논문 2012-07-20

압축 및 보안 기능이 있는 비행데이터 저장 시스템 구현

(Implementation of Flight Data Storage System with Compression and Security)

조 승 훈, 하 석 운*, 문 용 호
(Seung-Hoon Cho, Seok-Wun Ha, Yong-Ho Moon)

Abstract : In this paper, we propose a flight data storing system for effective data processing. Since the flight data contains critical information and their sizes are vast, encryption and compression would be needed to manage the flight data in effect. And we implemented the flight data storing system using an embedded board with DSP based on DPCM compression and AES encryption. Especially, we applied the reordering technique to advance the security function. From the simulations for two type data of voice and avionics, we found the developed system is well performed.

Keywords : Real-time system, Security, Compression, Aircraft, Flight data

Ⅰ. 서 론

일반적으로 항공기에는 비행데이터의 저장을 위해 데이터 전송 체계(DTS:Data Transfer System)와 블랙박스 [1-2] 등과 같은 장치가 탑재되어 있다. 이 장치들은 비행 임무 분석과 계획된 임무 대비 수행 이력을 확인하거나 항공기 사고 시 원인 규명을 통한 재발 방지 등을 위하여 파일럿의 음성, 항공기의 결함코드, 항공기 자세, 각종 운행 데이터 등을 수집하고 저장한다.

비행데이터 저장 장치에 기록된 각종 데이터는 기술적, 군사적으로 중요한 정보를 지니고 있다. 따라서 비상사태로 인해 데이터가 적군이나 경쟁사에 노출될 경우 매우 심각한 문제들이 발생될 수 있다. 이 같은 사태를 예방하기 위하여 현재 항공기내의 저장장치에는 Zeroize라는 데이터를 물리적으로 삭제할 수 있는 기능이 구현되어 있다. 그러나 이 기능은 포맷 동작의 완료까지 수 십초의 시간이 소요되고, 피탄과 같은 파손 또는 기계적 결함으로 인해 오작동할 가능성이 존재한다. 따라서 항공기의 비행데이터를 저장함에 있어서 보안성을 향상시킬 수 있는 방식을 도입하는 것은 매우 중요하고 시급한 일이다.

본 논문에서는 비행 중 획득되는 비행데이터에 대하여 압축 및 암호화를 수행하는 저장 시스템을 제시한다. 현재 항공기내에서 비행데이터 및 음성데이터는 다양한 통신 프로토콜에 의하여 전송되어진다. 그런데 이들 프로토콜에는 압축 및 보안 기능들이 탑재되어 있지 않다. 따라서 본 논문에서는 수신된 비행데이터에 DPCM(Differential Pulse Code Modulation) [3-4] 기반의 압축을 수행 후, 재정렬 방식 (Reordering)과 AES (Advanced Encryption Standard) 암호화 기법 [5]을 결합한 방식을 적용하여 비행데이터를 실시간으로 저장하는 시스템을 구현한다. 모의실험을 통하여 구현된 시스템에서 비행데이터가 효과적으로 압축, 암호화되는 것을 확인할 수 있다.

Ⅱ. 비행데이터 저장 방법

비행데이터의 효율적인 저장을 위해서는 방대한 비행데이터에 대하여 효율적으로 저장할 수 있어야 하고 비행 정보 유출을 대비하여 비행데이터의 보안 기능을 강화 할 필요가 있다. 또한 획득되는 비

* 교신저자(Corresponding Author)
논문접수 : 2012. 01. 31., 수정일: 2012. 02. 22.,
채택확정 : 2012. 04. 06.
조승훈, 하석운, 문용호 : 경상대학교 정보과학과
※ 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2012-H0301-12-3003)

행데이터를 실시간으로 저장하기 위해 고속으로 처리가 되어야 한다.

1. DPCM 기반의 비행데이터 저장

장시간의 비행으로 인하여 수집되는 비행데이터는 그 양이 방대하기 때문에 대용량의 메모리가 요구된다. 따라서 이러한 문제를 해결하기 위해서는 고효율의 압축 기술을 이용하여 데이터를 압축하는 것이 필요하다.

