情報保護學會論文誌
第14券 第1號, 2004. 2

통계분석에 강인한 심층 암호

유 정 재,[a)†] 오 승 철,[a)] 이 광 수,[a)] 이 상 진,[a)‡] 박 일 환[b)]
고려대학교 정보보호기술연구센터,[a)] 국가보안기술구소[b)]

Secure Steganographic Algorithm against Statistical analyses

Jeong-Jae Yu,[a)†] Seung-Cheol O,[a)] Kwang-Su Lee,[a)] Sangjin Lee,[a)‡] Il Hwan Park[b)]
Korea Univ. CIST,[a)] NSRI[b)]

요 약

초창기 심층 암호의 대부분은 원본 영상의 최하위비트를 비밀 메시지 비트로 치환하는 방식이었기 때문에 인간의 감각으로는 메시지 삽입 여부를 구별해낼 수 없었지만 통계적 분석에 의하여 원본과 은닉물의 구별은 물론, 비밀 메시지의 삽입량까지도 거의 추정해낼 수 있을 만큼 취약점을 내포하고 있었다. 우리는 Westfeld[1]와 Fridrich[2]가 판단의 기준으로 정한 통계량을 각각 분석하였고, 이에 근거하여 원본의 통계량을 유지하면서도 대용량의 메시지를 삽입할 수 있는 방법을 제안하고자 한다. 제안하는 방식은 단순히 원본 영상의 최하위 비트를 변화시켜 메시지를 삽입하는 방식이 아닌 원본의 실제 화소값이 랜덤하게 증가하거나 감소하는 방식으로 메시지를 삽입하게 된다.

ABSTRACT

Westfeld[1] analyzed a sequential LSB embedding steganography effectively through the χ^2-statistical test which measures the frequencies of PoVs(pairs of values). Fridrich[2] also proposed another statistical analysis, so-called RS steganalysis by which the embedding message rate can be estimated. This method is based on the partition of pixels as three groups ; Regular, Singular, Unusable groups. In this paper, we propose a new steganographic scheme which preserves the above two statistics. The proposed scheme embeds the secret message in the innocent image by randomly adding one to real pixel value or subtracting one from it, then adjusts the statistical measures to equal those of the original image.

Keywords: *steganography, χ^2-statistical test, RS steganalysis, blind detection*

Ⅰ. 서 론

예전부터 사람들은 비밀 정보를 전달, 보관하기 위하여 많은 방법을 동원하였다. 특정 문자를 난수에 대응시켜 의미없어 보이는 숫자의 나열을 보낸다든지, 일상적인 연애 편지 위에 소금물로 비밀 문장을 적어 보내고 수신자는 이 편지를 불 위에 쪼였을 때 나타나는 문장으로 그 숨은 뜻을 알아낸다는 식의 방법은 셜록 홈즈가 나오는 추리 소설의 단골 메뉴이다.

이러한 일련의 과정을 학문적으로 체계화한 것이 바로 암호학과 심층 암호이다. 전자의 경우처럼 암호학에서는 비밀키를 알지 못하는 사람이 그 내용을 알 수 없는 난수를 생성하여 수신자에게 전달한다. 제 3자가 전달 과정 중에 난수를 획득할 수는 있어도 그 내용을 알거나 변조할 수 없어야만 안전한 암호라고 할 수 있다. 반면, 후자의 경우에는 평범한 편지 위에 비밀스런 내용을 감추는 심층 암호 기법을 사용하고 있다. 심층 암호 통신에서도 암호 통신의 기법을 활용하긴 하지만 기본적으로 비밀 통신을 평범한 통

접수일: 2003년 8월 19일; 채택일: 2004년 2월 3일
† 주저자, shaehds@cist.korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr

신 속에 감추어서 제 3자는 또 하나의 통신이 이루어지고 있다는 사실 자체를 알 수 없어야만 비로소 안전한 심층 암호라고 할 수 있다.

그런데 구체적인 심층 암호의 사용이 지금까진 대부분 군사나 범죄의 용도로 사용되어 왔기 때문에 그리 활성화되지 못했으나 급증하고 있는 인터넷 상의 저작권 침해나 암호 통신에서 겪고 있는 키관리의 어려움에 대한 해결 방안으로 심층 암호가 주목받기 시작한다.[3] 나날이 발전하고 있는 정보 통신의 발달에 비해 개인 정보의 보호는 이를 뒷받침하고 있지 못한 상황이다.

따라서 지금처럼 대용량의 데이터 전송이 단시간 내에 가능해진 요즈음의 인터넷 환경에서는 암호화만으로 안전성을 확신할 수 없을 정도의 중요한 정보에 대하여 그 정보의 존재마저 감출 수 있는 심층 암호 통신이 잠재된 악의적인 공격을 회피할 수 있는 해결 방안으로 부각되고 있는 것이다.

