논문 2011-06-33

항공기에서 보안 강화된 음성 데이터 저장 방식

(A Security-Enhanced Storing Method for the Voice Data in the Aircraft)

조 승 훈, 서 정 배, 문 용 호*
(Seung Hoon Cho, Jeong Bae Suh, Yong Ho Moon)

Abstract: In this paper, we propose a security-enhanced storing method for the voice data obtained during the flight. When an emergency occurs during flight, the flight data in the storage device such as DTS or Blackbox can be exposed to antagonist or enemy. Currently, zeroize function is embedded in these devices in order to prevent this situation. However, this could not be operated if the system is malfunctioned or the pilot is wounded in the emergency. In order to solve this problem, the voice data compressed by the ADPCM is encrypted in the proposed method composed of the AES algorithm and a reordering method. The simulation results show that the security for the voice date is further enhanced due to the proposed method.

Keywords : Aircraft, Data transfer system, Blackbox, Speech data, ADPCM, Security, Encryption

1. 서 론

일반적으로 항공기에는 데이터 전송 체계 (DTS: Data Transfer System)와 블랙박스 [1-2] 등과 같은 비행데이터 저장장치가 탑재되어 있다. DTS는 비행 종료 후 비행 임무 분석과 계획 대비 수행 이력 확인을 위하여 내장된다. DTS에서는 사전 계획에 따라 수행되는 비행 과정에서 얻어지는 항공기의 결함, 표시점 (Markpoint), 항공기 자세, 음성 및 조종사의 조작 등과 같은 데이터가 수집, 저장된다. 한편, 블랙박스는 항공기 사고 시 원인 규명을 통한 재발 방지를 목적으로 탑재되는 장치로서 비행 중에 얻어지는 파일럿의 음성 및 오디오, 각종 운행 데이터 등이 기록, 저장된다. 현재 저장장치에서 비행 데이터는 실시간으로 압축되어 저장되고 있다.

저장 장치에 기록된 각종 비행데이터는 기술적, 군사적으로 중요한 정보를 지니고 있다. 따라서 비상사태로 인하여 항공기가 불시착하여 비행데이터가 노출될 경우 매우 심각한 문제들이 발생될 수 있다. 일반적으로 비행데이터는 관련 기술의 특징과 문제점을 파악하는 데 있어 중요한 단서를 제공한다. 따라서 경쟁사에서 비행 데이터를 확보한다면 핵심기술의 유출 및 이에 따른 경제적 피해가 발생될 것이다. 또한, 비행데이터가 적군에게 유출될 경우 전투력뿐만 아니라 작전 기밀의 노출에 따른 유, 무형의 막대한 피해가 예상된다. 이 같은 사태를 예방하기 위하여 현재 항공기내의 저장장치에는 Zeroize라는 물리적 삭제 기능이 구현되어 있다. 그러나 이 기능은 포맷 동작의 완료까지 수 십초의 시간이 소요되고, 피탄과 같은 파손 또는 기계적 결함으로 인해 오 작동할 가능성이 존재한다. 더구나 파일럿의 기절, 사망 등과 같은 신변이상으로 인해 작동이 불가능한 경우도 발생할 수 있다. 현재 차량용 블랙박스에서는 데이터 저장 시 DES[3]와 워터마킹[4] 기법을 적용함으로서 데이터의 안전한 보존을 도모하고 있다. 따라서 비행데이터의 저장에 있어서도 보다 강화된 보안 기술의 도입은 매우 중요하며 시급한 일이다.

비행데이터의 효과적인 저장을 위해서는 기본적

* 교신저자(Corresponding Author)
논문접수 : 2011. 03. 05., 수정일 : 2011. 04. 01.,
채택확정 : 2011. 04. 14.
조승훈: 경상대학교 정보과학과
서정배: (주)에어로매스터
문용호: 경상대학교 정보과학과/공학연구원
※ 본 연구는 중소기업청에서 주관하는 구매조건부 신제품개발사업(과제번호:S1065385)의 연구비 지원에 의하여 수행되었음.

