



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0124894
(43) 공개일자 2012년11월14일

(51) 국제특허분류(Int. Cl.)

G06F 21/24 (2006.01) H04L 9/14 (2006.01)

G06F 3/06 (2006.01)

(21) 출원번호 10-2011-0042814

(22) 출원일자 2011년05월06일

심사청구일자 2011년05월06일

(71) 출원인

경상대학교산학협력단

경상남도 진주시 진주대로 501 (가좌동)

(주) 에어로매스터

경상남도 사천시 사남면 해안산업로 345

(72) 발명자

문용호

경상남도 진주시 내동로348번길 10, 주공그린빌
아파트 104동 703호 (가좌동)

(74) 대리인

정홍식, 김태현, 이현수

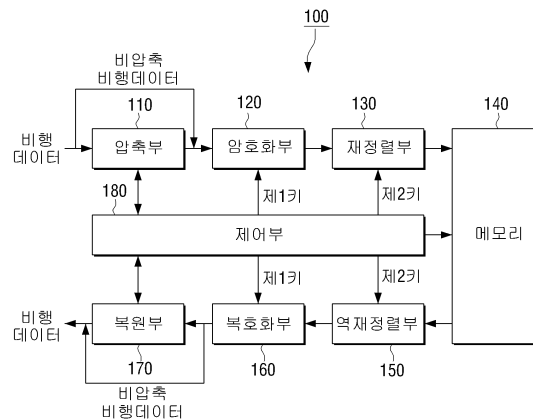
전체 청구항 수 : 총 9 항

(54) 발명의 명칭 비행데이터 저장장치 및 그 방법

(57) 요약

본 발명은 데이터 저장에 관한 것으로서 더욱 상세하게는 비행데이터를 압축하고, 키값을 이용하여 암호화하여 재정렬한 후 저장하며, 저장된 비행데이터를 키값을 이용하여 역재정렬하여 복호화한 후, 복원하기 위한 비행데이터 저장장치 및 그 방법에 관한 것으로서, 이를 위해 본 발명은 비행데이터를 처리하기 위한 압축부, 암호화부, 재정렬부, 메모리, 역재정렬부, 복호화부, 복원부, 및 제어부를 포함한다.

대표도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호 S1065385

부처명 중소기업청

연구사업명 구매조건부신제품개발사업

연구과제명 한국형 기동헬기용 데이터 전송체계(DTS) 개발

주관기관 (주) 에어로매스터

연구기간 2010.06.01 ~ 2011.05.31

특허청구의 범위

청구항 1

비행데이터의 암호화를 위한 암호화부;

상기 암호화부에서 암호화된 데이터의 재정렬을 위한 재정렬부;

상기 재정렬부에서 재정렬된 데이터의 저장을 위한 메모리;

상기 메모리에 저장된 재정렬된 데이터의 역재정렬을 위한 역재정렬부;

상기 역재정렬부에서 역재정렬된 데이터의 복호화를 위한 복호화부; 및

제1 키값을 제공하여 상기 데이터의 암호화와 복호화를 수행하고, 제2 키값을 제공하여 상기 데이터의 재정렬과 역재정렬을 수행하는 제어부;를 포함하는 것을 특징으로 하는 비행데이터 저장장치.

청구항 2

제 1항에 있어서, 상기 비행 데이터 저장장치는

상기 비행데이터가 압축되어 저장되는 데이터일 경우, 상기 비행데이터를 압축하는 압축부; 및

상기 압축부에서 압축된 비행데이터의 압축을 풀어 원 데이터를 복원하는 복원부를 더 포함하며,

상기 제어부는 상기 비행데이터의 속성 및 유형에 따라 상기 압축부 및 상기 복원부의 동작여부를 결정하는 것을 특징으로 하는 비행데이터 저장장치.

청구항 3

제 1항에 있어서, 상기 비행데이터는

전송 체계(DTS: Data Transfer System)나 혹은 블랙 박스에 기록되는 항공기의 결함자료, 표시점(Markpoint), 항공기의 고도, 속도, 자세와 같은 운항 데이터, 음성 및 동영상, 그리고 조종사의 조작 데이터를 포함하는 것을 특징으로 하는 비행데이터 저장장치.

청구항 4

비행데이터의 재정렬을 위한 재정렬부;

상기 재정렬부에서 재정렬된 데이터의 암호화를 위한 암호화부;

상기 암호화부에서 암호화된 데이터의 저장을 위한 메모리;

상기 메모리에 저장된 암호화된 데이터의 복호화를 위한 복호화부;

상기 복호화부에서 복호화된 데이터의 역재정렬화를 위한 역재정렬부; 및

제1 키값을 제공하여 상기 데이터의 암호화와 복호화를 수행하고, 제2 키값을 제공하여 상기 데이터의 재정렬과 역재정렬을 수행하는 제어부;를 포함하는 것을 특징으로 하는 비행데이터 저장장치.

청구항 5

제 4항에 있어서, 상기 비행 데이터 저장장치는

상기 비행데이터가 압축되어 저장되는 데이터일 경우, 상기 비행데이터를 압축하는 압축부; 및

상기 압축부에서 압축된 비행데이터의 압축을 풀어 원 데이터를 복원하는 복원부를 더 포함하며,

상기 제어부는 상기 비행데이터의 속성 및 유형에 따라 상기 압축부 및 복원부의 동작여부를 결정하는 것을 특징으로 하는 비행데이터 저장장치.

청구항 6

비행데이터를 디지털화시키는 A/D 코덱;

상기 A/D 코덱에서 디지털화된 데이터를 ADPCM(Adaptive Differential Pulse Code Modulation) 방식의 엔코딩(Encoding)을 통해 압축하는 ACPCM 엔코딩부;

상기 ACPCM 엔코딩부에 의해 압축된 데이터를 AES(Advanced encryption standard)방식으로 암호화하는 AES 암호화부;

상기 AES 암호화부에 의해 암호화된 데이터를 재정렬하기 위한 재정렬부;

상기 재정렬부에 의해 재정렬된 데이터의 저장을 위한 메모리;

상기 메모리에 저장된 데이터의 역재정렬을 위한 역재정렬부;

상기 역재정렬부에 의해 역재정렬된 상기 데이터를 AES 방식으로 복호화 하는 AES 복호화부;

상기 AES 복호화부에 의해 복호화된 상기 데이터를 ADPCM 방식의 디코딩(Decoding)을 통해 복원을 위한 ADPCM 디코딩부; 및

상기 ADPCM 디코딩부에 의해 디코딩된 상기 데이터의 D/A 변환을 위한 D/A 코덱; 을 포함하며,

상기 AES 암호화부와 상기 AES 복호화부는,

제1 키값을 제공받아 암호화와 복호화를 각각 수행하고,

상기 재정렬부와 상기 역재정렬부는,

제2 키값을 제공받아 재정렬과 역재정렬을 각각 수행하는 것을 특징으로 하는 비행데이터 저장장치.

