군 통신상에서 워터마킹 기술을 이용한 피아식별 방법

Identifying Friendly and Foe using a Watermarking Technique during Military Communication

이 종 관* 최 현 주*
Lee, Jong-Kwan Choi, Hyun Joo

ABSTRACT

In this paper, a watermark technique for identifying friendly and foe is proposed during communication. The speech signal is processed in several stages. First, speech signal is partitioned into small time frames and the frames are transformed into frequency domain using DFT(Discrete Frequency Transform). The DFT coefficients are quantized and the watermark signal is embedded into the quantized DFT coefficients. At the destination channel quantization errors of received signal are regarded as the watermark signal. Identification of friendly and foe are done by correlating the detected watermark and the original watermark. As in most other watermark techniques, this method has a trade off between noise robustness and quality. However, this is solved by a partial quantization and a noise level dependent quantization step.

Simulation results in the various noisy environments show that the proposed method is reliable for identification between friendly and foe.

주요기술용어(주제어) : Watermark(워터마크), DFT(이산 푸리에 변환), Quantization(양자화), Correlation Value(상관값)

1. 머리말

우리가 최근 세계 각국에서 일어나고 있는 정규전의 양상에서 본 것과 같이 또 많은 군사전문가들이 예측한 바와 같이 미래의 전쟁 아니 현재의 전쟁은 정보전자전에 기반하고 있다. 아군의 정보활동은 보장하고 적의 정보활동은 방해하는 정보전은 적의 전자기파를 도청하여 적의 의도 파악, 적을 기만하여 왜곡된 정보 제공으로 지휘통제체계 혼란 등 다양한 형태로 나타날 수 있다[1]. 유사시 적의 주요활동은 아군의 유·무선 통신 중에 유통되는 정보의 획득에 치중할 것은 자명하다.

구리, 광섬유 등의 전송매체를 사용하는 유선통신에 비해 전파를 전송 매체로 사용하는 군의 무선 통신은 이러한 적의 정보전 활동에 가장 취약한 부분이라 할 수 있다. 또한 무선 환경에 비해 전송채널 상에서 보다 안전한 보안성을 제공하기는 하지만 유선통신도 적의 도청 및 기만에 완벽하게 안전한 것은

† 2006년 8월 8일 접수~2006년 11월 20일 게재승인
* 육군사관학교(Korea Military Academy)
주저자 이메일 : c13525@kma.ac.kr

아니다. 또한 미래의 가상 적을 북한이라 가정하였을 때 피아가 동일한 언어를 사용하는 특수성을 고려하면 적이 아군의 유·무선통신을 도청하고 자신을 아군으로 오인케 기만하여 아군의 지휘통신체계를 교란시킬 여지가 충분히 있다. 신속하고 명확한 지휘통신체계의 유지가 전쟁의 승패를 좌우하는 중요한 요소임을 생각할 때 이에 대한 기술적, 전술적 대비가 반드시 필요할 것이다.

본 논문은 이러한 불명확한 피아식별에서 유발될 수 있는 정보전의 위험요소를 워터마킹을 이용하여 기술적으로 방지하는 방법을 제안한다. 제안한 방법은 송신측은 유·무선 음성정보에 피아를 식별할 수 있는 피아식별 정보(워터마크)를 원래의 음질에 큰 영향을 주지 않는 범위에서 삽입하고 수신측은 삽입된 워터마크를 적절히 추출하여 이를 바탕으로 통신하고 있는 상대방의 피아를 식별한다.

본 논문은 2장에서 현재 군 무선통신 상에서 피아를 식별하는 방법과 문제점, 그리고 새로운 피아식별 방법의 필요성에 대해서 살펴보고 3장에서는 워터마킹 기술에 대해 간단히 알아본다. 제안한 워터마킹 기술을 이용한 피아식별 방법에 대해 4장에서 자세히 살펴보고 다양한 채널 잡음 환경에서 제안한 피아식별 방법의 성능을 5장에서 실험을 통해 평가한다. 마지막 6장에서 제안한 방법의 발전 방향을 제시하고 결론을 끝으로 논문을 맺도록 한다.

