



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2015년09월14일

(11) 등록번호 10-1553148

(24) 등록일자 2015년09월08일

(51) 국제특허분류(Int. Cl.)

H04L 9/18 (2006.01) H04L 9/28 (2006.01)

(21) 출원번호 10-2014-0026104

(22) 출원일자 2014년03월05일

심사청구일자 2014년03월05일

(56) 선행기술조사문헌

KR1020020005438 A

류동렬 외 2명, 비트 확장성을 갖는 모듈러 곱셈 알고리즘 및 모듈러 곱셈기 설계, 통신정보보호학회논문지 제10권 제3호, 2009.09.

(73) 특허권자

울산대학교 산학협력단

울산광역시 남구 대학로 93

(72) 발명자

김성환

울산광역시 울주군 범서읍 굴화1길 55, 103동 2202호 (굴화강변월드메르디앙)

(74) 대리인

김종선, 이형석

전체 청구항 수 : 총 22 항

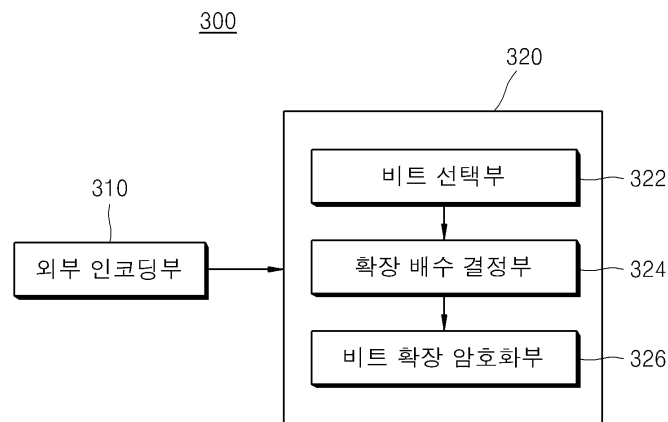
심사관 : 문형섭

(54) 발명의 명칭 비트 확장 방식을 이용한 암호화 장치 및 방법

(57) 요약

본 발명의 일 실시예에 따른 비트 확장 방식을 이용한 암호화 장치는 입력된 메시지의 이진 비트열로부터 각각의 비트 값을 선택하는 비트 선택부; 및 상기 선택된 비트 값 각각에 대해서, 복수의 난수(random number)를 이용하여 상기 비트 값 각각의 길이를 확장하여 확장 비트열을 생성하고, 상기 생성된 확장 비트열 각각을 조합하여 상기 메시지를 암호화하는 비트 확장 암호화부를 포함한다.

대표도 - 도3



명세서

청구범위

청구항 1

입력된 메시지의 이진 비트열로부터 각각의 비트 값을 선택하는 비트 선택부;

상기 비트 값 각각의 길이를 확장하기 위한 비트 확장 배수를 결정하는 확장 배수 결정부; 및

상기 선택된 비트 값 각각에 대해서, 복수의 난수(random number)를 이용하여 상기 비트 값 각각의 길이를 확장하여 확장 비트열을 생성하고, 상기 생성된 확장 비트열 각각을 조합하여 상기 메시지를 암호화하는 비트 확장 암호화부

를 포함하고,

상기 비트 확장 암호화부는

상기 결정된 비트 확장 배수를 기준으로, 상기 복수의 난수를 이용하여 상기 확장 비트열을 상기 비트 확장 배수에 대응하는 길이의 비트열로 생성하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 장치.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 비트 확장 암호화부는

상기 확장 비트열 중 제1 비트 영역을 상기 복수의 난수를 이용하여 생성하는 비트열 생성부;

상기 생성된 제1 비트 영역의 비트 값 각각을 논리 연산한 결과 값에 기초하여, 상기 확장 비트열 중 제2 비트 영역의 비트 값을 결정하는 비트 결정부; 및

상기 제1 및 제2 비트 영역을 포함하는 상기 확장 비트열을 각각 조합하는 비트열 조합부

를 포함하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 장치.