청구항 7

비행데이터를 제1 키값을 이용하여 암호화를 수행하는 암호화 과정;

암호화된 비행데이터를 제2 키값을 이용하여 재정렬을 수행하는 재정렬 과정;

재정렬된 비행데이터를 저장하는 저장 과정;

저장된 비행데이터를 제2 키값을 이용하여 역재정렬을 수행하는 역재정렬 과정; 및

역재정렬된 비행데이터를 제1 키값을 이용하여 복호화를 수행하는 복호화 과정; 을 포함하는 것을 특징으로 하는 비행데이터 저장방법.

청구항 8

제 7항에 있어서, 상기 비행데이터 저장방법은

상기 암호화 과정 전에, 상기 비행데이터가 압축되어 저장되는 데이터인 경우, 압축하는 압축 과정; 및

상기 복호화 과정 후에, 상기 비행데이터가 상기 압축 과정에서 압축된 데이터인 경우, 압축을 푸는 복원 과정을 더 포함하는 것을 특징으로 하는 비행데이터 저장방법.

청구항 9

제 7항에 있어서, 상기 비행데이터는

전송 체계(DTS: Data Transfer System)나 블랙 박스에 기록되는 항공기의 결함자료, 표시점(Markpoint), 항공기의 고도, 속도, 자세와 같은 운항 데이터, 음성 및 동영상, 그리고 조종사의 조작 데이터를 포함하는 것을 특징으로 하는 비행데이터 저장방법.

명세서

기술분야

본 발명은 데이터 저장에 관한 것으로서 더욱 상세하게는 비행데이터를 압축하고, 키값을 이용하여 암호화하

여 재정렬한 후 저장하며, 저장된 비행데이터를 키값을 이용하여 역재정렬하여 복호화한 후, 복원하기 위한 비행데이터 저장장치 및 그 방법에 관한 것이다.

배경 기술

- [0002] 최근 들어, 항공 기술에 관한 연구가 활발히 진행되고 있다.
- [0003] 일반적으로 항공기에는 데이터 전송 체계 (DTS: Data Transfer System)와 블랙박스 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 결함자료, 표시점 (Markpoint), 항공기 자세, 음성 및 동영상, 그리고 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 비행데이터는 실시간으로 압축되어 저장되고 있다. 그러나 저장장치에 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 비행데이터를 확보한다면 핵심기술의 유출 및 이에 따른 경제적 피해가 발생될 것이라는 문제점이 있었다. 또한, 비행데이터가 적군에게 유출될 경우 전투력뿐만 아니라 작전 기밀의 노출에 따른 유, 무형의 막대한 피해가 예상된다는 문제점도 있었다.
- [0004] 이 같은 사태를 예방하기 위하여 현재 항공기 내의 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. 이와 같은 이유로, 비행데이터의 저장에 있어서 보다 강화된 보안 기술의 도입은 매우 중요하며 시급한 일이다.
- [0005] 비행데이터의 효과적인 저장을 위해서는 기본적으로 압축과 실시간 처리가 요구된다. 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 문제는 비행데이터를 압축함으로써 해결될 수 있다. 현재 항공기의 운항 중에 얻어지는 음성 및 동영상은 기존에 알려진 압축 기술에 의하여 압축되어 저장되고 있으며 이 같은 저장 방식은 다른 유형의 비행데이터들의 저장에도 손쉽게 확대, 적용할 수 있다. 이상의 사실들은 강화된 보안 방식의 개발에 있어서 중요한 지침을 제시한다. 즉, 개발될 보안 방식은 압축 효율을 저하시키지 않으면서 실시간 처리에 문제를 야기하지 않아야 한다는 전제조건을 요구한다.

발명의 내용

해결하려는 과제

- [0006] 본 발명은 상술한 바와 같은 종래기술의 문제점을 해결하기 위해 안출된 것으로서, 본 발명의 목적은, 특히 비행데이터를 키값을 이용하여 암호화하고 재정렬하여 보안성을 강화하기 위한 비행데이터 저장장치 및 그 방법을 제공하는 것이다.

과제의 해결 수단

- [0007] 이를 위해 본 발명에 따르는 비행데이터 저장장치는, 비행데이터의 암호화를 위한 암호화부, 상기 암호화부에서 암호화된 데이터의 재정렬을 위한 재정렬부, 상기 재정렬부에서 재정렬된 데이터의 저장을 위한 메모리, 상기 메모리에 저장된 재정렬된 데이터의 역재정렬을 위한 역재정렬부, 상기 역재정렬부에서 역재정렬된 데이터의 복호화를 위한 복호화부, 및 제1 키값을 제공하여 상기 데이터의 암호화와 복호화를 수행하고, 제2 키값을 제공하여 상기 데이터의 재정렬과 역재정렬을 수행하는 제어부를 포함한다.
- [0008] 상기 비행 데이터 저장장치는 상기 비행데이터가 압축되어 저장되는 데이터일 경우, 상기 비행데이터를 압축하는 압축부, 및 상기 압축부에서 압축된 비행데이터의 압축을 풀어 원 데이터를 복원하는 복원부를 더 포함하며, 상기 제어부는 상기 비행데이터의 속성 및 유형에 따라 상기 압축부 및 상기 복원부의 동작여부를 결정한다.
- [0009] 상기 비행데이터는 전송 체계(DTS: Data Transfer System)나 혹은 블랙 박스에 기록되는 항공기의 결함자료,

표시점(Markpoint), 항공기의 고도, 속도, 자세와 같은 운항 데이터, 음성 및 동영상, 그리고 조종사의 조작 데이터를 포함한다.

[0010] 또한, 이를 위해 본 발명에 따르는 비행데이터 저장장치는 비행데이터의 재정렬을 위한 재정렬부, 상기 재정렬부에서 재정렬된 데이터의 암호화를 위한 암호화부, 상기 암호화부에서 암호화된 데이터의 저장을 위한 메모리, 상기 메모리에 저장된 암호화된 데이터의 복호화를 위한 복호화부, 상기 복호화부에서 복호화된 데이터의 역재정렬화를 위한 역재정렬부, 및 제1 키값을 제공하여 상기 데이터의 암호화와 복호화를 수행하고, 제2 키값을 제공하여 상기 데이터의 재정렬과 역재정렬을 수행하는 제어부를 포함한다.

