Journal of the Korea Industrial Information Systems Research Vol. 20 No. 3, Jun. 2015 :29-36
http://dx.doi.org./10.9723/jksiis.2015.20.3.029 ISSN:1229-3741

LSB 기법 기반 최적의 이미지 스테가노그래피의 연구

(A Study of Optimal Image Steganography based on LSB Techniques)

지 선 수[1)]
(Seon-Su Ji)

요 약 스테가노그래피는 은닉되어 전송되는 비밀 메시지의 존재 자체를 숨기는 기술이다. 일반적으로 은닉 자료의 지각 투명성, 수용 능력, 견고성 등을 기반으로 하는 새롭고 정교한 스테가노그래피 기법을 개발하는 것이 주목적 이다. 이 논문에서는 이미지 스테가노그래피 기법의 장점과 단점을 분석하고, 효과적인 적용방법을 제시한다. 결과적으로 재배열키를 적용하고, 보안성이 좋은 ELSB와 DCT를 기반으로 하는 이미지 스테가노그래피 기법이 효과적이다.

핵심주제어 : 이미지 스테가노그래피, 스테간 분석, 정보은닉, 최하위 비트(LSB)

Abstract Steganography is the technique of hiding the existence of a secret message that is communicated hiddenly. Generally, the main objectives of this paper is to develop newer and more sophisticated steganographic techniques based on perceptual transparency, robustness and capacity of the hidden data. This paper analyzes the advantages and disadvantages of image steganography techniques and proposes an effective method. As a result, the images steganography technique based on good ELSB and DCT which applies the rearranged key is secure and effective.

Key Words : Data Hiding, Image Steganography, Least Significant Bit(LSB), Steganalysis

1. 서 론

인터넷은 정보 검색에서부터 상품 구매와 인터넷 뱅킹에 이르기까지 현대를 살아가는 우리 모두의 활동 영역에서 핵심으로 자리매김하였다. 기하급수적으로 늘어나는 인터넷 이용인구의 성장과 이러한 사이버 공간에서 송수신되는 비밀통신의 중요성 또한 매우 중요하게 되었다. 현재의 인터넷 환경은 무한대의 메모리 크기가 제공되어 효율적으로 디지털 데이터를 전송할 수 있으며, 비밀 메시지를 삽입할 수 있는 매개 수단은 다양하고 복잡하게 이루어 졌다. 이러한 통신 수단은 긍정적인 측면에서 대부분의 이용자 이익을 위해 사용되고 있지만 부정적인 측면에서 오남용되고 있으며 특히, 악의적인 목적으로 이용하는 범죄자들에게 광범위하게 노출되어 있다. 역사가 기

* Corrensponding Author : ssji@gwnu.ac.kr
Manuscript receivrd March 30, 2015 / revised May 27 ,2015 / accepted June 9, 2015
1) 강릉원주대학교 정보기술공학과

록된 이후로 집단 간에 정보를 주고받을 때 위변조 방지와 보안성을 강화하기 위해 수많은 도구가 개발되었다. 현재까지 꾸준하게 연구되어지고 개발된 정보 은폐의 중요한 요소는 암호화와 정보은닉 기법이 있다. 정보은닉 방법에는 워터마킹과 스테가노그래피가 있다. 암호화는 메시지의 비밀을 유지하기 위해 불법 탈취자에 의해 이해될 수 없도록 애매모호한 형태로 변경하여 비밀통신을 보호하기 위한 것이다. 스테가노그래피의 최종 목표는 숨겨진 자료의 존재 자체를 감지할 수 없도록 하는 것이다. 이러한 요소들 모두는 매개체의 시각 및 청각적 품질을 저하시키거나 파괴되지 않으면서 허락된 수신자에게만 안전하게 무결성이 보장된 자료가 전달되게 하는 것이다[1-3]. 또한 눈으로 볼 수 없거나 은닉 요소로 인해 스테가노그래피에서 알려진 절차를 모를 경우 원래의 정보를 복구하는 것을 매우 어렵게 하는 것이다.