일반적으로 비행데이터는 샘플 간 연속성이 강한 특징을 지니고 있다. 이와 같은 이유로 비행데이터는 연산량의 추가가 매우 작고, 저전력의 고속처리가 가능한 DPCM 방식에 기초하여 압축 할 수 있다 [6]. 그림 1은 DPCM 과정을 나타낸다. 그림 1 에서 알 수 있듯이 DPCM은 최초 값은 전체 값을 전송하고, 그 이후에는 차이 값만을 취하여 전송한다. 식(1)은 이를 나타낸 것이다.

$$d(k) = D(k) - D(k-1) \qquad (1)$$

식(1)에서 $D(k)$와 $D(k-1)$는 현재 데이터와 이전에 처리된 데이터를 각각 나타낸다. 식(1)에서 $d(k)$는 차이 값으로 특성상 아주 작은 값을 가지게 된다. 따라서 $D(k)$ 대신 $d(k)$를 전송하는 것이 보다 더 효율적일 것이다. 또한 기존에 파일럿의 음성데이터에 있어서 DPCM 기반의 G.726을 적용하여 저장한 연구 결과가 발표되었었다 [7].

그러나 DPCM에 기반한 압축 방식은 복원 시, $d(k)$에 오류가 발생 할 경우 데이터가 올바르게 복원되지 않는다. 더구나 이러한 오류는 이후 데이터의 복원에서도 오류가 계속 발생되는 오류 전파 문제를 지닌다. 그림 1의 빗금으로 표시된 부분은 이를 잘 보여주고 있다.

2. AES를 이용한 비행정보 유출 방지

AES는 FIPS-197 암호화 표준으로서, SPN (Substitution Permutation Network)구조의 가변 블록 길이를 지원하는 블록 암호화 방식이다. 암호화에 사용되는 key는 128, 192, 256bit의 길이를 가질 수 있고 키 길이에 대하여 각각 10, 12, 14라운드의 연산을 수행한다. 그림 2는 AES 방식 [8]에 의한 암호화 과정을 나타낸다. 그림 2 에서 알 수 있듯이 마지막 라운드를 제외한 나머지 라운드는 비교적 간단한 연산인 순열연산과 치환연산으로 이루어진다.

