通信情報保護學會誌
第2卷 第4號, 1992. 12

아날로그 음성, 비디오 및 오디오 신호의 비화방식

The Scrambling Methods of the Analog Speech, Video and Audio Signal

이일우* · 조동호**

요 약

본고는 아날로그 음성, 비디오 및 오디오 신호의 비화방식에 대한 연구로써 정보의 대부분을 구성하고 있는 음성, 그리고 앞으로 요구가 증가될 것으로 예견되는 위성 TV 및 CATV의 비디오와 오디오의 아날로그 비화방식(scrambling)의 종류 및 각각의 알고리즘에 대해 고찰하였다.

1. 서 론

각종 통신망의 확충과 정보기기의 발달에 힘입어 점차 정보화 사회로 진전됨에 따라 각종 정보의 상호 교류가 활발해지고 있으며, 이에 따른 정보의 적절한 보호 대책이 요구되어지고 있다. 그 보호 대책으로는 정보에의 접근을 제한하는 것과 정보 자체를 암호화하는 방식이 있다. 전자는 주로 컴퓨터 등의 정보 센타로 정보를 요구할때 비밀번호 등과 같은 식별자(identifier)를 검사하여 접근을 막는 것이고 후자는 통신 선로상의 도청 등과 같은 정보 누출을 막기 위하여 정보 자체를 암호화하고 전송하는 것으로 정보의 종류와 위치에 따라 각기 적용하거나 함께 사용하기도 한다.

정보는 크게 그 특성에 의해 음성과 데이타 그리고 화상 정보로 분류할 수 있고 각각의 정보를 나타내는 신호의 특성이 다르기 때문에 정보를 암호화하는 방식도 신호 특성에 따라 선정하는 것이 효율적인 정보 보호 방안이다. 데이타 정보보호 방식은 제 1, 2차 세계 대전의 결과로 비약적으로 발전하여 군사적 목적외에 행정, 금융등의 상업적 측면에서도 많이 사용되고 있다. 대표적인 예로 미국의 표준 데이타 암호 방식으로 DES(Data Encryption Standard)가 있고, 일본에서는 DES를 좀더 향상시킨 FEAL-8 (Fast Data Encipherment Algorithm-8) 방식을 채택하였다. 또한 국내의 금융망에서도 미국의 DES 방식을 채택하여 운용중에 있다.

데이타 통신 및 팩시밀리 통신에 사용되는 모뎀에는 기존의 변조 방식 외에도 암호화하는 기법이 채택되어, 데이타 통신은 물론 팩시밀리를 통한 문서 통신도 어느정도 보안성을 확보하고 있다. 그러나 음성 정보의 경우, 가장 많은 정보의 교류 수단임에도

* 경희대학교 공과대학 전자계산공학과 대학원
** 경희대학교 공과대학 전자계산공학과 부교수, 경희대학교 전자계산소장

불구하고 군사적 목적외에도 많은 연구가 진행되지 않아 음성정보의 보호기술이 상당히 뒤떨어져 있는 실정이다. 또한 화상 정보도 정보화 사회로의 발전과 더불어 보안성 요구가 점차 증대하고 있으므로 그에 발맞추어 음성 및 화상 정보의 암호화 기술에 대한 연구가 매우 필요한 실정이다.

공중 전화망(PSTN : public switched telephone network)이나 이동 통신망(mobile telephone system)에서의 음성 비화는 그 네트워크 특성에 따라 디지탈 또는 아날로그 방식으로 이루어진다. 음성의 디지탈 비화방식은 디지탈 음성 부호화기의 디지탈 정보열을 섞음으로써 간단히 구현된다. 음성정보를 압축하는 방식에는 파형 부호화(waveform coding)과 원시 부호화(source coding) 방식이 있는데, 전자의 예로는 시간축상의 음성 신호를 그대로 압축하는 기법으로 PCM(pulse code modulation), ADPCM(adaptive differential pulse code modulation), ADM(adaptive delta modulation)등이 있다. 후자의 예로는 인간의 발성기관의 발성과정을 모델화하고 음성신호를 그 모델로 모델링하여 특징을 추출하는 기법으로 선형 예측 부호화(linear predictive coding, line spectrum pair, code excited linear prediction, vector sum excited linear prediction) 등이 있다. 지금까지의 기술 수준에서 중속도(16 Kbps) 이상에서는 파형 코더(waveform coder)를 사용하나, 저속도(8 Kbps 이하)에서는 원시 코딩(source coding) 기법이 음질이 훨씬 좋기 때문에 저속도 보코더로 사용된다[2),3)]. 그러나 아날로그 전화채널용 비화방식에 있어서는 아직까지 저속도 보코더의 음질 수준이 충분히 좋지는 않으므로 디지탈 비화기법 보다는 실시간 처리를 위해서 다소 복잡한 하드웨어가 요구되지만 음질이 양호한 아날로그 비화방식이 아직은 유효한 것으로 알려지고 있다[7)].

아날로그 음성 비화기법 중에서 FFT(Fast Fourier Transform) 비화방식은 매우 효과적이고, 음질도 상당히 좋으나 비도가 매우 낮아서 기밀 유지가 어렵다. 이러한 문제를 극복하기 위하여 기본적인 FFT 비화방식에 잡음에 해당하는 의사스펙트럼을 삽입하거나 특정 대역의 스펙트럼 크기를 변형하는 등의 비화 방식들이 제안되었다.

한편 위성 TV나 CATV에서의 비디오 및 오디오 정보에 대한 비화 방식에 대해서도 많은 연구가 이루어지고 있다. 첨단 복합 기술의 전략적인 확보라는 측면과 제2세대 무궁화 위성의 자체 개발능력의 배양외에도 세계적인 추세로 보아 위성에 의한 통신, 방송사업은 급속적으로 확산되고 있는데 이동통신 수요가 증가하고 개인 휴대통신이 일반화되면 위성에 의한 이동통신이 도입될 전망이다. 이에따른 개인 정보의 보호측면과 권한이 없는 사용자의 TV 수신을 효과적으로 방지하기 위한 대책이 절실히 필요하다. 위성통신은 beam coverage가 넓은 관계로 도청에 대한 위협이 가장 큰 통신 수단이다. 위성신호의 불법적인 도청을 방지하기 위하여 위성과 지구국 사이의 선로가 보호되지 않는다면 위성통신 사용자들에 대한 이용 저해요인으로 작용할 것이며 통신망 전반에 걸친 신뢰감을 저하시킬 것이다.

한편 CATV는 동축, 광 케이블 등과 같은 광대역을 전송할 수 있는 전송매체 케이블을 이용하여 음성, 오디오, 비디오 등의 정보를 가입자에게 전송하는 시스템이며 공중선전파에 의한 TV방송에 대응하여 케이블을 이용한 TV방송이라는 의미인데 CABLE TELEVISION의 약어로써 사용되고 있다. 광대역 CATV는 1채널의 TV방송만을 하는 기존의 방송에 비하여 하나의 케이블로 동시에 수십채널의 TV방송을 할 수 있다는 광대역 전송 능력과 쌍방향 정보통신이 가능하다는 특성을 갖고 있다. 우리나라는 1961년 8월에 유선방송 송수신 관리법을 제정 공포한 이후 단지 기존 TV의 프로그램을 재송신하거나 흥미위주의 비디오를 방송해주는 형태로만 발전해 왔다. 그러나 광대역 CATV는 2000년대 정보화 사회의 중추적 매체로써 뿐만 아니라 기술개발 측면의 파급효과와 관련 산업분야의 잠재적 수익성이 매우 높다는 점에서 관심의 대상이 되었으며 부당 사용자들의 불법 이용을 방지하기 위한 대책도 함께 대두되었다. 이에 본고에서는 가입자가 채널을 선택하고 interactive하게 사용할 수 있는 위성 TV 및 CATV에서의 오디오 및 비디오 정보비화 기법에 대해 고찰한다.

서론에 이어 2장에서는 아날로그 음성 신호의 비

화기법에 대한 방식을 소개하고, 또한 3장에서는 위성TV 및 CATV에서의 비디오 및 오디오 신호의 비화기법에 대해 설명하여 마지막으로 4장에서 결론을 맺는다.

2. 아날로그 음성 비화 방식

음성 신호의 비화방식은 다음의 두가지 분류로 나누어진다[2].