2. 군 통신의 피아식별 방법 및 문제점

현재 군에서 통신 시 사용하는 피아식별 방법을 간단히 소개하면 다음과 같다. 피아식별을 원하는 통신소는 상대방에게 몇 개의 숫자를 전달한다. 상대 통신소는 사전에 상호 약속된 연산 방법으로 받은 숫자에 대해서 연산을 하고 그 결과를 통보한다. 연산 결과를 통보 받은 통신소는 연산결과가 맞으면 아군으로 그렇지 않으면 적군으로 의심되는 통신소로 구분하게 된다. 이러한 방법은 비교적 간단하고 쉽게 피아를 식별할 수 있다는 장점이 있다. 하지만 숫자를 서로 주고받고 연산을 하고 결과를 통보하며 그 연산결과를 다시 확인하는 과정에서 적지 않은 시간이 소요될 수밖에 없다. 또한 통신 사용자 입장에서는 정보를 유통시키기 위한 사전 절차가 필요하다는 불편함이 있다. 따라서 신속한 정보유통을 필요로 하는 군통신 환경에서 이러한 피아식별 절차는 부적절하다 할 수 있다. 그러므로 신속한 정보유통을 필요로 하는 현대 전장을 고려할 때 통신을 위해 부가적인 사용자의 조작이 필요 없고 빠르게 피아를 식별할 수 있는 새로운 방법이 필요하다.

3. 워터마킹 기술[2,3]

디지털 기술의 발전과 그 편의성으로 인해 과거 아날로그 형태로 유통, 저장되었던 정보(이미지, 비디오, 음성, 오디오 등)들이 디지털 형태로 바뀌었다. 이로 인해 사용자의 정보 접근성은 크게 증가하였으나 이에 대한 역효과로 사용자가 저작권이 있는 정보를 불법적으로 쉽게 조작, 변경, 복제, 유통 시켜 컨텐츠 제작 업체의 물질적 피해를 증가시켰다. 이러한 불법적 활동을 방지하기 위해 원본 정보에 사용자들이 알아볼 수 없는 형태의 저작권 정보를 삽입하는 것이 워터마킹 기술이다. 워터마킹 기술을 이용하여 불법적으로 유통되는 정보들에 대해 사후에 원소유권자가 자신의 소유권을 워터마킹을 추출함으로써 증명할 수 있게 된다.

워터마킹 기술의 기본적인 개념은 다음과 같다. 원소유권자의 소유권을 증명할 수 있는 정보(예를 들면, 자신의 회사 로고 형태의 이미지, 비디오, 오디오, 음성 등)를 I라 하고 이것의 보안성을 강화하기 위해 암호화 하는 키(key)를 k라 하면 원정보에 삽입되는 워터마크 정보는 아래와 같이 표현될 수 있다.

$$w = f_0(I, k) \tag{1}$$

워터마크 정보는 원정보(X)의 질(quality)를 저하시키지 않는 범위에서 그리고 워터마크 정보를 변형시키는 각종 인위적, 비인위적 공격에 강인하도록 삽입되어 워터마크 정보가 삽입된 정보(Y)를 생성한다.

$$Y = f_1(X, w) \tag{2}$$

실제 유통되는 정보는 X가 아니라 Y이다. Y에 대해 워터마크 정보 w와 자신의 소유권을 증명할 수 있는 정보 I를 다시 추출하기 위한 방법에는 크게 두 가지로 구분할 수 있다.

$$\hat{I} = g(X, Y, k) \tag{3}$$

$$\hat{I} = g(Y, k) \tag{4}$$

Y로 부터 $\hat{I}$을 추출하기 위해 식 (3)와 같이 원정보 X를 필요로 하는 non-blind 워터마킹 방법과 식 (4)와 같이 원정보 X를 필요로 하지 않는 blind 워터마킹 방법이 있다.

Y가 유통되다가 저작권 문제의 법적 분쟁이 발생하였을 때 원소유권자는 Y에 대해서 식 (3) 또는 (4)의 방법으로 자신의 소유권을 증명해 줄 수 있는 정보 $\hat{I}$를 추출하여 자신의 소유를 주장하게 되는 것이다.

워터마킹 기술은 대립되는 두 가지 요구조건이 있다. 하나는 질(quality) 측면에서 사용자가 인지할 수 없을 정도로 워터마크가 삽입된 정보 Y는 원정보 X와 큰 차이가 없어야 하기 때문에 워터마크의 에너지가 최대한 작아야 한다는 것이다. 하지만 한편으론 유통 과정에서 생기는 각종 변형에 강인해야 하기 때문에 잡음 강인성 측면에서는 워터마크의 에너지가 최대화 되어야 한다[3]. 이렇게 대립되는 두 가지 요구조건을 만족하는 최적화된 알고리즘을 구현하는 것이 워터마킹 기술의 핵심이라 할 수 있다.