Simmons[4]이 Prisoner's Problem에서 비밀 통신이 가능함을 보인 후 본격적으로 심층 암호에 대한 연구가 시작되어 현재 수많은 심층 암호가 발표되어 있다. 그러나 이들의 대부분은 단순히 인간의 감각이 예민하지 못한 것에만 근거하였으므로 안전성을 보장하기는 어려웠다. 의심이 되는 데이터의 통계량을 분석하면 원본과 은닉물을 구별해낼 수 있었기 때문이다.

Westfeld[1] 등은 PoVs(pairs of values)의 통계량을 기준으로 하여 원본의 최하위 비트에 순차적으로 암호문을 삽입한 심층 암호를 효과적으로 구별할 수 있는 χ^2-통계 분석법을 제시하였고 Fridrich[2]등은 많은 실험을 통해 영상을 regular, singular, unusable 그룹으로 세분화한 후 이러한 비율에 근거하여 의심이 되는 영상의 비밀 메시지 삽입량을 추정하는 RS 통계법을 제안하였다.

RS 통계 분석은 순차적인 원본의 최하위 비트 삽입 심층 암호와 랜덤하게 메시지를 삽입한 심층 암호의 탐지는 물론이고, 심지어 메시지 삽입량까지 추정할 수 있었다.

본 논문에서는 지금까지 발표된 심층 암호의 통계적 분석을 고려하여 원본 영상의 통계적 특성을 메시지 삽입 후에도 유지시켜 통계 분석에 강인한 심층 암호를 제안하려고 한다. 본 논문에서 제안하는 방식은 기존의 심층 암호가 단순히 원본의 최하위 비트 혹은 하나의 비트 평면(bit plane)만을 변화시켜 비밀 메시지를 삽입하던 것에 비해 원본의 화소값을 랜덤하게 증가하거나 감소시켜 메시지를 삽입함으로써 원본의 PoVs 통계량을 유지하게 된다. 또한 메시지 삽입 후 삽입에 이용되지 않았던 부분을 활용하여 regular, singular, unusable 그룹의 비율을 맞춰 줌으로써 Fridrich 등이 제안한 RS 통계량도 유지한다. 이전에 발표되었던 통계량을 유지하는 심층 암호(F5,[5] Outguess[6])들이 오직 PoVs 통계량만을 만족하면서도 상대적으로 메시지 삽입량이 적었던 것에 비해 제안하는 심층 암호는 모든 원본 영상 화소값에 비밀 메시지를 k 비트씩 삽입할 수도 있다.

실험 결과, 위에서 제시한 통계적 분석법들은 물론 Provos 등이 제안한 변형된 χ^2-통계 분석법에도 탐지되지 않았다.

논문의 구성은 다음의 순서로 이루어진다. 2절에서는 지금까지 제안된 심층 암호의 통계 분석 방법들에 대하여 살펴보고 3절에서 우리가 SES(a Steganography Evading Statistical analyses)라고 부르는 심층 암호의 구체적인 알고리즘을 설명할 것이다. 4절에서는 실험 결과를 분석하고 5절에서 결론 및 앞으로의 과제에 대하여 논의하겠다.

Ⅱ. 심층 암호의 통계 분석

2.1 χ^2-통계 분석

대부분 심층 암호 통신를 실제 적용할 때 메시지 삽입 이전에 암호화 과정을 거치게 되므로 원본에는 암호문이 삽입되기 마련이다. 단순한 최하위 비트 치환 심층 암호라면 이 과정에서 시각적으로 드러나진 않지만 원본과 은닉물 사이에 심각한 통계적 차이를 발생시킬 수 있다. 즉, 메시지를 삽입하지 않은 원본의 인접한 두 화소, 혹은 색인값들(PoVs, pairs values)이 발생한 빈도를 살펴보면 변형을 가하지 않을 경우 서로 다르게 나타나지만 은닉물에서는 인접한 두 화소값들의 발생 빈도가 암호문의 통계적 분포 때문에 거의 비슷하게 되는 것이다.

이 차이를 Westfeld[1]등이 암호문의 랜덤성 테스트[7]과 비교하여 메시지 삽입 확률을 정량화하였고 이러한 심층 암호 분석 기법을 χ^2-통계 분석이라고 명명하였다. 구체적인 세부 과정은 다음과 같다.

1. 먼저 탐지하려는 그림에서 사용되는 색상들을 팔레트 상의 서로 인접한 두 색상씩 k개의 묶음으

로 구분한다.

