VoIP 환경을 위한 Low bit Encoding 스테가노그라픽 모델

Steganographic Model based on Low bit Encoding for VoIP

김 영 미*
Young-Mi Kim

요 약

본 논문에서는 VoIP(Voice over IP) 통신에서 효율적으로 사용할 수 있는 Low bit Encoding에 의한 새로운 스테가노그라피 모델을 제안한다. Low bit Encoding 방법을 사용하는 대부분의 스테가노그라피 모델은 비밀 메시지 삽입 용량에 제한이 있다는 것과 비밀 메시지 위치를 쉽게 인지할 수 있다는 문제점을 가지고 있다. 이러한 문제점을 개선하였고 사람의 가청구간을 벗어나는 영역에 1 비트 이상의 비밀 메시지를 삽입하여 커버 데이터에 숨길 수 있는 메시지의 삽입 용량을 향상시켰다. 은닉 위치는 삽입 메시지 길이를 시드로 가지는 의사난수를 이용하여 선택하여, 공격자가 은닉된 비밀 메시지를 쉽게 공격할 수 없도록 하였다. 제안된 모델은 VoIP환경 하에서 적합하도록 구현하였으며, 웨이브파일에 정보은닉을 하여 전송할 수 있을 뿐만 아니라 사용자에 대한 기본정보 및 인증 시스템에서 다양한 정보를 은닉 하는데 활용할 수 있다.

Abstract

This paper proposes new Steganographic model for VoIP that has very effective method using low bit encoding. Most of Steganographic models using Low bit Encoding have two disadvantages; one is that the existence of hidden secret message can be easily detected by auditory, the other is that the capacity of stego data is low. To solve these problems, this method embed more than one bit in inaudible range, so this method can improve the capacity of the hidden message in cover data. The embedding bit position is determined by using a pseudo random number generator which has seed with remaining message length, so it is hard to detect the stego data produced by the proposed method. This proposed model is able to use not only to communicate wave file with hidden message in VoIP environment but also to hide vary information which is user basic information, authentication system, etc.

☞ keywords: Steganography, Information Hiding, Low bit Encoding, Cover Data, Stego Data

1. 개 요

초고속 데이터 통신망의 발달로 인해 현재 다양한 디지털 멀티미디어 데이터가 네트워크를 통해 손쉽고 편리하게 전송된다. 특히 디지털 멀티미디어 콘텐츠들의 사용이 급속도로 확산되면서 정보 보호는 매우 중요한 부분이며 비밀 통신을 원하는 사용자들에게는 배제할 수 없는 문제이다. 정보 보호를 위한 방법의 하나인 정보 은닉(Information Hiding)기술에 관한 연구가 널리 수행되고 있으며, 다양한 방법의 메커니즘들이 개발되고 있다. 정보 은닉 기술 중 스테가노그라피(Steganography)는 디지털화 된 콘텐츠에 비밀정보를 숨겨서 송신자(sender) 및 수신자(receiver)간에 비밀 통신을 하는 기법이다[1].

스테가노그라피는 일반적인 커버 데이터(cover data)에 비밀 메시지를 은닉시켜 스테고 데이터(stego data)를 생성하는 것이며, 비정상적인 사용자의 접근으로부터 은닉된 비밀 메시지를 보호하는 것이다[4].

스테가노그라피에 응용될 수 있는 커버 데이터

* 정 회 원 : 경기대학교 전자계산학과 박사과정
rosekim@kyonggi.ac.kr
[2007/08/23 투고 - 2007/08/27 심사 - 2007/09/05 심사완료]

는 텍스트, 이미지, 동영상, 오디오등이 있으며 현재 가장 발전된 분야는 이미지를 이용한 스테가노그라피이다.

일반적으로 오디오 스테가노그라피에서는 음악을 듣는 청취자가 실제로 인식하지 못하는 부분에 데이터를 숨기기 때문에 실제 데이터가 숨겨져 있다는 것을 일반 청취자들은 알지 못한다. 뿐만 아니라 비밀 데이터를 은닉한 스테고 데이터의 크기가 원본 데이터의 크기와 같으면 청각적으로 거의 차이를 느끼지 못한다. 그러나 공격자 또는 일반 청취자가 은닉된 정보의 존재를 인지할 수 있다면 추출이나, 손상이 어렵다 하여도 안전하다고는 할 수 없다.

인증이나 저작권 보호 뿐 아니라 중요한 정보를 포함하는 파일을 전송할 때에 적용할 수 있는 많은 스테가노그라피 방법들이 개발되었다. 본 논문에서는 Low bit Encoding 방법을 사용하여 VoIP 환경 하에서 적용할 수 있는 스테가노그라피 모델을 제안하려고 한다.

