호핑 필터를 이용한 이차원 진폭 스크램블링 알고리즘에 관한 연구

°정지원, 고경환, 이경호, 원동호

성균관대학교 정보공학과

A Study on Two Dimensional Scrambling Algorithm using Hopping Filter

°Ji Won Jeong, Kyoung Hwan Ko, Kyoung Ho Lee, Dong Ho Won

SUNG KYUN KWAN UNIV.
Department of Information Engineerimg

요약

기존의 음성 정보 보호 방식의 단점인 비화의 감소, 키 수의 제한, 상관 관계를 이용한 제 3자의 해독 등의 문제점을 해결할 수 있는 호핑 필터를 이용한 이차원 진폭 스크램블링은 현대 아날로그 음성 신호에 있어서 강력한 비화 방식이다.

본 논문에서는 KAISER WINDOW FIR 필터를 이용하여 호핑 필터를 구성하였으며, 이차원 진폭 스크램블링 알고리즘의 최대 단점인 동기(synchronization)문제를 해결하기 위하여 variable delay를 이용한 알고리즘을 제안하였다. 또한, 시뮬레이션을 통하여 디지탈 신호에도 응용·고찰하였다.

1. 서론

유선 및 무선 통신망이 널리 보급되기 시작한 20세기 초부터 음성 신호를 인가받지 않은 제 3자로부터 보호하기 위한 비화 방식의 필요성이 크게 인식되기 시작하였다.

20세기 초와는 달리 현대에 이르러서는 정보화 사회의 성숙과 더불어 중요 정보의 음성 대역급 통신망을 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 이상의 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 대역을 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 1 차원 스크램블링 알고리즘(1-dimensional scrambling algorithm)이라 하고 혼합 방식을 2 차원 스크램블링 알고리즘(2-dimensional scrambling algorithm)이라 한다.

아날로그 신호의 초기 비화 방식은 비도가 극히 낮은 주파수 영역 스크램블링 위주로 발전되어 왔으나, 현재의 추세는 일정한 시간 길이를 갖는 시간 요소(time segment)로 분리한 후 이들을 적절히 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 장비의 주종을 이루고 있다.

그러나 기존의 방식은 키 수가 제한되어 있으며, 주파수 영역에서 음성의 잔여 이해도(residual intelligibility) 때문에 제 3 자가 상관 관계를 이용하여 공격할 수 있다는 문제와 시간 영역에서 송·수신간에 동기를 맞추는 문제가 가장 어려운 문제로 남아있다.[2,3]

호핑 필터를 이용한 이차원 진폭 스크램블링에는 난수 생성기에서 출력된 비트를 더하는 진폭 가산 스크램블링 알고리즘과 곱하는 진폭 승산 스크램블링 알고리즘이 있다.[4] 이는 시간 영역과 주파수 영역에서 진폭을 스크램블링하기 때문에 상관 계수를 0으로 하여 음성의 잔여 이해도를 완전히 없애 제 3자의 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 생성기에서 출력된 키 값을 이용한 variable delay weight 알고리즘을 제안하였다.

본 논문은 호핑 필터를 이용한 이차원 진폭 스크램블링의 전반적인 개요를 설명하고, 동기 문제를 해결하기 위하여 진폭 가산 스크램블링 알고리즘과 진폭 승산 스크램블링 알고리즘 대신 variable delay weight 알고리즘을 적용하였다. 또한 진폭 가산 스크램블링 알고리즘과 진폭 승산 스크램블링 알고리즘의 비도를 수학적으로 분석하였다. 호핑 필터를 이용한 이차원 진폭 스크램블링은 아날로그 신호에만 적용하였는데 본 논문에서는 디지탈 신호에 적용하여 시뮬레이션을 통하여 비도를 분석 하였다.

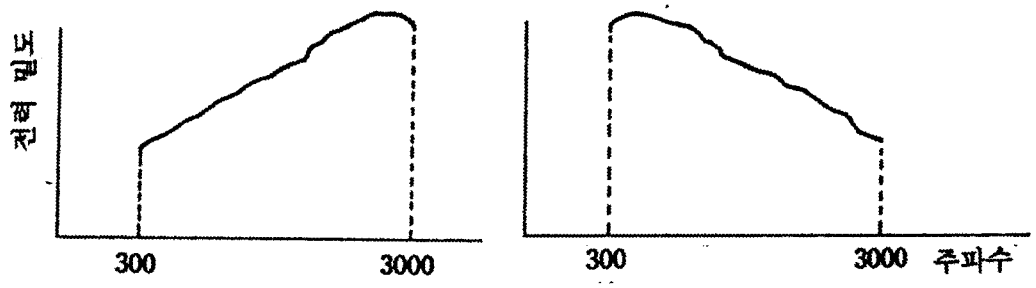
2. 기존 방식 검토

기존의 음성 비화 방식은 주파수 영역 스크램블링, 시간 영역 스크램블링, 그리고 혼합 방식이 주종을 이루고 있다. 본 장에서는 이 세 가지 방식을 간략하게 검토하겠다.

2.1 주파수 영역 스크램블링

2.1.1 음성 반전(speech inverter)

가장 간단한 방식으로 대역이 제한된 음성을 주파수 영역에서 반전시키는 방식으로 설계가 용이하고 복원된 음질은 좋으나 한 개의 키만을 사용하므로 비도가 매우 낮다.



(a) 원래 신호 (b) 반전 신호

그림 1. 음성 반전

2.1.2 대역천이 반전(band shift inverter)

음성신호를 다른 주파수 영역으로 천이시키고 음성 대역을 넘어서는 고주파 성분을 저주파 쪽으로 이동시키는 방식이다. 이 방식 또한 키 수의 제한과 음성의 잔여 이해도가 높다.

