비화 통신을 위한 비화기 설계 및 실시간 구현

Scrambler Design and Real Time Implementation for Secure Communication

석 광 원*, 여 송 필*, 박 중 호*, 정 정 균*, 두 현 웅*, 김 성 환*
(K. W. Seok*, S. P. Yeo*, J. H. Park*, J. K. Jung*, H. W. Doo*, S. H. Kim*)

요 약

전화선을 이용한 대화는 쉽게 도청되므로 개인의 비밀을 보장할 수 없다. 본 논문에서는 비밀이 보장되는 안전한 통신을 위한 비화기(scrambler)설계 및 실시간 구현을 제안하였다. 특히 동기 신호가 요구되지 않는 비화기 시스템을 설계함으로써 송신단의 동기 신호 첨가 하드웨어와 수신단의 동기 신호 검출 하드웨어가 필요없게 되므로 하드웨어적인 복잡성을 줄여 실시간 구현의 용이함을 얻었으며, 비화기 시스템에 새로운 이득 요소(gain factor)를 첨가하여 비화된 신호가 암호해독에 대한 안전성을 갖도록 하였다.

ABSTRACT

Conversations over telephone line are easily monitored and therefore acceptable level of security is not provided. In this paper, we propose the design of scrambler for secure communication and real time implementation of it. Especially, we can reduce the complexity of hardware and implement it easily by designing the scrambling system which doesn't require synchronization signal, and provide the scrambling filter with a sufficient level of security by adding new gain factor into the scrambling system.

Ⅰ. 서 론

오늘날 비밀이 보장되는 안전한 통신기술에 대한 높은 관심으로 음성 암호화의 많은 방법들이 발표되고 있다[1][2][6][7]. 정보의 중요성이 증대되고 있는 현대 정보화 사회에서 정보의 도청은 많은 손실을 초래할 수 있다.

기존의 아날로그 비화기 시스템(scrambling system)들은 음성신호를 주파수 혹은 시간 영역에서 변화시킨다. 일반적인 주파수 영역에서의 비화기 시스템은 신호를 몇 개의 주파수 대역으로 나눈 다음 그 주파수 대역의 순서를 바꾼다[3][5]. 또한 시간 영역에서의 비화기 시스템은 신호를 작은 시간 부분으로 나눈 다음 순서를 바꾼다[4][5]. 그러나 이 비화기 시스템들은 올바른 신호의 복원을 위하여 프레임 동기(frame synchronization)를 맞추어야 하므로 실제 구현이 복잡하게 되고, 복원 신호가 채널조건에 민감하게 된다.

이와 같은 이유에서 Lee[6][7]는 동기를 맞출 필요가 없는 시간과 주파수 영역에서의 비화기 시스템을 설계하여 하드웨어로 구현하였다. 또한 King[1]은 동기 오차에 둔감하기 위한 비화기 시스템의 통합 설계 방법을 제안하였다. 그러나 이 시스템들은 동기 신호 문제는 해결했지만 비화 정도가 낮아 암호해독에 대해 충분한 안전성을 제공하지 못하였다.

본 논문에서는 새로운 이득 요소를 첨가하여 동기 신호가 필요없으면서도 암호해독에 대해 안전성을 갖는 비화기 시스템을 제안하였다. 또한 이를 실시간으로 구현하여 실제 통신 시스템에 응용가능성을 보였다. 그리고 제안된 비화기 시스템의 성능을 평가하기 위하여 비화된 신호의 파형과 비화도 성능 평가의 척도가 되는 Residual Intelligibility를 구하여 King 방법[1]의 비화기 시스템과 비교 평가하였다.

Ⅱ. 동기 신호가 요구되지 않는 비화기의 제안

주기적 가변 이산 신호 필터를 다음 상태방정식의 집합으로 생각할 수 있다[1][8].

$$x(k+1) = A(k)x(k) + b(k)u(k)$$
$$y(k) = c^T(k)x(k) + d(k)u(k) \quad (1)$$

N-주기적 필터에 대해서 $A(k)$, $b(k)$, $c(k)$, $d(k)$는 N-주기적 벡터의 행렬이고, $u(k)$는 입력 스칼라이고, $y(k)$는 출

*서울시립대학교 전자공학과
Department of Electronic Engineering, Seoul City University
접수일자 : 1996년 7월 22일

력 스칼라이다.

