論 文

동기 문제 해결을 위한 호핑 필터를 이용한 음성 보호 방식의 최적화에 관한 연구

正會員 鄭 智 元* 正會員 李 庚 鎬* 正會員 元 東 豪*

A Study on Optimization of Speech Encryption Scheme using Hopping Filter in order to Solve the Synchronization Problem

Ji Won Chung*, Kyoung Ho Lee*, Dong Ho Won* *Regular Members*

要 約

호핑 필터를 이용한 이차원 진폭 스크램블링 알고리즘은 기존의 음성 보호 방식의 단점을 개선시킬 수 있는 아날로그 음성 신호에 있어서 강력한 보호 방식이다.

본 논문에서는 이차원 진폭 스크램블링 알고리즘의 최대 단점인 동기 문제를 해결하기 위하여 variable delay를 이용한 알고리즘을 제안하였다. 또한 PAM 신호를 가우시안 잡음이 존재하는 채널로 전송하였을 때 수신단에서는 복원된 음성 신호의 왜곡을 분석함으로써 최적의 보호 알고리즘 및 최적의 SNR 값을 시뮬레이션을 이용하여 나타내었다.

ABSTRACT

Two dimensional amplitude scrambling algorithm using the hopping filter, which improve the drawback of conventional speech encryption scheme, is powerful encryption scheme in analog sppech signal.

In this paper, we proposed the variable delay weight algorithm using hopping filter in order to solve the synchronization problem of two dimensional amplitude scrambling. Futhermore, analyzing the distortion of received signal which is transmitted in the gaussian noise channel, we determined the optimal encryption algorithm and optimal SNR using the simulation.

I. 서 론

유선 및 무선 통신망이 널리 보급되기 시작한 20세기 초부터 인가받지 않은 제3자로부터 음성 신호를 보호하기 위한 비화 방식의 필요성이 크게 인식되기 시작하였다.

20세기 초와는 달리 현대에 이르러서는 정보화 사회의 성숙과 더불어 중요 정보의 음성 대역급 통신망

*成均館大學校 情報工學科
Dept. of Infor. Eng., Sungkyunkwan Univ.
論文番號 : 93-170

을 이용한 전송이 널리 사용됨에 따라 새로운 음성용 비화 방식의 개발 필요성이 점점 증가하고 있는 추세이다.

음성 정보의 보호 방식에는 크게 비화되는 최소 단위에 따라 암호화와 스크램블링으로 구분된다. 암호화는 비트 단위의 입력 신호를 난수 생성기에 의해 생성되는 비트와 XOR 하는 방식으로 디지탈 신호에 주로 적용되며 스크램블링은 신호를 2 비트 이상으로 요소로 분리하여 각 요소가 난수 생성기에서 생성된 비트 값에 의해 변환 또는 재 배열되는 것으로 주로 아날로그 신호에 적용된다. 기존의 스크램블링 방식에는 음성 비화가 적용되는 영역에 따라 주파수 대을 분리하여 치환하는 주파수 영역 스크램블링 방식과 시간 영역에서 샘플링 순서를 치환하는 시간 영역 스크램블링 방식, 그리고 시간 영역 스크램블링과 주파수 영역 스크램블링을 결합시킨 혼합 방식이 있다[1]. 시간 영역 스크램블링 방식과 주파수 영역 스크램블링 방식을 1차원 스크램블링 알고리즘(1 dimensional scrambling algorithm)이라 하고 혼합 방식을 2차원 스크램블링 알고리즘(2 dimensional scrambling algorithm)이라 한다.

아날로그 신호의 초기 비화 방식은 비도가 상당히 낮은 주파수 영역 스크램블링 위주로 발전되어 왔으나, 현재의 추세는 일정한 시간 길이를 갖는 시간 요소(time segment)로 분리한 후 이들을 직접히 재배열하는 시간 영역 스크램블링을 주로 사용하고 있는 추세이다. 이는 현재 기술 수준으로 실현이 용이하고 비교적 높은 비도를 얻을 수 있다는 장점이 있어 상용화된 음성 비화용 장비를 주종을 이루고 있다.

그러나 기존의 방식은 키 수가 제한되어 있으며, 주파수 영역에서 음성의 잔여 이해도(residual intelligibility) 때문에 제3자가 상관 관계를 이용하여 공격할 수 있다는 문제와 시간 영역에서 송·수신간에 동기를 맞추는 문제가 가장 어려운 문제로 남아있다[2,3]. 이러한 문제점을 해결하기 위해 본문 [5]에서 호핑 필터를 이용한 이차원 전폭 스크램블링을 제안하였다. 이는 시간 영역과 주파수 영역에서 전폭을 스크램블링하여 상관 계수를 0으로 함으로써 음성의 잔여 이해도를 완전히 없애 제3자의 해독이라는 기존의 방식의 문제점을 개선시킬 수 있다. 아울러 난수 생성기에서 생성되는 키의 수를 확장시킴으로써 기존의 방식보다 비도를 더 증가시킬 수 있다는 장점을 갖고 있다. 그러나 비도가 높다는 장점 대신 이 알고리즘 역시 송·수신간에 동기를 맞추기 어렵다는 문제점을 안고 있다. 따라서 본 논문에서는 동기 문제를 해결하기 위하여 시간 영역의 난수 생성기에 출력된 키 값을 이용한 variable delay weight 알고리즘을 제안하였다. 또한, 본 논문에서는 음성 압축 방식으로 PARCOR 격자형 필터와 상관기를 이용하여 상관 계수와 잔차 신호를 생성하는 PARCOR 방식을 적용하였으며, 압축된 신호를 채널로 전송할 때 발생되는 에러를 정정하기 위해 기존의 convolutional 코딩 및 BCH 코딩보다 성능이 우수한 trellis 코딩을 채널 코딩으로 적용하였다. 부호화된 비트를 펄스 진폭 변조시켜 가우시안 잡음 채널로 송신하였을 때, 수신단에서는 송신단의 역 과정을 하여 복원된 음성 신호와 원 음성 신호의 차이인 왜곡을 분석함으로써 호핑 윈도우를 이용한 이차원 전폭 스크램블링 알고리즘인 전폭 가산 알고리즘과 전폭 승산 알고리즘 그리고 동기 문제를 해결하기 위해 제안한 variable delay weight 알고리즘의 성능을 분석하고 최적의 SNR 및 최적의 상관 계수의 차수를 시뮬레이션을 이용하여 나타내었다.