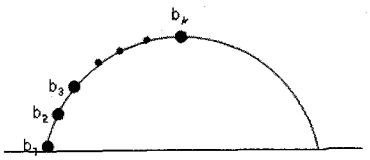
VoIP는 네트워크의 크기나 통신 주체들 사이의 거리에 거의 영향을 받지 않으므로 인터넷 전화망에서 사용되고 있다. VoIP는 IP패킷을 사용하여 수신자가 송신자에게 유사 오디오신호를 전송하는 인터넷 프로토콜로 본 연구에서는 유사 오디오 신호를 웨이브 파일로 접근한다[8]. 현재까지 많은 VoIP 관련 기술들이 개발되었고, 현재도 개발되고 있다. 이러한 이유에서 VoIP 통신에서 정보 은닉은 흥미로운 연구 분야임에 틀림없다.

논문의 구성은 2장에서는 기존 관련 연구들과 문제점을 살펴보고, 3장에서는 VoIP 환경에서 적용될 수 있는 스테가노그라피 방법을 제안하며, 4장에서는 여러 가지 실험 결과를 통하여 제안 방식을 비교 분석하고, 5장에서는 결론을 맺는다.

2. 관련연구

김 영실[2]은 16Bit PCM에서 Low bit Encoding을 이용하여 메시지 삽입을 그림1과 같이 사인곡선의 한 주기에 따라 i 비트 마다 삽입하였다.

$$p(b_j) = \frac{1}{i} \quad (\text{i=16, j}\in\{1,2,3 \cdots 16\}) \quad \text{(식 1)}$$



(그림 1) 사인곡선의 형태로 삽입된 비밀메시지

이 방법은 기존의 방법과는 달리 각각의 비트가 은닉되는 위치가 달라지므로 은닉된 비밀메시지 필터링이 어려워진다.

그림 1과 같이 일정한 간격으로 사인곡선 형태를 이루도록 비밀 메시지 비트를 삽입하는 경우 사인곡선의 한 주기에 따라 i 비트마다 삽입된 비밀 메시지의 위치를 알아낼 확률을 구하면 식 2와 같다. 즉 i 비트마다 비밀 메시지 1비트를 은닉하므로, $P(b_j) = \frac{1}{i}$이 된다. 필터링 된 b_j 위치를 이용하여 b_{j+1}의 위치를 알아낼 수 없고 $P(b_j)$와 마찬가지로 $P(b_{j+1}) = \frac{1}{i}$이 되므로 서로 독립사상이다. 따라서 비밀 메시지가 삽입된 위치를 알아낼 확률은 식 2와 같으며, 사인곡선의 한 주기에 은닉되는 비밀 메시지의 비트수가 필터링 될 확률은 16의 지수 승만큼 작아지게 된다.

$$P(b_1, \cdots, b_j) = \frac{1}{i^j} \quad \text{(식 2)}$$

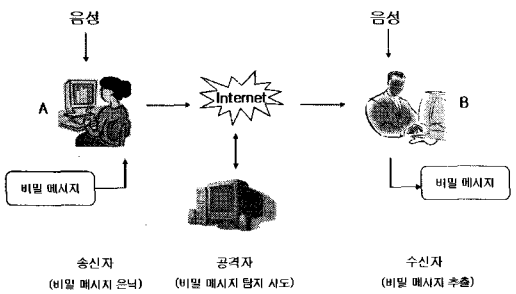
김 영실[2]에서 제안한 모델은 사인곡선 형태로 비밀 메시지가 삽입된 스테고 데이터와 커버 데이터의 실제 코드 값에 차이가 크다면 커버 데이터와 스테고 데이터의 파일 특성이 달라지므로 성공적인 은닉함수라고는 볼 수 없다. 즉 커버 데이터의 주기가 일정하지 않은 경우에는 사인곡선의 주기를 결정하는 것은 어렵다. 또한 삽입하는 비밀 메시지의 은닉위치가 커버 데이터를 벗어나는 경우에는 공격자에게 필터링 되기 쉽고 커버 데이터의 본질이 훼손될 수 있다는 문제점이 발생한다.

본 논문에서는 의사 난수(Pseudo Random Number)를 이용하여 주기성을 가지지 않고 은닉 위치를 임의로 선택하므로, 커버 데이터의 파형 주기에 영향을 주기 않으면서 필터링이 어렵다. 또한 선택된 위치의 웨이브 파일이 가청성의 범위를 벗어난 특정 임계 치 이상인 경우에만 비밀 메시지를 삽입함으로써 가청성(Audibility)을 유지할 뿐 아니라 비밀 메시지를 삽입하는 은닉 함수(Embedding Function)가 알려져도 비밀 메시지 검출이 쉽게 이루어지지 않도록 구현하였다.

