(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년12월16일
(11) 등록번호 10-1578055
(24) 등록일자 2015년12월10일

(51) 국제특허분류(Int. Cl.)
H04L 9/28 (2006.01) *H04N 21/2389* (2011.01)
(21) 출원번호 10-2010-7029039
(22) 출원일자(국제) 2009년06월30일
심사청구일자 2014년06월27일
(85) 번역문제출일자 2010년12월23일
(65) 공개번호 10-2011-0040779
(43) 공개일자 2011년04월20일
(86) 국제출원번호 PCT/EP2009/058161
(87) 국제공개번호 WO 2010/000727
국제공개일자 2010년01월07일
(30) 우선권주장
08305364.5 2008년06월30일
유럽특허청(EPO)(EP)
(56) 선행기술조사문헌
JP2008147926 A
JP2004219669 A
JP2007318212 A

(73) 특허권자
톰슨 라이센싱
프랑스 92130 이씨레뮬리노 루 잔다르크 1-5
(72) 발명자
마쏘우디, 에이욥
프랑스, 볼로뉴 빌런코트 에프-92100, 퀘 알퐁스 르 갈로 46, 톰슨
레페브레, 프레데릭
프랑스, 볼로뉴 빌런코트 에프-92100, 퀘 알퐁스 르 갈로 46, 톰슨
(74) 대리인
문경진, 김학수

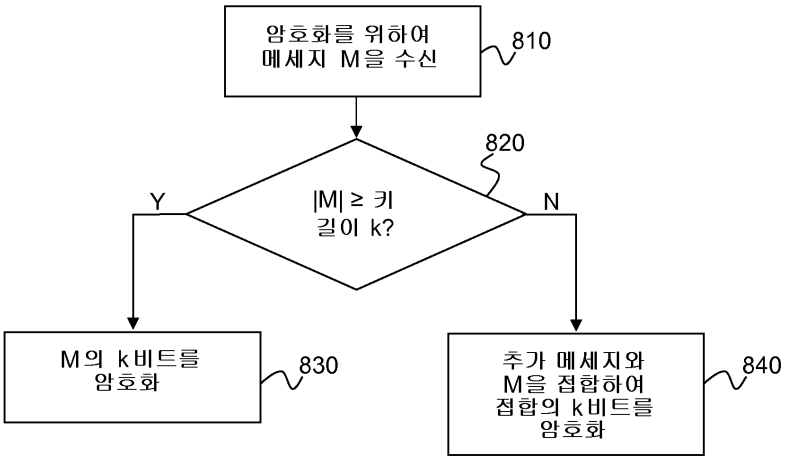
전체 청구항 수 : 총 11 항 심사관 : 문형섭

(54) 발명의 명칭 **선택적 데이터 암호화를 위한 방법 및 장치**

(57) 요 약

본 발명은 키(key) 길이 k를 갖는 암호화 키 K를 사용하여, 균일하게 배포된 심볼을 포함하는 적어도 하나의 메세지(M)의 암호화 방법에 관한 것이고, 암호화 이전에, 적어도 k 비트 길이의 길이가 늘어난 메세지를 얻기 위하여, 더 작은 메세지가 예를 들어, 패딩(padding) 또는 접합(concatenation)을 통해 길이가 늘어나는(840) 반면에, 적어도 k 비트만큼 긴 메세지의 k비트는 암호화된다(830). 따라서, 암호화 효율은 암호화 보안이 유지되는 동안 최적화된다. 암호화 방법은 메세지(M)을 포함하는 JPEG2000으로 인코딩된 패킷에, 특히 적합하다. 또한, 암호화 장치(710), 복호화 방법 및 복호화 장치(910)가 제공된다.

대 표 도 - 도8



명 세 서

청구범위

청구항 1

키(key) 길이 k를 갖는 암호화 키 K를 사용하여 메세지(M)를 암호화하는 방법으로서, 메세지(M)는 패킷의 페이로드이고, 비트스트림의 데이터를 포함하는, 메세지(M)를 암호화하는 방법에 있어서,

상기 방법은,

암호화 디바이스에서,

- 메세지(M)의 길이가 키 길이 k 보다 큰 지, 키 길이 k와 동일한지 또는 키 길이 k 보다 작은 지를 결정하는 단계,

- 메세지(M)의 길이가 키 길이 k 보다 큰 경우, 메세지(M)의 k 비트를 정확히 암호화하는 단계,

- 메세지(M)의 길이가 키 길이 k와 동일한 경우, 메세지(M)의 k 비트를 암호화하는 단계,

- 메세지(M)의 길이가 키 길이 k 보다 작은 경우,

- 적어도 k 비트 길이인 길이가 늘어난(lengthened) 메세지를 획득하기 위해 메세지(M)를 적어도 하나의 추가 메세지와 접합하는 단계로서, 적어도 하나의 추가 메세지는 비트스트림의 데이터를 포함하고, 추가 패킷의 페이로드인, 접합 단계,

- 길이가 늘어난 메세지의 k 비트를 정확히 암호화하는 단계를

포함하는, 메세지를 암호화하는 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

제 1항에 있어서, 메세지는 엔트로피 인코딩된 데이터(entropy encoded data)를 포함하는, 메세지를 암호화하는 방법.

청구항 5

제 4항에 있어서, 엔트로피 인코딩된 데이터는 콘텍스트 기반(context-based)의 코더에 의해 코딩된, 메세지를 암호화하는 방법.

청구항 6

제 1항에 있어서, 적어도 하나의 메세지(M)는 적어도 하나의 JPEG2000으로 인코딩된 코드블록인, 메세지를 암호화하는 방법.

청구항 7

키 길이 k를 갖는 암호화 키 K를 사용하여 메세지(M)를 암호화하기 위한 장치로서, 메세지(M)는 패킷의 페이로드이고, 비트스트림의 데이터를 포함하는, 메세지(M)를 암호화하기 위한 장치에 있어서,

상기 장치는,

- 메세지(M)의 길이가 키 길이 k 보다 큰 지, 키 길이 k와 동일한지 또는 키 길이 k 보다 작은 지를 결정하고,

- 메세지(M)의 길이가 키 길이 k 보다 큰 경우, 메세지(M)의 k 비트를 정확히 암호화하고,

- 메세지(M)의 길이가 키 길이 k와 동일한 경우, 메세지(M)의 k 비트를 암호화하고,

- 메세지(M)의 길이가 키 길이 k 보다 작은 경우,

- 적어도 k 비트 길이인 길이가 늘어난 메세지를 획득하기 위해 메세지(M)를 적어도 하나의 추가 메세지와 접합하되, 적어도 하나의 추가 메세지는 비트스트림의 데이터를 포함하고, 추가 패킷의 페이로드인, 접합하고,

- 길이가 늘어난 메세지의 k 비트를 정확히 암호화하도록 적응된 프로세서를

포함하는, 메세지를 암호화하기 위한 장치.