앞서 소개한 바와 같이 워터마킹 기술의 원래 목적은 디지털화된 콘텐츠의 불법 복제 방지에 있었으나 워터마킹 기술의 데이터 은닉의 효과를 이용하여 여러 분야에서 다양하게 응용, 활용될 수 있다. 예를 들어 평범하게 보이는 이미지 정보에 비밀 통신문을 삽입하여 적으로부터 안전하게 명령을 전달할 수 있는 비밀통신에 사용할 수 있으며 통신 중에 상호 약속된 특정 패턴의 정보를 음성, 영상, 비디오에 삽입하여 통신 상대자의 신분을 확인할 수 있는 인증에도 사용이 가능하겠다.

4. 피아식별을 위한 워터마킹 방법 제안

현재 사용되고 있는 군통신 상에서의 피아식별 방법은 피아식별 과정의 시간이 많이 소요되고 사용자가 직접 피아식별을 수행해야 하며 실제 정보를 유통시키기 위한 사전 작업이 필요하다는 불편함이 있다. 그래서 워터마킹을 이용해 기술적으로 피아식별을 자동적으로 수행하여 신속한 정보유통을 보장하는 방법을 제안한다.

가. 기술적 요구사항 및 특징

워터마킹 기술을 이용한 군통신 상 피아식별 방법은 다음과 같은 요구사항을 만족해야 한다. 첫째, 통신을 시작하여 중요 정보를 전달하기 전에 피아식별이 이루어져야 한다. 무선의 경우 호출명을 호명하였을 때 이미 피아식별이 이루어져야 하고 유선인 경우 자신의 신분을 밝히는 몇 초 사이에 피아식별이 이루어져야 한다. 둘째, 워터마킹 정보의 삽입으로 음질의 변화를 사용자가 느낄 수 없어야 한다. 피아식별로 인해 중요 정보 전달이 왜곡된다면 피아식별의 의미가 반감된다. 셋째, 잡음에 강인해야 한다. 군통신의 채널 특성상 강한 잡음에도 피아식별을 위한 워터마킹 정보의 추출이 가능해야 한다.

또한 군통신 중 피아식별을 위해 사용되는 워터마킹 기술의 특징은 다음과 같다. 첫째, 통신 중의 피아식별이므로 원본 정보를 알 수 없다. 따라서 피아식별을 위해 사용될 워터마크 기술은 워터마크 정보를 추출하기 위해 원본 정보를 이용할 수 없는 blind 워터마킹 기술이다. 둘째, 피아식별을 위해 삽입되어야 하는 정보의 양이 많을 필요가 없다는 것이다. 만약 비밀통신을 위해 워터마킹 기술을 사용한다면 많은 워터마크 정보의 삽입이 필수적이지만 본 논문에게 다루고자 하는 문제는 적인지 아군인지만을 구분하기 때문에 많은 워터마크의 삽입이 필요하지 않다. 셋째, 보안성의 향상을 위해 워터마크 정보에 대한 암호화가 필요하다.

위와 같은 군통신 중 피아식별 방법 구현에 있어 만족해야 하는 요구사항과 워터마크 기술의 특징을 기초로 다음과 같이 피아식별을 위한 워터마킹 삽입 및 검출 방법을 제안한다.

나. 전체 피아식별 방법 소개

제시하는 방법은 음성 정보를 프레임 단위로 처리하게 되는데 프레임 단위로 DFT(Discrete Fourier Transform)를 한 후 DFT 계수에 대해 양자화를 한다. 그리고 양자화된 DFT 계수에 워터마크 정보를 더한다. 여기서 양자화 레벨이 크면 삽입할 수 있는 워터마크 정보의 에너지도 크게 되어 상대적으로 잡음에 강인하게 되고 반면에 음질은 저하 된다. 반대로 양자화 레벨이 작으면 작을수록 삽입되는 워터마크 정보의 에너지는 작고 따라서 잡음에 강인할 수 없게 된다. 하지만 작은 에너지의 워터마크 신호를 삽입했기 때문에 음질은 크게 저하되지 않게 된다. 이와 같이 잡음의 강인성과 음질 보존 사이에서의 trade-off를 통신 환경에 따라 적응화 시키는 것이 제안한 피아식별 방법이 해결해야할 중요한 문제이다[4]. 우리는 위와 같은 trade-off 문제를 해결하기 위해 양자화 레벨을 일정 수준 이상으로 유지하여 잡음 강인성을 확보한 상태에서 음질을 향상시키는 방법을 사용하였다.

