논문 16-41-11-01 The Journal of Korean Institute of Communications and Information Sciences '16-11 Vol.41 No.11
http://dx.doi.org/10.7840/kics.2016.41.11.1329

암호화된 영상의 가역적 데이터 은닉을 위한 일반화된 섭동 함수 설계

김 영 훈◆, 임 대 운*, 김 영 식°

Design of Generalized Fluctuation Function for Reversible Data Hiding in Encrypted Image

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

요 약

최근 Zhang은 동기식 스트림 암호를 통해 암호화된 영상에 데이터를 은닉하는 방법을 제안하였다. 수신자는 먼저 암호화된 영상을 복호하고, 복호된 영상에 섭동 함수(fluctuation function)를 이용하여 공간 상관 특성 값을 계산함으로써 데이터를 추출한다. 그 후 Hong은 사이드 매치(side match) 기법을 이용하여 Zhang의 데이터 은닉 기법을 개선하였다. 본 논문에서는 데이터 추출과정에서 발생하는 오류를 감소시키기 위해 새로운 섭동 함수를 제안하고, 표본 영상들에 대한 컴퓨터 모의실험을 통해 제안하는 기법이 기존의 방법들보다 우수함을 검증하였다.

Key Words : encrypted image, reversible data hiding, fluctuation function, side-match

ABSTRACT

Recently, Zhang proposed a scheme to hide information in encrypted images using synchronous stream ciphers. After the receiver decrypts the encrypted image and extracts data by calculating the spatial correlation property value using the fluctuation function which is designed to calculate spacial correlation between adjacent pixels in a decrypted image. Then, Hong improved the Zhang's data hiding scheme by introducing the side match technique. In this paper, a novel fluctuation function is proposed to reduce the recovery errors which arise during extracting hidden data. Then, we also demonstrated that the proposed fluctuation function outperforms the previous functions through computer simulations for sample images.

Ⅰ. 서 론

정보통신 기술의 발달로 인해 오늘날 어느 곳이든 자유롭게 정보를 전달할 수 있게 되었다. 이에 따라 디지털 콘텐츠를 보호하기 위한 데이터 은닉 기술에 대한 관심 또한 높아지고 있다. 이 때 사용할 수 있는 방법으로 데이터를 암호화하는 것이 있지만[1,2], 이 경우 공격자에게 암호화된 정보가 존재한다는 사실이 알려지게 되어, 공격의 주요 대상이 될 수 있다. 따라서 이런 사실을 숨기기 위해 보호하고자 하는 데이터를 일반적인 커버 데이터에 은닉하는 방식에 대한 연구가 진행되었다. 이 경우 데이터가 은닉된 사실을 숨길 수 있기 때문에, 존재 노출로 인한 집중 분석의 대상이 되는 것을 피하는 것이 가능하다[3,4].

※ 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 : KICS2016-03-040, Received March 2, 2016; Revised July 2, 2016; Accepted October 25, 2016

최근 연구되는 디지털 데이터의 은닉 기술에 있어 원본 이미지를 손상시키지 않고 보존 가능한 "가역성(reversibility)"이 매우 중요한 요소로 인식되고 있다.

최근 몇 년간 제안된 가역적 데이터 은닉 기술로는 다음과 같은 것들이 있다. 두 개의 연속적인 화소의 차이를 확대하여 데이터를 은닉하는 차분 확장(difference expansion) 방법[5], 캐리 데이터 비트에 대한 여분의 공간을 생성하기 위해 무손실 압축을 수행하여 데이터를 은닉하는 방법[6], 히스토그램의 최소점을 이용하고 은닉된 데이터에 대한 화소의 그레이스케일 값을 변경하는 방법[7], 데이터 은닉을 위해 차분 확장과 히스토그램 시프팅을 사용하는 방법[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 있다. 그 외에도 비트 평면으로 나타낸 영상의 화소 값을 LSB(the least significant bit) 비트 정보를 검사하면서 무손실 압축 기법을 사용하여 은닉할 공간을 찾은 후에 데이터를 삽입하는 방법[12], 인접 화소들 간의 유사도에 기반 하는 방법[13], 예측 부호화와 히스토그램의 쉬프팅을 이용하는 방법[14], 픽셀 차분의 히스토그램 수정에 기반 하여 이진트리를 이용하는 방법[15], 예측 부호화를 통해 생성된 하이딩 트리를 이용하는 방법[16] 등이다. 국내에서도 동적으로 LSB 비트를 선택하는 방법[17], 격자 기반으로 데이터를 은닉하는 방법[18], 인접하는 화소간의 차이 값을 이용하는 방법[19], 개선된 하이딩 트리를 이용하는 방법[20], DQT(define quantization table)을 사용하여 3단계 과정을 통해 영상을 보호하는 방법[21], RS(Reed-Solomon) 부호를 활용한 이미지 공간상관관계 향상을 위한 전송 방법[22] 등 많은 연구가 진행되었다. 또한, 가역적 데이터 은닉 기법의 성능 향상을 위한 다양한 기술도 제안되었다[23-25].

이 중에서 Zhang은 이미지에 은닉되는 데이터와 디지털 콘텐츠를 비인가자로부터 보호받을 수 있도록 암호화된 이미지에 데이터를 은닉하고 추출하면서 원본 이미지를 복구할 수 있는 가역적 데이터 은닉 기법을 제안하였다. 또한, Hong은 데이터를 추출할 때 발생하는 오류를 감소시키고, 가역성을 증가시키기 위해 섭동함수(fluctuation function)를 개선하고 사이드 매치(side match)를 이용하는 기법을 제안하였다.

본 논문에서는 Zhang의 기법과 Hong의 기법을 일반화시킨 새로운 데이터 은닉 기법을 제안한다. 제안한 방식에서는 오류를 최소화하기 위해 데이터 추출 단계에서 원본 이미지를 판정할 때 사용하는 새로운 섭동 함수를 제안한다. 또한 새로 제안한 방식을 기존 기법들과 비교 및 분석하여, 새로운 제안의 우수성을 입증한다.