식(1)에서 $\bar{x}(k)=x(kN)$,

$\bar{u}(k)=[u(kN)\,u(kN+1)\cdots u(kN+N-1)]^T$

$\bar{y}(k)=[y(kN)\,y(kN+1)\cdots y(kN+N-1)]^T$

으로 놓으면 시불변 다중 입출력 상태방정식을 얻을 수 있다[1][8].

$$\bar{x}(k+1)=\bar{A}\,\bar{x}(k)+\bar{B}\,\bar{u}(k)$$
$$\bar{y}(k)=\bar{C}\,\bar{x}(k)+\bar{D}\,\bar{u}(k) \tag{2}$$

위의 식(1)과 식(2)는 같은 입출력 관계를 가진다. 그러나 다른 점은 식(2)에서 입출력의 크기가 N인 블록이다. 식(2)는 시불변이므로 블록 전달 행렬 $G(z)=\bar{C}(zI-\bar{A})^{-1}\bar{B}+\bar{D}$을 정의할 수 있다. 식(2)는 선형 시불변이므로 주기적 필터의 주파수 영역 해석이 가능하다.

$y(k)$와 $u(k)$의 z변환을 $Y(z)$과 $U(z)$이라 하고, $\bar{y}(k)$와 $\bar{u}(k)$의 z변환을 각각 $\bar{Y}(z)$, $\bar{U}(z)$이라 하면 위의 두 식은 다음의 관계를 가진다.

$W_N=e^{-j\frac{2\pi}{N}}$ 라 할 때

$$Y(z)=\sum_{l=0}^{N-1} z^{-l}\,\bar{Y}_l(z^N), \tag{3}$$

$$\bar{U}_i(z^N)=\frac{z^i}{N}\sum_{k=0}^{N-1} W_N^{ki}\,U(z\,W_N{}^k) \tag{4}$$

또한 $G(z)=[G_{l,k}(z)]_{l=0,\,k=0}^{N-1}$로 놓으면, $\bar{Y}(z)=G(z)\bar{U}(z)$이므로

$$\bar{Y}_l(z)=\sum_{i=0}^{N-1} G_{l,i}(z)\bar{U}_i(z) \tag{5}$$

이 된다,

따라서 위 식들을 정리하면

$$Y(z)=\frac{1}{N}\sum_{k=0}^{N-1}\left(\sum_{i=0}^{N-1} W_N^{ki}\left(\sum_{l=0}^{N-1} z^{i-l}\,G_{l,i}(z^N)\right)\right)U(z\,W_N^k)$$
$$=\frac{1}{N}\sum_{k=0}^{N-1} H_k(z)\,U(z\,W_N^k) \tag{6}$$

여기서 $H_k(z)$는 k번째 이동 대역의 전달 함수로 $H_k(z)=\sum_{i=0}^{N-1} W_N^{ki}\sum_{l=0}^{N-1} z^{i-l}\,G_{l,i}(z^N)$, $k=0,\cdots,N-1$이다.

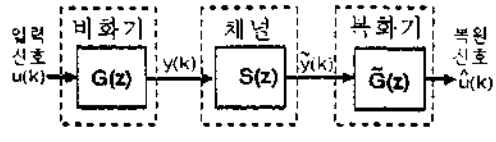

그림 1. 비화기 시스템 모델
Fig 1. Model of scrambling system

식(6)에서 출력 스펙트럼은 입력 스펙트럼의 이동, 변형된 형태들의 합임을 알 수 있다.

그림 1은 비화기 시스템 모델을 블록도로 나타낸 것인데, 여기서 $G(z)$은 송신단의 비화기 필터의 블록 전달 행렬을 나타내고 있고 $S(z)$은 채널 전달 함수를, $\tilde{G}(z)$은 수신단의 복화기 필터의 블록 전달 행렬을 나타내고 있다.

이 관계를 다위상(polyphase)모델로 표현하면 N-주기적 필터는 N개의 시불변 필터 $P_l(z)$를 평행하게 연결시킨 후, 이 필터들로부터의 출력을 주기적으로 선택하는 것과 같다. $P_l(z)=\sum_{i=0}^{N-1} z^{i-l}\,G_{l,i}(z^N)$의 관계를 가지고 있으며, $G_{l,i}(z)$, $0\le l\le N-1$은 $z^{-i}F_i(z)$의 다위상 표현의 N-성분이다.