2. 예상되는 인접한 원본의 색상 빈도, y_i^*를 대상 탐지 파일로부터 구한다.

$$y_i^* = \frac{|n_{2i} + n_{2i+1}|}{2}, \quad 0 \le i \le k-1$$

여기에서 n_{2i}와 n_{2i+1}는 검사하려는 영상의 인접한 두 색상 발생 빈도를 나타낸다.

3. 다음과 같이 χ^2값을 계산한다.

$$\chi^2_{k-1} = \sum_{i=1}^{k} \frac{(y_i - y_i^*)^2}{y_i^*}$$

y_i는 n_{2i}나 n_{2i+1}중에서 택일한다.

4. y_i와 y_i^*의 분포가 일치할 확률 p는 다음과 같이 가중 분포 함수의 여사건 확률로 주어진다. 여기에서 Γ는 Euler Gamma 함수를 나타낸다.

$$p = 1 - \frac{1}{2^{\frac{k-1}{2}} \Gamma(\frac{k-1}{2})} \int_0^{x_i^2} e^{-\frac{x}{2}} x^{\frac{k-1}{2}-1} dx$$

이 후 Provos[6]는 탐지 구간을 세분화하거나 PoVs의 샘플을 화소 x와 $(x+1)$에서 x와 $(x-1)$로 변형하여 χ^2-통계 분석 방법을 다시 적용한 변형된 χ^2-통계 분석을 제안하면서, 메시지 삽입 후에도 원본의 PoVs 통계량을 유지하는 Outguess를 발표하였다. Outguess는 랜덤하게 원본의 최하위 비트를 비밀 메시지 비트로 변화시킨 후 삽입에 이용되지 않은 나머지 원본의 최하위 비트들로 원본의 PoVs 통계량과 일치하도록 변화시키는 심층 암호 알고리즘이다.

이에 비해 우리가 제안하는 심층 암호는 단순히 원본의 최하위 비트 혹은 하나의 비트 평면만을 변화시켜 비밀 메시지를 삽입하지 않고 원본의 화소값을 랜덤하게 증가하거나 감소시켜 메시지를 삽입하였으므로 원본의 PoVs 통계량을 유지할 수 있다.

2.2 RS 통계 분석

Fridrich[2] 등은 실험에 기반하여 심층 암호를 개발하던 중 원본 영상의 고유한 특성을 발견하고 RS 통계 분석법을 제안하였다. RS 통계 분석은 최하위 비트 변환 기반의 심층 암호 탐지와 삽입 메시지량을 추정하는 분석법이다. 그 핵심 내용은 다음과 같다.

먼저 원본 C를 서로 공통 부분이 없으며 각각 n개의 원소를 갖는 집합들로 분할한다. 이러한 집합을 $G=(x_1, \ldots, x_n)$라고 할 때 판별 함수 f를 다음과 같이 정의한다.

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i| \qquad (1)$$

그리고 주기 2를 가지는 가역함수 F_1과 F_{-1}는 다음의 성질을 만족해야 한다.

$$F_i(F_i(x)) = F_0(x) = x, \ i \in \{-1, 1\}$$
$$F_1 : 0 \leftrightarrow 1, 2 \leftrightarrow 3, \ldots, 254 \leftrightarrow 255$$
$$F_{-1} : -1 \leftrightarrow 0, 1 \leftrightarrow 2, \ldots, 253 \leftrightarrow 254, 255 \leftrightarrow 256$$

그러면 플립(flipping) 가역함수 F_1과 F_{-1}사이에는 다음 식이 성립하게 된다.

$$F_{-1}(x) = F_1(x+1) - 1 \quad \text{for all } x \qquad (2)$$

즉, 다음의 식과 같이 정리할 수 있다.

$$F_1(x) = x \oplus 1,$$
$$F_{-1}(x) = \{(x+1) \oplus 1\} - 1$$

이 때 집합 G의 특성을 다음과 같이 결정한다.

Regular group : $G \in R \Leftrightarrow f(F_i(G)) > f(G)$
Singular group : $G \in S \Leftrightarrow f(F_i(G)) < f(G)$
Unusable group : $G \in U \Leftrightarrow f(F_i(G)) = f(G)$

또한 임의의 마스크 M을 집합 G에 적용한 것을 $F_M(G) = (F_{M(1)}(x_1), \ldots, F_{M(n)}(x_n))$이라고 나타낼 때, 이러한 마스크 M에 대하여 원본 C를 regular, singular, unusable 그룹으로 분류할 수 있다. 여기에서 마스크라 함은 영상 처리에 활용되는 일종의 변환이며, 보통 $m \times n$ 개의 내부 함수로 이루어져 있다. 많은 실험을 거쳐 Fridrich 등은 최하위 비트를 조작하지 않은 원본의 경우 대부분 다음과 같은 통계적 특성을 만족함을 발견하였다.

$$R_M + S_M \leq 100,\ R_{-M} + S_{-M} \leq 100$$
$$R_M \cong R_{-M},\ S_M \cong S_{-M} \quad (3)$$

여기에서 R_M과 S_M은 전체 영상에 대한 regular 그룹과 singular 그룹의 백분율을 각각 나타낸다.

