SPRT를 기반으로 하는 누적합 스테간 분석을 이용한 은닉메시지 감지기법

(Detecting Hidden Messages Using CUSUM Steganalysis based on SPRT)

지 선 수*
(Seon-su Ji)

요 약 스테가노그래피는 이미지의 외적인 면에서 미세한 변화를 가진 디지털 이미지에 자료를 은닉하기 위해 사용된다. 은닉이미지가 의심되는 스테고 신호 분석에서 개선된 통계량을 이용하여 갑작스러운 변화를 신속, 정확하게 감지하는 기법의 개발이 필요하다. 이 논문에서는 축차적인 스테가노그래피에서 은닉된 메시지를 감지하고 그 위치를 찾아내는 방법을 제시한다. 즉, 검사하는 이미지에 은닉메시지의 존재 유무를 결정하고 그 위치를 찾아낼 때까지 CUSUM-SPRT 스테간 분석을 기반으로 하는 통계적 검정을 반복한다. 논문에서 일반화된 수식을 위해 개선된 $S_j^{t^*}$를 이용한 통계량 g_t를 사용한다.

핵심주제어 : 브라운 운동과정, 누적합, 스테간 분석, 스테가노그래피, 이산코사인변환, 자료은닉, 축차확률비 검정

Abstract Steganography techniques can be used to hide data within digital images with little or no visible change in the perceived appearance of the image. I propose a steganalysis to detecting hidden message in sequential steganography. This paper presents adjusted technique for detecting abrupt jumps in the statistics of the stego signal during steganalysis. The repeated statistical test based on CUSUM-SPRT runs constantly until it reaches decision. In this paper, I deal with a new and improved statistic g_t by computing $S_j^{t^*}$.

Key Words : Brownian Motion Process, CUSUM, Data Hiding, DCT, SPRT, Steganalysis, Steganography

1. 서 론

인터넷이 현대인의 생활 중심에 자리매김하면서 인터넷 정보의 신뢰성에 대한 저평가에도 불구하고 인터넷 정보의 파급효과는 예측하기 어려울 정도로 매우 크다. 미래의 인터넷은 화면을 확장하는 것이 아니고 화면 밖으로 나와 현실을 확장해 나가는 방향으로 진행되어지고 있다. 이와 같은 환경에서 사진, 문서, 비디오, 오디오와 같은 아날로그 정보들이 디지털 정보로 변화되면서 수집되는 정보의 형태가 변경되었다. 이러한 기술들과 정보은닉 기법 등이 결합되어 디지털 신호에 필요한 정보를 숨기는 기술은 저작권 문제와 정보전송의 수단으로 이용되는 주요한 기술로 발

* 강릉원주대학교 정보기술공학과

전하게 되었다. 또한 수집된 정보의 종류와 규모가 대규모화되어 내용을 자동으로 식별, 분류하고, 분석하는 기술이 필요하게 되었다.

암호화된 메시지가 해독되거나 노출될 시점에서, 이미 비밀메시지의 정보는 가치가 거의 없어질 수 있다면 암호로서의 가치가 충분히 있다. 스테가노그래피 기법은 특별한 사전지식 없이 사용이 편리하기 때문에 테러리스트의 정보전달 수단의 적절한 도구로 이용되고 있다. 또한 스테가노그래피 기법은 상대적으로 적은 정보비트를 은닉하는데 많은 오버헤드가 요구됨에도 불구하고, 인터넷 환경에서 허가된 수신자에게만 은닉정보를 허용하는 도구로 많이 활용되고 있다. 스테가노그래피는 이미지 안에 메시지를 숨기는 기법으로 메시지를 숨기는 것과 더불어 그 이미지의 전송여부 자체를 알지 못하게 하는 것이 목적이다. 즉, 스테가노그래피는 암호화를 대신하는 것이 목적이 아니다. 암호화와 함께 스테가노그래피 기법을 사용해 보안 수준을 강화시키는 것이 주된 목적이다. 은닉정보가 송수신되는 사실을 인지하지 못하게 하는 스테고 기법은 제 3자의 공격 자체를 차단할 수 있어 암호화 이상의 가치와 효율성을 제공할 수 있다.