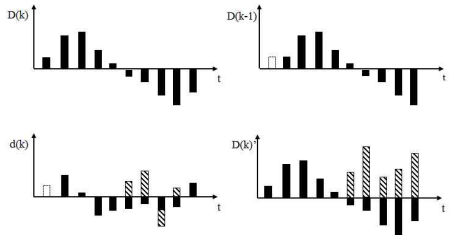

그림 1. 비행데이터에 대한 DPCM 동작 과정
Fig. 1. The procedure of the DPCM for the flight data

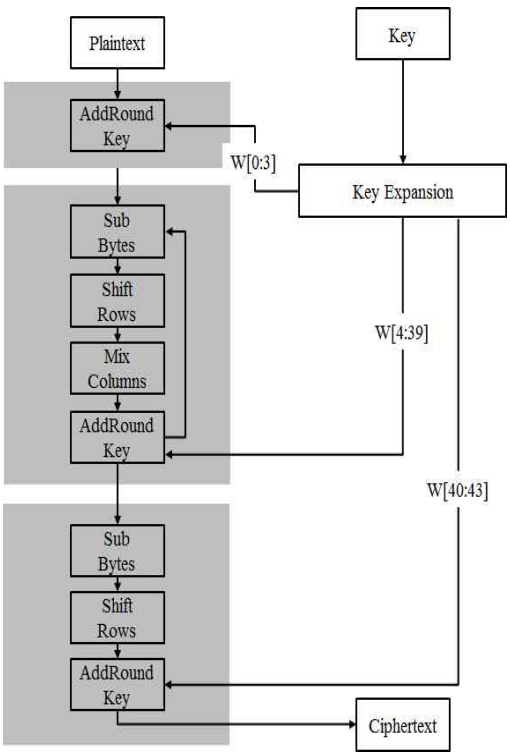

그림 2. AES 방식에 의한 암호화 과정
Fig. 2. The Procedure of encryption by AES

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

이와 같은 특징들로부터 AES 암호화 방식은 압

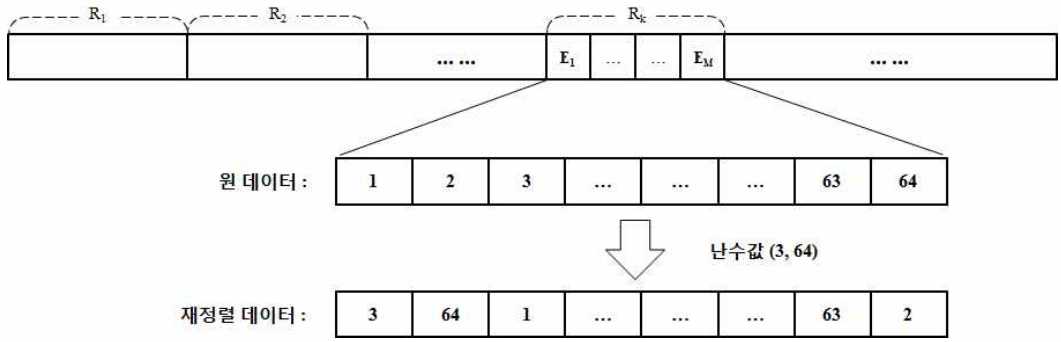

그림. 3 재정렬 방식의 동작 과정
Fig. 3. The mechanism of the reordering

축 효율을 유지하면서 실시간 처리가 가능한 효과적인 보안 방식이라는 것을 알 수 있다. 이에 제안 방식에서는 DPCM에 기반하여 압축이 수행된 비행 데이터에 AES 암호화를 적용한다. 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.

3. 재정렬 방식을 이용한 비행정보 유출 방지

본 논문에서는 보안 성능을 보다 더 강화하기 위하여 DPCM 기반 압축 방식의 오류 전파 특성에 기반한 재정렬 방식을 적용한다 [7]. 앞 장에서 언급한 바와 같이 DPCM 기반으로 압축된 데이터의 복원에 있어서 특정 순간에 발생하는 오류는 오류 전파 특성으로 인해 오랜 시간동안 데이터의 복원이 제대로 이루어지지 못 하게 한다. 따라서 특정 순간에 의도적으로 압축된 데이터를 훼손할 경우, 훼손 방식을 알지 못 한다면 올바른 데이터가 얻어질 수 없을 것이다.

그림 3은 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 데이터를 얻을 수 없게 된다. 그림 3은 킷값이 3와 64인 경우의 재정렬 되어진 데이터를 보여준다. 또한 역재정렬을 수행할 때 재정렬 키와 일치하지 않는 키가 입력될 경우 원래의 정렬된 데이터가 얻어지지 못 하게 된다. 이와 같은 이유로 본 시스템에서는 암호화 방식 외에 재정렬 방식을 통해 보안이 더욱 더 강화된다.

Ⅲ. 실시간 시스템 구현

기존의 비행데이터 저장 방식에 대한 연구는 음성데이터 [6]나 비행데이터 [7] 중 하나만을 처리하는 시스템이었다. 그러나 실제 비행데이터 저장장치는 각종 데이터들을 동시에 저장하는 시스템이다. 따라서 이들 데이터들을 통합하여 저장할 필요성이 있다.

일반적으로 비행데이터 저장장치는 연속해서 데이터가 입력되기 때문에 실시간성이 엄격하게 요구되므로 이를 만족하기 위해서는 하드웨어 플랫폼이 구축되어야 한다. 이에 본 논문에서는 실시간 비행데이터 저장 시스템을 개발하기 위하여 디지털 신호 처리에 최적화 된 DSP(Digital Signal Processor) 보드 상에서 DPCM에 기반한 압축 방식과 AES와 재정렬 방식을 결합한 보안강화 방식을 구현한다.

DSP는 디지털 신호처리를 위해 특별히 개발된 마이크로프로세서로서 디지털 신호를 실시간으로 처리하는데 최적화된 구조를 가지고 있다. 또한 입출력 신호 간의 D/A, A/D 변환을 손쉽게 수행 할 수 있다. 그림 4는 TI (Texas Instrument)사의 C6713 DSK이다. 또한 그림 5는 제시하는 시스템의 구성도이다. 그림에서 알 수 있듯이 음성데이터