채널 전달 함수를 $S(z)$으로 놓으면, 복호기 필터의 입력 신호는 채널을 통과한 신호 $\tilde{Y}(z)=S(z)Y(z)$으로 쓸 수 있으므로 복원된 신호 $\hat{U}(z)$은 다음과 같다.

$$\hat{U}(z)=\frac{1}{N}\sum_{k=0}^{N-1}\tilde{H}_k(z)\,\tilde{Y}(z\,W_N^k) \tag{7}$$

또한 위 식을 이용하여 입력 신호와 복원 출력 신호의 관계를 주파수 영역에서 표현하면 다음과 같다.

$$\hat{U}(z)=\sum_{k=0}^{N-1} M_k(z)\,U(z\,W_N^k) \tag{8}$$

여기서

$$M_k(z)=\frac{1}{N^2}\sum_{l=0}^{N-1}\tilde{H}_l(z)\,S(z\,W_N^l)\,H_{[k-l]}(z\,W_N^l) \tag{9}$$

$$[k-l]\equiv(k-l)\bmod \mathrm{N},\ 0\le[\mathrm{k-l}]\le \mathrm{N-1}$$

또한 m-샘플 동기 오차를 나타내기 위해 채널 전달 함수 $S(z)=z^{-m}$로 놓고 암호해독에 대한 안전성을 제공하기 위해 본 연구에서 제안한 새로운 이득 요소 C_l과 C_l^{-1}을 곱하면 식(9)를 다음과 같이 쓸 수 있다.

$$\hat{M}_{k,m}(e^{j\theta})=\frac{e^{-jm\theta}}{N^2}\sum_{l=0}^{N-1} W_N^{lm}\,\tilde{H}_l(e^{j\theta})\,C_l^{-1}\,C_l\,H_{[k-l]}(e^{j\theta}W_N^l) \tag{10}$$

인간의 귀는 음성의 위상왜곡에 민감하지 않으므로, 비화기 시스템이 동기 오차에 영향을 받지 않기 위한 조건은 다음과 같다.

(i) $|\hat{M}_{0,m}(e^{j\theta})|=1$

(ii) $|\hat{M}_{k,m}(e^{j\theta})|=0$ for $k=1,\cdots,N-1$
for $\theta\in[0,2\pi)$, $m=0,1,\cdots,N-1$.

이 조건들을 만족시키기 위한 조건들은 다음과 같다.

i) 비화기 필터의 모든 대역 통과 필터 $\{C_lH_l(e^{j\theta})\}_{l=0}^{N-1}$은

교차 대역없이 전주파수 대역을 포함해야 한다.

ii)또한 복화기 필터의 모든 대역 통과 필터 $\{C_l^{-1}\tilde{H}_l(e^{j\theta})\}_{l=0}^{N-1}$은 교차 대역없이 전주파수 대역을 포함해야 한다.

iii) $|\tilde{H}_l(e^{j\theta})|$와 $H_{|N-l|}(e^{j\theta}W_N^l)$은 같은 통과 대역을 가져야 한다.

iv) $|\tilde{H}_l(e^{j\theta})C_l^{-1}C_{|N-l|}H_{|N-l|}(e^{j\theta})| = N^2$

위의 조건을 만족하도록 비화기 필터의 대역 통과 필터 $\{C_l H_l(e^{j\theta})\}_{l=0}^{N-1}$와 복화기 필터의 대역 통과 필터 $\{C_l^{-1}\tilde{H}_l(e^{j\theta})\}_{l=0}^{N-1}$를 설계하기 위해 맵(map)을 도입할 수 있다[1]. 그림 2는 $N=4$인 경우의 여러 가지 맵들 중 하나를 나타내고 있다. 여기서 빗금친 직사각형은 통과 대역을 나타내고 있는데, X축에 투사한 대역은 비화기 필터의 대역 통과 필터 $\{C_l H_l(e^{j\theta})\}_{l=0}^{N-1}$의 대역이고 Y축에 투사한 대역은 복화기 필터의 대역 통과 필터 $\{C_l^{-1}\tilde{H}_l(e^{j\theta})\}_{l=0}^{N-1}$의 대역을 나타낸다. 그리고 iii)과 iv)의 조건을 만족시키기 위해 한 직사각형을 Y축으로 대칭 이동한 다음, 다시 X축으로 대칭 이동하면 다른 직사각형과 일치한다.(예 : 1과 8, 2와 7, 3과 6, 4와 5)