○ 아날로그 scrambling

○ 디지탈 encryption

아날로그 비화방식이 그림 1과 2에 나타나 있는데 두 방법의 차이는 실질적으로 비화되는 신호 형식의 차이이다. 디지탈 신호처리가 없는 그림 1의 아날로그 비화기에서는 전체 과정동안 신호는 아날로그 형태를 유지하는데 비해 디지탈 신호처리가 있는 그림 2의 아날로그 비화기에서는 신호가 비화되기 전에 디지탈 형태로 변환되며 전송시에는 다시 아날로그 신호로 재변환된다. 이 방식은 현재 대부분의 복잡한 비화 방식에서 이용되고 있다.

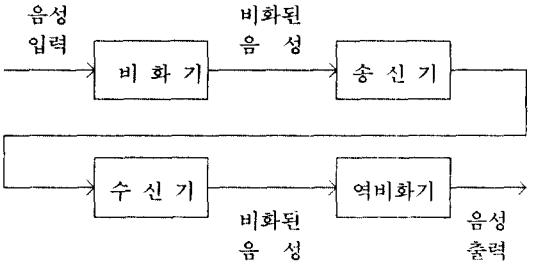


그림 1. 아날로그 음성 비화 방식
(디지탈 신호처리가 없는 경우)

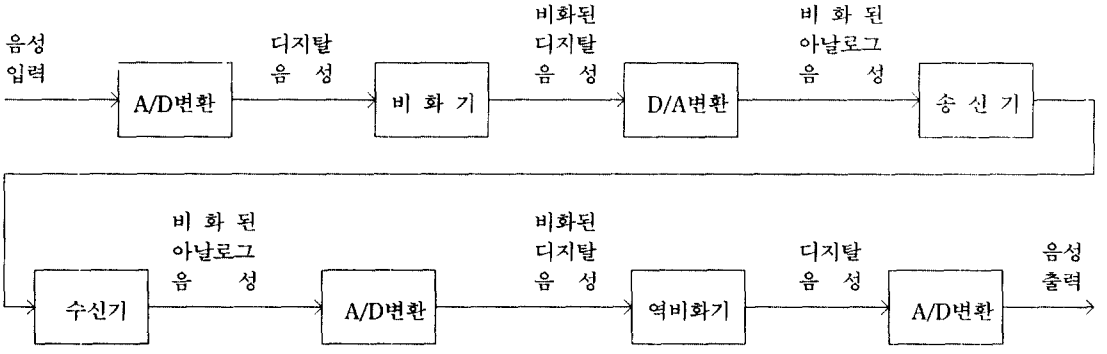


그림 2. 아날로그 음성 비화 방식(디지탈 신호처리가 포함된 경우)

디지탈 비화 방식은 그림 3에 나타나 있는데 앞서의 아날로그 비화방식과의 기본적인 차이점은 디지탈 음성부호화기의 디지탈 비트열이 섞인후에 디지탈 형태로 정보가 전송된다는 점이다.

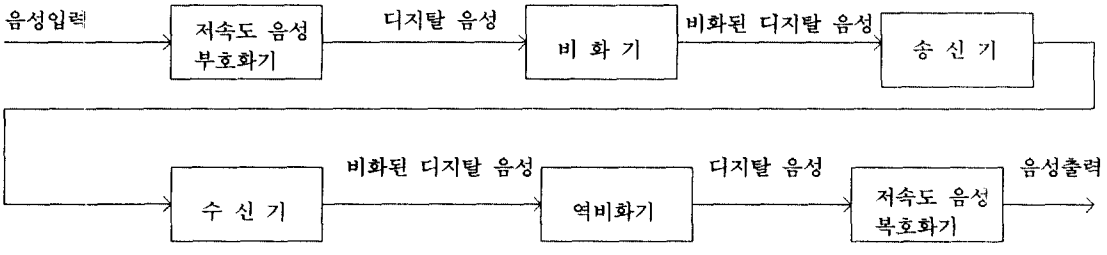


그림 3. 디지탈 음성 비화 방식

이제 여러가지 비화기법에 대해서 고찰해 보고 그것들의 구현 방안에 대해 살펴보기로 한다.

2.1. 주파수 영역 비화방식[3)]

(1) 주파수 역변환(Frequency inverters)

비화레벨이 매우 낮음에도 불구하고 주파수 역변환은 오랫동안 사용되어 왔다. 주파수 역변환은 신호의 주파수 성분 중에서 저 주파수는 고 주파수 부분으로 이동시키고 고 주파수들은 저 주파수영역(lower band)으로 이동시키는 기법인데 300~3000 Hz의 신호가 있을때 비화하기전의 신호와 비화된 신호가 그림 4에 잘 나타나 있다.

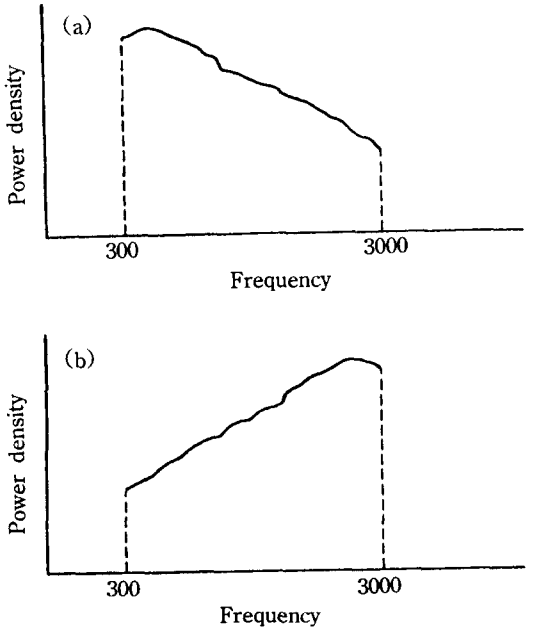


그림 4. 주파수 역변환 (a) 원래의 신호
(b) 주파수 역변환 후의 신호

(2) 대역-천이 역변환(Band-shift inverters)

대역-천이 역변환(band-shift inverter)은 주파수 역변환에 기반을 두고 있다. 300~3000Hz의 신호 대역에 대한 역변환 신호에서 역변환 신호가 원래 신호와 같은 대역에 있다면 전송 주파수는 3300Hz가 되어야 한다. 만일 전송 주파수를 4000Hz로 놓는다면 다음 그림 5(a)와 같은 역변환 신호의 스펙트럼을 얻을 수 있다. 이 역변환된 신호는 원래 신호와 대역이 같지 않게 되지만 3000Hz 이상의 신호를 저 주파수 대역으로 옮기면 원래의 신호와 같은 대역을 갖게 된다. 그 결과는 그림 5(b)와 같으며 이것이 대역-천이 역변환의 주된 개념이다. 일반적으로 (3300 + f)의 전송 주파수를 사용할 때 대역-천이 역변환 신호는 그림 5(c)에서와 같이 나타난다.

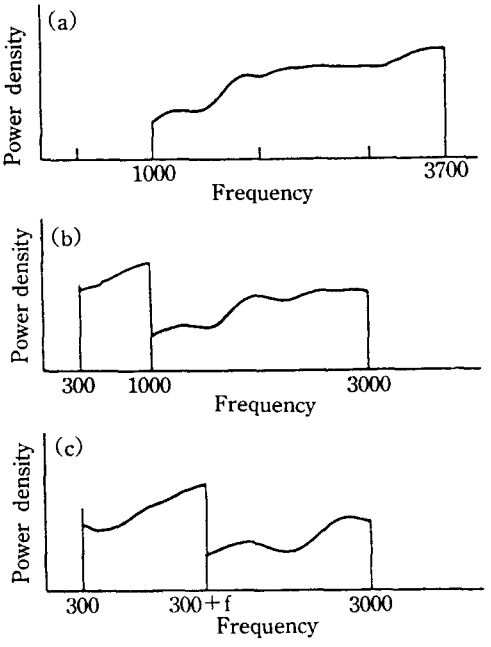


그림 5. 대역-천이 역변환
(a) 4000Hz의 전송 주파수를 사용했을때 주파수 역변환
(b) 4000Hz의 전송 주파수를 사용했을때 대역-천이 역변환
(c) (3300 + f)Hz의 전송 주파수를 사용했을때 대역-천이 역변환

(3) 대역 분할(Bandsplitters)기법

대역 비화방식(bandscrambler)이라고도 불리는 대역 분할(bandsplitter)기법은 현재 사용되고 있는 중요한 비화기법으로서 이 기법은 스펙트럼을 sub-bands로 나누고 각 sub-bands들을 재정렬하여 비

화를 수행한다. 좀더 복잡한 시스템에서는 몇몇 sub-bands들을 역변환시키기도 하는데 5개의 sub-bands를 가진 비화방식의 간단한 예가 그림 6에 나타나있다. 이 경우에 가능한 재순서(reordering) 수는 5 ! 이고 sub-bands의 역변환 가지수는 2^5이므로 결국 가능한 sub-bands의 재정렬(rearranging) 방법은 5 ! × 2^5 = 3840가지이다. 일반적인 식으로 나타내면 임의의 스펙트럼이 m개의 sub-bands로 나누어질 수 있을때 가능한 재정렬 수는 (m !) × 2^m이 될 것이다.

