음성통신 중 웨이브렛 계수 양자화를 이용한 비밀정보 통신 방법

이종관°
육군사관학교
c13525@kma.ac.kr

Secret Data Communication Method using Quantization of Wavelet Coefficients during Speech Communication

Jongkwan Lee°
Korea Military Academy

요 약

In this paper, we have proposed a novel method using quantization of wavelet coefficients for secret data communication. First, speech signal is partitioned into small time frames and the frames are transformed into frequency domain using a WT(Wavelet Transform). We quantize the wavelet coefficients and embedded secret data into the quantized wavelet coefficients. The destination regard quantization errors of received speech as seceret dat. As most speech watermark techniques have a trade off between noise robustness and speech quality, our method also have.

However we solve the problem with a partial quantization and a noise level dependent threshold. In additional, we improve the speech quality with de-noising method using wavelet transform. Since the signal is processed in the wavelet domain, we can easily adapt the de-noising method based on wavelet transform. Simulation results in the various noisy environments show that the proposed method is reliable for secret communication.

1. 머리말

본 논문에서는 음성신호의 웨이블렛 계수를 양자화하여 비밀정보를 송수신하는 방법을 제안한다. 비밀통신을 하는 방법에는 크게 통신하고자 하는 정보를 암호화하는 방법과 은닉하는 방법으로 나눌 수 있다. 암호화하는 방법은 통신을 도청하는 제3자가 비밀통신을 하고 있다라는 정보 자체는 노출될 수밖에 없어 제3자가 암호를 해독하려는 노력을 강구하게 한다. 그리고 현존하는 암호방법이 암호를 푸는 데 필요한 키를 구하는데 시간이 많이 걸린다는 것에 기초하고 있기 때문에 컴퓨터 기술의 발달로 언젠가는 해독될 수밖에 없는 한계를 가지고 있다. 하지만 비밀정보를 은닉하여 통신하는 방법은 비밀통신을 하고 있다라는 정보마저 도청하고 있는 제3자에게 제공하지 않기 때문에 제3자가 비밀통신을 알아내려고 하는 관심의 범주에서 벗어날 수 있다. 이러한 이유 때문에 도청하고자 하는 제3자에 대해 통신선로의 안전성을 완전히 보장받지 못하는 경우 비밀정보를 은닉하여 통신하는 방법은 정보를 암호화하여 통신하는 방법에 비해 안전할 수 있다.

이러한 비밀정보 송수신 방법으로 음성신호의 웨이블렛 계수의 양자화 오차에 비밀정보를 삽입하고 검출하여 비밀통신을 하는 방법을 제안한다. 양자화 오차를 이용한 정보 삽입 방법은 잡음에 강인하게 정보를 삽입하기 위해서는 양자화 레벨을 증가시켜 음질의 저하를 감수해야 하고 또 음질을 보존하기 위해서는 양자화 레벨을 감소시켜 삽입되는 정보의 강인성을 제한해야 하는 trade-off의 문제가 있었다. 하지만 제안한 방법은 웨이블렛 계수를 이용한 잡음제거 방법을 비밀정보 검출과 동시에 적용하고 웨이블렛 계수에 대해 부분적인 양자화를 하여 잡음에 강인하게 비밀정보를 삽입하면서도 음질을 보존할 수 있다.

본 논문은 2장에서 제안한 방법의 비밀정보 삽입과 검출 알고리즘에 대해 기술하고 3장에서 웨이블렛 계수를 이용한 잡음제거 방법과 제안한 방법과의 결합에 대해 살펴본다. 4장에서 실험을 통해 제안한 방법의 성능을 평가하고 5장 결론을 끝으로 논문을 맺도록 한다.

2. 제안한 비밀정보 송수신 알고리즘

대략적인 비밀정보 삽입 방법은 다음과 같다. 비밀정보는 웨이블렛 계수 영역에서 삽입되는데 프레임별로 WT(Wavelet Transform)를 한다. 웨이블렛 계수들에 대해 적절한 크기의 양자화 스텝으로 양자화를 하고 비밀정보를 삽입한다. 즉 양자화 오차가 비밀데이터가 되는 것이다. 이때 송수신측은 모두 어떤 양자화 레벨을 사용할 지 상호간 약속되어 있어야 한다. 비밀정보가 삽입된 웨이블렛 계수들은 IWT(Inverse WT)를 통해 다시 시간영역의 신호로 변환되어 전송된다. 수신단에는 도착한 음성에 대한 양자화 오차를 계산하여 비밀정보를 검출하고 웨이블렛을 이용한 잡음 제거 방법을 적용하여 음질을 향상시킨다.