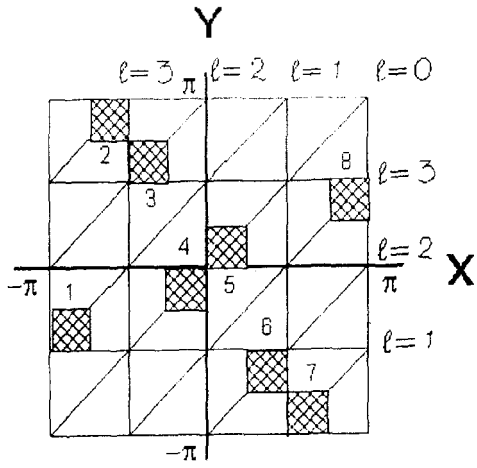

그림 2. $N=4$인 경우의 맵
Fig 2. Map for $N=4$

이런 규칙을 만족하는 맵을 구성하면 위의 네 가지 조건을 만족하는 비화기 필터의 대역 통과 필터 $\{C_l H_l(e^{j\theta})\}_{l=0}^{N-1}$와 복화기 필터의 대역 통과 필터 $\{C_l^{-1}\tilde{H}_l(e^{j\theta})\}_{l=0}^{N-1}$를 구할 수 있고, 식(6)을 이용하여 블록 전달 행렬 $G(z)$을 구하면 동기 오차에 영향을 받지 않으면서도 암호해독에 대해 안전성을 갖는 비화기 시스템을 구할 수 있다. 그런 다음 다위상모델에서 $P_l(z)=\sum_{i=0}^{N-1} z^{-i}G_{i,l}(z^N)$의 관계를 이용하여 주기적 필터인 $P_l(z)$으로 비화기 시스템을 구현할 수 있다.

Ⅲ. 실시간 처리 시스템의 구현

비화기 시스템을 실시간으로 구현하고자 할 때에 고려해야 할 가장 큰 문제는 각 샘플당 요구되는 연산량이다. 즉, 샘플링 주기 동안 한 샘플에 대해 요구되는 연산을 수행할 수 있어야만 실시간 구현이 가능하다.

본 논문에서는 TI(Texas Instruments)사의 TMS320C50 DSK(DSP Starter Kit)를 이용하여 실시간 비화기 시스템을 구현하였다. 하드웨어로 이 DSK를 선택한 이유는 TMS320C50이 클럭 주파수가 40MHz로 명령어(instruction)당 수행 시간이 25μsec 정도로 빠르고, 고정 소수점 연산(곱셈과 덧셈)을 한 클럭 동안 수행할 수 있으며, AIC(analog interface circuit) TLC32040을 탑재하여 최고 19.2kHz 이상으로 14bit A/D, D/A 변환을 수행할 수 있기 때문이다. 또한 DSK는 일단 컴퓨터로부터 프로그램을 다운로딩(downloading) 받은 후에는 독립적으로 동작이 가능하며, ROM에 프로그램을 써넣었을 경우는 완전 독립 동작이 가능하다. TLC32040은 샘플링 주파수, 입력단 증폭기(pre-Amp)의 이득, 입출력단의 저역 통과 필터의 차단 주파수를 소프트웨어적으로 조정할 수 있다.

그림 3의 TMS320C50 DSK의 블록선도에서 TMS320C50은 PC 및 TLC32040과 RS232 직렬 포트를 이용하여 시분할 방식으로 통신하며 TLC32040은 외부와 RCA 잭(Jack)을 이용하여 아날로그 신호를 입출력할 수 있다.

그리고 그림 4는 본 논문에서 사용한 실시간 비화기 시스템의 하드웨어 블록선도를 나타내고 있고, 그림 5는 그림 4의 하드웨어 블록선도에 나타나 있는 비화기(Scrambling) 필터와 복화기(Descrambling) 필터에서의 소프트웨어 흐름도를 나타내고 있다.