II. 기존 방식 검토

기존의 음성 비화 방식은 주파수 영역 스크램블링, 시간 영역 스크램블링, 그리고 혼합방식이 주종을 이루고 있다. 주파수 영역 스크램블링 방식에는 음성 반전(speech inverter)방식과 대역 천이 반전(band shift inverter)방식 그리고 대역 분리(band splitter) 방식이 있다. 음성 반전 방식은 가장 간단한 방식으로 대역이 제한된 음성을 주파수 영역에서 반전시키는 방식으로 실제가 용이하고 복원된 음질은 좋으나 한 개의 키만을 사용하므로 비도가 매우 낮다. 대역 천이 반전 방식은 음성 신호를 다른 주파수 영역으로 천이시키고 음성 대역을 넘어서는 고주파 성분을 저주파 쪽으로 이동시키는 방식이다. 이 방식 또한 키 수의 제한과 음성의 잔여 이해도가 높다. 대역 분리 방식은 음성 스펙트럼을 몇 개의 부대역(subband)으로 나눈 뒤 부대역들의 순서를 재배열하는 방식으로 음성 에너지와 주파수와의 관련성 때문에 해독이 용이하다. 주파수 영역 스크램블링 방식은 구현은 쉬우나 음성 보호 측면에서 치명적인 단점을 가지고 있다. 이러한 단점을 어느 정도 보완할 수 있는 시간 영역 스크램블링 방식에는 시간 성분 반전(reversed time segment)방식과 호핑 윈도우(hopping window) 방식이 있다. 시간 성분 반전 방식은 아날로그 신호

를 A/D 변환기를 거쳐 디지탈 신호로 변환한 후 몇 개의 샘플로 구성된 시간 성분으로 나누어 각 성분들에게 샘플 순서를 역으로 하여 D/A 변환하는 방식으로 음성의 잔여 이해도는 낮으나 비도가 낮고 송·수신간에 동기를 필요로 한다. 호핑 윈도우 방식은 블럭 시간 성분 치환 방식이라고 하며, 각 프레임내에서 치환의 순서에 따라 성분들을 전송하고 수신측에서는 역 치환을 함으로써 원래 신호를 복원할 수 있다. 시간 성분 경계면 사이의 갑작스러운 변화로 고주파 성분이 발생하여 음질의 저하를 초래한다. 시간 영역 스크램블링 방식은 주파수 영역 스크램블링 방식보다 비도가 높고 키 수가 확장되나 음질의 저하 및 송·수신간에 동기를 필요로 하는 단점이 있다. 위의 두 방식의 장·단점을 서로 절충하는 혼합 방식은 시간 영역 스크램블링과 주파수 영역 스크램블링을 결합시켜 비도를 높이고 키 수를 확장할 수 있다. 그러나 다른 방식과 마찬가지로 동기를 맞추는 문제가 여전히 남아있다.

이상에서 살펴본 기존의 방식은 다음과 같은 세가지 문제점을 가지고 있다.

① 음성의 잔여 이해도 때문에 제3자의 해독이 용이하다.

② 이용 가능한 주파수 대역이 제한되어 있으므로 사용할 수 있는 키 수가 제한된다.

③ 시간 영역 스크램블링에서 송·수신간에 동기를 맞추기 어렵다.

①, ②의 문제점은 음성의 비도 측면에서 치명적인 문제점이 되고, ③의 문제점은 하드웨어 측면에서 구현에 어려움이 있다. ①, ②의 문제점을 효율적으로 해결할 수 있는 방식이 호핑 필터를 이용한 이차원 진폭 스크램블링 알고리즘이다.

Ⅲ. 시스템 모델

본 논문의 전체 시스템 모델은 그림1과 같다. 200Hz ~3200Hz의 음성 신호 m(t)는 이차원 진폭 스크램블링 알고리즘에 의해 키 생성기에서 생성된 키 K에 따라 암호화된 음성 신호 s(t)로 된다. 채널의 대역폭을 효율적으로 이용하기 위해 암호화된 음성 신호 s(t)를 PARCOR 격자형 필터와 상관기를 이용하여 상관 계수와 잔차 신호를 생성하는 PARCOR 방식으로 음성을 압축한다.

압축된 신호를 채널로 전송할 때 발생되는 에러를 정정하기 위해 trellis 코딩을 한후 펄스 진폭 변조시켜 가우시안 잡음 채널로 송신하였을 때, 수신단에서는 송신단의 역 과정을 하여 복원된 음성 신호 $\hat{m}(t)$를 출력한다. 그림1의 전체 시스템 모델에서 각 블럭별로 상세한 설명은 다음 각 절에서 하겠다.

3.1 호핑 필터를 이용한 이차원 진폭 스크램블링 알고리즘

호핑 필터를 이용한 이차원 진폭 스트램블링은 기존의 비화 방식에 비해 비도를 높이고 음성의 잔여 이해도를 줄일 수 있기 때문에 효율적인 아날로그 음성 보호 방식이다. 호핑 필터를 이용한 일차원 진폭 스크램블링의 블럭도는 그림2와 같으며, 이는 서로 다른 주파수 대역을 갖고 있는 대역 통과 필터(band pass filter)들과 이득 조절장치, 난수 생성기, 그리고 D/A 변환기로 구성되어 있다.

대역폭이 200Hz~3200Hz인 음성 신호는 서로 다

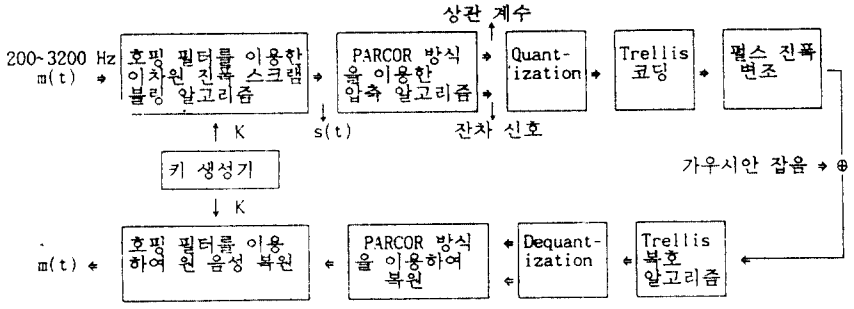


그림 1. 시스템 모델
Fig 1. System model

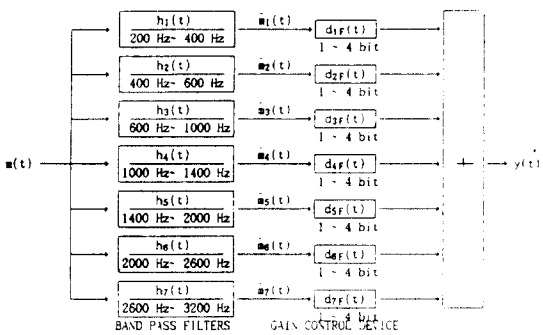
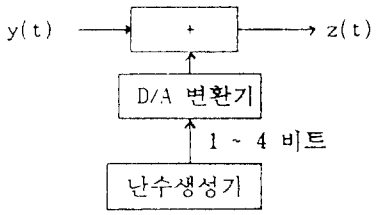


