스테고 이미지에서 은닉메시지 감지기법

(Locating and Searching Hidden Messages in Stego-Images)

지 선 수*
(Seon-Su Ji)

요 약 스테가노그래피는 인터넷에서 은닉메시지가 보내어지는 사실 자체를 숨기는 것이다. 일반적인 스테간 분석은 스테고 신호의 통계량에서 갑작스런 변화인 이상치를 감지하는 것이다. 혼합된 스테고 이미지에 비해 은닉자료가 매우 작은 경우 은닉된 자료의 감지와 위치를 찾아내는 일반적이고 효과적인 감지기법 즉, 이웃한 4개의 픽셀값을 이용한 삽입용량값과 카이스퀘어 검사기법 등을 함께 고려하는 개선된 방법을 제시한다.

핵심주제어 : 삽입용량, 스테간분석, 스테고 이미지, 이산코사인변환(계수), 이상치 감지, 카이스퀘어 검정

Abstract Steganography conceals the fact that hidden message is being sent on the internet. Steganalysis can be detected the abrupt changes in the statistics of a stego-data. After message embedding, I have analyzed for the statistical significance of the fact the occurrence of differences among the four-neighboring pixels. In this case, when a embedding messages within a images is small, use EC value and chi-square test to determine whether a distribution in an images matches a distribution that shows distortion from stego-data.

Key Words : Chi-square test, DCT(coefficient), Embedding capacity, Outliers detection, Steganalysis, Stego-images

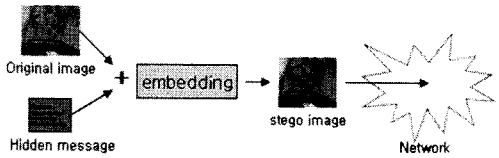
1. 서 론

정보화 사회에서의 비밀통신이란 약속된 특정한 수신인이 아니면 그것이 의미 있는 메시지인지 를 파악할 수 없는 방법을 이용하여 비밀메시지를 송수신하는 방법을 말한다. 경쟁자의 비밀정보를 가로채어 자신에게 유리한 정보를 획득, 위조하고자 하는 노력과 상대방에게 비밀정보가 노출되지 않도록 하는 연구는 과거, 현재 그리고 미래에 끊임없이 계속될 것이다. 그러나 불행하게도 정보를 보호하는 완벽한 송신 수단은 현재 존재하지 않으며, 인터넷에서 송신되는 정보는 항상 제 3자에게 위변조, 탈취될 수 있다는 것을 가정해야 한다.[11] 이러한 현실적 상황에서 암호화되거나 은닉된 정보를 획득하더라도 원래의 의미를 해독하기 위해 암호화된 정보를 분석하는데 시간과 비용이 은닉정보의 가치에 비해 많이 발생하도록 하는 것이 암·복호화 시스템을 개발하는 가장 중요한 핵심이다. 이상적인 상황이라면 허가 받지 않은 개인은 결코 암호화되거나 은닉된 메시지를 읽을 수가 없다. 그러나 현실에서 비밀 통신은 결국에는 상대방에게 노출될 수밖에 없는 시간의 문제이다. 최근 기업의 고객 정보 및 핵심 기술이 내부자에 의해 유출되는 사례가 점차 증가하고 있으며, 그 유출

* 강릉원주대학교 컴퓨터정보공학부

방법 또한 다양한 디지털 매체를 통해 급속하게 지능화되고 고도화되고 있다.

스테가노그래피는 <그림 1>과 같이 메시지 자체를 숨기고 위장하는 것이다. 스테가노그래피는 전달하려는 비밀정보를 그래픽, 사진, 비디오, 소리 파일 등에 단순하게 은닉하거나 암호화해 숨기는 심층암호 기술로써 정보를 교환하고 있다는 것을 숨기면서 통신을 하는 기술이다. 그러나 스테가노그래피는 암호화 기법과는 다르게 정보를 전송하는데 있어서 많은 양의 오버헤드를 요구하지만, 비교적 많은 양의 정보를 은닉할 수 있다.