3. 모델 설계

스테가노그라픽 모델을 사용하는 VoIP 통신은 다음 그림 2와 같이 나타낼 수 있다.

VoIP 통신에서 사람의 목소리는 웨이브파일로 변환하여 다양한 유형의 메시지를 은닉할 수 있는 오디오 스테가노그라피 시스템으로 접근할 수 있다. 또한, VoIP 환경에서 가장 일반적으로 사용하는 코덱인 G.711은 ITU(International Telecommunication Union)의 표준으로, G.711은 음성을 샘플링 수는 8 kHz, 양자화 비트수는 8로 인코딩한다. 따라서 본 연구에서는 프로토타입으로 RAW PCM(8,000 Hz, 8Bit)을 사용한다[5].



(그림 2) 스테가노그라픽 채널을 사용하는 VoIP 통신

PCM 방식의 웨이브 파일은 잡음과 간섭에 강하고, 전송 중 코딩된 신호를 효과적으로 재생하며, 신호 대 잡음비인 SNR(Signal to Noise Ratio)을 개선하기 위한 채널대역폭의 증가를 효과적으로 바꿀 수 있다. 또, 동일한 포맷으로 공통된 네트워크에서 다른 디지털 데이터에 삽입하기 쉽고, 특수한 변조나 암호화를 적용하기 쉽다[6].

일반적으로 웨이브 파일에 스테가노그라피를 가능하게 하는 기술에는 Low bit Encoding, Phase Encoding, Spread Spectrum, Echo Data Hiding 등이 있다[7]. 실제 가장 일반적으로 구현된 스테가노그라피 기법이 바로 Low bit Encoding으로 마지막 비트에 비밀 메시지 비트를 한 비트씩 삽입하는 방법이다.

본 논문에서 제안하는 알고리즘은 Low bit Encoding 방법이 가지고 있는 낮은 삽입 용량과 쉬운 필터링이라는 두 가지 문제점을 해결하기 위한 것이다.

실제 커버 데이터에 비밀 메시지를 은닉하는 은닉함수(Embedding Function) E 은 다음과 같이 정의할 수 있다.

은닉 함수 E

$$E(C_i, M) = S_i \qquad \text{(식 3)}$$

where C : 커버 데이터의 집합,
M : 비밀 메시지
S : 스테고 데이터의 집합
$i \in N$,
N : 총 샘플링 수

현재 상용화된 오디오 스테가노그라피 대부분이 Low bit Encoding 으로 비밀 메시지를 은닉하고 있다. 일반적으로 Low bit Encoding이 사용되는 가장 큰 이유는 비밀 메시지를 Low bit Encoding 한 후에 생성된 스테고 데이터가 커버 데이터와 가장 유사한 특성을 가지며 또한 간단히 구현할 수 있기 때문이다. 그러나 8비트 커버 데이터인 경우는 8비트마다 1비트씩 비밀 메시지를 은닉하기 때문에 비밀 메시지를 은닉하기 위해 사용할 수 있는 커버 데이터의 선정이 어렵다는 문제점을 가지고 있다. 이를 보완하기 위해선 스테고 데이터가 커버 데이터와 유사한 특성을 가지는 범위 내에서 커버 데이터에 은닉되는 비

밀 메시지를 1비트 이상으로 지정하면 된다. 본 논문에서는 한 비트 이상을 삽입하는 은닉 함수 E_k는 다음과 같이 정의한다.

은닉 함수 E_k

$$E_k(C_i, M) = S_i \quad \text{(식 4)}$$

where C : 커버 데이터의 집합,
M : 비밀 메시지
S : 스테고 데이터의 집합
i ∈ N,
N : 총 샘플링 수
k ={1,2,4,8}

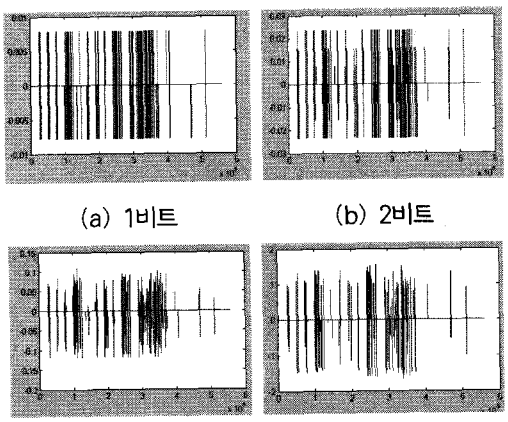
예를 들어, 커버 데이터에서 모든 샘플링 구간에 1 비트씩 은닉한 경우는 E_1, 2 비트를 은닉하는 경우는 E_2,, 4비트까지를 은닉하는 경우는 E_4,가 된다. 본 논문에서는 삽입 메시지를 16비트 2진수로 변환하였고, 웨이브 파일을 8비트로 샘플링하기 때문에 삽입 가능한 비트수는 1, 2, 4, 8이 된다.