그림 2. 일차원 진폭 스크램블링 알고리즘의 블럭도
Fig 2. Block diagram of one dimensional amplitude scrambling algorithm

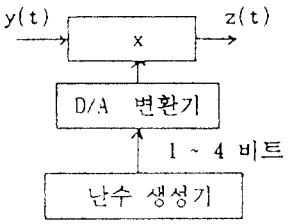
른 대역을 가진 대역 통과 필터를 통과시킨다. 필터를 통과한 주파수 대역의 서로 다른 신호들은 각각 이득 조절 장치(gain control device)에 입력된다. 이득 조절 장치는 각각의 난수 생성기에서 생성된 1~4 비트를 D/A 변환기를 이용하여 아날로그 값으로 변환한 후 이 값을 대역 통과 필터를 통과한 각 신호의 이득과 곱한다. 이는 각각의 주파수 대역에서 이득을 증가 혹은 감소시키며 난수 생성기에서 생성된 비트 값이 암호학적인 측면에서 키로 작용한다. 대역 통과 필터와 이득 조절 장치를 합하여 호핑 필터라고 부른다.

호핑 필터를 통과한 각 신호들은 다시 모두 더해져서 y(t)로 출력 된다. 여기까지의 과정은 주파수 영역에서만 진폭을 스크램블링 하였기 때문에 호핑 필터를 이용한 일차원 진폭 스크램블링이라 한다. 일차원 진폭 스크램블링을 적용시킨 후 다시 시간영역에서 난수 생성기에서 생성된 1~4 비트를 D/A 변환기를 이용하여 아날로그 값으로 변환한 후 y(t)와 더하기나 곱함으로써 다시 한번 시간 영역에서 스크램블링이 된다. 이러한 알고리즘은 시간 영역과 주파수 영역을 모두 스크램블링 하였기 때문에 호핑 필터를 이용한 이차원 진폭 스크램블링이라 한다. 시간 영역에서 y(t)와 더하는 알고리즘을 진폭 가산 스크램블링(Amplitude Addition Scrambling : 이하 AAS)알고리즘이라 하며, 곱하는 알고리즘을 진폭 승산 스크램블링(Amplitude Multiply Scrambling : 이하 AMS) 알고리즘이라 한다. 이 두 알고리즘을 그림3에 나타내었다.

기존의 스크램블링 방식은 대역을 분리하여 치환하기나 샘플링 순서를 치환 하는 방식과는 달리 호핑 필터를 이용한 이차원 진폭 스크램블링 방식은 분리된 대역의 진폭을 스크램블링하고 다시 시간 영역에서의 진폭을 스크램블링함으로써 암호 이해도의 증가, 비도의 감소라는 기존의 스크램블링 방식의 단점을 개선시킬 수 있다.



(a) 진폭 가산 스크램블링 알고리즘



(b) 진폭 승산 스크램블링 알고리즘

그림 3. 이차원 알고리즘
Fig 3. Two dimensional algorithm

그림3에서 200Hz~3200Hz의 주파수 대역을 가진 원래 신호 m(t)가 i개의 대역 통과 필터를 통과한 각 신호를 $\bar{m}_i(t)$라 하면 일차원 알고리즘의 출력 y(t)는 식(1)과 같다.

$$y(t) = \sum_{i=1}^{7} \bar{m}_i(t) \cdot d_{iF}(t) \qquad (1)$$

$d_{iF}(t)$는 시간에 따라 진폭을 변화시키는 함수를 나타내며 식 (2)와 같다. $D_{iF}(k)$는 i개의 난수 생성기에서 생성된 1~4 비트를 D/A 변환기를 이용하여 아날로그로 변환된 값을 나타낸다.

$$d_{iF}(t) = \sum_{k} g_F(t - kT_F) \cdot D_{iF}(k) \qquad (2)$$

단, $0.3125\ \text{ms} \le T_F \le 125\text{ms}$

호핑 필터는 200Hz~3200Hz의 주파수 대역의 신호만 필터링하므로 시간 영역에서의 필터링 시간 T_F는 난수 생성기에서 생성된 1~4 비트를 모두 포함하여 상한선(upper bound)을 1.25ms, 하한선(lower bound)을 0.3125ms로 정한다. 이는 T_F가 0.3125ms와 1.25ms 사이에서만 필터링 하겠다는 의미이다.

$$g_F(t-kT_F)\begin{cases}=1 & \text{if } kT_F \le t \le (k+1)T_F \\ =0 & \text{if otherwise}\end{cases} \quad (3)$$

진폭 가산 스크램블링 알고리즘과 진폭 승산 스크램블링 알고리즘의 출력을 각각 $z_{AAS}(t)$, $z_{AMS}(t)$라 하면 식(4)와 식(5)과 같다.

$$z_{AAS}(t)=y(t)+d_A(t)$$
$$=(\sum_{i=1}^{i=7}\bar{m}_i(t)\cdot d_{iF}(t))+d_A(t) \quad (4)$$

$$z_{AMS}(t)=y(t)\cdot d_A(t)$$
$$=(\sum_{i=1}^{i=7}\bar{m}_i(t)\cdot d_{iF}(t))\cdot d_A(t) \quad (5)$$

$d_A(t)$는 시간 영역에서의 난수 생성기에서 생성된 1~4 비트를 D/A 변환기를 이용하여 아날로그로 변환된 값을 나타낸다. 알고리즘의 키 수는 난수 생성기에서 생성된 비트 수에 의존한다. 일차원 알고리즘의 키 공간은 $2^1 \sim 2^7$이며 이차원 알고리즘의 키 공간은 $2^4 \sim 2^{28}$이다.

3.1.1 비도에 대한 수학적인 분석

아날로그 신호에서 비도가 높다는 의미는 송신단에 입력된 신호와 출력된 신호의 상관이 거의 0에 근접함을 말한다. 이는 난수 생성기에서 출력된 비트 값에 의존한다.