2.1 비밀정보 삽입

구체적으로 비밀데이터가 삽입되는 과정은 다음과 같다. 윈도우를 사용하여 음성 신호를 짧은 길이의 프레임으로 나눈다.

$$s_m[n] = s[mN+n]u[n],\ n = 0, 1, 2, \ldots, N \quad (1)$$

이때, $u[n]$은 윈도우 함수, N은 윈도우 길이를 나타내며 m는 0부터 시작하는 프레임의 순서를 나타낸다. 각각의 프레임에 대해 WT를 하여 웨이블렛 계수를 추출한다. $c_m[k]$은 m번째 프레임의 k번째 웨이블렛 계수를 의미한다.

$$c_m[k] = WT(s_m[n]), k=1, 2, \ldots, N \quad (2)$$

이 웨이블렛 계수를 사전에 송·수신자가 약속한 양자화 스텝으로 양자화 한다. $Q(\cdot)$는 양자화 함수를 $c_{mq}[k]$는 양자화 결과를 나타낸다.

$$c_{mq}[k] = Q(c_m[k]) \quad (3)$$

한편, 비밀정보는 디지털 과정을 통해 2진수의 비트스트림으로 변환되고 각 음성프레임에 삽입될 길이의 비트스트림으로 나눠진다. m번째 음성프레임에 삽입될 비밀데이터를 $sd_m[n]$이라 하자. 이때 n의 길이는 음성 프레임의 길이 N보다 클 수 없다.

양자화된 웨이블렛 계수에 비밀 데이터를 일정한 레벨로 더하여 비밀정보가 삽입된 웨이블렛 계수 $c_{mqs}[k]$를 얻는다. α는 0보다 크며 양자화레벨보다는 작은 상수이다. α는 양자화스텝에 따라 잡음의 강인성과 음질 저하 방지를 위해 그 값이 변하는 상수이다.

$$c_{mqs}[k] = c_{mq}[k] + \alpha \cdot sd[k] \quad (4)$$

식 (4)의 웨이블렛 계수를 IWT하여 다시 시간 영역의 신호 $s_{mqs}[n]$로 변환된다. 위와 같은 과정을 매 프레임마다 반복 수행한다. 그림 1은 입력이 음성신호에 비밀통신문이 삽입되는 전체 알고리즘을 도식화한 것이다.

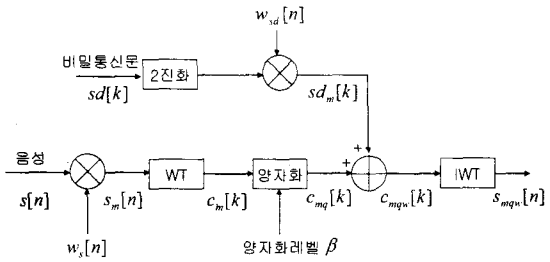

그림 1 비밀 정보 삽입 과정

양자화 레벨이 크면 클수록 삽입된 비밀정보는 잡음에 강인하게 되지만 양자화 오차를 많이 발생시켜 음질의 저하를 초래한다. 반면 양자화 레벨이 작으면 작을 수록 양자화 오차가 작기 때문에 음질은 보존될 수 있는 반면 삽입된 비밀정보는 전송 도중 잡음에 의해 왜곡될 수 있는 확률은 높아지게 된다. 이와 같이 잡음 강인성과 음질 보존 사이에는 trade-off가 발생하기 때문에 잡음 강인성을 가지면서 음질을 보존할 수 있는 적절한 양자화 레벨을 구하는 것이 제안한 방법의 성능을 크게 좌우하게 된다.

2.2. 비밀 정보 검출

수신 음성 신호에 대해 프레임별로 WT를 실시하고 송신측에서 사용한 동일한 양자화 레벨로 양자화를 한다. 양자화 오차를 워터마크 신호로 검출한다. 수신한 음성신호의 프레임을 $r[n]$, $r[n]$에 대한 WT 결과를 $rc[k]$라 하자. 양자화 오차는 아래와 같이 계산된다.

$$e_q[k] = |rc[k] - Q(rc[k])| \quad (5)$$

계산된 $e_q[k]$는 식(6)에 의해 0과 1의 비트스트림 신호 $\widehat{sd}[k]$로 변환된다.