일반적으로 이미지 파일의 전체 비율 중 숨기고자 하는 정보의 비율이 5~10%일 때 효율적인 정보 은닉이 가능하다. 정보가 은닉된 스테고 신호에서 신호 잡음비, 삽입용량, 카이스퀘어 검사기법 등을 이용하여 은닉자료의 존재 유무와 위치를 감지할 수 있다. 그러나 원본이미지에 비해 은닉자료가 매우 작게 혼합되어 있을 때 이웃한 2개의 픽셀 값을 이용한 카이스퀘어 검정법 등에 의해 은닉자료를 감지하는 것이 어렵다. 따라서 원본이미지에 비해 은닉자료가 1%이하의 작은 경우에 은닉자료의 감지와 위치를 찾아내는 연구가 많은 학자들에 의해 진행되어지고 있다.[1]-[3] 즉, DCT(discrete cosine transform) 계수를 기반으로 하는 통계량에서 갑작스럽고 미세한 변화를 감지하여 정확한 변화지점을 찾아내는 개선된 스테고 분석 방법이 필요하다.

이 논문에서는 혼합된 스테고 이미지에 포함된 작은 크기의 은닉된 정보를 감지하고, 그 위치를 찾기 위해 픽셀 값과 일반화된 수식을 기반으로 하는 누적합-축차적 확률비 검정기법을 이용하는 개선된 방법을 제시한다. 논문의 구성은 다음과 같다. 2장에서 이상치 감지기법 관련 연구에 대하여 조사한다. 3장에서는 이상치 감지를 위해 정확하고 일반화된 수식을 기반으로 하는 누적합-축차적 확률비 통계량을 가지고 은닉자료의 위치를 찾아내는 방법을 제시한다. 4장에서의 실험 및 적용결과를 가지고, 5장에서 결론을 제시한다.

2. 이상치 감지기법의 관련연구

스테간 분석의 궁극적인 목표는 혼합된 스테고 이미지에서 원본이미지를 분류하는 것과 숨겨진 이미지를 추출하여 제거한 후 은닉된 메시지의 위치를 찾아내는 것이다. 이때 대부분의 학자들은 이웃한 픽셀의 RGB 값과 관련된 수치 값 등을 이용하였다.

Trivedi와 Chandramouli의 연구[4][5]에서 스테간 분석을 위해 확률과정기법을 처음으로 이용되었으며, 스테간 분석을 두 가지 범주 -적극적 스테간 분석과 소극적 스테간 분석- 로 나누어 설명하였다. 확장된 스펙트럼 스테가노그래피를 이용하여 은닉된 메시지의 길이와 위치를 효과적으로 감지하기 위해 축차적 확률비 검정법을 기반으로 하는 축차적 스테간 분석 기법을 제시하였다. 또한 스테간 분석에서 미세하지만 갑작스러운 통계량 변화를 어떻게 감지하는가가 매우 중요하다. 한 시점에서 이미지 표본을 선택하여 변화지점을 감지하고 비밀 삽입키를 추정하는 누적합 스테간 분석 감지기법을 제시하였다. 또한 지역적 최강력(LMP: locally most powerful) 축차적 통계검정을 이용하는 스테간 분석에서 노이즈 신호에 낮은 메시지 신호문제를 연구하였다. 특히 스테고 끼워 넣기 알고리즘의 축차적 특성을 구별하기 위해 누적합과 LMP 기법을 조합하여 비정상적인 자료 분석을 하였다.

지선수의 연구[6]에서는 혼합된 스테고 이미지에서 원본이미지에 비해 은닉자료가 매우 작은 경우 은닉된 자료의 존재유무를 판정하는 일반적이고 효과적인 감지기법이 연구되었다. 즉, 이웃한 4개의 픽셀 값을 이용한 삽입용량 값과 카이스퀘어 검사기법 등을 함께 고려하는 개선된 방법을 제시하였다.