1) 워터마크 삽입

워터마크 정보의 삽입은 주파수 영역에서 수행된다. 음성 신호는 윈도우를 사용하여 짧은 길이의 프레임으로 나눠진다.

$$s_m[n] = s[mN+n]w[n],\ \mathrm{n} = 0, 1, 2, \ldots, \mathrm{N} \quad (5)$$

이때, w[n]은 윈도우 함수, N은 윈도우 길이를 나타내며 m는 0부터 시작하는 프레임의 순서를 나타낸다.

각각의 프레임에 대해 DFT를 하여 DFT 계수를 추출한다.

$$S_m[k] = \sum_{n=0}^{N-1} s_m[n] e^{-j\frac{2\pi nk}{N}},\ k = 0, 1, \ldots, N-1 \quad (6)$$

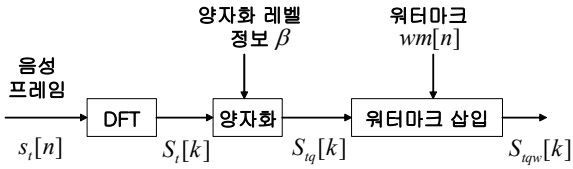
이 DFT 계수를 사전에 송·수신자가 약속한 양자화 레벨로 양자화 한다. $Q(\bullet)$는 양자화 함수를 $S_{mq}[k]$는 양자화 결과를 나타낸다.

$$S_{mq}[k] = Q(S_m[k]) \quad (7)$$

wm[n]을 워터마크 정보라 할 때 양자화된 DFT 계수에 워터마크 정보를 삽입하여 워터마크가 삽입된 DFT 계수 $S_{mqw}[k]$를 얻는다. α는 양자화 레벨에 따라 변하는 상수이다.

$$S_{mqw}[k] = S_{mq}[k] + \alpha \bullet wm[n] \quad (8)$$

식 (8)의 DFT 계수를 IDFT (Inverse DFT)하여 다시 시간 영역의 신호 $s_{mqw}[n]$로 변환하게 된다. 위와 같은 과정을 매 프레임마다 반복 수행한다. 그림 1은 입력 음성 프레임을 $s_t[n]$이라 했을 때 워터마크가 삽입되는 전체 알고리즘을 도식화한 것이다.



[그림 1] 워터마크 삽입 알고리즘

2) 워터마크 검출

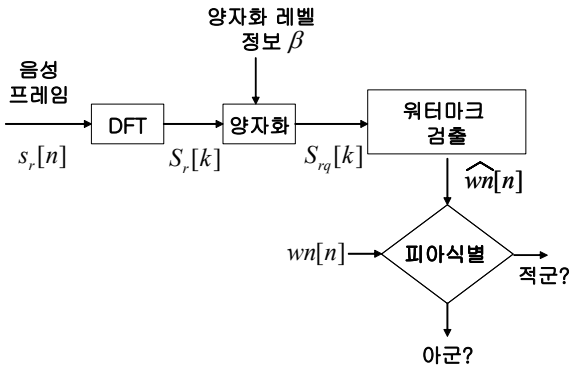
수신 신호에 대해 DFT를 실시하고 송신측에서 사용한 동일한 양자화 레벨로 양자화를 한다. 양자화 오차를 워터마크 신호로 검출한다. 수신한 음성신호의 m번째 프레임을 $y_m[n]$, $y_m[n]$에 대한 DFT 결과를 $Y_m[k]$라 하자. 검출된 워터마크 정보 $\widehat{wm}[n]$는 아래와 같이 계산된다.

$$\widehat{wm}[n] = Y_m[k] - Q(Y_m[k]) \quad (9)$$

검출된 워터마크 wm[n]은 원래 워터마크 $wm[n]$과의 상관값 $\lambda(wm, \widehat{wm})$를 측정하여 미리 설정된 문턱값 TH 보다 클 경우 아군으로 그렇지 않을 경우 적군으로 피아를 식별하게 된다.

$$decision = \begin{cases} our\ \ army, \lambda(wm, \widehat{wm}) > TH \\ enemy\ \ \ \ \ , \lambda(wm, \widehat{wm}) < TH \end{cases} \quad (10)$$

그림 2는 입력 음성 프레임이 $s_r[n]$이라 했을 때 워터마크를 검출하고 피아식별을 하는 전체 알고리즘을 대략적으로 도식화한 것이다.



[그림 2] 워터마크 검출 및 피아식별 알고리즘

3) 음질 향상 방안

앞서 언급한 바와 같이 양자화 레벨과 잡음 강인성은 상호 trade-off가 발생한다. 이는 모든 워터마킹 기술에서 해결해야할 근본적 문제이다. 그런데 군통신 환경이라는 특수성을 고려할 때 큰 양자화 레벨 사용으로 인한 음질 저하 보다는 잡음 강인성이 우선시 되어야 한다. 따라서 본 논문에서는 워터마크 정보가 최소한의 잡음 강인성을 확보하기 위해 양자화 레벨을 일정 수준 이상으로 유지하고 저하된 음질을 향상시키기 위한 방안을 고려한다.