으로 고 효율의 압축과 실시간 처리가 보장되어야 한다. 항공기는 경성 실시간 시스템 (Hard Real-Time System)의 대표적인 예로써 탑승자의 안전 보장을 위하여 실시간성의 보장이 강력하게 요구되고 있다. 그리고 장시간의 비행으로 인하여 수집되는 비행데이터는 그 양이 방대하기 때문에 대용량의 메모리가 요구된다. 이것은 궁극적으로 비용의 증가를 야기한다. 이러한 문제를 해결하기 위해서는 고 효율의 압축 기술을 이용하여 비행데이터를 압축하는 것이 필수적이다. 이상의 사실들은 강화된 보안 방식의 개발에 있어서 중요한 지침을 제시한다. 즉, 개발될 보안 방식은 압축 효율을 저하시키지 않으면서 실시간 처리에 문제를 야기하지 않아야 한다는 것이다.

본 논문에서는 비행중 획득되는 음성데이터에 대하여 암호화 방식과 재정렬 방식을 결합한 새로운 보안 방식을 제안한다. 현재 항공기에서 음성 데이터는 ADPCM(Adaptive Delta Pulse Coded Modulation) 기반의 ITU-T G.726 부호화 표준[5]에 의하여 압축되어 저장되고 있다. 제안 방식에서는 압축된 음성 데이터에 AES (Advanced Encryption Standard) 암호화 기법[6]을 적용한다. AES 암호화 방식은 입, 출력 데이터의 크기가 동일하기 때문에 압축 효율의 저하를 발생시키지 않는다. 그리고 암호화된 음성데이터에 재정렬 방식을 적용한다. 재정렬 방식은 ADPCM의 오류 전파 특성에 기반한 것으로 작은 계산량으로 보안성을 보다 더 향상시킨다. 모의실험을 통하여 제안 방식에 의한 음성 데이터의 저장은 보다 더 보안성을 강화시킴을 확인할 수 있다.

Ⅱ. 기존 항공기에서의 음성 데이터 저장

현재 항공기에서 음성데이터는 그림 1과 같은 과정을 통하여 저장된다 [7].

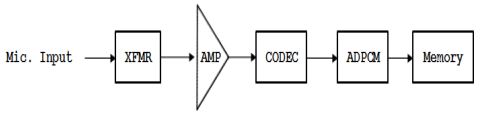


그림 1. 블랙박스에서의 음성 데이터 저장 과정
Fig. 1. The storing steps for the voice data in the Blackbox

그림 1에서 XFMR(Auto-Transformer)부를 거쳐 AMP부에서 증폭된 음성 신호는 CODEC부에 의하여 디지털 신호로 변환된다. 그리고 디지털화된 음성 데이터는 ADPCM부에서 ITU-T G.726 부호화 표준에 의하여 압축된 후 메모리에 저장된다. 음성데이터에 대한 이와 같은 처리 과정은 기존의 멀티미디어분야에서도 거의 동일하게 적용되고 있는 보편적 방식이다 [8-9].

일반적으로 음성데이터는 인간의 발성기관에서 생성되기 때문에 샘플간 연속성이 강한 특징을 지니고 있다. 이와 같은 이유로 음성데이터는 구현이 용이하며 저전력의 고속 처리가 가능한 ADPCM 방식에 기초하여 압축되어진다.

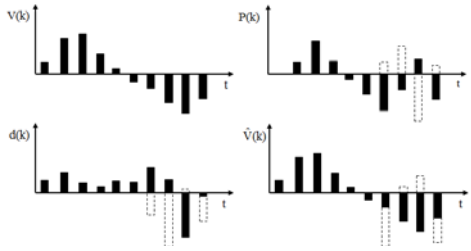


그림 2. 음성데이터에 대한 ADPCM 과정
Fig. 2. The procedure of the ADPCM for the voice data

그림 2는 음성데이터에 대한 ADPCM 과정을 보여준다. 그림에서 알 수 있듯이 ADPCM 방식은 이전에 처리된 음성데이터들을 이용하여 현재값을 예측하고, 이때 발생한 차이값을 주어진 비트들로 양자화한다. 식(1)은 이러한 과정을 나타낸다.

