비화된 신호 검출 소요 시간을 통한 키의 선택

°김 종현, 박 상규
한양대학교 전자통신공학과

Choice of Scrambling-Key by Measuring the Scrambled Signal Detection Time

°Jong Hyune Kim, Sang Kyu Park
Dept. of Electronic Communication Eng. Hanyang Univ.

요 약 문

본 논문에서는 복호키를 모르는 해독자의 입장에서 주파수 영역 비화 및 시간 영역 비화(의사 난수 치환 방법, 유니폼 치환 방법, 의사난수-유니폼 치환 방법)되어진 미지의 신호를 수신한 후 비화 영역을 판단하는 알고리즘과 원 신호를 검출하는 알고리즘을 제안하였다. 그리고 원 신호 검출 소요 시간을 측정한 후 사용하고자하는 스크램블링 방식에서 적절한 키를 선택하는 방법을 제시하였다.

각 비화 영역 신호의 세기와 3.6KHz 고역 통과 필터링 후의 신호의 세기를 비교·분석한 후 비화 영역을 판단하였으며, 퓨리에 변환 후의 신호의 특성과 영교차점(zero-crossing)을 비교·분석한 후 원 신호를 검출하는 알고리즘을 구현하였다. 그리고 각 영역 비화 신호에 대한 원 신호의 검출 시간을 비교하므로써 7일 동안 보호가 필요한 정보를 비화시키는데 필요한 비화 단위인 블럭의 크기(즉, 키의 크기)를 제안하였다.

제 1 장 서 론

음성 신호를 인가받지 않은 제 3자로부터 정보를 보호하기 위한 비화 방식의 필요성은 유선 및 무선 통신망이 보급되기 시작한 20세기 초부터 크게 인식되어져 왔으며 특히 현대 사회에 있어서 각종 통신망의 확충과 정보기기의 발달에 힘입어 고도의 정보화 사회로 변화되어 감에 따라 정보 교류가 활발해지고 있다. 이에 따라 정보의 교류는 생활의 중요한 부분이 되었으며 정보의 보호대책에 관한 요구가 급증하고 있다. 특히 스크램블링 방식은 구현이 용이하고 처리 시간이 빠르며 전송 대역폭이 확장되지 않는 장점이 있어 위성을 이용한 한정 수신 시스팀등의 상용 시스팀에 사용이 적합하다[1][7][9].

스크램블링 방식을 사용하는데 있어 가장 중요한 과정은 키를 선택하는 과정이며 정보를 보호하고자 하는 시간과 사용하고자 하는 스크램블링 방식에 따라 얼마만큼의 정보량을 가진 키를 선택해야하는지를 선택하는 과정은 필수적이다[1].

따라서 본 논문에서는 원 신호 및 각 비화 신호(시간 영역 비화 신호, 주파수 영역 비화 신호)와 3.6 KHz 고역 통과 필터링 후의 잔여 신호(원 신호, 각 영역 비화 신호)를 비교·분석하여 각 영역에서 비화된 신호를 수신한 후 어느 영역(주파수 영역, 시간 영역)에서 비화되었는가를 결정하는 알고리즘을 제시하였으며 비화 영역이 판단된 신호로부터 원 신호를 찾아내는 알고리즘을 제시하였다. 결론적으로 각 신호에 대해 원 신호를 검출하는 시간을 파라미터로하여 정보를 보호하고자하는 기간 동안의 키를 어떻게 선택해야하는가를 보였다[3][4].

제 2 장 아날로그 음성 신호 비화 기법

음성 신호의 비화는 전송되는 신호를 원래 정보와는 무관하게 만듬으로써 도청자로 하여금 전송

도중 의미 있는 정보를 획득하지 못하게 하는 방법으로 스크램블링 방식과 암호화 방식이 있다. 그 중 본 논문의 연구 대상이 되는 스크램블링 방식은 음성 신호를 여러개의 주파수 성분 또는 시간 성분으로 나눈 후 의사난수 발생기에 의해 각 요소를 변형 또는 자리바꿈을 하여 암호문을 만들어서 도청자로 하여금 이해할 수 없도록 하는 방식이다. 이 방식은 비화 후에도 음성의 고유 성분이 남아 있는 음성 잔여 이해도 때문에 비도를 증진시키는데 한계가 있으나 전송시 전송 대역폭이 확장되지 않고 제작이 간단하여 최근까지도 많이 사용되고 있다[1][8][9].

2.1 주파수 영역 비화 기법

음성 신호 비화 기법 중에서 가장 기본적이고, 간단하여 이해하기 쉽고, 설계하기에 용이한 방식으로 비교적 매우 낮은 비도를 제공하지만, 이 기법은 보다 더 복잡하고, 정교한 시스템에 응용되어지고 있으므로 주파수 영역 비화 기법의 중요성은 계속적으로 강조되고 있다. 주파수 영역 비화 기법에는 주파수 반전(frequency inversion), 대역 천이 반전(band-shift inversion), 그리고 대역 분할 방식(bandsplit)이 있으며 특히 대역 분할 방식은 현재 가장 많이 쓰이는 방식으로 여러 개의 부대역(sub-band)으로 신호의 스펙트럼을 나누어 재배열하므로써 비화 효과를 얻는다[1][9].