(그림 1) 원본이미지에 은닉메시지가 포함되는 과정

일반적으로 스테가노그래피의 공격방법은 크게 6가지로 나뉘어 설명된다.[6] 즉 은닉된 자료를 갖는 파일 등의 공격, 원본과 혼합된 파일 등의 모두를 공격, 사전에 전달되는 매개체가 알려진 원본파일 등의 공격, 은닉알고리즘이 알려진 상태의 공격, 은닉알고리즘과 메시지가 알려진 상태의 공격, 원본, 혼합된 파일, 알고리즘의 모든 요소를 공격하는 방법 등이다. 현재 멀티미디어 데이터 중에서 비교적 쉽게 다룰 수 있는 정지 영상 데이터를 이용한 스테가노그래피 기법이 많이 개발되어 활용되고 있다. 그 중에서 대표적인 방법 중 하나가 디지털 정지영상 데이터에 정보를 숨기는 대표적인 것이 LSB(least significant bit) 삽입방법이다. 또한 변환공간영역(transformed domain)에서 스테가노그래피가 많이 사용되고 있는데, 대표적인 것이 JPEG 압축 알고리즘에 사용된 DCT(discrete cosine transform) 영역에서 메시지를 숨기는 방법이 있다.[11]

스테가노그래픽 구조에서 은닉된 정보를 감지하기 위해 3가지 범주 -모델기반(model based), 통계량보전(statistics preserving), 덧씌우기기반(masking based)- 등으로 나누어 설명하며, 여기에서는 통계적 보전기법을 고려한다. 일반적으로 이미지가 삽입될 때 이상치가 발생하여 픽셀값의 퍼짐성 효과가 나타난다. 삽입되는 메시지 용량이 증가할수록 삽입된 자료는 통계적 기법, 예민한 시각적 능력 등에 의해 검출될 수 있기 때문에 원본이미지에 비해 은닉자료가 5%에서 10% 범위내에서 효율적인 정보은닉이 가능하다.[4][7] 또한 카이스퀘어 검사 등을 이용하여 은닉메시지 존재를 쉽게 감지할 수 있다. 그러나 원본이미지에 비해 은닉자료가 매우 작게 혼합되어 있을 때 기존의 이웃한 2개의 픽셀값을 이용한 카이스퀘어 방법 등에 의해 은닉자료를 감지하고 위치를 찾아내는 것이 어렵다. 따라서 원본이미지에 비해 은닉자료가 1%이하인 작은 경우에 은닉자료의 감지와 위치를 찾아내는 연구가 필요하다.

이 논문에서는 혼합된 스테고 이미지에 포함된 작은 크기의 은닉된 정보를 이웃한 4개의 픽셀값을 이용한 카이스퀘어 검사기법, 삽입용량(EC)값, 신호잡음비(SNR)값 등을 함께 이용하여 감지하고 위치를 찾는 개선된 기법을 제시한다. 논문의 구성은 다음과 같다. 2장에서 이상치 감지기법에 대한 관련 연구에 대하여 조사하고, 3장에서는 이상치 감지와 이웃한 4개의 픽셀값을 이용한 카이스퀘어 통계적 모델, 삽입용량, SNR 등을 가지고 은닉자료의 위치를 찾아내는 방법을 제시한다. 4장에서의 실험 결과를 가지고, 5장에서 결론을 제시한다.

2. 이상치 감지기법의 관련연구

일반적으로 이미지에 은닉자료가 혼합되었을 때 칼라이미지에서 혼합된 이미지의 87%를 찾아내고, 흑백이미지의 경우 61%를 감지한다. 그러나 원본이미지에 비해 은닉자료가 매우 작을 때 혼합이미지에서 은닉정보를 감지하는 것은 매우 어렵다. 스테간분석의 궁극적인 목표는 혼합된 스테고 이미지와 원본이미지를 분류하는 것과 숨겨진 이미지를 추출하여 제거한 후 은닉된 메시지의 위치를 찾아내는 것이다. 이때 대부분의 학자들은 이웃한 픽셀의 RGB 값과 관련된 수치값 등을 이용하였다.