제안한 방법으로 워터마킹을 삽입했을 때 음질이 저하되는 근본적인 이유는 양자화 오차와 워터마크 정보의 삽입에 의한 원신호와의 오차이다. 이러한 오차에서 발생하는 음질의 저하를 최소화하기 위한 방안에는 다음과 같은 것들이 있다.

첫째, 양자화 오차를 최소화하기 위해 워터마크 정보를 삽입하는 DFT 계수만을 양자화 하는 방법이 있다. 만약 256개의 DFT 계수 중에 실제 워터마크 정보가 삽입되는 128개의 DFT 계수만을 양자화 하게 되면 그 만큼 양자화 오차는 반으로 줄어들게 되어 음질을 향상시킬 수 있다. 그런데 이러한 방법을 사용하게 되면 삽입할 수 있는 워터마크 정보의 양은 제한을 받게 된다. 하지만 서두에 언급한 바와 같이 피아식별을 위한 워터마킹 방법은 많은 데이터를 삽입할 필요가 없기 때문에 이와 같은 방법은 음질을 향상시키기 위한 좋은 방안이 될 수 있다.

음성은 크게 에너지가 큰 유성음과 상대적으로 에너지가 작은 무성음으로 구분된다. 같은 크기의 잡음이 유성음, 무성음에 더해졌다고 했을 때 유성음 보다 무성음의 음질의 저하가 크다. 따라서 음질을 보존하기 위한 두 번째 방법으로 워터마크 삽입과 양자화를 유성음에만 하는 방안이 있다. 이 방안은 유·무성음을 정확히 구분할 수 있는 알고리즘이 필요하다. DFT 계수 내에 에너지가 큰 계수만을 선택하여 양자화와 워터마크 삽입을 하는 것도 음질을 향상시킬 수 있는 방안이 될 수 있다. 하지만 DFT 계수의 상대적 크기는 송·수신간 발생하는 채널 잡음에 매우 민감하게 변하기 때문에 실제 적용은 어렵다.

셋째, 채널 잡음을 정확하게 예측할 수 있다면 양자화 레벨을 채널 잡음의 크기에 따라 유연하게 변화시켜주는 것도 음질을 향상시키는 방법이 될 수 있다. 만약 채널 잡음이 심하다면 잡음에 강인하도록 양자화 레벨을 크게 하고 큰 에너지의 워터마크를 삽입하는 것이다. 반대로 채널 잡음이 심하지 않다면 양자화 레벨의 크기를 작게 하여 음질의 저하를 막을 수 있다.

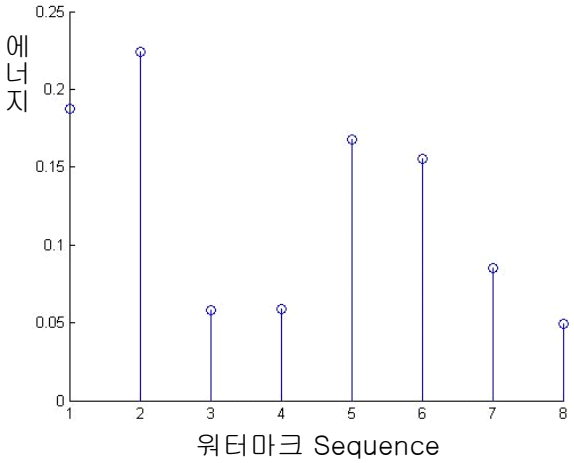
5. 실험결과

제안한 워터마킹 방법의 성능을 평가하기 위해 다양한 잡음 환경에서 피아식별 능력을 실험하였다. 송신 음성 신호는 8KHz로 표본화되고 16bit로 양자화된 PCM 신호이다. 음성은 32ms 단위로 해밍 윈도우(Hamming Window)를 이용하여 프레임화 하였다.