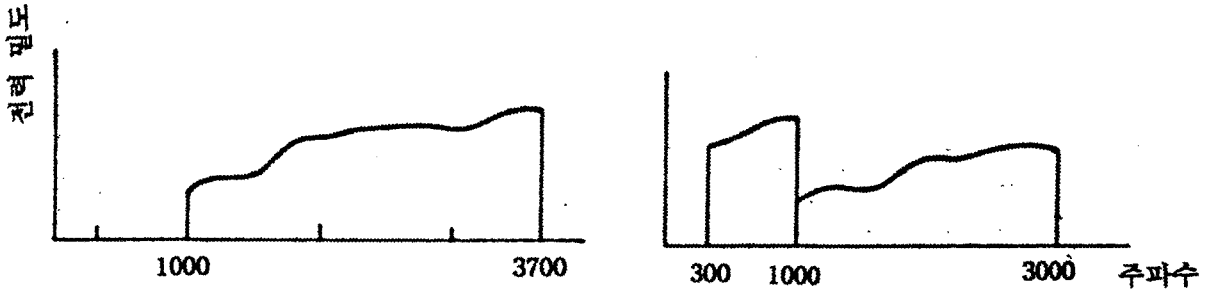


그림 2. 대역천이 반전

2.1.3 대역 분리(band splitter)

음성 스펙트럼을 몇 개의 부대역(subband)으로 나눈 뒤 부대역들의 순서를 재배열하는 방식이다. 이는 음성 에너지와 주파수와의 관련성 때문에 해독이 용이하다.

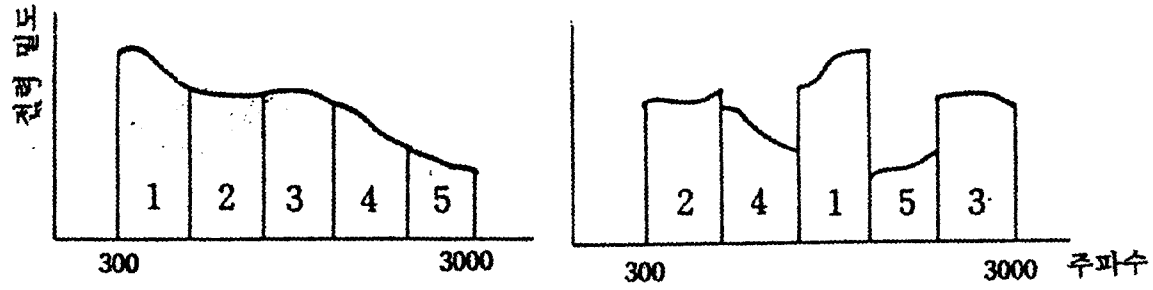


그림 3. 대역 분리

2.2 시간 영역 스크램블링

2.2.1 시간 성분 반전(reversed time segment)

아날로그 신호를 A/D 변환기를 거쳐 디지탈 신호로 변환한 후 몇 개의 샘플로 구성된 시간 성분으로 나누어 각 성분들에서 샘플 순서를 역으로 하여 D/A 변환 하는 방식이다. 이 방식은 음성의 잔여 이해도는 낮으나 비도가 낮고 송 수신간에 동기를 필요로 한다.

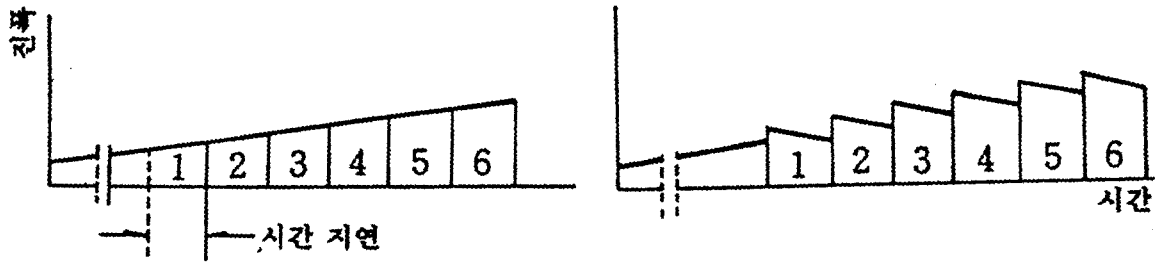


그림 4. 시간 성분 반전

2.2.2 호핑 윈도우(hopping wimdow)방식

이 방식은 블럭 시간 성분 치환 방식이라고도 불리우며, 각 프레임내에서 치환의 순서에 따라 성분들을 전송함으로써 이루어지며 수신측에서는 역치환을 함으로써 원래 신호를 복원할 수 있다. 시간 성분 경계면 사이의 갑작스러운 변화로 고주파 성분이 발생하여 음질의 저하를 초래한다.

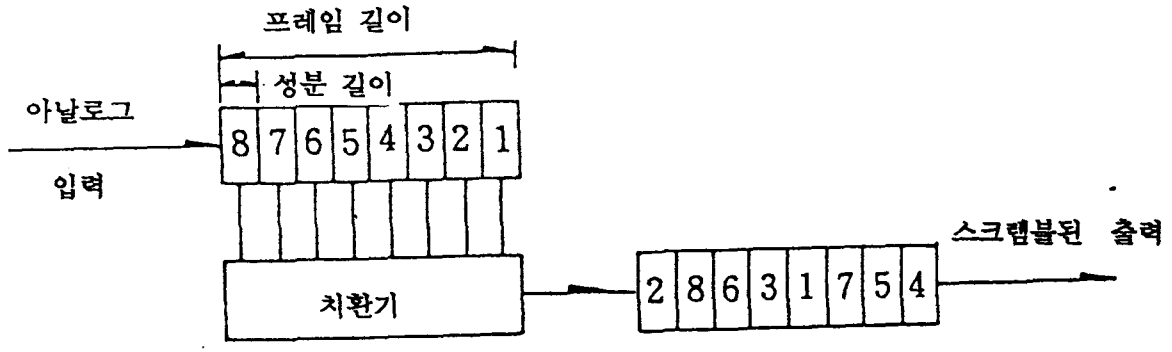


그림 5. 호핑 윈도우 방식

2.3 혼합 방식

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 3가지 문제점을 가지고 있다.

① 음성의 잔여 이해도 때문에 제 3자의 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 되며, ③의 문제점은 하드웨어 측면에서 구현에 어려움이 있다. ①, ②의 문제점을 효율적으로 해결할 수 있는 방식이 호핑 필터를 이용한 이차원 진폭 스크램블링 알고리즘이다.

