J Korea Industr Inf Syst Res Vol.19 No.1, 2014
http://dx.doi.org/10.9723/jksiis.2014.19.1.069

오디오 스테가노그래피에 자료를 숨기기 위한 개선된 LSB 기법

(Advanced LSB Technique for Hiding Messages in Audio Steganography)

지 선 수*
(Seon Su Ji)

요 약 오디오 스테가노그래피는 새로운 비밀통신 기술로서 발전한 은닉메시지를 기록하는 과학이며 예술이다. 그리고 오디오 스테가노그래피는 이진화 된 메시지를 이미지의 8번째 LSB 층에 숨기는 과정과 유사하다. 효과적인 스테가노그래픽 기법은 비밀자료를 많이 숨기고, 감지할 수 없게 하는 것이다. 이 논문에서는 외부적 공격으로부터 비밀 메시지를 안전하게 숨기기 위해 재배열 순서키와 수정된 LSB 기법에 의한 방법을 제안한다.

핵심주제어 : 암호화 재배열키, 오디오 스테가노그래피, 최하위 비트, 자료 은닉

Abstract Audio seganography is the art and science of writing hidden messages that evolves as a new secret communication method. And audio steganography is similar to the process of modifying the Least Significant Bit of image files 8th LSB layer embedding has been done for desired binary messages. The effective of steganographic tools is to obtain imperceptible and robust way to conceal high rate of secret data. The objective of this paper is to propose a method for hiding the secret messages in safer manner from external attacks by modified LSB technique and encryption rearrangement key.

Key Words : Audio Steganography, Data Hiding, Encryption Rearrangement Key, Least Significant Bit(LSB)

1. 서 론

인터넷은 정보검색에서부터 상품구매와 인터넷 뱅킹에 이르기까지 현대를 살아가는 우리 모두의 활동 영역에서 핵심으로 자리매김하였다. 그러나 인터넷이 모든 분야에 확장 적용됨으로써 긍정적인 효과가 있는 반면에, 최근 크고 작은 정보보안 사고가 끊임없이 발생하면서 정보보호에 대한 국가적, 사회적 요구가 매우 커지고 있다. 예를 들어 정보보호실태조사에서 국내 기업 중 62.6%가 자사 시스템에 대한 보안투자가 전무하고, 개인정보 처리자의 통제·관리가 미흡한 것으로 나타났다는 점은 기업들의 보안대책이 얼마나 허술한지를 보여주고 있다. 개인정보유출은 2차 및 3차 피해로 확대되어질 수 있기 때문에 지속적으로 발생하는 해킹사건에 적극적이며, 공격적 보안 대책을 강구하여야 한다[1][2]. 즉 오프라인에서 시민의 안전

* 강릉원주대학교 정보기술공학과, 교신전자
(ssji@gwnu.ac.kr)

과 위협으로부터 대응하기 위해 각종 치안대책을 마련하듯, 인터넷상에서도 개별 사용자가 안심하게 이용할 수 있도록 위협과 불안요소를 해결하고 대응책을 항상 준비하여야 한다. 정보화 시대에서 보안시스템 강화는 선택사항이 아닌 필수요소이며, 끊임없이 진화하고, 예방하고, 대응기술을 개발하여야 한다. 이러한 분야 중의 하나로써 일상적으로 사용하는 다양한 매체에 특정 정보를 숨기는 개념 즉, 스테가노그라피는 자료의 존재 자체를 은닉하여 상대방에게 비밀정보를 전달하는 가장 고전적인 암호화 기법이다. 일반적인 스테가노그래피 적용 방법은 다음과 같다[3][4].

