Journal of the Korea Academia-Industrial Cooperation Society
Vol. 12, No. 12 pp. 5878-5884, 2011

http://dx.doi.org/10.5762/KAIS.2011.12.12.5878

오디오 e-Book 스트리밍을 지원하는 스테가노그래피 모델

이윤정[1], 이봉규[1], 김철수[1*]
[1]제주대학교 전산통계학과

Secure Steganographic Model for Audio e-Book Streaming Service

Yunjung Lee[1], Bongkyu Lee[1] and Chul Soo Kim[1*]
[1]**Dept. of Computer Science and Statistics, Jeju National University**

요 약 본 논문은 오디오 e-Book 스트리밍 콘텐츠에 저작권과 인증과 관련되는 비밀 데이터를 인코딩하고 추출할 수 있도록, 스트리밍 서비스 특성에 적합한 스테가노그래피 서비스 모델과 알고리즘을 제안한다. 은닉 데이터는 송신측과 수신측에서 공유하는 비밀키 k를 사용하여 생성한 의사난수로 암호화하여 안전도를 높였다. 또한 은닉데이터가 커버데이터의 초반 일정구간 안에 랜덤하게 고루 분포하도록 하였고, 스트리밍의 상황을 고려하여 기타의 연산을 단순화하여 처리율을 높였다.

Abstract We present steganographic service model and algorism that fit feature of streaming audio book service in order to hide information of copyright and certificate of it. Secret information is encrypted with random numger by secret key that client and server share, so that increase confidentiality. We made secret data distributed randomly and evenly, and improved throughput by simplifying additional computations considering streaming environment.

Key Words : Audio-book, Steganography, Data hiding

1. 서론

DMB의 보급 및 대표적인 출판 판매업체에서 오디오 북 다운로드 서비스를 시작하면서 오디오 북을 비롯한 e-Book이 디지털 출판 시대의 총아로 떠오르고 있다. 많은 출판사와 서적 판매사가 디지털 오디오 북 제작과 판매를 확대하면서 보고 듣는 책으로 전환을 급격히 이루어지고 있는 것이다.

미국의 경우 이미 소설, 경영 전략서 등을 MP3에 기반을 둔 오디오 북으로 제작하여 정보 네트워크를 통해 차량 내에서 들을 수 있도록 서비스해주고 있다. 즉 이동하는 중에 운전자에게 오디오를 통한 서비스를 제공하는 방법이다. 이런 사례는 현재 우리나라의 경우도 현재 기존의 오디오북 방식을 통하여 자연스럽게 제공되고 있는 방법이다. 그러나 이런 서비스의 경우는 사용자가 미리 관련 파일을 MP3 플레이어에 다운받은 후 플레이어를 이용하여 듣는 서비스이기 때문에 다양한 서비스의 제공이라는 측면은 약하다. 또한 이동 중일 경우, 미리 다운받은 내용만을 반복하여 들을 수밖에 없는 한계를 가진다. 따라서 이런 문제점을 해결할 수 있는 자연스러운 서비스 기법이 오디오 e-Book 스트리밍 서비스 기술이 될 것이다. 이 기술은 텔레매틱스 등의 다양한 무선통신 분야에 적용될 수 있을 것이다. 그러나 이와 같은 방식으로 서비스가 이루어지면, 한편에서는 해당 e-Book 콘텐츠의 저작권을 위협하는 불법적인 스트리밍이 발생할 수 있는 여지가 존재한다.

스테가노그래피(steganography)는 메시지의 존재를 숨기면서 통신하는 기술로서, 평범한 메시지 안에 비밀 메시지가 존재한다는 사실을 제 3자가 알지 못하도록 숨기는 것이다. 이 기술은 비밀 메시지(은닉 데이터)를 감추기 위해 커버 데이터를 사용하는데, 이 커버 데이터로 일반 텍스트 문서를 사용하는 기법, 오디오 파일을 사용하

본 논문은 2008년도 제주대학교 학술연구지원사업에 의하여 연구되었음
*교신저자 : 김철수(kimcs@jejunu.ac.kr)
접수일 11년 10월 19일 수정일 (1차 11년 11월 22일, 2차 11년 12월 12일) 게재확정일 11년 12월 13일

는 기법, 이미지 파일을 사용하는 기법, 동영상 포맷을 사용하는 기법 등이 연구되고 사용되고 있다. 커버 데이터에 은닉 데이터가 인코딩 된 것을 스테고 데이터라고 부른다.