송신단에 입력되는 신호 $m(t)$와 출력 신호 $z(t)$의 상관 계수를 $C_{mz}(\tau)$라 하면 식(6)과 같다.

$$C_{mz}(\tau)=E[m(t)z(t+\tau)]-E[m(t)]E[z(t+\tau)] \quad (6)$$

$z(t+\tau)$는 출력 신호 $z(t)$를 시간 τ 만큼 이동시킨 것이다.

$C_{mz}(\tau)$의 이상적인 값은 0이어야 하며, 이는 출력 신호가 입력 신호의 정보를 갖고 있지 않음을 의미한다. 진폭 가산 알고리즘의 $C_{mz}(\tau)$를 살펴보면 다음과 같다.

$$E[m(t)z(t+\tau)]=E\Big[m(t)\Big(\Big(\sum_{i=1}^{i=7}\bar{m}_i(t+\tau)\cdot d_{iF}(t+\tau)\Big)\Big)+d_A(t+\tau)\Big)\Big]$$
$$=E\Big[\sum_{i=1}^{i=7}m(t)\bar{m}_i(t+\tau)d_{iF}(t+\tau))\Big]+E[m(t)d_A(t+\tau)]$$
$$=\sum_{i=1}^{i=7}E[m(t)\bar{m}_i(t+\tau)d_{iF}(t+\tau)]+E[m(t)d_A(t+\tau)] \quad (7)$$

$d_{iF}(t+\tau)$와 $d_A(t+\tau)$는 $\bar{m}_i(t+\tau)$에 대하여 독립적이기 때문에 식 (7)을 식 (8)과 같이 나타낼 수 있다.

$$E[m(t)z(t+\tau)]=\Big(\sum_{i=1}^{i=7}E[m(t)\bar{m}_i(t+\tau)E[d_{iF}(t+\tau)]\Big)$$
$$+E[m(t)]E[d_A(t+\tau)] \quad (8)$$

진폭 가산 스크램블링의 상관 계수를 구하기 위해 $d_{1F}(t+\tau)$, $d_{2F}(t+\tau)$,...,$d_{7F}(t+\tau)$의 평균을 u_{1F}, u_{2F},..., u_{7F}라 하고, 각 난수 생성기에서 생성된 비트들의 평균값은 같다고 하면, $u_{1F}=u_{2F}=,...,u_{7F}=u_F$이다. $d_A(t+\tau)$의 평균 값이 u_A라 하면 식 (9)와 같다.

$$E[m(t)z(t+\tau)]=u_F\sum_{i=1}^{i=7}E[m(t)\bar{m}_i(t+\tau)]+u_A E[m(t)] \quad (9)$$

식 (6)의 두번째 연산인 $E[m(t)]E[z(t+\tau)]$를 구하면 식 (10)과 같다.

$$E[m(t)]E[z(t+\tau)]=E[m(t)]E\Big[\sum_{i=1}^{i=7}\bar{m}_i(t+\tau)\cdot d_{iF}(t+\tau)+d_A(t+\tau)\Big]$$
$$=E[m(t)]\Big(\sum_{i=1}^{i=7}E[\bar{m}_i(t+\tau)\cdot d_{iF}(t+\tau)]+E[d_A(t+\tau)]\Big)$$
$$=E[m(t)]\Big(\sum_{i=1}^{i=7}E[\bar{m}_i(t+\tau)]E[d_{iF}(t+\tau)]+E[d_A(t+\tau)]\Big)$$
$$=u_F E[m(t)]\sum_{i=1}^{i=7}E[\bar{m}_i(t+\tau)]+u_A E[m(t)]$$
$$=u_F E[m(t)]E\Big[\sum_{i=1}^{i=7}\bar{m}_i(t+\tau)\Big]+u_A E[m(t)] \quad (10)$$

식 (9)에서 식 (10)을 빼면 진폭 가산 스크램블링 알고리즘의 $C_{mz}(\tau)$가 되면 식 (11)과 같다.

$$C_{mz}(\tau)=u_F\Big(E\Big[m(t)\sum_{i=1}^{i=7}\bar{m}_i(t+\tau)\Big]$$
$$-E[m(t)]E\Big[m(t)\sum_{i=1}^{i=7}\bar{m}_i(t+\tau)\Big]\Big) \quad (11)$$

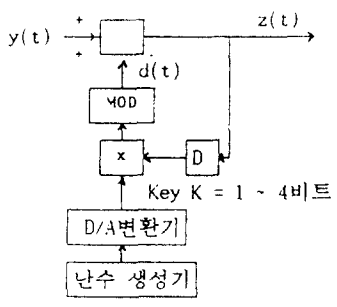
같은 방법으로 진폭 승산 스크램블링 알고리즘의 상관 계수를 구하면 식 (12)와 같다.

$$C_{mz}(\tau) = u_A \cdot u_B \left(E\left[m(t) \sum_{i=1}^{L-1} \bar{m}_i(t+\tau) \right] - E[m(t)]\, E\left[m(t) \sum_{i=1}^{L-1} m_i(t+\tau) \right] \right) \qquad (12)$$

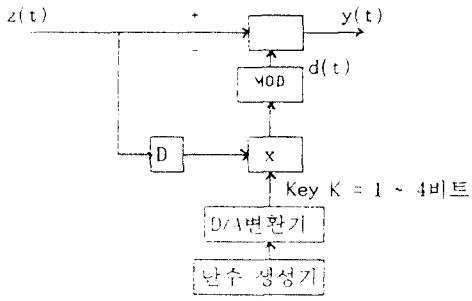
식 (11)과 식 (12)에서 알 수 있듯이 신호의 상관 계수는 난수 생성기에서 생성된 비트들의 평균값 u_A, u_B에 의존함을 알 수 있다. 따라서 신호의 산여 이해도 정도와 비도를 나타내는 상관 계수를 0에 근접하도록 하기 위해서는 비트들의 평균값이 0에 근접하도록 하는 난수 생성기를 선택하여야 한다.

3.2 Variable delay weight 알고리즘

시간 영역 스크램블링의 최대 단점은 송·수신단의 동기를 맞추기 어렵다는 문제이다. 송·수신간에 동기가 맞지 않으면 수신된 신호를 원 신호로 복호할 수 없기 때문에 심각한 문제이다. 호핑 필터를 이용한 이차원 진폭 스크램블링 역시 시간 영역에서 키를 이용하여 진폭을 스크램블링 하기 때문에 동기를 맞추기 어렵다는 단점을 갖고 있다. 이러한 단점을 해결하기 위하여 수신된 신호를 수신단 스스로가 지연시켜 동기를 맞추는 variable delay weight 알고리즘을 제안한다. variable delay weight 알고리즘은 디지탈 신호에서 비트 단위로 데이타를 처리하는 차동 부호기(differential encoder)를 변형한 것으로 여기에 난수 생성기, D/A 변환기, 모듈 연산이 첨가되어 아날로그 신호에서도 수신단 스스로가 동기를 맞출 수 있는 알고리즘이다. 그림9는 variable delay weight 알고리즘의 송·수신단을 나타낸다.