한편 5-band bandsplitter의 구현 예가 그림 7에 나타나 있다.

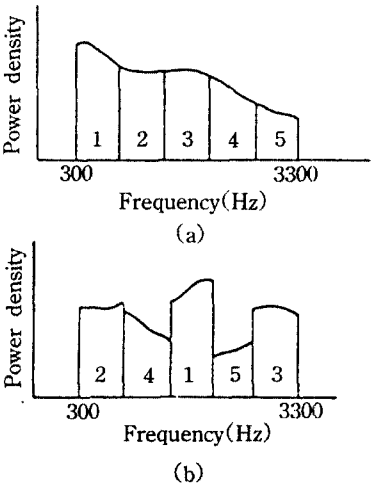
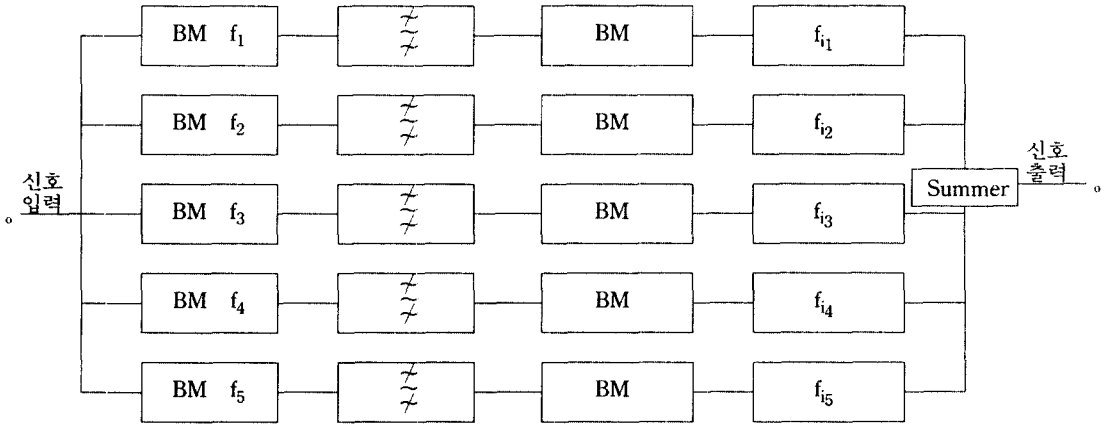


그림 6. Bandsplitter (a) sub-bands의 원래 순서 (b) scrambled 스펙트럼

(4) FFT 사용 기법

(가) 기본적인 FFT 비화 방식

아날로그 음성 비화방식 중 FFT 비화방식은 매우



(BM : balanced modulator, f_i : 전송 주파수)

그림 7. bandsplitter의 구현

효과적이고 음질도 상당히 좋은 기법이지만 비도가 낮아서 기밀 유지가 어렵다는 문제를 가지고 있다. 이런 단점을 해결하기 위한 방안으로 기본적인 FFT 비화방식에 의사 스펙트럼을 삽입하거나 특정 대역의 스펙트럼 크기를 변형하는 등의 여러 비화방식들이 제안되었다.

기본적인 FFT 비화 방식의 동작 과정은 다음과 같다. 전송측 즉 비화를 수행하는 측에서는 입력되는 음성 신호를 ADC(analong-to-digital converter)를 통하여 디지탈 신호로 변환하고 이 신호를 FFT 기법을 이용하여 주파수 영역으로 전환한다. 이 변환된 신호를 스펙트럼이라 부르는데, 스펙트럼을 나타내는 계수(FFT coefficient)들을 주어진 암호 key에 의해 섞게 된다. 이와같이 섞인 스펙트럼 계수들은

IFFT(Inverse Fast Fourier Transform)를 통해서 시간 영역의 디지탈 신호로 전환된다. 계속해서 이 디지탈 신호를 DAC(digital-to-analog converter)를 통하여 아날로그 신호로 변환한 후에, 상대편으로 전송한다. 수신하는 측에서는 비화과정과 역순으로 처리가 진행되는데 스펙트럼의 계수들이 암호화 키(key)에 의해 재정렬되어 복원된 음성 신호를 얻게 된다. 이 기본적인 FFT 비화방식이 그림 8에 나타나 있다.

이 기본적인 FFT 비화방식의 근간이 되는 개념은 시간 영역에서 음성 신호를 섞는 것 보다는 주파수 영역에서의 스펙트럼 계수를 섞는 것이 비도 측면에서 상당히 효과적이라는 사실에 기인한 것이다. 즉, 시간 영역의 음성신호는 이웃하는 신호와의 상관도(correlation)가 매우 높기 때문에 단순히 신호들을 재배치하는 것으로는 섞는 효과가 충분히 나타나지 않는다.

그러나 스펙트럼 계수들의 재배치도 일정 구간내에서 이루어지고, 시간축상의 음성 신호 보다는 상관도가 낮지만 permutation 방식이 무작위하게 이루어지기 때문에 원래 음성신호의 정보가 상당히 남아 있게 된다. 이는 해독자에게 비화된 음성을 해독할 수 있는 정보를 제공하므로 비교적 용이하게 해독되는 단점이 있다. 따라서 지금까지 기본적인 FFT 비화방식의 비도를 높이기 위하여 여러가지 알고리즘이 연구되어 왔고 제안되었는데, 어느정도의 비도를 향상시킨 대표적인 알고리즘이 의사 잡음 삽입 알고리즘이다.

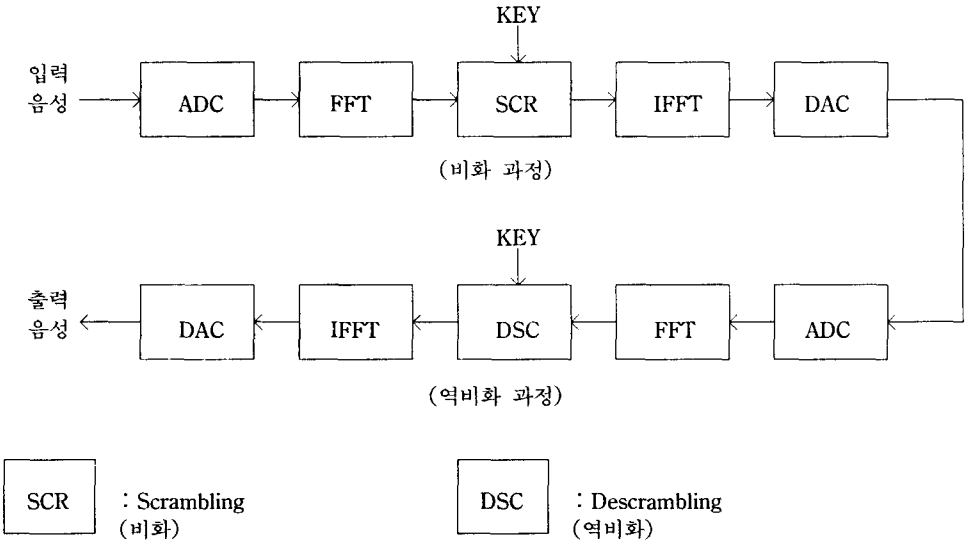


그림 8. 기본적인 FFT 비화방식

(나) 의사 잡음 삽입 알고리즘

스펙트럼의 계수들의 재배치 처리 이전에 잡음에 해당하는 스펙트럼을 삽입하는 방식으로, 재배치의 효과를 높임으로써 높은 수준의 비도를 확보하는 알고리즘이다. 이때 삽입하는 위치와 삽입 형태에 따라 여러가지 알고리즘이 제안되어 왔다. 또한 스펙트럼외에 시간축상의 음성신호에 임의의 잡음을 삽입하는 알고리즘도 제안되었다. 일반적으로 삽입하는 위치는 묵음구간에 해당하는 주파수 대역 또는 시간축 상의 대역으로 정해지고, 역비화 과정에서 삽입 위치를 검출하여 제거하는 것이 기본적인 원리이다. 이러한 잡음 삽입 알고리즘중에서 비교적 효과적이고 간단한 의사 잡음 삽입 알고리즘은 다음과 같다.