스테가노그래피 기법과 스테간 분석 사이의 끊임없는 도구의 개발 즉, 공격자에 대한 보안 조치와 취약점 파악의 노력은 향후 계속될 것이다. 따라서 비밀 메시지를 삽입하기 위한 효율적이고 새로우며, 더 정교한 스테가노그래피 기술 개발과 이를 탐지하기 위한 강력한 스테간 분석방법이 필요하다. 이 논문에서는 스테가노그래피의 적용 요소와 각각의 특성을 분석하여 최적의 기법을 제시한다.

2. 스테가노그래피

스테가노그래피는 인터넷 공간에서 사용할 수 있는 모든 매개체(텍스트, 이미지, 오디오, 비디오)에 비밀 자료의 존재 자체를 숨기는 매우 오래된 기법이다.

커버 매체의 형태에 따라 정보보호를 유지하기 위한 기본적인 스테가노그래피 모델[3-4]은 Fig. 1에서 보여준다. 여기에서는 커버 매체에 비밀 메시지를 삽입할 때 삽입하고자 하는 자료를 비트 패턴으로 변환한 후 암호화하며, 차 재배열 키를 이용하여 은닉 시점에 따라 배치 순서가 다르게 하는 기법을 추가하였다. 예를 들어 은닉하

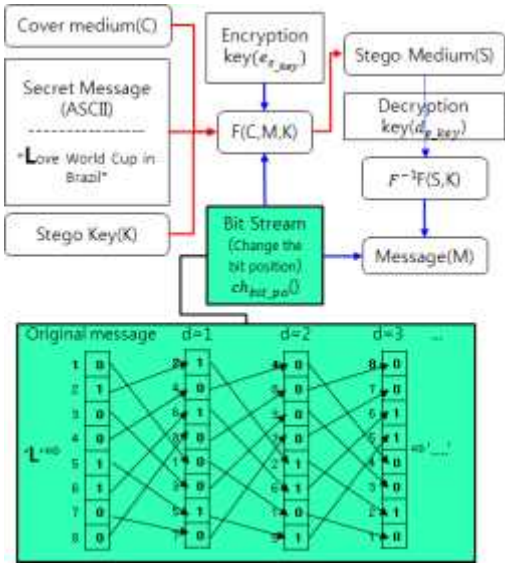

Fig. 1 Steganograohy encoder/decoder process

려는 비밀문자 L(76, '01001100')을 $d=2$일 경우 재배열함수에 적용하면 '00001101'이 된다. 그림에서 진하게 표시된 부분이다.

는 커버 매체, K는 스테고 키, M은 은닉하고자 하는 메시지, S는 스테고 매체라 할 때 다음과 같이 쓸 수 있다.

$$E : F(c, m \mid e_{s\_key}, ch_{bit\_po}) \rightarrow S$$
$$E_x : F^{-1}(S \mid d_{s\_key}, ch_{bit\_po}) \rightarrow m \quad (1)$$

여기에서 임의의 3가지 정보는 $c \in C$, $m \in M$, e_{s_key}, d_{s_key}, $ch_{bit_po} \in K$이며, e_{s_key}는 암호화키, d_{s_key}는 복호화키, $Ch_{bit_po}()$는 변경키에 따라 메시지의 비트 정보 위치를 바꾸는 함수이다. E_m은 커버 매체에 메시지가 삽입되는 과정을 나타내며, E_x는 스테고 매체로부터 메시지의 추출 과정을 의미한다.