본 논문의 구성은 다음과 같다. 2장에서는 Zhang이 제안한 기존의 암호화된 영상에 대한 데이터 은닉 기법을 설명한다. 3장에서는 Hong이 제안한 side match 기법을 자세히 설명한다. 그런 후에 4장에서는 제안하는 개선된 방법을 설명할 것이다. 5장에서는 제안한 방식의 모의실험을 통해 성능을 검증한 후에 마지막으로 6장에서 결론을 맺는다.

Ⅱ. 암호화된 영상의 가역적 데이터 은닉 기법

Zhang의 가역적 데이터 은닉 기법은 영상 암호화, 데이터 은닉, 영상 복호화, 그리고 데이터 추출 및 영상 복구의 네 단계로 구성된다[10]. 또한, 콘텐츠 소유자, 데이터 은닉자, 수신자, 이렇게 세 명의 사용자가 존재하는 것으로 가정한다.

최초 콘텐츠 소유자는 원본 영상을 암호화키를 사용하여 암호화된 영상을 생성하고 이를 데이터 은닉자에게 전송한다. 이때, 원본 영상의 비트들과 의사난수 비트들의 배타적 논리합 계산을 통해 영상을 암호화한다.

데이터 은닉자는 암호화키와는 별개인 데이터 은닉키를 사용하여 암호화된 영상에 삽입할 데이터를 은닉한 후 수신자에게 전송한다. 원본 영상이 암호화 되어있기 때문에 데이터 은닉자는 그 내용을 알지 못하며, 은닉되는 데이터에 따라 암호화된 영상을 일부 수정하여 데이터를 은닉한다. 은닉을 위해 먼저, 암호화된 영상을 임의의 정수 s에 대해 s^2개의 화소로 구성된 블록으로 분할하고 각각의 블록은 데이터 은닉키를 사용하여 두 개의 집합 S_0과 S_1로 랜덤하게 분리한다. 이때, 각 블록에는 하나의 비트가 은닉된다.

그림 1에서 좌측은 영상을 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 3비트를 반전시키고, 은닉할 비트가 1이면 S_1집합에 속한

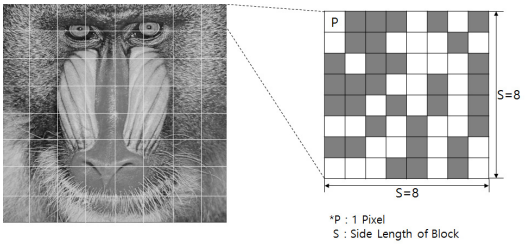


그림 1. 블록 분할과 집합 나누기의 예
Fig. 1. Block segmentation and set division

암호화된 LSB 3비트를 반전시킨다. 은닉할 비트에 따라 블록마다 집합 S_0과 S_1 중 하나에 속한 픽셀들만 변경되고 다른 하나의 집합에 속하는 암호화된 픽셀들은 변경되지 않는다.

수신자는 콘텐츠 소유자로부터 받은 암호화키를 사용하여 먼저, 암호화된 이미지를 복호한다. 복호된 영상은 원본 영상과 유사하다. 다음으로 데이터 은닉키를 사용하여 복호화 된 영상으로부터 삽입된 데이터를 추출하고 원본 영상을 복구한다.

은닉된 데이터를 추출하기 위해서 복호화 된 영상을 데이터 은닉키에 따라 데이터 은닉 시와 마찬가지로 다시 s^2개의 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 3비트를 반전시키고 이렇게 생성된 새로운 블록을 H_0라 가정한다.

마찬가지로 S_1집합에 속하는 화소의 LSB 3비트를 반전시킨 블록을 H_1이라 가정한다. 은닉을 위해 S_0 또는 S_1집합에 속하는 화소들의 LSB 3비트를 반전시켰을 것이므로 H_0과 H_1 중 하나의 블록만이 원본 이미지의 블록과 같아지고 다른 하나는 모든 LSB 3비트가 반전된 상태가 된다. 다시 말해 H_0과 H_1 중 하나의 블록은 왜곡이 최소화된 상태인 원본 영상으로 복구되고 또 다른 하나의 블록은 왜곡이 최대화된 영상이 된다.

일반적으로 영상은 주변 화소와의 유사한 값을 갖고 있는데, 데이터 은닉을 통해 영상에 왜곡이 발생하면 주변 화소들 간 값의 변화가 커진다. 이러한 왜곡은 영상의 공간 상관 특성을 계산하여 측정할 수 있으며 왜곡의 정도를 측정함으로써 H_0와 H_1 중 어느 쪽이 원본 영상인지 판정하게 된다.

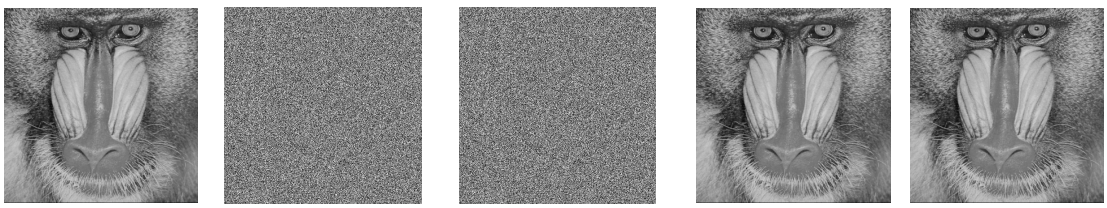
$s \times s$ 의 크기를 갖는 두 개의 블록 H_0과 H_1에 대해 블록의 주변 화소들 간 변화 값을 측정하기 위해서 다음의 섭동 함수를 사용해서 H_0와 H_1에 대한 공간 상관 특성 값을 계산하여 f_0과 f_1라 한다.

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

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 영상 복구를 수행한다. 원본 영상이 주변 픽셀 간의 상관관계가 더 높을 것이고 이것은 더 적은 섭동 값으로 나타날 확률이 높다. 그러므로 섭동값 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 영상으로 복구한다.

이는 가역적인 방식으로 특정 데이터를 은닉하고 추출하는 기술로, 암호화된 영상에 데이터 은닉을 수행하고 복호된 영상에서 데이터를 추출하기 위해 XOR 연산에 대해 동형(homomorphic) 특성을 갖는 동기식 스트림 암호를 사용한다.