오디오북 스트리밍 상황에서는 커버 데이터로 오디오북을 사용하게 되는데, 기존의 오디오 파일을 커버 데이터로 사용하는 연구를 스트리밍 상황에 적용하기에는 무리가 따른다. 본 연구에서는 스트리밍 서비스 환경에서, 오디오 e-Book 콘텐츠의 저작권과 인증에 관련된 은닉 데이터를 숨길수 있으면서도 스트리밍 특성에 적합한 스테가노그래피 모델을 제시한다.

2. 관련연구

최근 몇 년 동안, 오디오 분야에서 다양한 스테가노그래피 기술이 여러 가지 목적으로 연구되었다. 이 방법들은 인간의 청각시스템의 특성들을 이용하는 연구들이다.

[2-4]은 오디오 커버 데이터의 최하위 비트들을 변경하여 비밀 메시지를 심는 방법 (Least significant bits : LSBs)을 제안하였다. [2]는 LSBs 기술 위에 에러확산 기술을 접목시켰고, [3]은 에러를 최소한으로 줄이기 위한 기술을 도입하였으며(MER), [4]는 일정한 시간적 영역에서 에러를 엄폐하는 기술을 결합하는 알고리즘이다.

이와는 다르게, [5-7]은 웨이블릿 변형을 거친 LSBs에 은닉 데이터를 심는 방법들을 연구하였다. 일반적으로, LSBs 를 기반으로 하는 연구들은 숨겨지는 은닉 데이터의 양은 증가시키는 한편 오디오의 음질 저하를 줄이고자하는데 목적이 있다. [8]은 원본 커버 데이터 파일에 부가적으로 추가될 수밖에 없는 잡음을 최소한으로 줄이는 측면에서 LSB 기술을 설계하였다.

[11,12]의 연구들에서는 오디오 스테가노그래피 기법에 이미지 스테가노그래피 기술을 이용하는 방법을 제시하고 있다.

[13,14]는 스프레드 스펙트럼과 위상 변위 기술을 결합하여 잡음에 견고한 방법을 연구하였다. 이들 연구는 특정한 목적과 응용에 적합하도록 설계되었다.

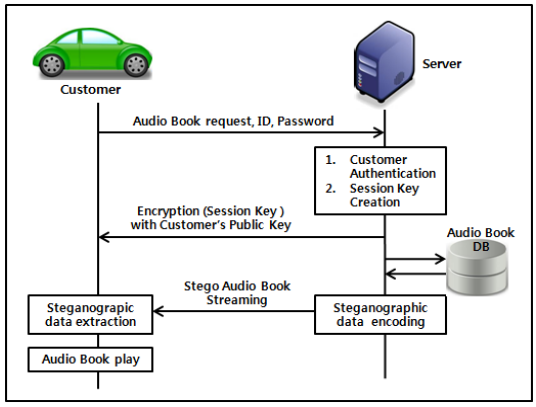
위의 연구들은 정적인 환경에서의 스테가노그래피 연구들로서, 스트리밍 환경과 같은 실시간 처리의 상황이 고려되어 있지 않기 때문에 이들을 오디오북 스트리밍에 적용하기에는 한계가 있다.

본 논문에서는 숨겨진 정보의 비인지성, 공격에 대한 안전성뿐 아니라, 오디오 스트리밍 상황에서 고려되어야 하는 스테가노그래피 인코딩, 추출 과정에서의 빠른 처리를 구현할 수 있는 스테가노그래피 모델을 제안한다.

3. 오디오 스트리밍 스테가노그래피

3.1 서비스 모델 구상도

오디오북 스트리밍 환경에서 스테가노그래피 서비스 모델은 그림 1과 같이 나타낼 수 있다.



[그림 1] 오디오북 스트리밍 스테가노그래피 서비스 모델
[Fig. 1] Audio-book streaming steganographic service model

서비스 요청자인 고객은 DMB나 인터넷 통신 채널을 통하여 오디오북 서버에게 서비스를 요청하고, 해당 서버는 요청된 오디오북을 DB에서 찾은 후, 저작권이나 해당 사업자가 숨기고자 하는 은닉 데이터를 오디오 북 파일 안으로 스테가노그래피 인코딩한 후, 스테고 데이터를 해당 고객에게 통신 채널을 통하여 제공한다. 고객은 실시간으로 전송되어오는 데이터에서 은닉 데이터를 추출하면서 오디오를 재생한다.