Pevn'y와 Fridrich[7]은 스테가노그래픽 알고리즘이 정보를 은닉하기 전에 공간영역으로 JPEG 이미지를 압축한 후, 은닉정보가 포함되는 동안 기본적인 양자화 행렬을 이용하여 압축이 이루어짐을 설명하였다. 스테가노그래피에서 2중으로 압축된 JPEG 이미지에

서 은닉정보를 감지하는 기법을 제시하였다. 이것은 기본적인 질적 요소(quality factor)의 추정문제에서 처음으로 완벽한 해결책을 보였다.

혼합이미지에서 스테간 분석을 위해 공간종속성을 완벽하게 수량화할 수 없음에도 불구하고 분석을 위한 수학적 공식을 제시하였다. 제시된 구조를 가지고 사전정보가 거의 없는 상태에서 은닉정보를 추출하는 맹인 분류 시스템(blind system identification)을 정의하였다. 실험을 위해 가우시안 분포를 가정하였으며, 확산 스펙트럼 스테가노그래피는 안전하다는 결론을 제시하였다.[1][8]

지금까지의 대부분 학자들은 은닉된 정보를 감지하기 위해 이웃한 DCT 계수를 기반으로 하는 카이스퀘어 검정방법을 이용하였다. 이와 같은 기법은 미세한 은닉정보의 경우 감지가 어렵고, 은닉위치를 찾아내는 것이 불가능에 가깝다. 이 논문에서는 스테고 이미지 신호 자료를 이용하기 위해 정확하고 일반화된 수식을 기반으로 하는 누적합-축차확률비 검정(cumulative sum -sequential probability ratio test: CUSUM-SPRT) 기법을 이용하여 은닉정보 존재유무와 그 위치를 판단한다.

3. 갑작스런 변화 감지

일반적으로 공간영역과 주파수영역을 상호 변화시키는 매핑기술의 대표적인 DCT는 임의의 데이터 배열을 코사인 함수의 합으로 표현할 수 있다는 성질을 이용한다. 또한 계산의 복잡성 때문에 m번째 블록의 DCT 계수는 다음의 공식에 의해 구하여 사용할 수 있다.[6][7]

$$d_{i,j}^{m} = round\left(\frac{\sum_{r,s=0}^{7} \frac{w(r)w(s)}{4} cos[\frac{r\pi(2i+1)}{16}] \cos[\frac{s\pi(2j+1)}{16}] B_{r,s}}{Q_{ij}} \right)$$
$$i,\ j \in \{0,\ 1,\ 2,\ ...,\ 7\} \qquad (1)$$

여기에서 $w(0)=\frac{1}{\sqrt{2}}$, $w(r>0 \text{ or } s>0)=1$이다. Q_{ij}는 양자화 행렬(quantization matrix)을 나타낸다.$B_{r,s}$, $r,\ s \in \{0,\ 1,\ 2,\ ...,\ 7\}$는 DCT 변환이 이루어지기 전의 블록내에서 0부터 255사이의 픽셀(밝기) 값을 의미한다. r과 s는 8×8 픽셀 블록의 계수 위치를 나타낸다.

이러한 DCT 계수를 생성하는 적절한 모델을 제시하여,[5] 확률변량을 생성한 후 외부자료가 끼워질 때 변화의 형태와 위치를 감지할 필요가 있다. 즉, 끼워지는 자료의 크기에 상관없이 변화량을 빠르게 인지하는 통계량 및 검정 모델이 필요하다.

t번째 시점에서 스테고 신호인 DCT 계수 y_t는 축차적 독립 확률변수로서 θ에 의해 모수화 된 확률밀도 $p_{\theta_l}(y)$를 갖는다고 가정한다.