청구항 4

제3항에 있어서,

상기 비트 결정부는

상기 제1 비트 영역의 비트 값 각각에 대한 배타적 논리합 연산을 수행하고, 상기 배타적 논리합 연산의 수행 결과에 기초하여 상기 제2 비트 영역의 비트 값을 결정하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 장치.

청구항 5

제4항에 있어서,

상기 비트 결정부는

상기 배타적 논리합 연산을 수행한 결과 값을 연산자로 정의하고, 상기 연산자와 배타적 논리합 연산을 수행하

는 비트 값을 피연산자로 정의할 때, 상기 연산자와 논리 연산한 결과 값이 원래의 비트 값과 동일하도록 하는 피연산자의 비트 값을 상기 제2 비트 영역의 비트 값으로 결정하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 장치.

청구항 6

제3항 내지 제5항 중 어느 한 항에 있어서,

상기 제2 비트 영역은

상기 확장 비트열 내 임의의 위치에 배치되는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 장치.

청구항 7

제1항에 있어서,

상기 확장 배수 결정부는

메시지의 길이와 보안성을 고려하여 상기 비트 확장 배수를 결정하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 장치.

청구항 8

제7항에 있어서,

상기 확장 배수 결정부는

상기 암호화된 메시지를 전송할 전송 채널의 보안성에 따른 목표 정보 손실률을 결정하고, 상기 결정된 목표 정보 손실률에 기초하여 상기 비트 확장 배수를 결정하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 장치.

청구항 9

제7항에 있어서,

상기 확장 배수 결정부는

상기 암호화된 메시지를 전송할 전송 채널의 수를 고려하여 상기 비트 확장 배수를 결정하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 장치.

청구항 10

제7항에 있어서,

상기 확장 배수 결정부는

상기 암호화된 메시지를 전송할 전송 채널의 목표 전송량에 기초하여 상기 비트 확장 배수를 결정하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 장치.

청구항 11

제1항에 있어서,

선형 부호화 알고리즘을 이용하여 상기 입력된 메시지를 부호화하는 외부 인코딩부

를 더 포함하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 장치.

청구항 12

제11항에 있어서,

상기 선형 부호화 알고리즘은

해밍 부호화 알고리즘을 포함하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 장치.

청구항 13

암호화 장치의 비트 선택부에서, 입력된 메시지의 이진 비트열로부터 각각의 비트 값을 선택하는 단계;

상기 암호화 장치의 확장 배수 결정부에서, 상기 비트 값 각각의 길이를 확장하기 위한 비트 확장 배수를 결정하는 단계;

상기 암호화 장치의 비트 확장 암호화부에서, 상기 선택된 비트 값 각각에 대해서, 복수의 난수(random number)를 이용하여 상기 비트 값 각각의 길이를 확장하여 확장 비트열을 생성하는 단계; 및

상기 암호화 장치의 비트 확장 암호화부에서, 상기 생성된 확장 비트열 각각을 조합하여 상기 메시지를 암호화하는 단계

를 포함하고,

상기 확장 비트열을 생성하는 단계는

상기 결정된 비트 확장 배수를 기준으로, 상기 복수의 난수를 이용하여 상기 확장 비트열을 상기 비트 확장 배수에 대응하는 길이의 비트열로 생성하는 단계

를 포함하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 방법.

청구항 14

삭제

청구항 15

제13항에 있어서,

상기 확장 비트열을 생성하는 단계는

상기 비트 확장 암호화부의 비트열 생성부에서, 상기 확장 비트열 중 제1 비트 영역을 상기 복수의 난수를 이용하여 생성하는 단계; 및

상기 비트 확장 암호화부의 비트 결정부에서, 상기 생성된 제1 비트 영역의 비트 값 각각을 논리 연산한 결과 값에 기초하여, 상기 확장 비트열 중 제2 비트 영역의 비트 값을 결정하는 단계

를 포함하고,

상기 메시지를 암호화하는 단계는

상기 비트 확장 암호화부의 비트열 조합부에서, 상기 제1 및 제2 비트 영역을 포함하는 상기 확장 비트열을 각각 조합하여 상기 메시지를 암호화하는 단계

를 포함하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 방법.