청구항 8

키 길이 k를 갖는 복호화 키 K를 사용하여 암호화된 메세지(M)를 복호화하는 방법으로서, 암호화된 메세지(M)는 패킷의 페이로드이고, 비트스트림의 암호화된 데이터를 포함하는, 암호화된 메세지(M)를 복호화하는 방법에 있어서,

상기 방법은,

복호화 디바이스(910)에서,

- 암호화된 메세지(M)의 길이가 키 길이 k 보다 큰 지, 키 길이 k와 동일한지 또는 키 길이 k 보다 작은 지를 결정하는 단계,

- 암호화된 메세지(M)의 길이가 키 길이 k 보다 큰 경우, 암호화된 메세지(M)의 k 비트를 정확히 복호화하는 단계,

- 암호화된 메세지(M)의 길이가 키 길이 k와 동일한 경우, 암호화된 메세지(M)의 k 비트를 복호화하는 단계,

- 암호화된 메세지(M)의 길이가 키 길이 k 보다 작은 경우,

- 적어도 k 비트 길이인 길이가 늘어난 메세지를 획득하기 위해 암호화된 메세지(M)를 적어도 하나의 추가적인 암호화된 메세지와 접합시키는 단계로서, 적어도 하나의 추가적인 암호화된 메세지는 비트스트림의 암호화된 데이터를 포함하고, 추가 패킷의 페이로드인, 접합 단계,

- 길이가 늘어난 메세지의 k 비트를 정확히 복호화하는 단계를

포함하는, 암호화된 메세지를 복호화하는 방법.

청구항 9

키 길이 k를 갖는 복호화 키 K를 사용하여 암호화된 메세지(M)를 복호화하기 위한 장치로서, 암호화된 메세지(M)는 패킷의 페이로드이고, 비트스트림의 암호화된 데이터를 포함하는, 암호화된 메세지(M)를 복호화하기 위한 장치에 있어서,

상기 장치는,

- 암호화된 메세지(M)의 길이가 키 길이 k 보다 큰 지, 키 길이 k와 동일한지 또는 키 길이 k 보다 작은 지를 결정하고,

- 암호화된 메세지(M)의 길이가 키 길이 k 보다 큰 경우, 암호화된 메세지(M)의 k 비트를 정확히 복호화하고,

- 암호화된 메세지(M)의 길이가 키 길이 k와 동일한 경우, 암호화된 메세지(M)의 k 비트를 복호화하고,

- 암호화된 메세지(M)의 길이가 키 길이 k 보다 작은 경우,

- 적어도 k 비트 길이인 길이가 늘어난 메세지를 획득하기 위해 암호화된 메세지(M)를 적어도 하나의 추가적인 암호화된 메세지와 접합시키되, 적어도 하나의 추가적인 암호화된 메세지는 비트스트림의 암호화된 데이터를 포함하고, 추가 패킷의 페이로드인, 접합시키고,

- 길이가 늘어난 메세지의 k 비트를 정확히 복호화하도록 적응된 프로세서를

포함하는, 암호화된 메세지를 복호화하기 위한 장치.

청구항 10

제 9항에 있어서, 메세지는 엔트로피 인코딩된 데이터를 포함하는, 암호화된 메세지를 복호화하기 위한 장치.

청구항 11

제 10항에 있어서, 엔트로피 인코딩된 데이터는 콘텍스트 기반의 코더에 의해 코딩된, 암호화된 메세지를 복호화하기 위한 장치.

청구항 12

제 9항에 있어서, 적어도 하나의 메세지(M)는 적어도 하나의 JPEG2000으로 인코딩된 코드블록인, 암호화된 메세지를 복호화하기 위한 장치.

청구항 13

제 9항 내지 제 12항 중 어느 한 항에 있어서, 암호화된 메세지(M)는 패킷의 페이로드(payload)의 적어도 일부분인, 암호화된 메세지를 복호화하기 위한 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 일반적으로 데이터 암호화에 관한 것이고, 더 구체적으로, 패킷화된 비트스트림에 구성되는 이미지 데이터의 암호화에 관한 것이다.

배 경 기 술

[0002] 이 섹션은 아래에 서술되고 및/또는 주장되는 본 발명의 다양한 양상에 관련될 수 있는, 기술의 다양한 양상을 독자들에게 소개하는 것으로 의도된다. 본 논의는 독자들에게 본 발명의 다양한 양상에 대한 더 나은 이해를 돕기 위해 배경 정보를 제공하는데 도움이 된다고 믿어진다. 따라서, 이러한 설명은 종래 기술의 인정으로서가 아닌, 이러한 관점으로 읽혀야 한다.

[0003] 설명적인 예시로서, 다음의 서술은, 예를 들어, JPEG2000 인코딩에 의해 얻어지는 비디오 데이터 스트림과 같은, 패킷화 된 비디오 데이터 스트림의 보호에 관한 것이다. 하지만, 당업자라면, 본 발명의 데이터 보호는, 데이터가 필수 특성을 갖는 패킷에 전송되는 유사한 분야에서도 역시 사용될 수 있다고 인식할 것이다.

[0004] 비디오 데이터를 암호화를 통해 보호하는 것은, 특히 조건부 액세스 텔레비전 시스템(conditional access television system)에서 오랫동안 알려져 왔다. 도 1은 콘텐츠 액세스 제어에 대한 전형적인 종래기술의 접근법을 도시한다. 비디오 신호(CNT)는 먼저, 표준 압축 인코더를 사용하여 인코딩 되고(110), 그런 후에, 결과 비트스트림(CNT')은 (DES, AES, 또는 IDEA와 같은) 대칭 암호화 표준을 사용하여 암호화된다(120). 그런 후에, 암호화된 비트 스트림[CNT']은, 인코딩된 비트 스트림(CNT')을 얻기 위하여 암호화된 비트스트팀[CNT']을 복호화하는(130), 수신기에 의해 수신되고, 이 인코딩된 비트 스트림(CNT')은 적어도 이론상으로 초기 비디오 신호와 동일한 비디오 신호(CNT)를 얻기 위하여 디코딩 된다(140). 완전히 계층화되었다고 불리는 이러한 접근법에서, 압축 및 암호화는 완전히 개별적인 처리다. 매체 비트 스트림은 고전적 평문(plaintext) 데이터로 처리되고, 평문에서 모든 심볼(symbol) 또는 비트는 동등한 중요성을 갖으며, 즉, 심볼은 균일하게 배포된다고 가정된다.