일반적으로 원본이미지와 혼합이미지를 비교하기위하여 유효하지 않더라도 끼워넣기 과정에서 왜곡개념을 도입하여 사용한다. Aura는 덮개매체에서 비트를 선택하기위한 의사난수 순열을 이용

하였다. 또한 비밀키와 덮개크기가 변하지 않게 남아 있다면 선택된 비트는 같은 것이라고 결론지었다.[1] Provos는 일반적인 스테가노그래픽 기술이 덮개매체에 있는 통계적인 특성을 변경시킬 수 있는 방법을 지적하였다. 즉, 주어진 원본이미지에 은닉이미지를 끼워 넣은 혼합된 스테고 이미지의 색상주파수가 변화될 수 있다. 예를 들어 JPEG 이미지에 있는 포함된 자료의 특정한 프로그램을 평가한다. 이러한 프로그램에 의해 숨겨진 정보를 감지하기 위하여 숨겨진 정보를 나르는 이미지의 색상분포를 추정하고 관찰 분포에 대응하는 것과 비교하는 확장된 카이스퀘어 검사기법을 이용하였다.[12]

Farid와 Davidson 등은 주어진 이미지에서 비밀메시지의 위치를 감지하기 위해 이상치를 이용한 통계적 기법과 인공신경망을 이용하였다. 특수한 기법을 이용하여 메시지를 은닉할 경우 포함된 메시지를 구별하거나 위치를 찾아내는 것은 매우 어려운 작업이라고 결론 내었다.[2][9] 스테고 이미지에서 은닉메시지를 감지하기 위해 비모수적 모델을 고려하고, 이상치를 분류하는데 데이터 마이닝 기법과 총 픽셀 수의 0.33%의 상위 이상치를 표시하여 은닉자료를 최대 96%까지 구별할 수 있음을 보였다. 이때 거리와 분포를 고려하였다. 또한 각 픽셀의 단순한 벡터모델은 공간적으로 흥미 있는 픽셀을 구별하게 할 수 있다. 이미지에서 비정상적인 주름선, 직선과 같은 것을 제거하기위한 이미지 복원접근에 Ising모델을 적용하였다. 에너지 구성에서의 교란이 발생할 경우 에너지가 증가된다는 것을 이용하여 에너지량을 계산하여 은닉이미지를 감지하였다. 특히 흑백이미지일 경우 이웃한 픽셀값이 같은 명암도를 갖는다면 색체범위에서의 작은 변화는 픽셀 명암도에 변화를 주지 못한다는 것을 확인하였다.[4][5] Dang과 Kota는 주파수영역으로 공간영역에서 픽셀값에 대응하기위해 이산 퓨리에 변환함수를 이용하였으며 이러한 접근형태가 숨기려는 메시지의 능력에는 제한이 있으나 좀 더 좋은 견고성을 제시할 수 있음을 보였다.[3] 혼합이미지에서 스테간분석을 위해 공간종속성을 완벽하게 수량화할 수 없음에도 불구하고 마코브 체인을 모델화하여 실질적인 스테간분석 알고리즘을 수행하기위한 다루기 쉬운 예측구조를 분석적으로 제공하였다. 또한 감지오류비율을 4%까지 낮게 대역확산은닉의 특성을 감지하는 방법을 제안하였다.[13]

3. 이상치 감지모델

스테고 이미지 신호에서 정보은닉의 존재유무를 판단하기위해 사용하는 확률변수 n_k는 θ에 대해 모수화된 확률밀도 $p_\theta(n)$을 갖는다고 가정한다. 여기에서 θ는 스칼라 혹은 벡터값을 가질 수 있다.

$$n_k = x_k + \gamma h_k, \quad k=1, 2, ..., N \tag{1}$$

여기에서 x_k는 k번째 원본신호의 DCT 계수(coefficient)이다. h_k는 가우시안 분포를 따르는 메시지 통신(message carrier)이며, γ는 메시지 길이이다. 이를 기반으로 다음과 같은 두 개의 가설을 설계할 수 있다.

$$H_o : \theta = \theta_o (no\ embedded\ message)$$
$$H_1 : \theta = \theta_1 (embedded\ message)$$

실제 적용에서는 모수 θ_o와 θ_1의 사전정보가 전혀 알려지지 않을 때 즉, 주어진 이미지 정보만을 가지고 은닉메시지의 존재유무를 판단할 수밖에 없다.