그림 2는 가역적 데이터 은닉 기법의 각 단계별 영



(a) 원본 영상 (original) (b) 암호화된 영상 (encrypted) (c) 은닉된 영상 (data embedding) (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

상을 보여준다. (a)는 원본 영상으로 사용된 512×512 크기의 흑백 바분 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. (a), (d), (e)는 육안으로는 영상의 차이가 거의 나지 않아 분간하기 매우 어렵다는 것을 알 수 있다.

Zhang의 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. 기존 섭동 함수는 계산하려는 화소를 기준으로 상, 하, 좌, 우 네 개의 인접 화소 값들을 사용하며 블록의 최외곽 화소들은 공간 상관 특성 값을 직접 계산하지 않고 참조만 하고 있다.

다시 말해, 블록으로 분류할 때 사용되는 화소의 범위와 섭동 함수를 계산 할 때 사용되는 화소의 범위가 다르기 때문에 원본 영상의 블록 판정에 대한 정확성이 떨어지고 섭동 값을 기준으로 한 복구 오류 확률이 0이 아닌 문제를 갖고 있다.

예를 들어, 1개의 블록 크기가 8×8 이라면, 총 64개의 화소로 구성되며 이 중 43.75%인 28개의 화소가 섭동 함수를 계산할 때 사용되지 않는 블록의 최외곽 화소가 된다. 그림 3(a)는 512×512의 흑백 Sailboat 영상이고, (c)는 (a)를 대상으로 데이터 추출 시 s=8인 경우에 비트 오류(원본 영상과 복구한 영상을 비트 단위로 비교해봤을 때 서로 다른 값을 가지고 있는 경우)가 발생한 블록을 검은색 점으로 시각화한 그림이다. 또한 그림 3(b)는 512×512의 흑백 baboon 영상이고, (d)는 (c)와 마찬가지로 (b)를 대상으로 s=8인 경우에 비트 오류가 발생한 블록을 검은색으로 시각화한 그림이다. 그림을 통해 baboon영상은 얼굴의 털 부분에서 오류가 많이 발생했음을 알 수 있다. 이러한 복구 오류는 Zhang의 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.

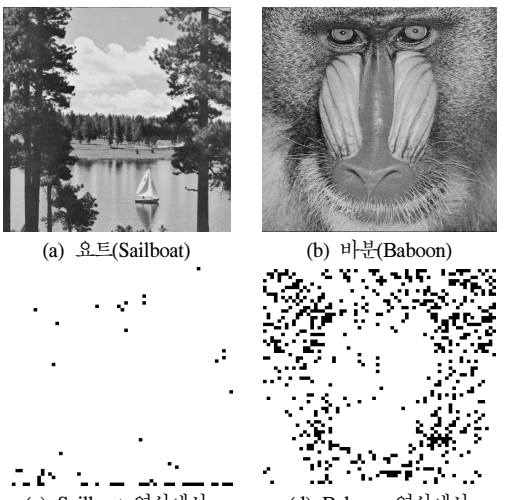


그림 3. s=8인 경우 오류가 발생한 블록
Fig. 3. Blocks of incorrect bit-extraction with the cover Sailboat and Baboon image for s=8

Ⅲ. 사이드 매치를 이용한 데이터 은닉 기법

Hong은 블록의 섭동 값을 계산할 때 사용하는 개선된 섭동함수를 제안하였으며, 오류 발생률을 감소시키기 위해 사이드 매치 기법을 적용했다[11]. Hong의 섭동함수는 두 개의 인접한 화소들의 절대차를 누적하며, 다음의 수식 (2)와 같이 블록 내에서 좌, 우 화소들의 절대 차를 누적시킨 값과 상, 하 화소들의 절대 차를 누적시킨 값을 계산하여 더한다.

$$f=\sum_{u=1}^{s_2}\sum_{v=1}^{s_1-1}|p_{u,v}-p_{u,v+1}|+\sum_{u=1}^{s_2-1}\sum_{v=1}^{s_1}|p_{u,v}-p_{u+1,v}| \tag{2}$$

Hong의 사이드 매치 방식을 적용한 데이터 추출 및 영상 복구 단계는 먼저 각 블록마다 데이터 은닉키를 사용하여 나눈 집합 S_0과 S_1에 대해, S_0집합에 속하는 화소의 LSB 3비트를 반전시킨 블록인 H_0과 S_1 집합에 속하는 화소의 LSB 3비트를 반전시킨 블록인 H_1에 대해 각각 수식 (2)를 사용하여 섭동 값을 계산한다. 이때, H_0에 대한 섭동 값을 f_0이라 가정하고, H_1에 대한 섭동 값을 f_1이라 가정한 후 수식 (3)과 같이 두 섭동 값의 절대차를 계산한다.

$$A=|f_0-f_1| \tag{3}$$

블록마다 수식 (3)을 적용하여 도출된 결과 A에 따라 각 블록들을 내림차순으로 정렬하고 우선순위가 높은 블록부터 데이터 추출 및 영상 복구를 수행한다. 이때, 블록들 간의 경계에 있는 화소들의 상관관계가

매우 높기 때문에 복구되지 않은 블록을 주변에 있는 복구된 블록의 경계 화소와 결합하는 사이드 매치 기법을 적용한 후 결합된 블록에 대해 다시 섭동함수를 수행하여 섭동 값을 계산한다.

그림 4에 사이드 매치 기법의 흐름도를 수식으로 표현하였다. 흐름도에서 P는 가로 블록의 수, Q는 세로 블록의 수, N은 블록의 총 개수를 의미한다. 내림차순으로 정렬된 우선순위에 따른 복구하고자 하는 블록을 b_i라 하고, i의 범위는 최초 우선순위인 0부터 시작하여 마지막 우선순위인 $N-1$번 블록에 대해 섭동함수를 계산한다.