$$d(k) = V(k) - P(k), \quad where\ P(k) = f(\hat{V}(k-1),,, \hat{V}(k-n)) \tag{1}$$

식(1)에서 $V(k)$와 $P(k)$는 현재 음성데이터와 이전에 처리된 음성데이터들로부터 얻어지는 예측값을 각각 나타낸다. 그리고 $f(\bullet)$는 예측 함수를 의미한다. 식(1)의 $d(k)$는 작은 비트들을 이용한 양자화 과정을 통하여 부호화된 후 메모리에 저장된다.
한편, 식(2)는 압축된 데이터의 복원을 나타낸다.

$$\hat{V}(k) = P(k) + \hat{d}(k), \quad where\ \hat{d}(k) = Q(d(k)) \tag{2}$$

여기서 $Q(\bullet)$는 양자화 과정을 의미한다. 식(1)과 식(2)로부터 복원된 음성데이터는 양자화 오차로

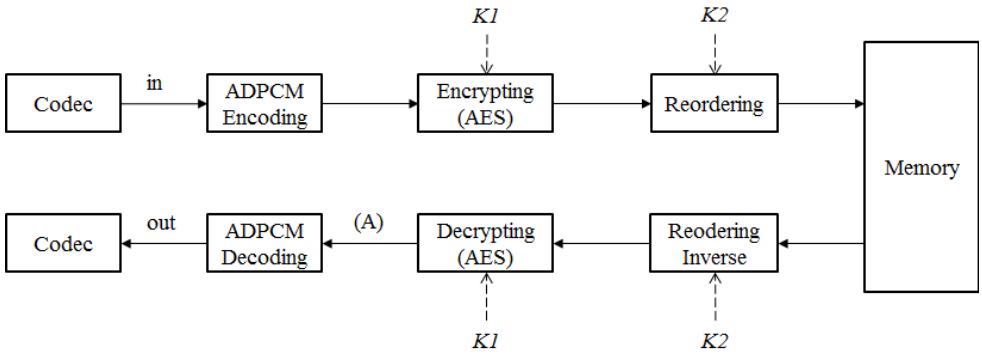


그림 3. 제안하는 보안 방식에 기반한 음성데이터 저장 과정
Fig. 3. The procedure of the storing for the voice data based on the proposed method

인하여 원래의 음성데이터와 완벽하게 동일하지 않음을 알 수 있다. 그러나 양자화 오차는 예측 오차에서 발생하는 것이므로 음성 신호를 인지하는 데 큰 지장을 초래하지는 않는다.

그런데 이 방식은 복원시 예측값에 오류가 발생할 경우 데이터가 올바르게 복원되어지지 않는다. 더구나 이러한 오류는 이후 데이터의 복원에서도 오류가 계속 발생되는 오류 전파 문제를 지닌다. 그림 2에서 점선으로 표시된 부분은 이를 잘 보여주고 있다.

Ⅲ. 제안하는 보안 방식

그림 3은 제안하는 시스템의 전체 구성도이다. Codec을 거쳐 디지털화된 음성 데이터는 ADPCM Encoding을 거쳐 압축이 된다. 그리고 압축된 비트열이 AES 방식으로 암호화된 후 재정렬 방식을 거쳐 또 다시 암호화된 후 메모리에 저장되게 된다. 저장된 음성데이터의 복원은 저장 과정을 역순으로 적용시키며 이때 저장에서 사용된 키값들이 이용되어야 한다.

1. AES 암호화를 이용한 보안

AES는 FIPS-197 암호화 표준으로서, SPN (Substitution-Permutation Network)구조의 가변 블록 길이를 지원하는 블록 암호화 방식이다. SPN은 입력 블록을 여러 개의 부분블록들로 나누고 각 부분블록을 S-box로 입력하여 대치시키고 S-box의 출력을 P-box로 전치하는 과정을 반복한다. 암호화에 사용되는 키(key)는 128, 192, 256bit의 길이를 가질 수 있고 키 길이에 대하여 각각 10, 12, 14라운드의 연산을 수행한다. 그림 4는 AES 방식[10]에 의한 암호화와 복호화 과정을 나타낸다. 그림에서 알 수 있듯이 마지막 라운드를 제외한 나머지 라운드는 비교적 간단한 연산인 순열연산과 치환연산으로 이루어진다.