청구항 16

제15항에 있어서,

상기 확장 비트열 중 제2 비트 영역의 비트 값을 결정하는 단계는

상기 제1 비트 영역의 비트 값 각각에 대한 배타적 논리합 연산을 수행하는 단계; 및

상기 배타적 논리합 연산의 수행 결과에 기초하여 상기 제2 비트 영역의 비트 값을 결정하는 단계를 포함하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 방법.

청구항 17

제16항에 있어서,

상기 배타적 논리합 연산을 수행한 결과 값을 연산자로 정의하고, 상기 연산자와 배타적 논리합 연산을 수행하는 비트 값을 피연산자로 정의할 때,

상기 배타적 논리합 연산의 수행 결과에 기초하여 상기 제2 비트 영역의 비트 값을 결정하는 단계는

상기 연산자와 논리 연산한 결과 값이 원래의 비트 값과 동일하도록 하는 피연산자의 비트 값을 상기 제2 비트 영역의 비트 값으로 결정하는 단계

를 포함하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 방법.

청구항 18

제15항 내지 제17항 중 어느 한 항에 있어서,

상기 제2 비트 영역은

상기 확장 비트열 내 임의의 위치에 배치되는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 방법.

청구항 19

제13항에 있어서,

상기 비트 확장 배수를 결정하는 단계는

메시지의 길이와 보안성을 고려하여 상기 비트 확장 배수를 결정하는 단계

를 포함하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 방법.

청구항 20

제19항에 있어서,

상기 비트 확장 배수를 결정하는 단계는

상기 암호화된 메시지를 전송할 전송 채널의 보안성에 따른 목표 정보 손실률을 결정하는 단계; 및

상기 결정된 목표 정보 손실률에 기초하여 상기 비트 확장 배수를 결정하는 단계

를 포함하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 방법.

청구항 21

제19항에 있어서,

상기 비트 확장 배수를 결정하는 단계는

상기 암호화된 메시지를 전송할 전송 채널의 수를 고려하여 상기 비트 확장 배수를 결정하는 단계를 포함하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 방법.

청구항 22

제19항에 있어서,

상기 비트 확장 배수를 결정하는 단계는

상기 암호화된 메시지를 전송할 전송 채널의 목표 전송량에 기초하여 상기 비트 확장 배수를 결정하는 단계를 포함하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 방법.

청구항 23

제13항에 있어서,

암호화 장치의 외부 인코딩부에서, 선형 부호화 알고리즘을 이용하여 상기 입력된 메시지를 부호화하는 단계를 더 포함하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 방법.

청구항 24

제23항에 있어서,

상기 선형 부호화 알고리즘은

해밍 부호화 알고리즘을 포함하는 것을 특징으로 하는 비트 확장 방식을 이용한 암호화 방법.

발명의 설명

기술 분야

[0001] 본 발명의 실시예들은 암호화 기술에 관한 것으로, 더욱 상세하게는 비트 확장 방식을 이용한 암호화 장치 및 방법에 관한 것이다.

배경 기술

[0002] 암호(cryptography)는 경제, 금융분야에서 널리 사용된 이래로, 동일성의 인증(Authentication), 암호화 키에 대한 관리(Key Management), 디지털 서명(Digital Signature) 및 신원 확인(Identity Verification) 등 광범위하게 사용되고 있다.