표 1은 이 기법에서 사용되는 섭동함수를 분류한 것으로 b_i의 주변 블록 중 오른쪽 블록과 아래쪽 블록의 복구 여부에 따라서 상황별로 U_1, V_1, U_2, V_2를 기존의 Hong의 기법에 사용되는 수식 (2)를 변경한 다음의 수식 (4)에 대입한 것이다.

$$f=\sum_{u=1}^{U_1}\sum_{v=1}^{V_1}|p_{u,v}-p_{u,v+1}|+\sum_{u=1}^{U_2}\sum_{v=1}^{V_2}|p_{u,v}-p_{u+1,v}| \quad (4)$$

다시 말해, b_i에 대해 표 1을 통해 각 경우를 분류하고 이에 대응하는 U_1, V_1, U_2, V_2를 수식 (4)에 대입하여 섭동 값을 계산한다.

사이드 매치는 먼저, b_i을 기준으로 오른쪽 블록과

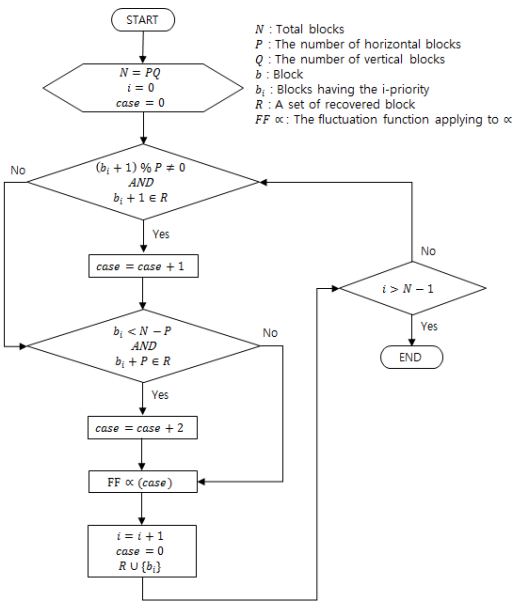


그림 4. Side match 기법의 흐름도
Fig. 4. The flowchart of the side match

표 1. 주변 블록의 복구 여부에 따라 제안된 기법에 적용할 수 있는 섭동함수의 분류
Table 1. Classification of the fluctuation function that can be applied to the proposed method according to whether the neighboring block was recovered

case	recovered block		U_1	V_1	U_2	V_2
	right	bottom				
0	no	no	S_2	S_1-1	S_2-1	S_1
1	yes	no	S_2	S_1	S_2-1	S_1
2	no	yes	S_2	S_1-1	S_2	S_1
3	yes	yes	S_2	S_1	S_2	S_1

아래쪽 블록이 존재하지 않거나 둘 다 복구되지 않았다면 case 0을 적용하여 섭동함수를 수행한다. case 1은 b_i을 기준으로 오른쪽 블록이 존재하고 복구된 경우 섭동함수에 적용하고, case 2는 b_i을 기준으로 아래쪽 블록이 존재하고 복구된 경우 적용한다. 만약 오른쪽 블록과 아래쪽 블록이 모두 존재하고 복구된 경우는 case 3을 적용하여 섭동함수를 수행한다.

그림 5에 블록마다 우선순위가 부여된 예를 나타내었다. 예를 들어, 그림과 같이 우선순위가 부여된 9개의 블록이 있다면 1-우선순위를 갖는 블록은 오른쪽 블록과 아래쪽 블록이 존재하지 않기 때문에 case 0을 적용하여 수식 (4)에 대입한다. 2-우선순위를 갖는 블록도 마찬가지로 case0을 적용한다. 3-우선순위를 갖는 블록은 오른쪽 블록과 아래쪽 블록이 존재하고 모두 복구되었기 때문에 오른쪽 블록인 1-우선순위를 갖는 블록의 왼쪽 경계에 있는 화소들과 결합하고 2-우선순위를 갖는 블록의 위쪽 경계에 있는 화소들과 결합한 후 case 3을 적용한다. 4-우선순위를 갖는 블록은 오른쪽 블록이 존재하고 이미 복구되었기 때문에

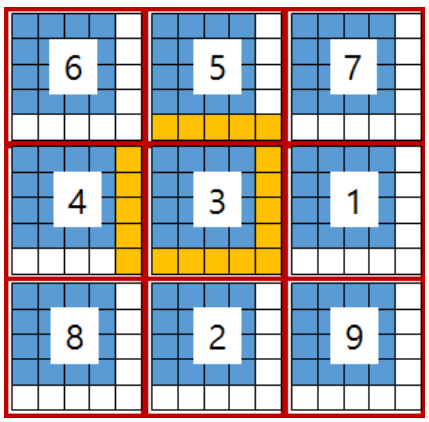


그림 5. 블록마다 우선순위가 부여된 예
Fig. 5. The example assigned priority ranking for each block

3-우선순위를 갖는 블록의 왼쪽 경계에 있는 화소들과 결합한 후 case 1을 적용한다.

이와 같이 모든 블록에 대해 사이드 매치를 적용한 후 새롭게 구해진 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 추출된 비트들을 결합함으로써 은닉 메시지를 얻고 복구된 블록들을 모아 하나의 원본 이미지로 복구한다.

이 기법은 복구하고자 하는 블록보다 우선순위가 높은 블록들이 이미 복구가 된 블록이기 때문에 원본 이미지의 블록 값을 갖게 되고 우선순위가 높은 블록의 경계 화소와 복구되지 않은 블록과의 결합을 통해 더 정확한 공간상관 정도를 계산할 수 있다.

Ⅳ. 문제 분석 및 개선된 기법 제안

4.1. 기존 기법의 문제점

기존 기법들에는 섭동 값을 이용한 원본 영상 블록 판정에 대한 정확성이 떨어지고 영상 복구 오류 확률이 0이 아닌 문제를 갖고 있다. 섭동 함수가 갖고 있는 자체적인 한계로 인해 발생하는 오류율을 낮추는 방법으로 그림 6과 같이 블록 내의 화소 개수를 결정하는 s를 크게 하는 방법이 있지만, 기존 두 기법 모두 s가 커질수록 하나의 영상에 은닉할 수 있는 데이터의 용량은 줄어든다.

