1999년도 대한전기학회 정기총회 및 추계학술대회 논문집 1999. 11. 20

대역 스크램블을 이용한 음성 보호방식

지형근* 이동욱
동국대학교 전기공학과

Speech Encryption Scheme Using Frequency Band Scrambling

Hyung-Kun Ji*, Dong-Wook Lee
Dongguk University

Abstract - The protection of data which we want to keep secret from invalid users has become a main topic nowadays. This paper introduces a encryption scheme for protecting speech signals from eavesdropping. The proposed encryption scheme adopts a secure voice cryptographic algorithm based on the scrambling in frequency band. In order to improve the conventional speech signal encryption scheme, we have randomly permuted DCT coefficients of speech signal. Simulation results are included to show the performance of the proposed algorithm for secure transmission of speech signals.

1. 서 론

최근 들어 우리가 서로 교류하는 정보의 형태가 대단히 다양하게 되었다. 그에 따라 컴퓨터를 이용한 정보처리영역도 기존의 문자정보 이외에 영상, 음향 등의 여러 감각매체를 대상으로 확대된 지 이미 오래다. 현대의 다매체 시대를 맞이하여 컴퓨터 정보처리의 기술개발로 인해 매체정보의 안전 및 효과적인 보안에 대한 필요성이 요구되고 있다. 이러한 필요성은 정보의 보안이란 문제를 대두시키고 정보보안을 위해 암호체계, 또는 정보보호 시스템을 이용하여 정보를 보호하고 있다. 정보보안 체계는 암호 알고리즘을 이용하여 구현되는데, 암호 알고리즘이란 자신의 데이터를 허가 받지 않은 사용자로부터 안전하게 보호하기 위해서 사용하는 기법으로 수학적 혹은 확률적인 이론에 그 기반을 둔다. 즉, 누구나 쉽게 알아볼 수 있는 형태의 데이터(예를 들면, 텍스트, 이미지, 사운드) 등의 평문(Plain Text)을 다른 사람이 알아볼 수 없는 형태의 데이터(Cipher Text)로 변형함으로써 이를 해독할 수 없는 사용자는 이 데이터로부터 어떠한 정보도 얻지 못하게 하는 기법을 말한다. 이러한 형태의 데이터 변형은 "키(Key)" 라고 하는 특별한 자료 구조에 의존한다. 다시 말하면 데이터를 변형 하는데 사용되는 변형 규칙이나 순서 혹은 알고리즘에 적용되는 임의의 키 값에 의해 사용자마다 서로 다른 암호화된 데이터를 생성하게 된다. 따라서 자신의 키를 안전하게 보호하는 것은 암호 알고리즘 사용에 있어서 가장 기본적인 사항이다. 현재 암호시스템은 크게 대칭 암호계와 비대칭 암호계로 분류된다. 이 두 암호를 살펴보면, 대칭 암호시스템을 대표하는 알고리즘은 DES로 알려져 있고, 비대칭 암호시스템을 대표하는 알고리즘은 RSA로 알려져 있다. 이 알고리즘들은 키 값을 기반으로 하여 데이터를 암호화한다. 그 밖에도 키 값을 기반으로 하는 난수 형태의 암호화 방법은 스트림을 이용방법과 스크램블을 이용하는 방법 또는 대역필터를 이용한 크기변환 등 여러 가지 방법들이 있다. 이 방법들 중 몇 가지 방법을 살펴보면, 스트림을 이용하는 방법은 난수 알고리즘에 의한 난수와 데이터를 XOR 하는 방법을 사용하여 입력 대이터를 암호화한다. 스크램블을 이용하는 방법은 일정 전치행렬을 사용하여 일정 단위 데이터의 위치 전치를 통하여 입력 데이터을 암호화한다. 주파수영역에서의 대역필터를 이용하는 방법은 주파수 대역을 분할하여 각각의 대역의 시간영역의 크기를 바꾸어 입력 데이터를 암호화한다. 이 방법들과 달리 여기서 제안된 방법은 주파수 영역에 데이터를 이용한 방법으로 난수발생에 따르는 주파수의 대역을 전치 하여 입력 데이터를 암호 데이터로 만드는 방법을 제시한다. 응용에는 음성의 보안에 필요로 하는 비화기 및 음성정보의 내용을 보호하는 목적으로 이용하는 곳에 사용할 수 있다. 정보에 중요성이 날로 강조되는 시점있어서, 이 논문이 제안한 방법은 정보를 보호 하는 한 가지 방법을 제시하였다.이 분야의 연구는 앞으로도 필요성이 요구되며 더욱 발전할 것이다.