삽입되는 비트수를 무조건 늘리게 되면 커버 데이터와 스테고 데이터와의 실제 코드 값의 차이가 커지게 되고, 커버 데이터가 손상되므로 공격자는 커버 데이터에 이상이 있다고 생각할 것이며, 쉽게 은닉된 비밀 메시지를 필터링 할 수 있다. 따라서 실제 커버 데이터의 손상을 적게 하면서, 삽입 가능한 비트수를 찾기 위해서는 E_1, E_2, E_4, E_8과 커버 데이터와의 비트 차이가 어느 정도 나는지를 파일 구성 면에서 분석해 보아야 한다. 김 영실[2]은 16비트 PCM 웨이브 파일을 16진수 코드로 읽어서 커버 데이터로 사용하였다. 실험 결과에서 커버 데이터와 스테고 데이터와의 비트 값 차이는 거의 비슷하였으나 6비트 이상으로 삽입된 경우 현저히 많은 비트 값 차이가 나는 것을 알 수 있다. 이는 커버 데이터를 16진수 코드로 읽은 경우에는 커버 데이터와 스테고 데이터 간의 변화를 최소화하며 즉 커버 데이터의 특성을 유지하고, 커버 데이터의 삽입 용량을 높일 수 있는 이상적인 삽입 비트 수가 2비트부터 4비트 사이라는 것을 알 수 있다.

본 연구에서는 일정 간격으로 샘플링 한 각 샘플마다 진폭 값에 데이터를 은닉하므로 김 영실[2]의 연구 결과를 적용하거나 비교할 수 없다. 그러나 각 샘플마다 은닉하는 경우가 웨이브 파일을 16진수 코드로 읽어서 커버 데이터로 사용한 김 영실[2]의 삽입용량보다 커진다는 것은 당연하다.

그림 3은 매트랩을 이용하여 커버 데이터와 스테고 데이터의 차의 파형을 출력한 결과이다. X축은 샘플링 주파수이고 Y축은 진폭을 나타낸다. 삽입 비트수가 1, 2, 4 인 경우에는 차이 값이 비슷하나 8 비트인 경우에는 완연하게 차이가 발생하였다. 또한 청각적으로도 1, 2, 4 인 경우에는 커버 데이터와 스테고 데이터의 차이를 느낄 수 없었으나, 8인 경우에는 잡음을 느낄 수 있었다.

인간이 감지할 수 있는 소리의 범위는 나이, 성별, 환경 등에 따라 다르지만 보통 20Hz에서 20kHz 사이인 경우가 대부분이므로 20Hz이하이거나 20kHz인 부분에 비밀 메시지를 삽입하면 청각적으로는 구분을 할 수 없다.



(a) 1비트 (b) 2비트

(c) 4비트 (d) 8비트

(그림 3) 스테고 데이터 - 커버 데이터 의 파형

따라서 본 연구에서는 PCM으로 인코딩된 진폭 값을 16비트 2진수로 변환하여서 하위 4비트까지

비밀 메시지를 삽입한다.

Low bit Encoding은 공격자가 은닉된 비밀 메시지를 쉽게 공격 할 수 있다는 문제점을 가지고 있다. 이러한 문제점을 개선하기 위해 비밀 메시지가 은닉되는 삽입 위치의 선택은 고정된 구간 안에서 의사난수를 이용하여 random offset을 계산하고 현재 bit 위치에 offset을 더함으로써 결정한다[3].

의사난수를 이용하여 비밀 메시지를 삽입하는 위치지정함수 SI(Selection Index)는 다음과 같이 정의한다.

$$b_0 = 0$$
$$b_i = b_{i-1} + R_i(x) \quad \text{for } i = 1, \ldots, m \qquad \text{(식 5)}$$

여기에서 b_i는 i 번째 선택된 비트의 위치를 나타내며, $R_i(x)$는 비밀 메시지 중 삽입하고 남은 메시지를 x라고 했을 때 x를 seed로 생성된 의사난수(Pseudo Random Number)이다. 삽입 위치가 커버 데이터의 범위를 벗어나지 않도록 하기 위해 의사난수의 범위는 평균은닉간격 $[1,n]$ (Mean Interval for Embedding) 을 초과하지 않는 범위 내에서 생성한다.