만약 512×512 크기의 영상을 12×12 크기의 블록으로 나누는 경우 총 1,820개의 블록이 생성되며 하나의 블록 당 하나의 비트를 은닉할 수 있기 때문에 총 1,820 비트(약 228 바이트)의 데이터를 은닉할 수 있다.

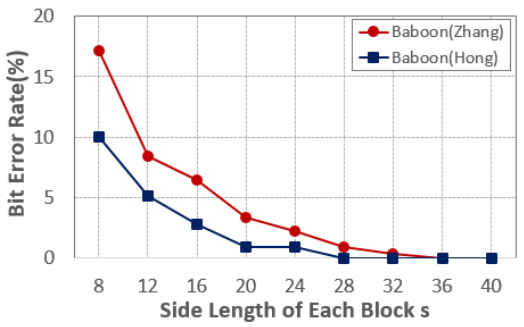


그림 6. s의 변화에 따른 비트 오류율
Fig. 6. BER according to the changing of s-parameter

표 2. 영상의 크기와 s의 변화에 따른 은닉할 수 있는 데이터의 수
Table 2. The number of data being able to hide according to size of image and changing of s-parameter

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

표 2는 s의 변화량에 따라 은닉할 수 있는 데이터의 수를 영상 크기별로 수치화 한 것이다. 결과적으로 s가 작을수록 은닉할 수 있는 데이터의 수는 많지만 BER(bit error rate)이 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.

또한, 데이터 은닉자가 데이터가 은닉된 암호화된 영상을 수신자에게 전송할 때 제3자에게 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.

Hong 기법의 경우에는 Zhang의 기법보다 비트 오류율을 크게 감소시킬 수 있지만, 블록에 우선순위를 부여한 후 복구하는 과정에서 섭동 값을 최대 블록 당 2번씩 계산하고 저장해야하므로 시간복잡도와 공간복잡도가 크게 증가한다는 문제가 있다.

4.2. 개선된 기법 제안

본 논문에서 제안하는 기법은 오류 최소화를 위해 데이터 추출 단계에서 공간 상관 특성을 계산할 때 사용하는 섭동 함수를 개선한다. 그림 7에 제안하는 기법의 블록도를 나타내었다. 기존 기법과의 가장 큰 차이점으로 최적의 α 계산(Optimal α Calculation) 단계가 추가되어 제안하는 기법은 총 다섯 단계로 구성된다.

기존 기법에서는 데이터 은닉자가 데이터 은닉만을 수행하였지만, 제안하는 기법은 최적의 α 계산을 수

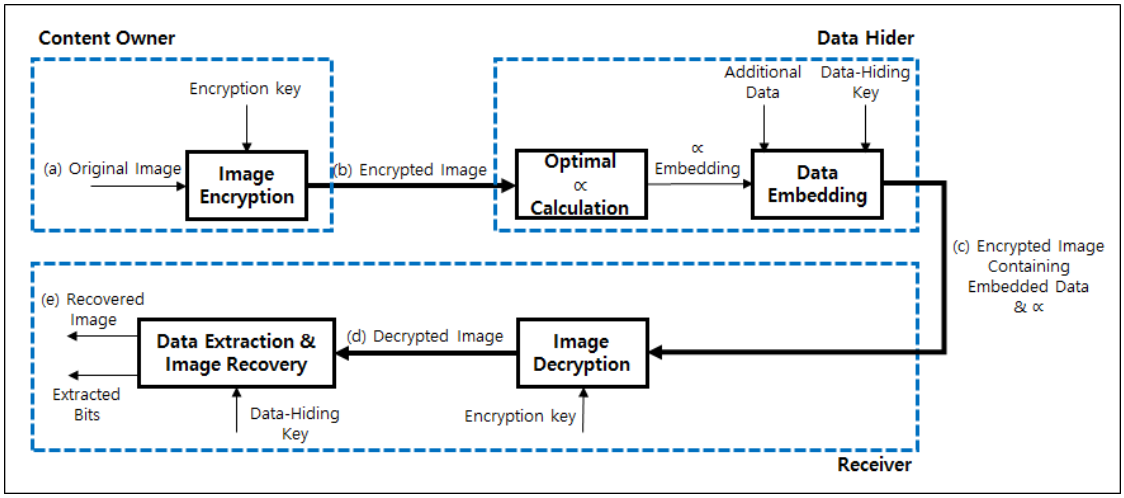


그림 7. 제안 기법의 블록도
Fig. 7. A block diagram of the proposed method

행한 후에 도출된 α을 은닉할 데이터와 함께 은닉한다. 은닉된 α는 수신자가 데이터 추출 및 영상 복구를 수행할 때 사용되며 이를 통해 기존 기법들보다 비트 오류율을 감소시킬 수 있다. 단, α에 따라 비트 오류율은 달라지며 이는 데이터 은닉 기법의 중요한 성능 척도이기 때문에 α를 안전하게 송신하기 위해서 오류 정정 부호(error correcting code)를 사용한다.

그림 8에 최적의 α 계산 과정을 흐름도로 나타내었다. 콘텐츠 소유자로부터 암호화된 이미지를 수신한 데이터 은닉자는 먼저 α와 max, 그리고 정밀도를 결정한다. α는 기존의 섭동함수를 변경하여 가장 낮은 비트오류율을 갖는 최적의 경우를 계산하기 위해 필요한 값이며, max는 α의 최대값, 그리고 정밀도는 α의 단위를 나타낸다.