$$\widehat{sd}[k] = \begin{cases} 1, & TH_1 < e_q[k] < TH_2 \\ 0, & otherwise \end{cases} \quad (6)$$

식 (6)에서 TH_1, TH_2는 양자화오차를 0과 1을 판별하기 위한 문턱값이다. 전송 채널에 더해지는 잡음의 pdf(Probability Distribution Function)가 가우시안(Gaussian) 분포이고 양자화레벨이 β라 하자. 식 (4)에서 일반적으로 $\alpha = \frac{\beta}{2}$로 정의된다. 즉, 전송하고자 하는 비밀데이터가 0일 때는 원본 신호에 0을 더하고 비밀데이터가 1일 때는 원본 신호에 $\beta/2$를 더하는 것이다.

$$f(x, \sigma, \mu=0) = \frac{1}{\sigma\sqrt{2\pi}} \exp(-\frac{x^2}{2\sigma^2}) \quad (7)$$

$$f(x, \sigma, \mu=\frac{\beta}{2}) = \frac{1}{\sigma\sqrt{2\pi}} \exp(-\frac{(x-\beta/2)^2}{2\sigma^2}) \quad (8)$$

식 (7), (8)은 각각 비밀정보가 0과 1일 때 수신측에서의 확률밀도함수이다. 비밀정보 0을 보낼 때는 분산이 σ이고 평균이 0인 가우시안 분포이고 1을 보낼 때는 분산이 σ이고 평균이 β인 가우시안 분포가 된다. 따라서 그림 2에서와 같이 수신측에서 에러를 최소화 하는 방법은 문턱값 TH_1, TH_2 을 각각 $\beta/4$, $3\beta/4$로 하는 것이다. 이때 전송 에러확률 P_F는 $2 \cdot erfc(\beta/4)$이고 전송 성공확률 P_D은 $1 - 2 \cdot erfc(\beta/4)$이다. 즉 같은 확률 특성을 갖는 잡음환경일 때 양자화레벨 β가 클수록 에러는 작아진다. 하지만 양자화레벨이 커질수록 양자화오차가 커지기 때문에 음질의 저하를 야기할 수 있다. 따라서 비밀정보 삽입으로 인한 음질 저하 방지와 에러 확률의 최소화 사이에는 trade-off가 발생한다.

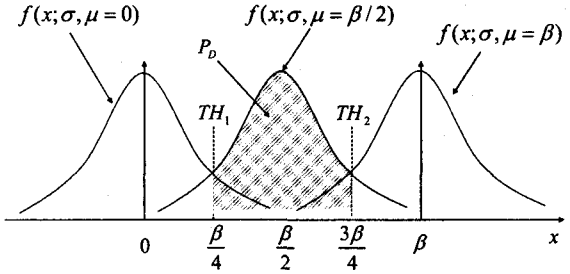

그림 2 문턱값의 결정

그림 3는 입력 음성 프레임이 $r_m[n]$이라 할 때 비밀정보를 검출하는 전체 알고리즘을 대략적으로 도식화한 것이다.

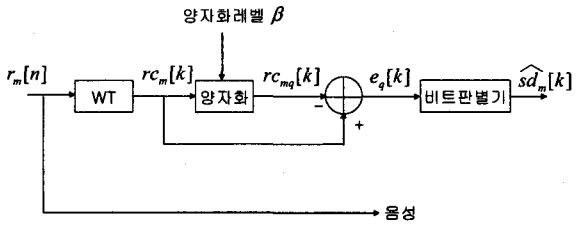

그림 3 비밀정보 검출 과정

3. 웨이블렛을 이용한 잡음 제거

웨블렛 변환은 잡음을 제거하는 강력한 도구로 최근 등장하였다. Donoho와 Johnston은 웨이블렛 변환을 이용하여 웨이블렛 계수를 간단히 조작함으로써 잡음을 제거하는 방법을 제안하였다. 잡음제거 방법은 다음과 같이 3단계 과정을 거친다.

① 오염된 음성 신호를 웨이블렛 변환한다.
② 웨이블렛 계수들을 적절한 문턱값을 설정하여 조작하여 잡음을 제거한다.
③ 조작된 웨이블렛 계수들을 IWT하여 잡음 제거된 신호를 얻는다.

적절한 문턱값을 설정하고 웨이블렛 계수를 조작하는 자세한 방법은 [6, 7]을 참고한다.