[0003] 암호화 기술은 메시지 전송의 안전을 보장하기 위하여 자주 사용된다. 상기 암호화 기술은 전송측(transmission side)에서 평문(plaintext)을 부호화(encrypt)하고, 수신측(receiving side)에서 암호문(ciphertext)을 해독(decrypt)하는 것을 포함한다.

[0004] 데이터 암호화 표준(Data Encryption Standard: DES)은 여러 나라들과 ANSI(American National Standards Institute)에서 표준으로 채용된 블록 단위 암호화 프로토콜이다. 이외에도 암호화 프로토콜에는 3-DES 및 AES(Advanced Encryption Standard) 등이 있다.

[0005] 암호 해독은 해독키의 관리 소홀, 비밀번호의 예측 가능성, 또는 통신망에서 키보드 입력에 대한 모니터링 등으로도 가능하다. 암호를 해독하는 기술로는 단순 암호문 공격(Ciphertext Only Attack), 평문 공격(Known Plaintext Attack), 선택 평문 공격(Chosen Plaintext Attack), 최적 선택 평문 공격(Adaptively Chosen

Plaintext Attack), 시간 공격(timing attack) 및 DPA(또는 '전력 분석'이라 함) 공격 등이 있다.

[0006] 관련 선행기술로는 한국 등록특허공보 제10-0571178호(발명의 명칭: 메시지의 암호화 및 복호화 방법, 등록일자: 2006년 04월 07일)가 있다.

발명의 내용

해결하려는 과제

[0007] 본 발명의 일 실시예는 암호화하고자 하는 메시지의 비트 길이를 확장하여 암호화함으로써 정보 전달 채널(주 전송 채널)의 보안성을 향상시킬 수 있으며, 이를 통해 도청 채널로의 정보 전달을 최소화하여 다양한 환경에서 목표된 정보 손실량을 보장할 수 있도록 하는 비트 확장 방식을 이용한 암호화 장치 및 방법을 제공한다.

[0008] 본 발명이 해결하고자 하는 과제는 이상에서 언급한 과제(들)로 제한되지 않으며, 언급되지 않은 또 다른 과제(들)은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0009] 본 발명의 일 실시예에 따른 비트 확장 방식을 이용한 암호화 장치는 입력된 메시지의 이전 비트열로부터 각각의 비트 값을 선택하는 비트 선택부; 및 상기 선택된 비트 값 각각에 대해서, 복수의 난수(random number)를 이용하여 상기 비트 값 각각의 길이를 확장하여 확장 비트열을 생성하고, 상기 생성된 확장 비트열 각각을 조합하여 상기 메시지를 암호화하는 비트 확장 암호화부를 포함한다.

[0010] 본 발명의 일 실시예에 따른 비트 확장 방식을 이용한 암호화 장치는 상기 비트 값 각각의 길이를 확장하기 위한 비트 확장 배수를 결정하는 확장 배수 결정부를 더 포함하고, 상기 비트 확장 암호화부는 상기 결정된 비트 확장 배수를 기준으로, 상기 복수의 난수를 이용하여 상기 확장 비트열을 상기 비트 확장 배수에 대응하는 길이의 비트열로 생성할 수 있다.

[0011] 상기 비트 확장 암호화부는 상기 확장 비트열 중 제1 비트 영역을 상기 복수의 난수를 이용하여 생성하는 비트열 생성부; 상기 생성된 제1 비트 영역의 비트 값 각각을 논리 연산한 결과 값에 기초하여, 상기 확장 비트열 중 제2 비트 영역의 비트 값을 결정하는 비트 결정부; 및 상기 제1 및 제2 비트 영역을 포함하는 상기 확장 비트열을 각각 조합하는 비트열 조합부를 포함할 수 있다.

[0012] 상기 비트 결정부는 상기 제1 비트 영역의 비트 값 각각에 대한 배타적 논리합 연산을 수행하고, 상기 배타적 논리합 연산의 수행 결과에 기초하여 상기 제2 비트 영역의 비트 값을 결정할 수 있다.