3. 호핑 필터를 이용한 이차원 진폭 스크램블링 알고리즘

호핑 필터를 이용한 이차원 진폭 스크램블링은 기존의 비화 방식에 비해 비도를 높이고 음성의 잔여 이해도를 줄일 수 있기 때문에 효율적인 아날로그 음성 보호 방식이다.

본 장에서는 시스템 모델에 대한 전반적인 개요와 이차원 알고리즘인 진폭 가산 스크램블링 알고리즘과 진폭 승산 스크램블링 알고리즘의 비도를 수학적으로 분석하였다.

3.1 시스템 모델

호핑 필터를 이용한 이차원 진폭 스크램블링의 시스템 모델은 그림 6.과 같으며, 이는 서로 다른 주파수 대역을 갖고 있는 대역 통과 필터(band pass filter)들과 이득 조절 장치, 난수 생성기, 그리고 D/A 변환기로 구성되어 있다.

대역폭이 200 Hz ~ 3200 Hz 인 음성 신호는 서로 다른 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.

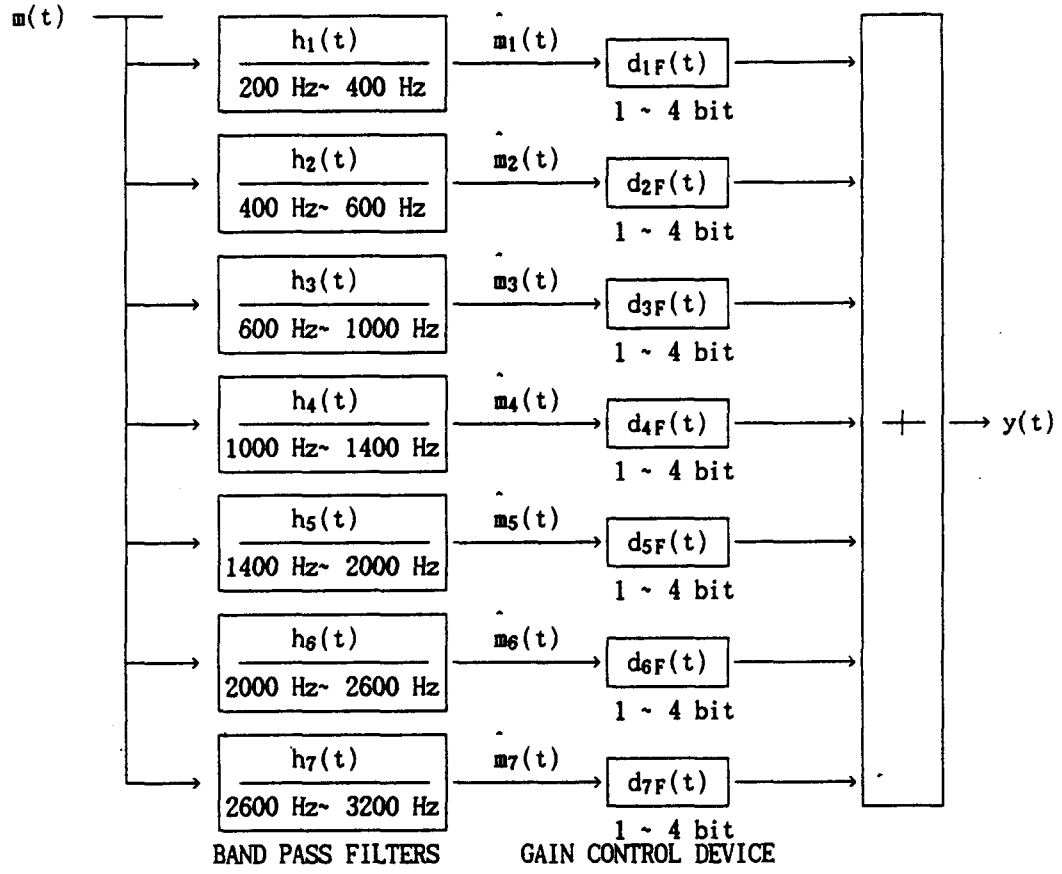
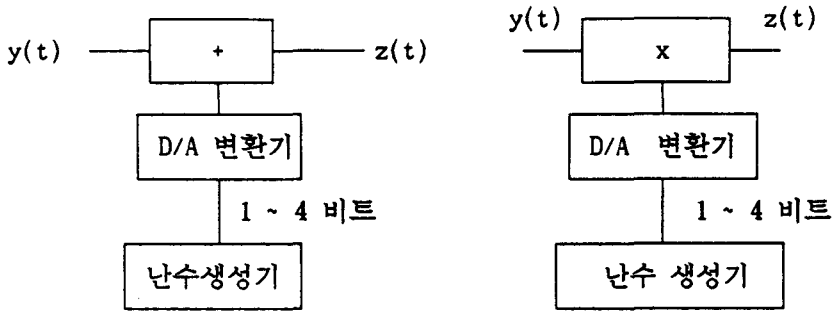


그림 6. 시스템 모델

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 시간 영역에서 난수 생성기에서 생성된 1 ~ 4 비트를 D/A 변환기를 이용하여 아날로그 값으로 변환한 후 y(t)와 더하거나 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(AAS : Amplitude Addition Scrambling)알고리즘이라 하며, 곱하는 알고리즘을 진폭 승산 스크램블링(AMS : Amplitude Multiply Scrambling)알고리즘이라 한다. 이 두 알고리즘을 그림 7.에 나타내었다.

기존의 스크램블링은 대역을 분리하여 치환하거나 샘플링 순서를 치환 하는 방식과는 달리 호핑 필터를 이용한 이차원 진폭 스크램블링은 분리된 대역의 진폭을 스크램블링하고 다시 시간 영역에서의 진폭을 스크램블링함으로써 잔여 이해도의 증가, 비도의 감소라는 기존의 스크램블링의 단점을 개선시킬 수 있다.