$$y_t = x_t + \rho w_t, \quad \text{t=1, 2, ..., N} \qquad (2)$$

여기에서 θ_l, $(l=0, 1)$는 스칼라 혹은 벡터 값을 가질 수 있다. 임의의 시점 t에서 x_t와 w_t는 독립이라고 가정하고, $x_t \in R$는 t번째 원본신호의 DCT 계수이다. $w_t \in R$는 가우시안 분포를 따르는 끼워 넣어지는 메시지 운반대(message carrier)이며, $\rho > 0$는 메시지 길이이다. 즉, $x_t \sim N(0, \sigma_o^2)$와 $w_t \sim N(0, \sigma_1^2)$이며, $y_t \sim N(0, \sigma_o^2 + \rho\sigma_1^2)$이다. 최하위 표본 평균수를 사용한 SPRT를 기반으로 다음과 같은 가설을 설계할 수 있다.

$$H_o: \theta = \theta_o$$
$$H_1: \theta = \theta_1 \text{(원본 메시지에 변화가 있다)} \qquad (3)$$

통계량에서 변화가 이루어진 후에 θ_o는 θ_1이 된다. 즉, $\theta_o \neq \theta_1$의 관계가 있으며, y_{t_o}부터 y_{t_1}까지에서 은닉메시지가 삽입된 것이라고 판단한다.

Wald[9]는 두 단순 가설에 대해 축차확률비 검정의 절차를 제안하였다. Page[10]는 확률과정에서 갑작스런 변화를 감지하기 위해 두 개의 한계값 h와 $-\gamma$를 가지고 반복되는 가설검정을 기반으로 SPRT 기법을 제안하였다. SPRT에 의해 사용되는 관측값 수는 고정된 잘못된 신호와 잘못된 오류 확률에 대한 확률변수이다. 반복되는 축차확률비 검정을 기반으로 하는 스테간 분석 통계량은 (4)식과 같으며, 이러한 통계적 검정은 결정이 될 때까지 계속하여 반복 수행한다.

$$S_1^t = \sum_{i=1}^{t} s_i \begin{cases} \geq h, & H_1 \text{ 채택} \\ < -\gamma, & H_o \text{채택} \\ t = t+1, & o/w \end{cases} \quad (4)$$

여기에서 로그 우도비(log likelihood ratio)는 다음과 같이 정할 수 있다. 일반적으로 s_i는 변화가 주어지기 전에는 음수값을 가지며, 변화가 주어진 후에는 양수값을 가진다. 이때 수식을 단순화 하기위해 s_i 대신에 $s(y_i)$를 사용한다.

$$s(y_i) = \ln \frac{p_{\theta 1}(y_i)}{p_{\theta_o}(y_i)} \quad (5)$$

결정한계는 잘못될 신호 확률(α)과 실수할 확률(β)에 관해서 정의된다. 즉, 통계량 S_1^t의 경계선 h의 초과에 대한 기대값을 μ라 할 때 Wald 등식을 참고로 수정된 결정영역은 다음과 같이 나타낼 수 있다.[9]

$$h \approx \ln \frac{1-\beta}{\alpha} - \mu \quad (6)$$

정지시간(stopping time) τ는 검정에 필요한 최소의 표본수를 나타내는 결정표본수 즉, (7)식을 이용하여 정할 수 있다. SPRT를 적용할 때 $\gamma = 0$으로 사용하여도 큰 무리가 없음을 Page 등이 보였다.[4][10] 그러므로 여기에서는 (6)식과 같이 수정된 h만을 구하여 사용한다.

$$\tau_{-\gamma,h} = \min\{t : S_1^t \geq h \cup S_1^t \leq -\gamma,\ \gamma \geq 0\} \quad (7)$$

반복되는 누적합-축차확률비 검정기법을 이용하는 스테간 분석을 위한 통계량은 다음과 같이 적용할 수 있다.

$$g_t = \begin{cases} g_{t-1} + s_t, & g_{t-1} + s_t > 0 \\ 0, & o/w \end{cases} \quad (8)$$