2. 대역 스크램블을 이용한 음성보호 알고리즘

음성신호에 주파수 대역을 일정하게 나누어 난수열에 따라 연속적인 전치를 통해 그 대역을 스크램블 하게된다. 여기서 제안하는 방법은 주파수 대역에 모든 데이터들을 같은 위치에 전치 하는 것이 아니라 난수열에 변화에 따라 그 위치가 바꾸어지는 알고리즘을 제안했다.

2.1 시스템 모델

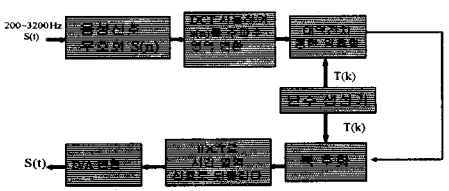

그림 2.1시스템 모델

S(t): 200 Hz ~ 3200 Hz 의 음성신호
T(k): 초기 키 값k에 따라 난수 발생
DCT: 불연속 코사인변환

음성신호 s(t)를 A/D 변환하면 부호화한 음성신호 S(n)된다. S(n) 신호들을 DCT(불연속 코사인 변환) 변환하여 주파수 대역에 정보들로 바꾸어 주면 이 정보들은 난수발생기에 발생한 난수의 불규칙한 순서대로 전치 한다. 이 과정이 대역 전치를 통해 음성신호를 보호하는 방법이다. 다시 원래의 신호들로 복원하려면, 암호를 푸는 쪽에서 같은 난수를 발생하여 전치 한 위치에 있는 데이터들을 본래의 위치로 역전치하여 주파수영역 안에 원래의 데이터 신호를 얻는다.

2.2 음성 스크램블 알고리즘

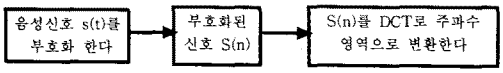

그림 2.2 음성신호의 DCT변환

그림 2.2에 음성신호 변환을 수식으로 표현하면, 음성신호 s(t)가 샘플링 과정을 거치면 식(1)과 같다.

$$S(n) = s(k\,T_s) \tag{1}$$

식(1)은 식(2)의 DCT변환 정의 식에 $x(n)$에 대입된다.

$k=1,\ldots,N$ 에서

$$y(k) = \sum_{n=1}^{N} w(n)x(n)\cos\frac{\pi(2n-1)(k-1)}{2N} \tag{2}$$

$w(n)$은 $\quad 2\le n\le N, \quad w(n)=\sqrt{\frac{2}{N}}$

$\qquad\qquad n=1, \quad w(n)=\frac{1}{\sqrt{N}}$ 이다.

w(n)은 DCT 변환의 계수 부분이다.

$k=1,\ldots,N$에서

$$y(k) = \sum_{n=1}^{N} w(n)S(n)\cos\frac{\pi(2n-1)(k-1)}{2N} \tag{3}$$

식(1)을 수식(2)에 대입하여 식(3)으로 표현한다. 주파수영역으로 변환된 신호 $y(k)$는 각각의 일정 개수 의 대역들로 나누어진다.

$$y(k) = y_1(k_1) + y_2(k_2) + \ldots \\ \ldots\ y_{n-1}(k_{n-1}) + y_n(k_n) \tag{4}$$

각각의 나누어진 대역들은 난수 생성기의 난수들에 의해 대역 순서를 전치 하는데 만약 N개의 대역으로 나누어진다면 난수 발생기의 조건은 N개의 난수를 중복되지 않게 발생해야한다. 또한 연속된 $y(k)$가 들어 올 때마다 난수 발생기는 다시 새로운 난수를 발생해야 한다.

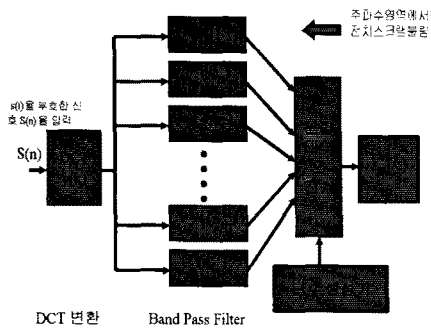

그림 2.3 음성 스크램블 알고리즘

$y(k)$는 전치 되어 Y_T로 변환 할 때 데이터들의 손실 없이 단지 위치에 변화만 가져야 한다. 그림2.3은 음성을 전치 스크램블 하는 과정을 나타내는 그림이다.