2.1 스테가노그래피의 형태

일반적으로 스테가노그래피는 공간적, 변환적, 적응적 기법으로 구분하여 설명되어진다. 공간적인 스테가노그래피는 숨겨진 자료에서 이미지 픽셀 값에 약간의 비트 값을 변경하는 것이다. 예를 들어 최하위 비트(least significant bit, LSB)

기반 스테가노그래피는 많은 요소의 감지할 수 없는 왜곡을 피하면서 커버 매체의 LSB에 비밀 메시지를 은닉하는 간단한 기술이다. 공간 영역에서 약한 저항성을 보완하기 위해 DCT(discrete cosine transform), DWT(discrete wavelet transform), SVD(singular value decomposition)와 같은 변환적인 스테가노그래피 기술을 사용한다. 좀 더 강력한 보안성을 위해 공간적과 변환적인 기법의 장점이 모두 사용되는 적응적 기법이 적용된다[5-6]. Fig. 2에서 정보와 매개체 그리고 적용 기법에 따라 분류된 자료를 은닉하는 스테가노그래피 기술을 보여준다.

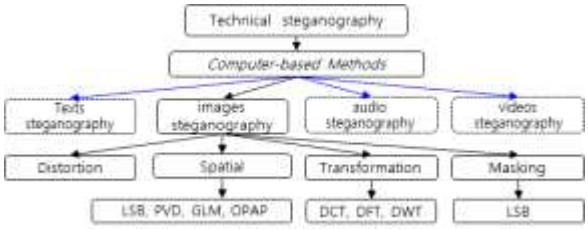

Fig. 2 Classification of steganography techniques

일반적으로 이미지 스테가노그래피 기법에서 공간 영역, 변환 영역, 왜곡 기법으로 나누어 적용되어진다.

2.1.1 Spatial Domain Technique

LSB 기반 스테가노그래피는 감지할 수 있는 왜곡을 도입하지 않고 픽셀 값의 LSB에서 비밀 메시지를 숨기는 간단한 방법 중 하나이다. 여기에서 LSB의 값의 변화는 인간의 시각적 한계 때문에 감지할 수 없다. 그러나 이러한 공간 영역의 방법은 영상처리나 잡음, 압축 등의 외적 요소와 공격 등에 약하다는 단점이 있다. 즉 공간 영역 LSB 기법은 커버 이미지에 많은 비밀 메시지를 저장할 수 있지만 숨겨진 자료가 단순한 공격에 의해 노출될 수 있다. 일반적으로 지금까지 사용되어지는 공간 영역 기술은 다음과 같이 분류된다[7].

-Edges based data embedding(EBE)
-Least significant bit(LSB)
-Pixel value differencing(PVD)
-Random pixel embedding(RPE)

PVD 방법은 일반적으로 삽입 비트의 깊이를 결정하는 두 개의 연속적인 픽셀의 차이를 계산함으로써 공격자로부터 감지할 수 없는 효과를 제공한다. 그러나 픽셀 값 차이에서 숨겨진 자료 비트 크기가 두 픽셀 사이의 간단한 관계를 이용하여 커버 이미지의 두 개의 연속적인 픽셀들 사이의 차이에 의해 추정될 수 있는 단점이 있다.

2.1.2 Transform Domain Technique

커버 이미지에 비밀 정보를 숨기는 복잡한 방법인 알고리즘과 변환 기법을 이용한다. 신호의 주파수 영역에서 주파수 계수를 변화시켜 자료를 삽입하는 과정은 공간 영역에서 동작하는 삽입 원칙보다 강하고 효과적이다. 즉 공간 영역의 방법보다 외부적 공격에 강한 특징을 가지고 있다. 대부분의 효과적인 스테가노그래픽 시스템은 공간 영역 기술의 장점을 가지고 있는 변환 영역 기법 안에서 작동한다. 일반적으로 지금까지 사용되어지는 변환 영역 기술은 다음과 같이 분류된다[7-8].

-Discrete Fourier transformation(DFT)
-Discrete cosine transformation(DCT)
-Discrete Wavelet transformation(DWT)

DCT 기법은 이산푸리에변환(DFT)과 유사하며, 이미지에서 픽셀 값의 위치를 확산시키는 효과를 준다. DWT는 계층적 이미지를 분해하는 수학적 도구로써 비정지 신호를 처리하는 데 유용하며, 주파수와 이미지의 공간 영역 모두를 설명할 수 있는 정보를 제공한다[6].