확률밀도함수 $f(y_t : \theta)$를 갖고 순차적으로 얻어지는 확률변수 $\{y_1, y_2, \ldots\}$에서 (5)식을 참고로 s_t라 하고, (3)식에 대한 축차확률비 검정을 적용한다. 이때 s_t의 분포를 구하는 것은 어렵기 때문에 s_t를 브라운 운동과정(brownian motion process)으로 근사시킨다. 이 방법은 Reynolds [11]가 적용한 예에서 찾아볼 수 있다. 이러한 기법은 독립인 확률변수들의 합을 브라운 운동과정으로 근사시키는 것은 순차분석에서 많이 사용하는 방법이다. $y(t)$는 평균이 $E(s) \cdot t$, 분산이 $Var(s) \cdot t$인 브라운 운동과정을 따른다고 가정하고, 결정표본수는 브라운 운동과정에서의 정지시간 τ로 추정될 수 있다. 결정표본수가 어느 정도 큰 경우 $y(t)$는 s_t로 근사시킬 수 있으므로 s_t의 기대값은 $y(t)$를 이용하여 추정할 수 있다. 즉, 다음과 같이 구할 수 있다.

$$\begin{aligned} E(s_t) &\approx E(y(t) | h \leqq y(t) \leqq h^*) \\ &= h + \frac{1}{2} ln \frac{\theta_1}{\theta_o} \end{aligned} \quad (9)$$

여기에서 $h^* = h + \ln \frac{\theta_1}{\theta_o}$이다. 따라서 h의 초과에 대한 기대값 μ를 (10)식과 같이 구하여 수정된 결정영역 (6)식에서 사용한다.

$$\mu = E(s_t) - h \approx \frac{1}{2} ln \frac{\theta_1}{\theta_o} \quad (10)$$

실제 적용에서는 모수 θ_o의 값은 주어지고, θ_1의 사전정보가 전혀 알려지지 않을 때 주어진 이미지 정보만을 가지고 은닉메시지의 존재유무를 판단할 수밖에 없다. 이 논문에서는 척도모수(scale parameter)의 검정에 관해서만 생각한다. 즉, (3)식에서 모수 $\theta = \sigma$로 대체하여 가설 검정식을 재정의 하여 사용한다.

x_t와 y_t는 평균이 0인 정규분포를 따른다고 가정할 때 Trivedi와 Chandramouli는 우도비를 얻기 위해 Wald의 가중함수를 이용하였다. 이들은 σ_1이 특정분포를 따른다고 가정한 상태에서 S_j^t를 구하기 위한 수식을 제시하였으며, $g_t = (S_{t-N_t+1}^t)^+$을 이용하여 CUSUM-SPRT 분석을 하였다.[5][12] 이러한 경우에 수식 S_j^t의 적용제한과 오류가 따를 수 있다. 실제 적용에서 σ_1에 대한 사전 정보가 없기 때문에 σ_1에 의

존되지 않는 일반적인 상황에서도 적용이 가능한 수식으로 개선할 필요가 있다. 즉, 정확하면서도 일반화된 수식을 위해 (11)식을 제시하였다. 식이 유도되는 과정은 Appendix를 참고한다.

$$S_j^{t^*} = \ln \sigma_o + \lambda_{j,t} + \ln\Gamma(\frac{N_t - 1}{2}) - \frac{\mathrm{N_t} - 1}{2}\ln(\lambda_{\mathrm{j,t}}) - \ln(2) \qquad (11)$$

여기에서 $\lambda_{j,t} = \sum_{i=j}^{t} \frac{y_i^2}{2\sigma_o^2}$ 이다. $\Gamma()$는 감마함수를 나타내며, $\Gamma(n) = (n-1)!$ 이다. 또한 $g(t-1) > 0$ 일 경우 $N_t = N_{t-1} + 1$ 이며, 그 외의 경우에는 $N_t = 1$ 을 적용한다.