본 논문에서는 오디오북 스트리밍의 상황에서 실시간으로 스테가노그래피 데이터의 인코딩과 추출을 보다 안전하고 빠르게 하기 위한 LSB 삽입 방법을 제안한다.

3.2 비밀키 생성과 분배

고객 C 는 원하는 오디오북에 대한 request 와 본인의 ID, Password 를 오디오북 서버로 전송한다. 오디오북 서버는 보내온 ID, Password 로 고객을 인증하고, 현재 Session에서 사용할 비밀키 k 를 생성한 후, 이를 고객 C 의 Public Key 인 *K-c-pub* 로 암호화하여 k' 를 고객에게 전송한다.

$$k' = E\{k\}_{K\text{-}c\text{-}pub} \quad \text{(식 1)}$$

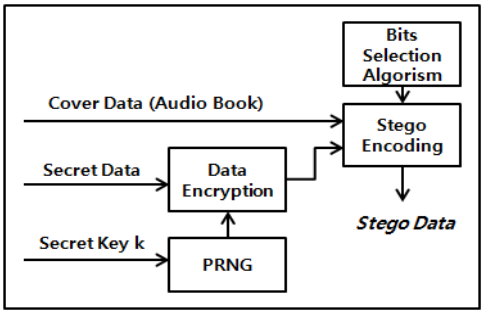
고객 C는 전송되어온 값을 본인의 Private Key인

K-c-pr 로 복호화하여 비밀키 *k* 를 얻는다.

$$k = D(k')_{K\text{-}c\text{-}pr} = D(\ E\{k\}_{K\text{-}c\text{-}pub}\ )_{K\text{-}c\text{-}pr} \quad \text{(식 2)}$$

3.3 은닉 데이터 인코딩

오디오북 서버는 해당 오디오북 파일을 오디오북 DB에서 찾은 후, 오디오북 파일 안으로 암호화된 은닉 데이터를 인코딩하여 삽입한다. 처리과정은 그림 2와 같다.



[그림 2] 스테가노그래피 인코딩
[Fig. 2] Steganographic encoding

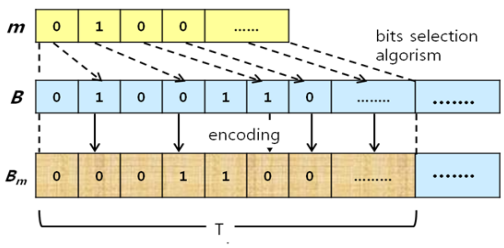
의사난수 생성기는 오디오북 서버와 고객이 공유하고 있는 비밀키 *k* 를 seed 값으로 하여 차례로 난수를 발생시킨다. 비밀 데이터 *X* 는 이 난수들을 대칭키로 하는 블럭 암호 알고리즘을 이용하여 *X'* 로 암호화된다. 은닉 데이터를 암호화하면 보안 레벨을 증가시켜, 인증되지 않은 제 3자가 인코딩 알고리즘을 알게 되더라도 삽입된 은닉 데이터에는 접근할 수 없다는 이점이 있다.

$$RN_i = PRNG(k)_i \quad \text{(식 3)}$$

$$X_i' = E(X_i)_{RNi} \quad \text{(식 4)}$$

where *RN* : 난수
PRNG: 의사난수 발생기
$i = 1, \ldots, n$
$X = \{X_1, X_2, \ldots, X_n\}$
$X' = \{X_1', X_2', \ldots, X_n'\}$

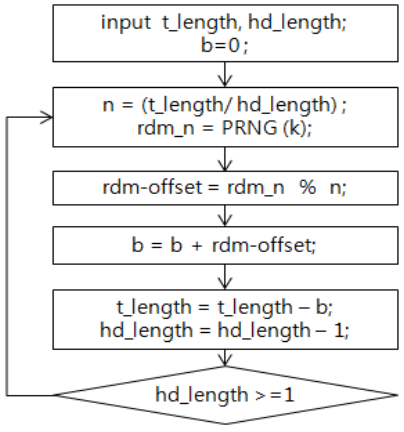
대부분의 오디오북은, 음악파일로 대변되는 기타의 어떤 오디오 파일보다도 재생용량이 크고 시간적으로 길기 때문에 수신자가 어느 시점에 데이터 수신을 멈추게 될지 모른다. 따라서 대부분의 수신자가 수신하고 있을 법한 일정한 시간 T 안에 은닉 데이터를 다 삽입하여야 한다[그림 3].