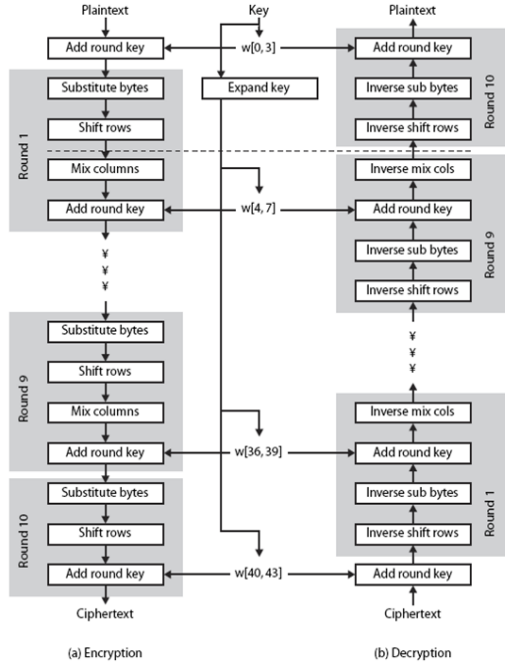


그림 4. AES 방식에서의 암호화 및 복호화 블럭도
Fig. 4. The block diagram of the encryption and decryption based on the AES

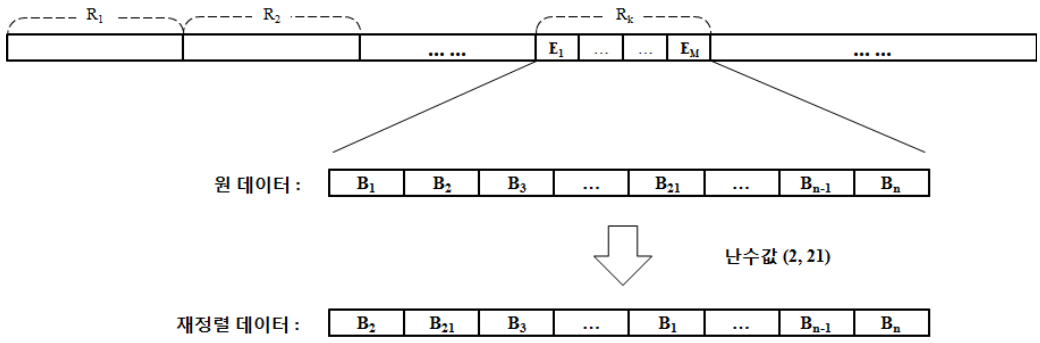


그림 5. 재정렬 방식의 동작 과정
Fig. 5. The mechanism of the reordering method

AES 암호화에서 입력 블록은 키의 길이와 동일한 크기를 가진다. 그리고 암호화된 블록의 크기는 입력 블록의 크기와 동일하다. 따라서 압축된 비트열을 AES 방식으로 암호화할 경우 압축효율의 감소가 발생하지 않는다. 그리고 AES 방식은 다른 암호화 방식에 비하여 고속 동작이 가능하고 프로그램 코드가 간단하다고 알려져 있다. 또한 현재 실제

표준으로 사용되고 있는 방식으로 알려진 모든 공격에 강하며 SPN 구조로 인해 많은 병렬성을 제공한다. 그러므로 최근 요구되고 있는 멀티코어를 통한 고속연산을 더 원활히 수행할 수 있는 장점을 지니고 있다.