4. 실험 및 적용

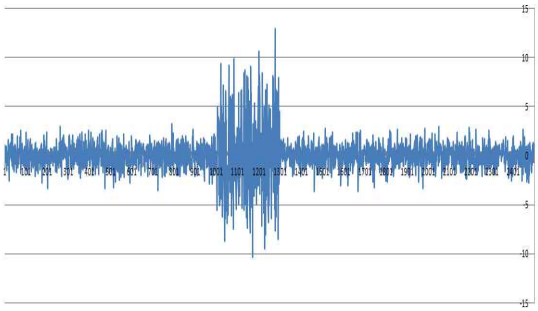
DCT 계수는 (2)식을 기본으로 하여 생성된 확률변량을 이용하여 결정된다고 가정하고, 임의의 ρ가 주어진 상태에서 확률수를 발생시키도록 한다. 신뢰성을 고려하여 5,000번의 모의실험을 반복하였다. 이 논문에서는 1블록 단위를 고려하고 ρ, α, β, σ 등이 주어진 상태에서 모의실험, DCT 변환, $S_j^{t^*}$, h 등을 구하는 과정은 JAVA와 Matlab을 이용하여 구현하였다.

<표 1> α, β가 주어질 때 수정된 경계선

α	β	$(-\gamma$	$h)$	$h^p = \ln\frac{1-\beta}{\alpha}$
0.01	0.01	0	4.118	4.595
0.01	0.05	0	4.077	4.553
0.01	0.10	0	4.023	4.499
0.05	0.01	0	2.508	2.985
0.05	0.05	0	2.467	2.944
0.05	0.10	0	2.413	2.890

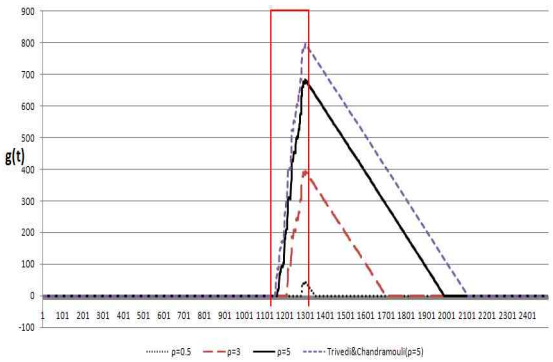
$\rho = 0.5,\ 3,\ 5$, 제1종 오류(α)와 제2종 오류(β)가 0.01, 0.05, 0.10으로 주어졌을 경우 수정된 경계선을 각각 구하면 <표1>과 같이 나타낼 수 있다.

원본이미지에서 임의의 시점($N(0,\ \sigma^2)$을 따르며, $\rho = 5$일 때 생성된 자료에 1100부터 1300까지에 은닉정보를 삽입할 경우)에 비밀자료를 삽입하는 과정을 고려할 때 DCT 계수의 변동 폭 결과는 (그림 1)과 같이 표시할 수 있다.



(그림 1) $N(0,\ \sigma^2)$, $\rho = 5$일 경우 스테고 이미지에서 통계적인 갑작스런 변화의 예

Trivedi와 Chandramouli가 제시한 방법과 (11)식의 $S_j^{t^*}$를 계산한 후 $g_t = (S_{t-N_t+1}^{t^*})^+$를 각각 구하여 표시하였다. 즉, $\rho = 0.5,\ 3,\ 5$일 때 각각의 경우에 g_t (CUSUM) 통계량을 기반으로 하는 스테간 분석결과는 (그림 2)에서 확인할 수 있다.