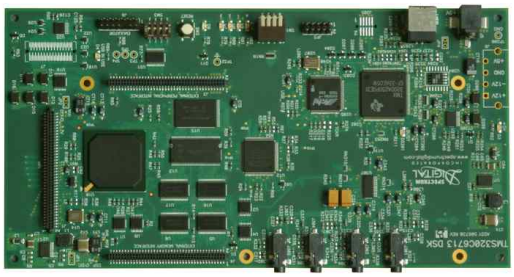

그림 4. TI C6713 DSK
Fig. 4. Texas Instrument C6713 DSK Board

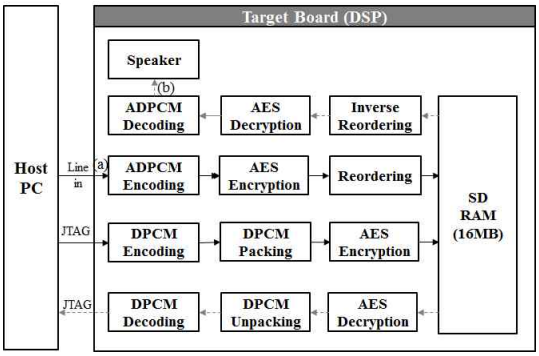

그림 5. 제시하는 시스템의 Block Diagram
Fig. 5. The block diagram of the proposed system

및 비행데이터는 각각 Line-in과 JTAG interface를 통해 DSP 보드에 입력되어 전송 된 후, 압축 및 암호화 과정을 거쳐 SD-RAM에 저장된다. 이후 복원에서는 음성데이터의 경우 Speaker를 통해 복원된 음성을 청취할 수 있고 툴을 통해 그 파형을 확인할 수 있다. 비행데이터의 경우에는 JTAG를 이용하여 복원된 파형을 host에서 확인할 수 있다.

IV. 모의실험 및 결과

본 논문에서는 제시하는 시스템의 성능을 검증하기 위하여 모의실험을 수행하였다. 실험을 위한 하드웨어 설정은 표 1과 같이 설정하였다. 또한 AES 연산의 암호화 블록의 크기는 128bit로 수행하였고 DPCM에 의하여 생성되는 차이 값은 4bit로 부호화하였다. 제안 방식의 압축 효율은 표 2와 같다. 표에서알 수 있듯이 비행데이터와 음성데이터를 DPCM에 기반하여 압축한 결과 75% 이상의 압축 이득을 얻을 수 있었다.

표 1. 실험 환경
Table 1. The simulation environments

	Host PC	Target Board
OS	Win XP 32bit	NONE
Processor	Pentium4 (3Ghz)	C6713 (300Mhz)
Memory	1GB RAM	256Kb RAM

표 2. 제시된 방식의 압축 이득
Table 2. The compression gain by the proposed method

	기존 방식	제시된 방식	이득
비행데이터	7,520 bytes	1,504 bytes	80%
음성데이터	940,128 bytes	235,032 bytes	75%

표 3. 제시된 방식 적용에 의한 데이터 손실율
Table 3. The loss factor by applying the proposed method

	적용 전	적용 후
비행데이터	3,008개	3,008개
음성데이터	470,064 개	470,064 개

그림 6은 그림 5의 (A)와 (B)에 해당하는 파형과 재정렬 키가 일치하지 않는 경우의 (B') 파형을 나타낸 것이다. 그림에서처럼 일치하지 않는 재정렬 키를 입력한 경우 원래의 데이터를 얻을 수 없다. 또한 그림 7은 (A), (B)와 일치하지 않는 AES 킷값을 입력한 경우의 파형 (B'')를 나타낸 것이다. 그림 6과 마찬가지로 원래의 데이터를 복원할 수 없다. 이것은 비상사태 발생 시에 저장 된 데이터가 유출되더라도 실제 비행 정보는 안전하게 보전된다는 것을 의미한다.

일반적으로 실시간 임베디드 시스템에서 샘플링 주기보다 데이터 처리 속도가 늦을 경우 센싱 된 데이터에 대해 손실이 발생하게 된다. 따라서 본 시스템이 실시간성을 만족한다면 입력되는 샘플의 개수와 최종 복원 시 샘플의 개수가 동일해야 할 것이다. 표 3은 제시된 방식의 적용 전과 후의 샘플의 개수를 나타낸다. 표를 통해 제안 방식이 실시간성을 만족함을 확인할 수 있다.