[그림 3] 은닉 데이터 인코딩 범위 T
[Fig. 3] Secret data encoding block T

LSB는 삽입되는 은닉 데이터의 위치가 노출되기 쉬워 제 3자에 의한 스테고 분석 공격에 취약하다. [10]의 연구는 의사난수를 이용하여 랜덤 값을 산출하고 이를 offset으로 하여 현재 은닉 데이터 삽입된 위치에 offset을 증가시켜 다음 은닉 위치를 선정하였다.

본 논문은 위의 문제들을 해결하면서도, 주어지는 일정시간 *T* 에 적합하도록 하기 위하여 [10]의 알고리즘을 수정하고 단순화 한다. 그로 인해 연산시간을 줄이고, 일정 시간 *T* 안에 모든 은닉 데이터를 고루 삽입할 수 있는 위치선정 알고리즘을 제안한다[그림 4]. t_length 는 모든 은닉 데이터가 삽입되는 일정시간 *T*의 길이, hd_length 는 은닉 데이터 길이, b 는 은닉 데이터가 삽입되는 위치로 한다.



[그림 4] 은닉 데이터 인코딩과 추출을 위한 위치 선정 알고리즘
[Fig. 4] Bits selection algorism for hiding data encoding and extraction

n = (t_length/ hd_length) ;
: 남아있는 *t_length* 와 *hd_length* 로부터 평균은닉간격 *n* 을 산출한다.

rdm_n = PRNG (k);
rdm-offset = rdm_n % n;
: 비밀키 *k* 를 사용하여 의사난수 *rdm_n* 을 생성한다. *rdm_n*을 *n*으로 mod 연산하여 은닉 데이터 삽입위치가 평균 은닉간격 *n*을 벗어나지 않는 범위에서 무작위로 정해지도록 한다.

b = b + rdm_offset;
: 현재의 위치에 *rdm_offset*을 더하여 다음 은닉위치를 정한 후 은닉 데이터 bit를 인코딩하여 삽입한다.

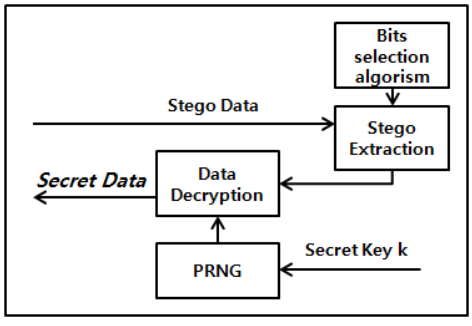
t_length = t_length – b;
hd_length = hd_length – 1;
: 남은 일정시간 *t* 와 남은 은닉 데이터를 재 연산한다.

은닉 데이터의 인코딩 위치가, 남아있는 *t_length*에 의존하기 때문에 은닉위치가 랜덤하게 일정시간 *T* 전체에 골고루 분포하게 된다. 위의 '삽입과 추출을 위한 위치 선정 알고리즘'은 은닉 데이터의 추출에서도 동일하게 적용할 수 있다.

오디오북 서버는 위와 같이 은닉 데이터가 스테가노그래피 인코딩된 오디오북을 통신채널을 통하여 고객에게 전송한다.

3.4 은닉 데이터 추출

고객은 통신채널을 통하여 스테고 오디오북을 전송 받은 후, 비밀키 *k* 와 '삽입과 추출을 위한 위치 선정 알고리즘'을 이용하여 은닉 데이터가 숨겨진 위치를 찾아낸 후, 해당 위치에서 암호화된 은닉데이터를 추출한다. 그림 5는 수신측에서의 은닉 데이터 추출 과정을 도식화하였다.