(그림 2) $\rho = 0.5,\ 3,\ 5$일 경우 Trivedi& Chandramouli의 방법과 수정된 g_t 통계량을 기반으로 한 스테간 분석결과

ρ값이 클수록 g_t값의 변화는 급격하게 나타남을 확인할 수 있다. Trivedi와 Chandramouli가 제시한 기존의 방법과 수식 계산의 일반화와 정확성이 추가된 수정된 방법에서 변화를 감지하는데 차이가 없었다. 갑

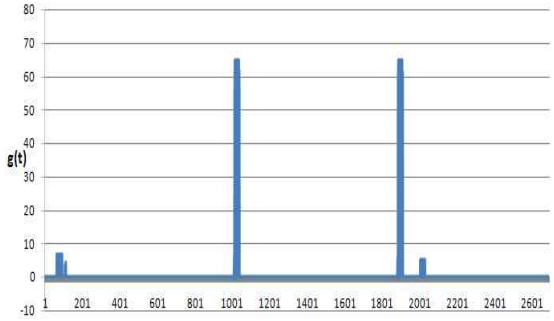
작스런 g_t값의 변화로 은닉정보를 감지하고, 은닉위치를 1131부터 1331까지에서 확인할 수 있다. 즉, Trivedi와 Chandramouli가 제시한 수식과 (11)식을 사용한 개선된 방법을 비교할 때 비슷한 결과가 나타남을 확인할 수 있다.

$\alpha = 0.01$, $\beta = 0.05$일 때 ρ변화에 따라 수정된 경계선을 사용할 경우 통계량 변화를 지적한 평균횟수는 <표 2>와 같다. 수정된 경계선을 사용하여 이상신호를 감지하는 것이 효율적임을 확인할 수 있다.

<표 2> $\alpha = 0.01$, $\beta = 0.05$, 수정된 경계선을 사용할 때 통계량 변화를 감지하는 평균횟수

ρ	h	$h^{\rho} = \ln\frac{1-\beta}{\alpha}$
0.5	7.545	3.182
1	18.908	13.273
2	25.637	16.083
3	61.182	53.182

실제 은닉된 이미지에서의 결과를 보기 위해 원본 흑백이미지(512×512, 32,533Byte)에 78Byte 크기의 은닉메시지를 삽입한 스테고 이미지(512×512, 33,472 Byte)의 경우를 생각한다.



(그림 3) 실제 은닉이미지가 포함된 경우 g_t(CUSUM) 통계량을 기반으로 한 스테간 분석 결과

실제로 은닉이미지가 포함될 때 (1)식을 이용하여 DCT 계수를 추출한 후 수정된 (11)식을 이용하는 g_t 통계량을 기반으로 스테간 분석 결과는 (그림 3)과 같이 표시할 수 있다. (그림 3)에서와 같이 은닉정보가 삽입된 구간에서 g_t값이 급격하게 변화하는 것을 확인할 수 있다.

5. 결 론

은닉정보가 송수신되는 사실을 인지하지 못하게 하는 스테고 기법은 제 3자의 공격 자체를 차단할 수 있어 암호화 이상의 가치와 효율성을 제공할 수 있다. 스테고 이미지 신호를 기반으로 하고, 논문에서 제시된 수식의 일반성과 정확성이 반영된 CUSUM 통계량 g_t를 활용하였다. 이때 실제 적용에서 σ_1에 대한 사전 정보가 없기 때문에 수식 전개가 정확하면서도 일반화된 개선된 (11)식을 사용하는 것이 합리적이다. 누적합-축차확률비 검정 기법을 이용하여 미세한 은닉정보 존재유무와 그 위치를 정확하게 판단할 수 있음을 확인하였다. 즉, 원본이미지에 비해 은닉정보의 크기가 1%이하일 때 은닉유무와 그 위치를 판단하는 것이 어려울 경우 누적합-축차확률비를 이용한 스테간 분석이 효율적임을 확인하였다. 비슷한 환경에서 Markov Chain을 이용하여 혼합이미지로부터 은닉자료를 분석하는 연구는 향후 진행되어야 할 부분이다.

참 고 문 헌

[1] R. Chandramouli and N. D. Memon, "Steganography Capacity: A Steganalysis Perspective", Proc. SPIE Security and Watermarking of Multimedia Contents, Vol. 3, pp. 1019-1022, 2003.

[2] N. Provos, "Defending Against Statistical Steganalysis", 10th USENIX Security Symposium, Washington, D.C. pp. 323-335, 2001.