그리하여 위의 통계적 가설을 바탕으로 은닉물의 최하위 비트 메시지 삽입량을 추정할 수 있다. 일반적으로 최하위 비트 치환 방식으로 심층 암호 통신을 하고 $p\%$ 가량의 메시지를 삽입해야 한다면 원본 영상의 절반 정도인 $(p/2)\%$의 최하위 비트를 변형시켜야만 한다.

따라서 2×2 마스크 $M=[F_0 F_1 : F_1 F_0]$를 실험 영상에 적용하면, $R_M(p/2)$, $S_M(p/2)$ 두 점의 값을 알 수 있고, 마찬가지 방법으로 마스크 $-M=[F_0 F_{-1} : F_{-1} F_0]$에 대응하는 두 점 $R_{-M}(p/2), S_{-M}(p/2)$도 얻을 수 있다.

또한 실험 영상의 모든 화소에 플립 함수 F_1을 적용하면, 결과적으로 초기에 최하위 비트가 $(p/2)\%$ 변화되어 있던 영상은 $100-(p/2)\%$ 변화되는 효과를 가져온다.

따라서 $R_M(100-p/2)$, $S_M(100-p/2)$와 $R_{-M}(100-p/2)$, $S_{-M}(100-p/2)$를 알 수 있다. 마지막으로 원본 영상에 최대로 메시지를 삽입한다면 거의 원본 최하위 비트의 50% 정도가 변화하는 것으로 볼 수 있고, Fridrich는 이 때의 R_M과 S_M이 유사함을 실험적 가설로 추가하여 그림 1과 같은 RS 통계 그래프를 유추하였다.

$$R_M(50) \cong S_M(50) \quad (4)$$

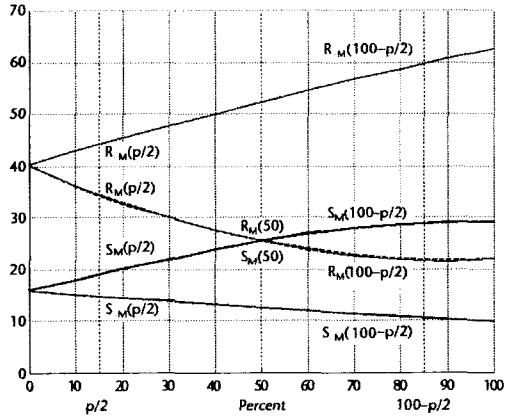


그림 1. RS 통계 그래프

R_M과 S_M은 2차 보간으로, R_{-M}과 S_{-M}은 1차 보간법을 사용하였을 때 식(5)와 같은 방정식을 유도할 수 있으며, 메시지 삽입 확률 p는 식(6)으로 주어진다.

$$2(d_1+d_0)x^2+(d_{-0}-d_{-1}-d_1-3d_0)x + d_0-d_{-0}=0 \quad (5)$$

$$d_0 = R_M(p/2) - S_M(p/2)$$
$$d_1 = R_M(1-p/2) - S_M(1-p/2)$$
$$d_{-0} = R_{-M}(p/2) - S_{-M}(p/2)$$
$$d_{-1} = R_{-M}(1-p/2) - S_{-M}(1-p/2)$$
$$p = x/(x-1/2) \quad (6)$$

메시지 삽입 추정 확률은 식(5)에서 절대값이 작은 근을 취하는데 우리는 이 삽입 확률이 0이 되도록 메시지 삽입 후 R_M과 R_{-M}의 비율을 조정할 것이다. 플립핑 함수는 주기가 2인 특성을 가지므로, 다음 식 $F_M(R)=S$, $F_M(S)=R$은 항상 성립하게 된다.

Fridrich 등이 실험 결과로 제시한 것처럼 RS 통계 분석은 최소 2%내외의 삽입 메시지 추정 오차가 발생한다. 제안하는 SES 심층 암호는 랜덤 플립핑 함수를 이용하여 메시지를 삽입하므로 은닉물의 RS 통계량이 원본 RS 통계량과 큰 차이가 발생하지 않고, 메시지 삽입 후 안전성을 위하여 메시지 삽입에 이용되지 않는 원본 영상 화소를 조정하여 은닉물의 RS 통계량을 오차 범위 내로 일치시킨다.