2.1.3 Distortion Technique

왜곡 기술은 원래의 커버 이미지와 비밀 메시지가 삽입된 왜곡된 커버 이미지 사이의 차이를 확인하는 디코더 과정 동안에 원본 커버 이미지의 정보가 필요하다. 스테고 이미지가 주어진 메시지 픽셀에서 커버 이미지와 다른 경우에 메시지 비트는 1의 값을 부여한다. 반대일 경우 메시지 비트 값을 0으로 설정한다. 이미지의 통계적

속성에 영향을 주지 않는 방식으로 인코더는 픽셀 값을 1로 수정할 수 있다[3,7]. 일반적으로 스테가노그래피 기법에서 공격자로부터 탈취를 보호하기 위해 커버 이미지는 한 번 이상 사용하지 않는다. 또한 메시지가 부정확한 정보와 함께 인코딩 된다면 변화는 역전될 수 있으며 원래의 메시지가 노출될 수 있는 단점이 있다.

2.2 LSB Mehtod

LSB 기반의 접근법은 공간 영역에서 스테가노그래피 알고리즘의 대표적인 유형이다. LSB의 장점은 커버 이미지의 LSB에 비밀 메시지의 비트 정보를 삽입시키는 것으로 쉽고 단순하며, 폭넓게 이용되는 기법이다.

2.2.1 (Sequential) Least Significant Bit Encoding(LSB)

픽셀에서 마지막 비트를 최하위 비트라고 부르며, '1'에 의해서만 픽셀 값에 영향을 미칠 수가 있다. LSB 스테가노그래피는 커버 이미지의 최하위 비트에 비밀 메시지의 비트 정보를 대체하는 간단한 기술이며, 현시점에서 LSB 삽입 방법은 매개체내에서 메시지를 숨기는 여러 기법 중의 기초가 되고 있다. 그리고 비밀성을 확보하기 위해 삽입하기 전에 비밀 메시지를 암호화 한다[3,8]. 인터넷에서 사용되는 모든 멀티미디어 객체를 커버 매체로 이용할 수 있다.

2.2.2 Random Least Significant Bit Embedding (RLSB)

LSB 삽입 기법의 단점은 이진화 표현으로 이루어진 두 값 형태에서 감지할 수 있는 인위적인 자료가 존재한다는 것이다. RLSB는 히스토그램 영역에서 쌍으로 이루어지는 규칙적인 이진화 값의 형태를 흩으러 놓으므로 보안 수준을 높이는 효과를 줄 수 있다. 커버 매체의 LSB 중에서 피보나치 알고리즘에 의해 생성된 무작위로 선택된 픽셀에 비밀 메시지의 비트 정보를 숨기는 기법이다. 1과 0의 숫자가 동일하고, 스테가노그래피를 이용하여 삽입되어야 하는 비밀 메시지에 랜덤하게 분포될 경우 각각의 쌍으로 이루어진 값에서 두 값의 주파수는 메시지 삽입전과 후가 동일하다[9].

2.2.3 Edge Least Significant Bit Embedding(ELSB)

일반적으로 이미지에서 가장자리 픽셀을 사용한다. 커버 이미지에서 두 LSB 비트를 마스킹하는 것에 의해 불가시화 한 이미지(masked image)를 계산할 수 있다. 다음으로 캐니에지(Canny Edge) 검출 방법을 사용하여 가장자리 픽셀을 구별한다[4,9]. 임의적인 가장자리 픽셀을 선택한 후 가장자리 픽셀의 LSB 비트에 메시지를 삽입한 스테고 객체를 신뢰되는 수신자에게 송신할 수 있으므로 견고성이 향상된다. 가장자리 픽셀을 계산하기 위해 동일한 불가시화 한 이미지를 사용하기 때문에 송신자와 수신자는 동일한 가장자리 픽셀 정보를 이용할 수 있다.