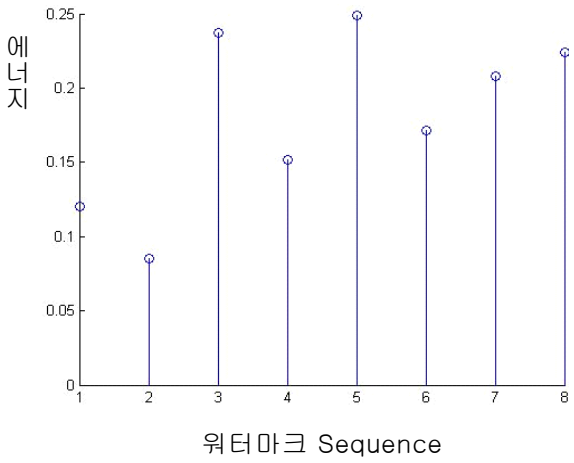
총 78개의 프레임 중 처음부터 39번째의 프레임에만 워터마크를 삽입하였다. 워터마크의 길이는 8비트이며 [1, 1, 0, 0, 1, 1, 0, 0] 라는 정보를 갖고 있다. 워터마크가 삽입되는 8개의 DFT 계수만을 양자화하여 음질의 저하를 최소화하였다.

그림 3은 SNR(신호대 잡음비)이 20dB이고 양자화 레벨이 β일 때 수신 측에서 워터마크 신호를 검출한 결과이다.

그림을 통해 알 수 있듯이 비교적 쉽게 워터마크정



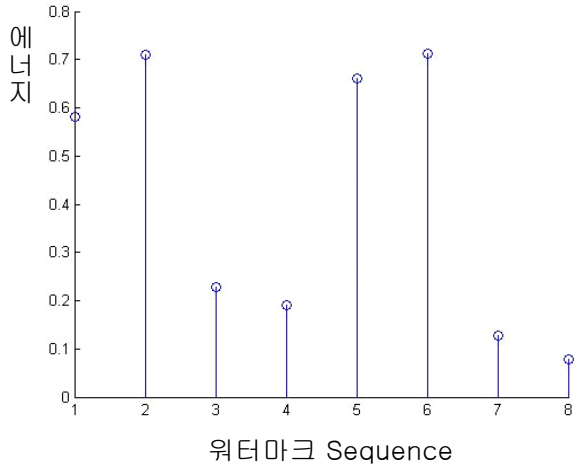
[그림 3] SNR이 20dB, 양자화 레벨이 β일 때 워터마크 검출



[그림 4] SNR이 10dB, 양자화 레벨이 β일 때 워터마크 검출

보를 식별할 수 있고 음질 확인 결과 음질의 저하도 크지 않다. 그림 4는 SNR이 10dB인 것을 제외하고 그림 3의 실험 조건과 모두 동일할 때 워터마크를 추출한 결과이다. 양자화 레벨에 비해 잡음의 영향이 커 정확한 워터마크 검출이 불가능하다.

하지만 양자화 레벨을 3β로 하고 워터마크 에너지를 3배로 하여 음질의 저하를 감수하면 그림 5와 같이 비교적 명확하게 워터마크를 검출할 수 있다. 실험에 의하면 채널 잡음에 의해 SNR이 10dB가 되었



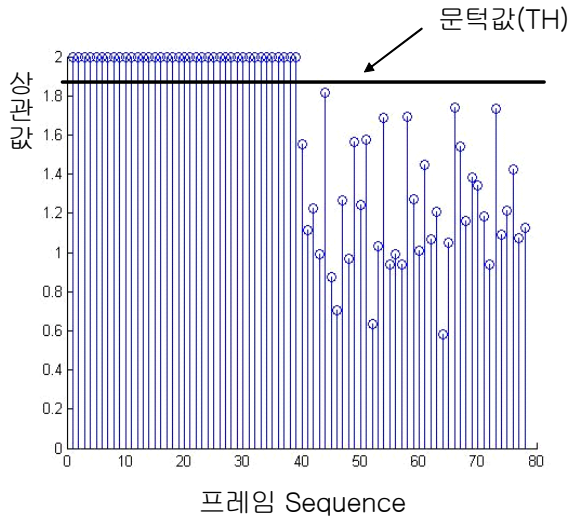
[그림 5] SNR이 10dB, 양자화 레벨이 3β 일 때 워터마크 검출

기 때문에 큰 양자화 레벨을 사용하여 발생하는 양자화 오차에 의한 음질 저하는 상대적으로 크지 않다. 또한 워터마크가 삽입되는 DFT 계수만을 양자화 하였기 때문에 양자화 오차의 영향은 제한적인 것으로 판단된다.

이와 같이 채널 환경에 의해 선택되어지는 양자화 레벨과 워터마크 정보 에너지는 시스템의 성능을 결정 하는 중요한 파라미터이다.