[0005] 이러한 기법은 콘텐츠의 전송이 강제되지 않을 때 적합하지만, (메모리, 전력 또는 계산 성능과 같은) 리소스가 제한되는 상황에선 부적합하다고 판단된다. 이러한 기법을 적용하는 다른 방식은, 예를 들어, 암호화된 데이터를 처리하기 위한 처리기의 성능을 증가시키기 위해 때때로 요구되는 것이다.

[0006] 게다가, 다수의 연구는 높은 전송률과 제한된 허용 대역폭을 갖는 이미지 및 비디오 콘텐츠의 특정 특징을 나타내는데, 이 연구는 이러한 콘텐츠에 대한 표준 암호법 기술의 부적합함을 증명한다. 이 연구는, 연구원들이 부분적으로 암호화된 비트 스트림의 결과는 암호화된 서브셋의 복호화 없이는 사용될 수 없다고 예상으로 비트 스트림의 서브셋에 암호화를 적용함으로써, "선택적 암호화", "부분 암호화", "소프트(soft) 암호화", 또는 "지각

적(perceptual) 암호화"로 불리는 콘텐츠를 안전하게 하는 새로운 기법을 조사하게 한다. 일반적인 접근법은 콘텐츠를 2가지 부분으로 나누는 것이다; 제 1 부분은 고유 신호의 이해하기 쉬우나, 저 품질인 버전으로 재구성을 허용하는, 신호의 기본부(예를 들어, 이산 코사인 변환(DCT) 분해에서 직류(DC) 계수 또는 이산 웨이블렛(wavelet) 변환(DWT) 분해에서 저주파 층)이고, "향상" 부라 불릴 수 있는 제 2 부분(예를 들어, 이미지의 DCT 분해에서의 교류(AC) 계수, 또는 DWT에서의 고주파 층)은 이미지의 세밀한(fine) 세부사항의 복구와 고유 신호의 고품질 버전의 재구성을 허용한다. 이러한 기법에 따라, 오직 기본 부만 암호화되는 반면에, 향상 부는 암호화되지 않고 송신될 수 있거나, 또는 경량인(light-weight) 스크램블링을 사용하는 일부 경우에 있게 된다. 목표는, 이진 스트림 그 자체가 아닌, 콘텐츠를 보호하는 것이다.

[0007] 도 2는 종래 기술에 따른 선택적 암호화를 도시한다. 인코딩 및 디코딩은 도 1과 같이 수행된다. 선택적 암호화에서, 선택적 암호화 파라미터(240)에 따라 인코딩된 비트 스트림(CNT')이 암호화 된다(220). 예를 들어, 이들 파라미터는, 언급된 바와 같이, 오직 DC 계수 또는 저 주파 층만이 암호화되어야 하는 반면에, 인코딩된 비트 스트림(CNT')의 나머지는 암호화되지 않은 상태로 남아있어야 한다는 것을 나타낸다. 그런 후에, 부분적으로 암호화된 비트 스트림[CNT']은 선택적 암호화 파라미터(240)에 따라, (부분적으로) 복호화 된다(230).

[0008] 예시적인 선택적 암호화 기법은 T. 쿤켈먼(T. Kunkelmann) 및 R. 레이네마(R. Reinema)에 의해 "멀티미디어 통신 표준에 대한 확장 보안 아키텍쳐(A Scalable Security Architecture for Multimedia Communication Standards)"(멀티미디어 계산 및 시스템 '97){IEEE 국제 회의(1997년 6월 3일~6일, 캐나다, 온타리오, 오타와),(1997년 6월 3일, US, IEEE Comput. Soc, 미국, CA, 로스 알라미토스)}에 서술되어 있다. 8x8 블록을 암호화하기 위하여, 64보다 작은 2개의 정수가 선택되는데; 하나의 정수는 DC 성분에 대한 수이고, 다른 하나는 AC 성분에 대한 수이다. 그런 후에, 개별적인 블록은, 예를 들어, 64비트의 키 길이를 갖는 DES(예를 들어, 스취어 B(Scheier B)에 의해, 제 2 개정판, "DES의 적용 암호법 및 설명", John Wiley & Sons, Inc(뉴욕), 1996년 1월 1일, 페이지 270-277, XP002237575, ISNB: 978-0-471-11709-4, C에서의 프로토콜, 알고리즘, 및 소스 코드)를 사용하여 암호화된다. US 2001/0033656에 서술된 방법과 같이, 다른 적합한 블록 암호화 방법 또한 명백히 사용될 수 있다. 처리는 다수의 AC 및/또는 DC 성분이 암호화될 때까지, 반복된다. 즉, 전체의 성분이 암호화되는 것이 아닌, 각 성분이 완전히 암호화되는 것이다.

[0009] 본 발명이, 본 발명의 제한적이지 않은 실시예로서, 또한 사용되는 JPEG2000에 특히 적합하기에, 이러한 표준의 관련된 부분 즉, JPEG2000의 코드 스트림 구조에 대한 간략한 소개가 이제부터 제공될 것이다.

[0010] JPEG2000 코드 스트림은 패킷으로 구성되고, 코드 스트림 패킷은 해상도, 계층, 성분, 및 영역(precinct)이라 불리는 엔티티의 특정 조합으로부터 데이터를 전송하는 최소단위이다. R 해상도, L 층, P 영역 및 C 성분으로 압축된 이미지는, 따라서, RxLxCxP 패킷을 초래한다.

[0011] JPEG2000은 내장된 비트 스트림을 사용하고: 코드 스트림은 이전에 코딩된 스트림상에 악영향 없이, 임의의 패킷의 제공된 끝 부분을 자를 수 있다.

[0012] 도 3은 메인 코드 스트림 구조를 도시하고, 이 구조는 다음을 포함한다:

[0013] · 메인 헤더(310)는 코드 스트림의 시작(Start of Code Stream)(SOC = 0xFF4F) 마커 세그먼트(312)와 메인 헤더 마커 세그먼트(314)를 포함한다, 이 SOC 마커는 코드 스트림의 시작을 나타내고, 제 1 마커로서 요구된다. 메인 헤더 마커 세그먼트는 예를 들어, 진행 순서, 메인 코딩 스타일, 성분 코딩 스타일, 타일 크기와 같은 사용자에 의해 정의된 다수의 압축 파라미터를 지시한다.