이후 데이터 은닉 단계, 이미지 복호화 단계, 데이터 추출 단계를 차례로 수행한다. 이때 수행되는 섭동함수는 다음의 수식 (5), 수식 (6)과 같이 α를 적용한 섭동함수이다. 수식 (5)는 Zhang의 섭동함수를 개선한 것이고 수식 (6)은 Hong의 섭동함수를 개선한 것이다.

$$f=\sum_{u=2}^{s-1}\sum_{v=2}^{s-1}\left|p_{u,v}-\frac{p_{u-1,v}+p_{u,v-1}+p_{u+1,v}+p_{u,v+1}}{4}\right|^{\alpha} \tag{5}$$

$$f=\sum_{u=1}^{U_1}\sum_{v=1}^{V_1}|p_{u,v}-p_{u,v+1}|^{\alpha}+\sum_{u=1}^{U_2}\sum_{v=1}^{V_2}|p_{u,v}-p_{u+1,v}|^{\alpha} \tag{6}$$

제안하는 기법의 예로, 그림 8과 같이 α는 0.1, max는 3, 그리고 정밀도를 0.1로 결정하면 α는 0.1부터 max보다 같거나 작을 때까지 α를 적용하여 섭동함수를 수행하고 정밀도에 따라 α를 0.1씩 증가시키면서 반복적으로 수행한다. 이 단계를 모두 수행하면

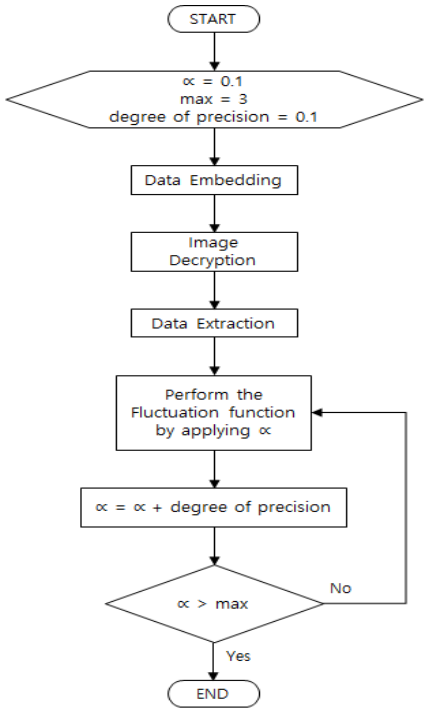
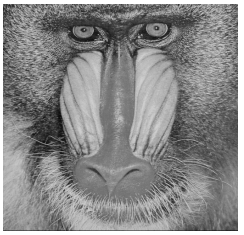


그림 8. 최적의 α 계산 과정의 흐름도
Fig. 8. The flowchart of the optimal α calculation process


(a) 레나(Lena)


(b) 바분(Baboon)


(c) 요트(Sailboat)

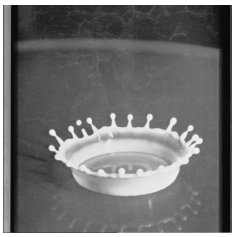

(d) 물방울(Splash)

그림 9. 모의실험을 위해 사용된 샘플 영상
Fig. 9. Sample image used for simulation

입력한 α에 대응하는 비트 오류율을 구할 수 있으며 최종적으로 가장 낮은 비트 오류율을 갖는 최적의 α를 도출할 수 있다.

데이터 은닉자에 의해 도출된 최적의 α는 그림 7의 데이터 은닉 단계에서 데이터와 함께 삽입한 후에 수신자에게 전송한다. 이때, 삽입된 α는 비트 오류율을 낮출 수 있는 중요한 데이터이기 때문에 전송 시 손실을 방지하기 위해 오류 정정 부호를 사용한다. 데이터와 α가 은닉된 암호화된 영상을 전송받은 수신자는 영상을 복호한 후 데이터 추출 및 영상 복구를 수행하고 전송받은 최적의 α를 적용하여 섭동 값을 계산한다.

본 논문에서 제안하는 섭동 함수는 원본 영상 블록 판정 시 기존의 섭동함수에 α제곱으로 가중을 조절함으로써 기존 기법보다 더 정밀하게 판정할 수 있다. 이는 기존 기법보다 연산양은 증가하지만 원본 이미지에 대한 판정의 신뢰도를 높일 수 있게 된다.

V. 성능 검증

제안된 기법의 성능 검증을 위해 그림 9와 같은 512×512 크기의 흑백 영상인 Lena, Baboon, Sailboat, Splash 영상을 USC-SIPI image database에서 다운로드 받은 후 샘플 입력 영상으로 사용하였다[26].

BER을 기준으로 기존 기법과 제안하는 기법의 성능을 비교하기 위해 표 3과 같이 데이터 은닉 기법들을 세부적으로 분류하였다.

표 3. 성능 비교를 위한 데이터 은닉 기법의 세부적 분류
Table 3. The detailed classification of data hiding to compare the performance

class	fluctuation function	side match	αth power (Proposed)	method proposed by
①	Zhang	no	no	Zhang's paper
②	Zhang	no	yes	our paper
③	Hong	yes	no	Hong's paper
④	Hong	no	yes	our paper
⑤	Hong	yes	yes	our paper

표 4. Lena 영상에서 α의 변화에 따른 BER 성능 비교
Table 4. BER performance comparison with various α in Lena image

α	Side length of each blocks		
	8	12	16
0.5	0.54	0.06	0
1.0	0.27	0	0
1.1	0.27	0	0
1.2	0.27	0	0
1.3	0.24	0	0
1.4	0.22	0	0
1.5	0.27	0	0

표 5. Baboon 영상에서 α의 변화에 따른 BER 성능 비교
Table 5. BER performance comparison with various α in Baboon image

α	Side length of each blocks		
	8	12	16
0.5	11.67	6.18	3.61
1.0	9.99	5.10	2.83
1.1	9.96	4.88	2.93
1.2	9.94	4.88	2.73
1.3	9.94	4.71	2.54
1.4	9.84	4.65	2.44
1.5	10.01	4.88	2.44

표 6. Sailboat 영상에서 α의 변화에 따른 BER 성능 비교
Table 6. BER performance comparison with various α in Sailboat image

α	Side length of each blocks		
	8	12	16
0.5	2.20	0.45	0
1.0	1.54	0.23	0
1.1	1.56	0.17	0
1.2	1.46	0.23	0
1.3	1.46	0	0
1.4	1.51	0	0

먼저 표 4, 5, 6은 각각 Lena, Baboon, Sailboat 영상에서 α의 변화에 따른 BER 성능을 나타내었다. Lena와 Baboon 영상의 경우 $\alpha=1.4$에서 BER 성능이 가장 우수했고, Sailboat 영상의 경우 블록의 크기가 8인 경우 $\alpha=1.1$에서 블록의 크기가 12인 경우 $\alpha=1.2$에서 BER 성능이 가장 우수했다.