이와 같은 특징들로부터 AES 암호화 방식은 압축 효율을 유지하면서 실시간 처리가 가능한 효과적인 보안 방식이라는 것을 알 수 있다. 이에 제안하는 보안 방식에서는 압축된 음성 데이터에 AES 암호화를 수행한다. 저장된 데이터가 불가피하게 유출되더라도 AES 암호화로 인하여 원래의 데이터를 얻기 위해서는 매우 긴 시간이 필요할 것이다. 따라서 이것은 사고 발생 후 대응 방안을 마련할 수 있는 충분한 시간을 확보할 수 있게 한다.

2. 재정렬 방식을 이용한 보안

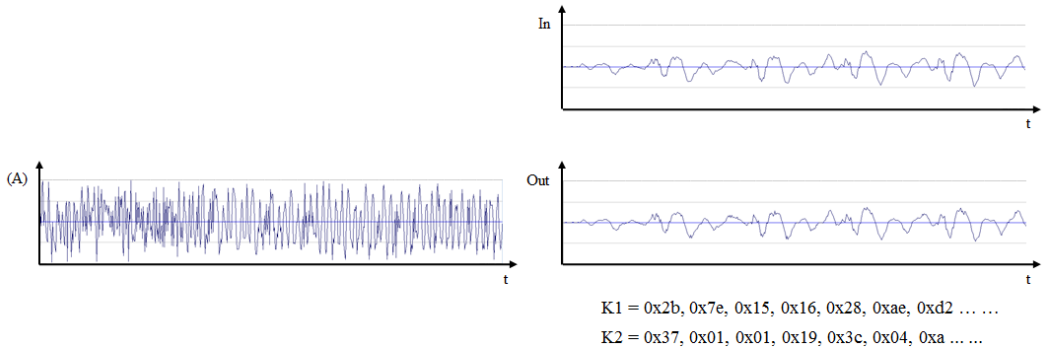
보안 성능을 보다 더 강화하기 위하여 본 논문에서는 ADPCM의 오류 전파 특성에 기반한 재정렬(Reodering) 방식을 제안한다. 앞 장에서 설명한 바와 같이 ADPCM 방식으로 압축된 데이터의 복원에 있어서 특정 순간에 발생하는 예측값의 오류는 오랜 시간동안 데이터의 복원이 제대로 이루어지지 못하게 한다. 따라서 특정 순간의 예측값을 의도적으로 훼손할 경우 훼손방식을 알지 못한다면 올바른 데이터가 얻어 질 수 없을 것이다. 이러한 특성에 기반하여 본 논문에서는 효율적인 보안 방식을 제안한다.

그림 5는 제안하는 재정렬 방식의 구성 및 동작 과정을 나타낸다. R은 재정렬을 수행하는 단위 블록으로 M개의 E블록으로 구성된다. E블록은 암호화를 수행하는 기본 단위로서 128, 192, 256bit가 될 수 있다. 또한 M개의 E블록을 구성하는 B는 1byte의 크기를 가지고, 재정렬 방식을 수행하는 기본 대상이 된다.

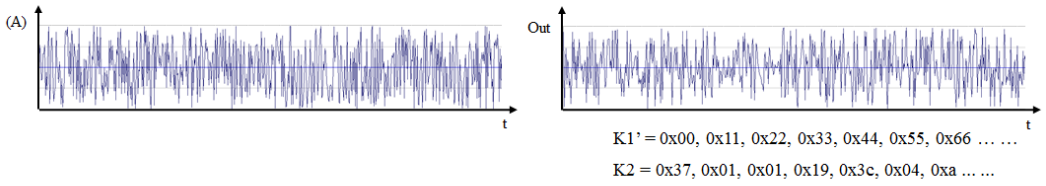
재정렬 방식의 동작 과정은 각 R블록의 첫 번째와 두 번째 B블록을 재정렬 키가 지시하는 위치에 존재하는 B블록들과 교체하는 것으로 이루어진다. 따라서 4개의 B블록들이 인위적으로 훼손되어 재정렬 키를 모를 경우 원래의 음성 데이터를 얻을 수 없게 된다. 그림 5는 킷값이 2와 21인 경우의 재정렬 되어진 데이터를 보여준다. 또한 역재정렬을 수행할 때 재정렬 키와 일치하지 않는 키가 입력될 경우 원래의 정렬된 데이터가 얻어지지 않아서 올바른 음성신호가 재생되지 못 한다. 이와 같은 이유로 제안된 시스템에서는 암호화 방식 외에 재정렬 방식을 통해 보안이 더욱 더 강화된다.

