J Korea Industr Inf Syst Res Volume 17 Number 5
http://dx.doi.org/10.9723/jksiis.2012.17.5.037

LSB 기법을 이용하는 개선된 오디오 스테가노그래피

(The Improved-Scheme of Audio Steganography using LSB Techniques)

지 선 수*
(Seon-su Ji)

요 약 오디오 스테가노그래피는 오디오 매체(신호)에 암호화된 비밀 메시지를 은닉하여 전송하는 일반적이고, 폭넓게 이용되는 통신기법이다. 인간은 청각시스템의 지각능력의 한계 때문에 커버 오디오 파일과 스테고 오디오 파일의 지각품질(perceptual quality) 차이는 없다. 또한 공격자로부터의 안전성과 견고성 측면에서 LSB 기법은 디지털화된 오디오 신호에 메시지를 삽입하는 효율적이고, 경제적인 방법으로 널리 이용되고 있다. 이 논문에서는 LSB 기법을 기반으로 하고, 디지털화된 비밀 메시지의 비트별 위치를 변경하고, 암호화한 후 커버 오디오 매체에 은닉하는 개선된 방법을 제시한다.

핵심주제어 : 비트 수정, 오디오 스테가노그래피, 자료 은닉, LSB

Abstract Audio steganography is quite similar to the procedure of modifying the least significant bit(LSB) of image media files. The most widely used technique today is hiding of secret messages into a digitized audio signal. In this paper, I propose a new method for hiding messages from attackers, high data inserting rate is achieved. In other words, based on the LSB hiding method and digitized to change the bit position of a secret message, an encrypted stego medium sent to the destination in safe way.

Key Words : Audio Steganography, Bit Modification, Data Hiding, Least Significant Bit

1. 서 론

시간과 장소 그리고 언어적, 세대별 계층에 관계없이 손쉽게 접근할 수 있는 인터넷 환경에서 개인 정보보안에 대한 중요도가 강화되고 있는 추세이다. 미국의 9 11 테러(september 11 attacks)에서 테러리스트들 간의 정보 전달 도구로 스테가노그래피(steganography)가 사용된 흔적이 발견된 이후에 전송매체에 비밀 메시지를 삽입하는 스테가노그래피 알고리즘에 대한 연구가 광범위하게 이루어지고 있다. 은닉된 비밀 메시지의 존재 자체를 감추는 비밀통신의 한 분야인 스테가노그래피는 비밀자료를 텍스트, 이미지, 오디오 등 커버 데이터라 불리는 전송 매체(호스트 매체라고도 한다)에 숨겨진 스테고 매체(stego medium)를 전송하는 방법이다. 즉 허가되지 않은 자는 비밀 메시지가 숨겨져 있다는 사실 자체를 알지 못하도록 하며, 이미지 및 오디오 파일 등과 같은 다양한 디지털 매체를 통해 전달하고자 하는 메시지를

* 강릉원주대학교 정보기술공학과 (ssji@gwnu.ac.kr)

은닉하여 전송하는 것을 말한다. 일반적으로 스테가노그래피는 지각투명성(perceptual transparency)과 비밀 메시지를 삽입하는 높은 전송 비(high data rate/ capacity)를 요구한다. 여기에서 오디오 스테가노그래피는 두 가지 조건을 모두 충족할 수 있다[1][2].

$$\text{커버 (호스트) 매체} + [\text{비밀 메시지} + \text{스테고 키}] = \text{스테고 매체} \quad (1)$$

인간의 시각과 청각 등은 사물을 보거나 청취하는 능력의 한계 때문에 약간의 수정이 가해진 사물과 소리를 감지하여 미세한 차이를 파악하는 것은 현실적으로 매우 어렵다. 즉 오디오 신호에 비밀 메시지를 삽입하고 추출하는 기법이 효과적으로 사용될 수 있는 것은 인간의 청각시스템에서 순간적인 인간의 소리에 대한 지각시간(perceptual time)이 짧다는 특성을 역이용한 것이다[3].