[그림 5] 스테가노그래피 추출
[Fig. 5] Steganographic extraction

세부과정은 다음과 같다. 고객은 Session 초기에 오디오북 서버가 전송한 비밀키 *k* 를 seed 값으로 하여 의사난수 생성기로 난수들을 생성할 수 있다. 스테고 데이터로부터 추출된 암호화된 은닉 데이터 *X′* 는 이 난수들을 이용하는 대칭키 복호화 알고리즘에 의하여 *X* 로 복호화된다.

$$RN_i = PRNG(k)_i \quad \text{(식 5)}$$

$$X_i = D(X_i')_{RNi} \quad \text{(식 6)}$$

where $i = 1, \ldots, n$
$X' = \{X_1', X_2', \ldots, X_n'\}$
$X = \{X_1, X_2, \ldots, X_n\}$

4. 분석 및 성능평가

4.1 은닉 데이터의 안전성 분석

은닉 데이터 인코딩에서, 오디오북 서버는 암호화된 은닉 데이터를 인코딩하여 삽입한다. 여기서, 비밀키 *k* 를 seed로 하는 의사 난수 생성기로 난수들을 생성하게 되고, 이것으로 은닉 데이터를 블록 암호화한다. 이때, 은닉 데이터 각각의 블록을 암호화하는데 다른 키가 사용된다. 만일 허락되지 않은 제 3자가 그중 하나의 키를 알게 되고, 암호문의 일부를 분석하여 일부 원문을 얻게 되더라도 나머지 은닉 데이터에는 접근할 수 없게 되기 때문에 보안 레벨이 증가하게 된다.

또한 오디오북 커버 데이터 내에서, 은닉 데이터의 다음 인코딩 위치가 남아있는 일정시간을 고려하여 랜덤하게 결정되기 때문에, 은닉 위치를 찾고자하는 분석시도에도 견고하다.

4.2 인코딩 연산 시간 분석

본 절에서는 제안하는 알고리즘의 성능을 분석하기 위하여, 은닉 데이터의 인코딩 연산 시간을 계산한다. 은닉 데이터 bit 순서를 *b1, b2, …, bn* 라고 하고, 은닉 데이터 블록 1개의 인코딩처리 시간을 t_b 하면, t_b 는 다음과 같다.

$$t_b = t_{hint} + t_{rdm-n} + t_{rdm-offset} + t_b + t_{t-length} + t_{hd-length} \quad \text{(식 7)}$$

여기서, t_{hint} 는 은닉 간격 연산시간, $t_{rdm\text{-}n}$ 은 의사난수 생성시간, $t_{rdm\text{-}offset}$ 은 mod 연산을 사용한 은닉 위치 offset 연산시간, t_b 는 다음 은닉 위치 연산시간, $t_{t\text{-}lengh}$ 는 남은 일정시간 연산시간, $t_{hd\text{-}length}$ 는 남은 은닉 데이터 연산시간이다.

n 개 bit 에 대하여 인코딩 위치를 정하고 해당 위치에 인코딩 시키는 전체 시간 T 는 다음과 같다.

$$T = \sum_{i=1}^{n} t_{b_i} \quad \text{(식 8)}$$

$$T = \sum_{i=1}^{n} (t_{hint_i} + t_{rdm-n_i} + t_{rdm-offset_i} + t_{b_i} + t_{t-length_i} + t_{hd-length_i})$$

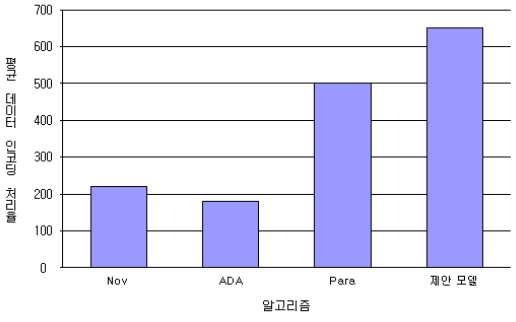
여기서, 다음 은닉 위치 연산시간 t_b 와, 남은 일정시간 연산시간 $t_{t\text{-}lengh}$, 남은 은닉 데이터 연산시간 $t_{hd\text{-}length}$ 은 미미한 수준이기에 무시할 수 있다. 따라서 전체 시간 T 는 다음과 같다.

$$T \approx \sum_{i=1}^{n} (t_{hint_i} + t_{rdm-n_i} + t_{rdm-offset_i}) \quad \cdots\cdots \text{(식 9)}$$

결과적으로, 전체 연산시간 T는 은닉 간격에 대한 나누기 연산과, 의사난수 생성 연산, 모드 연산에 대한 복잡도에 의존한다.