[0014] · 하나 이상의 타일-부 헤더(320a, 320b)는 타일-부 마커의 시작(Start of Tile-part marker)(SOT = 0xFF90)(322), 타일-부 정보(324a, 324b) 및 데이터 마커의 시작(SOD = 0xFF93)(326)을 각각 포함한다. 인식되는 바와 같이, SOT(322) 및 SOD(326)는 표준 값을 갖는 반면에, 타일-부 정보(324a, 324b)는 타일에 대한 정보를 포함하고; 예를 들어, 부분 정보 324a는 이 정보가 타일 0에 속하는 반면에, 타일 부 정보(324b)는 이 정보가 타일 1에 속한다는 것을 나타낸다. 적어도 하나의 타일-부 헤더(320a, 320b)는 타일-부 헤더(320a, 320b), 및 주로 다음의 비트 스트림(330a, 330b)를 포함하는 각 타일-부의 시작 시 요구되고, 여기에서, SOD 마커는 압축된 데이터를 내포하는 비트 스트림(330a, 330b)의 시작을 지시한다.

[0015] · 코드 스트림의 종료(340)(End of Code Stream): 이러한 마커(EOC = 0xFFD9)는 코드 스트림의 종료를 나타낸다.

[0016] 보이는 바와 같이, 비트 스트림은 패킷을 형성하는 패킷 헤더와 패킷 데이터로 주로 구성된다. 도 4는 패킷 헤더(420)와 패킷 데이터(440)를 포함하는 예시적인 JPEG2000 패킷을 도시한다. 패킷 헤더는 사용자가 결정한 옵

션에 따라, 비트스트림 또는 메인 헤더에서 사용될 수 있다. 도 4는 비트 스트림 내의 이러한 헤더의 사용을 나타낸다: 패킷 헤더의 시작(410)(Start of Packet header)(SOP = 0xFF91)및 패킷 헤더의 종료(430)(End of Packet header)(EPH = 0xFF92)는 각각 패킷 헤더(420)의 시작과 종료를 나타낸다.

[0017] 패킷 데이터에 대하여, 일부 코드 워드(word) - 범위[0xFF90; 0xFFFF]의 코드 워드가 JPEG2000에 예약될 수 있다는 것이 언급되어야 한다. 이러한 예약된 코드 워드는 스트림의 메인 구축 블록의 범위를 정하는 마커로 사용된다. 예를 들어, SOT(0xFF90), SOD(0xFF93) 및 EOC(0xFFD9)은 이러한 예약된 코드 워드다. 이 코드 스트림을 암호화할 때, '정상'(즉, 예약되지 않은) 코드 워드가, 값이 예약되는 암호화 된 코드 워드를 초래하지 않는다는 것을 보증하는 것이 중요하다. 패킷 데이터는 인코딩된 엔트로피(entropy)이고, 이 엔트로피의 특성은 패킷 데이터가, 이후에 서술될 암호법으로의 보안 선택적 암호화에 매우 적합되도록 한다.

[0018] 패킷 헤더(420)는 패킷 데이터를 올바르게 파싱 및 디코딩하기 위하여, 디코더에 의해 요구되는 정보를 포함한다.

[0019] · 제로 길이 패킷: 현재 패킷이 비어있는지 아닌지를 나타냄.

[0020] · 코드-블록 포함: 각 영역에 대하여, 태그(tag) 트리는 포함되는 코드 블록을 위한 포함 정보를 인코딩하기 위하여 사용됨.

[0021] · 제로-비트판(bitplane) 정보: 각 영역에 대하여, 태그 트리는 제 1 비 제로 비트-판을 인코딩.

[0022] · 코딩 패스(passes)의 개수: 호프만(Huffman)-스타일 코드 워드는 각 코드 블록을 위해 포함되는 코딩 패스의 개수를 인코딩하는데 사용됨.

[0023] · 각 코드 블록으로부터 압축된 데이터의 길이.

[0024] "압축되지 않은 및 압축된 이미지의 선택적 암호화를 위한 기술", 지능형 시각 시스템에 대한 진보된 개념의 회보(ACIVS: Proceedings of Advanced Concept for Intelligent Vision Systems)(2002)(벨기에, 겐트, 2002년 9월 9-11일)에서, M. 반 드루겐브럭(M. Van Droogenbroeck) 및 R. 베네데트(R. Benedett)는 선택적 암호화를 호프만 코더에 적용하는 것을 제안한다. 게다가, JPEG 호프만 코더는, 엔트로피를 다루기 위하여, 코드 워드/심볼로 연속된 제로를 없앤다. 추가된 비트는 비 제로 계수의 크기 및 기호를 완전히 구체화 시키기 위하여, 이러한 코드 워드에 추가되고, 오직 이들의 추가된 비트만이 DES 또는 IDEA를 사용하여 암호화된다.

[0025] ACM 멀티미디어 시스템 저널(Journal), 멀티미디어 보안에 대한 특집 "웨이블릿-패킷으로 인코딩된 이미지 데이터의 선택적 암호화"(2003)에서, A.포머(A. Pommer) 및 A. Uhl(A. Uhl)은 이미지의 웨이블릿 패킷 인코딩의 헤더 정보의 AES 암호화를 기초로 하는 알고리즘을 제안하였고, 이 헤더는 서브-밴드(sub-band) 트리 구조를 구체화한다.

[0026] 이미지 처리에 대한 IEEE 국제 회의(ICIP 2004), "JPEG2000 코드스트림의 준수(compliant) 암호화"(싱가폴, 2004년 10월)에서, Y. 우(Y.Wu) 및 R. H. 뎅(R. H. Deng)은 패킷에 코드블록 기여(CCPs)를 반복적으로 인코딩하는 JPEG 인가 암호화 알고리즘을 제안한다. 암호화 처리는 스트림 암호(cipher) 또는 블록 암호, 바람직하게는 산술 모듈 추가(arithmetic module addition)를 하는 스트림 암호를 사용하여 (패킷 데이터에서) CCP에 작용한다. 키 스트림은 리베스트(Rivest) 암호 4(RC4)를 사용하여 생성된다. 각 CCP는, 이 CCP가 금지 코드 워드(즉, 범위[0xFF90, 0xFFFF]에서의 임의의 코드 워드)를 가지지 않을 때까지, 반복적으로 암호화된다.