[0011] 상기 비행 데이터 저장장치는 상기 비행데이터가 압축되어 저장되는 데이터일 경우, 상기 비행데이터를 압축하는 압축부, 및 상기 압축부에서 압축된 비행데이터의 압축을 풀어 원 데이터를 복원하는 복원부를 더 포함하며, 상기 제어부는 상기 비행데이터의 속성 및 유형에 따라 상기 압축부 및 복원부의 동작여부를 결정한다.

[0012] 그리고 이를 위해 본 발명에 따르는 비행데이터 저장장치는 비행데이터를 디지털화시키는 A/D 코덱, 상기 A/D 코덱에서 디지털화된 데이터를 ADPCM(Adaptive Differential Pulse Code Modulation) 방식의 엔코딩(Encoding)을 통해 압축하는 ACPCM 엔코딩부, 상기 ACPCM 엔코딩부에 의해 압축된 데이터를 AES(Advanced encryption standard)방식으로 암호화하는 AES 암호화부, 상기 AES 암호화부에 의해 암호화된 데이터를 재정렬하기 위한 재정렬부, 상기 재정렬부에 의해 재정렬된 데이터의 저장을 위한 메모리, 상기 메모리에 저장된 데이터의 역재정렬을 위한 역재정렬부, 상기 역재정렬부에 의해 역재정렬된 상기 데이터를 AES 방식으로 복호화 하는 AES 복호화부, 상기 AES 복호화부에 의해 복호화된 상기 데이터를 ADPCM 방식의 디코딩(Decoding)을 통해 복원을 위한 ADPCM 디코딩부, 및 상기 ADPCM 디코딩부에 의해 디코딩된 상기 데이터의 D/A 변환을 위한 D/A 코덱, 을 포함하며, 상기 AES 암호화부와 상기 AES 복호화부는, 제1 키값을 제공받아 암호화와 복호화를 각각 수행하고, 상기 재정렬부와 상기 역재정렬부는, 제2 키값을 제공받아 재정렬과 역재정렬을 각각 수행한다.

[0013] 그리고 본 발명에 따르는 비행데이터 저장방법은 비행데이터를 제1 키값을 이용하여 암호화를 수행하는 암호화 과정, 암호화된 비행데이터를 제2 키값을 이용하여 재정렬을 수행하는 재정렬 과정, 재정렬된 비행데이터를 저장하는 저장 과정, 저장된 비행데이터를 제2 키값을 이용하여 역재정렬을 수행하는 역재정렬 과정, 및 역재정렬된 비행데이터를 제1 키값을 이용하여 복호화를 수행하는 복호화 과정, 을 포함한다.

[0014] 상기 비행데이터 저장방법은 상기 암호화 과정 전에, 상기 비행데이터가 압축되어 저장되는 데이터인 경우, 압축하는 압축 과정, 및 상기 복호화 과정 후에, 상기 비행데이터가 상기 압축 과정에서 압축된 데이터인 경우, 압축을 푸는 복원 과정을 더 포함한다.

[0015] 상기 비행데이터는 전송 체계(DTS: Data Transfer System)나 블랙 박스에 기록되는 항공기의 결합자료, 표시점(Markpoint), 항공기의 고도, 속도, 자세와 같은 운항 데이터, 음성 및 동영상, 그리고 조종사의 조작 데이터를 포함한다.

발명의 효과

[0016] 본 발명의 다양한 실시 예에 따르면, 비행데이터를 2단계로 보안 처리함으로써 정보의 유출을 방지하는 효과가 있다.

[0017] 따라서 본 발명의 다양한 실시 예에 따르면, 궁극적으로 기밀 사항인 비행데이터의 유출로 발생하는 경제적 군사적 손실을 미연에 방지할 수 있는 효과가 있다.

도면의 간단한 설명

[0018] 도 1은 본 발명의 일 실시 예에 따르는 비행데이터 저장장치를 보여주기 위한 블록도.

도 2는 본 발명의 다른 실시 예에 따르는 비행데이터 저장장치를 보여주기 위한 블록도.

도 3은 본 발명의 또 다른 실시 예에 따르는 비행데이터 저장장치를 보여주는 블록도.

도 4는 본 발명의 또 다른 실시 예에 따르는 비행데이터 저장장치에서 제1 키를 제공받아 AES 방식으로 (a)암호화와 (b)복호화를 수행하는 방법을 보여주는 블록도.

도 5는 본 발명의 또 다른 실시 예에 따르는 재정렬부가 제 2키값을 입력받아 재정렬하는 동작을 보여주는 예시도.

도 6은 본 발명의 일 실시 예에 따르는 비행데이터 저장방법을 보여주는 순서도.

도 7은 보안기능이 존재하지 않는 기존 저장 방식에서의 음성신호 파형을 보여주는 그래프.

도 8은 본 발명을 적용한 시스템에서 재정렬키가 올바르게 입력되고 복호화 키가 다른 경우에 얻어지는 파형을 보여주는 그래프.

도 9는 복호화 키가 올바르게 입력되었고 재정렬 키가 일치하지 않는 경우의 파형을 보여주는 그래프.

도 10의 경우는 복호화 키와 재정렬 키가 모두 일치하지 않는 경우의 파형을 보여주는 그래프.