(a) 송신단



(b) 수신단

그림 4. Variable delay weight 알고리즘
Fig 4. Variable delay weight algorithm

그림 4에서 송신 신호 z(t)는 현재 송신기에 입력되는 신호 y(t)와 이전에 입력된 신호 y(t-1)에 난수 생성기에서 생성된 키 값을 곱한 값의 모듈러 연산인 d(t)의 함으로 출력된다. 송신 신호 z(t)는 식(13)과 같다.

$$z(t) = y(t) + d(t) \qquad (13)$$

$$d(t) = k \cdot z(t-1) \pmod{A}$$

A : 신호의 진폭

수신기는 현재 수신단에 입력되는 신호 z(t)와 이전에 입력된 신호 z(t-1)에 난수 생성기에서 생성된 키 값을 곱한 값의 모듈러 연산인 d(t)를 차감함으로써 원래의 신호를 복호한다. 그러므로 수신단에서는 이전에 입력되어진 신호에만 의존하여 원래의 신호를 복호할 수 있기 때문에 수신단 스스로가 자발적으로 동기를 맞춘다. 디지탈 신호에서 한 비트를 지연시켜 송·수신함으로써 수신단 스스로가 동기를 맞추듯이 아날로그 신호에서도 이와 같은 원리를 바탕으로 디지탈 신호에서의 자가 동기 알고리즘을 약간 변형 시켜 동기를 수신단 스스로 맞추게 구성하였다. 식 (14)는 수신단에서 복호된 원래 신호를 나타낸다.

$$y(t) = z(t) - d(t) \qquad (14)$$

$$d(t) = k \cdot z(t-1) \pmod{A}$$

본 논문에서의 위의 송·수신단을 진폭 가산 스크램블링 알고리즘과 진폭 승산 스크램블링 알고리즘 대신 동기를 맞추기 위해 variable delay weight 알고리즘을 제안하였으며 스크램블링된 음성 신호 및 왜

곡에 대한 분석은 IV장에서 언급하였다.

3.3 PARCOR방식을 이용한 음성 압축 알고리즘

본 논문에 적용된 음성 압축 알고리즘은 입력 음성 신호의 스펙트럼 분석과 주기 성분을 제거하기 위해 LPC(Linear Prediction Coding)방식에서 얻어진 예측 신호와 원음성 신호와의 차인 잔차 신호를 부호화하여 전송하는 APC(Adaptive Prediction Coding) 방식과는 달리 순방 예측 신호와 후방 예측 신호를 상관기를 이용하여 사다리꼴 모양으로 필터링함으로써 필터 계수와 잔차 신호를 부호화하여 전송하는 PARCOR방식이다. PARCOR 방식을 이용한 음성 압축 알고리즘은 그림5와 같다.

그림5에서 $f_t^{(p)}$는 t개의 스크램블링된 신호 s_t의 전방 예측 오차이며 $g_t^{(p)}$는 s_t를 1 sample 지연시킨 후방 예측 오차이다. p는 입력 신호가 필터링되는 차수이다.

상관기에서 출력되는 상관 계수 $k_1, k_2, \cdots, k_p$는 자기 상관 계수 R_0와 1 sample 지연시킨 신호의 상관 계수 R_1의 비이다. 상관기에서 출력되는 상관 계수 k_p의 값은 식 (15)와 같다.

$$\begin{aligned} k_1 &= R_1 / R_0 \\ &\vdots \quad \vdots \\ k_p &= R_p / R_{p-1} \end{aligned} \tag{15}$$

상관기에서 출력되는 상관 계수값을 이용하여 전방 예측 오차 $f_t^{(p)}$와 후방 예측 상관기에서 출력되는 상관 계수값을 이용하여 전방 예측 오차 $f_t^{(p)}$와 후방 예측 오차 $g_t^{(p)}$를 구하면 식 (16)과 같다.

$$f_t^{(p)} = f_t^{(p-1)} - k_p \cdot g_t^{(p-1)}$$

$$g_t^{(p)} = g_t^{(p-1)} - k_p \cdot f_t^{(p-1)} \tag{16}$$

스크램블링된 s_t와 필터링 된 신호의 차인 신호 e(i)는 입력된 신호의 갯수인 t개 만큼 계속 반복하여 구한다. 잔차 신호 e(i)는 식 (17)과 같다.

$$e(i) = \sum_{i=1}^{t+1} f_t^{(p)} \tag{17}$$

입력된 샘플 수만큼 계속 반복하여 t개의 잔차 신호와 p개의 상관 계수를 4 비트씩 양자화 하여 trellis 부호기로 보낸다.

본 논문에서는 p를 5, 10, 15로 변화하여 각 알고리즘에 대하여 시뮬레이션을 하였으며 결과는 IV장에 나타내었다.

3.4 Trellis 코딩과 펄스 진폭 변조

양자화된 비트를 채널로 전송할 때 발생되는 에러를 정정하기 위해 기존의 convolutional 코딩 및 BCH 코딩 보다 성능이 우수한 trellis 코딩을 채널 코딩으로 적용하였다. 부호기의 모델은 그림6과 같다.

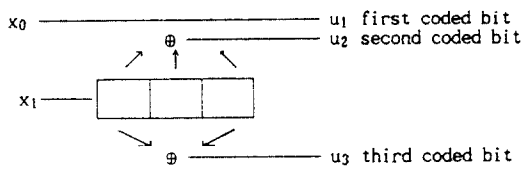


그림 6. 부호기(rate = 2/3)
Fig 6. Encoder(rate = 2/3)

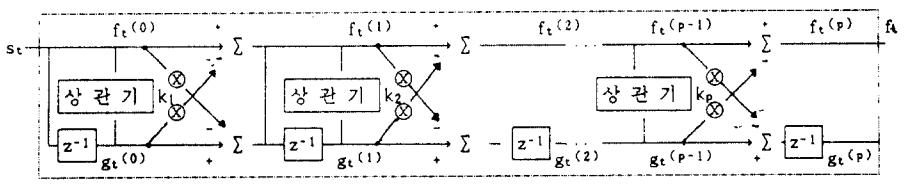


그림 5. PARCOR 방식을 이용한 음성 압축 알고리즘 블럭도
Fig 5. Block diagram of speech compression algorithm using PARCOR scheme