[0027] 통신 및 멀티미디어 보안, 편집자, A. 리오이(A. Lioy) 및 D. 마조치(D.Mazzocchi)의 "JPEG2000 비트 스트림의 선택적 암호화"에서, 통신 및 멀티미디어 보안(CMS '03)에 대한, IFIP TC6/TC11 제 6회 공동 실무 회의의 회보, 컴퓨터 과학에 대한 강의 노트의 볼륨(volume) 2828, 페이지(194 내지 204),(이탈리아, 튜린, 2003년 10월). 스프링어 벌래그(Springer Verlag), R. 노슨(R. Norcen) 및 A. 우홀은, JPEG2000이 인코딩된 비트스트림인지와, 진행 순서(progression order) JPEG2000으로 압축된 이미지에서, 가장 중요한 데이터가 비트스트림의 시작부에서 송신된다는 것을 진술한다. 이를 기초로, 제안된 기법은 선택된 패킷 데이터의 AES 암호화에 있다. 알고리즘은 패킷 데이터를 식별하기 위하여, 2가지 선택적 마커 SOP 및 EPH (도 4에 도시되는 바와 같이)를 사용한다. 그런 후에, 이 패킷 데이터는, 패킷 데이터가 가변적인 길이를 갖기에, CFB 모드로 AES를 사용하여 암호화된다. 상이한 진행 순서(해상도 및 계층 진행 순서)를 갖는 2 종류의 이미지(손실 및 무손실 압축된)에 대한 실험이 수행되었다. 평가 기준은 암호화된 데이터의 주어진 양에 대해 얻어진 시각적 손상이다. 손실 압축된 이미지에 대하여, 계층 진행이 더 나은 결과를 갖는다는 점이 발견되었다. 무손실 압축된 이미지에 대하여, 해상도 진행이 더 나은 결과를 갖는다.

[0028] 유럽 특허 출원 EP 08300093.5는 각 패킷이 하향 속도로 패킷을 배열하도록, 속도당 왜곡률을 사용하는 개선된 해결책을 제공하고, 사전 결정된, 누적 왜곡량에 도달할 때까지, 패킷을 암호화한다.

발명의 내용

해결하려는 과제

[0029] 하지만, 출원인은, 패킷 데이터를 암호화할 때 개선에 대한 여지가, 여전히 존재한다는 것을 발견했다.

[0030] 그러므로, 암호화된 콘텐츠의 보안을 용인할 수 없게 줄이는 것 없이, 암호화에 대한 추가의 향상을 허용하는 해결책에 대한 필요성이 존재한다고 인식될 수 있다. 본 발명은 이러한 해결책을 제공한다.

과제의 해결 수단

[0031] 제 1 양상에서, 본 발명은, 키 길이 k를 갖는 암호화 키 K를 사용하여, 균일하게 배포된 심볼 중 적어도 하나의 메세지(M)의 암호화 방법에 관한 것이다. k 비트의 길이를 갖는 적어도 하나의 메세지(M) 각각의 k 비트가 암호화되고; k 비트보다 긴 적어도 하나의 메세지(M) 각각의 메세지(M)의 전체 길이보다 작은 적어도 k 비트(at least k bits and less than the whole length of message M)가 암호화된다.

[0032] 바람직한 제 1 실시예에서, k 비트보다 작은 적어도 하나의 메세지(M)은 적어도 k 비트만큼 긴, 길이가 늘어난 메세지를 얻기 위하여 길이가 늘어난다. 길이가 늘어난 메세지가 k 비트만큼 긴 경우, 길이가 늘어난 메세지의 k비트는 암호화되고; 길이가 늘어난 메세지가 k 비트보다 긴 경우, 길이가 늘어난 메세지의 전체 길이보다 작은, 적어도 k비트는 암호화된다. 적어도 하나의 메세지(M)은 패딩(padding) 또는 적어도 하나의 추가 메세지와 접합(concatenation)을 통하여 길이가 늘어난다는 것은 장점이다.

[0033] 바람직한 제 2 실시예에서, k 비트보다 긴 메세지의 정확하게 k 비트는 암호화된다. 균일하게 배포된 심볼이 더 초래된다는 것은 장점이다.

[0034] 바람직한 제 3 실시예에서, 적어도 하나의 메세지(M)은 JPEG2000으로 인코딩된다.

[0035] 제 2 양상에서, 본 발명은, 키 길이 k를 갖는 암호화 키 K를 사용하여, 균일하게 배포된 심볼 중 적어도 하나의 메세지(M)의 암호화를 위한 장치에 관한 것이다. 장치는 k 비트의 길이를 갖는 적어도 하나의 메세지(M) 중 각 메세지의 k 비트를 암호화하기 위하여; 및 k 비트보다 큰 적어도 하나의 메세지(M) 중 각각의 메세지(M)의 전체 길이보다 작은 적어도 k 비트를 암호화하기 위하여, 적응되는 처리기를 포함한다.

[0036] 제 3 양상에서, 본 발명은, 키 길이 k를 갖는 복호화 키를 사용하여, 적어도 하나의 암호화된 메세지([M])의 복호화 방법에 관한 것이다. 복호화 디바이스는 k 비트의 길이를 갖는 적어도 하나의 암호화된 메세지([M])의 각 메세지의 k 비트를 복호화하고, k 비트보다 더 긴, 각 적어도 하나의 메세지(M) 중 각각의 메세지 (M)의 전체 길이보다 작은 k비트를 복호화한다.

[0037] 제 4 양상에서, 본 발명은 키 길이 k를 갖는 암호화 키 K를 사용하여, 적어도 하나의 암호화된 메세지([M])의 복호화를 위한 장치에 관한 것이다. 본 장치는 k 비트의 길이를 갖는, 각 적어도 하나의 메세지(M) 중 각각의 메세지(M)의 전체 길이보다 작은 적어도 k 비트를 복호화한다.

[0038] 본 발명의 바람직한 특징은, 첨부 도면을 참조하여 제한적이지 않은 예시로, 지금부터 서술될 것이다.

발명의 효과

[0039] 본 발명은 상술된 종래 기술의 암호화에 대한 문제점을 개선하고, 보다 향상된 암호화 기법을 제공하는 효과를 갖는다.

도면의 간단한 설명

[0040] 도 1은 콘텐츠 액세스 제어에 대한, 전형적인 종래 기술의 접근법을 도시하는 도면.

도 2는 종래 기술에 따른 선택적 암호화를 도시하는 도면.

도 3은 종래 기술의 JPEG2000 메인 코드 스트림 구조를 도시하는 도면.

도 4는 종래 기술의 예시적인 JPEG2000 패킷을 도시하는 도면.

도 5는 종래 기술에 따른, 이미지의 코딩으로부터 출력(emanate)하는JPEG2000 패킷을 도시하는 도면.