2.2 시간 영역 비화 기법

아날로그 음성 신호의 비화를 위해 보다 많은 변형 방법의 가지수를 지닐 수 있는 시간 영역에서 음성신호를 시간 성분으로 나누어 재배열하여 전송하는 방식이며 시간 성분 반전, 시간 요소 비화 방식, 그리고 시간 샘플 비화 방식이 있다.

시간 샘플 스크램블링 방식에는 치환 순서를 결정하는 방법에 따라 의사 난수 치환 방법(pseudorandom permutation), 유니폼 치환 방법(uniform permutation) 그리고 이 두가지 방법을 결합한 의사 난수-유니폼 치환 방법(pseudorandom-uniform permutation)이 있다. 의사 난수 치환 방법은 쉬프트 레지스터의 상태에 따라 치환 순서를 결정하며, 유니폼 치환 방법은 모듈라 개념을 도입하여 치환 순서를 결정하고 의사난수-유니폼 치환 방법은 의사 난수 치환 방법과 유니폼 치환 방법을 결합한 형태로써 키의 가지수를 증가시키고자 개선된 방법이다[2][5][6].

제 3 장 비화 영역 판단과 원 신호 검출

완전한 비도(perfect security)를 보장하는 비화 시스템은 존재하지 않으며, 현재 사용되고 있는 비화 방식들도 송신자와 수신자사이에 완전한 신뢰성을 보장할 수는 없다. 키를 알고 있는 수신자는 송신자가 보내고자하는 정보를 올바르게 수신할 수 있다. 그러나, 해독자는 키를 모르기 때문에 올바른 신호를 검출할 수가 없으며 올바른 신호를 검출한다하여도 많은 시간이 소요된다. 이 장에서는 신호의 동기와 비화 블럭의 크기를 알고있다는 가정하에 복호키를 모르는 해독자의 입장에서 미지의 신호를 수신한 후 듣기 시험이 아닌, 기계 즉 컴퓨터로써 수신한 미지의 신호가 어떤 방식으로 비화되었는지를 밝히는 비화 영역 판단 알고리즘과 원 신호를 검출하는 알고리즘을 구현한다.

3.1 연구 방법과 분석 대상 신호

키를 알지못하는 해독자의 입장에서 전송로상의 미지의 신호를 획득하였을 때에 의미있는 정보를 얻기 위해서는 먼저 미지 신호의 비화 여부를 판단하여야 한다. 듣기 시험을 거치지 않고 동기를 알고 있는 미지 신호의 비화 여부, 비화 영역 판단 그리고 원 신호로의 검출과정을 알아내기 위해서는 원 신호와 비화 신호간의 차이점과 각 영역 비화 신호의 특성을 알아야만 한다. 원 신호 및 각 비화 영역 비화 신호간의 특성을 알아내기 위해서 다음과 같은 연구 방법 및 분석 대상 신호를 선택하였다.

샘플수는 35,000이며 샘플의 크기는 2^{16}인 30대 중반의 남성의 음성 신호(그림 3.1)를 연구의 음성 데이타로 사용하였으며, 원 신호를 각각 2,048개의 샘플로 구성된 18개(신호 0 부터 신호 17)의 부분

신호들로 구분하여 연구를 수행하였다. 이러한 신호들 중 휴지(음성 성분이 거의 없어 신호의 세기가 미약한) 부분에 의한 값들은 음성 전반적인 신호분석에 있어서 별로 중요한 요소가 아니며 음성 신호 그 자체 값들에 비중을 두기 위해서 음성이 어느 정도 포함되었다고 판단되는 세기가 비교적 큰 신호 10개(신호 2, 신호 3, 신호 4, 신호 5, 신호 9, 신호 11, 신호 12, 신호 13, 신호 14, 신호 15)를 취하고 신호의 음성 성분이 거의 없는 나머지 8개의 신호를 무시하였다.

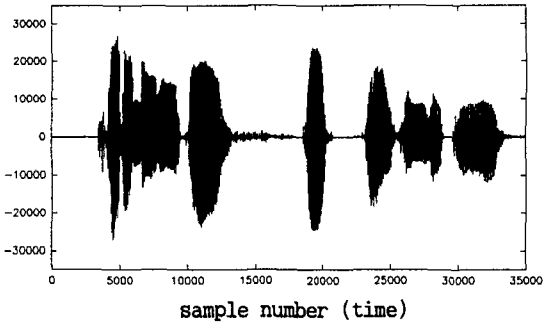


그림 3.1 샘플링된 음성정보 "털이 많아서 꼭 원숭이 같아요"

주파수 영역에서의 비화 방법은 대역 분할 방식의 하나인 롤링 대역 분할 방식을 이용하여 주파수 영역에서 한 블럭 당 2,048개의 샘플을 갖는 대역들로 분할하고, 다시 각 대역을 256개의 샘플들로 구성된 총 8개의 부분 대역으로 나누어 각 성분을 길이 8인 키를 가지고 치환하여 비화하였다. 그리고 비화 영역 판단을 위한 알고리즘에서 시간 영역 비화 방법은 시간 샘플 비화 방식을 이용하여 2,048개의 샘플을 한 블럭으로 나눈 다음 256개 샘플/성분으로 분할하고 의사난수-유니폼 치환 방법을 이용하여 치환·비화하였다. 또한 신호 검출을 위한 알고리즘에서는 의사 난수 치환 방법, 유니폼 치환 방법 그리고 의사난수-유니폼 치환 방법과 같이 세가지 방법에 대하여 알아보았다. 여기에서 원 신호, 각 비화 신호(시간 영역 비화 신호, 주파수 영역 비화 신호)와 3.6 KHz 고역 통과 필터링 후의 잔여 신호(원 신호, 각 영역 비화 신호)를 비교·분석 하였다.