일반적으로 공간영역과 주파수영역을 상호 변화시키는 매핑기술의 대표적인 DCT는 임의의 데이터 배열을 코사인 함수의 합으로 표현할 수 있다는 성질을 이용한다. 또한 계산의 복잡성 때문에 2차원 8×8 DCT 계수는 다음의 공식에 의해 구하여 사용할 수 있다.[4][12]

$$C(u,v) = \frac{1}{4}\rho(u)\rho(v)\sum_{i=0}^{7}\sum_{j=0}^{7} f(i,j) \cdot \cos\left[\frac{(2i+1)u\pi}{16}\right]\cos\left[\frac{(2j+1)v\pi}{16}\right] \tag{2}$$

여기에서 u, v는 2차원 8×8 블록에서 계수의 위치를 나타낸다. u, $v \in \{0, 1, 2, ..., 7\}$에 대해

$\rho(u)$와 $\rho(v)$는 다음 식에 의해 사용된다.

$$\rho(u)=\begin{cases}\frac{1}{\sqrt{2}}, & u,\ v=0\\ 1, & \text{이외의 경우}\end{cases} \quad (3)$$

$f(i,j)$는 DCT 변환이 이루어지기 전의 블록내에서 0부터 255사이의 픽셀(밝기)값을 의미한다. i, j는 블록내에서 각 픽셀의 위치를 의미한다.

지금까지의 대부분 학자들은 변조된 이미지를 감지하기위해 두 개의 이웃한 픽셀값을 기반으로 한 카이스퀘어 검정방법을 이용하였다. 이와 같은 기법은 미세한 은닉정보의 경우 감지가 어렵다는 단점이 있다. 이 논문에서는 스테고 이미지 신호 n_k를 기반으로 하여, 현재의 픽셀값과 이웃한 4개의 픽셀값의 평균값과의 차이를 고려하는 수정된 통계량을 가지고, 은닉정보 존재유무를 판단하기 위해 카이스퀘어 값을 활용하며, 삽입용량값과 SNR값 등을 확인한다.

...	...	...	...	...
...	$n_{i-1,j-1}$	$n_{i-1,j}$	$n_{i-1,j+1}$	...
...	$n_{i,j-1}$	n_{ij}	$n_{i,j+1}$	...
...	$n_{i+1,j-1}$	$n_{i+1,j}$	$n_{i+1,j+1}$	...
...	...	...	...	...

Lee와 Chen[8]이 제안한 것과 비슷하게 서로 이웃한 4개의 픽셀값을 기반으로 각 픽셀(i, j)의 삽입용량(EC:embedding capacity)은 다음과 같이 계산한다.

$$K(i,j)=\log_2 D(i,j) \quad (4)$$

여기에서 $D(i,j)$는 다음과 같이 각각 계산하여 사용할 수 있다.

$$D(i,j)=\max\{n_{i-1,j-1},\ n_{i-1,j},\ n_{i,j-1},\ n_{i,j}\} - \min\{n_{i-1,j-1},\ n_{i-1,j},\ n_{i,j-1},\ n_{i,j}\} \quad (5)$$

일반적으로 예민한 시각적 능력에 따라 흑백이미지의 경우 삽입용량의 허용한계 값 $U(i,j)$를 다음과 같이 정하여 사용한다. 이때 경험적으로 t값은 191로 설정하여 사용한다.[8]

$$U(i,j)=\begin{cases}4, & \text{if } n_{i,j}\leq t\\ 5, & \text{이외의 경우}\end{cases} \quad (6)$$

각각의 픽셀에서 삽입용량을 계산한 후 이상치 존재 가능성을 검사하여, 은닉메시지의 길이와 이동된 LSB 평면을 확인할 수 있다.
이웃한 4개의 픽셀값을 기반으로 이웃한 값의 평균을 다음과 같이 계산할 수 있으며,

$$y^{*}_{2i,2j}=\frac{n_{2i-1,2j-1}+n_{2i-1,2j}+n_{2i,2j-1}+n_{2i,2j}}{4}$$
$$y_{2i,2j}=n_{2i,2j}, \quad (7)$$