커버 (호스트) 매체 + [비밀 자료] = 스테고 매체 (1)

여기에서 커버 매체로 텍스트, 오디오, 이미지, 동영상 등 인터넷에서 활용되는 모든 매체를 사용할 수 있다. 이때 일반적으로 다양한 디지털 매체를 통해 자료를 숨겨 전송하는 스테가노그라피 기술은 두 가지 기본 요건을 충족해야한다. 첫 번째 요구 사항은 인위적인 자료 추가에 따른 왜곡을 감지할 수 없는 지각 투명성(perceptual transparency), 즉 커버 매체와 스테고 매체가 인간의 청각 및 시각 시스템에 의해 식별되어서는 안 된다. 두 번째 제약 조건은 커버 매체에 삽입되는 비밀 자료의 은닉 속도와 삽입율이다.

오디오 신호에 비밀 자료를 삽입하고 추출하는 기법이 효과적으로 사용될 수 있는 것은 인간의 청각 시스템에서 순간적인 인간의 소리에 대한 지각시간(perceptual time)이 짧고, 낮은 소리간의 미세한 차이를 구별하기가 불가능하다는 현실적인 특성을 역이용한 것이다. 스태가노그라피에서 커버 매체에 비밀 자료를 삽입하는 가장 많이 사용하는 LSB(Least Significant Bit) 삽입방법은 커버 매체에 비밀 자료를 은닉하기 위해서 가장 일반적이고 쉬운 방법 중의 하나이다. 그러나 경고성 측면에서 LSB 삽입방법은 다른 방법에 비해 외부적 공격에 매우 취약하다[4][5]. 이 논문에서는 이러한 약점을 개선하기 위해 비트 패턴으로 변환한 비밀 자료의 각각의 정보와 삽입 시점에 따라 변동되는 커버 매체의 재배열 순서키와 암호화 연산을 추가하여 커버 오디오 매체의 LSB에 삽입하는 방법을 제안한다. 제안한 모델이 비밀 자료의 수용량과 스태고 매체의 지각투명성이라는 두 가지 요소를 만족하는지 평가하기 위해 SNR(signal to noise ratio)을 사용하였다.

이 논문에서의 구성은 다음과 같다. 2장에서 오디오 스테가노그래피를 이용한 은닉된 비밀 자료 전달기법과 관련된 연구에 대하여 조사한다. 3장에서는 비밀 자료의 삽입 시점에 따라 변동되는 재배열 순서키와 암호화 연산을 기반으로 하고 LSB를 이용하는 오디오 스테가노그래피에 비밀 자료를 포함시키는 개선된 방법을 보여준다. 4장에서 적용 결과를 가지고, 결론을 제시한다.

2. 관련 연구

일반적인 방법으로 오디오 스테가노그래피에서 비밀 자료는 커버 오디오 파일의 바이너리 시퀀스(binary sequence)에 약간의 변형을 가져오면서 오디오 신호에 포함된다. 이때 자료를 커버 매체에 삽입하는 형태에 따라 LSB Encoding, Parity Coding, Phase Coding, Spread Spectrum 등이 있다[4][5][6].

2.1 LSB Encoding

디지털 오디오 파일에 정보를 은닉하는 단순하고, 효율적인 방법으로 가장 많이 이용된다. 일반적으로 비교적 큰 자료를 은닉할 때 적절하게 활용되며, 이상적인 자료 전송속도는 1 KHz 마다 1 Kbps이다. LSB 인코딩이 진행되는 동안 LSB를 이용하는 수가 증가하거나 수정된 LSB 층의 깊이가 커짐에 따라 포함된 자료가 통계적으로 감지하는 확률이 증가되고, 스테고 개체의 지각 투명성은 감소한다. 즉 삽입하는 자료의 크기가 클수록 잡음이 커지고, 감지될 수 있는 위험성이 증가된다. LSB 기법은 외부 공격에 대해 견고하지 않는 단점을 포함하고 있다. 이와 관련되어 신뢰할 수 없는 외부 접근 및 공격에 대해 안전성과 견고성을 높이고, 혼돈과 확산을 가중시킬 수 있는 개선된 기법이 필요하다.