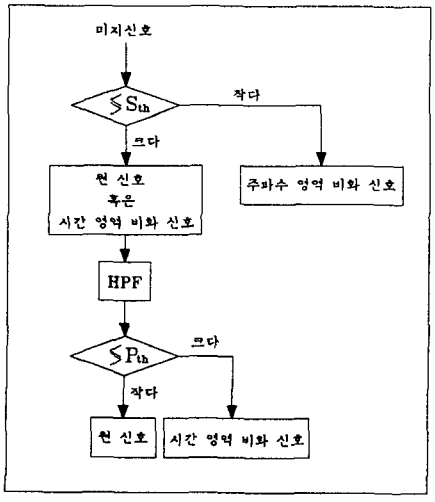


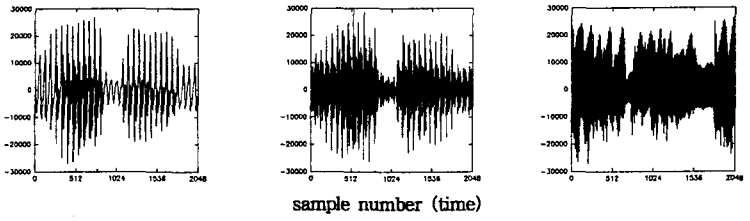
그림 3.2 비화 여부 및 비화 영역 판단 과정 흐름도

3.8 KHz~4.0 KHz의 통과 대역(pass band), 0 Hz~3.4 KHz의 정지 대역(stop band) 그리고 3.4 KHz~3.8 KHz의 사이드 밴드(side band)의 특성을 갖는 실제적인 고역 통과 필터를 소프트웨어로 구현하여 사용하였다.

원 신호 및 각 비화 신호의 구분 및 비화 영역 판단 과정을 처리하기 위해서 그림 3.2와 같은 과정을 수행하였다.

3.2 미지 신호 자체 분석을 통한 각 신호의 판별

원 신호를 시간 영역 비화 및 주파수 영역 비화를 시킨 후 각 비화 신호 및 원 신호와의 차이점을 알아낸다. 그림 3.3은 원 신호, 주파수 영역 비화 신호(27051943순) 시간 영역 비화 신호를 보여준다. 그림에서 보여주는 신호는 우리가 선택한 10개의 신호 중에서 신호의 세기가 비교적 큰 신호 2이다.



(a) (b) (c)

그림 3.3 신호 2와 9의 원 신호(a), 주파수 영역 비화 신호(b) 및 시간 영역 비화 신호(c) 형태

3.2.1 주파수 영역 비화 과정이 수행된 신호의 특징[3]

주파수 영역 비화 과정이 수행된 신호의 특성을 알아내기 위해서는 먼저 퓨리에 변환 특성을 알아야 할 필요성이 있다. 식 (1)을 이용하여 시간 영역 신호 x(n)을 주파수 영역으로 변환시킬 수 있다.

$$X[k] = \sum_{n=0}^{N-1} x[n]\, e^{-j(2\pi/N)kn} \qquad \text{여기서 N은 주기.} \qquad (1)$$

원 신호 S와 주파수 영역에서 비화된 신호 S'의 일반적인 페이저도를 그림 3.4와 같이 나타낼 수 있다. 그림 3.4와 같이 원 신호가 실수값일 때 원 신호 S는 실수축상에 나타나며, 주파수 영역에서 비화된 신호의 크기는 동일하지만 위상이 변화된 신호로써 원 신호와 같은 반지름을 갖는 원주상에 나타난다. 즉, 변화된 신호의 크기는 $\sqrt{(x'^2+y'^2)}$로서 원의 반지름과 같고, 위상은 $\tan^{-1}\frac{y'}{x'}$이다. 원 신호 S와 주파수 영역 비화 신호 S'는 크게 다음과 같은 두가지 특징을 갖는다.

① $|x'|+|y'| \geq |x|$ S'=S일때 등호 성립.
② $|x'| \leq |x|$ S'=S일때 등호 성립.

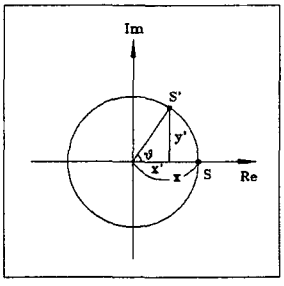


그림 3.4 원 신호 및 주파수 영역 비화 후 신호의 페이저도

주파수 영역 비화 신호의 특성을 알아내기 위해서 위와 같은 부등식을 이용하였으며, 3.2.2절과 3.4절에 자세하게 다루기로 한다.