IV. 모의실험

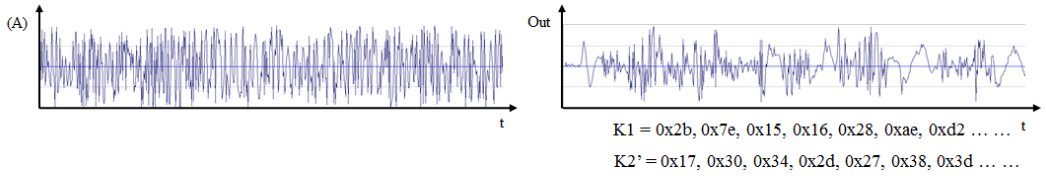
본 논문에서는 제안 방식을 검증하기 위하여 16kHz의 표본화 주파수에 의하여 얻어진 샘플을 16bit로 양자화함으로써 생성된 30초 분량의 음성 데이터를 이용하여 모의실험을 수행하였다. 이때 ADPCM Encoding은 32kbps로, AES 암호화 블록



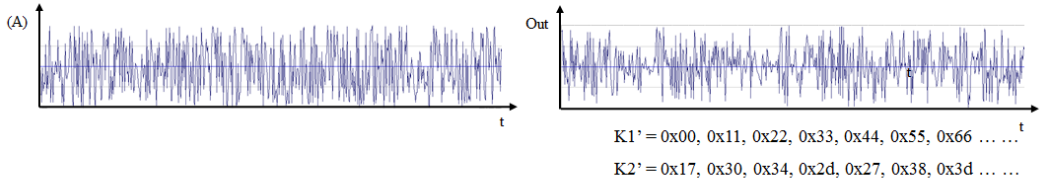
(a) 정상적인 동작 시 음성 파형



(b) AES 복호화 오류 시 음성 파형



(c) 역재정렬 오류 시 음성 파형



(d) 복호화 및 역재정렬 오류 시 음성 파형

그림 6. 모의실험 결과

Fig. 6. The simulation results

의 크기는 128bit로 설정하여 실험을 수행하였다.

제안방식의 효과를 확인하기 위하여 복원시 K1과 K2를 각각 임의로 입력한 경우와 두 가지 모두 임의로 입력한 경우에 대하여 복원된 최종 출력 파형들을 비교하였다. 먼저, 최종 출력 파형들이 인지될 수 있는지 청취한 결과 모든 유형의 실험에서 원래의 음성을 인식하는 것이 불가능한 것을 확인할 수 있었다.

제안 방식의 효과를 보다 객관적으로 파악하기 위하여 각각의 경우에 대한 복원 파형을 비교해 보았다. 그림 6은 실험 유형에 따른 음성 신호 중 0.6초부터 0.95초까지를 두 배로 확대하여 나타낸 것이다. (a)는 보안기능이 존재하지 않는 기존 저장 방식에서의 음성신호 파형이다. (b)는 제안 방식을 적용한 시스템에서 암호화 키와 복호화 키가 다른 경우에 얻어지는 파형을 나타낸 것이다. 이 경우 재정렬 키 K2가 올바르게 입력되더라도 K1이 일치하지 않으면 인식이 불가능한 파형이 생성되는 것을

알 수 있다. (c)는 복호화 키가 올바르게 입력되었고 재정렬 키가 일치하지 않는 경우를 나타낸다. (b)의 경우에 비해 비교적 잡음이 덜 생기지만 원래의 파형과 비교하여 전혀 다른 것을 알 수 있다. 이것은 64byte마다 2 byte씩만을 재정렬을 해주어도 ADPCM의 오류 전파 특성으로 인해 데이터가 제대로 복원이 되지 않는 특성에 의하여 발생하는 현상이다. (d)의 경우는 복호화 키와 재정렬 키가 모두 일치하지 않는 경우의 파형을 나타낸 것이다. 앞에서의 경우와 마찬가지로 원래의 파형과는 전혀 다른 파형이 얻어진다. 또한 (b)와 (c)로부터 2개의 키가 동시에 노출되지 않는 한 원래의 음성 데이터가 재생되지 않는 것을 확인할 수 있다.