(a) 진폭 가산 스크램블링 알고리즘 (b) 진폭 승산 스크램블링 알고리즘

그림 7. 이차원 알고리즘

그림 6.에서 200 Hz ~ 3200 Hz의 주파수 대역을 가진 원래 신호 $m(t)$가 i개의 대역 통과 필터를 통과한 각 신호를 $m_i(t)$라 하면 일차원 알고리즘의 출력 $y(t)$는 식 (1)과 같다.

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

$d_{iF}(t)$는 펄스 진폭 변조(PAM) 과정을 나타내며 식 (2)와 같다. $D_{iF}(k)$는 i개의 난수 생성기에서 생성된 1 ~ 4 비트를 D/A 변환기를 이용하여 아날로그로 변환된 값을 나타낸다.

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

단, $0.3125\ \text{ms} \le T_F \le 1.25\ \text{ms}$

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

$g_F(t - kT_F)$는 게이트 함수를 나타내며 식 (3)과 같다.

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

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.

$$z_{AAS}(t) = y(t) + d_A(t)$$

$$= \left(\sum_{i=1}^{i=7} \hat{m}_i(t) \cdot d_{iF}(t) \right) + d_A(t) \qquad (4)$$

$$z_{AMS}(t) = y(t) \cdot d_A(t)$$

$$= \left(\sum_{i=1}^{i=7} \hat{m}_i(t) \cdot d_{iF}(t) \right) \cdot d_A(t) \qquad (5)$$

$d_A(t)$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 ~ 2^7 이며 이차원 알고리즘의 키 공간은 2^4 ~ 2^{28} 이다.

3.3 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.

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

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

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

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

$$= E\left[\sum_{i=1}^{i=7} m(t)\hat{m}_i(t+\tau) d_{iF}(t+\tau) \right] + E[m(t)d_A(t+\tau)]$$

$$= \sum_{i=1}^{i=7} E[m(t)\hat{m}_i(t+\tau) d_{iF}(t+\tau)] + E[m(t)d_A(t+\tau)] \qquad (7)$$

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

$$E[m(t)z(t+\tau)] = \left\{ \sum_{i=1}^{i=7} E[m(t)\hat{m}_i(t+\tau)E[d_{iF}(t+\tau)] \right\} + E[m(t)]E[d_A(t+\tau)] \qquad (8)$$

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

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

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

$$\begin{aligned} E[m(t)]E[z(t+\tau)] &= E[m(t)]E\left[\sum_{i=1}^{i=7} \hat{m}_i(t+\tau)\cdot d_{iF}(t+\tau) + d_A(t+\tau) \right] \\ &= E[m(t)]\left[\sum_{i=1}^{i=7} E[\hat{m}_i(t+\tau)\cdot d_{iF}(t+\tau)] + E[d_A(t+\tau)] \right] \\ &= E[m(t)]\left[\sum_{i=1}^{i=7} E[\hat{m}_i(t+\tau)]E[d_{iF}(t+\tau)] + E[d_A(t+\tau)] \right] \\ &= u_F E[m(t)] \sum_{i=1}^{i=7} E[\hat{m}_i(t+\tau)] + u_A E[m(t)] \\ &= u_F E[m(t)] E\left[\sum_{i=1}^{i=7} \hat{m}_i(t+\tau) \right] + u_A E[m(t)] \end{aligned} \qquad (10)$$

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

$$C_{mz}(\tau) = u_F\left(E\left[m(t)\sum_{i=1}^{i=7} \hat{m}_i(t+\tau)\right] - E[m(t)]\, E\left[m(t)\sum_{i=1}^{i=7} \hat{m}_i(t+\tau)\right] \right) \qquad (11)$$

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

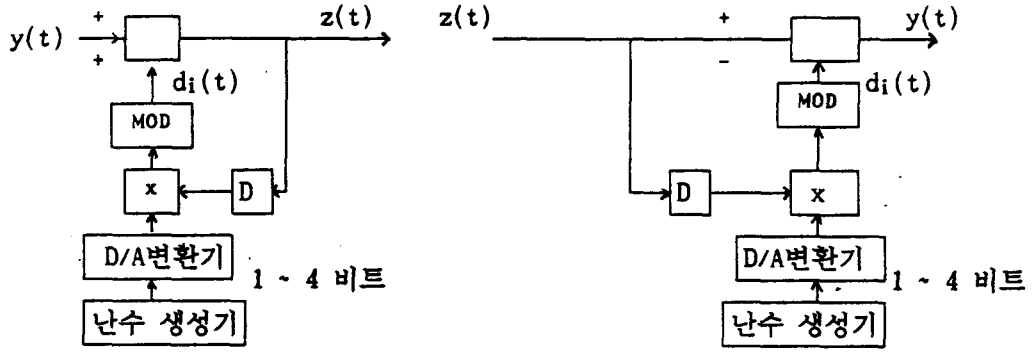
$$C_{mz}(\tau) = u_A\cdot u_F\left(E\left[m(t)\sum_{i=1}^{i=7} \hat{m}_i(t+\tau)\right] - E[m(t)]\, E\left[m(t)\sum_{i=1}^{i=7} \hat{m}_i(t+\tau)\right] \right) \qquad (12)$$

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

4. Variable delay weight 알고리즘

시간 영역 스크램블링의 최대 단점은 송·수신단의 동기를 맞추기 어렵다는 문제이다. 송수신간에 동기가 맞지 않으면 수신된 신호를 원래의 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, 묘듈 연산이 첨가되어 아날로그 신호에서도 수신단 스스로가 동기를 맞출 수 있는 알고리즘이다. 그림 8.은 variable delay weight 알고리즘의 송·수신단을 나타낸다.