3.2.2 각 비화 영역 신호의 특성 및 구분

원 신호 및 각 영역 비화 신호의 특성을 알아내기 위하여 미지의 신호 자체 분석에 의한 판별방법을 시도한다. 먼저 식(2)와 같이 각 신호의 샘플들을 절대값을 취한 후 합의 평균치를 가지고 각각의 신호들을 분석해 본다.

$$P = \frac{1}{n} \sum_{i=1}^{2048} |A_i| \qquad (2)$$

여기서 A_i는 i번째 샘플값이고, n은 2,048이다.

식 (2)에 의해 구해진 원 신호 및 각 영역 비화 신호에 대한 값들은 표 3.1과 같다.

주파수 영역 비화 신호의 식 (2)에 의한 값은 실수값만을 취하고 허수값은 고려하지 않았다. 연구를 수행함에 있어 송신자·수신자와의 동기가 완벽하게 맞고 키만을 모른다고 가정하였기 때문에 송신자가 수신자에게 보내는 실수부와 허수부를 해독자 역시 알 수 있으며 허수부를 제외한 실수부만을 고려하므로써 원 신호, 주파수 영역 비화 신호, 그리고 시간 영역 비화 신호를 구분할 수 있다.

3.2.1절의 주파수 영역 비화 신호의 특성 ②에서 볼 수 있듯이 신호가 동일한 경우에는 원 신호 및 각 영역 비화 신호의 세기 P의 값이 원 신호=시간 영역 비화 신호>주파수 영역 비화 신호순으로 세기가 구분이 된다. 그러나 신호 5의 주파수 영역 비화 신호의 P의 값이 신호 4의 원 신호의 P값보다 크듯이 신호의 세기가 다른 신호를 비교함에 있어서는 식(2)을 가지고는 전체적인 임계값을 정하는데 어려움이 있다. 그리하여 명확한 임계값을 결정하기 위하여 다음과 같이 수식 (3)을 이용한다.

$$S = \frac{1}{10} \sum_{j} P_j \qquad (3)$$

여기서 j는 비교적 신호의 세기가 큰 신호 5, 2, 9, 3, 11, 15, 13, 12, 4, 14번째 신호의 순서를 나타낸다.

식 (3)은 신호가 있는 부분으로 판단하여 우리가 선택한 10개의 신호의 세기 P를 모두 더한 후 평균값을 나타낸다. 원 신호 및 각 영역 비화 신호의 식 (3)에 의한 평균값은 다음과 같다.

• 원 신호 : 4,006 • 시간 영역 비화 신호 : 4,002 • 주파수 영역 비화 신호 : 2,129

또한 주파수 영역에서 있어서 임의의 다른 키를 선택하였을 때의 값은 다음과 같다.

• 주파수 영역 비화 신호 ▸ (36520741순) : 2,489 ▸ (14365072순) : 2,025

표 3.1 각 신호의 샘플들을 절대값을 취한 후의 평균값

발췌신호	원 신호	시간 영역 비화 신호	주파수 영역 비화 신호
신호 5	6752	6753	3468
신호 2	6386	6371	3453
신호 9	5358	5342	2704
신호 3	3887	3887	2245
신호 11	3493	3498	1789
신호 15	3297	3293	1778
신호 13	3209	3205	1724
신호 12	3100	3099	1606
신호 4	2802	2802	1563
신호 14	1778	1775	960
평균값	4006	4002	2129

위와 같이 식 (3)에 의한 평균값을 비교해 본 결과 시간 영역 비화 신호와 원 신호의 평균값은 같음을 확인하였고, 주파수 영역 비화 신호의 평균값들은 이 값들보다 적다는 사실을 확인할 수 있다. 주파수 영역 비화 후 시간 영역 비화 신호로 환원된 신호의 경우 원 신호의 순서(즉, 01234567순)와 유사한 순서(예를 들면, 01234576, 10234567 등등)의 키를 선택할 경우 위상의 변화가 별로 없기 때문에 허수부를 제외한 실수값이 원 신호의 값에 비해 덜 적어지고, 원 신호의 순서와 아주 다른 순서의 키를 선택할 경우 위상의 변화가 많아 원 신호에 비해 많이 작아짐을 알 수 있다. 서로 다른 임의의 키를 가지고 주파수 영역과 원 신호를 비교하는 과정에서 원 신호의 순서와 유사한 순서의 키를 선택할수록 원 신호의 평균값과 가까와지고 원 신호의 순서와 아주 다른 순서의 키를 선택할수록 원 신호의 평균값보다 훨씬 적어짐을 확인할 수 있다. 이러한 사실은 신호 검출 과정에서 미지의 신호로부터 주파수 영역 비화 신호로 판단되어진 신호를 원 신호로 검출하는데 유용하게 사용되어진다.