발명을 실시하기 위한 구체적인 내용

- [0019] 이하에서는 첨부된 도면들을 참조하여 본 발명의 실시 예에 따른 비행데이터 저장장치 및 그 방법을 상세히 설명한다.
- [0020] 도 1 내지 도 10의 동일 부재에 대해서는 동일한 도면 번호를 기재하였다.
- [0021] 본 발명의 기본 원리는 키값을 이용하여 비행데이터를 암호화와 재정렬화의 2단계 보안처리를 하여 저장하고, 보안처리된 비행데이터를 키값을 이용하여 복호화와 역재정렬화로 복원하는 것이다.
- [0022] 아울러, 본 발명을 설명함에 있어서, 관련된 공지 기능 혹은 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단된 경우 그 상세한 설명은 생략한다.
- [0023] 도 1은 본 발명의 일 실시 예에 따르는 비행데이터 저장장치를 보여주기 위한 블록도이다.
- [0024] 도 1을 참조하면, 본 발명에 따르는 비행데이터 저장장치(100)는 비행데이터의 압축을 위한 압축부(110), 압축부(110)에서 압축된 데이터 혹은 압축되지 않은 입력 비행데이터의 암호화를 위한 암호화부(120), 암호화부(120)에서 암호화된 데이터의 재정렬을 위한 재정렬부(130), 재정렬부(130)에서 재정렬된 데이터의 저장을 위한 메모리(140), 메모리(140)에 저장된 재정렬된 데이터의 역재정렬을 위한 역재정렬부(150), 역재정렬부(150)에서 역재정렬된 데이터의 복호화를 위한 복호화부(160), 복호화부(160)에서 복호화된 데이터의 복원을 위한 복원부(170), 및 비행데이터의 유형에 따라 데이터 압축부(110) 및 복원부(170)의 동작여부를 결정하고, 데이터의 암호화와 복호화를 수행하도록 제1 키값을 제공하고, 데이터의 재정렬과 역재정렬을 수행하도록 제2 키값을 제공하는 제어부(180)를 포함한다.
- [0025] 도 1과 같이 구성된 본 발명의 일 실시 예에 따르는 비행데이터 저장장치(100)를 자세히 설명하면 다음과 같다.
- [0026] 우선, 일반적으로 항공기에는 데이터 전송 체계 (DTS: Data Transfer System)와 블랙박스 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 결함자료, 표시점 (Markpoint), 항공기 자세, 음성 및 동영상, 그리고 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. 따라서 비행데이터는 DTS와 블랙박스에 기록되는 데이터를 의미한다.
- [0027] 이와 같은 비행데이터의 효과적인 저장을 위해 압축부(110)는 비행데이터를 고효율로 압축한다. 왜냐하면, 장시간의 비행으로 인하여 수집되는 비행데이터의 양은 방대하기 때문에 대용량의 메모리가 요구되므로 비용이 증가한다. 이와 같은 이유로 비용이 증가되는 것을 방지하기 위해서 비행데이터는 고효율로 압축되는 것은 필수적이다.
- [0028] 한편, 비행데이터에는 압축되지 않는 비행데이터도 존재하기 때문에, 제어부(180)는 비행데이터의 유형에 따라 압축여부를 결정하여 만약, 입력되는 비행데이터가 압축되지 않는 데이터라면 압축부(110)를 거치지 않고 바로 암호화부(120)에서 암호화된다.
- [0029] 그 후, 암호화부(120)는 이와 같이 압축된 비행데이터 혹은 압축되지 않은 입력 비행데이터를 암호화한다.
- [0030] 여기서 암호화부(120)는 제어부(180)에서 제공된 제1 키값을 이용하여 비행데이터를 암호화한다.
- [0031] 그러면, 재정렬부(130)는 제어부(180)에서 제공된 제2 키값을 이용하여 비행데이터를 재정렬한다.

- [0032] 여기서 키값은 통상의 지식에 기반하여 다양한 방식들에 의하여 설정될 수 있다.
- [0033] 이와 같이 비행데이터는 제1 키값이 적용되어 암호화되고, 제2 키값이 적용되어 재정렬되는 2단계 보안 과정을 거쳐 안전한 형태로 메모리(140)에 저장된다.
- [0034] 한편, 메모리(140)에 저장된 비행데이터를 출력하는 경우에는, 우선 역재정렬부(150)는 재정렬부에서 사용된 제2 키값을 제어부(180)로부터 입력받아서 재정렬된 비행데이터의 역재정렬을 수행한다.
- [0035] 그 후, 복호화부(160)는 암호화부에서 사용된 제1 키값을 제어부(180)로부터 입력받아서 암호화된 비행데이터를 복호화한다.
- [0036] 마지막으로 복원부(170)는 압축부(110)에서 압축한 비행데이터를 복원한다.
- [0037] 만약, 입력되는 비행데이터가 압축되지 않은 데이터였기 때문에 압축부(110)에서 압축되지 않은 경우에는, 복원부(170)에서 압축을 풀어 복원시키지 않는다.
- [0038] 즉, 압축부(110)와 복원부(170)의 적용 여부는 비행데이터의 압축여부 따라 제어부(180)에서 결정된다.
- [0039] 그러면, 복원된 비행데이터는 재생되어 사용자에게 항공기의 비행 정보를 제공할 수 있다.
- [0040] 도 2는 본 발명의 다른 실시 예에 따르는 비행데이터 저장장치를 보여주기 위한 블록도이다.
- [0041] 도 2를 참조하면, 본 발명의 다른 실시 예에 따르는 비행데이터 저장장치(200)는 비행데이터의 압축을 위한 압축부(110), 압축부(110)에서 압축된 데이터 혹은 압축되지 않은 입력 비행데이터의 재정렬을 위한 재정렬부(130), 재정렬된 데이터의 암호화를 위한 암호화부(120), 암호화부(120)에서 암호화된 데이터의 저장을 위한 메모리(140), 메모리(140)에 저장된 암호화된 데이터의 복원을 위한 복호화부(160), 복호화부(160)에서 복호화된 데이터의 역재정렬을 위한 역재정렬부(150), 역재정렬부(150)에서 역재정렬된 데이터의 복원을 위한 복원부(170), 및 비행데이터의 유형에 따라 데이터 압축부(110) 및 복원부(170)의 동작여부를 결정하고, 데이터의 암호화와 복호화를 수행하도록 제1 키값을 제공하고, 데이터의 재정렬과 역재정렬을 수행하도록 제2 키값을 제공하는 제어부(180)를 포함한다.
- [0042] 도 2와 같이 구성된 본 발명의 다른 실시 예에 따르는 비행데이터 저장장치(200)는 도 1과 비교하여 설명하면 다음과 같다.
- [0043] 즉, 도 2는 도 1의 암호화부(120)와 재정렬부(130)에서 수행되는 비행데이터의 암호화와 재정렬화는 순서에 상관없이 어느 한쪽이 우선하여 수행되어도 된다는 것을 보여주기 위한 블록도이다.
- [0044] 마찬가지로, 도 2는 도 1의 역재정렬부(150)와 복호화부(160)에서 수행되는 비행데이터의 역재정렬화와 복호화가 순서에 상관없이 어느 한쪽이 우선하여 수행되어도 된다는 것을 보여주기 위한 블록도이다.
- [0045] 즉, 비행데이터의 암호화와 재정렬화는 어느 한쪽이 우선 수행되더라도, 복호화와 역재정렬화 과정이 순서에 상관없이 수행되어도 된다는 의미이다.
- [0046] 도 3은 본 발명의 또 다른 실시 예에 따르는 비행데이터 저장장치(300)를 보여주는 블록도이다.
- [0047] 도 3은 도 1과 도 2의 비행데이터 저장장치(100, 200)가 처리하는 비행데이터를 음성 데이터에 국한하여 설명하도록 한다.
- [0048] 도 3을 참조하면, 본 발명의 또 다른 실시 예에 따르는 비행데이터 저장장치(300)는 음성 데이터를 디지털화시키는 A/D 코덱(310), A/D 코덱(310)에서 디지털화된 음성 데이터를 ADPCM(Adaptive Differential Pulse Code Modulation) 방식의 엔코딩(Encoding)을 통해 압축하는 ACPCM 엔코딩부(320), ACPCM 엔코딩부(320)에서 압축된 음성 데이터를 제1 키값을 제공받아 AES(Advanced encryption standard) 방식으로 암호화하는 AES 암호화부(330), 제2 키값을 제공받아 AES 암호화된 음성 데이터의 재정렬을 위한 재정렬부(340), 재정렬된 음성 데이터의 저장을 위한 메모리(350), 제 2키값을 제공받아 저장된 음성 데이터의 역재정렬을 위한 역재정렬부(360), 제1 키값을 제공받아 역재정렬된 음성 데이터의 AES 방식으로 복호화하는 AES 복호화부(370), 압축된 음성 데이터를 ADPCM 방식의 디코딩(Decoding)을 통해 복원을 위한 ADPCM 디코딩부(380), 및 디코딩된 음성 데이터의 D/A 변환을 위한 D/A 코덱(390)을 포함하여 구성된다.
- [0049] 도 3을 참조하면, 본 발명의 또 다른 실시 예에 따르는 비행데이터 저장장치(300)의 동작은 다음과 같다.
- [0050] 우선, A/D 코덱(310)은 음성 데이터의 처리를 위해 디지털화한다. 이와 같이 디지털화된 음성 데이터는 ADPCM 엔코딩부(320)에 의해 ADPCM(Adaptive Differential Pulse Code Modulation) 방식의 엔코딩(Encoding)을 통해