그림6에서 보는 바와 같이 부호기는 rate 1/2의 부호기에 uncoded 1 bit를 첨가 시킨 형태이다. trellis diagram의 위의 두 branch는 입력 비트 x_0x_1이 00 또는 10이며 아래의 두 branch는 x_0x_1이 01 또는 11을 나타낸다. 일반적으로 신호 공간에서 8 PAM은 4 PAM 보다 각 신호들 사이의 최소 거리가 좁아진다. 즉, M PAM에서 M이 증가할수록 오류율이 더욱 증가하는 것을 알 수 있으며 이는 전송 속도의 증가에 따라 성능이 감소되는 것을 의미한다. 이때 trellis coding이 적용되는데 이는 신호들 사이의 거리가 좁혀지더라도 수신된 신호를 복호할 때 trellis에 존재하는 신호의 거리만 넓혀 주면 절대 거리의 감소를 보상할 수 있다. 그림6의 부호화 비트에 대한 set나 partition은 다음의 세가지 규칙에 의한다.

1) 같은 state에서 발생하는 천이는 subset B0, B1의 waveform에 할당된다.
2) 한 state에서 결합되는 천이는 subset B0, B1의 waveform에 할당된다.
3) Parallel transition은 subset C0, C1, C2, C4로 할당된다.

그림 7(a)의 기준 4 PAM 신호를 위의 세가지 규칙에 의하여 변조된 신호로 할당하면 그림 7(b)와 같다.

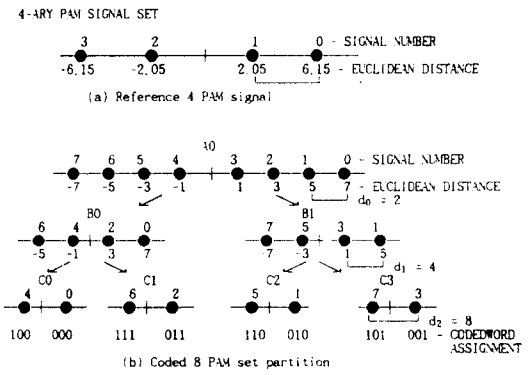


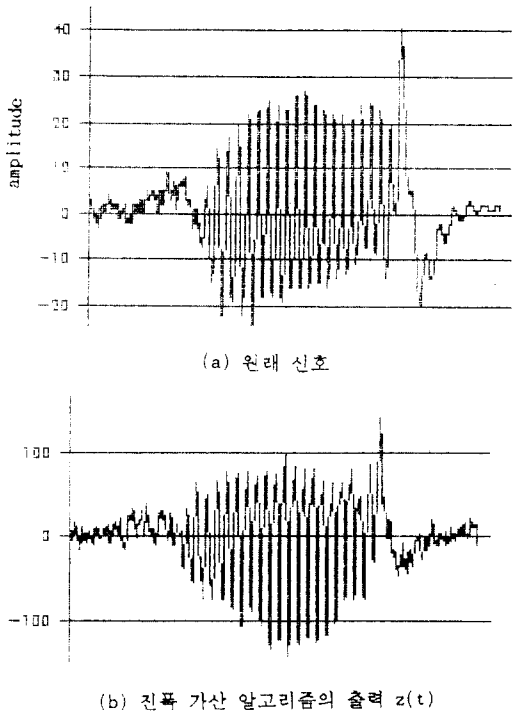
그림 7. Set partition에 의한 8 PAM의 code word 할당
Fig 7. Code word assignment of 8 PAM for set partition

그림6의 부호기를 통하여 출력된 3비트를 그림 7(b)의 set partition에 대응하여 펄스 진폭 변조된 신호가 가우시안 잡음 채널로 전송된다. 수신된 신호는 송신단의 역과정을 거쳐 다시 원 신호로 복원된다. 복원된 신호의 왜곡(distortion)을 각 알고리즘에 대하여 분석함으로써 최적의 알고리즘 및 SNR을 성할 수 있으며 결과는 IV장에 나타내었다.

Ⅳ. 결과 및 검토

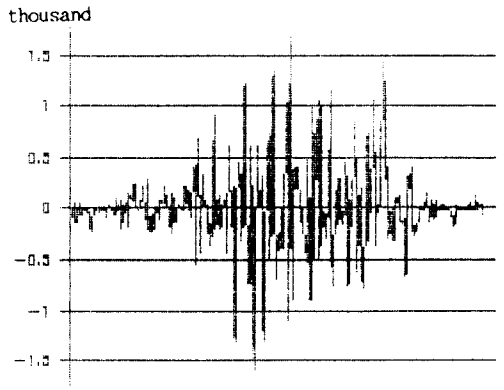
3.1절에서 살펴본 호핑 필터를 이용한 이 차원 진폭 스크램블링 알고리즘인 AAS, AMS 알고리즘과 동기 문제를 해결하기 위해 제안한 variable delay wright 알고리즘의 출력 z(t)는 그림8과 같다.

그림 8(a)는 음절 "10"에 대한 음성 신호를 시간 영역에서 나타낸 것으로 주파수 대역이 200Hz ~ 3200Hz로 제한되어 있다. (b), (c), (d)는 그림2의 일차원 스크램블링 알고리즘의 출력 신호 y(t)를 진폭 가산 알고리즘, 진폭 승산 알고리즘, variable delay weight 알고리즘을 통과한 출력 z(t)의 파형이다. 그림 8(b)는 원래 신호에 비해 진폭만 변화되고 파형은 거의 변하지 않았으므로 도청자는 쉽게 도청할 수 있다. 이에 반해 그림 8(c)는 원 신호보다 진폭도 높고 파형이 변화됨을 알 수 있다. 즉, 진폭 가산

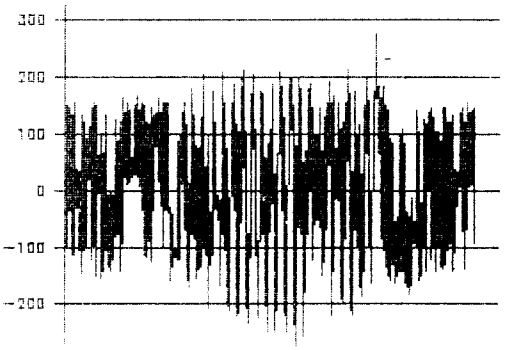


(a) 원래 신호

(b) 진폭 가산 알고리즘의 출력 z(t)



(c) 진폭 승산 알고리즘의 출력 z(t)



(d) variable delay weight 알고리즘의 출력 z(t)

그림 8. 음성 신호에 대한 세가지 알고리즘의 출력
Fig 8. output of 3-algorithm for speech signal

스크램블링 알고리즘보다 진폭 승산 스크램블링 알고리즘이 비도가 높다는 것을 알 수 있다. 그림 8(d)는 제안한 variable delay weight 알고리즘을 통과한 출력 z(t)로서 그림 8(b), (c)보다 더 랜덤하기 때문에 비도가 타 알고리즘에 비해 더 높음을 알 수 있다.