[0013] 상기 비트 결정부는 상기 배타적 논리합 연산을 수행한 결과 값을 연산자로 정의하고, 상기 연산자와 배타적 논리합 연산을 수행하는 비트 값을 피연산자로 정의할 때, 상기 연산자와 논리 연산한 결과 값이 원래의 비트 값과 동일하도록 하는 피연산자의 비트 값을 상기 제2 비트 영역의 비트 값으로 결정할 수 있다.

[0014] 상기 제2 비트 영역은 상기 확장 비트열 내 임의의 위치에 배치될 수 있다.

[0015] 상기 확장 배수 결정부는 메시지의 길이와 보안성을 고려하여 상기 비트 확장 배수를 결정할 수 있다.

[0016] 상기 확장 배수 결정부는 상기 암호화된 메시지를 전송할 전송 채널의 보안성에 따른 목표 정보 손실률을 결정하고, 상기 결정된 목표 정보 손실률에 기초하여 상기 비트 확장 배수를 결정할 수 있다.

[0017] 상기 확장 배수 결정부는 상기 암호화된 메시지를 전송할 전송 채널의 수를 고려하여 상기 비트 확장 배수를 결정할 수 있다.

[0018] 상기 확장 배수 결정부는 상기 암호화된 메시지를 전송할 전송 채널의 목표 전송량에 기초하여 상기 비트 확장 배수를 결정할 수 있다.

[0019] 본 발명의 일 실시예에 따른 비트 확장 방식을 이용한 암호화 장치는 선형 부호화 알고리즘을 이용하여 상기 입력된 메시지를 부호화하는 외부 인코딩부를 더 포함할 수 있다.