압축된다.

- [0051] 압축된 음성 데이터는 제1 키값을 제공받은 AES 암호화부(330)에 의해 암호화된다.
- [0052] AES는 FIPS-197 암호화 표준으로서, SPN(Substitution-Permutation Network)구조의 가변 블록 길이를 지원하는 블록 암호화 방식이다.
- [0053] SPN은 입력 블록을 여러 개의 부분블록들로 나누고 각 부분블록을 S-box로 입력하여 대치시키고 S-box의 출력을 P-box로 전치하는 과정을 반복한다. 암호화에 사용되는 제1 키(key)는 128, 192, 256bit의 길이를 가질 수 있고 제1 키 길이에 대하여 각각 10, 12, 14라운드의 연산을 수행한다.
- [0054] 도 4는 본 발명의 또 다른 실시 예에 따르는 비행데이터 저장장치(300)에서 제1 키를 제공받아 AES 방식으로 (a)암호화와 (b)복호화를 수행하는 방법을 보여주는 블록도이다.
- [0055] 도 4를 참조하면, 본 발명의 또 다른 실시 예에 따르는 비행데이터 저장장치(300)의 제1 키값을 제공받은 AES 암호화부(330)가 음성 데이터를 암호화하고 제1 키값을 제공받은 AES 복호화부(370)가 암호화된 음성 데이터를 복호화하는 것을 보여주는 블록도이다.
- [0056] 도 4를 참조하면, 마지막 라운드를 제외한 나머지 라운드는 비교적 간단한 연산인 순열연산과 치환연산으로 구성된다.
- [0057] 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 본 발명의 또 다른 실시 예에 따르는 AES 암호화부(330)는 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.
- [0058] 이와 같이 AES 암호화부(330)에 의해 음성 데이터가 암호화되면, 재정렬부(340)에서 암호화된 음성 데이터의 재정렬을 수행한다.
- [0059] 도 5는 본 발명의 또 다른 실시 예에 따르는 재정렬부(340)가 제 2키값을 입력받아 재정렬하는 동작을 보여주는 예시도이다.
- [0060] 본 발명의 또 다른 실시 예에서는 보안 성능을 보다 더 강화하기 위하여 ADPCM의 오류 전파 특성에 기반한 재정렬(Reodering) 방식을 제안한다.
- [0061] 상술한 바와 같이 ADPCM 방식으로 압축된 데이터의 복원에 있어서 특정 순간에 발생하는 예측값의 오류는 오랜 시간 동안 데이터의 복원이 제대로 이루어지지 못하게 한다. 따라서 특정 순간의 예측값을 의도적으로 훼손할 경우 훼손방식을 알지 못한다면 올바른 데이터가 얻어질 수 없을 것이다. 이러한 특성에 기반하여 본 발명의 또 다른 실시 예에서는 효율적인 보안 방식을 제안한다.
- [0062] 도 5를 참조하면, 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.
- [0063] 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. 도 5는 제2 키값(난수 생성 방식에 의하여 얻어진)이 2와 21인 경우의 재정렬된 데이터를 보여준다. 또한, 역재정렬을 수행할 때 재정렬 키와 일치하지 않는 키가 입력될 경우 원래의 정렬된 데이터가 얻어지지 않아서 올바른 음성신호가 재생되지 못한다. 이와 같은 이유로 본 발명의 또 다른 실시 예에 따르는 비행데이터 저장장치(300)는 시스템에서는 암호화 방식 외에 재정렬 방식을 통해 보안이 더욱 더 강화된다.
- [0064] 도 2의 예와 마찬가지로 본 발명의 또 다른 실시 예에 따르는 비행데이터 저장장치(300)의 AES 암호화부(33

0)와 재정렬부(340)의 위치는 서로 바뀔 수 있고, AES 복호화부(370)와 역재정렬부(360)의 위치도 서로 바뀔 수 있다.