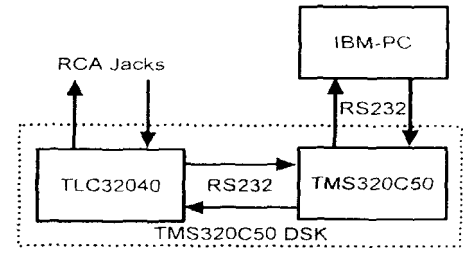

그림 3. TMS320C50 DSK의 블록선도
Fig 3. Block diagram of TMS320C50 DSK

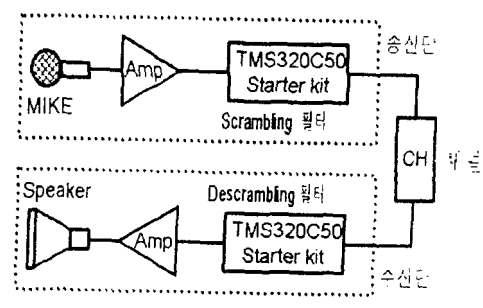

그림 4. 비화기 시스템의 하드웨어 블록선도
Fig 4. Hardware block diagram of scrambling system

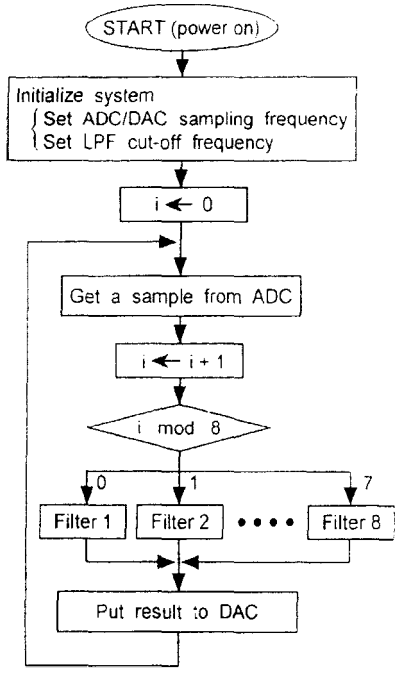

그림 5. $N=8$인 경우의 소프트웨어 흐름도
Fig 5. Software flowchart for $N=8$

송신단에서는 마이크로부터 음성 신호를 입력받아 증폭기를 거쳐 표준 RCA 잭으로 비화기 필터단에 입력한다. 비화기 필터단에서는 DSK에 탑재된 AIC의 A/D 변환기를 이용하여 8kHz, 14bit 샘플링을 수행한 후 80차의 FIR(finite impulse response) 필터 연산을 수행한다. 이때 입력 신호의 샘플링시 엘리어싱(aliasing)을 피하기 위하여 차단 주파수 4kHz의 저역 통과 필터를 거친 후 8kHz로 샘플링을 하게 된다. TMS320C50은 32bit 고정 소수점 연산을 수행하여 그 결과를 다시 AIC의 D/A 변환기를 이용하여 RCA 잭으로 내보내게 된다. D/A 변환에서도 A/D 변환에서와 마찬가지로 차단 주파수 4kHz의 저역 통과 필터를 통과하게 된다.

송신단을 거쳐 비화된 신호는 채널을 통과한 후 수신단에 입력된다. 수신단에 입력된 신호는 복화기 필터를 거친 후 증폭되어 스피커를 통하여 수신자가 듣게 된다. 이때 복화기 필터의 구조는 필터 계수를 제외하고는 비화기 필터와 같이 FIR 필터 연산을 수행한다.

Ⅳ. 실험 및 결과 고찰

본 논문의 성능을 평가하기 위하여 King의 논문과 같은 맵의 대역을 사용하여 블록 전달 행렬 $G(z)$을 구한 다음 주기적 필터로 구현하였으며, 일반 대화시 음성이 대개 저주파수대역에 존재하므로, 비화된 신호의 인식률을 낮게 하기 위해 비화된 신호가 저주파수 대역에서는 작은 값을, 고주파수 대역에서는 큰 값을 가지도록 여러 가지 이득 요소 C_i과 C_i'에 대해서 실험하였다. 이득 요소를 결정할 때 각각의 값이 너무 차이가 나면 교차대역에서 왜곡이 발생하여 정확히 음성을 복원할 수 없으므로, 각 값들의 크기 비가 10배를 넘지 않도록 하였다.