4.3 인코딩 처리율 비교

알고리즘을 비교 분석하기 위하여, 은닉 데이터 인코딩 처리율을 비교 하였다. 커버 데이터로 오디오북 파일 MP3, 여성 목소리, 스테레오, 2분 30초(1.18MB), 스테레오 파일을 사용하였으며, 일정시간 T = 1분, 은닉 데이터로는 799B 텍스트 파일로 실험 하였다. 그림 6은 제안 알고리즘과 기존 연구 Nov[1], ADA[3], Para[9] 를 은닉 데이터 평균 인코딩 처리율 (bps) 을 비교한 결과이다.

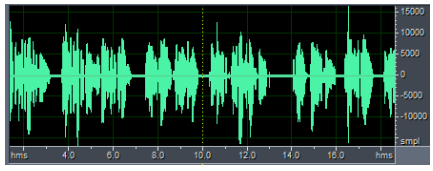


[그림 6] 기존연구와 제안알고리즘 처리율비교
[Fig. 6] Comparison of encoding rates

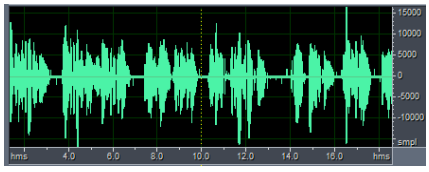
위의 결과는 제안한 은닉 데이터 인코딩 알고리즘의 처리율이 기존의 세 알고리즘보다 높다는 것을 보여주고 있다. 대부분의 연구들은 삽입위치 결정을 랜덤화하기 위해 높은 복잡도의 연산을 수행하는 반면, 제안한 알고리즘은 스트리밍의 상황을 고려하여 기타의 연산을 단순화 하였기 때문이다.

4.4 웨이브 스펙트럼 분석

본 논문에서 제안하고 있는 알고리즘을 시각적으로 분석하기 위하여 웨이브 스펙트럼을 이용하여 비교하였다. 이를 위하여 쿨 에디트 (Cool Edit Pro)를 사용하였으며, 오디오북 원본 커버 데이터와, 제안한 알고리즘으로 처리한 스테고 데이터의 웨이브 파형을 비교하였다. 일정시간 T = 1분 중 초반 20초의 그림이다. 그림 7는 시간영역 (time-domain)에서의 차이를, 그림 8은 주파수영역 (frequency-domain)에서의 차이를 캡처한 것인데, 그 둘 사이의 시각적인 차이를 느끼기 힘들 정도로 차이가 작다는 것을 알 수 있다.

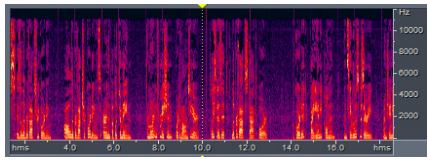


(a) 오디오북 커버 데이터

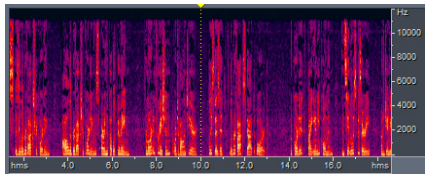


(b) 제안 스테고 데이터

[그림 7] 스펙트럼 시간영역 비교
[Fig. 7] Spectrum in time-domain



(a) 오디오북 커버 데이터



(b) 제안 스테고 데이터

[그림 8] 스펙트럼 주파수영역 비교
[Fig. 8] Spectrum in frequency-domain

5. 결론

본 연구에서는 스트리밍 서비스 환경에서, 오디오 e-Book 콘텐츠의 저작권과 인증에 관련된 은닉 데이터를 숨기기 위해 스트리밍 특성에 적합한 스테가노그래피 서비스 모델과 알고리즘을 제안하였다. 비밀키를 사용하여 생성한 의사난수로 은닉 데이터를 블록 암호화하여 보안 레벨을 증가시켰다. 또한 은닉 데이터가 오디오북 커버 데이터의 일정시간 안에 랜덤하게 고루 분포하도록 하여 은닉 위치 분석에 견고하도록 하였고, 스트리밍의 상황을 고려하여 기타의 연산을 단순화여 처리율을 높였다.