2.2 Phase Coding

작은 변화를 도입하기 보다는 디지털 신호의 위상 스펙트럼에서 위상변화로 자료 비트를 인코딩하여 신호 대 감지되는 잡음(noise)비에 관해 감지할 수 없는

인코딩을 달성한다. 일반적으로 세그먼트의 절대적인 위상은 변경할 수 있지만 세그먼트 인접 그룹 간의 위상 차이는 유지되어야 하며, 외부적 요소에 의한 직접적인 영향에 민감하지 않다. 소리의 위상요소는 잡음으로써 인간의 청각으로 감지할 수 없다는 사실을 역이용한다. 오디오 스테가노그래피의 잡음 유도 방법의 단점을 해결할 수 있으며, 작은 변화를 도입하는 것 보다는 디지털 신호의 위상 스펙트럼에서 위상 이동으로 자료 비트를 인코딩한다. 비밀 자료의 첫 번째 신호 구간에서 인코딩되기 때문에 자료 전송속도가 낮고 복잡하다는 단점이 있다.

2.3 Parity Coding

표본에서 구별된 영역으로 신호를 분해하고, 각 표본 영역의 패리티 비트에 비밀 자료로부터 각 비트를 은닉한다. 표본의 영역으로 신호를 분해하고 표본 영역의 패리티 비트에 비밀 자료로부터 각 비트를 인코딩한다. 송신자가 자료 비트 인코딩을 선택함으로써 삽입된 신호가 조금씩 변화할 수 있다. 또한 외부적 공격에 약하다. 일반적인 패리티 코딩은 다음과 같이 진행된다.

1. 이진화 컬럼 벡터로 숨기려는 비밀 자료를 준비한다.
2. 오디오 파일에서 처음 44 바이트를 이동하여 커버 매체의 잔여 바이트를 나눈다. 이 영역은 자료 요소의 수에 의해 정의된다.
3. 각 영역에서 요소의 수를 확인한다. 선택된 영역의 패리티 비트가 삽입하는 비밀 자료 비트와 일치하지 않을 경우 영역에서 표본 중에 하나의 LSB를 반대 정보로 바꾸어 준다. 결과를 가지고 스테고 매체를 구성한다.

2.4 Spread Spectrum(SS)

가능한 주파수를 최대한으로 걸쳐 인코딩된 자료를 분산하려고 시도한다. 이것은 무작위로 전체 오디오 파일을 통해 자료 비트를 확산하는 LSB 인코딩의 구현 방법과 유사하다. 그러나 LSB 인코딩과는 달리 SS 방식은 실제 신호의 독립적인 코드를 사용하여 오디오 파일의 주파수 스펙트럼을 통해 비밀 자료를 분산시킨다. 따라서 최종 신호가 실제로 전송에 필요한 것은 초과 대역폭이 차지한다. 이 방법은 견고하고 높은 수준의 보안을 유지할 수 있지만 오디오 파일에 소음이 추가될 수 있는 위험요소가 있다. 또한 변환 및 역변환 과정에서 지연이 발생할 수도 있다.

오디오 스테가노그래피에서 비밀 자료를 삽입하는 형태에 따른 장단점을 비교하였다. Parity coding 기법은 다른 방법에 비해 상대적으로 단점이 노출되는 반면에 LSB 기법은 신뢰성과 적용성 측면에서 비교적 우수한 기법이다. Phase 기법은 watermarking에서 기본적으로 사용되는 것으로 비밀 자료가 전체적으로 분산되지 않기 때문에 공격자에게 쉽게 노출될 수 있다. 일반적으로 오디오 스테가노그래피를 평가하는 요소로서 삽입용량(payload capacity), 비인지성(imperceptibility), 견고성(robustness), 실시간적합도(real time suitability)를 사용한다[4][7][8]. <표1>에서 오디오 신호에 적용되는 스테가노그래피의 요소별 평가를 보여준다.