[3] A. Rocha and S. Goldenstein, "Steganography and Steganalysis in Digital Multimedia: Hype or Hallelujah?", RITA, Vol. 15, No. 1, pp. 83-110, 2008.

[4] S. Trivedi and R. Chandramouli, "Secret Key Estimation in Sequential Steganography", IEEE Transactions on Signal Processing, Vol. 53, No. 2, pp. 746-757, 2005.

[5] S. Trivedi and R. Chandramouli, "Active Steganalysis of Sequential Steganography", Proc. SPIE Security and Watermarking of Multimedia Contents, Special Session on Steganalysis, pp. 123-130, 2003.
[6] 지선수, "스테고 이미지에서 은닉메시지 감지기법", 한국산업정보학회논문지, 제 13권, 제 3호, pp. 37-43, 2009.
[7] Tom'a˘s Pevn'y and Jessica Fridrich, "Detection of Double-compression in JPEG Images for Applications in Steganography", USAF Research Paper, 2008.
[8] R. Chandramouli, A Mathematical Framework for Active Steganalysis, Multimedia Systems© Springer-Verlag, 2003.
[9] A. Wald, Sequential Analysis, Wiley, New York, 1947.
[10] E. Page, "Continuous Inspection Schemes", Biometrica, Vol. 41, pp. 100-115, 1954.
[11] M. R. Reynolds, Jr, "Approximayion to the Average Run Length in Cumulative Sum Control Charts", Technometrics, Vol. 17, pp. 65-71, 1975.
[12] A. Patel, M. Shah, R. Chandramouli, and K. P. Subbalakshmi, "Covert Channel Forensics on the Internet: Issues, Approaches and Experiences", International Journal of Network Security, Vol. 5, No. 1, pp. 41-50, 2007.

Appendix

σ_1에 대한 확률분포가 $D(0,\sigma^2)$이라 할 때 로그 우도비, 베이지안 기법, 역감마함수의 성질 등을 이용하여 다음과 같이 구할 수 있다.

$$S_j^{t^*} = \ln\left[\int_0^\infty \frac{(\frac{1}{\sqrt{2\pi}\,\sigma_1})^{N_t} e^{-\sum_{i=j}^{t}\frac{y_i^2}{2\sigma_1^2}}}{(\frac{1}{\sqrt{2\pi}\,\sigma_o})^{N_t} e^{-\sum_{i=j}^{t}\frac{y_i^2}{2\sigma_o^2}}} d\sigma_1\right]$$

$$= \ln\left[(\sigma_o)^{N_t} e^{\sum_{i=j}^{t}\frac{y_i^2}{2\sigma_o^2}} \int_0^\infty (\frac{1}{\sigma_1})^{N_t} e^{-\sum_{i=j}^{t}\frac{y_i^2}{2\sigma_1^2}} d\sigma_1\right]$$

치환을 위해 $x=\sigma_1^2$이라 놓는다. 여기에서 전개되는 $\sigma_1 = x^{\frac{1}{2}}$, $d\sigma_1 = \frac{1}{2}x^{-\frac{1}{2}}dx$ 등을 이용하여 구할 수 있다.

$$= \ln\left[\frac{(\sigma_o)\, e^{\lambda_{j,t}}\, \Gamma(\frac{N_t-1}{2})}{2\cdot(\lambda_{j,t})^{\frac{N_t-1}{2}}}\right]$$

$$= \ln\sigma_o + \lambda_{j,t} + \ln\Gamma(\frac{N_t-1}{2}) - \frac{N_t-1}{2}\ln(\lambda_{j,t}) - \ln(2)$$

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 컴퓨터정보공학부 교수
- (현)강릉원주대학교 정보기술공학과 교수
- 관심분야 : 혼잡제어, 정보보안(암호키, 정보은닉), 이미지 프로세싱

논 문 접 수 일 : 2010년 08월 05일
1차수정완료일 : 2010년 09월 12일
게 재 확 정 일 : 2010년 09월 15일