의사 잡음 삽입방식은 스펙트럼 계수들을 몇개의 블록으로 나누고, 각 블록의 에너지가 현저히 적은

블록을 삽입 위치로 정하여 특정 형태의 블록을 기존 블록과 대치 삽입하는 알고리즘이다. 이때 삽입하는 위치를 수신측 즉, 역비화 과정에서 정확히 검출해야 되는데 삽입하는 패턴을 임의로 하면 삽입 위치 정보를 음성신호와 함께 전송해야 된다. 이러한 문제를 피하기 위해 동일 패턴을 삽입하고 수신측에서 이 패턴을 검출함으로써 위치 정보의 별도 전송 없이 삽입 블록을 제거한다. 이 더미 스펙트럼(dummy spectrum) 삽입 방식이 그림 9에 나타나 있다. 그러나 이 방식의 복원된 음성 신호의 음질은 기본적 FFT 비화 방식에 비해 현저히 저하되고, 변환(transform)이 적용된 구간 경계에서의 edge effect 때문에 클릭(click) 음이 생성된다. 또한 비도를 좀더 높이기 위하여서는 삽입 블록이 많아지도록 삽입 위치를 정하는 임계값을 낮추어야 하는데 이 경우 복원된 음질의 현격한 저하를 초래한다.

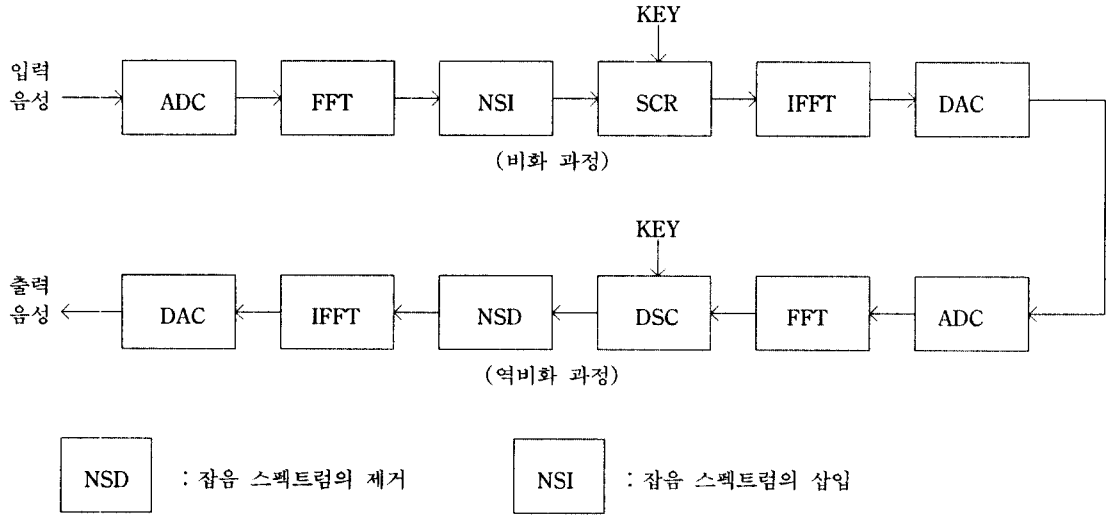


그림 9. 의사 잡음 삽입방식

(다) 개선된 FFT 비화 알고리즘[7]

의사 잡음 삽입 방식을 부가한 기존의 FFT 비화 방식의 성능을 향상시키기 위하여 기본적인 FFT 비화방식에 pre/post 필터링과 해밍 윈도우(hamming window) 및 적응 의사 스펙트럼의 삽입을 추가한 새로운 알고리즘이 제안되었는데 제안된 알고리즘의 전체 블록도는 그림 10과 같다.

① Pre/Post filtering(preemphasis와 deemphasis)

음성신호의 유성음은 저주파수 대역에 대부분의 에너지가 몰려 있는데 비해 묵음과 무성음 신호는 비교적 주파수 전대역에 걸쳐 고르게 에너지가 분포하게 된다. 이러한 현상은 유성음의 경우 입술의 방사와 성문 모양의 효과에 기인하는 것으로 주파수가 증가함에 따라 약 6dB의 기울기를 갖고 에너지가 감소하는 특성을 지닌다. 이러한 특징은 비화 알고리즘의 섞는 효과를 반감시켜 비도를 저하시키는 한 요인이 된다. 따라서 비도를 향상시키기 위해서는 스펙트럼의 형태를 섞기전에 평활화하는 것이 필요하다. 이러한 평활화는 preemphasis 필터를 통해서 구현이 가능하고 그 원리는 식(1)과 같이 시간축상의 함수로 간단히 나타낼 수 있다.

$$\hat{s}[n] = s[n] - 0.95 \times s[n-1] \qquad (1)$$

여기서 $\hat{s}[n]$은 필터링된 음성 신호이고, $s[n]$은 원래의 음성 신호이다. 이렇게 필터링된 음성 신호는 수신측에서 역비화 과정의 맨끝 부분 즉 아날로그 신호로의 변환 직전에 deemphasis filtering을 거침

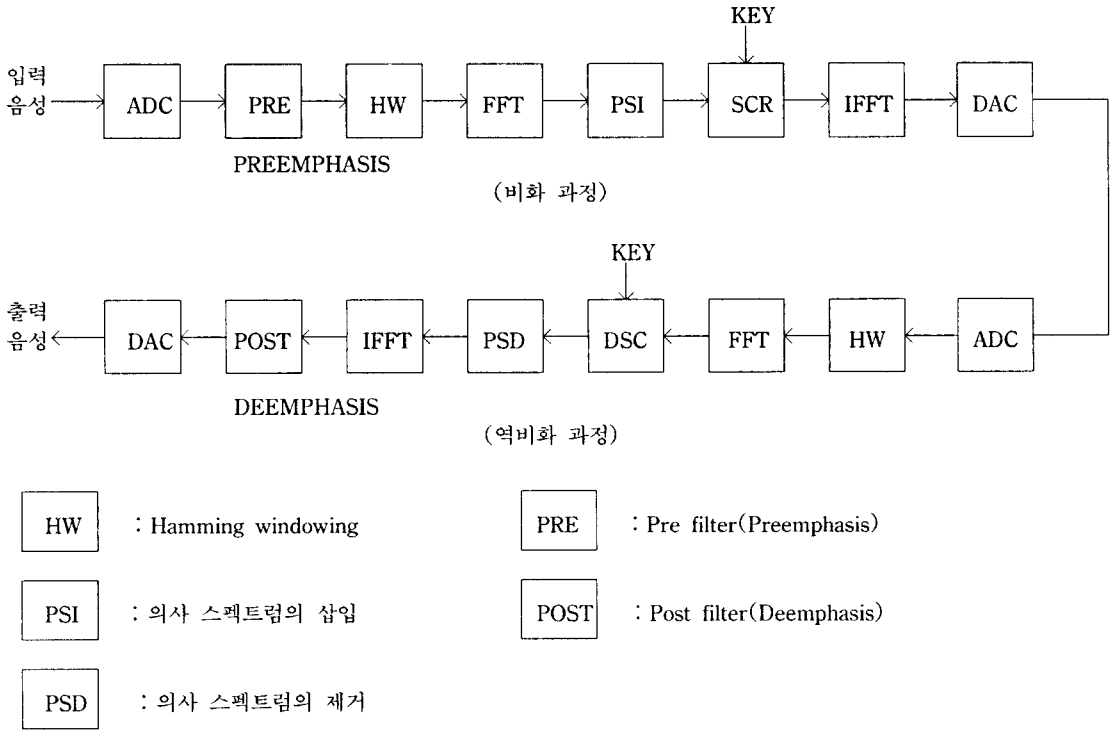


그림 10. 제안한 비화기의 블록도

으로써 preemphasis 필터 효과가 제거된다. 이때 Deemphasis filtering에 관한 수식은 아래 식 (2)와 같이 표시된다.

$$s[n] = \hat{s}[n] + 0.95 \times s[n-1] \quad (2)$$

여기서 비화의 주된 개념은 스펙트럼의 계수들을 섞는 방식(block cipher)이나 음성신호의 전송이 실시간에 이루어져야 한다는 점이다. 이러한 제약 조건은 한번에 섞는 단위에 제한을 두게 되는데, 보통 수십 msec 단위로 스펙트럼의 계수를 구하고 섞게 된다. 이와같이 단위(frame) 마다 비화 처리를 행하기 위해 FFT를 수행하여 스펙트럼을 구하고 그 계수들을 섞고, 다시 IFFT를 이용하여 시간축상의 데이타를 얻는다. 또한 수신측의 역비화 과정도 마찬가지로 프레임마다 처리를 행하게 되는데 이러한 프레임마다의 처리과정은 프레임사이에서 일어나는 edge effect를 유발하여 복원된 음성신호의 음질 저하를 초래한다. 이를 SNR 척도를 이용하여 정량적으로 측정하면 미약한 값의 저하로 나타나지만 실제의 청취 실험에서는 단위 주기의 클릭음이 현저하게 들린다. 이러한 음질의 왜곡을 어느정도 회복시키기 위하여 일반적으로 대역 통과 필터(band pass filter)를 사용한다. 그러나 여기서 구현한 pre/post filter인 preemphasis와 deemphasis의 처리 효과가 대역 필터 역할을 거의 수행하기 때문에 복원 음성의 음질 향상을 위해 별도의 대역 필터를 필요로 하지 않는 장점이 있다. 즉 pre/post filter는 복원음성의 음질 향상에 상당히 기여함을 알 수 있다.