2.3 난수 발생기

-난수 발생기의 조건
:주파수 영역을 N개의대역으로 나누었다면 이 대역을 전치하기 위해 $1\sim N$ 번째의 난수를 발생하되 중복이 없어야 한다.

-난수 연산의 기본 수식
:mod 연산을 기본으로 한다

$$NK(k) = \mathrm{mod}(c + K_k, N) + 1 \tag{5}$$

$C = C+1$
N: 분리된 대역의 개수
K_k: 초기 값 (키 값)
C: 난수 발생 카운터

-난수 발생기의 key

난수발생기의 기본 입력 key는 N! 이다. N은 대역의 개수를 나타내고 있으며 중복되지 않게 1에서 N까지에 일련 된 수를 나열하는 경우의 수에 대한 가지 수를 갖는다. C는 카운트를 나타내는 최종 값 또한 키에 한 형태로 사용 할 수 있다. 그림 2.4는 식(5)을 수행하는 알고리즘의 순서도를 표현한 그림이다.

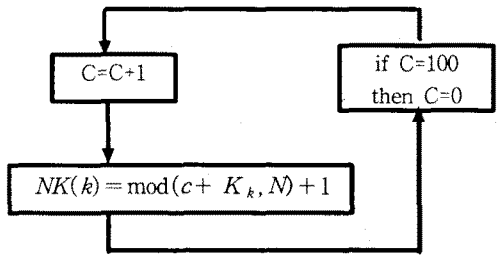

그림2,4 난수 발생알고리즘

2.4 음성 역 스크램블 알고리즘

$Y_T(k)$을 각각 N 개로 나누어 다음 난수 생성기에 난수 발생순서대로 역전치 한다. 역전치 한 $Y(k)$는 IDCT 변환하기 위해 (6)식을 대입한 결과인 (7)식에 연산을 수행한다.

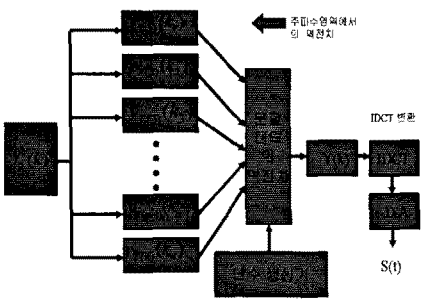

그림2.5 역 스크램블 알고리즘

그림 2.5에 역 스크램블 알고리즘의 과정을 간단히 수식으로 표현하면

$$Y_T(k) = y_1(k_1) + y_2(k_2) + \ldots + y_{n-1}(k_{n-1}) + y_n(k_n) \quad (6)$$

식(6)을 불연속 코사인 변환표현식(7)에 대입하여 음성부호 신호 $s(n)$을 얻는다.

$$k = 1, \ldots, N$$

$$x(n) = \sum_{n=1}^{N} w(n) Y(k) \cos \frac{\pi(2n-1)(k-1)}{2N} \quad (7)$$

$w(n)$가 $2 \le n \le N$ 인 경우 $w(n) = \sqrt{\frac{2}{N}}$

$n = 1$인 경우 $w(n) = \frac{1}{\sqrt{N}}$

$x(n) = s(n)$와 같다. $s(n)$의 신호를 D/A변환하여 원 음성신호를 얻어 본래의 음성을 복원 할 수 있다.

3. 음성 스크램블 알고리즘 실험

실험은 MATLAB을 이용하였다. "지금 편지가 왔습니다"라는 3.6초 정도에 음성 wave 파일을 사용해 제안한 알고리즘을 실험하였다. 약 8만개에 부호 화된 음성신호 중 100개를 한 개의 프레임으로 정한 후 DCT변환된 한 프레임을 10개의 대역으로 나누어 전치 하였다. 난수 발생조건은 C=100에서 "0"으로 초기화한다. 즉 8만 개의 음성 data중 800번 초기화를 한다.