적당한 임계값을 정한 후 미지 신호의 식 (3)에 의한 평균값이 임계값보다 적은 경우 주파수 영역 비화 신호로 판단 가능하며, 그렇지 않을 경우 원 신호 및 시간 영역 비화 신호로 판단할 수 있다. 이 분석방법에 의한 결과 임계값(S_{th})은 3,700으로 정하였고, 서로 다른 임의의 키를 갖고서 이끌어 낸 결과이기에 알맞은 임계값으로 판단되어진다. 즉, 미지의 신호를 수신하였을때 그 신호의 S값이 3,700을 넘을 경우 그 신호는 원 신호 또는 시간 영역 비화 신호로 구분 가능하고, 임계값을 넘지 않을 경우 주파수 영역 비화 신호로 판단 가능하다.

3.3 원 신호와 시간 영역 비화 신호의 판별

원 신호인 음성은 일반적으로 0.3 KHz와 3 KHz사이에 대부분의 신호가 집중되어 있다. 즉 3 KHz이상의 고역 통과 필터를 사용할 경우 음성신호는 거의 남아있지 않게 된다. 반면에, 시간 영역 비화 신호인 경우 각각의 샘플들을 시간 영역에서 치환하였기 때문에 원 신호에 비해 아주 많은 고주파성분이 나타나게 된다. 이러한 이론적인 기초위에서 원 신호 및 시간 영역 비화 신호의 주파수 영역에서의 고주파 성분을 비교·분석한 결과 두 신호간의 차이점을 발견할 수 있었다. 원 신호와 시간 영역 비화 신호를 동일한 3.6 KHz 고역 통과 필터를 통과 시킨 후 원 신호는 거의 남아있지 않고 시간 영역 비화 신호는 다량으로 남아있음을 확인하여 3절에서와 같이 10개의 신호부분을 취한 후 각 샘플의 절대값을 취한 값을 비교한 결과 임계값을 결정할 수 있다. 임계값은 잔여 신호에 대한 식 (2)에 의한 P 값을 비교한 결과를 가지고 결정한다.

잔여 신호의 식(2)에 의한 신호의 세기 P의 값은 신호의 세기가 틀려질 경우에도 원 신호와 시간 영역 비화 신호간의 구분을 명확히 지을 수가 있다. 표 3.2에서 보는 바와 같이 원 신호의 고역 통과 후 잔여 신호의 최대값인 27이 시간 영역 비화 신호의 최소값인 474보다 훨씬 작다. 여기에서 우리는 임계값을 200으로 결정할 수 있다. 즉, 미지의 발췌 신호의 P값이 200보다 작다면 원 신호로 구

표 3.2 원 신호 및 시간 영역 비화 신호의 3.6 kHz HPF 통과 후의 잔여 신호들에 대한 식 (2)에 의한 신호의 세기

발췌신호	원 신호	시간 영역 비화 신호
신호 5	17	1309
신호 2	15	2174
신호 9	5	3032
신호 3	9	898
신호 11	5	918
신호 15	10	886
신호 13	6	597
신호 12	27	474
신호 4	19	531
신호 14	9	500

분 가능하고, 200보다 크다면 시간 영역 비화 신호로 구분 가능하다.

그림 3.5는 원 신호의 3.6 KHz 고역 통과 필터링 후의 잔여 신호이며, 그림을 통해 고역 통과 후의 원 신호와 시간 영역 비화 신호의 잔여 신호의 특성을 확연히 구분할 수 있다.

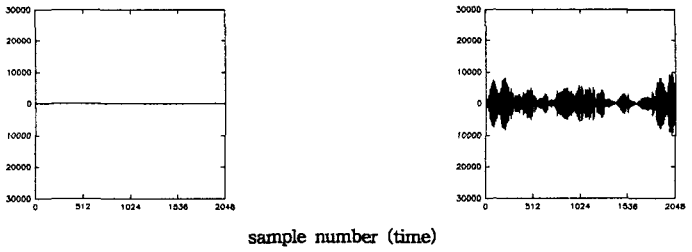


그림 3.5 원 신호(신호 2) 및 시간 영역 비화 신호의 필터링 후 잔여 신호

3.4 주파수 영역 비화 신호 검출 알고리즘

3.2절과 3.3절에서 각 신호의 비화 영역 구분을 지었으며, 이 절에서는 주파수 영역 비화 신호를 원 신호로 검출하는 구체적인 알고리즘을 구현한다. 미지의 신호를 3.2절에서 밝힌 비화 영역 판단 기준에 의하여 주파수 영역에서 비화되었다고 판단되는 신호를 먼저 FFT 변환 후 주파수 영역에서 부분대역 치환 키의 길이가 8개이기 때문에 8!의 모든 가능한 키를 가지고 비화된 신호의 주파수 대역을 역치환 시킨다. 이와 같은 과정을 수행한 후의 결과는 1개의 원 신호와 8!-1개의 비화된 신호가 남게 된다. 3.2.1절에서 밝힌 바와 같이 주파수 영역 비화 후의 신호는 위상값을 갖게 되기 때문에 실수부와 허수부를 갖게 된다. 특성 ①에서 실수부와 허수부를 합한 값중 최소가 되는 값은 위상이 0° , 90° , 180° 그리고 270° 일때이며 이중 양의 실수부를 지닌 값을 찾아내면 그 신호가 바로 원신호가 된다.