② 해밍 윈도우(Hamming window)

기존의 FFT 비화기는 일정 구간의 단위마다의 처리를 위해 구형(rectangular) 윈도우 기법을 채택하는데 이는 복원 음성의 음질을 저하시킨다. 여기서 음질 저하가 발생함에도 불구하고 다른 윈도우 기법을 채택하지 않는 것은 계산량이 비교적 적게 되어 실시간 구현이 가능하기 때문이다. 그러나 급

격한 마이크로 회로의 발달로 다른 윈도우 기법의 처리도 간단히 실시간으로 구현할 수 있기 때문에 음질향상을 위해서 구형 윈도우 기법 대신에 해밍 윈도우 기법을 채택한다.

이 해밍 윈도우는 구형 윈도우 기법에 비하여 계산량은 증가하나 edge effect가 감소하고, 실제의 전송 라인상의 에러에 대하여 내구성을 향상시킨다. 즉 인접하는 단위간의 연결이 해밍 윈도우의 중첩 효과에 의해 좋아지고, 가중치 효과에 따라 국부적인 에러를 윈도우 전구간으로 smoothing하여 내구성을 향상시킨다. 이때 한 프레임의 길이를 10msec로 하고, 윈도우의 길이를 30msec, 즉 3개의 프레임으로 하며 한 프레임씩 움직이는 슬라이딩 윈도우(sliding windowing) 기법을 채택한다. 여기서 해당 주기의 시간축상의 데이타 수와 FFT 변환기법에 의한 데이타 수가 달라지게 되는데 이는 overlap addition method로 해결한다.

③ 적응 의사 스펙트럼 삽입

의사 스펙트럼 삽입의 목적은 스펙트럼의 계수들을 섞기전에 원래의 음성 스펙트럼의 형태를 변환시켜 비음성 형태를 갖게 함으로써 섞는 효과를 향상시키고, 해독자가 해독시 이미 알고 있는 음성 스펙트럼의 형태 정보를 무력화하는 것이다. 의사 스펙트럼의 삽입에는 그 삽입 위치와 삽입하는 형태에 따라 기법이 다양하고, 그 효과가 상당히 달라지게 된다. 여기서 삽입위치와 삽입 형태는 다음과 같이 결정한다.

㉠ 삽입 위치 결정 알고리즘

먼저 삽입 위치는 한단위를 연속되는 블록으로 나누고, 각 블록을 의사 스펙트럼으로 대치 삽입할 것인가를 판단하여 삽입이 결정된 블록의 위치로 정한다. 이때의 한 블록의 길이는 5~6개의 스펙트럼 계수를 갖도록 한다. 삽입을 결정하는 방식은 각각의 블록의 에너지를 계산하고, 각 블록의 에너지를 프레임의 블록 중에서 최대 에너지를 갖는 블록의 에너지와 비교한다. 이때 에너지의 비가 일정 수준이하가 되는 블록을 대체하여 삽입할 블록으로 정하고, 그 위치를 삽입 위치로 한다. 에너지 비교치인 E_r을 구하는 식은 아래 식 (3)과 같다.

$$E_r = 20 \times \log_{10}\left(\frac{\text{segment energy}}{\text{max. segment energy}}\right) \quad (3)$$

이러한 기준을 음성 신호 전구간에 대하여 적용하면 음성이 존재하는 구간과는 달리 묵음의 구간에서는 삽입이 음성구간과는 뚜렷이 구분되게 결정되어 음성구간을 판별할 수 있는 정보가 남게된다. 이는 해독자에게 음절적 분석 정보를 제공함으로써 비도가 떨어지게 된다. 따라서 묵음 구간에서의 삽입 위치 결정 알고리즘을 별도로 설정하여 비화 후의 음성 신호에서 음절적 구별 정보를 제거한다. 즉 먼저 음성 구간과 묵음 구간을 각 블록의 절대 에너지로 판단하고, 묵음 구간으로 판단되는 블록은 에너지 비교치와는 상관없이 대체 삽입함으로써 음성 구간과 구별할 수 없도록 하는 것이다. 여기에서는 음성 신호를 12bit 크기의 8KHz 샘플링 데이타 80개(10 msec) 음성신호를 256개의 FFT 계수로 변환하여 한 프레임으로 하고, 그 프레임을 연속되는 5개의 계수들의 길이를 갖도록 52개의 블록을 만든다. 이러한 환경에서 반복적인 실험을 거쳐 묵음 구간과 음성 구간에 있어서의 삽입 위치 결정에 필요한 임계값이 표 1에 나타나 있다. 표에 나타낸 묵음 구간에 대한 임계값은 최대값을 1로 정규화한 경우의 절대값으로 임계값 이하인 에너지는 묵음 구간으로 분류한다.

표 1. 임계값

종 류	값
THD(음성)	-15 dB
THD(묵음)	0.05

㉡ 삽입 스펙트럼의 형태

의사 스펙트럼의 형태를 결정하는 것은 비도를 향상 시키는 것 뿐만이 아니라, 수신측의 삽입 위치 검출에 있어서도 매우 중요하다. 먼저 비도를 높이기 위해서는 비화된 신호가 비음성 형태이며 평활화가 잘 되어야 한다. 이는 삽입하는 스펙트럼은 음성의 스펙트럼의 형태를 갖는 의사 스펙트럼이 되어야 하고, 또한 단위내에서 최대 에너지를 갖는 블록의 에너지를 가져야함을 의미한다. 따라서 음성신호의

특정 부분(유성 모음의 최대 에너지를 함유하는 부분)의 스펙트럼의 형태를 삽입 형태로 정하고, 그 크기는 단위마다의 최대 에너지와 같도록 적응한 형태의 스펙트럼을 삽입하는 것이다. 그러나 묵음 구간에서는 원래 신호의 에너지가 상대적으로 매우 작기 때문에 해당 단위에 적응하는 크기를 적용하면 삽입되는 스펙트럼도 작게된다. 이것은 음성 구간과 묵음 구간의 변별적 정보가 되므로 묵음 구간에서는 자체 크기에 적응시키지 않고 묵음 구간의 앞에오는 음성 구간의 크기에 적용한다. 또한 의사 스펙트럼이 음성 스펙트럼과 유사하기 때문에 수신측에서 삽입 위치를 검출하기가 매우 어려워 송신측에서 비화된 음성 신호와 함께 삽입 위치 정보를 전송해야 한다.

그러나 이 경우 삽입 위치 정보의 누출 위험이 따를 뿐만이 아니라 별도의 전송 채널등을 필요로 하기 때문에 복잡도가 증가한다. 이러한 정보 누출과 복잡도의 증가를 피하기 위하여 삽입 패턴을 특정화 한다. 즉 수신측에서 삽입 위치 정보의 수신없이도 용이하게 삽입 위치를 검출할 수 있도록 하는 것이다. 음성 종류에 따라 적응되는 특성을 살리기 위하여 크기는 위에서 언급한 적응 형태로 유지하고 위상을 나타내는 데이타로 특정화를 수행한다.

일반적인 음성 신호의 위상은 부호의 측면에서 전체적으로 균형을 이루고 있기 때문에 삽입하는 의사 스펙트럼의 위상이 항상 음 또는 양의 부호만 갖게되면 삽입 블록의 갯수가 추정될 수 있다. 이러한 삽입 정보가 비화 신호에 남지 않도록 삽입되는 스펙트럼의 위상부호를 음과 양으로 번갈아 삽입한다. 이는 수신측에서 역비화를 수행한 후에 스펙트럼상에서 쉽게 삽입 의사 스펙트럼을 검출하여 삽입 의사 스펙트럼의 제거를 용이하게 하며 해독자에게는, 역비화 되지 않은 스펙트럼 상에서 삽입 위치 추정을 불가능하게 한다.