- [0065] 도 6은 본 발명의 일 실시 예에 따르는 비행데이터 저장방법을 보여주는 순서도이다.
- [0066] 도 6을 참조하면, 본 발명의 일 실시 예에 따르는 비행데이터 저장방법(600)은 비행데이터를 압축하는 압축 과정(S610), 압축된 비행데이터 혹은 압축되지 않은 입력 비행데이터를 제1 키값을 이용하여 암호화를 수행하는 암호화 과정(S620), 암호화된 비행데이터를 제2 키값을 이용하여 재정렬을 수행하는 재정렬 과정(S630), 재정렬된 비행데이터를 저장하는 저장 과정(S640), 저장된 비행데이터를 제2 키값을 이용하여 역재정렬을 수행하는 역재정렬 과정(S650), 역재정렬된 비행데이터를 제1 키값을 이용하여 복호화를 수행하는 복호화 과정(S660), 및 복호화된 비행데이터의 복원을 위한 복원 과정(S670)을 포함한다.
- [0067] 도 6과 같이 구성된 본 발명의 일 실시 예에 따르는 비행데이터 저장방법(600)에 있어서도, 암호화 과정(S620)과 재정렬 과정(S620) 중 어느 하나가 우선 수행되더라도 동일하게 동작한다. 마찬가지로, 역재정렬 과정(S650)과 복호화 과정(S660) 중 어느 하나가 우선 수행되더라도 동일하게 동작한다.
- [0068] 그리고 비행데이터의 압축 수행 여부를 판단하여(S605), 원 데이터 형태가 압축되지 않는 형태의 데이터라면 압축 과정(S610)을 생략한다.
- [0069] 마찬가지로 비행데이터의 압축 수행 여부를 판단하여(S665), 원 데이터 형태가 압축되지 않는 형태의 데이터라면 복원 과정(S670)을 생략한다.
- [0070] <모의실험>
- [0071] 본 발명의 또 다른 실시 예에 따르는 비행데이터 저장장치는 16khz의 표본화 주파수에 의하여 얻어진 샘플을 16bit로 양자화함으로써 생성된 30초 분량의 음성 데이터를 이용하여 모의실험을 수행하였다. 이때 ADPCM Encoding은 32kbps로, AES 암호화 블록의 크기는 128bit로 설정하여 실험을 수행하였다.
- [0072] 본 발명의 또 다른 실시 예에 따르는 비행데이터 저장장치의 효과를 확인하기 위하여 복원 시 제1 키(K1)와 제2 키(K2)를 각각 임의로 입력한 경우와 두 가지 모두 임의로 입력한 경우에 대하여 복원된 최종 출력 파형들을 비교하였다.
- [0073] 먼저, 최종 출력 파형들이 인지될 수 있는지 청취한 결과 모든 유형의 실험에서 원래의 음성을 인식하는 것이 불가능한 것을 확인할 수 있었다.
- [0074] 본 발명의 또 다른 실시 예에 따르는 비행데이터 저장장치의 효과를 보다 객관적으로 파악하기 위하여 각각의 경우에 대한 복원 파형을 비교해 보았다.
- [0075] 도 7 내지 도 10은 실험 유형에 따른 음성 신호 중 0.6초부터 0.95초까지를 두 배로 확대하여 나타낸 것이다.
- [0076] 도 7은 보안기능이 존재하지 않는 기존 저장 방식에서의 음성신호 파형을 보여주는 그래프이다.
- [0077] 도 8은 본 발명을 적용한 시스템에서 재정렬키가 올바르게 입력되고 복호화키가 다른 경우에 얻어지는 파형을 보여주는 그래프이다. 이 경우 재정렬 키 K2가 올바르게 입력되더라도 K1이 일치하지 않으면 인식이 불가능한 파형이 생성되는 것을 알 수 있다.
- [0078] 도 9는 복호화 키가 올바르게 입력되었고 재정렬 키가 일치하지 않는 경우의 파형을 보여주는 그래프이다. 도 8의 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.
- [0079] 도 10의 경우는 복호화 키와 재정렬 키가 모두 일치하지 않는 경우의 파형을 보여주는 그래프다. 상술한 경우와 마찬가지로 원래의 파형과는 전혀 다른 파형이 얻어진다. 또한, 도 8과 도 9로부터 2개의 키가 동시에 노출되지 않는 한 원래의 음성 데이터가 재생되지 않는 것을 확인할 수 있다.
- [0080] DTS나 블랙박스과 같은 비행데이터 저장장치는 비상사태 발생 시 데이터 유출을 방지하기 위한 보안장치로서 Zeroize 기능을 보유하고 있다. 그러나 이 장치는 실제 환경에서 오작동하거나 미작동할 가능성이 매우 높다. 이러한 문제점을 해결하기 위하여 본 발명에서는 암호화 방식과 재정렬 방식을 결합한 효과적인 보안 방식을 제안하였다. 청취 실험을 통하여 키값을 모를 경우 출력 파형의 인지가 불가능함을 확인하였고 파형 비교를 통해 그 효과를 객관적으로 검증하였다. 또한, 본 발명은 음성데이터뿐만 아니라 다른 비행데이터의 저장에도

적용이 가능한 특징을 지닌다.

[0081] 이상과 같이 본 발명은 비록 한정된 실시 예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시 예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

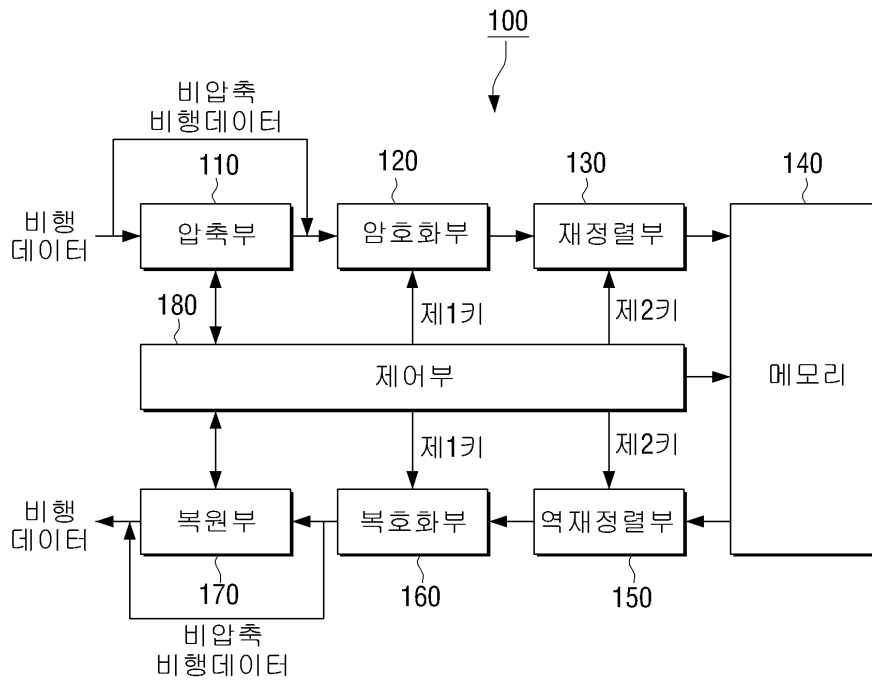
[0082] 그러므로 본 발명의 범위는 설명된 실시 예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐만 아니라 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