- [0020] 상기 선형 부호화 알고리즘은 해밍 부호화 알고리즘을 포함할 수 있다.
- [0021] 본 발명의 일 실시예에 따른 비트 확장 방식을 이용한 암호화 방법은 암호화 장치의 비트 선택부에서, 입력된 메시지의 이진 비트열로부터 각각의 비트 값을 선택하는 단계; 상기 암호화 장치의 비트 확장 암호화부에서, 상기 선택된 비트 값 각각에 대해서, 복수의 난수(random number)를 이용하여 상기 비트 값 각각의 길이를 확장하여 확장 비트열을 생성하는 단계; 및 상기 암호화 장치의 비트 확장 암호화부에서, 상기 생성된 확장 비트열 각각을 조합하여 상기 메시지를 암호화하는 단계를 포함한다.
- [0022] 본 발명의 일 실시예에 따른 비트 확장 방식을 이용한 암호화 방법은 상기 암호화 장치의 확장 배수 결정부에서, 상기 비트 값 각각의 길이를 확장하기 위한 비트 확장 배수를 결정하는 단계를 더 포함하고, 상기 확장 비트열을 생성하는 단계는 상기 결정된 비트 확장 배수를 기준으로, 상기 복수의 난수를 이용하여 상기 확장 비트열을 상기 비트 확장 배수에 대응하는 길이의 비트열로 생성하는 단계를 포함할 수 있다.
- [0023] 상기 확장 비트열을 생성하는 단계는 상기 비트 확장 암호화부의 비트열 생성부에서, 상기 확장 비트열 중 제1 비트 영역을 상기 복수의 난수를 이용하여 생성하는 단계; 및 상기 비트 확장 암호화부의 비트 결정부에서, 상기 생성된 제1 비트 영역의 비트 값 각각을 논리 연산한 결과 값에 기초하여, 상기 확장 비트열 중 제2 비트 영역의 비트 값을 결정하는 단계를 포함하고, 상기 메시지를 암호화하는 단계는 상기 비트 확장 암호화부의 비트열 조합부에서, 상기 제1 및 제2 비트 영역을 포함하는 상기 확장 비트열을 각각 조합하여 상기 메시지를 암호화하는 단계를 포함할 수 있다.
- [0024] 상기 확장 비트열 중 제2 비트 영역의 비트 값을 결정하는 단계는 상기 제1 비트 영역의 비트 값 각각에 대한 배타적 논리합 연산을 수행하는 단계; 및 상기 배타적 논리합 연산의 수행 결과에 기초하여 상기 제2 비트 영역의 비트 값을 결정하는 단계를 포함할 수 있다.
- [0025] 상기 배타적 논리합 연산을 수행한 결과 값을 연산자로 정의하고, 상기 연산자와 배타적 논리합 연산을 수행하는 비트 값을 피연산자로 정의할 때, 상기 배타적 논리합 연산의 수행 결과에 기초하여 상기 제2 비트 영역의 비트 값을 결정하는 단계는 상기 연산자와 논리 연산한 결과 값이 원래의 비트 값과 동일하도록 하는 피연산자의 비트 값을 상기 제2 비트 영역의 비트 값으로 결정하는 단계를 포함할 수 있다.
- [0026] 상기 제2 비트 영역은 상기 확장 비트열 내 임의(random)의 위치에 배치될 수 있다.
- [0027] 상기 비트 확장 배수를 결정하는 단계는 메시지의 길이와 보안성을 고려하여 상기 비트 확장 배수를 결정하는 단계를 포함할 수 있다.
- [0028] 상기 비트 확장 배수를 결정하는 단계는 상기 암호화된 메시지를 전송할 전송 채널의 보안성에 따른 목표 정보 손실률을 결정하는 단계; 및 상기 결정된 목표 정보 손실률에 기초하여 상기 비트 확장 배수를 결정하는 단계를 포함할 수 있다.
- [0029] 상기 비트 확장 배수를 결정하는 단계는 상기 암호화된 메시지를 전송할 전송 채널의 수를 고려하여 상기 비트 확장 배수를 결정하는 단계를 포함할 수 있다.
- [0030] 상기 비트 확장 배수를 결정하는 단계는 상기 암호화된 메시지를 전송할 전송 채널의 목표 전송량에 기초하여 상기 비트 확장 배수를 결정하는 단계를 포함할 수 있다.
- [0031] 본 발명의 일 실시예에 따른 비트 확장 방식을 이용한 암호화 방법은 암호화 장치의 외부 인코딩부에서, 선형 부호화 알고리즘을 이용하여 상기 입력된 메시지를 부호화하는 단계를 더 포함할 수 있다.
- [0032] 상기 선형 부호화 알고리즘은 해밍 부호화 알고리즘을 포함할 수 있다.
- [0033] 기타 실시예들의 구체적인 사항들은 상세한 설명 및 첨부 도면들에 포함되어 있다.

발명의 효과

- [0034] 본 발명의 일 실시예에 따르면, 암호화하고자 하는 메시지의 비트 값의 길이를 확장하여 암호화함으로써 정보 전달 채널(주 전송 채널)의 보안성을 향상시킬 수 있으며, 이를 통해 도청 채널로의 정보 전달을 최소화하여 다양한 환경에서 목표된 정보 손실량을 보장할 수 있다.

[0035] 본 발명의 일 실시예에 따르면, 비트 길이의 확장 시 메시지의 길이와 보안성을 고려하여 비트 확장 배수를 결정함으로써, 정보 전달 채널로의 전송에 최적으로 확장된 길이의 비트로 메시지를 암호화할 수 있으며, 이를 통해 정보 전달 채널로 전송되는 메시지에 대한 보안성을 보다 향상시킬 수 있다.

[0036] 본 발명의 일 실시예에 따르면, 복수의 난수, 및 난수들과의 논리 연산을 통해 결정된 비트 값을 이용하여 비트 길이를 확장시킴으로써, 보안에 강하면서도 한정된 자원과 시간에서 효율적인 암호 및 복원이 가능하도록 할 수 있다.