그림 6은 송신측에서 삽입한 워터마크 정보와 수신측에서 검출한 추정된 워터마크 정보와의 상관값을 나타낸다. 워터마크는 첫 번째 프레임에서부터 39번째 프레임에 삽입하였고 나머지 프레임엔 워터마크를 삽입하지 않았다. 그림에서 알 수 있는 바와 같이 워터마크를 삽입한 프레임의 상관값이 워터마크가 삽입되지 않은 프레임의 상관값에 비해 일반적으로 큰 값을 갖는 것을 알 수 있다. 그렇기 때문에 적절한 문턱값을 설정하면 식 (10)을 이용하여 피아를 식별할 수 있다. 상관값 λ는 다음과 같은 식을 이용하여 구하였다[2].

$$\lambda(wn[n], \widehat{wn}[n]) = \frac{\sum_{n=1}^{N} (wn[n] \bullet \widehat{wn}[n])}{\sqrt{\sum_{n=1}^{N} (\widehat{wn}[n] \bullet \widehat{wn}[n])}} \quad (11)$$



[그림 6] 상관도 측정 결과

두 벡터간의 상관계수 범위는 일반적으로 -1에서 +1로 알려져 있으나 식 (11)에서는 분모에 제곱근을 씌웠기 때문에 상관계수의 범위가 -2에서 +2가 된다. 그런데 삽입된 워터마크 $wm[n]$의 원소가 모두 양수이고 워터마크를 검출하는 과정에서의 양자화 방법으로 truncation 양자화를 하였다면 상관계수 범위는 0에서 2까지가 된다. 그림 6에서 상관도 범위가 0에서 2까지인 것은 양수의 워터마크를 삽입하고 truncation 양자화를 실시하였기 때문이다.

실제 워터마크 검출 결과는 해당 프레임의 에너지가 많고 적음에 따라 다르게 나타날 수 있다. 따라서 신뢰성 있는 피아식별을 위해서는 특정한 한 프레임의 워터마크 검출 결과가 아닌 여러 프레임에서의 워터마크 검출 결과를 피아식별의 판단 근거로 사용할 필요가 있다. 표 1은 다양한 잡음 환경에서 워터마크가 삽입된 프레임들에서의 평균 상관값(A)와 워터마크가 삽입되지 않은 프레임들에서의 평균상관값(B)을 나타낸다. 워터마크가 삽입된 프레임의 개수와 삽입되지 않은 프레임의 개수는 각각 39개이며 A/B는 워터마크가 삽입되지 않은 프레임에서의 평균상관값과 워터마크가 삽입된 프레임에서의 평균상관값의 상대적 크기비를 나타낸다.

A/B 값이 클수록 워터마크의 삽입여부를 쉽게 판단할 수 있는 것을 의미한다. 표에서 보는 바와 같

[표 1] 잡음환경별 평균상관값 측정 결과

구 분	A	B	A/B
clean	2	0.8833	2.2642
0dB	1.3185	1.1536	1.1429
5dB	1.5697	1.2753	1.2308
10dB	1.8534	1.2767	1.4517
20dB	1.9892	1.2800	1.5540
30dB	1.9999	1.2820	1.5599

A : 워터마크가 삽입된 프레임들의 평균상관값,
B : 워터마크가 삽입되지 않은 프레임들의 평균상관값

[표 2] 제안한 피아식별 방법을 이용했을 때의 오거부율/오인식률(단위 : %)

SNR \ 양자화 레벨	0.5β	β	1.5β	2β
5dB	93.45/0	32.52/0	3.34/0	0.61/0
10dB	42.10/0	1.52/0	0/0	0/0
15dB	3.34/0	0/0	0/0	0/0
20dB	0/0	0/0	0/0	0/0
25dB	0/0	0/0	0/0	0/0

이 SNR이 낮을수록 A/B의 값이 작아진다는 것을 알 수 있다. 때문에 잡음 환경에 따라 A값, B값을 참고하여 적절한 문턱값을 선택하면 여러 프레임에서의 워터마크를 고려한 신뢰성 있는 피아식별이 가능하다.

표 2는 다양한 잡음 환경에서 약 1초 길이의 660개 음성에 대해 제안한 방법을 적용했을 때 오인식률(FAR : False Acceptance Rate)과 오거부율(FRR : False Rejection Rate)를 계산한 결과이다. 문턱값은 추정한 워터마크 정보가 실제 워터마크 정보와 동일할 때의 상관값의 80%를 사용하였다.

표에서 확인한 바와 같이 오인식률은 모든 경우에 대해 완벽한 성능을 보이지만 오거부율은 잡음 환경에 따라 다소 높아질 수 있다. 하지만 잡음 환경에 따라 적절히 β값과 문턱값을 조정하면 오거부율을 충분히 낮출 수 있다.