제안한 방법은 3장에서 설명한 바와 같이 웨이블렛 계수들을 이용하여 비밀정보를 삽입한다. 따라서 비밀정보를 검출하는 과정에서 웨이블렛 변환을 이용한 잡음 제거 방법을 쉽게 적용할 수 있어 전송과정에서 저하된 음질을 향상시킬 수 있다. 이는 잡음에 강인한 비밀정보 삽입을 위해 양자화 레벨을 증가시켜 저하된 음질을 향상시킬 수 있는 방안이 된다.

5. 실험 결과

제안한 비밀정보 송수신 방법의 성능을 평가하기 위해 다양한 잡음 환경에서 실험을 하였다. 송신 음성 신호는 8KHz로 표본화되고 16bit로 양자화된 PCM 신호이다. 음성은 32ms 단위로 해밍 윈도우(Hamming Window)를 이용하여 프레임화 하였다. 비밀정보가 삽입되는 웨이블렛 계수만을 양자화하여 음질 저하를 최소화하였다.

먼저 다양한 잡음환경 및 양자화레벨 β에 따라 송신단에서 제안한 방법에 의해 삽입된 비밀정보가 수신단에서 얼마나 정확하게 검출되는지 알아본다. 한 프레임당 256개의 웨이블렛 계수 중에서 8개의 계수에만 비밀정보를 삽입하였다. 표 1은 800비트의 비밀데이터를 삽입하였을 때 수신측에서의 오류가 발생한 비트의 개수이다.

표에서 보는바와 같이 양자화레벨이 커질수록 에러 비트의 개수는 급격이 줄어든다. 하지만 양자화레벨의 증가는 양자화오차에 의한 음질 저하의 원인이 된다. 한편 SNR이 증가할수록 에러 비트의 개수는 감소함을 알 수 있다. 따라서 음질의 저하를 막고 에러확률을 낮추기 위해서는 잡음환경에 따라 양자화레벨을 적절하게 조정할 필요가 있다.

SNR / 양자화 레벨	5dB	10dB	15dB	20dB	25dB
β	377	276	65	3	0
1.5β	323	122	9	0	0
2β	215	39	1	0	0
2.5β	148	9	0	0	0
3β	81	3	0	0	0

표 1 양자화레벨 및 잡음환경에 따른 에러 비트 개수

제안한 방법에 의한 음질의 저하를 평가하기 위한 음질 측정은 각 음성 신호의 평균 로그 스펙트럼 거리(LSD: log-spectral distance)로 판단하였다[4, 5]. 측정한 두 신호 사이의 거리가 0이면 두 신호는 동일한 신호이며 거리가 멀수록 서로 다른 신호로 판단할 수 있다.

다음은 실제 제안한 방법으로 송신단에서 비밀정보를 삽입하고 수신단에서 검출한 결과이다. 비밀정보는 'Sixty and two years ago, Sejong University launched'이다. 표 1의 결과를 토대로 잡음환경이 5dB일 때는 양자화 레벨을 3β 10dB일 때는 2.5β등 SNR이 높아질수록 양자화 레벨은 작게 선택하였다. 비밀정보가 삽입되기 전의 음성신호를 s(t), 비밀정보가 삽입된 이후 채널잡음에 의해 오염된 신호를 y(t)라 하였을

때 음질을 평가하기 위해 s(t)와 y(t) 사이의 로그스펙트럼 거리 LSD1를 계산하였다. 그리고 웨이브렛 변환을 이용한 잡음제거 방법에 의해 처리된 음성 신호 $\hat{s}(t)$와 비밀정보 삽입전의 음성 신호 s(t)의 로그스펙트럼 거리 LSD2를 계산하여 음질 저하 정도를 평가하였다.

SNR / 양자화레벨	수신 통신문	LSD1/ LSD2
5dB / 3 β	□ lt3 UnF tWo$)ecrR aDl SLhmgDUnivEr3Ydy, lau.IhEd	2.37/ 2.18
10dB / 2.5 β	Sixty and two years ago, CgZong!UNiversity lau.sled	2.05/ 1.88
15dB / 2 β	Sixty and two years ago, Sejong University, launched	1.75/ 1.67
20dB / 1.5 β	Sixty and two years ago, Sejong University, launched	1.46/ 1.44
25dB / β	Sixty and two years ago, Sejong University, launched	1.17/ 1.16

표 2 제안한 방법에 의한 비밀정보 수신 결과

송신문: Sixty and two years ago, Sejong University launched

표 2에서 보는 바와 같이 SNR이 5dB이고 양자화 레벨이 3 β인 경우 비밀정보가 제대로 수신되지 않았다. 그리고 SNR이 10dB이고 양자화레벨이 2.5 β인 경우 일부 문자가 제대로 수신되지 못했지만 의미 파악을 할 수 있는 정도이다. 하지만 그 외의 경우에는 완벽하게 비밀정보를 수신할 수 있었다. 한편 웨이브렛 변환을 이용한 잡음 제거 방법을 통하여 음질을 개선하였다. 웨이블렛 잡음 제거 전의 LSD1과 잡음 제거 후의 LSD2를 비교하면 모든 경우에 대해 음질이 개선되었음을 알 수 있다.