2.3 최근 연구동향

최근에 대부분의 스테가노그래피 연구에서 LSB를 기반으로 하는 은닉 기법이 주로 이용되어졌으며, 다음과 같은 영역으로 연구되어지고 있다[5]. 즉 커버 이미지에 대용량 비밀 자료를 효과적으로 삽입하는 방법, 공간 영역에서 좀 더 새롭고, 개선된 스테고 개체를 감지할 수 없는 기법, 스테간 분석에 대응하는 효과적인 저항성 방법, 커버 이미지의 주파수 영역에서 비밀 메시지를 효과적으로 삽입하는 방법, 스테고 이미지만을 이용한 효과적인 비밀 메시지 추출 방법과 이미지 왜곡을 줄이고 PSNR과 수용 능력을 개선하는 영역으로 연구되어지고 있다.

3. 분석도구

일반적으로 스테가노그래피 기술의 성능을 평가하기 위해 보안성, 수용 능력, 지각 투명성을 이용한다. 스테가노그래피 알고리즘의 성능은 여러 가지 특성을 사용하여 측정할 수 있다.

3.1 Evaluation Criteria

스테가노그래피 기술의 성능을 평가하기 위한 요소는 ①지각 투명성, ②수용 능력, ③견고성 및 보안성, ④위변조 방지(저항성), ⑤계산 복잡도, ⑥파일 크기의 변화 등이 있다.

Table 1에서 스테가노그래피 알고리즘의 커버 매체 유형에 따라 측정 도구별 특성을 보여준다. 스테가노그래피 기법을 적용할 때 커버 매체로써 이미지를 사용하는 것이 나쁘지 않다는 것을 확인할 수 있다[9-10]. Table 2는 이미지 스테가노그래피에서 사용하는 기법, 측정 방법과 성능에 따라 장점과 단점을 보여준다[7,9]. 공간적과 변환적 측면에서 측정 도구와 적용기법에 따라 장점과 단점이 서로 맞물려서 존재함을 확인할 수 있으며, 이미지 스테가노그래피의 경우 전반적으로 보안성을 강화해야함을 알 수 있다.

Table 1 Steganograhic measure and pattern its factors

Measures	Text	Image	Audio	Video
①	medium	high	high	high
②	low	medium	high	high
③	low	medium	high	high
④	low	high	high	high
⑤	low	low	high	high
⑥	low	medium	high	medium

Table 2 Image steganograhy analysis

Domain	Method	①	②	③	④	⑤
Spatial	LSB	○	X	X	X	○
Spatial	ELSB	○	○	X	X	○
Spatial	PVD	○	○	X	X	X
Transform	DCT	○	X	X	○	X
Transform	DWT	X	X	X	○	X
Distortion	-	X	X	X	-	-

Table 3은 이미지 스테가노그래피에서 사용되는 기법에 따라 성능을 보여준다[3,7,9]. 평가적인 면에서 적응적 기법을 이용한 LSB와 DCT를 기반으로 하는 스테가노그래피를 사용하는 것이 효과적이다.

Table 3 Performance of image steganograhy algorithm

Comparison	Single -LSB	Adaptive		DCT Walsh Transform	DCT&Wavelet& Walsh Wavelet
		LSB&PVD	LSB& DCT		
Invisibility	low	medium	high	high	high
Capacity	high	high	high	high	medium
Robustness	low	medium	high	medium	high
Encryption	low	high	high	high	high
PSNR	medium	-	high	-	low

Table 2와 Table 3에서와 같이 공간 영역에서 LSB 기술은 높은 수용 능력을 가지고 있지만, 통계적 공격을 예방하지 못하며, 쉽게 노출될 수 있는 취약점이 있다. DCT, DWT 적용방법을 활용하는 적응적 스테가노그래피는 외부 공격에 쉽게 노출되지 않으며, 변환 영역에서 계수를 수정하고, 이미지 왜곡을 최소화하기 때문에 효과적인 결과를 얻을 수 있다. 숨겨진 메시지의 크기가 작을 때는 매우 효과적이지만 수용 능력이 작다는 단점이 있다. 그러나 DWT 영역에서 삽입 기법을 적용하면 구조적인 결과를 확인할 수 있으며, DCT 삽입 기법의 단점을 보완할 수 있으나 계산적인 측면에서 매우 복잡하게 된다.