표에서 알 수 있는 것처럼 주어진 이미지의 픽셀 분포에 따라서 BER 특성은 크게 변할 수 있다. 따라서 최적의 α를 찾기 위해서는 은닉하고자 하는 이미지에 대해서 최적값을 찾는 과정이 선행되어야 한다. 최적값을 찾기 위해서는 모든 α을 일정하게 변화시키면서 오류율을 비교해야한다. 그러나 α의 값에 따른 오류 변화가 크지 않으므로 0.1 단위로 0.5에서 1.5까지 10번 정도 계산해 보는 것으로 충분하며, 따라서 일반 복구과정을 10번 반복해보는 정도로 복잡도가 증가하게 된다.

그러나 한 번 복구 과정이 동작하는데 512×512 크기의 이미지의 경우 일반적인 PC환경에서 데이터 복구에 수십 밀리초 이내의 시간이 걸리기 때문에, 본 논문에서 제안하는 방법을 적용하더라도 총 10번 반복을 1초 이내의 시간 동안 수행할 수 있다. 따라서 반복 회수의 증가에 따른 성능 향상을 고려하여 본 논문에서 제안하는 방법을 사용할 수 있다.

그림 10, 그림 11, 그림 12, 그림 13은 각각 Lena, Baboon, Sailboat, Splash 영상에 대해 표 3의 세부적인 분류를 적용하여 도출된 BER을 그래프로 도식화한 것이다. 각 그림에서 볼 수 있듯이 제안하는 기법이 기존 기법보다 전체적으로 BER이 감소했음을 확인할 수 있다. 예를 들어, Lena 영상에 대해서 s가 8일 때 Zhang의 기법 ①과 제안기법 ②의 경우 1.12%에서 0.66%로 BER이 감소했으며 Hong의 기법 ③과 제안기법 ④, ⑤의 경우 0.27%에서 최대 0.22%로 감소했음을 확인할 수 있다. 특히, Baboon 영상의 경우 s가 28일 때 제안기법 ⑤에서 BER은 0을 달성했다.

표 7에서는 기존 방식인 Zhang의 방법과 [23]에 제시된 섭동함수 변형 방식을 새로 제안한 방법 중에서 최적의 α를 사용했을 때의 BER 성능을 비교하였다. [23]에서는 Zhang의 섭동 함수를 좀 더 복잡한 형태로 변형하는 방식으로 BER 성능을 개선하였으나, 본 논문에서는 Zhang 또는 Hong 등이 제안한 것과 동일한 형태의 섭동함수를 일반화시켜서 α승을 하는 방식으로 변경하여 계산하였다. 그 결과 표 7에서 알 수 있는 것처럼 본 논문에서 제안하는 방식이 기존 방식들보다 모든 테스트 이미지에 대해서 BER 성능이 더 우수한 것을 확인할 수 있었다.

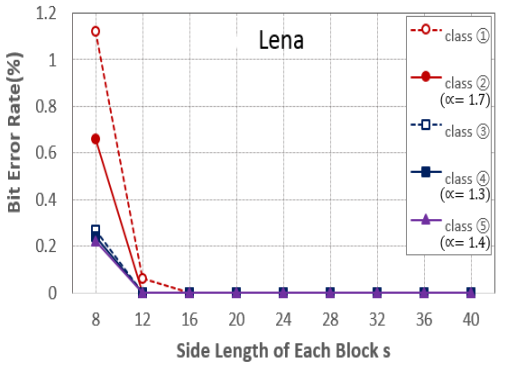


그림 10. Lena 영상에 대한 기존/제안 기법의 BER 비교
Fig. 10. BER Comparison of conventional and proposed method for Lena image

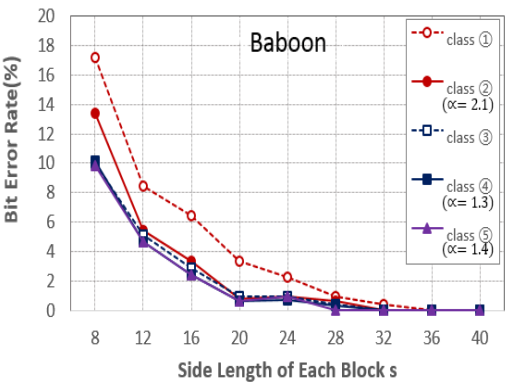


그림 11. Baboon 영상에 대한 기존/제안 기법의 BER 비교
Fig. 11. BER Comparison of conventional and proposed method for Baboon image

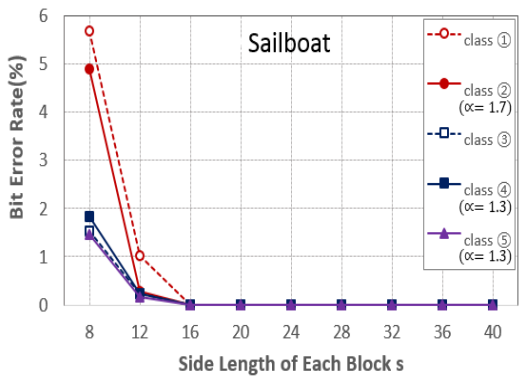


그림 12. Sailboat 영상에 대한 기존/제안 기법의 BER 비교
Fig. 12. BER Comparison of conventional and proposed method for Sailboat image

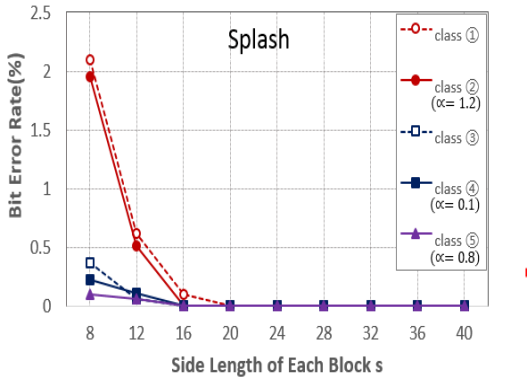


그림 13. Splash 영상에 대한 기존/제안 기법의 BER 비교
Fig. 13. BER Comparison of conventional and proposed method for Splash image