V. 결 론

DTS나 블랙박스와 같은 비행데이터 저장장치는 비상사태 발생시 데이터 유출을 방지하기 위한 보안장치로서 Zeroize 기능을 보유하고 있다. 그러나 이 장치는 실제 환경에서 오작동하거나 미작동할 가능성이 매우 높다. 이러한 문제점을 해결하기 위하여 본 논문에서는 암호화 방식과 재정렬 방식을 결합한 효과적인 보안 방식을 제안하였다. 청취 실험을 통하여 킷값을 모를 경우 출력 파형의 인지가 불가능함을 확인하였고 파형 비교를 통해 그 효과를 객관적으로 검증하였다. 또한, 제안 방식은 음성 데이터 뿐만 아니라 다른 비행데이터의 저장에도 적용이 가능한 특징을 지닌다.

참고문헌

[1] 박훈, 남주훈, 전향식, 주정민, "소형항공기용 결합된 비행기록장치와 음성기록장치 설계", 한국항공우주학회 춘계학술발표회 논문집, pp. 359-363, 2005.

[2] 주정민, 안이기, 박훈, 남주훈, "소형항공기용 비행 및 음성기록장치 최적설계", 대한기계공학회 창립 60주년 기념 추계학술대회 강연 및 논문초록집, pp. 2557-2561, 2005.

[3] 박노춘, "차량용 블랙박스 시스템 및 차량용 블랙박스 해독방법과 그 프로그램 소스를 저장한 기록 매체", 특2002-0068186, 2002.

[4] 유종태, 허용석, "이중 저장구조를 가지는 차량용 블랙박스", 특2009-0104300, 2009.

[5] "40, 32, 24, 16 kbit/s adaptive differential pulse code modulation", International Telecommunication Union, Available at http://www.itu.int/en/ITU-T/publications/Pages/recs.aspx.

[6] "Advanced encryption standard", .National Institute of Standards and Technology (U.S.), Available at http://www.nist.gov/index.html.

[7] Honeywell Product Description, "Solid-state cockpit voice recorder", Available at http://www51.honeywell.com.

[8] Nobuo Terui Hidetaka Takahashi, "Digital voice recoding/reproducing apparatus", U. S. Patent 5710813, Jan. 1998.

[9] 정태식, "멀티미디어 데이터의 암호화 장치, 멀티미디어 데이터의 암호화 방법 및 멀티미디어 데이터의 암호화 기능을 구비한 휴대용 단말기", 특 2009-0043044, 2009.

[10] William Stalling, Cryptography and Network Security - Principles and Practice, 3rd Ed., Prentice Hall, 2002.

저 자 소 개

조 승 훈 (Seong Hoon Cho)

2011년 : 경상대학교 정보과학과 학사.
현재, 경상대학교 정보과학과 석사과정.
관심분야 : 임베디드 시스템 소프트웨어, 신호처리, SoC.

Email : espresso@gnu.ac.kr

서 정 배 (Jeong Bae Suh)

1985년 : 한국항공대학교 항공 기계공학과 학사).
현재, (주)에어로매스터 대표이사.
관심분야 : 임베디드 소프트웨어, Avionics.

Email : aeromaster@amc21.co.kr

문 용 호 (Yong Ho Moon)

1992년 : 부산대학교
전자공학과 학사.
1994년 : 부산대학교
전자공학과 석사.
1998년 : 부산대학교
전자공학과 박사.

1998~2001년 : 삼성전자 DM연구소 책임연구원.
현재, 경상대학교 정보과학과 부교수.
관심분야 : 영상처리, 동영상압축, 임베디드 시스템, SoC.
Email : yhmoon5@gnu.ac.kr