(8)식을 이용하여 카이스퀘어 통계량을 계산한 후 기각역과 비교하여 은닉자료의 삽입 유무를 판단한다. 즉, $\chi^2_{ad}>\chi^2_{(df,\ \alpha)}$이면 이미지에 은닉정보가 존재해 있는 스테고 이미지라고 판단한다.

$$\chi^2_{ad}=\sum_{i=1}^{df/2}\sum_{j=1}^{df/2}\frac{(y_{2i,2j}-y^{*}_{2i,2j})^2}{y^{*}_{2i,2j}} \quad (8)$$

여기에서 df는 자유도, α는 유의수준을 나타낸다. 인접된 두 분포가 같은 확률 p값은 다음 식에 의해 구할 수 있다. 여기에서 $\Gamma(df)$는 감마분포를 나타낸다.

$$p=1-\frac{1}{2^{\frac{df}{2}}\Gamma(\frac{df}{2})}\int_0^{\chi^2_{ad}} x^{\frac{df-2}{2}}e^{-\frac{x}{2}}dx \quad (9)$$

신호와 잡음신호의 비율을 정량적으로 나타내기 위한 지표로서 사용되는 신호 잡음비(SNR: signal to noise ratio)는 다음과 같이 계산할 수 있다.[8][10]

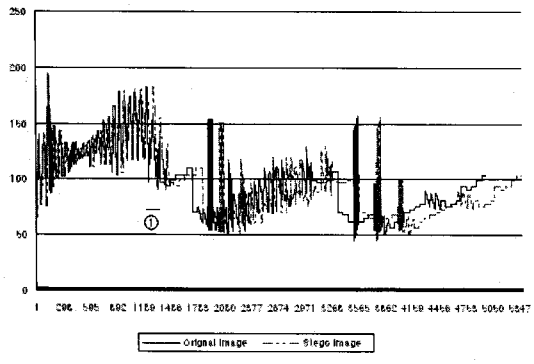
$$SNR = 10 \cdot \log_{10} \frac{L^2}{\frac{1}{n \cdot m} \sum_{i=1}^{n} \sum_{j=1}^{m} (y_{2i,2j} - y^*_{2i,2j})^2} \quad (10)$$

여기에서 L은 이미지의 최대신호수준을 나타내며, 8비트 기준의 흑백이미지인 경우 255를 이용한다. n과 m은 이미지의 행의 수와 열을 수를 각각 나타낸다. 일반적인 자료일 때 SNR값이 15, 이미지일 경우 32이상이면 양호한 수준으로 판단한다. SNR의 비율이 감소한다는 것은 정보가 잡음으로 인해 손실될 수 있다는 특성을 가지고 은닉이미지의 존재 가능성을 확인할 수 있다.

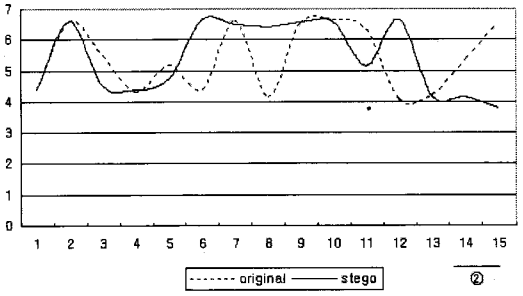
(4), (8), (10)식을 이용하여 스테고 이미지에서 은닉자료의 위치를 감지할 수 있음을 확인한다. 여기에서는 원본 흑백이미지(512×512, 32,533Byte)에 78Byte 크기의 은닉메시지를 삽입한 스테고 이미지(512×512, 33,472Byte)의 경우만을 생각한다. 이때 1블록 단위를 고려한 상태에서 이웃한 4개의 픽셀값 등을 구하는 과정을 JAVA와 MatLab 언어를 이용하여 구현하였다.

4. 적용 및 결과

<그림2>에서 원본이미지와 스테고 이미지 픽셀값을 비교할 때 특정영역, 예를 들어 ①부분에서의 이상신호를 참고로 하여 은닉자료가 존재한다는 것을 확인한다. 그러나 현실적으로 스테고 이미지 정보만 얻을 수 있으므로 스테고 이미지 정보만을 가지고 각 블록에서 Provos[12]가 사용한 방법, (8)식에 의해 제시된 방법, p값, EC값, SNR값 등을 확인해 본다.