Ⅲ. 제안 알고리즘

3.1 SES 심층 암호

SES(a Steganography Evading Statistical analyses) 심층 암호는 이름의 유래에서 알 수 있는 것처럼 원본 영상의 알려진 통계량을 만족하도록 고안된 심층 암호 기법이다. SES 알고리즘은 랜덤 플립핑과 간단한 실수 계산만으로 이루어졌기 때문에 구현 또한 용이하다. 구체적인 과정은 다음과 같다.

1. 원본 영상의 RS 통계량을 계산하여 메모리에 저장한다.
2. 비밀 메시지를 암호화하고 메시지의 길이를 앞부

분에 연접시킨다.

$S = l \| c_1 \| \ldots \| c_n = s_1 \| \ldots \| s_{n+1}, \quad l = n$

3. 삽입될 메시지(메시지 크기+암호문)의 비트와 원본 영상 화소의 최하위 비트를 순차적으로 비교한다. 일치하면 플립 함수 F_0를 적용하고 일치하지 않으면 플립 함수 F_1과 F_{-1}을 랜덤하게 적용하여 은닉 영상 화소의 최하위비트를 삽입 메시지 비트와 일치시킨다.

$$x'_i = \begin{cases} x_i & \text{if} \quad s_i = LSB(x_i) \\ F_j(x_i) & otherwise \end{cases}$$

여기에서 j는 암호학적으로 안전한 난수 발생기로부터 랜덤하게 선택한다.

$j = r \in \{-1, 1\}$

4. 메시지 삽입이 모두 끝난 후 은닉물 전체의 RS 통계량을 계산한다. 원본의 RS 통계량과 비교하여 2%이상 오차 발생 시 삽입하고 남은 원본 영상의 화소를 조정하여 은닉물의 RS 통계량을 원본과 2% 이내로 일치시킨다. $d_0 - d_{-0} = 0$이 되면 식(5)와 (6)에서 알 수 있듯이 삽입 메시지 추정 확률 p도 0이 된다. 다음 식 $F_M(R) = S$, $F_M(S) = R$을 이용하여 R_M과 R_{-M}의 비율을 일치시키도록 한다.

그리고 위의 심층 암호 기법은 한 화소당 k비트의 메시지까지 확장하여 삽입할 수도 있다. 과정 3의 플립핑 함수를 랜덤한 정수 연산으로 정의해주면 된다. 예를 들어 하나의 영상 화소에 2비트의 메시지를 삽입한다고 하자. 삽입해야 할 2비트 메시지가 $00_{(2)}$이고 영상 화소의 최하위 2비트가 $01_{(2)}$이라면 원본 화소값을 랜덤하게 3을 더하거나 1을 빼서 화소의 최하위 2비트가 삽입할 비밀 메시지 $00_{(2)}$과 일치하도록 변형한다. 마찬가지 방식으로 삽입 메시지가 $01_{(2)}$, $10_{(2)}$, $11_{(2)}$의 경우에도 F_1을 적절한 정수의 덧셈 연산으로 영상 화소의 최하위 2비트를 비밀 메시지와 일치시키는 함수로 정의하고, F_{-1}을 뺄셈 연산으로 정의하여 랜덤하게 적용시킨다.

Westfeld 등이 제안한 PoVs 통계량은 은닉 영상 화소값들이 두 개씩 서로 쌍을 이루어 비슷하게 분포하게 되는 특성에 근거한 것이므로 위의 과정 3처럼 똑같은 값을 가지는 화소 x에 대하여 랜덤하게 더하거나 뺀다면 x가 $(x+1)$이나 $(x-1)$과 서로 상관 관계를 갖지 않게 된다. 또한 Provos가 제안한 변형된 χ^2-통계 분석법처럼 샘플링 구간을 달리하거나 샘플을 x와 $(x+1)$에서 x와 $(x-1)$로 변형하여 분석해도 SES 심층 암호로 삽입한 은닉 영상에서 별다른 특징을 발견할 수 없었다.

보다 안전한 심층 암호 통신을 해야할 경우 원본 영상 1/2 이상의 화소를 RS 통계량 조정에 사용할 수 있다면 거의 모든 실험 영상에 대하여 RS 통계 분석을 통한 탐지를 회피할 수 있었다. 표 1 참조.

3.2 안전성 분석

SES 심층 암호는 메시지 삽입 효과를 주위 화소에 골고루 분산 시키기 때문에 PoVs 통계량을 유지시킨다. 다음은 대략적인 증명 과정이다. 이 증명 과정을 확장할 수 있으므로 여기에서는 한 화소당 한 비트 삽입에 대해서만 언급하겠다.