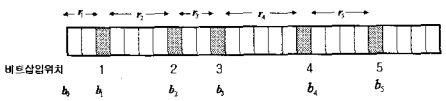
$$n = \partial\left(\frac{l(C)}{l(S)} \times C_p\right) \qquad \text{(식 6)}$$
$$C_p = P(C_i \geq \delta)$$

$l(C)$: 커버 데이터의 총 샘플링수

$l(S)$: 비밀 메시지의 총 비트수

δ: 임계값

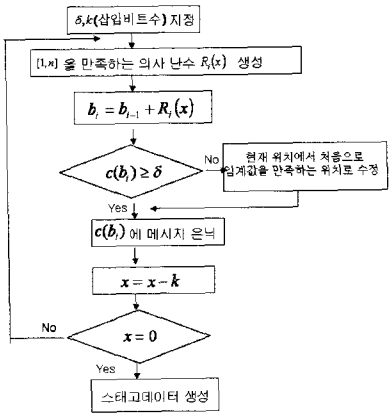
이때 삽입 위치의 샘플링 값이 임계값보다 크지 않은 경우에는 현재위치에서 처음으로 임계값을 만족하는 위치를 찾아서 b_i 값으로 선택한다.



(그림 4) 남은 메시지를 seed로 사용했을 때의 비트 선택 위치

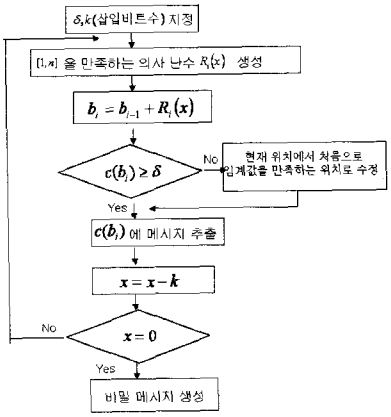
즉, 비밀 메시지 선택 위치가 남은 메시지 길이에 의존하게 되므로 은닉되는 위치가 랜덤하게 웨이브 파일 전체에 골고루 분포하게 된다. 의사난수 생성 시 남은 메시지길이를 seed로 사용하므로 의사난수 값은 메시지가 은닉된 후에만 변화되고, 동일한 선택과정을 이용하면 스테고 데이터로부터 은닉된 비밀 메시지를 추출해 낼 수 있다.

지금까지 설명한 비밀 메시지 삽입과정은 그림 5와 같다.



(그림 5) 메시지 은닉 과정

스테고 데이터로부터 비밀 메시지를 추출하는 과정은 그림 6과 같다.



(그림 6) 메시지 추출 과정

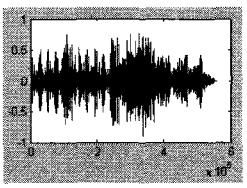
4. 성능 평가

일반적으로 스테가노분석은 시각적, 청각적, 그리고 통계적 방법을 이용하여 분석한다[9]. 따라서 본 연구에서도 인간의 HVS(Human Visibility System)측면, HAS(Human Auditory System)측면, 통계적(Statistical Analysis)측면으로 비교 분석하였다. 실제 실험은 스테레오를 모노로 변환시켜서 실험을 하였고 스테레오로 처리 시에도 동일한 방법하게 적용할 수 있다. 모노로 처리한 스테고 데이터는 복사하여 스테레오로 간단하게 생성할 수 있다.

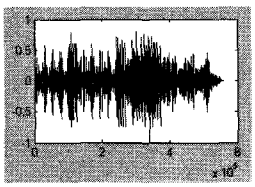
VoIP 환경에 적용하기 위해 샘플링 수는 8kHz, 양자화 비트수는 8, 삽입 비트수 k=4, 임계치 δ =0.4로 하였다. 또한 제안된 모델의 실험결과는 Invisible Secrets 4[10], StegHide[11]와 비교하였다.

4.1 HVS(Human Visibility System) 측면

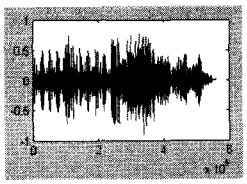
본 논문에서 제안한 스테가노그라피 알고리즘을 이용하여 파형을 분석해보면 시각적으로는 구분하기 힘들다. 그림 7은 매트랩에서 커버 데이터와 스테고 데이터들의 파장을 캡처한 것인데, 웨이브 파형을 보면 커버 데이터와 스테고 데이터를 구분하기 어렵다. 스테고 데이터와 커버 데이터의 차이를 파형으로 보았을 때도 그 차이가 극히 작다는 것을 확인할 수 있다.