향후 연구로는 오디오북 스트리밍을 사용하는 사용자의 습성에 적합하도록, 은닉 데이터가 삽입되는 일정시간과 임계값을 최적화 시키는 연구가 이루어져야한다.

References

[1] F.A.P. Peticolas, R.J. Anderson, and M.G. Kuhn, “Information Hiding – A Survey,”IEEE Trans.Proc. Thy, Vol. 87, No.7, pp. 1062-1078, July 1999.

[2] N. Cvejic, T. Seppanen, “Increasing robustness of LSB audio steganography using a novel embedding method,” In Proc. IEEE Int. Conf. Info. Tech:Coding and Computing, Vol.2, pp.533-537, April 2004.

[3] N. Cvejic, T. Seppanen, “Increasing the capacity of LSBbased audio steganography.’’ IEEE Workshop on Multimedia Signal Processing, pp. 336-338, 2002.

[4] S.S. Agaian, D. Akopian, O. Caglayan, S. A. D’Souza, “Lossless Adaptive Digital Audio Steganography,” In Proc. IEEE Int. Conf. Signals, Systems and Computers, pp. 903- 906, November 2005.

[5] A. Delforouzi, M. Pooyan, “Adaptive Digital Audio Steganography Based on Integer Wavelet Transform”, Special Issue on Digital Watermarking and Multimedia Security of "Circuits, Systems and Signal Processing (CSSP).", Feb. 2008.

[6] M. Pooyan, A. Delforouzi, “LSB-based Audio Steganography Method Based on Lifting Wavelet Transform”, in Proc. 7th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT'07), December 2007, Egypt.

[7] N. Cvejic, T. Seppanen, “A wavelet domain LSB insertion algorithm for high capacity audio steganography,” In Proc. IEEE Digital Signal Processing Workshop, Callaway Gardens, GA, p. 53 – 55, October 2002.

[8] K. Gopalan, “Audio steganography using bit modification,” Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Vol. 2, pp. 421-424, April 2003.

[9] C. Krätzer, J. Dittmann, T. Vogel, and R. Hillert, “Design and evaluation of steganography for voice-over-ip,” in Proc. IEEE Int. Symp. Circuits Syst., May 2006, pp. 2397 – -3234.

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

[11] P. Bao and X. Ma, “MP3-Resistant Music Steganography based on Dynamic Range Transform,’’ IEEE Int. Sym. Intelligent Signal Processing and Communication Systems, pp. 266-271, Nov. 18-19, 2004, Seoul, Korea.

[12] R. A. Santosa, P. Bao, “Audio-to-image wavelet transform based audio steganography,” IEEE Int. Symp. , pp. 209-212, June 2005, Zadar, Croatia.

[13] H. Matsuka, “Spread Spectrum Audio Steganography using Sub-band Phase Shifting,” IEEE Int. conf. Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP' 06), pp. 3-6, Dec. 2006, Pasadena, CA, USA.

[14] K. Gopalan, “Audio steganography by cepstrum modification,” In Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Vol. 5, pp. 481-484, March 2005.

이 윤 정(Lee, Yunjung) **[정회원]**

- 2002년 8월 : 고려대학교 대학원 컴퓨터과학과 (이학박사)
- 2004년 9월 ~ 현재 : 제주대학교 전산통계학과 교수

<관심분야>
정보경영, 정보통신

이 봉 규(Lee, BongKyu) **[정회원]**

- 1995년 2월 : 서울대학교 컴퓨터공학과 박사
- 1996년 2월 ~ 현재 : 제주대학교 자연과학대학 전산통계학과 교수

<관심분야>
영상처리, SoC

김 철 수(Kim, Chul Soo) **[정회원]**

- 1982년 2월 : 연세대학교 대학원 수학과 (이학석사)
- 1988년 8월 : 연세대학교 대학원 수학과 (이학박사)
- 2003년 3월 ~ 2005년 5월 : 제주대학교 전산원장
- 1989년 4월 ~ 현재 : 제주대학교 전산통계학과 교수

<관심분야>
데이터마이닝, 전산통계, 퍼지응용