2.2. 시간 영역 비화 방식[3)]

시간 영역 비화방식은 크게 3가지의 범주로 나누어질 수 있다.

- Reversed time segmentation
- Time element 비화방식
  - hopping window
  - sliding window
- Time sample 비화방식

(1) Reversed time segmentation

Reversed time segmentation기법은 매우 낮은 비도를 갖고 있으며 결과적으로 단순한 음성 보호 기법으로 간주되는 방식이다. 그러나 이 기법은 마이크로프로세서를 가지고 쉽게 구현이 되며 단순하고 가격이 저렴하므로 많이 적용되고 있다.

Reversed time segmentation기법의 첫번째 단계에서 아날로그 신호는 샘플링되고 이 샘플들은 time 세그먼트들로 나누어지며 메모리에 저장된다. 각 세그먼트에 들어있는 샘플들은 reverse temporal 순서에 의해 비화된 후에 D/A 컨버터에 전달된다. 1~6의 time 세그먼트를 가진 전형적인 시스템이 그림 11에 나타나 있다. 한편 그림 12는 N개의 샘플들을 가진 각 세그먼트에서 샘플들의 마지막 순서(order)를 보여준다. 전형적으로 time 세그먼트의 기간은 50~400msec 사이이며, 그림에서와 같이 긴 time 세그먼트는 긴 지연 시간을 초래하지만 더 낮은 residual intelligibility를 갖는다.

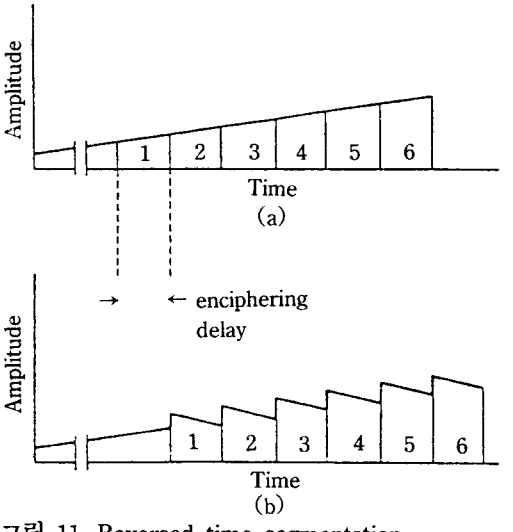


그림 11. Reversed time segmentation
(a) 원래 음성 신호 (b) 비화된 음성신호

원래 샘플 순서 ...A_{11}.....A_{1N} A_{21}.....A_{2N} A_{31}.....A_{3N} A_{41}.....A_{4N}

→ ← 암호화 지연(enciphered delay)

마지막 샘플 순서 .....A_{1N}.....A_{11} A_{2N}.....A_{21} A_{3N}.....A_{31} A_{4N}

그림 12. Reversed time segmentation을 위한 샘플들의 재정렬(reordering)

(2) 시간요소 비화방식(time element scrambling)

앞서 살펴본 대역 분할방식 (bandsplitting)과 유사한 개념으로써 이 기법은 종종 시간 영역 다중화 (TDM : time division multiplexing) 또는 TSP (time segment permutation)이라 부르기도 한다. 이 기법의 목적은 음성 신호의 time 세그먼트 번호를 섞는 것이며 hopping(fixed) 윈도우와 슬라이딩 윈도우 기법의 두가지 종류가 있다.

(가) 호핑 윈도우(Hopping window)기법

이 기법에서 아날로그 신호는 프레임(frame)이라 불리는 등간격의 시간구간(time periods)으로 나누어지고 각 프레임은 다시 세그먼트(segments)라 불리는 등간격의 작은 시간 간격으로 나누어진다. 입력된 아날로그 신호는 각 프레임내의 세그먼트를 permuting하므로써 비화를 행하는데 8개의 세그먼트로 프레임을 나누었을때의 예가 그림 13에 나타나 있다.

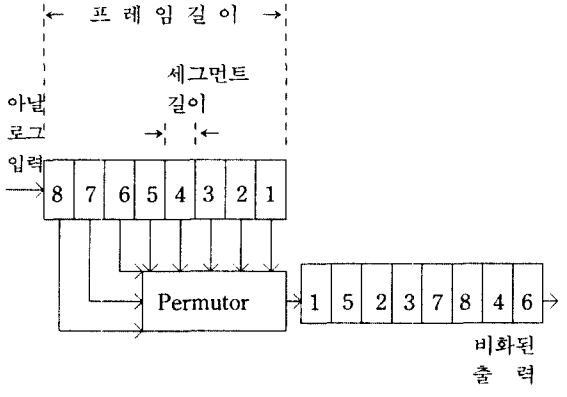


그림 13. Hopping window기법

(나) 슬라이딩 윈도우(Sliding window)기법

슬라이딩 윈도우 기법은 어떠한 순간에도 store에 있는 모든 세그먼트를 평균적으로 같게 한다. 예를 들어, 임의 시간에 시간지연을 초과하지 않도로 하는 제한을 부가한다면 스토어의 어떠한 element도 선택할 수 있다. 선택된 element는 전송되는 즉시 스토어에서 지워지므로 같은 element가 두 번이상 전송되지는 않는다. 그러나 이 기법은 특정한 스토어는 전혀 엑세스 되지 않을 수도 있다. 즉 특정한 element는 전형 전송되지 않으므로 수신단에서 심각한 문제를 일으킬 수 있는데 이 문제는 각 세그먼트에 최대 지연한계를 두고 이 한계에 도달한 세그먼트는 다시 선택되게 함으로써 피할 수 있다. 그리고 지연한계는 수신단에 존재하는 스토어의 갯수를 고려하여 결정한다.

표 2. 비화 과정의 예

입 력	Storage elements				선택된	출 력
세그먼트	4	3	2	1	스토어	세그먼트
1	–	–	–	1	1	–
2	–	–	2	1	2	–
3	–	3	2	1	3	–
4	4	3	2	1	4	–
5	5	3	2	1	4	4
6	5	3	2	6	1	1
7	5	3	2	7	1	6
8	5	3	8	7	2	2
9	5	9	8	7	3	3
10	5	9	8	10	1	7
11	11	9	8	10	4	5
12	11	9	12	10	2	8
13	11	9	13	10	2	12
14	11	9	14	10	2	13
15	11	9	15	10	2	14
16	11	16	15	10	3	9
17	11	16	15	17	1	10
18	18	16	15	17	4	11
19	18	19	15	17	3	16
20	18	19	20	17	2	15
–	18	19	–	17	2	20
–	–	19	–	17	4	18
–	–	–	–	17	3	19
–	–	–	–	–	1	17

이 기법에서 역비화는 아직 수신되지 않은 메세지를 고려하여 수신된 각 element를 정확한 위치에 재배치하는 역할을 수행하며 역비화기를 통과하는 시간지연은 비화과정에서의 시간지연과 같다. 비화과정과 역비화 과정의 예가 다음 표 2와 3에 나타나 있다.

2.3. 2차원 비화방식과 일반적 구현 기법

지금까지 주파수와 시간 영역에서의 비화 방식에 대해서 살펴보았다. 이에 각 기법의 장단점을 이용하고 그것들을 결합할 수 있는 방법들에 대해 살펴보기로 한다. 주파수 영역 비화방식과 시간 영역 비화방식의 결합형태를 2차원 비화방식(two-dimensional scrambling)이라고 하며 가능한 결합 기법들을 살펴보면 다음과 같다.

표 3. 역비화 과정의 예

입 력	Storage elements				선택된	출 력
세그먼트	4	3	2	1	스토어	세그먼트
4	–	–	–	4	1	–
1	–	–	1	4	2	–
6	–	6	1	4	3	–
2	2	6	1	4	4	–
3	2	6	3	4	2	1
7	7	6	3	4	4	2
5	7	6	5	4	2	3
8	7	6	5	8	1	4
12	7	6	12	8	2	5
13	7	13	12	8	3	6
14	14	13	12	8	4	7
9	14	13	12	9	1	8
10	14	13	12	10	1	9
11	14	13	12	11	1	10
16	14	13	12	16	1	11
15	14	13	15	16	2	12
20	14	20	15	16	3	13
18	18	20	15	16	4	14
19	18	20	19	16	2	15
17	18	20	19	17	1	16
–	18	20	19	–	1	17
–	–	20	19	–	4	18
–	–	20	–	–	2	19
–	–	–	–	–	3	20

○ 시간 요소 비화방식/가변 클럭 속도(Time element scrambling/Varying clock rates)

: 이 방식은 본질적으로 시간 요소 비화방식에 주파수 변조의 형태만 단지 더하는 것이다. 이 과정을 위해서 시간 요소(time element) 비화방식은 아날로그 신호를 디지탈 신호형태로 전환시켜야 한다.