이 논문에서 오디오 스테가노그래피와 암호화 기법을 사용하여 삽입된 메시지 존재 자체를 제 3자가 전혀 알 수 없도록 비밀 메시지를 안전하게 전달하는 개선된 기법을 제시한다. 논문에서의 구성은 다음과 같다. 2장에서 오디오 스테가노그래피를 이용한 은닉된 비밀 메시지 전달기법과 관련된 연구에 대하여 조사한다. 3장에서는 오디오 스테가노그래피에 비밀 메시지를 포함시키는 개선된 방법을 제시한다. 이때 오디오 동작에 영향을 미치지 않는 범위에서 은닉정보를 삽입하며, 적절한 크기 이상의 자료를 삽입할 수 있어야 하며, 삽입 전 후 흔적을 최소화해야 한다. 이를 위해 파일크기의 변화가 없도록 하며, 스테고 파일에서의 삽입 정보로 인한 왜곡(distortion) 수준을 판단하기 위해 신호 대 잡음비(SNR : signal to noise ratio)를 계산한다. 4장에서 적용 결과를 가지고, 결론을 제시한다.

2. 오디오 스테가노그래피 기법

오디오 스테가노그래피에서 비밀 메시지는 커버 오디오 파일의 바이너리 시퀀스(binary sequence)에 약간의 변형을 가져오면서 오디오 신호에 포함된다. 이때 인코딩되는 비밀 메시지 길이는 오디오 파일에서 표본의 총 개수보다 작아야 한다[4]. 일반적으로 가장 많이 사용되는 방법은 위상(phase) 코딩과 최하위 비트(LSB : least significant bit) 코딩 방법이 있다.

2.1 Phase Coding

신호 대 잡음비의 관점에서 안 들리게 인코딩을 이루는 디지털 신호의 위상 스펙트럼의 변화와 같은 비밀 메시지를 인코딩한다. 일반적으로 세그먼트의 절대적인 위상은 변경할 수 있지만 세그먼트 인접 그룹간의 위상 차이는 유지되어야 하며, 외부적 요소에 의한 직접적인 영향에 민감하지 않다. 소리의 위상요소는 잡음(noise)으로서 인간의 청각으로 감지할 수 없다는 사실을 이용한다. 오디오 스테가노그래피의 잡음 유도 방법의 단점을 해결할 수 있으며, 작은 변화를 도입하는 것 보다는 디지털 신호의 위상 스펙트럼에서 위상이동으로 메시지 비트를 인코딩한다. LSB 방법에 비해 복잡하고, 비교적 적은 자료를 은닉할 때 이용하며, 견고성이 우수하고, 디지털 워터마크(digital watermark) 기법 등에서 많이 활용된다. 비밀 메시지의 첫 번째 신호 구간에서 인코딩되기 때문에 자료 전송속도가 낮다는 단점이 있다. 일반적인 구현방법은 다음과 같다[3][4][5].

1단계 : 읽어 들인 오디오 신호는 작은 세그먼트들로 쪼개어진다.

2단계 : 이산푸리에 변환(DFT : discrete fourier transform)은 위상과 푸리에 변환 크기의 행렬을 만들어 각 세그먼트에 적용한다.

3단계 : 수정된 연속적인 세그먼트 사이의 위상 차이를 계산한다.

4단계 : 연속적인 세그먼트 사이의 위상 변화는 비교적 쉽게 감지된다. 따라서 세그먼트의 절대적인 위상은 변경할 수 있지만, 이웃한 세그먼트 사이의 상대적인 위상 차이는 보존되어야 한다. 이를 위해 비밀 메시지는 다음과 같은 형태로 첫 번째 신호 세그먼트의 위상벡터에 삽입한다.

$$phase\_new = \begin{cases} \frac{\pi}{2} & if\ message\ \ bit = 0 \\ -\frac{\pi}{2} & if\ message\ \ bit = 1 \end{cases} \quad (2)$$

5단계 : 새로운 위상 행렬은 첫 번째 세그먼트의 새로운 위상과 원래의 위상 차이를 활용하여 만든다.

6단계 : 새로운 위상 행렬과 원본 크기의 행렬을 사용하여 음향 신호의 역 이산푸리에 변환을 적용하고, 다시 함께 오디오 세그먼트를 연결하여 복원한다.