Table 4에서 LSB 적용 기법에 따라 성능평가별 장점과 단점을 보여주며[9], (*)표시는 Fig. 1에서 제시한 것과 같이 비밀 메시지에 암호키와 다중재배열키를 적용한 것이다. 견고성과 저항성 면에서 ELSB를 적용하는 것이 효과적임을 확인할 수 있다.

Table 4 Evaluation of LSB techniques

Comparison	LSB	RLSB	ELSB
Pixel components	sequential	random	edge
③	low	low	medium(→high*)
④	low	medium	high(→high*)
⑤	low	low	medium

3.2 Evaluation Tools

커버 이미지에 비밀 메시지를 삽입하는 과정에서 스테고 이미지의 왜곡 정도를 측정하는 도구로 PSNR(peak signal to noise ratio)를 (2) 식으로 구할 수 있다[8,10].

$$SNR \quad 10 \cdot \log_0 \frac{C_{max}^2}{MSE} \tag{2}$$

여기에서 MSE(mean square error)는 (3) 식으로 계산할 수 있다.

$$MSE = \frac{1}{mn} \sum_{i=1}^{m} \sum_{j=1}^{n} (Ste_{ij} - Cov_{ij})^2 \tag{3}$$

DCT 알고리즘을 적용할 때 커버 이미지에 자료를 삽입하는 용량을 (4) 혹은 (5) 식으로 계산할 수 있다[10-11].

$$Capacity = \frac{m \cdot n}{64} \cdot b(c-15) \tag{4}$$

$$Capacity = \frac{1}{2} \cdot \log_2(1 + signal\ to\ noise) \tag{5}$$

여기에서 일반적으로 C_{max}는 255를 사용하며, PSNR이 40보다 작을 경우 왜곡이 심각하여 원본 이미지와 비교자체를 할 수 없다. Ste_{ij}는 생성된 스테고 이미지를 나타내며, Cov_{ij}는 커버 이미지를 나타낸다. 또한 i, j는 이미지의 좌표를 나타내며, m, n은 커버 이미지의 차원을 표시한다. c는 삽입된 계수의 수, b는 각 계수에서 비트의 수를 의미한다.

자료의 보안적인 측면에서 ELSB는 LSB와 RLSB 보다 안전하며, 저장 용량은 근소하게 감소할 수 있다. 따라서 이미지의 가장자리에서 비밀 메시지를 삽입하기 위해 LSB를 기반으로 하는 이미지 스테가노그래피 알고리즘을 이용하는 것이 효과적임을 확인한다.

4. 적 용

논문에서 사용된 비밀 메시지의 크기는 1,032 바이트이며, 비밀 메시지를 비트 패턴으로 변환한 후 스트림 암호를 이용하여 암호화하였으며, 재배열함수($d=2$, 재배열키 : 51627384)를 적용한다. 여기에서 사용한 커버 매체의 크기는 25,478바이트이다. 최하위 비트의 2비트에 정보를 은닉하여도 지각 투명성에 문제가 없기 때문에 커버 매체의 마지막 2비트를 마스킹하여 비트화된 비밀메시지를 은닉하는 방법을 적용한다. 알고리즘을 구현하는 과정은 J2SE을 이용하였다. 이미지 품질을 평가하는 모수로 정규화 된 상호상관, 평균 값 차이, 최대값 차이 등을 기반으로 하며, 삽입 용량, 지각 투명성, PSNR을 확인한다.