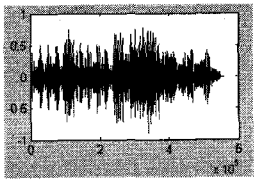
(a) 커버 데이터



<제안 모델>

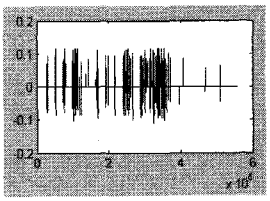


<StegHide>

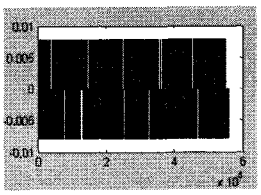


<Invisible Secrets 4>

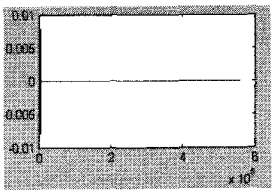
(b) 스테고 데이터



<제안 모델>



<StegHide>



<Invisible Secrets 4>

(c) 스테고 데이터 - 커버 데이터

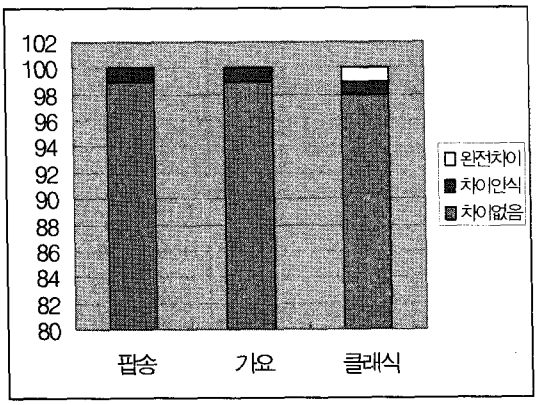
(그림 7) 커버 데이터와 스테고 데이터의 파형

StegHide를 이용하여 생성된 스테고 데이터는 획일적으로 전체 커버 데이터에 선형적으로 메시지를 삽입하였고, Invisible Secrets 4는 메시지를 앞쪽에만 치우쳐서 삽입이 되는 문제점을 가지고 있다. 따라서 두 가지 방법 모두 쉽게 필터링 될 수 있다는 문제점을 가지고 있다. 반면에 본 연구에서 제안한 모델은 전체 파형에서 파형이 큰 위치에만 무작위로 삽입되어 있어서 공격자가 필터링하기 어렵다.

4.2 HAS(Human Auditory System) 측면

다소 주관적인 평가기준이기는 하지만 100명의 학생들에게 청각 실험을 하였다. 3가지 종류의 12개 음악 파일을 커버 데이터와 스테고 데이터로 구분하여 들려주었다. 대부분의 학생들은 커버 데

이터와 스테고 데이터의 차이를 느끼지 못했다. 그림 8은 청각실험 결과를 나타낸 것이다. 음악의 장르별로 차이는 거의 없었다. 따라서 제안된 방법으로는 사람의 목소리를 웨이브 파일로 변환하였을 때 각 개인의 음성상의 특징은 비밀 메시지 은닉에 거의 영향을 주지 않음을 알 수 있다.



(그림 8) 음악 장르별 웨이브 파일 청각 실험

4.3 SA(Statistical Analysis) 측면

스테고 데이터가 커버 데이터에 어느 정도 유사하게 생성되었는지 확인하기 위해 평균, 표준편차(standard deviation), PSNR(Peak Signal to Noise Rate) , 상관계수(correlation coefficient) 등의 통계량을 측정하였다. 그림 9에서 스테고 데이터와 커버 데이터의 상관관계를 분석한 결과 임계값을 증가시키면 기본 통계량들은 거의 변화가 없으나 상관계수는 1에 더 가까워서 커버 데이터와 스테고 데이터가 거의 유사한 특성을 가지고 있음을 알 수 있다. 임계값 증가에 따라 커버 데이터와 스테고 데이터의 통계량 값이 같게 나온 것은 총 샘플링 수에 비해서 삽입 메시지 비트수가 상대적으로 작기 때문이다. 즉 커버 데이터에 비밀메시지를 은닉할 수 있는 최대 임계값을 찾는 것이 커버 데이터에 가장 유사한 스테고 데이터를 생성할 수 있음을 통계적으로 확인할 수 있다.