도 6은 본 발명의 실시예 아이디어를 사용하여 암호화된 메세지(M)을 개략적으로 도시하는 도면.

도 7은 본 발명의 바람직한 실시예에 따른 선택적 암호화를 위한 암호화 디바이스를 도시하는 도면.

도 8은 본 발명의 바람직한 실시예에 따른 선택적 암호화를 위한 방법을 도시하는 도면.

도 9는 본 발명의 바람직한 실시예에 따른 복호화 디바이스를 도시하는 도면.

발명을 실시하기 위한 구체적인 내용

[0041] 본 발명은, 본 발명의 놀라운 결과물에 도달하기 위하여, 시발점으로 JPEG2000의 고유적인 특성을 사용한다. JPEG2000에서, 패킷에 대한 코드블록 기여(CCP)가 초래된다. 게다가, 코드블록은 콘텍스트(context) 기반인 CABAC(콘텍스트-적응 산술 부호화: Context-Adaptive Binary Arithmetic Coding) 코더에 의해 인코딩된다. 즉, 암호법 보안을 보증하기 위하여, 전체 패킷보다 적은 패킷을 암호화하는 것을 가능하게 하는, 데이터의 시작부에 액세스 없이 CCP를 올바르게 디코딩하는 것은 불가능하다.

[0042] 도 5는 종래 기술에 따른 인코딩된 이미지에 대응하는 다수의 JPEG2000으로 인코딩된 패킷을 도시한다. 이 패킷은 특정 품질 계층(L)에 대응하는 패킷이 동일한 행에 있도록 정렬되었다.

[0043] 도 6은 n_e개의 바이트가 암호화될, n바이트를 갖는 메세지(M)을 도시한다. M은, 예를 들어, JPEG200의 경우에서, 초래될 수 있는 균일하게 배포된 심볼로 구성된다. 메세지(M)이 페이로드(payload)로 여겨질 수 있다는 것 즉, 메세지(M)이 임의의 헤더를 포함하지 않지만, 전체 메세지(M)은 수신기에 사용된다는 것이 언급되어야 한다. 메세지(M)으로부터 암호화를 위한 데이터의 양, 즉 n_e를 결정하기 위하여, 암호화율(ER)로 암호화되는 메세지(M)(CCP로 나타나는)을 고려하면:

[0044] $$ER = \frac{n_e}{n} = \frac{n_e}{|M|}$$

[0045] 여기에서 |M|은 메세지(M)의 비트의 개수이다.

[0046] 암호법 보안을 보증하는 최소 암호화율을 얻기 위하여, 미터법의 사용은 암호화된 메세지의 예측 불가능을 측정하기 위하여 사용된다.

[0047] 메인 아이디어는 공격자가 언어 심볼의 확률 분포에 대한 완벽한 지식을 갖는 경우, 최적화된 무차별 공격을 고려하는 것이다. X는 언어에서 X의 값을 취하는 이산 랜덤 변수이다.

[0048] $$L^{n_e}, X \in \{X_1, X_2 \cdots X_{|L^{n_e}|}\}$$

[0049] 공격자는 모든 가능한 값을, 이 값의 확률의 내림순으로 함으로써, 값의 추측을 시도할 수 있다

[0050] $$p_1 \geq p_2 \cdots \geq p_{|L^{n_e}|}$$

[0051] 이 식은 추측작업(W)을 제공하고:

[0052] $$W(X) = \sum_{i=1}^{|L^{n_e}|} i \cdot p_i$$

[0053] 여기에서 W(X)는, 공격자가 올바른 메세지 X를 찾기 이전에 시도해야 하는 예상된 추측의 횟수이다.

[0054] 코드블록 기여가 균일하게 배포된 데이터를 출력하는 산술 코딩을 사용하여 코딩된다는 것이 언급된다.

[0055] $$p_i = \frac{1}{|L^{n_e}|} = \frac{1}{|\sum|^{n_e}}$$

[0056] 여기에서 ∑는 코드블록 기여에 대한 알파벳이다. 이 식은 추측 작업을 제공한다:

[0057] $$W(X) = \frac{1}{|\sum|^{n_e}} \sum_{i=1}^{|\sum|^{n_e}} i = \frac{|\sum|^{n_e}+1}{2}$$

[0058] 한편으로, 공격자가 키 추측을 사용하는 경우, 올바른 키를 검색하기 위하여, 추측되어야 할(또는 시도되어야 할) 키 W(K)의 예상된 수가 제공되고, k-비트 키에 대하여,

[0059] $$W(K) = \sum_{i=1}^{2^k} \frac{i}{2^k} = \frac{2^k+1}{2}$$

[0060] 에 의해 제공된다.

[0061] 2개의 후자의 식으로부터, 메세지 공간에 대한 무차별 공격이 W(X)≥W(K) 경우의 키 추측보다 어렵다고 결론내릴 수 있고, 이는 또한,

[0062] $$|\sum|^{n_e} \geq 2^k$$

[0063] 로 표현될 수 있다.

[0064] 그러므로, 암호화된 부분의 크기는,

[0065] $$n_e \geq \frac{k}{\log_2(|\sum|)}$$

[0066] 에 의해 결정되는 더 낮은 범위(bound)를 갖는다.

[0067] JPEG2000 선택적 암호화 알고리즘의 예시적인 실시예에서, 전형적인 값은

[0068] · 잘 연구된 암호화 알고리즘 AES-128을 통해, k = 128

[0069] · |∑| = 256

[0070] 을 포함한다.

[0071] 이는,

[0072] $$n_e \geq 16$$

[0073] 을 제공한다.

[0074] 제공된 이러한 파라미터를 요약해보면, 암호화된 부분은, 적어도 암호화 키(128 비트 = 16 바이트)만큼 길고; 그렇지 않으면, 암호화 알고리즘은 무시될 수 있으며, 평문 공간상에서의 무차별 공격이 공격자에게 더 쉬워진다는 것이 권고된다. 따라서, 암호화 효율은, 암호화된 비트의 개수가 k내지 |M|-1인 경우, 암호화 보안을 유지하면서 증가된다.

[0075] 일반적인 JPEG2000의 경우에서, 본 발명에 따라, $Pack_e$에 속하고, p 코드 블록{m_1, m_2,...,m_p}로부터 기여를 내

포하는 패킷 데이터를 고려함으로써, 암호법 보안을 보증하기 위해, 각 코드블록 기여로부터 적어도 $\frac{k}{\log_2(|\sum|)}$ 바이트가 암호화 되어야 한다. 당업자라면 이러한 결과가 다른 적합한 인코딩 방법으로부터 초래되는 데이터에 일반화될 수 있다고 인식할 것이다.