(그림 2) 원본이미지와 스테고 이미지의 픽셀값 비교



(그림 3) 원본이미지와 스테고 이미지에서 각각의 삽입용량 비교

<그림3>에서 원본이미지와 스테고 이미지의 삽입용량을 비교할 때 ②부분영역에서 삽입용량이 감소하는 것을 확인할 수 있다.

이웃한 픽셀값을 고려할 때 혼합된 스테고 이미지의 경우 각 픽셀의 평균 삽입용량은 5.18 (≥ 4.0)이므로 수치값 만으로 이미지에 은닉정보가 존재한다고 할 수는 없다는 것을 <표1>에서 확인할 수 있다. 또한 SNR값이 충분히 크므로 왜곡된 정보가 존재하지 않는다라고 판단할 만큼 매우 양호한 수준으로 결론지을 수 있다. 즉, 왜곡된 정보의 존재를 판단할 수 없다.

<표 1> 2(4) NBD 픽셀값을 이용한 각각의 삽입용량과 SNR값

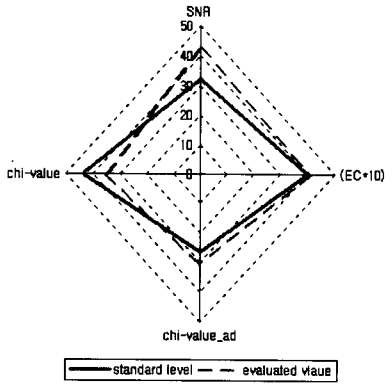
구분	EC	SNR	정보은닉
2 NBD pixel	5.18	40.9	false negative
4 NBD pixel	4.10	42.0	false negative

원본이미지에 비해 은닉자료가 0.24%인 경우 이웃한 픽셀값을 기반으로 한 카이스퀘어 검정기법을 적용하면 은닉메시지가 존재한다는 것을 감지하지 못한다는 것을 <표2>에서 확인할 수 있다. 즉, 현시점에서 귀무가설을 기각할만한 정보를 가지고 있지 않다.

<표 2> 기존방법과 수정된 방법에 의한 카이스퀘어 값과 각각의 p값

구분	$\chi^2 > \chi^2_{(df,\,\alpha)}$	p값	정보은닉
기존방법 Provos[12]방법	35.05 < 43.77	0.998	false negative
수정방법	30.38 > 26.29	0.994	true detection

은닉메시지가 있을 경우 p값이 높게 나타날 수 있다는 것을 이용하여 은닉메시지의 위치를 감지할 수 있지만 은닉자료가 작을 경우 원본이미지와 스테고 이미지를 구분하는 것은 거의 불가능함을 확인할 수 있다.
그러나 이웃한 4개의 픽셀값을 고려할 때 삽입용량의 한계점 가까이 변함(그림4 참조)에 따라 은닉정보의 존재를 의심할 수 있다. 또한 <표 2>에서 유의수준(α)이 0.05일 경우 제시된 이웃한 4개의 픽셀값을 이용한 카이스퀘어 값을 이용할 경우 이미지에 은닉정보가 포함되어 있다고 판단할 수 있다. 따라서 은닉정보가 매우 작은 경우 EC값과 함께 제시된 4NBD 픽셀값을 이용한 카이스퀘어 검정법이 효과적임을 확인할 수 있다.



(그림 4) SNR, EC, Chi-square 값 비교

5. 결 론

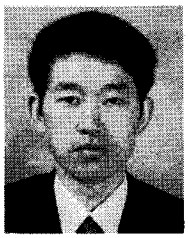
송신되는 특정정보가 전달하고자 하는 수신자 이외의 의도적인 공격자에게 읽히거나 내용이 파악되는 것을 막기 위해 원본이미지에 특정 메시지를 은닉하고 암호화할 때 스테가노그래픽 에 의한 정보전달 방법은 보완수준을 더욱 강화 할 수 있다. 원본이미지에 비해 은닉정보가 15%이상이 될 경우 스테고 이미지는 일그러지거나 이미지 품질이 급격하게 떨어질 수 있어 정보은닉기법으로서의 가치가 소멸된다. 원본이미지에 비해 은닉정보의 크기가 1%이하일 경우 은닉유무 자체를 판단하는 것은 매우 어렵다. 또한 SNR값이 양호한 수준으로 형성되어 왜곡정보가 포함되어 있다고 할 수 없다.