2.2 LSB Encoding

디지털 오디오 파일에 정보를 은닉하는 일반적이고 효율적인 방법이다. 일반적으로 인코딩 전 후에 파일의 크기 변화가 없으며, 비교적 큰 자료를 은닉할 때 적절하게 이용할 수 있다. 이때 삽입용량인 이상적인 데이터 전송속도는 1 KHz 마다 1 Kbps이다. 예를 들어 16비트로 나타내는 오디오 파일에서 'A(01000001)'를 삽입하기 위해 8개의 연속적인 LSB가 필요하며, 커버 오디오의 연속적인 LSB에 'A'의 이진 비트가 각각 교체된다. 그러나 LSB 기법은 외부 공격에 대해 견고하지 않는 단점을 포함하고 있다[1][5][6]. 이와 관련되어 불손한 외부 공격에 대해 안전성과 견고성을 높이는 개선된 기법이 필요하다. 즉 LSB 기법에서 암호화가 이루지기 전에 디지털화된 비밀 메시지 비트의 위치변화를 추가하여 암호화 알고리즘을 거치면서 혼돈과 확산을 가중시킬 수 있다.

3. 개선된 오디오 스테가노그래피

커버 오디오 매체에 비밀 메시지를 삽입할 때 삽입하고자 하는 메시지 비트의 재배열과 암호화키가 고려된 LSB를 기반으로 하는 오디오 스테가노그래피를 제안한다.

3.1 제안된 방법

기존의 LSB를 이용한 오디오 스테가노그래피 기법에 애모모호성을 가중시키기 위해 변환된 메시지 비트 수준을 재배열한 후 암호화 과정을 적용하는 기법을 제안한다.

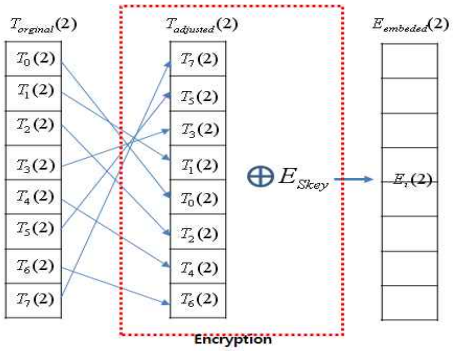
3.1.1 Encoding

기본적인 인코딩 단계는 다음과 같다.

1단계 : 커버 오디오 매체($O(m)$), 은닉하려는 비밀 메시지($H_{message}$), 숨기고자 하는 시작 시점(위치)(t_{Begin}), 스테고 키(E_{Skey})를 읽어 들인다.

2단계 : 바이트 형태로 커버 오디오 파일을 받아서 비트의 바이너리 시퀀스($O_l(m)$, $m = 1, 2, ..., M$, $l = 0, 1, ..., 7$, M은 커버 오디오의 샘플 크기이다)로 변환한다[3][4]. 즉 양자화 단계를 거치면서 비트 패턴으로 변환한다. 숨기고자 하는 시작 위치(t_{Begin})를 참고하여, 오디오 영역의 시간 영역에서 삽입하고자 하는 잠재적 블록을 설정한다.

3단계 : 삽입하고자 하는 비밀 메시지를 비트 패턴으로 처리한다. 즉 하나의 메시지 문자가 8비트 단위로 변환($T_i(n)$, $n = 1, 2, ..., N$, $i = 0, 1, ..., 7$, N은 삽입되는 메시지의 글자 개수이다)되고, 다음 단계에서 비트의 위치를 재배열한다.



<Fig 1> 비밀 메시지에서 2번째 글자(n=2)의 비트 재배열과 암호화 과정

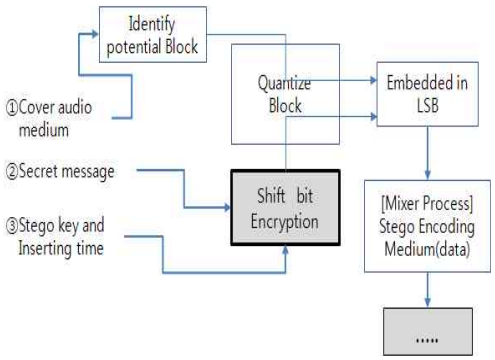
4단계 : 3단계에서 변형된 메시지 비트와 암호화키를 이용하여 논리 연산을 수행한다. 삽입 위치를 참고한 잠재적인 삽입 블록에서 삽입하고자 하는 문자의 비트 정보($E_i(n)$)를 커버 오디오 각각의 최하위 비트(LSB)에 대체한다. 참고로 삽입 시작 시점에서 LSB의 연속 8비트에 '0'을 입력하고, 비밀 메시