다음 표 1은 여러 가지 이득 요소에 대해 실험한 다음, 0-2 kHz의 저주파수 대역의 평균 전력값과 2-4 kHz의 고주파수 대역의 평균 전력값의 상대적 비 $R_{H/L}$를 나타내고 있으며, 실험 1은 C_1, …, C_7을 각각 {0.3, 0.5, 2, 2.5, 2, 0.5, 0.3}으로, 실험 2는 {0.5, 0.7, 2.5, 2, 2.5, 0.7, 0.5}로, 실험 3은 {2, 2.5, 0.7, 0.5, 0.7, 2.5, 2}로, 실험 4는 {2.5, 2, 0.3, 0.5, 0.3, 2, 2.5}로, 실험 5는 {0.3, 2.5, 0.5, 2, 0.5, 2.5, 0.3}으로 정하였을 때를 나타내고 있다.

표 1. 여러 가지 이득 요소에 대한 실험결과
Table 1. Experimental results for various gain factors

	실험 1	실험 2	실험 3	실험 4	실험 5
$R_{H/L}$	91.6	28.7	0.14	0.15	3.16

비화된 신호의 $R_{H/L}$ 값이 클수록 저주파수 대역에서는 작은 값을, 고주파수 대역에서는 큰 값을 가지게 되므로 비화가 잘 되었음을 알 수 있다. 따라서 맵의 이동을 관찰하여 비화된 신호의 인식률이 적게 되도록 이득 요소값을 선정할 수 있다.

신호의 암호화 정도를 파악하기 위하여 '누나' 라는 음성을 8kHz 샘플링하여 비화기 필터를 통과시킨 후, 스피커를 통해 비화된 소리를 피실험자가 직접 듣게 하였으며, 또한 신호의 복원정도를 알아보기 위하여 이 비화된 신호를 복화기 필터를 통과시킨 후 스피커를 통해 들어보았다. 그림 6은 원신호의 파형과 스펙트럼을 나타내고 있다. 음성 신호가 2kHz미만의 저주파수 대역에 집중되어 있음을 알 수 있다.

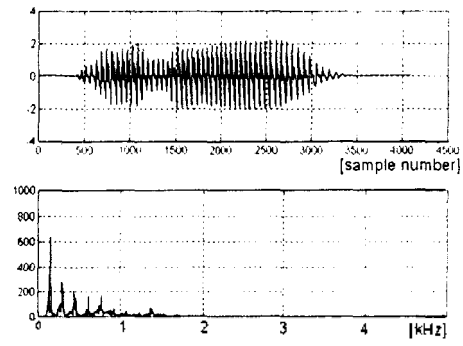

그림 6. 원신호 "누나"의 파형과 스펙트럼
Fig 6. Waveform and spectrum of original signal "nuna"

그림 7(a)는 King 방법의 비화기 필터로부터 얻은 비화된 신호를 나타내고 있으며, 그림 7(b)는 이와 비교하기 위한 제안된 방법의 비화기 필터로부터 얻은 비화된 신

호를 나타내고 있다. 제안된 방법의 비화된 신호의 진폭 스펙트럼값이 저주파수 대역에서 더 작고 신호의 암호화에 기여하는 고주파수 대역에서 더 크므로 암호화가 더 잘된 것을 알 수 있다.

그리고 동기 오차에 대한 신호의 복원 정도를 알아보기 위하여 3개 샘플 오차에 대해 음성 신호를 복원하여 그림 8에 나타내었다. 그림 8(a)는 King 방법의 복화기 필터로부터 얻은 복원 신호를 보여주고 있으며, 그림 8(b)는 제안된 방법의 복화기 필터의 복원 신호를 보여주고 있다. 제안된 방법의 복화기 필터와 King 방법의 복화기 필터 모두가 동기 신호에 영향을 받지 않고 신호를 잘 복원하고 있음을 알 수 있다.