<Table 1> 오디오 신호에 적용되는 스테가노그래피의 요소별 평가

구분	삽입용량	비인지성	견고성	실시간적합도
LSB	높음	중간	낮음★	높음
Phase	낮음★	높음	높음	중간
Parity	중간	중간	낮음★	낮음★
SS	높음	낮음★	높음	낮음★

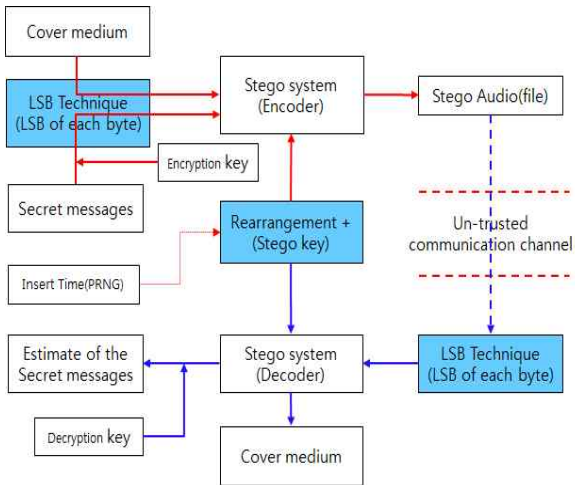
<표1>에서와 같이 LSB 삽입기법은 다른 방법에 비해 복잡성 측면에서 외부적 공격에 취약하므로 이러한 약점 즉, 견고성을 개선할 필요가 있다.

3. 개선된 오디오 스테가노그래피

커버 오디오 매체에 비밀 자료를 삽입할 때 삽입하고자 하는 비트 자료, 은닉 시점에 따라 변동되는 재배열 순서키를 이용하여 커버 오디오 매체에 임의로 재배열하는 것과 암호화 기법을 사용하는 수정된 LSB 오디오 스테가노그래피를 제안한다.

3.1 제안된 방법

<그림1>에서 커버 매체에 비밀 메시지가 삽입되고, 추출되는 과정을 보여준다. 그림에서 진하게 표시된 영역은 논문에서 제안한 부분으로 비밀 자료가 삽입되는 시점에 따라 배치 순서가 다른 재배열키와 암호화를 통해 견고성을 높일 수 있다.



<Fig 1>커버 매체에 메시지 삽입/추출 과정

제안된 알고리즘에서 encoding 순서는 다음과 같다.

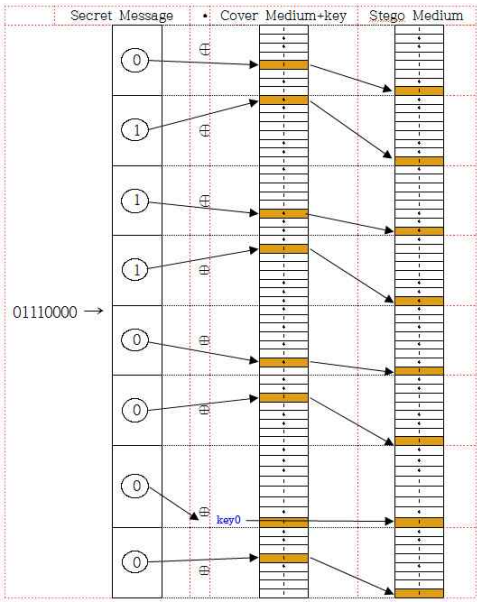
단계1: 커버 매체인 오디오 파일과 은닉하려는 자료를 읽어 들인 후 비트 패턴으로 변환한 다음 각 바이트 단위로 오디오 파일의 LSB를 참조한다. 이때 비밀 자료의 삽입 시점에 따라 변동되는 재배열 순서 키를 참고한다.

단계2: 비트 패턴으로 변환된 비밀 자료와 커버 매체의 비트별 논리적 연산과 순환을 기반으로 한다. 즉 비트화 된 비밀 자료와 재배열 순서 키에 의해 선택된 커버 오디오 파일의 임의의 비트를 기반으로 하여 XOR 연산을 한다.