(a) 송신단 (b) 수신단

그림 8. variable delay weight 알고리즘

그림 8. 에서 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 합으로 출력된다. 송신 신호 z(t)는 식 (13)과 같다.

$$z(t) = y(t) + d(t) \tag{13}$$

$$d(t) = k \cdot z(t-1)(\ \mathrm{mod}\ 2A)$$

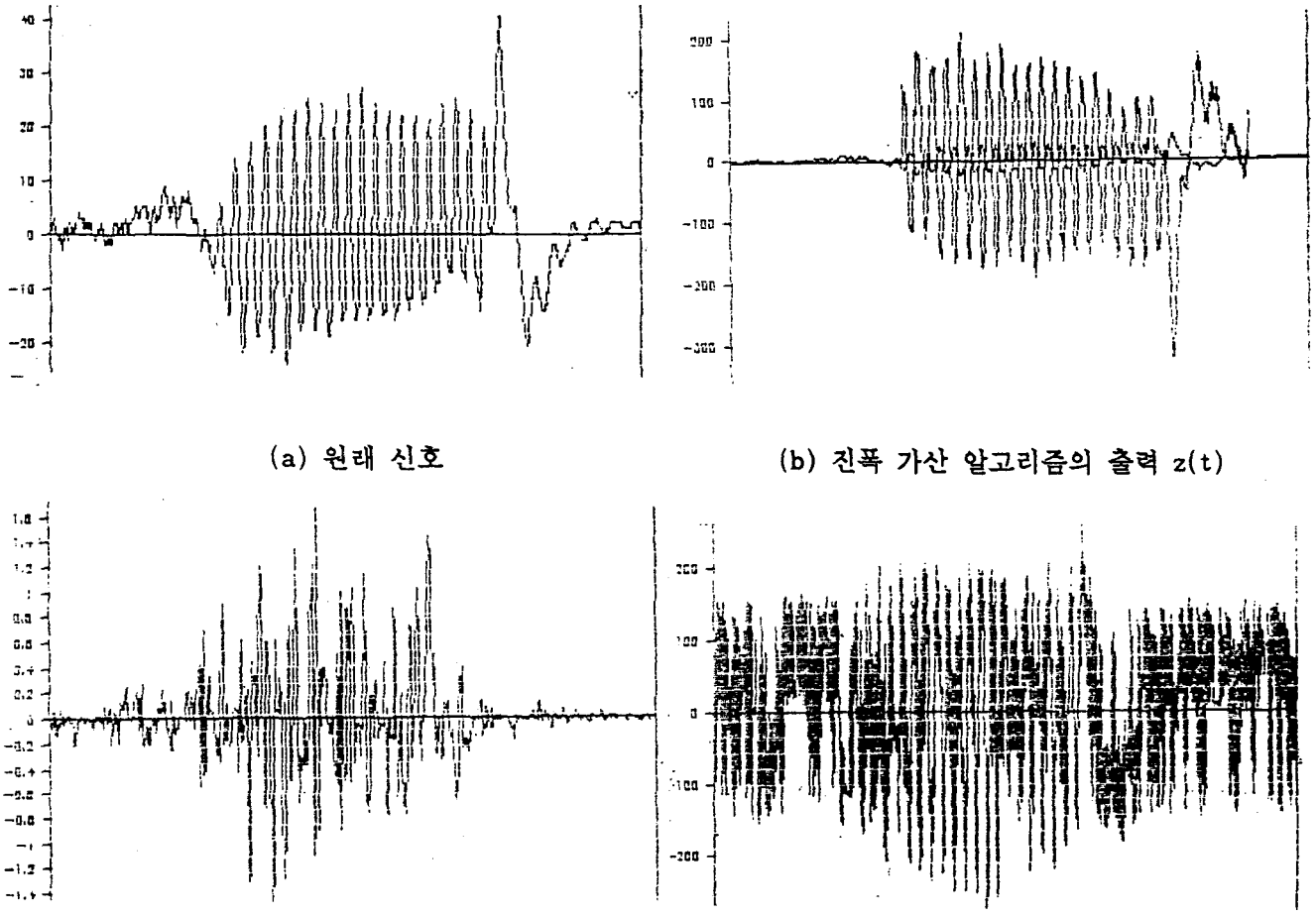
A : 신호의 진폭

수신기는 현재 수신단에 입력되는 신호 z(t)와 이전에 입력된 신호 z(t-1)에 난수 생성기에서 생성된 키 값을 곱한 값의 모듈러 연산인 $d_i(t)$를 차감함으로써 원래의 신호를 복호한다. 식 (14)는 수신단에서 복호된 원래 신호를 나타낸다.

$$y(t) = z(t) - d(t) \tag{14}$$

$$d_i(t) = k \cdot z(t-1)(\ \mathrm{mod}\ 2A)$$

본 논문에서는 위의 송·수신단을 진폭 가산 스크램블링 알고리즘과 진폭 승산 스크램블링 알고리즘 대신 동기를 맞추기 위해 variable delay weight 알고리즘을 제안한다. 그림 9.는 위에서 언급한 세가지 알고리즘을 시뮬레이션하여 나타낸 출력 파형이다.



(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 9. 음성 신호에 대한 세가지 알고리즘의 출력

그림 9.(a)는 음절 " 10 "에 대한 음성 신호를 시간 영역에서 나타낸 것으로 주파수 대역이 200 ~ 4 kHz로 제한되어 있다. (b), (c), (d)는 그림 6.의 음성 신호에 대한 시스템 모델에서 출력된 신호 y(t)를 진폭 가산 알고리즘, 진폭 승산 알고리즘, variable delay weight 알고리즘을 통과한 출력 z(t)의 파형이다. 그림 9.(b)는 원래 신호에 비해 진폭만 변화되고 파형은 거의 변하지 않았으므로 도청자는 쉽게 도청할 수 있다. 이에 반해 그림 9.(c)는 원 신호보다 진폭도 높고 파형이 변화됨을 알 수 있다. 즉, 진폭 가산 스크램블링 알고리즘보다 진폭 승산 스크램블링 알고리즘이 비도가 높다는 것을 알 수 있다. 그림 9.(c)는 제안한 variable delay weight 알고리즘을 통과한 출력 z(t)로서 그림 9.(b), (c)보다 비도가 더 높음을 알 수 있다. 그러나, variable delay weight 알고리즘은 채널 특성

상 에러율이 높을 수 있는 단점이 있기 때문에 오류 정정 부호(error correction code)를 삽입 시켜야 한다.