그러나 제시한 이웃한 4개의 픽셀값을 기본으로 하는 통계량을 이용할 경우 EC값은 의심되는 영역 가까이 위치함을 확인하였다. 또한 카이스퀘어 검정방법을 사용할 경우 감지가 가능하다는 것을 확인할 수 있다. 따라서 원본이미지에 비해 은닉이미지의 크기가 매우 작은 경우에 즉, 인터넷에서 획득한 스테고 이미지에서 은닉정보의 존재와 위치를 감지하기 위해 이웃한 4개의 픽셀값을 이용한 EC값, 카이스퀘어 검정방법을 함께 사용하는 것이 효과적이다. 같은 조건에서 CUSUM-SPRT를 이용하여 혼합된 스테고 이미지로부터 은닉자료의 유무를 감지하고 위치를 찾아내는 기법은 향후 좀 더 연구가 진행되어야 한 부분이다.

참 고 문 헌

[1] T. Aura, "Practical invisibility in digital communication", Journal on Selected Areas in Communications, Vol. 16, No. 4, pp. 474-481, 1988.
[2] G. Berg, I. Davidson, M. Y. Duan and G. Paul, "Searching For Hidden Messages: Automatic Detection of Steganography", Conference : Innovative Applications of Artificial Intelligence, 2003.
[3] Xuan-Hien Dang and K. C. S. Kota, "Case Study : An Implementation of a Secure. Steganographic System", Security and Management '06 : LasVegas, Nevada, USA, pp. 84-90, 2006.
[4] I. Davidson and G. Paul, "Locating Secret Messages in Images", KDD'04, Seattle, Washington, USA, 2004.
[5] I. Davidson, G. Paul and S. S. Ravi, "Steganography Using Spatially Interesting Pixels", [Online] Available http://www.cs.albany.edu/~davidson/, 2004.
[6] S. D. Dickman, "An Overview of Steganography", [Online] Available www.infosec.jmu.edu/reports/jmu-infosec-tr-2007-002.pdf, 2007.
[7] Roshidi Din and Azman Samsudin, "Digital

Steganalysis Computational Intelligence Approach", Internation Journal of Computers, Issue 1, Vol. 3, pp. 161-170, 2009.
[8] Y. K. Lee and L. H. Chen, "High capacity image steganographic model", In IEE Proceedings Vision, Image and Signal Processing, 2000.
[9] H. Farid, "Detecting Steganographic Messages in Digital Images", Technical Report TR2001-412, Dartmouth College, 2001.
[10] D. Fu, Y. Q. Shi, D. Zou and G. Xuan, "JPEG Steganalysis Using Empirical Transition Matrix in Block DCT Domain", IEEE MMSP 2006, Canada, 2006.
[11] S. S. Ji, "Detecting Steganographic Contents Using EWM Statistics", KSIIS, Vol. 13, No. 3, pp. 54-62, 2008.
[12] N. Provos, "Defending Against Statistical Steganalysis", 10th USENIX Security Symposium, Washington, DC. pp. 323-335, 2001.
[13] K. Sullivan, U. Madhow, S. Chandrasekaran and B. S. Manjunath, "Steganalysis for Markov Cover Data With Applications to Images", IEEE Transactions on Information Forensics and Security, Vol. 1, No. 2, 2006.



지 선 수 (Seon-Su Ji)

- 정회원
- 1984년 충남대학교 계산통계학과(학사)
- 1986년 중앙대학교 응용통계학과(석사)
- 1993년 중앙대학교 응용통계학과(박사)
- 2006년 명지대학교 컴퓨터공학과(박사수료)
- 원주대학 컴퓨터정보관리과 교수
- 강릉대학교 컴퓨터공학부 교수
- (현)강릉원주대학교 컴퓨터정보공학부 교수
- 관심분야 : 혼잡제어, 정보보안(암호학), 이미지 프로세싱

논문접수일 : 2009년 6월 25일
논문수정일 : 2009년 7월 30일
게재확정일 : 2009년 8월 10일