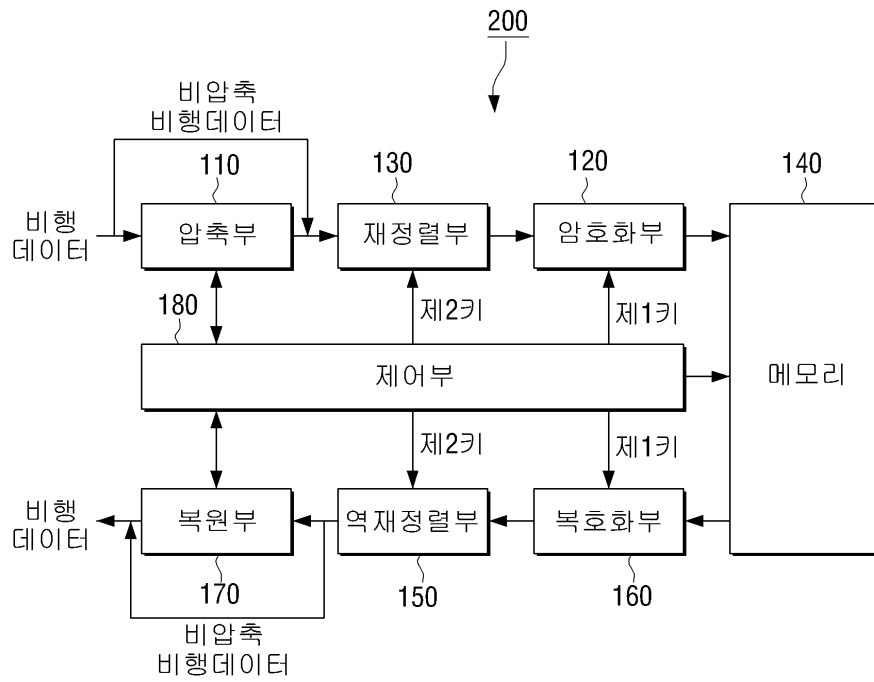
[0083] 100: 비행데이터 저장장치 110: 압축부
120: 암호화부 130: 재정렬부
140: 메모리
150: 역재정렬부
160: 복호화부 170: 복원부
180: 제어부