지 끝부분의 연속 8비트에 '1'을 각각 삽입한다. 인코딩 단계이며, 스테고 오디오 신호 형태($S_l(m)$)로 쓰여 진다.

5단계 : 2단계부터 4단계를 반복 작업한다.

$$Input\{O(m), H_{message}, t_{Begin}, E_{S\,key}\}$$
$$Determine\ (potential\ embedding\ block)\,|t_{Begin}$$
$$Audio\,|\,QIM \rightarrow O_l(m),\ H_{message} \rightarrow T_i(n)$$
$$\{T_{adjusted}(n) \oplus E_{Skey}(n)\}_{Encryption} \rightarrow E(n)$$
$$\{E_i(n) \rightarrow O_l(m)\}_{incoding} \rightarrow S_l(m)$$

<그림 1>은 숨기고자 하는 비밀 메시지에서 2번째 글자에서 비트가 재배열되어 사용자에 의해 주어진 암호화키와 논리적 연산이 적용되어가는 암호화 과정을 보여준다.



<Fig 2> 제안된 알고리즘에서에서의 인코딩 과정

<그림 2>에서 제안된 알고리즘의 인코딩 과정을 표현하였다. 삽입 시점을 이용한 잠재적 삽입 블록을 선택하고, 비밀 메시지의 비트 재배열과 암호화를 기반으로 하여 혼합 단계를 거쳐 신뢰하는 수신자에게 전달되는 과정을 표시하였다.

3.1.2 Decoding

기본적인 디코딩 단계는 다음과 같다.

1단계 : 신뢰되고 인증된 수신자가 받은 스테고 신호($S_l(m)$)와 스테고 키, 삽입 위치(t_{Begin}) 등의 정보를 획득한다.

2단계 : $S_l(m)$는 바이트 형태로 스테고 오디오 파일을 받아서 비트의 바이너리 시퀀스 로 변환한다. 즉 양자화 기법을 이용하여 비트 패턴으로 변환한다.

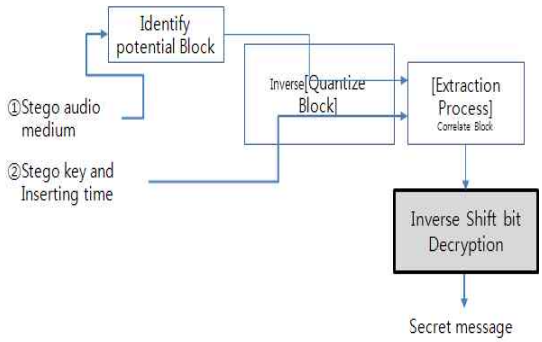
3단계 : 스테고 신호의 바이너리 시퀀스를 검사한 후 삽입 위치를 참고하여, 삽입 블록에서 LSB의 메시지 비트를 추출하는 작업을 한다.

4단계 : 추출된 비트를 8개씩 누적화한 후 <그림1>을 참고하여 비트를 역으로 재배별 한다. 여기에서 계산한 값을 이용하여 숨겨진 메시지를 복원하는 작업을 한다.

5단계 : 2단계부터 4단계를 반복 작업한다.

$$Receives\{S(m), t_{Begin}, E_{S\,key}\}$$
$$Find\ (potential\ embedding\ block)\,|t_{Begin}$$
$$\{S_l(m)_{Decryption} \rightarrow E_i(n)\}_{decoding} \rightarrow T_i(n)$$

<그림 3>에서 디코딩(복호화) 과정을 표시하였다. <그림 3>과 <그림 4>에서 진하게 표시된 영역은 논문에서 제안한 부분이다.