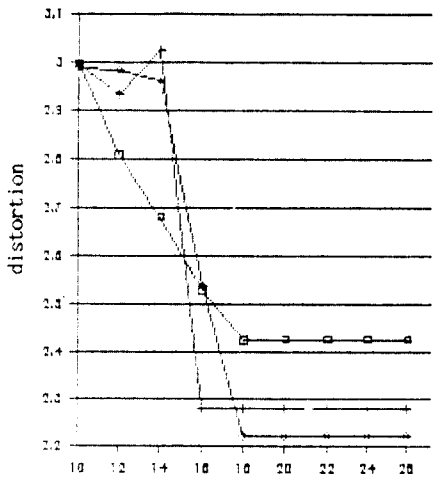
3.3절에서 언급한 PARCOR 방식을 이용한 음성 압축 알고리즘에서 상관 계수의 차수인 p의 값을 5, 10, 15로 변화하여 가우시안 잡은 채널로 전송하여 복원된 신호의 왜곡을 각 알고리즘에 대하여 분석한 결과는 그림 9와 같다.

왜곡의 정도를 나타내는 d는 원 신호 $\hat{m}_t$평균 자승 오차이며 식 (18)과 같다.(N은 음성의 샘플수)

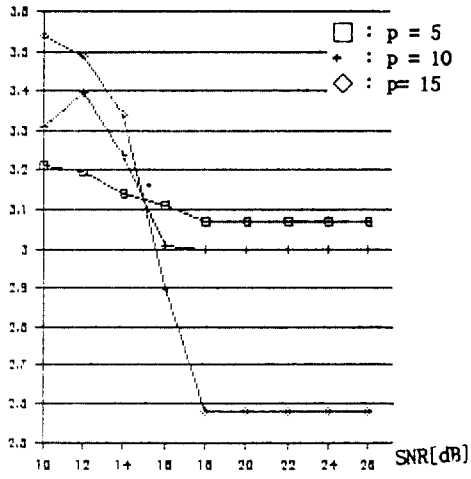
$$d=\frac{1}{N}\sqrt{\sum(m_t-\hat{m}_t)^2} \qquad (18)$$

그림 9(a)는 상관 계수의 차수 p가 5, 10, 15일 때 호핑 필터를 이용한 이차원 진폭 스크램블링으로 AAS 알고리즘을 이용하여 각 SNR에 대해 왜곡을 나타내었다.

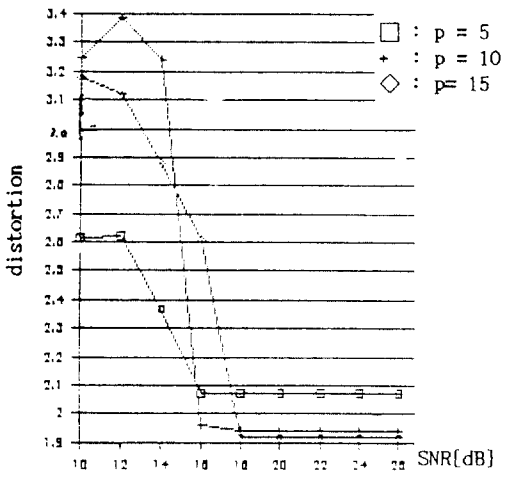
p=5, p=15일 때 SNR이 18 dB부터 왜곡이 일정하며 p=10일 때에는 17 dB부터 일정하다. SNR이 15 dB까지는 p=5일 때가 가장 왜곡이 적으며 18 dB 이상일 때에는 p=15일 때가 가장 왜곡이 적다. 18 dB를 기준으로 볼 때, p=15일 때가 p=5와 p=10일 때보다 왜곡이 약 0.2, 0.05 정도 낮다. p가 15



(a) AAS 알고리즘



(b) AMS 알고리즘



(c) variable delay weight 알고리즘

그림 9. AAS, AMS, variable delay weight알고리즘에 대한 왜곡

Fig 9. Distortion for AAS, AMS, variable delay weight algorithm

이상일 때에는 시뮬레이션 결과 왜곡의 차이가 작기 때문에 p=10에서 p=15 사이의 최적의 상관 계수의 차수이며 최적의 SNR은 18 dB이다.

그림 9(b)는 호핑 필터를 이용한 이차원 진폭 스크램블링을 AMS 알고리즘을 이용하여 각 SNR에 대해 왜곡을 나타내었다.

p=5, p=10일 때 SNR이 17 dB부터 왜곡이 일정하며 p=15일 때에는 18 dB부터 일정하다. SNR이 15 dB까지는 p=5일 때가 가장 왜곡이 작으며 18 dB 이상일 때에는 p=15일 때가 가장 왜곡이 작다. 18 dB를 기준으로 볼 때, p=15일 때가 p=5와 p=10일 때보다 왜곡이 약 0.5, 0.4 정도 낮다. p=5, p=10일 때에는 왜곡의 차이가 적으며 p=15일 때 왜곡이 급격히 적어짐을 알 수 있다. 따라서 AAS 알고리즘 일 경우 최적의 상관 계수의 차수는 15이며 최적의 SNR은 18 dB이다.

그림 9(c)는 호핑 필터를 이용한 이차원 진폭 스크램블링을 variable delay weight 알고리즘을 이용하여 각 SNR에 대해 왜곡을 나타내었다.

p=5, p=10일 때 SNR이 16 dB부터 왜곡이 일정하며 p=15일 때에는 18 dB부터 일정하다. SNR이 16 dB 까지는 p=5일 때가 가장 왜곡이 적으며 18 dB 이상일 때에는 p=15일 때가 가장 왜곡이 적다. 18 dB를 기준으로 볼 때, p=15일 때가 p=5와 p=10일 때보다 왜곡이 약 0.15, 0.02정도 낮다. p=10, p=15일 때에는 왜곡의 차이가 적기 때문에 p=10에서 p=15 사이가 최적의 상관 계수의 차수이며 최적의 SNR은 18 dB이다.