5. 디지탈 신호에의 응용

호핑 필터를 이용한 이차원 진폭 스크램블링 알고리즘은 아날로그 신호에 주로 적용되는데 본 장에서는 이 알고리즘을 디지탈 신호에의 적용에 대해 살펴본다.

그림 10.은 디지탈 신호에의 시스템 모델이며, 아날로그 신호의 시스템 모델(그림 6.)과 차이점은 입력단에 저역 통과 필터가 있다는 점이다.

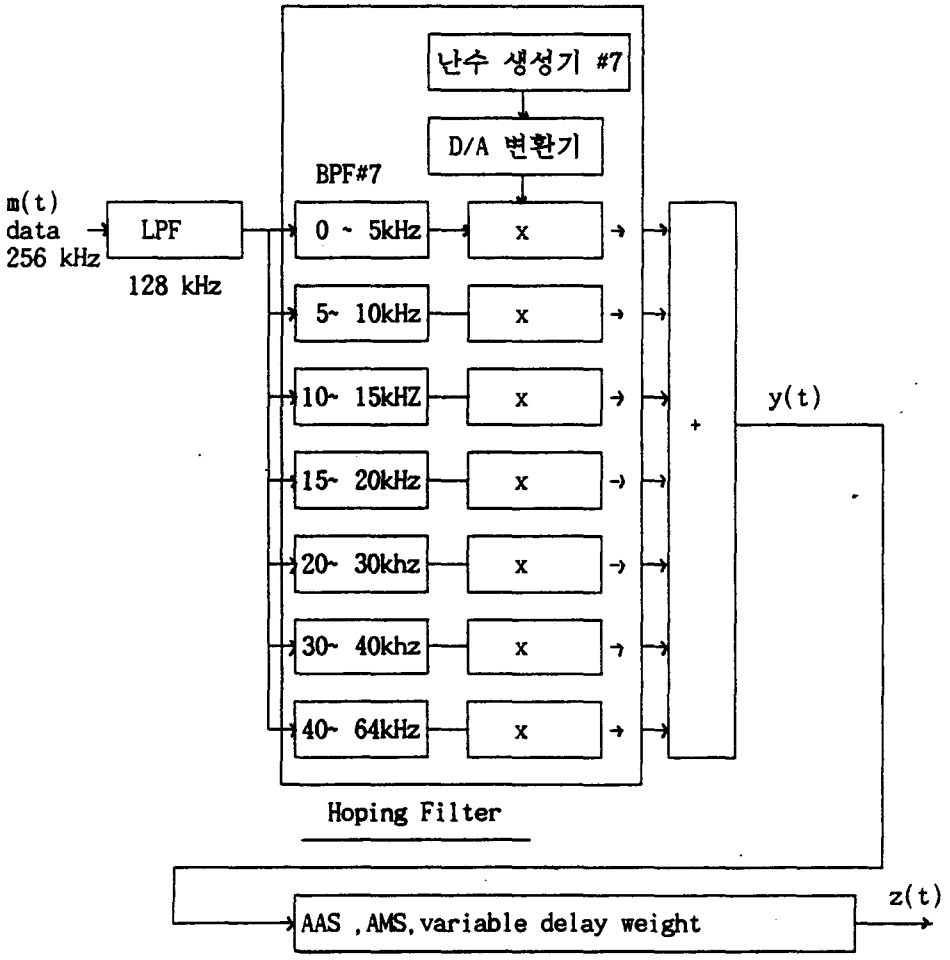
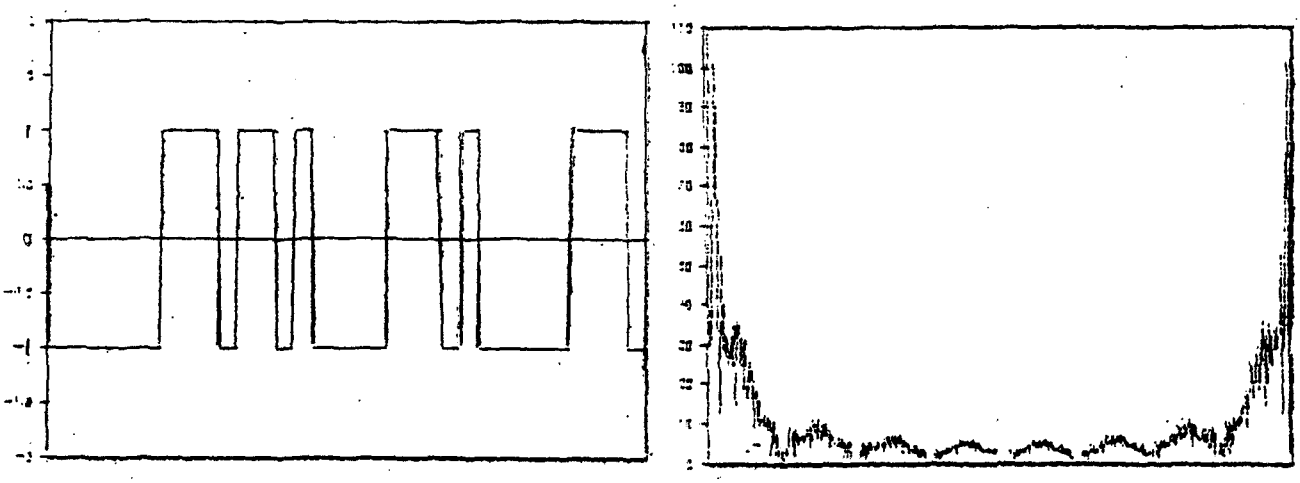