<Fig3> 제안된 알고리즘에서에서의 디코딩 과정

오디오 품질은 커버 오디오 파일의 크기에 의존하며, LSB 코딩을 이용할 경우 비밀 메시지가 포함된 스테고 오디오 파일의 크기와는 차이가 없어야 한다. 또한 제안된 방법의 성능을 확인하기위해 RMSE(root mean square error), SNR, PSNR(peak SNR) 등을 살펴본다. 즉 신호와 잡음신호의 비율을 정량적으로 나타내기 위한 지표로서 사용되는 신호 대 잡음비는 (3) 식으로 계산할 수 있다[7][8].

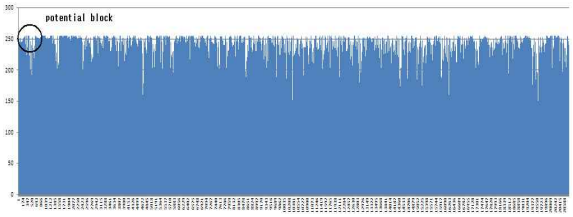
$$SNR = 10 \cdot \log_{10} \frac{\sum_{i}^{p} stego(i)^2}{\sum_{i=1}^{p} |cover(i) - stego(i)|^2} \quad (3)$$

여기에서 $cover(i)$와 $stego(i)$는 i번째 커버 및 스테고 매체의 신호 수준값을 각각 나타낸다. p는 오디오 표본의 수를 나타낸다. SNR의 값이 감소한다는 것은 정보가 잡음으로 인해 손실될 수 있다는 특성을 가지고 은닉 메시지의 존재 가능성을 확인할 수 있다. 수치값이 클수록 잡음보다 신호 크기가 커서 깨끗한 음을 재생할 수 있으며, 비밀 메시지 삽입으로 인한 왜곡이 미세하다는 의미이다. 일반적인 자료일 때 SNR 값이 15, 오디오일 경우 40이상이면 양호한 수준 즉, 커버와 스테고 매체 사이에 청각적인 차이가 없는 것으로 판단할 수 있다.

3.2 적용 및 결과

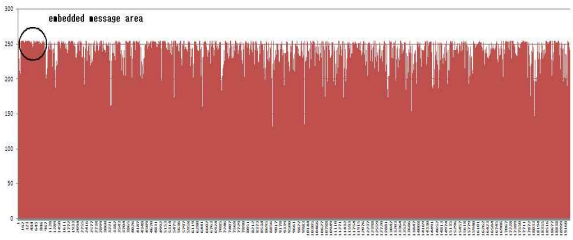
여기에서 사용된 오디오 파일은 60Kbyte, 10sec 이상 동작되는 웨이브 파일(.wav)로 제한한다. 그리고 비밀 메시지의 길이는 N자 이내로 제한한다. 알고리즘을 구현하는 과정은 J 2SE와 MatLab을 이용하였다. 여기에서는 비밀 메시지를 커버 오디오 파일의 초반부에 삽입하였다.

- 커버 오디오 파일(LoopyMusic.wav, 8bit file)
- 940,794Byte(작동시간 10sec)
- 비밀 메시지(1,088Byte(980자))
- 삽입 위치(1ms)/스테고 키(34)



<Fig 4> 비밀 메시지가 삽입되기 전의 커버 오디오 신호(값)

<그림 4>과 <그림 5>는 커버 오디오 파일에 비밀 메시지가 삽입되기 전과 후의 상태를 표시하였다. <그림 5>에서 원형의 점선 표시는 비밀 메시지가 삽입된 영역을 의미한다. <표 1>에서 커버 오디오 파일과 스



<Fig 5> 비밀 메시지가 삽입된 후의 스테그 오디오 신호(값)

테고 오디오 매체의 크기와 각각의 인코딩 및 디코딩 시간을 보여준다. 비밀 메시지 삽입 전과 후에 오디오 파일의 크기는 차이가 없음을 확인하였다. 또한 인코딩보다는 디코딩 소요시간이 5-10%정도 크다는 것을 확인하였다. <그림 1>에서와 같이 오디오 스테가노그래피에서 비밀 메시지의 비트 재배열로 인한 적절한 애매 모호성이 추가되고, 암호화가 이루어 질 경우 내·외부적 및 이상적 요인에 의한 정보유출 가능성을 최소로 억제할 수 있다.