주파수 영역 비화 신호의 원 신호로의 검출과정을 밝힌 흐름도는 그림 3.6과 같다. 그림에서 S_{r+i}는 실수부와 허수부의 합을 나타낸다.

3.5 시간 영역 비화 신호 검출 알고리즘

시간 영역 비화 신호의 검출과정은 먼저 시간 영역 비화 신호로 판단되어진 신호를 가능한 모든 키를 대입하여 역 치환 과정을 수행한 후에 영교차율을 비교하여 원 신호를 찾아내면 된다. 영교차점(zero-crossing)이란 신호 파형이 시간축을 지나는 모든 경우에 발생한다. 다시 말하면 신호 파형이 크기가 영(zero)인 점을 지나는 횟수를 나타내며 초당 영교차점의 수(영교차율, Zero-Crossing Rate)는 음성 신호의 특성을 파악하는 중요한 요소가 된다. 일반적으로 음성신호의 영교차점의 범위는 2,500 crossings/s를 넘지 않으며 음성신호는 평균적으로 대략 1,400 crossings/s이며, 비음성신호는 4,900 crossings/s이다[4]. 그러므로 위와같이 가능한 모든 키를 역치환하여 역 치환에 필요한 키의 가지수만큼의 신호들의 영교차점들을 비교하여 본 후 2,500 crossings/s 를 넘지 않는 신호를 찾아낸 결과 그 신호가 원 신호로 복호된 신호임을 확인하였다. 즉 원 신호로 복호된 신호만이 2,500 crossings/s를 넘지 않으며, 즉 원 신호는 가장 작은 영교차율을 갖고 있으며 잘못된 키를 이용하여 역치환 과정이 수행된 신호는 여전히 비화된 신호와 같은 특성을 갖고 있으며 비음성신호로 간주된다. 이와 같은 결과는 의사 난수 치환 방법, 유니폼 치환 방법 그리고 의사난수-유니폼 치환 방법으로 비화시킨 모든 경우에 대하여 동일한 결과이며 영교차점을 비교하여 원 신호를 찾아내는 시간 영역 비화 신호 검출과정의 흐름도는 그림 3.6과 같다.

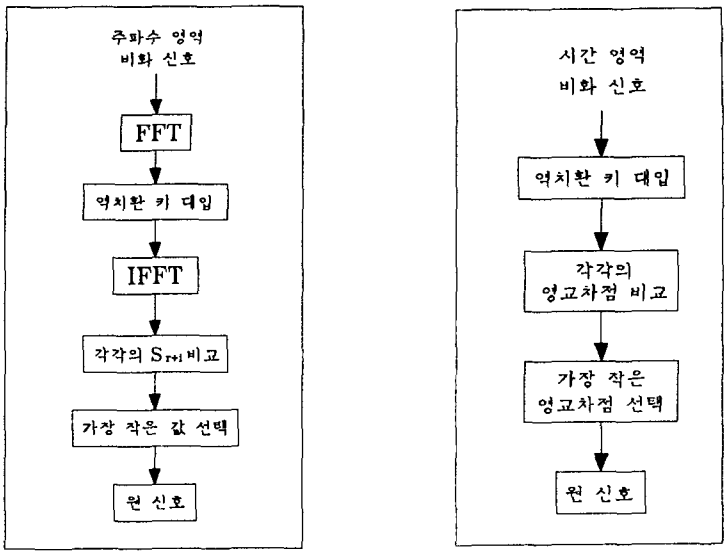


그림 3.6 주파수 및 시간 영역 비화 신호의 원 신호로의 검출과정

제 4 장 키의 선택

제 3장에서는 주파수 영역 비화 신호 및 시간 영역 비화 신호를 검출하는 알고리즘을 알아보았다. 이 장에서는 이러한 알고리즘을 이용하여 비화 블럭의 크기와 동기를 알고 있지만 복호키를 모르는 해독자의 입장에서 미지의 신호를 수신하여 원 신호를 검출하여봄으로써 블럭의 크기에 따른 신호 검출 소요 시간을 파라미터로 하여 우리가 필요한 비도에 맞는 키를 선택하는 기준을 설정하였다. 즉 키를 알지 못하는 해독자로부터 정보를 7일 동안 보호할 수 있는 비화 방식을 구성하는데 있어 키를 선택하는 기준을 마련한다. 키를 알지 못하는 해독자가 원 신호를 알아내는데 7일이 필요한 정도의 비도가 필요하다는 것은 현재의 보호하고자하는 정보가 7일 후에 누출이 된다하더라도 정보로서의 중요성을 상실한다는 의미이다. 정보를 보호하고자 하는 데 키의 선택은 가장 중요한 문제이며 더불어 송·수신자간의 안전한 사전 정보 교환은 필수적으로 동반되어야 한다.