$P(X = x)$를 원본 영상 화소 x에 대한 확률 분포라고 하고, $P(Y = y)$를 SES를 이용하여 메시지를 삽입한 은닉 영상 화소 y에 대한 확률 분포라고 하자. 만약 삽입하는 메시지 비트의 분포가 랜덤하다면 은닉 영상 화소의 확률 분포 $P(Y = n)$은 식(7)를 만족하게 된다.

$$\begin{aligned} P(Y = n_i) &= \frac{1}{2} P(X = n_i) \\ &+ \frac{1}{4} P(X = n_{i-1}) + \frac{1}{4} P(X = n_{i+1}) \\ P(Y = n_{i+1}) &= \frac{1}{2} P(X = n_{i+1}) \\ &+ \frac{1}{4} P(X = n_i) + \frac{1}{4} P(X = n_{i+2}) \end{aligned} \tag{7}$$

그러면 일반적으로 다음 식이 성립함을 알 수 있다. 여기에서 $y = n_i^*$는 실험 영상에서 관찰할 수 있는 이론적인 은닉 영상 화소의 산술 평균이다.

$$\begin{aligned} P(Y = n_i^*) &= \frac{1}{2}\{P((Y = n_i) + P((Y = n_{i+1})\} \\ &= \frac{3}{8}\{P((X = n_i) + P((X = n_{i+1})\} \\ &+ \frac{1}{8}\{P((X = n_{i-1}) + P((X = n_{i+2})\} \\ P(Y = n_i^*) &\neq P(Y = n_i) \\ \text{nor} \quad P(Y = n_i^*) &\neq P(Y = n_{i+1}) \end{aligned}$$

따라서 SES를 이용하여 메시지를 삽입한 은닉 영상은 최하위 비트 치환 방식의 은닉 영상에서 나타나는 PoVs 통계량의 유사성이 발견되지 않음을 알 수 있다. 그리고 SES 심층 암호 알고리즘은 자체적으로 메시지 삽입 후에 RS 통계량이 원본과 크게 달라졌을 경우에 이를 보정해주기 때문에 RS 통계 분석에도 강인성을 보인다.

Ⅳ. 실험 결과

χ^2-통계 분석과 RS 통계 분석을 통해서 삽입 확률이 모두 0인 160개의 BMP 파일 영상을 대상으로하여 각각 10kbytes, 40kbytes, 70kbytes의 암호문을 삽입한 후 통계 분석을 하였다. 실험 영상은 디지털 카메라 촬영 후 BMP로 변환한 영상과 컴퓨터로 생성한 영상(fractal image), 그리고 24비트 만화 등 여러 가지 특성의 영상들을 선정하였다. 또한 삽입 용량의 비교가 편리하도록 원본의 크기는 모두 $512\times379\times24\cong570$kbytes으로 고정하였다. 암호문과 난수의 생성 방식은 비밀키 암호인 AES[8]를 사용하였다.

그림 2는 한 화소당 1비트 삽입 방식으로 40KB의 메시지를 삽입한 은닉 영상이다.

표 1은 160개의 은닉 영상에 대하여 각각의 통계분석법에 의해 탐지된 영상의 개수를 나타낸다. χ^2-통계 분석 시 예상 은닉 영상의 분포와 실험 영상의 분포 간의 유사도 p값이 90%이상일 때 은닉 영상으로 판별하였으며, Provos가 제안한 확장된 알고리즘을 이용하였다. RS 통계 분석의 경우에는 탐지의 임계치 p를 각각 2%와 4%로 달리 했을 때의 결과를 보여준다.

표 5는 기존의 심층 암호 알고리즘과의 비교를 위하여 동일한 조건하에 최하위 비트 치환 심층 암호 알고리즘인 contraband[9]을 이용한 실험 결과를

표 1. 160개 은닉 영상의 분석 결과(1bit/pixel)

	10KB	40KB	70KB
χ^2-통계 분석	0/160	0/160	0/160
RS 통계 분석(4%)	0/160	0/160	4/160
RS 통계 분석(2%)	0/160	3/160	9/160

표 2. 160개 은닉 영상의 분석 결과(2bits/pixel)

	70KB	100KB	140KB
χ^2-통계 분석	0/160	1/160	2/160
RS 통계 분석(4%)	1/160	3/160	7/160
RS 통계 분석(2%)	2/160	5/160	12/160

그림 2. 원본 영상

그림 3. 40KB 삽입 은닉 영상(1bit/pixel)

표 3. 원본과 은닉 영상의 RS 통계량

	원본영상	은닉영상(40KB)
마스크 M을 적용한 후 Regular Group의 개수	59160	58100
마스크 -M을 적용한 후 Regular Group의 개수	58952	58304
마스크 M을 적용한 후 Singular Group의 개수	26878	27919
마스크 -M을 적용한 후 Singular Group의 개수	26943	27850

표 4. 그림 3, 4, 5의 신호대 잡음비

	S/N(dB)
shore018.bmp	52.537
Lena.bmp	52.596
Baboon.bmp	42.468

그림 4. 140KB 삽입 은닉 영상(2bits/pixel)

보여주고 있다.