Fig. 3은 MSE에 따라 삽입 용량과 PSNR 값의 관계를 보여준다. 전체적으로 보아 LSB와 ELSB를 각각 적용할 때 ELSB를 이용한 삽입용량은 미세하게 감소하고, PSNR 값의 차이는 거의 없다. ELSB는 각 픽셀에서 마지막 2 비트를 마스킹한다는 측면과 Fig. 1에서 제시한 비트화된 비밀 메시지에 다중재배열키와 암호화키를 이용함으로 위변조의 저항성과 견고성이 강화되었

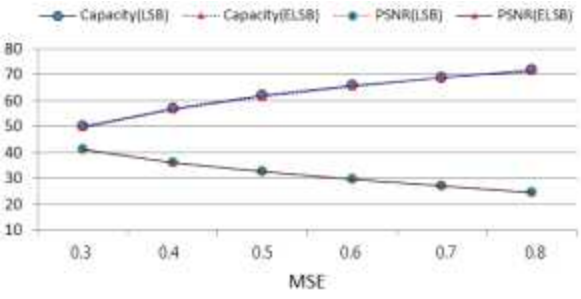

Fig. 3 Effect of MSE, capacity, PSNR

Cover image(25,478) JPEG, DCT/LSB, ELSB	Stego image(26,277) message(1,032)
	

Fig. 4 Cover and Stego image(Byte)

다는 것을 확인한다. 또한 MSE 값이 커짐에 따라 삽입 용량이 증가하지만 PSNR 값은 작아짐을 확인한다.

커버 이미지에 비밀 메시지가 삽입되는 전과 후의 결과는 Fig. 4에서 보여주며, 왜곡을 판단하기 위한 PSNR 값은 49.678으로써 스테고 이미지가 외부적 영향에 의한 왜곡으로 판단된다고 할 수는 없다.

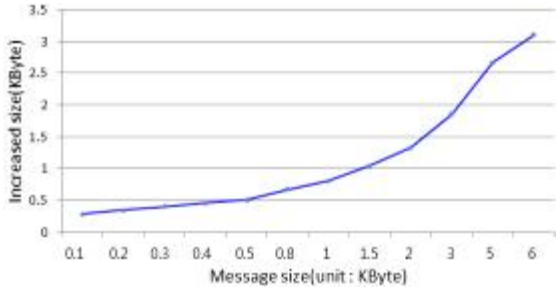

Fig. 5 Comparison of Stego size against message size(KByte)

Fig. 5는 숨겨지는 메시지의 크기가 커짐에 따라 스테고 매체의 크기가 커지는 것을 보여주며, 은닉 메시지가 커버 매체의 2% 미만일 경우에 증가폭이 크다는 것을 확인할 수 있다. Fig. 6은 숨겨지는 메시지가 100Byte, 200Byte, 400Byte에 따라 스테고 매체의 픽셀값 변화를 보여준다.

그러므로 커버 매체의 크기에 변화가 있음에도 원본 이미지와 커버 이미지의 차이는 시각적으로 구분할 수 없다. LSB와 ELSB를 적용할 때 지각 투명성, 삽입용량과 PSNR 값에서 차이가 거의 없다. 논문에서 제시한 Fig. 1에서의 방법과 같이 비밀 메시지를 삽입할 때 다중재배열키와 암호화 키를 사용하고, ELSB를 적용함으로써 Table 4에

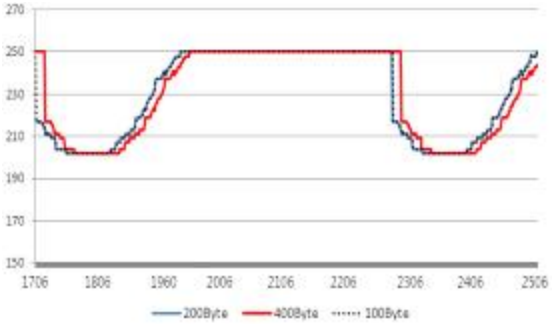

Fig. 6 Pixel values of Stego against message size

서와 같이 저항성과 견고성이 향상됨을 확인하였다.