4.1 주파수 영역 비화의 키의 선택

주파수 영역 비화 신호를 수신하여 원 신호를 검출하는 과정에 있어서 대입하는 역치환 키의 가지수는 시간 영역 비화 신호 검출시에 비해 많지 않으나 주파수 영역으로 변환하는 과정, 키를 대입하는 과정, 실수부와 허수부를 처리하는 과정 그리고 시간 영역으로 역 변환하는 과정등을 수행하기 때문에 컴퓨터를 이용하여 알맞은 복호키를 찾아내고 올바른 정보를 알아내는데 비교적 시간이 많이 걸린다. 그러나 주파수 영역 비화 신호에 있어서 키의 가지수가 많지 않으므로 음성 잔여 이해도가 비교적 높아 듣기 시험을 통해 해독될 수 있다는 단점을 지니고 있다. 키의 길이를 8개로 택하였을때 원 신호를 검출하는데 필요한 시간은 3시간 40분정도이며, 키의 길이를 9로 선택할 경우 총 키의 갯수는 362,880 (=9!)개이며 컴퓨터를 이용하여 원 신호를 검출하는데 1일 9시간정도가 소요된다. 키의 길이를 10이상으로 선택할 경우 7일 동안 정보를 보호는데 충분하지만 음성 잔여 이해도가 비교적 높기때문에 듣기 시험을 통해 해독될 수 있다는 단점을 지니고 있음을 유념하여야 한다.

4.2 시간 영역 비화의 키의 선택

먼저 의사 난수 치환 방법에 있어서 키를 모른다는 것은 키를 생성하는데 필요한 원시다항식과

초기치 벡터를 모른다는 것과 동일한 의미를 지닌다. 의사 난수 치환 방법에 있어서 키의 가지수는 원시다항식과 영벡터를 제외한 초기치를 곱한 값과 같다. 블럭의 크기가 512 (=2^9)일때 원 신호를 검출하는데 필요한 시간은 340초가 걸리며 이러한 블럭의 크기는 정보를 보호하고자하는데 적합하지 않으며 블럭의 크기를 훨씬 더 크게 설정하여야만 한다. 블럭의 크기를 16,384 (=2^{14})을 선택할 경우는 원시다항식의 개수는 756개이며 역치환에 사용되는 총키의 개수는 1.239×10^7개이며 원 신호를 검출하는데 필요한 시간은 2일 2시간정도가 걸린다. 블럭의 크기를 32,768 (=2^{15})을 선택할 경우는 원시다항식의 개수는 1,800개이며 역치환에 사용되는 총키의 개수는 5.898×10^7이며 원 신호를 검출하는데 필요한 시간은 9일 20시간정도가 걸리며 7일의 비도가 필요한 정보를 보호하고자할때 블럭의 크기를 32,768이상으로 설정하여야만 한다.

유니폼 치환 방법에 있어서 키를 모른다는 것은 암호화 과정에서 블럭의 크기와 서로소인 수를 모른다는 것과 같은 의미이다. 블럭의 크기가 256일때에는 원 신호를 검출하는데 필요한 시간은 1.04초가 소요되며 블럭의 크기를 알고있다는 가정하에서는 적합하지 않는 방법으로 판단된다.

의사난수-유니폼 치환 방법은 키를 증가시키기 위해 의사 난수 치환 방법과 유니폼 치환 방법을 결합한 방법으로 키의 가지수는 원시 다항식의 수, 영벡터를 제외한 초기치 벡터의 수 그리고 블럭의 크기와 서로소인 수를 곱한 값으로 위의 두 방법에 비하여 키의 개수가 현저하게 많다. 블럭의 크기가 256일때 키의 가지수는 518,160 (=127×255×16)개이며 원 신호를 검출하고자 하는데 소요되는 시간은 1시간 36분 34초이다. 즉 키의 가지수를 더욱 증가시키기 위해서는 블럭의 크기를 더욱 크게 정하여야만하며 블럭의 크기를 512로 정하면 키의 가지수는 원시다항식의 수 (48개), 영 벡터를 제외한 가능한 초기치 벡터의 수 (511개) 그리고 1을 제외한 유니폼 치환 방법에서 정한 블럭의 크기와 서로소인 수 (255개)를 곱한 값인 6,254,640개이며 원 신호를 검출하는데 필요한 시간은 3일 17시간 정도가 소요된다. 그러므로 블럭의 크기를 1,024로 정하면 7일 이상 정보를 보호하는데 충분하다.

비화 단위인 블럭의 크기가 알려져 있는 정보를 7일 이상 보호하고자 할때 의사 난수 치환 방법에서는 블럭의 크기를 32,768 이상으로 정하여야하고 유니폼 치환 방법은 적합한 방법이 아니라고 판단되며 의사난수-유니폼 치환 방법을 사용할 경우 1,024 이상의 크기를 갖는 블럭을 정하여야 한다. 각 비화 방법에 있어서 블럭의 크기에 따른 키 검출 소요 시간은 표 4.1과 같다.