비화기의 객관적인 비화도 성능 평가를 위해서 Residual Intelligibility(R.I.), 신호대 잡음비(SNR) 등이 사용되는 데, 실제 사람을 대상으로 하는 R.I.가 많이 사용된다[1][5][6][7]. 따라서 본 논문에서도 제안된 방법의 비화도 성능 평가를 위하여 R.I. 검사를 하였다. 기본적으로 Jayant[5]와 Lee[6]의 검사방법과 같게 하였다. zero에서 nine까지의 숫자 중에서 연속된 네 자리 숫자(예 : two, three, seven, five)20개 샘플을 비화시킨 다음, 50명의 피실험자에게 들려준 후 최상의 추측한 소리를 받아쓰게 하여 수행한 다음 표 2에 나타내었다.

표 2에서 보는 바와 같이 제안된 방법의 R.I. 수치가 King 방법의 R.I. 수치보다 낮으므로 제안된 방법의 비화된 신호가 비화가 더 잘 되었다는 것을 알 수 있다. 또한 R.I. 수치와 비화된 신호의 암호해독에 대한 안전성이 역의 관계가 있으므로 제안된 방법의 비화된 신호가 King 방법의 비화된 신호보다 암호화가 잘 되었다는 것을 알 수 있다.

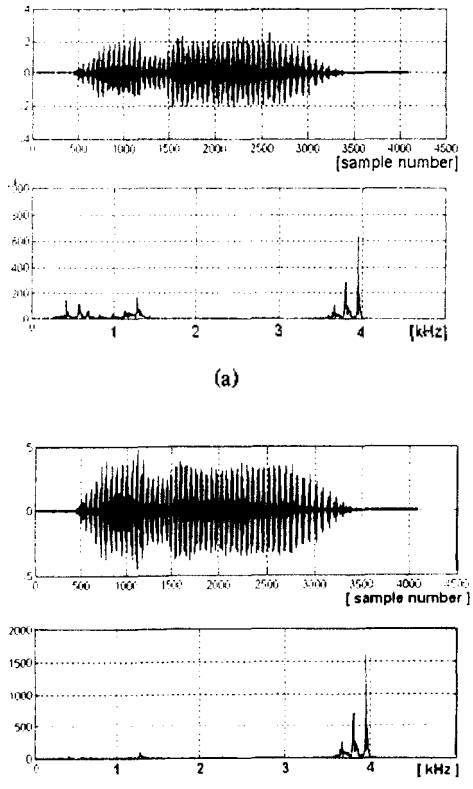

그림 7. 비화기 필터로부터 얻은 비화된 신호의 파형과 스펙트럼
(a) King의 방법 (b) 제안된 방법

Fig 7. Waveform and spectrum of the scrambled signal obtained scrambling filter
(a) King's method (b) Proposed method

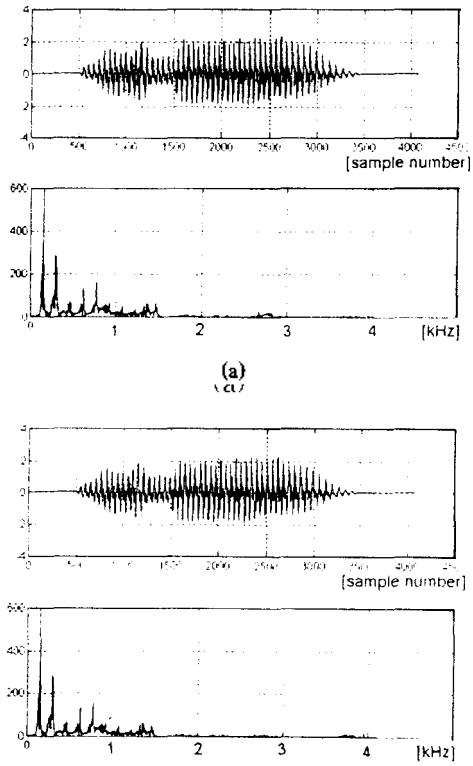

그림 8. 복화기 필터로부터 얻은 복원 신호의 파형과 스펙트럼 (3개 샘플 오차)
(a) King의 방법 (b) 제안된 방법

Fig 8. Waveform and spectrum of the recovered signal obtained descrambling filter(3 samples error)
(a) King's method (b) Proposed method

V. 결 론

본 논문에서는 비밀이 보장되는 안전한 통신을 위하여 새로운 아득 요소를 첨가함으로써 암호해독에 대해 안전성을 제공하는 비화기 설계와 이의 실시간 구현을 제안하였다.