(a) sampling=8000, l=4, δ=0.4

	커버 데이터	스테고 데이터	스테고-커버
mean	-0.000028	-0.000028	-0.000058
standard deviation	0.089216	0.089216	0.089290
variance	0.007959	0.007959	0.007973
MSE	0.141054	0.141054	0.000057
PSNR	56.636953	56.636953	90.604298
correlation coefficient	0.9996		

(b) sampling=8000, l=4, δ=0.5

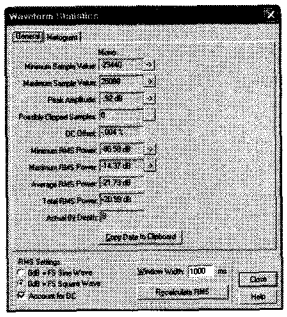
	커버 데이터	스테고 데이터	스테고-커버
mean	-0.000028	-0.000029	-0.000042
standard deviation	0.089216	0.089214	0.089290
variance	0.007959	0.007959	0.007973
MSE	0.141054	0.141055	0.000021
PSNR	56.636953	56.636955	94.97158
correlation coefficient	0.9998		

(c) sampling=8000, l=4, δ=0.6

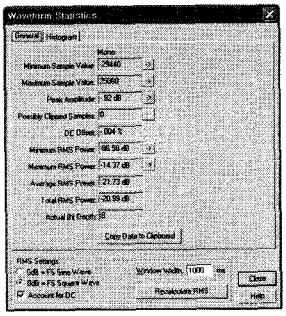
	커버 데이터	스테고 데이터	스테고-커버
mean	-0.000028	-0.000029	-0.000037
standard deviation	0.089216	0.089215	0.089238
variance	0.007959	0.007959	0.007971
MSE	0.141054	0.141057	0.000016
PSNR	56.636953	56.636957	96.05814
correlation coefficient	0.9999		

(그림 9) 임계값 변화에 따는 스테고 데이터의 통계량

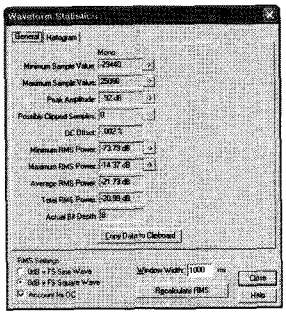
또한 스테고 데이터의 음질이 어떻게 변화했는지를 측정하기위해 최대진폭(Peak Amplitude), DC Offset, RMS등을 쿨 에디터를 통하여 분석하였다. 그림 10에서와 같이 커버 데이터와 제안 모델의 스테고 데이터는 각종 통계량의 변화가 없었다. StegHide나 Invisible Secrets 4를 이용한 경우에는 DC Offset이 -0.004%에서 각각 -0.02%와 0%로 변화하였고 Minimum RMS Power가 -86.58dB에서 -73.79dB과 -100.66dB로 변화하였다.



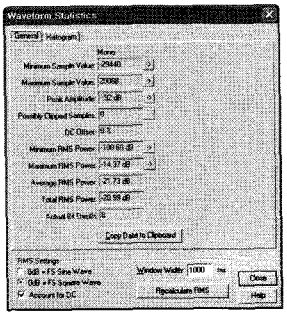
<제안 모델>



(a) 커버 데이터



<StegHide>

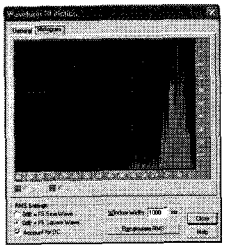


<Invisible Secrets 4>

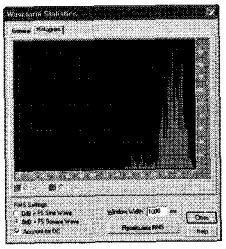
(b) 스테고 데이터

(그림 10) 쿨 에디터를 이용한 각종 통계량 비교

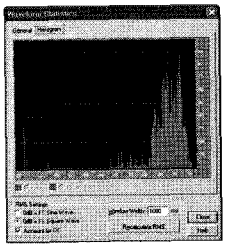
그림 11은 쿨 에디터에서 분석한 Wave form statistical histogram이다. 웨이브 파일의 진폭을 나타낸 것으로 x축은 진폭을 dB로, y축은 진폭의 빈도수를 백분율로 표시한 것이다. 그림을 보면 본 연구에서 제안한 모델이 커버 데이터에 가장 유사한 파장을 가지고 있는 것을 확인할 수 있다. 특히, StegHide 방법은 히스토그램 분포가 커버 데이터와 많은 차이가 있음을 알 수 있다.