[0076] 하지만, 암호화를 최적화하기 위하여, 정확히 이러한 바이트의 개수가 암호화되는 것이 바람직하다. 이러한 목적으로, 인코딩 처리 동안, 메타데이터(metadata)는 각 패킷에 대하여 각 코드블록 기여의 길이를 제공하는 $Pack_e$에 생성될 수 있다. 코드블록 기여가 $\frac{k}{\log_2(|\sum|)}$ 보다 작은 경우, 전체 코드블록 기여는 암호화된다. 이러한 접근법은 암호화 보안을 보증하는 타겟 응용 요구를 위한 가장 낮은 암호화율의 달성을 허용할 수 있다.

[0077] 예시적인 JPEG2000 실시예에서, 128비트(AES-128 이 사용될 시)를 암호화하는 것은, 위에서 언급한 바와 같이 충분하다.

[0078] L_e에서 오직 최상위층만이 암호화를 위해 선택되는 경우에, 최소 암호화 율이 달성된다. 그런 후에, 암호법으로의 보안 암호화를 위하여, 동일한 시각적 왜곡이 달성된다.

[0079] 도 7은 본 발명의 바람직한 실시예에 따른, 선택적 암호화를 위한 암호화 디바이스를 설명한다. 암호화 디바이스(710)는 적어도 하나의 처리기(아래에 "처리기")(720), 암호화할 적어도 하나의 메세지(M)의 수신에 대한 입력(730), 암호화된 메세지([M])의 출력을 위한 출력(740)을 포함한다.

[0080] 도 8을 더 참조해 보면, 처리기(720)는 암호화를 위하여 메세지(M)을 수신하는데 적응된다,{단계(810)}. 단계(820)에서, 처리기는, 메세지 길이|M|가 암호화 키 K의 길이 k보다 더 긴지, 또는 길이 k와 동일한지를 결정한다. 만일, 메세지 길이|M|이 암호화 키 K의 길이 k보다 길거나 같다면, 처리기(720)는 단계(830)에서, k 비트, 바람직하게는, 암호화 키 K를 사용하는 메세지(M)의 제 1 k비트를 암호화한다. 이와 반대로, 만일 메세지 길이|M|가 암호화 키 길이 k보다 작으면, 처리기(720)는 적어도 k비트만큼 긴 메세지를 얻기 위하여 추가의 메세지와 메세지(M)을 접합하고, 암호화 키 K를 사용하는 접합된 메세지의 k 비트를 암호화한다(840). 장점으로, 접합이 오직 암호화 목적에 대한 것이고, 이는 암호화되고, 접합된 메세지가 후에, 메세지 각각의 암호화된 메세지로 분리되는 것을 말하는 것으로 언급되어야 한다. 또한, 너무 작은 메세지(M)을 패딩함으로써, 패딩 된 메세지(M)이 k비트를 포함하는 것이 가능할 수 있다는 점이 언급되어야 한다. 이러한 경우에서, 수신기가 패딩을 제거할 수 있도록 패딩에 관한 정보를 추가하는 것이 필요할 수 있다.

[0081] JPEG2000에서, 최우선 품질 계층(L)으로부터 동일한 해상도(R), 성분(C), 영역(P)을 갖는 메세지로 필요한 경우, 메세지(M)을 접합하는 것은 바람직하다. 즉, $R_iC_iP_iL_i$에 대응하는 메세지는, 접합의 길이가 요구된 길이를 가질 때까지, $R_iC_iP_iL_{i+1}$(최상의 층인 L_0와) 등에 대응하는 메세지와 접합된다.

[0082] 대부분의 경우에서, 메세지 M이 패킷의 페이로드 부분이라고 인식된다. 또한, 메세지(M)이 패킷의 패이로드의 부분이라는 것도 당연히 가능할 것이다. 이들 경우에서, 헤더 부는 암호화되지 않는다.

[0083] 도 9는 본 발명의 바람직한 실시예에 따른 복호화 디바이스를 도시한다. 복호화 디바이스(910)는 적어도 하나의 처리기(아래에 "처리기")(920), 복호화를 위한 적어도 하나의 메세지([M])를 수신하기 위한 입력(930), 및 복호화된 메세지(M)을 출력하기 위한 출력(940)을 포함한다.

[0084] 도면에 도시되지 않더라도, 복호화 방법은 도 8에 도시된 암호화 방법을 반영한다. 처리기(920)는 복호화를 위하여 메세지[M]를 수신하는데 적응된다. 처리기(920)는 메세지 길이|M|가 복호화 키 K의 길이 k 보다 길거나 같은지를 결정한다. 만일 메세지 길이|M|가 복호화 키 K의 길이 k 보다 길거나 같다면, 처리기(920)는 적어도 복호화 키 K를 사용하는 메세지 [M]의 k비트 - 암호화 디바이스에 의해 암호화된 k 비트를 복호화한다. 이와 반대로, 메세지 길이|M|가 암호화 키 길이 k보다 작으면, 처리기(920)는 적어도 암호화 키만큼 긴 접합된 메세지를 얻기 위하여, 암호화된 메세지([M])를 접합하고, 복호화 키 K를 사용하여 접합된 메세지의 k 비트를 복호화한다. 패딩이 암호화 중에 사용되는 경우, k 비트보다 작은 메세지가 존재하지 않게 되어, 각 메세지는 복호화 키 K를 사용하여 복호화될 수 있고, 패딩은 필요한 경우, (아마도 전송기에 의해 제공된 정보를 사용하

여) 제거될 수 있다.

[0085] 복호화 디바이스가 임의의 접합된 메세지를 분리시키 것을 더욱 손쉽게 할 수 있기에, 메세지(M)이 패킷의 페이로드의 적어도 일부일 수 있다는 것은 장점이다.

[0086] 바람직한 실시예에서 인식되는 바와 같이, 키 K는 대칭 키, 즉 암호화 키고, 복호화 키도 동일하다. 하지만, 예를 들어, 타원 곡선을 기초로 하는, 비대칭 암호화 기법을 사용하는 것 또한 가능할 수 있다. 이러한 경우에서, 암호화할 메세지의 비트의 수를 결정하는 것은 복호화 키의 길이다.

[0087] 서술 및 (적합하다면) 청구항 및 도면에 개시된 각 특징은 개별적으로, 또는 임의의 적합한 조합으로 제공될 수 있다. 하드웨어에 구현되는 것으로, 서술된 특징은 또한 반대로, 소프트웨어에도 구현될 수 있다. 연결은 적합하다면, 무선 연결 또는 유선 연결로 구현될 수 있고, 반드시 직접 또는 전용 연결로 구현되는 것은 아니다.