단계3: 커버 오디오 매체의 각 바이트별 LSB에 2단계에서 계산된 비트 정보를 은닉하는 과정을 수행한다. 이때 <그림2>를 참고한다.

단계4: 2단계와 3단계를 반복한다.

여기에서 최초 은닉위치, 재배열 순서 키는 임의로 설정한다. <그림2>는 비밀 자료, 예를 들어 p('0111000')가 재배열 순서 키에 의해 선택되어진 커버 매체의 비트 정보와 암호화를 거쳐 LSB에 재배열되는 과정을 보여준다. 암호화키와 재배열 순서는 은닉자료가 삽입되는 시점에 따라 정해질 수 있다. ⊕은 XOR 함수를 나타낸다.



<Fig 2> 비밀 자료에서 p('0111000')가 커 오디오 매체에 삽입되는 과정

제안된 알고리즘에서 decoding 순서는 다음과 같다.

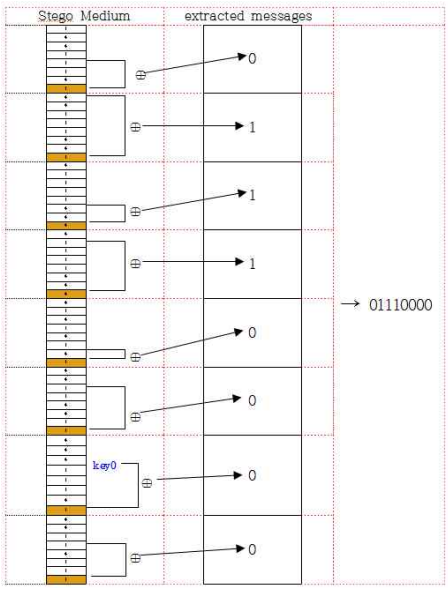
단계1: 스테고 오디오 파일을 읽어 들인 후 비트 패턴으로 변환한 다음 각 바이트 단위로 LSB를 참조한다.

단계2: LSB 정보를 기반으로 하여 재배열키의 역순서에 의해 선택된 비트와 복호화 키 그리고 최초 삽입위치를 참고하여 바이트 단위로 추출한다.

단계3: 추출된 비트 패턴의 자료를 참고하여 재배열 순서 키에 의해 선택되어진 커버 오디오 매체의 비트별 논리적 연산과 역순서를 기반으로 은닉된 비밀 자료를 추정한다. 이때 <그림3>을 참고한다.

단계4: 2단계와 3단계를 반복한다.

<그림3>은 스테고 오디오 파일로부터 임의의 역배열 순서, 복호화 키 등을 이용하여 비밀 자료를 추출하는 과정을 보여준다.



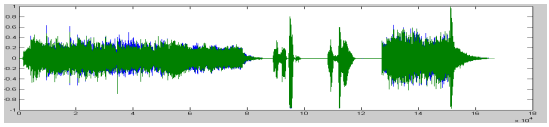
<Fig 3> 스테고 오디오 파일에서 비 밀 자료를 추출하는 과정

3.2 적용

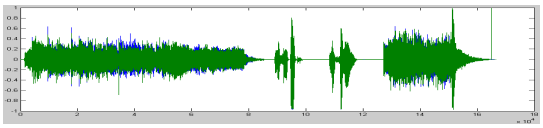
논문에서 사용된 오디오 파일은 100Kbyte, 10sec 이상 동작되는 웨이브 파일(.wav)로 제한한다. 알고리즘을 구현하는 과정은 J2SE와 MatLab을 이용하였다. 여기에서는 다음 자료를 이용하여 비밀 자료를 커버 오디오 파일의 최초 은닉시점(H_{point}) 이후부터 삽입하였다.

· 커버 오디오 파일(Funny.wav, 8bit file)
· 335,504Byte(작동시간 10sec)
· 비밀 자료(114Byte(92자))
· 재배열 순서키(O_{key}='516273k4'), k=8
· H_{point}=44

<그림4>와 <그림5>는 커버 오디오 매체의 주파수 신호와 커버 오디오 매체에 비밀 자료가 삽입된 스테고 오디오 매체의 주파수 신호를 각각 나타낸다.