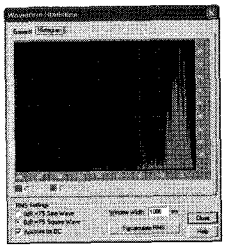
(a) 커버 데이터



<제안 모델>



<StegHide>



<Invisible Secrets 4>

(b) 스테고 데이터

(그림 11) 쿨 에디터를 이용한 히스토그램 비교

5. 결론

일반적인 오디오 스테가노그라피에서는 웨이브

파일을 커버 데이터로 사용한 경우 커버 데이터의 Low bit에 비밀 메시지를 1비트씩 삽입하기 때문에 공격자에게 쉽게 필터링 될 수 있고, 1비트씩 삽입함으로 비밀 메시지를 은닉하기 위해 사용되는 커버 데이터의 크기가 커야 한다는 문제점을 내포하고 있다. 특히, VoIP 환경 하에서 사용할 수 있는 웨이브는 사람의 목소리를 웨이브로 변환하여 사용해야 하므로 파일 사이즈가 작은 경우에 특히 효과적으로 적용을 할 수 있어야 한다.

본 논문에서는 이러한 문제점을 개선하여 VoIP 환경에서 적용할 수 있는 스테가노그라피 알고리즘을 제안하였다.

첫째, 커버 데이터에 숨길 수 있는 메시지의 크기를 향상시키기 위해 사람의 가청구간을 벗어나는 영역에 비밀 메시지를 삽입하였고 삽입 시에도 1비트가 아닌 일정 비트이상을 삽입함으로서 낮은 삽입 용량을 향상시켰다.

둘째, 비밀 메시지 삽입 시에는 은닉 위치를 일정 간격마다 하지 않고 삽입메시지를 시드로 하여 의사난수를 만들어서 위치를 지정하였다.

Low bit Encoding에서 발생되는 공격자가 은닉된 비밀 메시지를 쉽게 공격 할 수 있다는 문제점을 개선하기 위해 비밀 메시지가 은닉되는 삽입 위치의 선택은 고정된 구간 안에서 의사난수를 이용하여 random offset을 계산하고 현재 bit 위치에 offset을 더함으로써 결정하였다.

제안된 모델을 실험한 결과 커버 데이터와 스테고 데이터의 각종 통계량이나 파형에 거의 변화가 일어나지 않았고 현재 상용 스테가노그라픽 모델과 비교해 본 결과 보다 향상된 모델임을 확인할 수 있었다.

이 시스템은 VoIP환경 하에서 웨이브파일에 정보은닉을 하여 전달할 수 있을 뿐 아니라 사용자에 대한 기본정보 및 인증 시스템에서 다양한 정보를 은닉 하는데 활용할 수 있다.

향후에는 커버 데이터와 비밀 메시지를 스캔한 후 최적의 임계값을 지정할 수 있는 연구가 이루어져야 한다.

참 고 문 헌

[1] T. Aura, Practical invisibility in digital communication, In Proceeding of information Hiding - First International Workshop. Springer-Verlag, May/June 1996.

[2] 김 영실, 김 영미, 백 두권, 개선된 Lowbit Endcoding 방법을 이용한 StegoWaveK의 구현, 정보과학회논문지 : 컴퓨팅의 실제, 제9권 제4호,pp470-485

[3] N. Provos, Probabilistic method for Improving Information Hiding. CITI Technical Report01-1, 2001.

[4] N. Provos and P. Honeyman, Hide and Seek: An Introduction to Steganography. IEEE Security & Privacy Magazine, May/June 2003.

[5] N. AOKI, A Band Extension Technique for G.711 Speech Using Steganography, IEICE TRANS COMMNUN., VOL.E89-B, NO6 JUNE, 2006, pp1896-1898

[6] http://www.rfdh.com/bas_com/2-10.htm

[7] http://www.snotmonkey.com/work/school/405/methods.html

[8] J.Dittmann, T. Vogel andd R. Hillert, Design and Evaluation of Steganography for Voice-over-IP, Circuits and Systems, 2006.

[9] Young-Shil Kim, Young-Mi Kim, Jin-Yong Choi, Doo-Kwon Baik, Information Hiding System StegoWaveK for Improving Capacity, New Horizons of Parallel and Distributed Computing,Springer/Kluwer book,2005, pp 271-298

[10] http://www.invisiblesecrets.com

[11] http://steghide.sourceforge.net

◐ 저 자 소 개 ◑

김 영 미(Young-Mi Kim)
1982년 동국대학교 통계학과(이학사)
1984년 동국대학교 대학원 통계학과(이학석사)
2006년 - 현재 경기대학교 대학원 전자계산학과 박사과정
E-mail : rosekim@kyonggi.ac.kr