6. 결 론

점점 전투공간이 시·공간적으로 확대되고 다차원화 되면서 안전한 통신에 대한 수요는 폭발적으로 늘어날 것이다. 또한 적이 아군에 대한 중요 통신 정보를 획득하고 이를 이용하여 적을 아군으로 오인케하는 각종 기만으로 지휘통신체계를 마비시키려는 적의 노력은 점점 고도화될 것이다. 이에 군통신에서 워터마킹 기법을 이용한 피아식별 방법을 제안하였다. 제안한 방법은 주파수 영역에서 양자화 오차를 이용하여 워터마킹을 삽입하고 전송 과정에서 잡음으로 오염된 워터마크 신호와 원래의 워터마킹 신호의 상관값을 계산하여 피아식별의 자료로 사용한다. 음질 보다는 신뢰성 있는 정보유통에 더 큰 가치를 부여하는 군통신의 특수성을 고려하여 높은 신뢰성 확보를 위해 여러 프레임에서의 워터마크 검출 결과를 피아식별의 판단 자료로 사용하였다. 또한 최소한의 잡음 강인성 보장을 위해 양자화 레벨을 고정하고 음질을 향상시키는 방법을 강구하였다.

제안한 방법의 성능 측정을 위해 여러 잡음 환경에서 실험을 실시하였다. 실험 결과 양자화 레벨에 따라 워터마크의 잡음 강인성과 음질 사이에 trade-off가 발생하였다. 즉, 양자화 레벨을 크게 하면 잡음 강인성은 좋아지지만 음질은 저하되고 반대로 양자화 레벨을 작게 하면 잡음에 대한 강인성은 저하되지만 음질은 보존된다. 이러한 trade-off를 극복하기 위해 전체 프레임에 대해 양자화를 하지 않고 워터마크가 삽입되는 DFT 계수만을 양자화하는 방법으로 음질과 잡음 강인성을 동시에 만족시켰다. 다양한 잡음환경에서 실험을 실시한 결과 제안한 방법이 오인식률에 대해 완벽한 성능을 보였고 양자화 레벨과 문턱값을 적절히 조정한다면 오거부율도 충분히 낮출 수 있다는 것을 증명하였다. 또한 짧은 음성신호(약 1초)에도 충분히 피아식별이 가능함을 보였다.

기존의 군통신 상에서의 피아식별 방법은 신속한 정보유통을 필요로 하는 전시 상황을 고려할 때 피아식별 판단에 소요되는 시간이 과다하고 사용자 입장에서 실제적인 정보유통을 위한 사전 작업이 필요하다는 불편함이 있었다. 하지만 제안한 방법은 음성통화 중에 피아식별을 짧은 시간에 자동적으로 수행하여 위 두 가지 문제를 모두 해결하였다.

제안한 방법의 성능을 향상시키기 위해서는 잡음환경을 정확히 판단하여 잡음환경에 따라 양자화 레벨을 세밀하게 조정할 수 있는 방법이 필요하다. 또한 양자화 레벨을 시간적으로 변화시킬 때 조정된 양자화 레벨에 대한 정보를 어떻게 송·수신자가 공유할 수 있을 지에 대한 연구도 더불어 진행되어야 할 것이다. 제안한 방법은 음성을 프레임 단위로 분할하여 각각에 대해 DFT를 실시하고 DFT 계수에 워터마크 정보를 삽입하였다. 차후 보다 계량된 성능의 피아식별 방법 연구를 위해 다양하게 주파수를 분할하여 표현할 수 있는 웨이블렛(wavelet) 계수나 계수들 간의 상관성이 적은 캡스트럼(Cepstrum) 계수에 제안한 방법을 적용하여 실험할 필요가 있다. 마지막으로 삽입되는 워터마크 정보 자체를 암호화하면 보다 강화된 보안성을 제공할 수 있을 것이다. 또한 제안한 방법을 이용하여 워터마크 정보를 다량 삽입하면 비밀통신의 방법으로 발전이 가능하다.

참 고 문 헌

[1] 황춘식 외 7인, “정보전자전”, 황금알, 2005.

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

[3] 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] A. R. Gurijala and J. R. Deller, Jr., "Speech Watermarking by Parametric Embedding with an l_∞ Fidelity Criterion", Eurospeech2003 in Geneva, 2003.

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

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

[7] X. Huang, Alex Acero and H. W. Hon, "Spoken Language Processing", Prentice Hall, 2001.