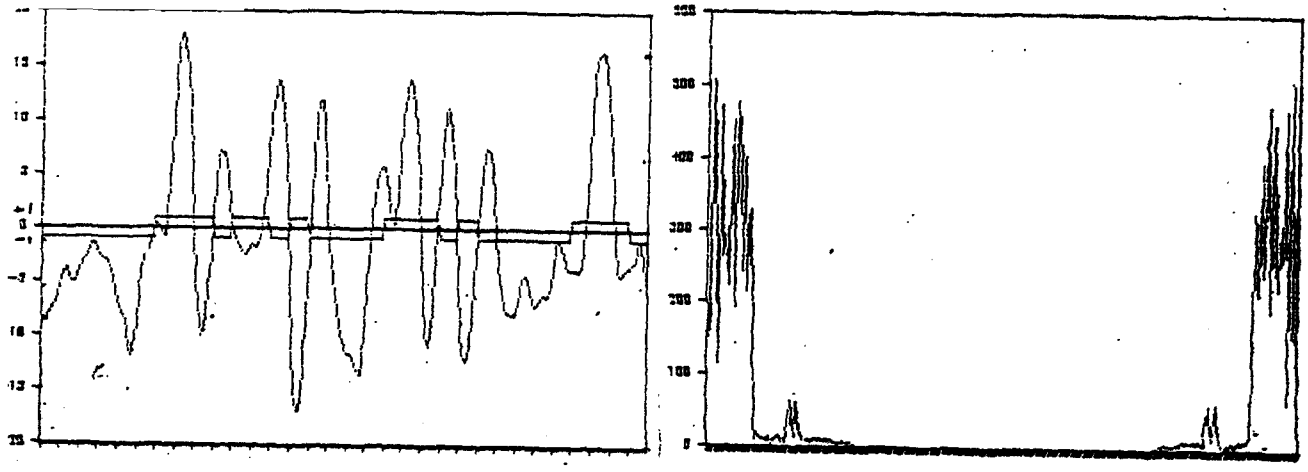
그림 10. 디지탈 신호의 시스템 모델

32 kHz 의 신호를 8 kHz 로 샘플링하여 데이타 속도가 256 kHz인 디지탈 신호가 송신단에 입력된다. 일단 입력되는 신호는 차단 주파수(f_c)가 128 kHz(데이타 속도의 1/2)인 저역 통과 필터를 통과하고 난 뒤 3장에서 언급한 아날로그 신호에의 적용 과정과 동일하며 키 공간 역시 동일하다(2^1~ 2^{28}). 저역 통과 필터와 대역 통과 필터는 KAISER WINDOW FIR 필터로써 구성하였으며 sidelobe가 거의 존재하지않는 날카로운 필터 특성을 가져야 한다. 이 알고리즘을 디지탈 신호에 적용시킬 경우 역시 동기 문제의 단점을 가지고 있으므로 variable

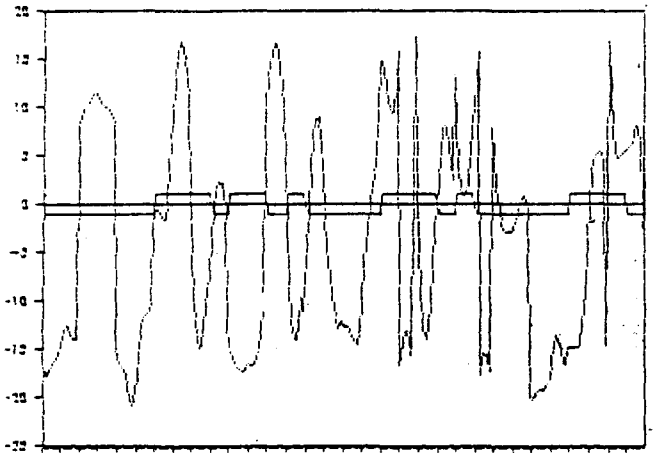
delay weight 알고리즘을 진폭 가산, 진폭 승산알고리즘 대신 적용 가능하다. 그림 11.은 호핑 필터를 이용한 이차원 진폭 스크램블링 알고리즘을 디지탈 신호에 적용하였을 때 입·출력 파형을 나타낸 것이다.