본 논문에서 설계한 비화기 필터를 실제 음성 신호에 적용해 본 결과, 다른 비화기 필터보다 인식률이 더 낮은 비화된 신호를 만들어 냈으며, 또한 복화기 필터는 동기

표 2. Residual Intelligibility 검사 결과
Table 2. Test results of Residual Inte- lligibility

R.I. 방법		King의 방법	제안된 방법
각 숫자에 대한 R.I. 평균값 (%)	zero	23.5	24.3
	one	25.6	26.2
	two	21.4	30.9
	three	44.8	26.8
	four	28.8	23.4
	five	22.4	25.7
	six	50.2	25.8
	seven	39.5	29.3
	eight	40.6	28.1
	nine	30.9	21.5
R.I.의 평균값 (%)		32.8	26.2

신호에 관계없이 원신호를 잘 복원하고 있음을 확인할 수 있었다. 이와 같이 동기 신호를 보낼 필요가 없으므로 다른 비화기 시스템보다 쉽게 구현할 수 있었다.

정보의 중요성이 증대되고 있는 현대 정보화사회에서 비밀이 보장되는 안전한 통신을 위한 본 논문에서 제안한 비화기 시스템은 기존의 복잡한 비화기 시스템을 대신하여 유용하게 사용될 수 있으리라 사료된다.

참 고 문 헌

1. C. W. King, C. A. Lin, "A *Unified Approach to scrambler* Filter Design," IEEE Trans. Signal Processing, vol. 43, No. 8, pp. 1753-1765, 1995.
2. R. Ishii and M. Kakishita, "A design method for a periodically time-varying digital filter for spectrum scrambling," IEEE Trans. Acoust., Speech, Signal Processing, vol. 38, pp. 1219-1222, 1990.
3. K. Sakurai, K. Koga, and T. Muratani, "A speech scrambler using the fast fourier transform technique," IEEE J. Select. Areas Commum., vol. SAC-2, pp. 434-442, 1984.
4. S. C. Kak and N. S. Jayant, "On speech encryption using waveform scrambling," Bell Syst. Tech. J., vol. 56, pp. 781-808, 1977.
5. N. S. Jayant et al., "A comparison of four methods for analog speech privacy," IEEE Trans. Commum., vol. COM-29, pp. 18-23, 1981.
6. L. S. Lee, G. C. Chou, and C. S. Chang, "A new frequency domain speech scrambling system which does not require frame synchronization," IEEE Trans. Commum., vol. COM-32, pp. 444-456, 1984.
7. L. S. Lee and G. C. Chou, "A new time domain speech scrambling system which does not require frame synchronization," IEEE J. select. Areas Commum., vol. SAC-2, pp. 443-455, 1984.
8. R. A. Meyer and C. S. Burrus, "A unified analysis of multirate and periodically time-varying digital filter," IEEE Trans. Circuits Syst. [Video Technol.], vol. CAS-22, pp. 162-168, 1975.

▲석 광 원(K. W. Seok) 1972년 11월 22일생

1995년:서울시립대 전자공학과 졸업
1995년~현재:동 대학원 전자공학과 재학중
※관심분야:제어 및 신호 처리, 의용 전자, 음성모델링

▲여 송 필(S. P. Yeo) 1953년 4월 16일생
1975년:숭실대 전자공학과 졸업
1980년:숭실대 전자과학과 공학석사
1991년~현재:서울시립대 전자공학과 대학원 재학중
※관심분야:제어 및 신호 처리

▲박 중 호(J. H. Park) 1970년 9월 7일생

1996년:서울시립대 전자공학과 졸업
1996년~현재:동 대학원 전자공학과 재학중
※관심분야:제어 및 신호 처리, 의용 전자

▲두 현 웅(H. W. Doo) 1970년 2월 15일생

1996년:서울시립대 전자공학과 졸업
1996년~현재:동 대학원 전자공학과 재학중
※관심분야:제어 및 신호 처리, 의용 전자

▲정 정 균(J. K. Jung) 1974년 2월 26일생

1996년:서울시립대 전자공학과 졸업
1996년~현재:동 대학원 전자공학과 재학중
※관심분야:제어 및 신호 처리, 의용 전자

▲김 성 환(S. H. Kim):제15권, 제1호 참조