표 7. 기존 방식과의 BER 성능 비교
Table 7. BER performance comparison with previous scheme

	Lena	Baboon	Sailboat
s = 8			
Zhang	1.07%	16.28%	6.35%
[23]	0.46%	13.5%	3.47%
Proposed	0.27%	9.84%	1.46%
s=12			
Zhang	0.06%	8.11%	1.25%
[23]	0%	7.26%	0.4%
Proposed	0%	4.65%	0.23%

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

Image / reduction	Lena	Ba boon	Sail boat	Spla sh
①, ②	41%	22%	13%	7%
③, min(④,⑤)	19%	2%	5%	73%

표 8은 앞선 모의실험 결과 중 은닉할 수 있는 데이터의 수는 가장 많지만 비트 오류율 또한 가장 큰 경우인 s가 8일 때 각 기법들을 비교하여 BER의 감소율을 측정한 결과이다. 첫 번째 감소율은 Zhang의 기법 ①과 ①에 제안기법을 적용한 ②를 비교한 결과이고, 두 번째 감소율은 Hong의 기법 ③과 ③에 제안기법을 적용한 ④와 ⑤중 최소 BER을 갖는 기법과 비교한 결과이다.

표 8에서 볼 수 있듯이 모든 영상 및 기법에 대해 BER 수치가 감소했음을 확인할 수 있으며 특히, 표 9에 나타낸 바와 같이 Splash 영상의 경우 BER이 0.37에서 0.1로 73%가 감소하였으며 0에 가까운 오류율을 달성했음을 확인할 수 있다.

은닉된 데이터를 추출할 때 사용하는 섭동함수는 특정 픽셀과 주변 픽셀 사이의 차이를 추정하는데 사용하게 되지만, 사용하는 커버 이미지에 따라서 성능에 차이를 보여준다. 예를 들어 커버 이미지 자체에서 주변 픽셀 간의 변화의 폭이 원래 큰 이미지의 경우 섭동함수를 통한 거리 추정을 통한 은닉정보 판별의 정확도는 그렇지 않은 이미지에 비해서 더 떨어지게 된다. 다양한 선행 연구에서 여러 형태의 섭동 함수가 제시되고 있으나, 대부분의 연구에서 단일한 섭동함수를 모든 이미지에 적용하도록 하고 있다. 그러나 하나의 섭동함수로 모든 형태의 커버 이미지에서 좋은 성능을 기대할 수 없기 때문에, 본 논문에서는 다른 접근으로 이미지에 가장 적합한 섭동 함수를 은닉 단계에서 찾는 방식을 제안하였다. 본 논문에서 제시한 바와 같이 α승을 통해서 기존의 섭동 함수에 변화를 주게 되면, 픽셀간 상관도를 추정하는 섭동함수의 스펙트럼을 크게 넓힐 수 있으며, 여러 섭동함수 중에서 가장 적합한 섭동함수(혹은 α)를 은닉 단계에서 찾아서 복구시 삽입된 데이터를 정확하게 추출하는 확률을 높일 수 있다.

본 논문에서 제안하는 기법은 BER 성능 측면에서 기존 기법들에 비해 더 우수하며 최적의 α를 계산하여 적용하는 제안된 섭동 함수로 영상의 공간 상관 특성 값에 가중을 조절함으로써 원본 영상 판정에 대한 신뢰성이 증가하였다. 이는 데이터 은닉자가 미리 섭동 값을 계산해야하므로 연산이 많아지기는 하지만 α 제곱을 통해 공간 상관 특성 값의 가중을 조절하여 비트 오류율을 최소화할 수 있다.

또한, 하나의 기법에만 한정되지 않고 Zhang과 Hong의 기법들 모두 제안하는 기법을 적용한 후 BER을 최소화시킴으로써 Zhang의 암호화된 영상의 가역적 데이터 은닉 기법을 바탕으로 하는 많은 기법들에 적용하여 성능을 증가시킬 수 있는 범용성을 검증하였다.

Ⅵ. 결 론

본 논문에서는 암호화된 영상에 데이터를 은닉하는 가역적 데이터 은닉 기법의 은닉된 데이터를 추출하는 과정에서 발생하는 오류를 감소시키기 위한 일반화된 섭동 함수를 제안하였다.

최적의 α를 미리 계산하고 이를 은닉할 데이터와

함께 은닉한 후 데이터 추출 시 α제곱을 이용하여 섭동 함수의 가중을 조절함으로써 비트 오류율을 최소화시킬 수 있었다. 특히, 입력으로 사용한 모든 영상 및 기법에 대해 BER을 감소시킴으로써 성능 측면에서 본 논문이 제안한 기법의 우수성을 입증할 수 있었다.

References

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

[2] 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 2013.

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

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

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

[6] 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.

[7] 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.

[8] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721-730, 2007.

[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. Sign. Process. 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. Sign. Process. 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. 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 Sign. Process.*, vol. 20, no. 4, pp. 1116-1128, 2010.

[14] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Sign. Process.*, 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 and Syst. for 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, pp. 35-43, 2010.

[17] 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 C-ISC-W'12,* pp. 56-59, Dec. 2012.

[18] 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.

[19] 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.

[20] J.-H. Choi and K.-Y. Yoo, "A reversible steganography scheme using improved hiding tree," in *Proc. KICS Int. Conf. Commun.*, pp.

176-177, Jun. 2011.

[21] S. W. Kim, S. Yoo, J. Shin, and J. Ryou, "A study on the protection method for the medical image using DQT encryption," in *Proc. KICS Int. Conf. Commun.*, pp. 205-206, Jeju Island, Korea, Jun. 2013.

[22] 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.

[23] Y.-H. Kim, D.-W. Lim, and Y.-S. Kim, "Design of fluctuation function to improve BER performance of data hiding in encrypted image," *J. KICS*, vol. 41, no. 3, pp. 307-316, Mar. 2016.

[24] 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.

[25] 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.

[26] Image database [Online], Available: http://sipi.usc.edu/database/

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 부교수

<관심분야> 암호학, 정보보안, 정보이론, 오류정정 부호, 하드웨어 보안