비화 방법		치환 블럭의 크기	키의 가지수	키 검출 소요 시간
주파수 영역 비화		8	40320 개	약 3시간 40분
		9	362880 개	약 1일 9시간
시간 영역 비화	의사 난수 치환 방법	512	4080 개	340 초
		16384	1.239×10^7 개	약 2일 2시간
		32768	5.898×10^7 개	약 9일 20시간
	유니폼 치환 방법	256	32512 개	1.04초
	의사난수-유니폼 치환 방법	256	518160 개	1시간 37분
		512	6254640 개	약 3일 17시간

표 4.1 블럭의 크기에 따른 키 검출 소요 시간

4.3 한정 수신 시스템에의 응용[11]

현재 미국, 유럽 그리고 일본에서는 위성 방송을 이용한 한정수신 시스템의 방송이 실현화되고 있다. 또한 우리나라에서도 역시 TV프로그램이나 데이타 서비스를 요금을 지불한 가입자들에게만 정상적으로 제공하고 그렇지 않은 미가입자등에게는 수신을 불허하는 한정 수신이 부분적으로 시행되고 있으며 앞으로 더욱 증가될 전망이다. 한정 수신 시스템은 미가입자들이 정보를 이용할 수 없게 하기 위하여 송신단에서는 정보를 보호할 필요성이 있으며 정보를 보호하는 방법으로는 아주 높은 비도를 필요로 하며 값이 많이 드는 군용과는 달리 비도가 높지는 않으나 가격이 저렴한 스크램블

링 방법을 채택하고 있다. 먼저 송신단에서 서비스하고자 하는 정보를 스크램블러로 비화시킨 후 가입자와 미가입자 구분없이 전파를 송신한다. 가입자는 암호화된 신호를 올바르게 복호할 수 있는 키를 가지고 있기 때문에 비화 신호를 수신한 후 올바른 정보를 서비스를 받을 수 있지만 미가입자는 복호키가 없기 때문에 비화 신호를 받는다 하여도 서비스를 받을 수 없다. 복호하는데 필요한 키를 가입자들에게만 분배하는 것은 필수적이며 주로 비도가 높은 블럭 정보보호방식인 DES나 공개키 정보보호방식인 RSA를 사용하여 암호화시킨 후 분배한다. 7일간 비도를 보장한다고 할때 7일후에는 비화된 정보를 복호할 수 있는 키를 해독자가 알아낼 수 있다는 의미이며 7일마다 키를 교환하여 가입자들에게 새로운 키를 분배해야만 한다.

제 5 장 결 론

본 논문에서는 복호키를 모르는 제 3자의 입장에서 주파수 영역 또는 여러가지 방법의 시간 영역 비화를 통해 비화된 미지의 신호를 수신한 후 원 신호를 찾아내는 알고리즘을 제안하였다. 그리고 각 영역 비화 신호를 원 신호로 복호하여 그 시간을 알아냄으로써 사용하고자 하는 비화 방식에서 적절한 키를 선택하는 방법을 연구하였다.

주파수 영역 비화시 7일 정도 정보를 보호하고자하는 경우 10이상의 키의 길이를 선택하여야 하며, 이 방식에 있어 10이상의 키를 선택할 경우에 컴퓨터를 이용하여 원 신호를 검출하는 데 7일 이상이 소요되지만 음성 잔여 이해도가 비교적 높기때문에 듣기 시험을 통해 해독될수 있다는 단점을 지니고 있음을 유념하여야 한다. 시간 영역 비화시 의사 난수 치환 방법에서는 블럭의 크기를 32,768 이상으로 정하여야 한다. 그리고 유니폼 치환 방법은 블럭의 크기가 알려져 있을때는 적합한 방법이 아니고 의사난수-유니폼 치환 방법을 사용할 경우 1,024의 크기를 갖는 블럭을 정하여야 한다.

한정 수신 시스템은 많은 인가된 수신자들을 대상으로하기 때문에 비도는 아주 높지는 않으나 가격이 저렴한 스크램블링 방식이 가장 적합하며 현재 많이 쓰이고 있다. 적절한 키를 선택한 후 가입자들에게 비도가 높은 DES나 RSA방식으로 분배한 후 정보를 스크램블링 방식으로 정보를 송신하는 방법을 한정 수신 시스템에 사용할 수 있으리라 예상된다.

참고 문헌

[1] H. J. Baker, F. C. Piper, *Secure Communications*, Academic Press, 1985.

[2] S. C. Kak, N. S. Jayant, "On Speech Encryption Using Waveform Scrambling," *B.S.T.J.*, Vol.56, No.5, pp781-808, May-June 1977.

[3] Alan V. Oppenheim, Ronald W. Schafer, *Discrete-Time Signal Processing*, Prentice Hall Internation Inc, 1989.

[4] Douglas O'Shaugnessy, *Speech Communication : Human and Machine, Addison Wesley*, 1987.

[5] M. R. Samber, N. S. Jayant, "Speech Encryption by Manipulations of LPC Parameters," *B.S.T.J.*, Vol.55, No.9, pp.1373-1388, Nov. 1976.

[6] 신 재성, 시간 샘플 비화 기법을 위한 치환 방법의 개선, 한양대학교 석사논문, 1993.

[7] 원치선, 김재공, "위성방송을 위한 TV신호의 암호화 기술 동향," 통신정보보호학회 제 3권 제 4호, pp 58-65, Sep.1993.

[8] 이일우, 조동호, "아날로그 음성, 비디오 신호의 비화 방식," 통신정보보호학회 제 2권 제 4호, pp. 75-90, Dec. 1992.

[9] 한국전자통신연구소, 현대암호학, 한국전자통신연구소, 1991.