표 1에서 시사하는 바와 같이 암호문의 삽입량에 상관없이 χ^2-통계 분석으로는 SES 심층 암호에 의한 삽입 영상을 구별할 수 없었으며, 암호문의 삽입량이 적을수록 즉, RS 통계량을 조절할 수 있는 영역이 많을수록 RS 통계 분석에도 강인함을 볼 수 있다. 570/8=71.25이므로 한 화소당 1비트의 메시지를 삽입할 경우 최대 삽입량의 약 50% 가량을 RS 통계량 조정에 사용(40KB)했을 때 거의 탐지되지 않음을 확인할 수 있다.

그리고 표 2는 SES를 이용하여 한 화소당 삽입 메시지 비트를 확장했을 때의 실험 결과를 보여주고 있다. 한 화소당 삽입할 메시지 비트 k는 사용할 환경에 따라 적절히 조절할 수 있으며 우리는 $k=2$인 경우에 대해 실험하였다. 메시지 삽입량이 증가할수록 원본 영상에 대한 변형은 그만큼 증가하게 되므로 한 화소 당 1비트 삽입 방식보다는 많은 은닉 영상에 대하여 다소 높은 메시지 삽입 확률이 나타났지만 그래도 거의 대부분의 은닉 영상이 탐지 확률 이하의 수치를 보이고 있다. 단순 최하위 비트 치환 심층 암호에 비해 2배의 삽입량을 가지면서 통계 분석을 90%

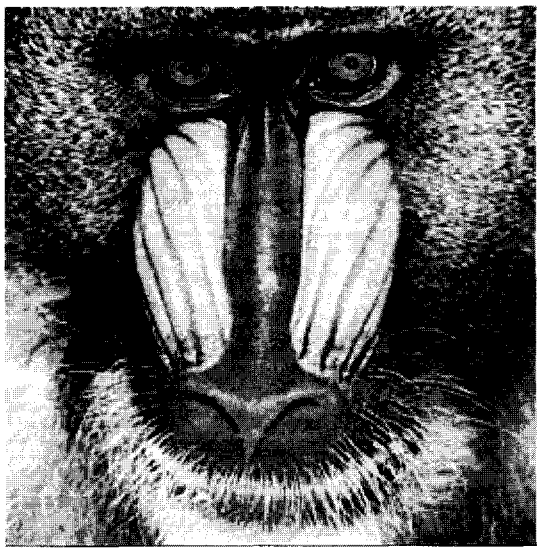


그림 5. 140KB 삽입 은닉 영상(2bits/pixel)

표 5. 160개 은닉 영상의 분석 결과(contraband)

	10KB	40KB	70KB
χ^2-통계 분석	141/160	153/160	160/160
RS 통계 분석(4%)	160/160	160/160	160/160
RS 통계 분석(2%)	160/160	160/160	160/160

이상 회피한 심층 암호 기법은 아직까지 발표되지 않았다.

표 3은 그림 2와 원본 영상과의 RS 통계량을 보여준다. 비록 원본 영상의 RS 통계량과는 다소 차이가 있지만, 은닉물의 R_M과 R_{-M}, 그리고 S_M과 S_{-M}의 개수가 거의 유사하여 식(3)의 통계량을 만족하고 있다. 심층 암호 통신에서는 원본 영상보다 삽입할 비밀 메시지의 가치가 더욱 중요하기 때문에 한 번 메시지 삽입에 이용한 원본 영상을 중복해서 사용한다거나 유통시키는 일 없이 은닉물 생성 후 바로 삭제하는 것이 일반적이다. 따라서 심층 암호의 분석을 원본 영상없이 은닉 영상을 탐지(blind detection) 해야 한다고 가정하여도 무방하므로 SES 심층 암호로 생성된 은닉 영상만으로는 탐지가 거의 불가능하다고 볼 수 있다.

그림 4와 그림 5는 한 화소 당 2비트 메시지를 삽입할 삽입하는 기법으로 140KB의 메시지를 삽입한 은닉 영상이며, 표 4는 주어진 실험 영상의 신호대 잡음비이다.