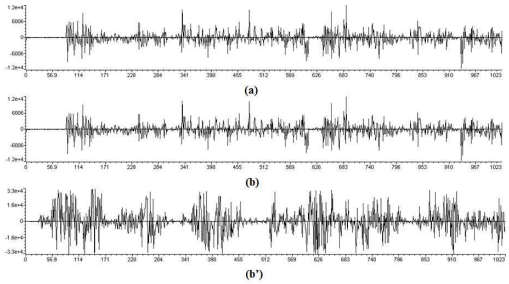

그림 6. 재정렬 키가 일치하지 않는 경우의 출력파형과 정상적인 출력파형의 비교
Fig. 6. Comparison between the output waveform generated from the unconformable reordering key and the proper output waveform

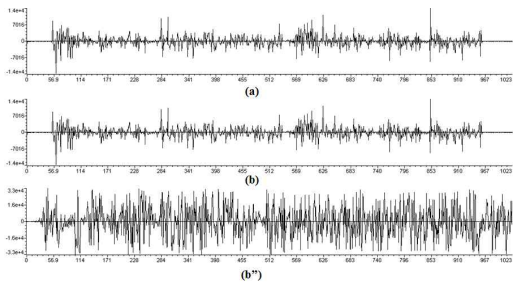

그림 7. AES 키가 일치하지 않는 경우의 출력파형과 정상적인 출력 파형의 비교
Fig. 7. Comparison between the output waveform generated from the unconformable AES key and the proper output waveform

V. 결론

DTS나 블랙박스와 같은 장치는 방대한 양의 비행데이터를 저장한다. 또한 비상사태 발생 시 데이터 유출을 방지하기 위한 보안장치로서 Zeroize 기능을 보유하고 있다. 그러나 이 장치는 실제 환경에서 정상적으로 동작하지 못 할 가능성이 높다. 이러한 문제점을 해결하기 위하여 DPCM에 기초한 압축방식의 적용 및 재정렬 방식과 AES 암호화를 결합한 보안 방식을 통하여 효율적인 데이터 저장을 실시간으로 처리하는 방식을 구현하였다. 모의실험을 통해 이 방식은 압축효율이 높고 보안성이 뛰어난 것을 확인할 수 있었다. 또한 제시된 방식이 실시간성을 만족함을 확인할 수 있었다.

참고문헌

[1] 박훈, 남주훈, 전향식, 주정민, “소형항공기용 결합된 비행기록 장치와 음성기록장치 설계,” 한국항공우주학회 춘계학술발표회 논문집, pp.358-363, 2005.

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

[3] 이문호, C언어 영상 통신의 신호 처리, 대영사, 1999.

[4] 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

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

[6] 조승훈, 전정수, 문용호, 하석운, “효과적인 비행데이터 저장 방식,” 제 7회 국방기술 학술대회, pp.482-488, 2011.

[7] 조승훈, 서정배, 문용호, “항공기에서 보안 강화된 음성 데이터 저장 방식,” 대한임베디드공학회 논문지, Vol. 6, No. 4, pp.255-261, 2011.

[8] W. Stalling, Cryptography and Network Security Principles and Practice, Prentice Hall, 2002.

저 자 소 개

조 승 훈

2011년 2월: 경상대학교 정보과학사(공학사).
2012년 4월 현재: 경상대학교 일반대학원 정보과학과 석사과정.

관심분야: 임베디드 시스템, Real-time OS, 영상처리.
Email: espresso@gnu.ac.kr

하 석 운

1995년: 부산대학교 전자공학과 공학박사.
2002년: 미국 캘리포니아대학교(UCR) 방문연구.
1993년~현재: 경상대학교 정보과학과 교수.

관심분야: 디지털영상처리, 임베디드 시스템소프트웨어, 항공영상처리
Email: swha@gnu.ac.kr

문 용 호

1998년: 부산대학교 전자공학과 공학박사.
1998년~2001년: 삼성전자 DM연구소 책임연구원.
2007년~현재: 경상대학교 정보과학과 부교수.
2012년 2월~현재: 미국 캘리포니아대학교(UCSB) 교환 교수.

관심분야: 영상 처리, 동영상 압축, 임베디드 시스템, SoC.
Email: yhmoon5@gnu.ac.kr