도면

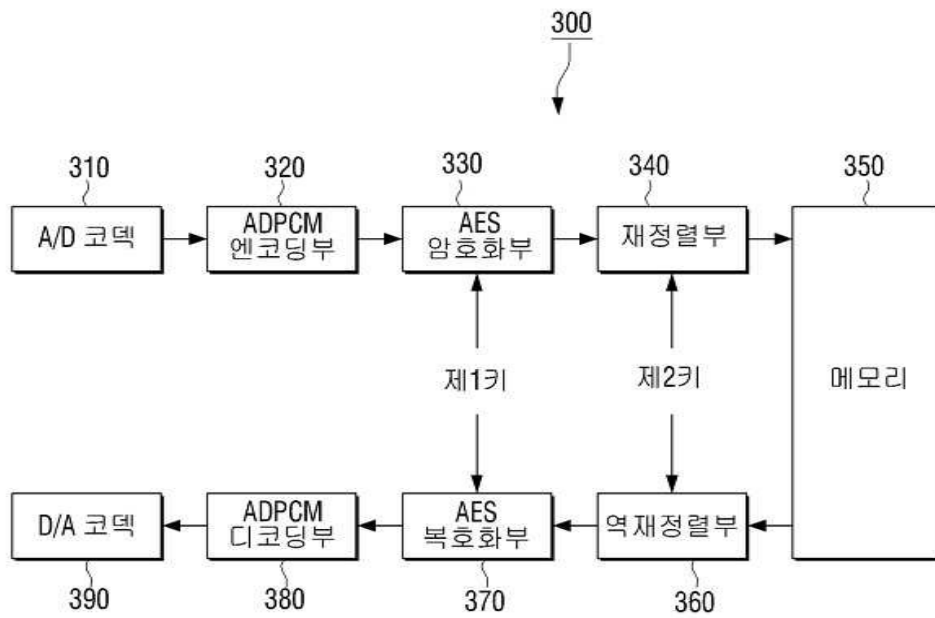
도면1



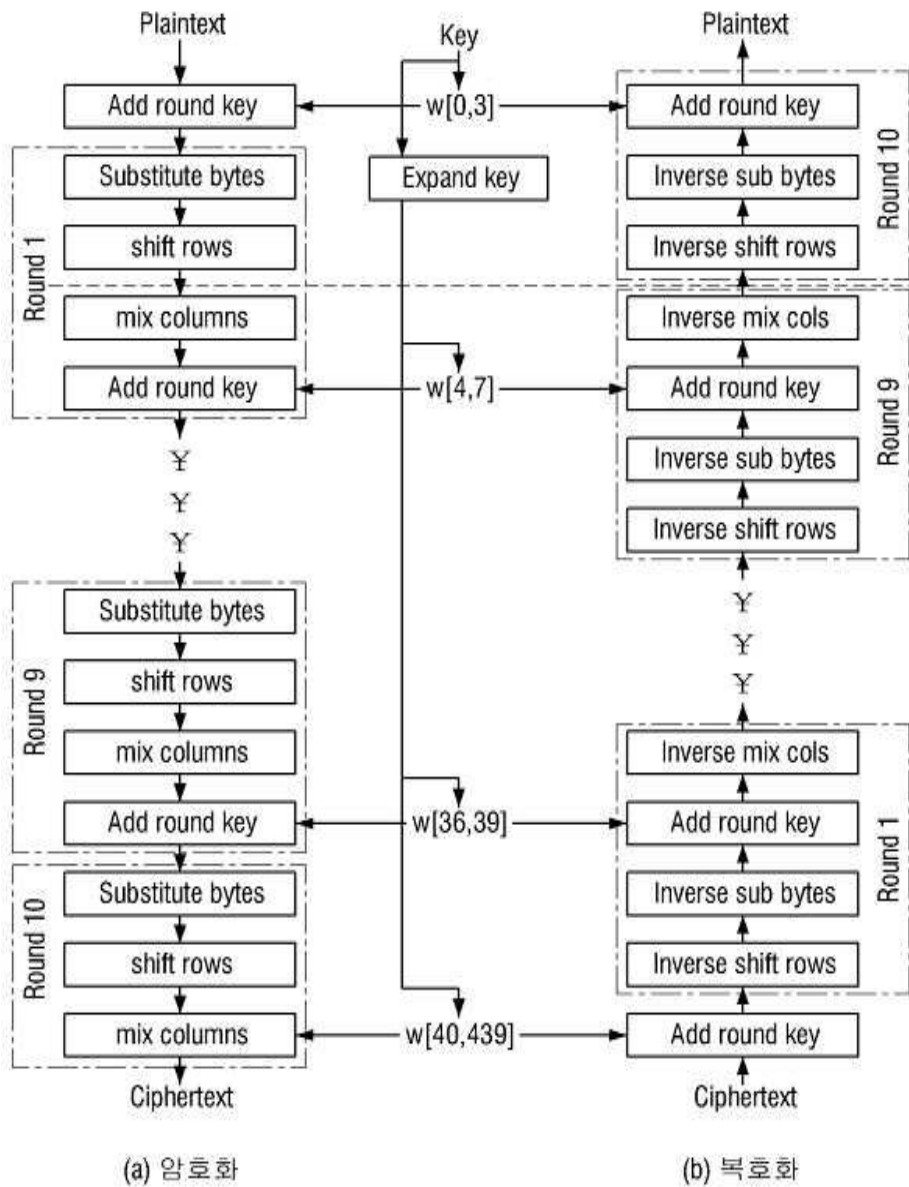
도면2



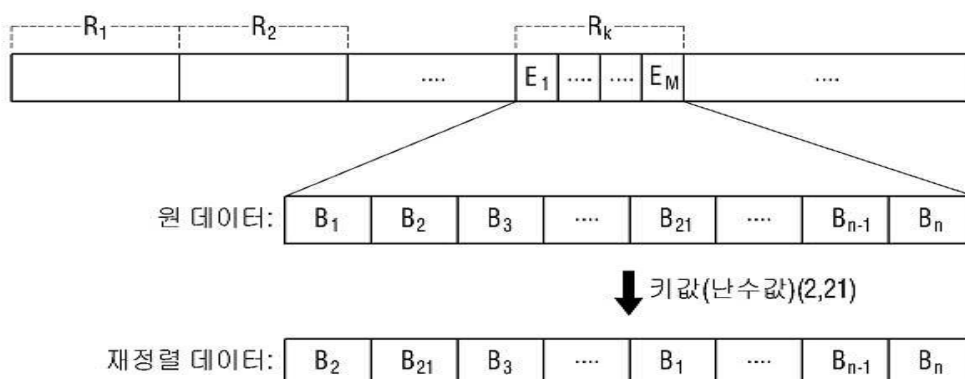
도면3



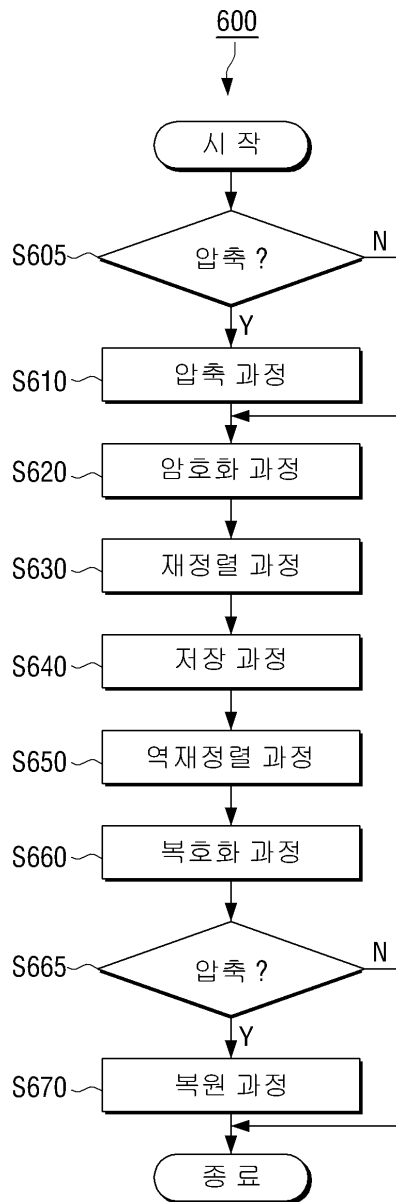
도면4



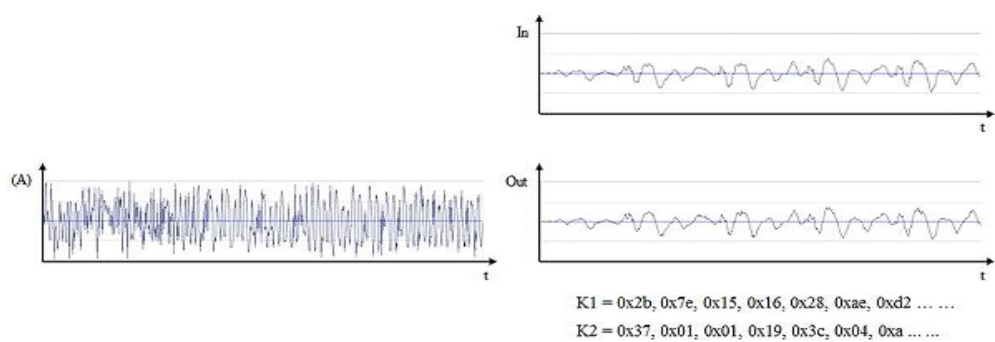
도면5



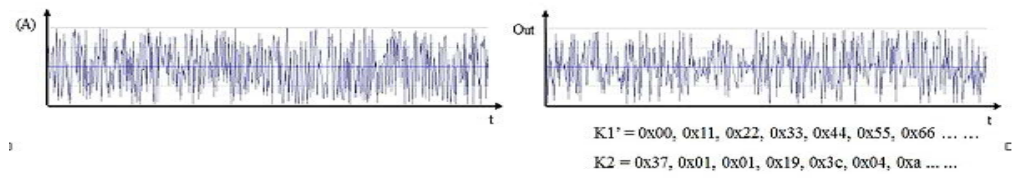
도면6



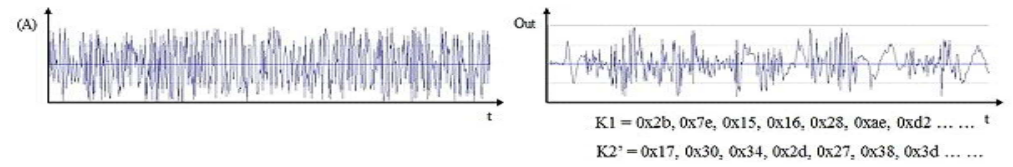
도면7



도면8



도면9



도면10