결론으로 위의 세 알고리즘의 최적의 SNR은 18 dB 이다. 18 dB 이상일 때, 최적의 이차원 진폭 스크램블링 알고리즘은 variable delay weight 알고리즘이며 18 dB 이하일 때에는 AAS 알고리즘이다. 18 dB 이하일 때 variable delay weight 알고리즘이 왜곡이 많은 이유는 이전의 음성 샘플이 다음 음성 샘플에 영향을 미치기 때문에 복호기에서 에러를 검출하지 못한 경우 다음 샘플로 계속 영향을 미친다. AMS 알고리즘은 그림 8(b)에서 알 수 있듯이 진폭이 크게 때문에 4 비트로 양자화하면 양자 에러가 매우 크기 때문에 다른 두 알고리즘 보다 왜곡이 심한 것을 알 수 있다.

V. 결 론

기존의 음성 비화 방식은 주파수 영역에서 에너지와 주파수 스펙트럼과의 관련성과 음성의 잔여 이해도 때문에 항상 제3자에게 정보가 누출될 수 있는 치명적인 단점을 가지고 있으며, 시간 영역에서 송수신간의 동기가 문제점으로 남아 있다. 특히, 고주파 성분의 손실로 음성 질의 저하를 초래할 수 있으므로 대역이 제한된 음성 신호는 비도의 증가 상실과 대역 확산 및 음질 저하의 단점이 서로 절충(trade off)되어야 한다. 또 하나의 큰 단점은 암호학적인 측면에서 볼 때, 키 공간이 작다는 것이다. 키 공간이 작다는 단점을 보완하기 위하여 시간 영역 스크램블링과 주파수 영역스크램블링을 결합시켜 키 공간을 확장시킨 혼합 방식이 주로 사용되고 있지만 위의 문제점을 만족스럽게 보완하지는 못한다.

본 논문에서 소개한 호핑 필터를 이용한 이차원 진폭 스크램블링 알고리즘은 기존의 방식이 위치를 스크램블링 하여 잔여 이해도를 포함한 것과는 달리 신호의 진폭을 스크램블링하여 잔여 이해도를 가질 수 없다. 또한 호핑 필터를 이용하여 주파수를 분할시켜 각각 다수 생성된 비트를 이용하여 진폭을 스크램블링하기 때문에 키 공간이 더욱 더 확장된다. 그러나 동기 문제는 여전히 남아있다. 그러므로 호핑 필터를

이용한 이차원 진폭 스크램블링 알고리즘으로 적용된 AAS 알고리즘과 AMS 알고리즘 대신 모듈 연산이 첨가된 variable delay weight 알고리즘을 제안하였으며, 이는 이전에 수신된 신호를 이용하여 수신단 스스로 동기를 맞추기 때문에 동기 문제를 해결할 수 있으며, 비도도 타 알고리즘에 비해 높다는 것을 시뮬레이션을 통하여 알 수 있다. 그러나 실제로 음성 데이타를 음성 압축, 채널 코딩하여 가우시안 잡음 채널로 전송하였을 때 복원된 음성 데이타에 대한 왜곡을 각 알고리즘에 대해 분석하여야만 최적의 알고리즘 및 최적의 상관 계수 차수 그리고 최적의 SNR을 정할 수 있다. 음절 "10"에 대해 샘플 수를 2048개로 하여 시뮬레이션 한 결과, 최적의 SNR은 18 dB이며 최적의 상관 계수 차수 p는 AAS 알고리즘과 variable delay weight 알고리즘 일 경우 p=10~p=15이며 AMS 알고리즘 일 경우 p=15이다. 18 dB 이상일 때, 최적의 이차원 진폭 스크램블링 알고리즘은 variable delay weight 알고리즘이며 18 dB 이하일때에는 AAS 알고리즘이다. 18 dB 이하일 때 varible delay weight 알고리즘이 왜곡이 많은 이유는 복호기에서 에러를 검출하지 못한 경우 에러가 발생한 샘플이 다음 음성 샘플에 영향을 미치기 때문이다.

AMS 알고리즘의 출력 음성은 진폭이 크기 때문에 4 비트로 양자화하면 양자 에러가 발생하여 성능에 심각한 영향을 미치게 됨을 알 수 있으므로 두 알고리즘 보다 양자화 비트 수를 더 많이 필요로 함을 알 수 있다.

참 고 문 헌

1. 한국전자통신연구소, 현대 암호학, 한국전자통신연구소, 1991.
2. Allen Gersho, "Perfect Secrecy Encryption of Analog Signals," IEEE Journal on Selected Areas in Comm., vol.SAC-2, PP. 460-466, 1984.
3. N. S. Jayant, "Analog Scramblers for speech privacy," Comput. Security, vol.21, pp.275-289, 1982.
4. Alex Goniotakis, Ahmed k.Elhakeem, "Security Evalution of a New Anglog Speech Privacy/Scrambling Device Using Hopping Filter," IEEE Journal on Selected Areas in Comm., vol. 8, 781-799, 1991.
5. Enrico Del Re, Romano Fantacci, and Damiano Maffucci, "A New Speech Signal Scrambling Method for Secure Communications," IEEE Journal on Selected Areas in Comm., vol. 7, PP. 474-480, 1989.
6. R. L. Rivest, A. Shanir, and L. Adlman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Commun. ACM, vol. 21, pp. 120-126, 1978.
7. Ungerboeck, G. "Channel Coding with Multilevel/Phase Signals," IEEE Trans. Inform. Theory, Vol.IT-28, pp.55-67, Jenuary 1982.

鄭 智 元(Ji-Won Chung) 정회원
1989년 : 성균관대학교 전자공학과 졸업(공학사)
1991년 : 성균관대학교 대학원 전자공학과 졸업(공학석사)
1990년 11월 ~ 1992년 1월 : 금성정보통신 연구소 연구원
1992년 3월 ~ 현재 : 성균관대학교 대학원 정보공학과 박사과정

元 東 豪(Dong-Ho Won) 정회원
1976년 : 성균관대학교 전자공학과 졸업
1978년 : 성균관대학교 대학원 졸업
1978년 ~ 1980년 : 한국전자통신 연구소 연구원
1985년 ~ 1986년 : 일본 동경 공대 객원 연구원
1988년 : 성균관대학교 공학박사
1982년 ~ 현재 : 성균관대학교 정보공학과 조교수, 부교수, 교수

李 庚 鎬(Kyoung-Ho Lee) 정회원
1991년 : 성균관대학교 정보공학과 졸업(공학사)
1993년 : 성균관대학교 대학원 정보공학과 졸업(공학석사)
1993년 ~ 현재 : 성균관대학교 대학원 정보공학과 박사과정