[0088] 본 발명이 바람직한 실시예, JPEG2000에 제한되지 않지만, 압축된 픽처의 유사한, 층 아키텍처를 갖는 다른 시스템에서도 동일하게 사용될 수 있다는 점이 인식된다.

[0089] 청구항에 나타나는 참조 번호는 오직 설명의 목적이고, 청구항의 범주에 대한 제한적인 영향이 있어선 안된다.

부호의 설명

[0090] 710 : 암호화 유닛 720 : 처리기

810 : 암호화를 위하여 메세지(M)을 수신

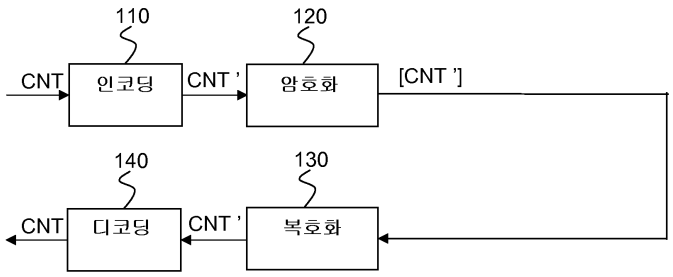
820 : |M| ≥ 키 길이 k 830 : M의 k비트를 암호화

840 : 추가 메세지와 M을 접합하여 접합의 k 비트를 암호화

910 : 복호화 유닛 920 : 처리기

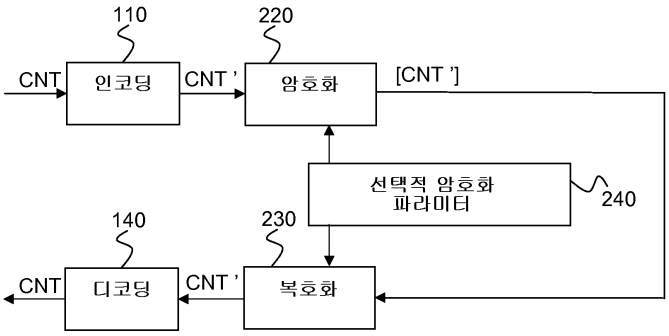
도면

도면1



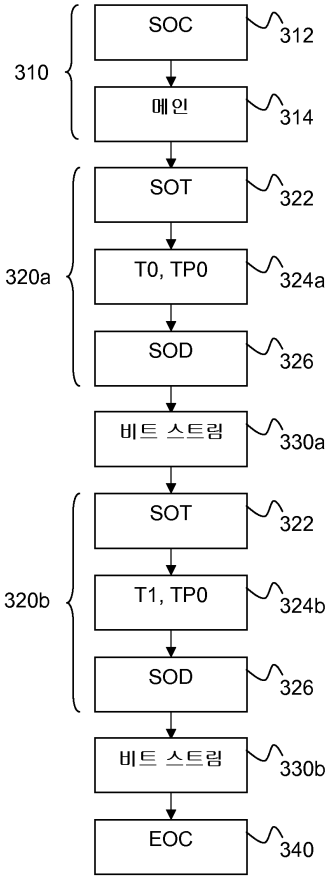
(종래 기술)

도면2



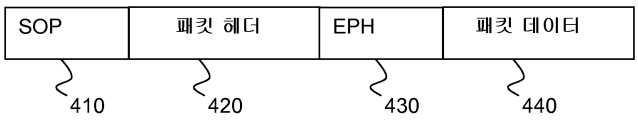
(종래 기술)

도면3



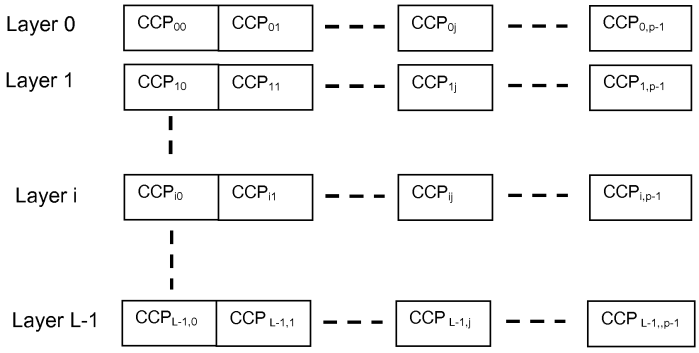
(종래 기술)

도면4



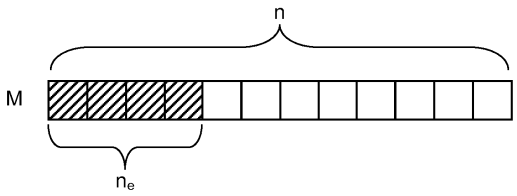
(종래 기술)

도면5

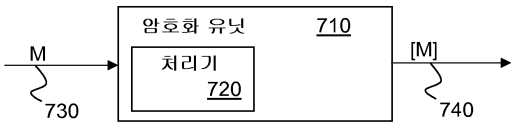


(종래 기술)

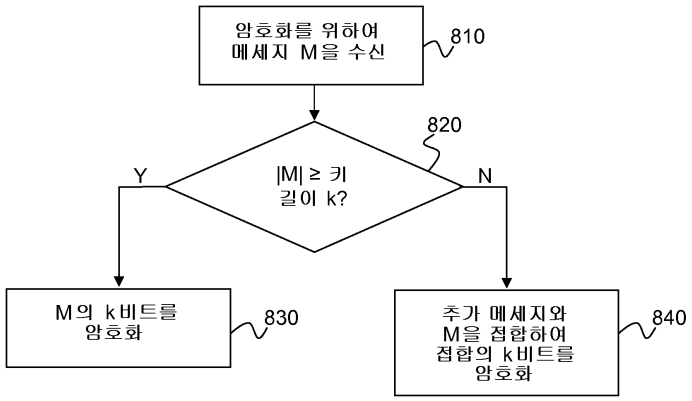
도면6



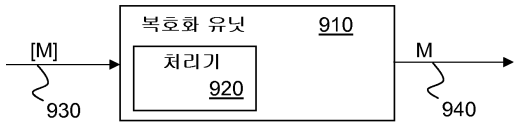
도면7



도면8


암호화를 위하여
메세지 M을 수신
810
820
|M| ≥ 키
길이 k?
Y
N
M의 k비트를
암호화
830
추가 메세지와
M을 접합하여
접합의 k비트를
암호화
840

도면9


복호화 유닛
910
[M]
처리기
920
M
930
940