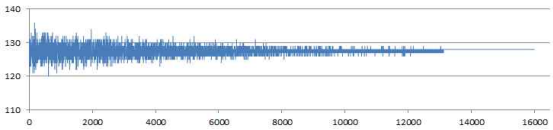


<Fig 4> 커버 오디오 매체 주파수 신호

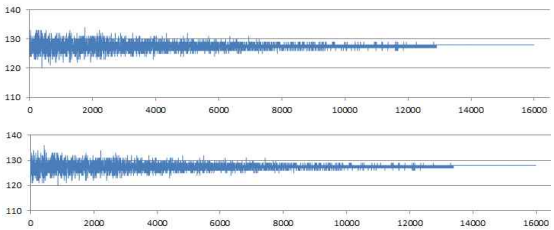


<Fig 5> 스테고 오디오 매체 주파수 신호

커버 오디오 매체와 스테고 오디오 매체의 파일크기와 비밀자료의 삽입전과 후의 주파수 신호에서 차이가 없음을 확인하였다. <그림6>과 <그림7>은 커버 오디오 매체의 인코딩 값과 커버 오디오 매체에 비밀자료가 삽입된 후 스테고 오디오 매체의 인코딩 값을 각각 나타낸다.



<Fig 6> 커버 오디오 매체의 인코딩 값



<Fig 7> 스테고 오디오 매체의 인코딩 값(삽입문자 90(위쪽), 150(아래쪽))

<표2>에서 삽입되는 비밀 자료의 크기에 따라 커버 매체와 스테고 매체의 인코딩값의 차이를 확인하기 위해 대응평균 t 검정을 한 결과를 표시하였다. <그림6>과 <그림7> 그리고 <표2>에서와 같이 t값이 매우 작으며, p값이 0.9내외이므로 통계적으로 유의적인 결과로 볼 수 없다. 즉 커버 매체와 스테고 매체의 인코딩 값의 차이가 없다는 것을 확인하였다. 커버 매체에 비밀 자료가 삽입되는 것으로 인해 왜곡된 정보가 존재한다고 할 수 없을 만큼 비밀자료 삽입전과 후의 인코딩 값에도 차이가 없다는 것을 확인하였다.

<Table 2> 커버 매체와 스테고 매체의 인코딩값의 차이를 확인하기 위한 t값

구분	t value	p vlaue
Ⅰ(30)	-0.19	0.84
Ⅱ(60)	0.04	0.96
Ⅲ(90)	0.05	0.95
Ⅳ(150)	-0.01	0.98

제안된 방법의 성능을 확인하기 위해 신호와 잡음 신호의 비율을 정량적으로 나타내기 위한 지표로서 사용되는 신호 대 잡음비(SNR)와 최대 SNR은 (2)와 (3)식으로 각각 계산할 수 있다[9].

$$SNR = 10 \cdot \log_{10} \frac{\sum_{i}^{m} stg(i)^2}{\sum_{i=1}^{m} |cov(i) - stg(i)|^2} \quad (2)$$

$$PSNR = 10 \cdot \log_{10} \frac{(max)^2}{MSE} \quad (3)$$

여기에서 $MSE = \frac{1}{m} \sum_{i=1}^{m} |cov(i) - stg(i)|^2$으로 계산할 수 있으며, max는 매체의 신호 수준에서 최대값을 나타낸다. $cov(i)$와 $stg(i)$는 i번째 커버 및 스테고 매체의 신호 수준값을 각각 나타낸다. m은 오디오 표본의 수를 나타낸다.