5. 결 론

커버 이미지는 적어도 전체 영역과 은닉 영역을 원만하게 세분화되어야 하며, 메시지 은닉은 여러 개의 기법이 조합된 복합적인 방법으로 수행되어야 한다. 그러므로 LSB와 RLSB 삽입 방법은 공격자로부터 정보의 탈취가 용이하므로 가장자리 픽셀에 메시지를 은닉하는 ELSB와 DCT 기반이 적용된 이미지 스테가노그래피로 구현되어야 한다. 즉 비트화 된 비밀 메시지의 위치를 바꾸고, 암호화 과정을 추가함으로서 보안성과 견고성이 추가되는 ELSB와 DCT 기반의 적응적 방법의 이미지 스테가노그래피 기법이 효과적이다. 스테고 개체의 품질을 유지하면서 인간의 가시력 및 청취력의 한계를 역이용하며, 복합적인 에지검출(multiple edge detection) 기반의 스테가노그래피 기법은 향후에 연구되어져야 할 영역이다.

Reference

[1] S. S. Ji, “Advanced LSB Technique for Hiding Messages in Audio Steganography”, KIISC, Vol 17, No. 5, pp. 37-42, 2014. (journal)

[2] Ruchi Jain, “An Extensive Survey on Image Steganography”, International Journal of Emerging Technology and Advanced Engineering, Vol 4, Issue 3, pp. 674-679, 2014. (journal)
[3] Kanzariya Nitin K. and Nimavat Ashish V., “Comparison of Various Images Steganography Techniques”, International Journal of Computer Science and Management Research, Vol 2, Issue 1, pp. 1213-1217, 2013. (journal)
[4] S. Sharda and S. Budhiraja, “Image Steganography : A Review”, International Journal of Emerging Technology and Advanced Engineering, Vol 3, Issue 1, pp. 707-710, 2013. (journal)
[5] Sandeep Singh and Aman Singh. “A Review on the Various Recent Steganography Techniques”, International Journal of Computer Science and Network, Vol 2, Issue 6, pp. 142-156, 2013. (journal)
[6] Suvarna Patil and Gajendra Singh Chandel, “Literature Survey on DWT Based Image Steganography”, International Journal of Computer Science and Mobile Computing, Vol 3, Issue 2, pp. 904-909, 2014. (journal)
[7] Mehdi Hussain and Mureed Hussain, “A Survey of Image Steganography Techniques”, International Journal of Advanced Science and Technology, Vol 54, pp.113-123, 2013. (journal)
[8] Stuti Goel, Arun Rana and Manpreet Kaur, “A Review of Comparison Techniques of Image Steganography”, Journal of Electrical and Electronics Engineering, Vol 6, Issue 1, pp. 41-48, 2013. (journal)
[9] K. N. BrahmaTeja, G. L. Madhumati and K. R. Koteswara Rao, “Data Hiding Using EDGE Based Steganography”, International Journal of Emerging Technology and Advanced Engineering, Vol 2, Issue 11, pp. 285-290, 2012. (journal)
[10] Hossein Sheisi, Jafar Mesgarian, and Mostafa Rahmani, “Steganography: Dct Coefficient Replacement Method and Compare With JSteg Algorithm”, International Journal of Computer and Electrical Engineering, Vol 4, No. 4, pp. 458-462, 2012. (journal)
[11] J. R. Smith and B.O. Comisky. Modulation and information hiding in images. In R. Anderson, editor, *Information Hiding, First International Workshop,* volume 1174 of *Lecture notes in Computer Science,* pp. 207 - 226. Springer-Verlag, Berlin, 1996.

지 선 수(Seon-Su Ji)

- 정회원
- 1984년 충남대학교 계산통계학과(학사)
- 1986년 중앙대학교 응용통계학과(석사)
- 1993년 중앙대학교 응용통계학과(박사)
- 2006년 명지대학교 컴퓨터공학과(박사수료)
- (현)강릉원주대학교 정보기술공학과 교수
- 관심분야 : 혼잡제어, 정보보안(암호키, 정보은닉), 스테가노그래피