○ 시간 요소 비화방식/주파수 역변환(Time element scrambling/Frequency inversion)

: 시간 요소(time element) 비화방식에 주파수 역변환 기법을 첨가하는 것이다. 여기서 주목할 것은 시간 요소 비화방식은 디지탈 형태의 신호를 생성한다는 것이다.

○ 시간 요소 비화방식/대역 분할(Time element scrambling/bandsplitting)

: 결합기법 중에서 가장 이상적인 방식으로써 hopping 윈도우기법을 사용하는 시간 요소 비화방식과 대역 비화방식(bandscrambler)을 결합한 것이다.

3. 아날로그 비디오 및 오디오 신호의 비화방식

3.1. 비디오 신호 비화방식

TV신호는 비디오와 오디오 신호 요소의 합성으로 구성되는데 비디오 정보의 비화는 신호의 특성을 변화시키는 과정으로써 동기펄스와 같은 신호들이 원래의 위치로부터 제거되고, 천이되는 반면에 비디오 신호는 영향을 받지 않는다. 비디오 신호는 신호 파형의 역변환, 전력 레벨의 천이, 시간에 대한 천이, 간섭신호의 첨가 등의 기법으로 원래의 신호를 변화시킬 수 있다[6]. 한편 비디오 정보의 수요가 증가하고 다양한 cable 채널을 제공하는 CATV(Cable TV)가 가정에 보급되므로써 "pay-TV"의 개념이 나타나게 되었으며, pay-TV회사들은 시청료를 내지 않은 시청자(nonpaying viewers)들의 비인가 수신을 방지하기 위한 방안을 모색하게 되어 비디오 신호의 비화방식이 많이 연구되고 있다[5].

(1) 비디오 역변환(Video inversion)

전체 비디오와 동기 파형을 역변환하는 이 기법은 Cable TV비화 시스템에서 사용하는 방식으로써 케이블 시스템의 효과적인 비화를 제공한다. TV 수신자는 역변환된 비디오 신호를 수신하여 그 신호를 복호화 한다[4].

비디오 역변환 기법을 사용하면 동기 펄스와 화상 정보는 역방향의 형태를 가지며 또한 컬러 burst 정보도 180°위상 천이를 통하여 역변환된다. 비디오 역변환 기법이 그림 14에 나타나 있다.

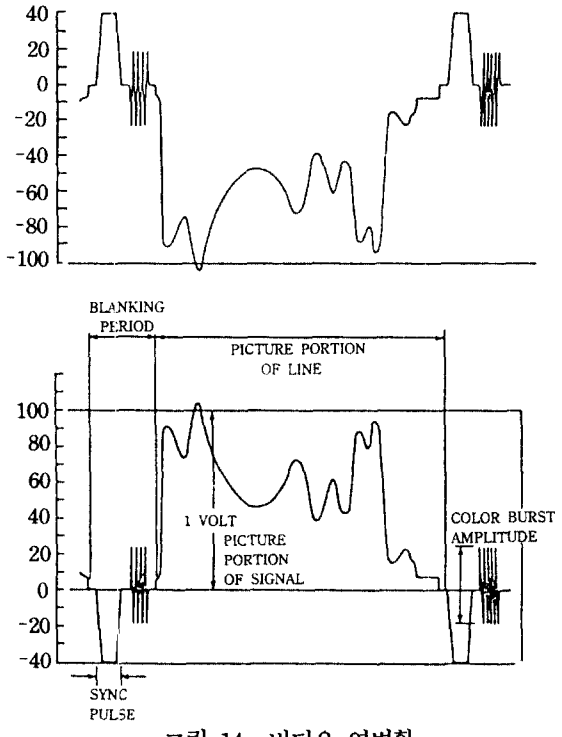


그림 14. 비디오 역변환

(2) 정현파 동기 천이(Sinewave sync shifting)

비디오 신호에 사인파를 첨가(addition)하는 이 기술에는 line frequency 정현파 또는 linewave multiple-frequency 정현파가 첨가된다.

정현파 전압을 신호의 비디오 영역에 삽입하는데 그 결과로 TV 수신자는 동기를 찾을 수 없게 되어 화면이 흐르거나 찌그러지게 된다. 그러나 이 방법은 대역폭이 제한되어 있는 위성방송에서는 효율적인 비화기법이 될 수 없다. 한편 정현파의 첨가로 비디오 신호의 진폭을 증가시키게 되며 overderivation의 원인이 되고 화면의 왜곡을 가져오게 된다.

(3) 펄스 동기 천이(Pulse sync shifting)

동기 펄스를 신호의 비디오 영역에 삽입하는 이 기법은 수평이나 수직 동기에 적용할 수 있다. 정현파 동기 천이 기법과 달리 이 기법에서는 동기 interval만이 영향을 주게된다. 이때 비디오 신호에 더해진 비화 파형과 역비화 파형은 본질적으로 펄스열이다.

이 방식에서는 수평과 수직 동기 펄스는 gating 펄스에 의해 active 비디오 영역으로 천이되며 TV 수신자의 동기 분리 회로 (sync separation circuit)는 동기 정보와 active 비디오 정보를 구별할 수 없게 된다.

(4) 동기 대체(Sync replacement)

수평 또는 수직동기가 비표준 파형으로 대체되는 이 기법은 북미와 유럽에서 많이 사용되어 왔으며, OAK Orion과 Video Cipher II 시스템에서 이용되었다. 동기 정보가 디지탈 데이타에 의해 대체되는 동기 대체 기법의 예가 그림 15에 나타나 있다.

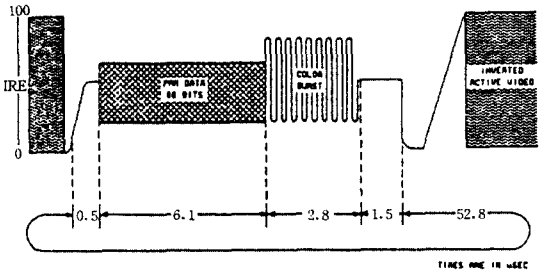


그림 15. 동기 대체(Sync replacement)

(5) 활성 역변환(Active inversion)

비디오 정보의 active 역변환기법인 이 방식은 line-by-line 기반으로 비디오 정보의 비도를 좀더 높이는 방법이다. 몇몇 시스템에서는 비도가 낮은 field-by-field 기반으로 비디오 정보를 역변환시키는 경우도 있다.

Active 역변환 비화기법에는 2가지 형태가 있는데 key와 nokey 형태이다. keyed 역변환은 nokeyed

역변환 기법에 비해 비도가 떨어지고, key는 전형적으로 수평 blanking interval에서 한 펄스인데 이 key는 비디오 신호의 극성을 가리킨다. 한편 nokey 시스템은 line 구조에서 비디오 극성이 나타나지 않는다.

(6) 절단 및 역변환(Cut and invert)

Line video는 여러개의 세그먼트로 나누어지고 비디오의 극성(polarity)은 미리 정렬된 세그먼트 수를 이용하여 역변환된다. 이 기법은 아날로그 회로보다 디지탈 방식에서 구현하기가 적합하기 때문에 많은 유럽의 시스템에서는 디지탈 방식으로 구현하고 있다. 만일 라인당 세그먼트의 수가 결정되어 있다면 역변환 지점은 검출될 수 있을 것이다. 절단 및 역변환 기법의 예가 그림 16에 나타나 있다. 이 기법에서는 역변환된 비디오 신호와 보통 비디오 신호 사이의 전력 차이(offset)로 인한 문제점이 발생할 수 있다.

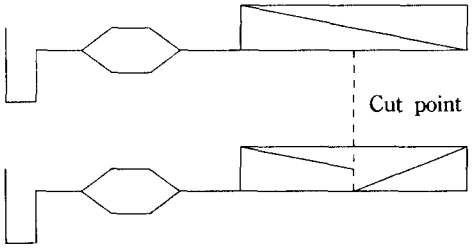


그림 16. 절단 및 역변환(Cut and Invert)

(7) 절단 및 순환(Cut and rotate)

비디오 정보를 미리 정렬된 세그먼트로 분할하고 정해진 cut 지점을 기준으로 하여 비디오 정보를 순환시키는 기법이다. 유럽에서는 매우 효과적인 비화 기법으로 채택하고 있으며 한 라인당 세그먼트의 수는 256으로 나타나 있다. 여기서 cut point는 한 바이트(8 bits)로써 정의된다.

