 데이터를 은닉하는 것에 중점을 두었다. 현재의 데이터 은닉 기법은 과정, 기법, 결과 등 각 목적에 맞게 연구되어지고 있으며, 사회적 이슈나 기술적 발전에 맞추어 여러 아이디어들이 제안되고 있다. 또한, 정적 매체에 데이터를 은닉하는 현재의 기술과 달리 동영상과 같은 동적 매체에 데이터를 은닉하여 정보를 보호하거나 공격하는 시대가 다가오고 있다. 급격하게 발전하는 기술과 점점 다양해지는 정보, 커져가는 데이터에 대한 체제 및 관리정책 등에 따라 데이터 은닉 기법 등을 계속 발전시켜야 할 것이다.

References

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice. New Jersey*: Pearson Education, 2003.

[2] M. Park, E. Cho, and T. T. Kwon, "Multi server password authenticated key exchange using attribute-based encryption," *J. KICS*, vol. 40, no. 8, pp. 1597-1605, Aug. 2015.

[3] J.-H. Kim, S.-K. Yoo, and S.-H. Lee, "Fully homomorphic encryption scheme without key switching," *J. KICS*, vol. 38, no. 5, pp. 428-433, May 2015.

[4] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn "Information hiding-a survey," in *Proc. IEEE, special issue on protection of multimedia content*, May 1999. Invited paper.

[5] R. J. Anderson and F. A. P. Petitcolas. "On the limits of steganography," *IEEE J. Sel. Areas on Commun.*, vol. 16, pp. 474-481, 1998.

[6] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890-896, Aug. 2003.

[7] M. U. Celik, G. Sharma, A. M. Tekalp, and E.Saber, "Lossless generalized-lsb data embedding," *IEEE Trans. Image Process.,* vol. 14, no. 2, pp. 253-266, Feb. 2005.

[8] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354-362, 2006.

[9] L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using

interpolation technique," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 1, pp. 187-193, 2010.

[10] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Processing Lett.*, vol. 18, no. 4, pp. 255-258, Apr. 2011.

[11] W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Processing Lett.*, vol. 19, no. 4, pp. 199-202, Apr. 2012.

[12] J. Fridirich, M. Goljan, and R Du, "Lossless data embedding for all image formats," *SPIE Proc. photonics West, Electronic Imaging, Security and Watermarking of multimedia Contents*, vol. 4675, pp. 572-583, 2002.

[13] Y. C. Li, C. M. Yeh, and C. C. Chang, "Data hiding based on the similarity between neighboring pixels with reversibility," *Digital Signal Processing*, vol. 20, pp. 1116-1128, 2010.

[14] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Processing*, vol. 89, no. 6, pp. 1129-1143, 2009.

[15] W. L. Tai, C. M. Yeh, and C. C. Chang, "Reversible data hiding based on histogram modification of pixel differences," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 6, pp. 906-910, Jun. 2009.

[16] H. C. Wu, H. C. Wang, C. S. Tsai, and C. M. Wang, "Reversible image steganographic scheme via predictive coding," *Displays*, vol. 31, no. 1, pp. 35-43, Jan. 2010.

[17] C.-C. Chang, C.-C. Lin, and Y.-H. Chen, "Reversible data-embedding scheme using differences between original and predicted pixel values," *Inf. Secur.*, vol. 2, no. 2, pp. 35-46, 2008.

[18] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in video compression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 6, pp. 774-778, 2007.

[19] Y.-S. Kim, C.-J. Ryu, and S.-J. Han, "Refined reversible data hiding scheme in encrypted image," in *Proc. KIIT Summer Conf.* 2011, pp. 78-82, May 2011.

[20] J.-H. Jeong, K.-J. Kang, Y.-S. Kim, and D.-W. Lim, "Reversible data hiding scheme using dynamic bit selection in encrypted image," in *Proc. KIISC Int. Conf.* 2012, pp. 56-59, Dec. 2012.

[21] Y.-S. Kim and D.-W. Lim, "Reversible data hiding scheme based on lattices," *J. KMMS*, vol. 16, no. 4, pp. 27-33, Dec. 2012.

[22] S.-H. Cho, D.-S. Kim, and K.-Y. Yoo, "Improved reversible data hiding scheme based on difference value of adjacent pixels," in *Proc. KICS Int. Conf. Commun.*, pp. 205-206, Jeju Island, Korea, Jun. 2013.

[23] T.-S. Kim, M.-H. Jang, and S.-H. Kim, "Transmission methods using RS codes to improve spatial relationship of images in reversible data hiding systems," *J. KICS,* vol. 40, no. 8, pp. 1477-1484, Aug. 2015.

김 영 훈 (Young-Hun Kim)

2014년 2월 : 한국산업기술대학교 컴퓨터공학과 학사

2014년 3월~현재 : 동국대학교 정보보호학과 석사과정

2014년 3월~현재 : 동국대학교 부호 및 암호 연구실 연구원

<관심분야> 암호 및 보안, 제어시스템 보안, 개인정보보호

임 대 운 (Dae-Woon Lim)

1994년 2월 : 한국과학기술원 전기 및 전자공학과 학사
1997년 2월 : 한국과학기술원 전기 및 전자공학과 석사
2006년 8월 : 서울대학교 전기·컴퓨터공학부 박사
1995년 9월~2002년 8월 : LS 산전선임 연구원
2006년 9월~현재 : 동국대학교 정보통신공학과 부교수
<관심분야> 무선통신, 부호이론, 신호설계, 암호 및 보안, 제어시스템 보안

김 영 식 (Young-Sik Kim)

2001년 2월 : 서울대학교 전기공학부 졸업
2003년 2월 : 서울대학교 전기컴퓨터공학부 석사
2007년 2월 : 서울대학교 전기컴퓨터공학부 박사
2007년 3월~2010년 8월 : 삼성전자 책임연구원
2010년 9월~현재 : 조선대학교 정보통신공학과 조교수
<관심분야> 암호학, 정보보안, 정보이론, 오류정정 부호, 하드웨어 보안