V. 결 론

본 논문에서 제시하는 SES 심층 암호는 잘 알려진 통계적 심층 암호의 분석법을 고려하여 이러한 통계량을 유지시킨 심층 암호이기 때문에 χ^2-통계 분석이나 RS 통계 분석으로는 탐지되지 않는다. 또한 Outguess나 F5 심층 암호처럼 어느 한 가지만의 통계 특성을 만족시킨다거나 제한된 메시지 삽입량을 가지지도 않는다. 지금까지 알려진 통계 분석에 안전하게 메시지를 삽입하면서도 단순 최하위 비트 치환 심층 암호보다 많은 메시지 삽입도 가능하다.

향후 메시지 삽입 시 비밀키에 의해 랜덤하게 삽입할 수 있도록 일대일 함수(permutation)기법과 은닉물의 RS 통계량이 보다 원본의 통계량에 근접하도록 하는 연구가 보완되어질 예정이다. 또한 공간 영역에서 제안된 심층 암호 기법을 주파수 영역으로 확장하여야 보다 실용적인 심층 암호 통신을 가능하게 할 것이다.

참 고 문 헌

[1] A. Westfeld and A. Pfitzmann: "Attacks on Steganographic Systems," *Information Hiding*, LNCS vol. 1768, Springer-Verlag, 1999, pp.61~76

[2] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color and gray-scale image," Magazine of IEEE Multimedia, 2001, pp. 22-28.

[3] C. Craver, "On public-key steganography in the presence of an active warden," in Information Hiding: Second International Workshop, IH'98, D. Aucsmith, ed., vol. 1525 of Lecture Notes in Computer Science, Springer- Verlag, 1998, pp. 355-368.

[4] G. J. Simmons, "The Prisoner's Problem and the Subliminal Channel," in Advances in Cryptology, Proceedings of CRYPTO'83, Plenum Press, 1984 pp.51~67.

[5] A. Westfeld, "F5—A Steganographic Algorithm," Information Hiding, 4th International Workshop, LNCS 2137, Springer-Verlag 2001, pp. 289-302.

[6] N. Provos, "Defending Against Statistical Steganalysis," in Proceedings of the 10th USENIX Security Symposium, 2001, pp. 323-335.

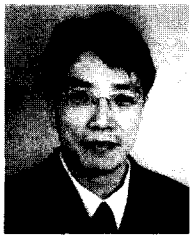
[7] U. Maurer, "A universal statistical test for random bit generators," in Advances in Cryptology - CRYPTO'90, A. J. Menezes and S. A. Vanstone, eds., vol. 537 of Lecture Notes in Computer Science, Springer-Verlag, 1991, pp. 409-426.

[8] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

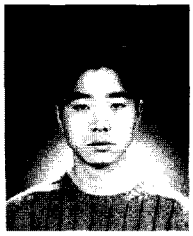
[9] Contraband, http://www.biol. rug.nl/hens/j/contrabd.exe.

〈著者紹介〉

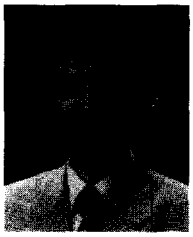
유 정 재 (Jeong-Jae Yu) 학생회원
1998년 8월: 고려대학교 수학과 졸업
2003년 8월: 고려대학교 정보보호 대학원 석사
2003년 9월~현재: 고려대학교 정보보호 대학원 박사 과정
〈관심분야〉 정보은닉이론, 디지털 워터마킹, 정보보호 프로토콜



오 승 철 (Seung-Chul O)
2002년 2월: 고려대학교 수학과 졸업
2002년 3월~현재: 고려대학교 정보보호 대학원 석사 과정
〈관심분야〉 정보은닉이론, 디지털 워터마킹



이 광 수 (Kwang-Su Lee)
1998년 8월: 고려대학교 수학과 졸업
2000년 8월: 고려대학교 수학과 석사 졸업
2000년 9월~현재: 고려대학교 수학과 박사 과정
〈관심분야〉 대수학, 정보은닉이론, 디지털 워터마킹



이 상 진 (Sangjin Lee)
1987년 2월: 고려대학교 수학과 학사
1989년 2월: 고려대학교 수학과 석사
1994년 2월: 고려대학교 수학과 박사
1989년 10월~1999년 2월: 한국전자통신원구원
1999년 3월~현재: 고려대학교 정보보호대학원 부교수
〈관심분야〉 정보은닉이론, 비밀키 암호, 컴퓨터 포랜식스

박 일 환 (Il-hwan Park)
1988년 2월: 고려대학교 수학과 학사
1990년 2월: 고려대학교 수학과 석사
1996년 2월: 고려대학교 수학과 박사
1996년 5월~1999년 12월: 한국전자통신연구원
2000년 1월~현재: 국가보안기술연구소
〈관심분야〉 정보보호기술