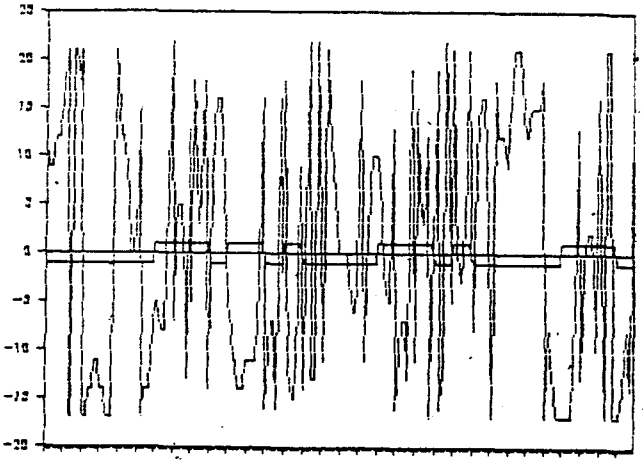
(a) 원 디지탈 신호의 시간 영역과 주파수 영역



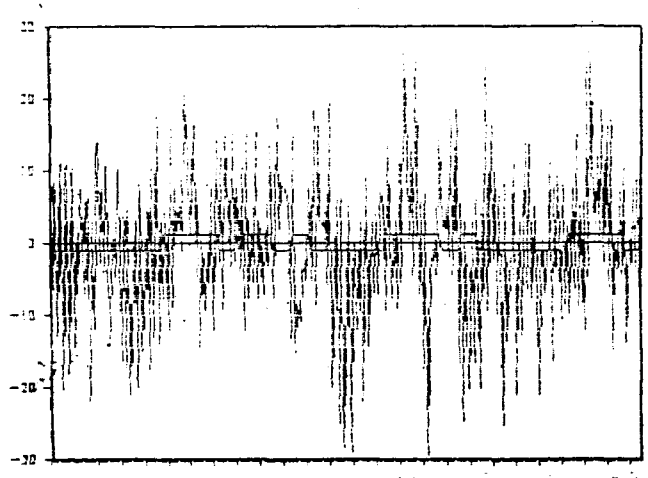
(b) 그림 10.에서 y(t)의 시간 영역과 주파수 영역



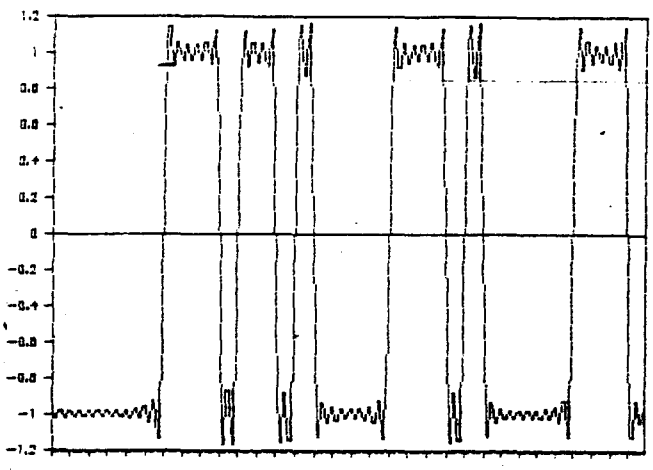
(c) 진폭 가산 알고리즘의 출력 파형



(d) 진폭 승산알고리즘의 출력 파형



(e) variable delay weight 알고리즘의 출력 파형



(f) 복호된 신호

그림 11. 256 kHz 디지탈 신호의 각 알고리즘 출력 파형

그림 11.(a)는 데이타 속도가 256 kHz인 디지탈 신호의 시간 영역과 주파수 영역을 나타내며 그림 11.(b)는 일차원 알고리즘(그림 10.)의 출력 y(t)의 파형을 나타내었다. 이는 원래 신호를 128 kHz의 저역 통과 필터와 주파수 대역이 서로 다른 대역 통과 필터들을 통과한 뒤 이 신호들을 난수 생성기에서 생성된 1 ~ 4 비트를 D/A 변환기를 이용하여 아날로그로 변환된 값과 곱하여 모두 더한 신호의 출력 파형으로 원래 신호의 파형과 약간 비슷하다. 일차원 알고리즘의 출력 y(t)를 다시 이차원 알고리즘인 진폭 가산 알고리즘, 진폭 승산 알고리즘, 제안한 variable delay weight 알고리즘을 통과한 출력 z(t)의 파형이 그림 11.의 (c),(d),(e)에 나타내었다. 음성 신호와 마찬가지로 진폭 가산 스크램블링 알고리즘보다 진폭 승산 스크램블링 알고리즘이 비도가 높다는 것을 알 수 있으며, variable delay

weight 알고리즘 출력 파형 역시 타 알고리즘에 비해 비도가 높다는 것을 알 수 있다.

신호를 복호할 때 수신단에서는 송신단의 역 과정을 거치면 된다. 즉, 수신된 신호 z(t)는 난수 생성기에서 생성된 값을 진폭 가산 알고리즘일 경우 빼고, 진폭 승산 알고리즘일 경우 나누고 variable delay weight 알고리즘일 경우 지연된 신호와 곱하여 차감하면 y(t)가 된다. y(t)를 다시 대역 통과 필터를 거쳐 PAM 과정을 하기 위하여 난수 생성기에서 생성된 값을 나누어 모두 더하면 원래의 신호 m(t)가 된다. 그림 11.(f)에 복호된 신호의 파형을 나타내었다. 펄스에 리플이 나타나는 이유는 입력단에 저역 통과 팔터를 이용하여 고주파 성분을 제거하였기 때문이다.

6. 결론

기존의 음성 비화 방식은 주파수 영역 스크램블링과 시간 영역 스크램블링, 그리고 시간 영역 스크램블링과 주파수 영역 스크램블링을 결합시킨 혼합 방식이 있다. 주파수 영역 스크램블링은 주파수 영역에서 음성의 잔여 이해도와 에너지와 주파수 스펙트럼과의 관련성 때문에 항상 제 3자에게 정보가 누출될 수 있는 치명적인 단점을 가지고 있다. 음성의 잔여 이해도와 비도 감소의 문제를 어느 정도 보완할 수 있는 시간 영역 스크램블링은 송·수신간의 동기와 대역이 확산되는 단점을 가지고 있다. 특히, 고주파 성분의 존재로 음성 질의 저하를 초래할 수 있다. 따라서 대역이 제한된 음성 신호에서 시간 영역 스크램블링은 비도의 증가 장점과 대역 확산의 단점이 서로 절충(trade-off) 되어야 한다.

암호학적인 측면에서 볼 때, 위의 두 스크램블링 방식의 또 하나의 단점은 키 공간이 적다는 것이다. 키 공간이 적다는 단점을 보완하기 위하여 시간 영역 스크램블링과 주파수 영역 스크램블링을 결합시켜 키 공간을 확장시킨 혼합 방식이 주로 사용되고 있다.

본 논문에서 소개한 호핑 필터를 이용한 이차원 진폭 스크램블링 알고리즘은 기존의 방식이 위치를 스크램블링 하여 잔여 이해도를 포함한 것과는 달리 신호의 진폭을 스크램블링 하여 잔여 이해도를 거의 없앤다. 또한 호핑 필터를 이용하여 주파수를 분할시켜 각각 난수 생성기에서 생성된 비트를 이용하여 진폭을 스크램블링하기 때문에 키 공간이 더욱 더 확장된다. 그러나 동기 문제와 대역 확산의 문제는 여전히 남아있다. 그러므로 진폭 가산 스크램블링 알고리즘과 진폭 승산 스크램블링 알고리즘 대신 모듈 연산이 첨가된 variable delay weight 알고리즘을 제안 하였다. variable delay weight 알고리즘은 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 에러율이 다소 높아질 우려가 있으므로 BCH 부호, REED SOLOMAN 부호, 길쌈 부호등의 오류 정정 부호의 적용이 요구된다.

RSA와 같은 디지탈 신호에의 암호 방식는 구현이 어려워 상용화 되기 어려우나,[6] 본 알고리즘을 디지탈 신호의 암호 방식으로 적용시킬 경우, 구현이 용이하며 적합한 통신 환경에서는 널리 유용하리라 사료된다.

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 Analog Speech Privacy / Scrambling Device Using Hopping Filter, " IEEE Journal on Selected Areas in Comm.,vol. 8, PP. 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. Shamir, and L. Adlman, " A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Commun. ACM, vol. 21, pp. 120 - 126, 1978.