<Table 3> 커버 매체에 비밀 자료의 크기가 다르게 삽입될 때 SNR 값

구분	SNR	PSNR	SNR*	기준
Ⅰ(30)	80.487	83.852	-	> 40
Ⅱ(60)	80.662	84.165	48.39	
Ⅲ(90)	79.881	87.990	-	
Ⅳ(150)	79.971	87.657	49.28	

<표 3>에서는 커버 매체에 비밀 자료의 크기가 다르게 삽입될 때 SNR 값을 보여준다. (*)표시된 것은 고정된 배열키를 사용했을 경우의 값을 표시한 것이다. 예를 들어 60자(73byte)가 삽입될 경우 SNR 값은 80.662이며, PSNR은 84.165로 충분히 크다. 따라서 커버 매체에 비밀 자료가 삽입될 경우에도 왜곡된 정보가 존재하지 않는다라고 판단할 만큼 양호한 수준이라고 결론지을 수 있다.

4. 결 론

스테가노그래피를 적용할 때 기밀성 적용과 함께 비밀 자료가 삽입되었다는 흔적이 나타나지 않는 것이 중요하다. 커버 오디오 파일에 비밀 자료가 삽입된 다음에 인코딩 전과 후의 파일의 크기에 변화가 없으며, 인코딩 및 디코딩 시간이 매우 짧다는 것을 확인하였다. 오디오 스테가노그래피에 비밀 자료가 삽입될 때 SNR 값을 비교하면, 왜곡의 흔적을 찾아낼 수 없음을 확인할 수 있다. 비트 패턴으로 변환된 자료에서 각각의 비트정보와 삽입 시점에 따라 변동되는 재배열 순서키에 의해 선택되어진 커버 오디오 매체의 비트 정보를 암호화하여 커버 매체의 LSB에 재배열함으로써 애매모호성이 증가되고 견고성 측면에서의 취약점을 크게 감소시킬 수 있다. 즉 확산과 혼돈을 동시에 부여할 수 있다.

Reference

[1] 방송통신위원회, "정보보호실태조사와 정보보호지수", http://www.kcc.go.kr/, 2012. 03. 27.

[2] 지선수, "스테고 이미지에서 은닉메시지 감지기법", KIISC, Vol. 14, No. 3, pp. 37-43, 2009.

[3] B. Santhi, G. Radhika and S. R. Reka, "Information Security using Audio Steganography-A Survey", Research Journal of Applied Sciences, Engineering and Technology, Vol. 4, No. 14, pp. 2255-2258, 2012.

[4] S. Swaminathan, H. Manikandan and S. Suganya, "High Confidentiality Based Secured Communication through Audio", European Journal of Scientific Research, Vol. 73, No. 2, pp. 157-162, 2012.

[5] G. Nehru and P. Dhar, "A Detailed look of

Audio Steganography Techniques using LSB and Genetic Algorithm Approach", International Journal of Computer Science Issues, Vol. 9, No. 2, pp. 402-406, January 2012.
[6] M. L. MatKiah, B. B. Zaidan, A. A. Zaidan, A. Mohammed Ahmed and Sameer Hasan Al-bakri, "A Review of Audio based Steganography and Digital Watermarking", International Journal of the Physical Sciences, Vol. 6, No. 16, pp. 3837-3850, August 2011.
[7] A. Z. Al-Othmani, A. A. Manaf and A. M. Zeki, "A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation", International Journal of Computer Science Issues, Vol. 9, No 1, pp. 30-37, January 2012.
[8] V. L. Reddy, A. Subramanyam and C. Reddy, "Implementation of LSB Steganography and its Evaluation for Various File Formats", International Journal of Advanced Networking and Applications 868, Vol. 2, Issue 5, pp. 868-872, 2011.
[9] S. Malviya, M. Saxena, K. K. Nayak and A. Khare, "Audio Steganography in a Nutshell", International Journal of Electronics Communication and Computer Technology, Vol. 2, pp. 219-222, 2012.

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

논 문 접 수 일 : 2014년 01월 14일
1차수정완료일 : 2014년 02월 10일
2차수정완료일 : 2014년 02월 17일
게 재 확 정 일 : 2014년 02월 19일