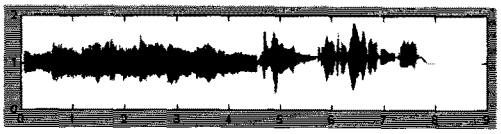

그림 3.1 입력 음성 파형

그림 3.1은 "지금 편지가 왔습니다"라는 3.6초 정도의 음성 wave파일에 파형을 나타내고 있다. 다음 그림 3.2는 그림 3.1에 음성 파형을 제안한 알고리즘에 넣어 실험한 결과부터 얻어진 음성 파형에 그림이다.

그림 3.2 스크램블된 음성 파형

주파수가 아주 불규칙한 형태의 파형을 나타내고 있음을 알 수 있다. 실제 음성을 들어보면 심한 노이즈가 섞여 쉽게 식별 할 수 없는 형태의 음성이 된다. 스크램블한 음성을 복원하는 알고리즘은 2.4절에 있는 역 스크램블 알고리즘과 동일한 절차를 수행한다. 다만 난수 발생기는 스크램블에 사용된 난수발생기와 동일한 키 그리고 역 스크램블 알고리즘으로 역전치를 수행한다. 복호화도 100개씩을 한 프레임으로 하여 역전치 한다. 이러게 하면 그림 3.3과 같은 복호화한 음성신호를 볼 수 있다. 원 음성신호와 동일한 음성 파형임을 확인 할 수 있다. 복원된 음성신호를 들었을 때, 원 음성신호와 거의 차이를 느낄 수 없었다.

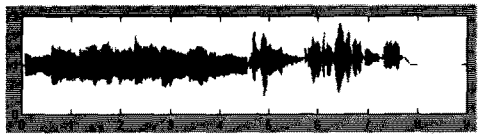

그림 3.3 역 스크램블된 음성 파형

4.결 론

음성신호를 보호하는 목적으로 제안한 알고리즘은 실험을 통해 몇 가지 사실들을 알 수 있었다. 먼저 첫째로 외부로부터 역 스크램블을 통하지 않고는 음성을 식별할 수 없다는 것이며, 기존방법과 달리 프레임마다 전치 위치가 다르다는 것이다. 둘째로 난수 발생기에 키의 개수들은 음성 정보를 보호하는데 충분한 크기를 가지고 있으며, 주파수 대역에서 전치가 이루어지는 스크램블에 잘못된 복원을 시도한다면 주파수 영역에 정보들은 손상되어 식별 할 수 없는 음성신호들이 된다. 셋째로는 본 논문에서 제안한 난수 발생 알고리즘은 기존 방법들과 다르게 각각의 프레임마다 난수가 발생하는 경우이며, 실험에서 원 음성신호에 스크램블한 신호는 주파수가 불규칙한 형태를 이루고 있음을 확인 할 수 있었다. 실제로 음성을 식별하기에 어려움이 있음을 확인 할 수 있었다. 넷째로 역 스크램블한 음성신호는 원래의 음성신호와 거의 일치하는 것을 볼 수 있었다. 또한 원 음성과 거의 같은 음색과 음량을 가지고 복원된 것도 확인 할 수 있었다. 이와 같은 몇 가지 결과들은 더 많은 응용분야에 이용할 수 있으며, 본 논문에서 제안 한 방법은 음성 비화기 및 정보데이터들을 보호하는 수단으로 사용되어질 수 있다. 오늘날 정보 보안이 더욱더 중요시되는 시점에서 정보를 보호할 수 있는 연구가 더욱 많이 진행되고 앞으로도 더 발전하리라 생각한다.

[참 고 문 헌]

[1] Vladimir Milosevic, Vlado Delic,Vojin Senk, "Hadamard transform application in Speech srcrambling", Proc. IEEE Conf. Digital Signal Processing, pp 361- 364, 1997

[2] 정지원, 이경호, 원동호 "동기 문제 해결을 위한 호핑 필터를 이용한 음성 보호 방식의 최적화에 관한 연구", 한국통신학회논문집, pp 1666-1687, 1994

[3] 하재철, 박영호, "디지탈 음성보호 시스템의 구현", 통신 신호처리합동학술대회, pp 54-57, 1993

[4] 최진택, 송재영, "스트림 암호에서 개선된 알고리즘을 이용한 암호 키 발생 방법", 한국통신학회논문집, pp 604-611,1989

[5] 이민섭, "현대 암호학", 교우 출판사, 1999

[6] Gordon E. Carlson, "Singnal and Linear System Analysis", John Wiley & Sons Inc,1998

[7] Udo Zolzer "Digital Audio Signal Processing", John Wiley & Sons Inc,1995