<Table 1> 인코딩/디코딩 시간과 파일크기 변화

구분	시간(ms)	파일크기
인코딩	2,328	변화없음
디코딩	2,454	변화없음

<표 2>에서는 커버 매체에 비밀 메시지가 삽입될 때 SNR 값을 보여준다. 표에서와 같이 SNR 값은 49.28이며, PSNR은 87.9로 충분히 크다. 따라서 왜곡된 정보가 존재하지 않는다라고 판단할 만큼 매우 양호한 수준이라고 결론지을 수 있다. 즉 오디오를 이용한 비밀 메시지 삽입 기법에서 왜곡된 정보의 존재를 판단할 수 없으므로 제안된 방법이 효율적인 은닉정보 전달 수단임을 확인할 수 있다. 또한 같은 조건에서 이미지에 비밀자료를 삽입할 경우[9]보다 SNR 값이 높다는 것을 확인하였다.

<Table 2> 커버 매체에 비밀 메시지가 삽입될 때 SNR값

구분	자료크기	RMSE	SNR	quality
Audio1	1,088	0.94	48.39	> 40
Audio2	1,088	0.76	49.28	
Image	1,088	-	42.00	> 32

결론적으로 공격자는 비밀 메시지가 삽입된 오디오

파일을 감지하기가 어려울 뿐만 아니라, 의심되는 스테고 오디오 파일을 찾아냈을 경우에도 은닉메시지를 추출하는데 무거운 부담을 줄 수 있다. 즉 공격자가 비밀메시지를 파악하기가 불가능에 가깝다고 볼 수 있다.

4. 결 론

스테가노그래피를 적용할 때 암호화를 보완하는 것과 더불어 비밀 메시지가 삽입되었다는 흔적을 없애는 것이 중요하다. 커버 오디오 파일에 비밀 메시지가 삽입된 인코딩 전 후의 파일의 크기에 변화가 없으며, 인코딩 및 디코딩 시간이 매우 짧다는 것을 확인하였다. 오디오 스테가노그래피에 비밀 메시지를 삽입할 경우, SNR 값을 비교하면, 왜곡의 정도가 매우 양호함을 확인하였다. 커버 매체와 스테고 매체의 차이가 없다고 판단할 수 있다. 따라서 비트화 된 비밀 메시지의 비트별 위치를 바꾸고, 암호화 과정을 추가함으로서 공격자에게 정보은닉 존재 유무의 애매 모호성과 해독의 어려움을 동시에 부여하여 할 수 있다.

참 고 문 헌

[1] H. B. Kekre, A. Athawale, S. Rao and Uttara Athawale, "Information Hiding in Audio Signals", International Journal of Computer Applications, Vol. 7. No. 9, pp. 14-19, October 2010.

[2] 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.

[3] K. Geetha and P. Vanitha Muthu, "Implementation of ETAS(Embedding Text in Audio Signal) Model to Ensure Secrecy", International Journal on Computer Science and Engineering, Vol. 2, No. 4, pp. 1308-1313, 2010.

[4] 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.

[5] 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, January 2012.

[6] F. Djebbar, B. Ayady, H. Hamamz and K. Abed-Meraim, "A view on latest audio steganography techniques", Innovations in Information Technology, 2011 International Conference, pp. 409-414, 2011.

[7] H. Shahadi1 and R. Jidin. "High Capacity and Resistance to Additive Noise Audio Steganography Algorithm", International Journal of Computer Science Issues, Vol. 8, No. 2, pp. 176-184, 2011.

[8] L. A. Jorj, H. H. Saleh and N. F. Hassan, "Data Hiding in Audio File by Modulating Amplitude", Eng. & Tech. Journal, Vol. 28, No. 5, pp. 941-952, 2010.

[9] S. S. Ji, "Locating and Searching Hidden Messages in Stego-Images", KIISC, Vol. 14, No. 3, pp. 37-43, 2009.

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 : 2012년 08월 02일
1차수정완료일 : 2012년 08월 28일
2차수정완료일 : 2012년 09월 06일
게 재 확 정 일 : 2012년 09월 19일