6. 결론 및 발전방향

본 논문에서 음성 신호의 웨이블렛 계수 양자화를 이용한 비밀 정보 송수신 방법을 제안하였다. 제안한 방법은 양자화 레벨에 따라 삽입된 비밀 정보의 잡음에 대한 강인성과 비밀 정보 삽입으로 인해 발생하는 음질의 저하 사이에 trade-off가 발생하므로 제안한 방법의 성능을 극대화하기 위해서는 잡음 환경에 따라 적절한 양자화 레벨을 설정할 필요가 있다. 상반되는 두 가지 특성을 만족시키기 위해 모든 웨이블렛 계수를 양자화하지 않고 비밀정보가 삽입되는 계수들에만 양자화를 하였고 추가적으로 음질의 저하를 최소화하기 위해 웨이블렛 변환을 이용한 잡음제거 방법을 함께 사용하였다. 비밀정보 삽입 및 검출이 웨이블렛 영역에서 처리되므로 웨이블렛 변환을 이용한 잡음제거 방법은 제안한 방법과 동시에 사용이 가능하였다. 이를 통해 음질의 저하를 방지하면서 잡음에 강인하게 비밀정보 삽입을 하였다.

제안한 방법에서 양자화 레벨, 윈도우 길이, 프레임별 삽입된 비밀 정보의 길이, 사용한 웨이블렛의 종류 등이 암호화 키와 같은 역할을 할 것이다. 즉 제3자가 제안한 방법을 이용한 비밀정보 송수신 여부를 알더라도 비밀정보의 내용을 알기 위해서는 앞서 언급한 파라미터들을 정확히 알고 있어야 한다. 만약 삽입되는 비밀정보를 암호화 한다면 제안한 방법의 안전성은 보다 향상될 수 있다.

한편 비밀정보의 에러 검출 및 정정을 위한 부호화 방법을 사용하고 정확한 VAD(Voice Activity Detector)를 이용하여 채널 잡음에 대한 정보를 정확히 추출할 수 있다면 가장 최적화된 양자화 레벨을 쉽게 결정할 수 있어 제안한 방법의 성능이 크게 향상될 것이다. 제안한 방법이 실제적인 상황에서 적용되기 위해서는 향후 다양한 채널 잡음 환경에서의 실험을 통해 적절한 양자화 레벨 선택 방법에 대한 연구가 필요할 것이다.

참 고 문 헌

[1] Stefan Katzenbeisser and Fabien A.P. Petitcolss, "Information Hiding techniques for steganography and digital watermarking", Artech House Inc, 2000.

[2] Fabien A.P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, "Information Hiding - A Survey", Proc. of the IEEE, special issue on protection of multimedia content, pp 1062-1078 , July 1999.

[4] S. Quanckenbush, T. Barnwell and M. Clements, "Objective Measure of Speech Quality", Prentice Hall, U.S.A., 1988.

[5] L. Thorpe and W. Yang, "Performance of Current Perceptual Objective Speech Quality Measure.", IEEE Workshop on Speech Coding Processings, pp. 144-146, June 1999.

[6] D.L. Donoho, "Nonlinear wavelet methods for recovering signals, images and densities from indirect and noisy data," Proceedings of Symposia in Applied Mathematics, vol.47, pp. 173-205, 1993.

[7] D.L. Donoho, "De-noising by soft-thresholding," IEEE Trans. Inform. Theory, vol. 41, no 3, pp. 613-627, May, 1995.

[8] D.L. Donoho and I.M. Johnstone, "Ideal spatial adaptation by wavelet shrinkage", Biometrika, vol. 81, no.3, pp. 425-255, 1994.

[9] Jong Kwan Lee and Chang D. Yoo, "Wavelet Speech Enhancement Based on Voice/Unvoiced Decision," in Proceedings of Internoise 2003, pp. 4149-4156, Jeju, Seogwipo, Aug. 2003.