(8) 라인 혼합(Line shuffle)

필드나 프레임에서 라인의 시퀀스를 변경시켜서 결국 라인이 다른 순서로 전송되게 하는 기법인데 예를 들면 라인 15가 라인 211의 위치에서 전송되게 하는 것이다. 이 기법은 좀 더 비도가 높은 비화기법의 한 종류이며 사용자에게 상당한 호감을 갖게 하는 기법이다. 즉 라인 혼합 기법은 비디오 라인의 순서를 재정렬해서 전송하는데 그림 17에 그 과정이 잘 나타나 있다.

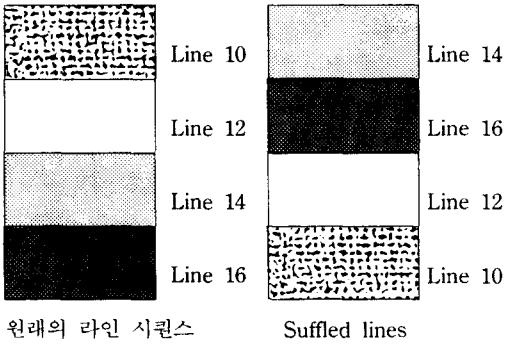


그림 17. 라인 혼합기법(Line shuffle)

3.2. 오디오 신호 비화방식

오디오 신호의 대역폭은 비디오 신호의 대역폭보다 상대적으로 좁다. 초기의 오디오 비화방식은 오디오 정보를 감추기 위해 secondary subcarrier를 삽입하거나 기본 오디오 subcarrier를 고주파로 재변조하는 등의 간단한 기법을 사용하였으나 근래에는 아날로그 오디오 입력을 디지탈 스트림으로 변환시키는 비용이 싸고 고속처리가 가능하며, 비도가 높은 비화기법이 개발되고 있다. 이 디지탈 오디오 신호는 제어 및 주소정보에 섞여서 비디오 신호에 끼워져 전송된다. 오디오 정보는 4.5MHz 신호로 주파수 변조되어 비디오 신호에 더해져서 전송되는데 전송시의 오디오 정보의 전송파는 FM 방송에서 사용되는 ±75KHz 대신에 ±25KHz의 편차한계를 가진다는 조건이외에는 표준 FM 무선신호와 비슷하다. 만일 오디오 신호가 4.5MHz가 아니라면 수신측에서는 소리가 들리지 않든지 단지 랜덤잡음(hiss)만이 들리게 된다.

오디오 신호 비화방식에서 오디오 subcarrier는 화상전송파의 4.5MHz 대역에 위치하고 TV 신호의 주파수 성분과 구별된다. 그림 18에 오디오 인코딩

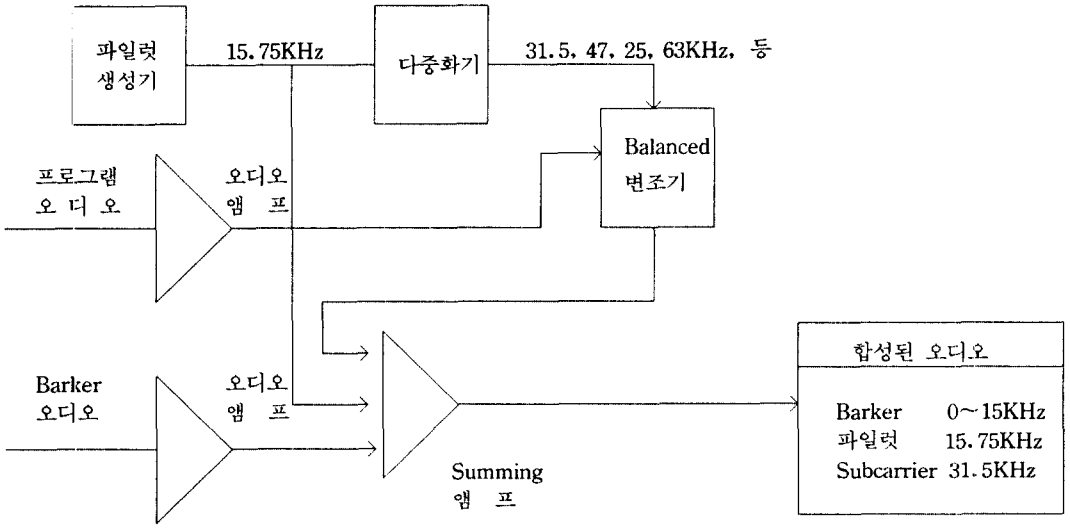


그림 18. 오디오 인코딩-방식 블럭도

방식이 나타나 있다.

(1) FM'd audio

오디오 신호는 30 또는 70KHz를 사용하는 초음파 전송파로 주파수 변조되고 채널 오디오용 0~11KHz 대역은 다른 목적으로 사용되는 이른바 "Barker 채널"에 할당된다. 이러한 형태의 오디어 비화기법은 비인가자의 불법 사용이 쉽기 때문에 비도가 그다지 높지 않으며, 전송 주파수가 알려져 있으면 PLL (phase lock loop) 복조기를 만들어 도청하는 것이 가능하다.

(2) 스펙트럼 역변환(Spectrum inversion)

0~11KHz의 오디오 스펙트럼을 전송 주파수를 기준점으로 하여 저주파수는 고주파수로 바꾸고 고주파수는 저주파수로 바꾼다. 이 기법은 북미와 유럽에서 사용되어온 방법이며 전송 주파수로는 오디오 대역폭 보다 높은 12.5KHz 또는 15KHz 주파수가 사용된다.

4. 결 론

지금까지 아날로그 음성, 비디오 및 오디오 신호의 비화방식에 있어서 비화 신호의 비도를 높이고 복원 신호의 품질을 향상시키기 위해 많은 연구가 수행되어 왔으며 그 결과 여러 비화 알로리즘들이 제안되어 왔다. 이에 본 고에서는 아날로그 음성과 비디오 및 오디오 신호의 비화방식에 대해 고찰해 보았다. 현재 우리나라의 아날로그 신호의 비화 기술은 초보단계이나 아날로그 음성전화의 비화에 대한 사용자 요구와 위성TV 및 CATV의 비화모듈의 수요가 급증할 전망이다. 따라서 아날로그 신호의 비도를 높이고 품질을 향상시키기 위해서 아날로그 음성, 비디오 및 오디오 신호의 비화 방식에 대한 연구가 절실히 필요한 실정이다.

참 고 문 헌

1. Jon E. Natvig, "Evaluation of six Medium Bit-Rate Coders for the Pan-European Digital Mobile Radio Systems", in IEEE Journal on selected Areas in Communications, Vol.6, No.2, pp.324-331. Feb., 1988.

2. Enrico Del Re et al., "A new speech signal scrambling method for secure communications : Theory, Implementation, and Security Evalua-

tion", in Journal on Selected Areas in Communications, Vol.7, No.4, pp.474-480, May 1989.

3. Henry. J. Beker and Fred C. Piper, "Secure Speech Communications", Academic Press, 1985.

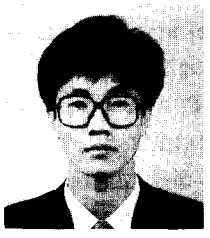
4. F. Baylin et al., "World Satellite TV and Scrambling methods", baylin Publications, pp. 177-187, 1990.

5. Rudolf F. Graf and William Sheets, "Video Scrambling & Descrambling for Staellite & Cable TV", SAMS, pp.1-32, 1987.

6. Brent Gale, Frank Baylin, "Satellite and Cable TV Scrambling and Descrambling", Baylin/Gale Productions, pp.71-92, 1986.

7. 공병구, "아날로그 음성 비화기의 비도 및 음질 향상에 관한 연구", 석사학위 논문, 경희대, 1992.

□ 著者紹介



이 일 우

1992년 2월 경희대학교 공과대학 전자계산공학과 학사
1992년 2월～현재 경희대학교 공과대학 전자계산공학과 대학원
관심분야 : 컴퓨터 네트워크, 이동통신, BISDN, 멀티미디어 통신, 정보통신 보호기법

조 동 호

1979년 2월 서울대학교 공과대학 전자공학과 학사
1981년 2월 한국과학기술원 전기 및 전자공학과 석사
1985년 2월 한국과학기술원 전기 및 전자공학과 박사
1985년 3월～1987년 2월 한국과학기술원 통신공학연구실 선임연구원
1987년 3월～현재 경희대학교 공과대학 전자계산공학과 부교수
1989년 9월～현재 경희대학교 전자계산소장
관심분야 : 컴퓨터 네트워크, 이동통신, BISDN, 멀티미디어 통신, 정보통신 보호기법