도면의 간단한 설명

[0037] 도 1은 본 발명의 일 실시예에 따른 비트 확장 방식을 이용한 암호화 장치를 설명하기 위해 도시한 블록도이다.
 도 2는 도 2의 비트 확장 암호화부의 상세 구성을 설명하기 위해 도시한 블록도이다.
 도 3은 본 발명의 다른 실시예에 따른 비트 확장 방식을 이용한 암호화 장치를 설명하기 위해 도시한 블록도이다.
 도 4 내지 도 6은 본 발명의 일 실시예에 따른 비트 확장 방식을 이용한 암호화 방법을 설명하기 위해 도시한 흐름도이다.
 도 7은 본 발명의 다른 실시예에 따른 비트 확장 방식을 이용한 암호화 방법을 설명하기 위해 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0038] 본 발명의 이점 및/또는 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나, 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 것이며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하며, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성요소를 지칭한다.

[0039] 이하에서는 첨부된 도면을 참조하여 본 발명의 실시예들을 상세히 설명하기로 한다.

[0040] 도 1은 본 발명의 일 실시예에 따른 비트 확장 방식을 이용한 암호화 장치를 설명하기 위해 도시한 블록도이다.

[0041] 도 1을 참조하면, 본 발명의 일 실시예에 따른 비트 확장 방식을 이용한 암호화 장치(100)는 비트 선택부(110), 확장 배수 결정부(120), 및 비트 확장 암호화부(130)를 포함할 수 있다.

[0042] 상기 비트 선택부(110)는 입력된 메시지의 이진 비트열로부터 각각의 비트 값을 선택한다. 이를 위해, 상기 비트 선택부(110)는 상기 입력된 메시지를 분석하여 이진 비트열을 추출하고, 상기 추출된 이진 비트열로부터 순차적으로 각각의 비트 값을 선택할 수 있다.

[0043] 예를 들어, 상기 비트 선택부(110)는 상기 입력된 메시지를 분석한 결과로서 이진 비트열 '1100'을 추출할 수 있으며, 상기 추출된 이진 비트열 '1100'으로부터 비트 값 '1', '1', '0', '0'을 각각 순차적으로 선택할 수 있다.

[0044] 상기 확장 배수 결정부(120)는 상기 비트 값 각각의 길이를 확장하기 위한 비트 확장 배수를 결정한다. 여기서, 상기 비트 확장 배수는 상기 비트 값 각각의 길이를 확장하기 위한 배수 값으로서, 상기 비트 확장 배수가 ℓ (2 이상의 자연수)일 경우, 상기 비트 값 각각은 ℓ 비트의 길이로 확장될 수 있다.

[0045] 예를 들어, 상기 입력된 메시지의 이진 비트열이 위의 예에서와 같이 '1100'인 것으로 가정한다. 이러한 경우, 상기 비트 확장 배수를 3이라 가정하면, '1', '1', '0', '0'의 비트 값 각각의 길이는 '001', '111', '110', '101'과 같이 확장될 수 있다.

[0046] 참고로, 상기 비트 확장 배수는 그 값이 클수록 정보량이 늘어나고 보안성이 향상되는 반면에, 그 값이 작을수록 정보량이 줄어들고 보안성이 떨어지기 때문에 정보량과 보안성을 모두 고려하여 결정되는 것이 바람직하다.

즉, 상기 확장 배수 결정부(120)는 메시지의 길이와 보안성을 고려하여 상기 비트 확장 배수를 결정할 수 있다.

[0047] 예를 들어, 상기 확장 배수 결정부(120)는 암호화된 메시지를 전송할 전송 채널의 보안성에 따른 목표 정보 손실률을 결정하고, 상기 결정된 목표 정보 손실률에 기초하여 상기 비트 확장 배수를 결정할 수 있다. 또한, 상기 확장 배수 결정부(120)는 상기 암호화된 메시지를 전송할 전송 채널의 수를 고려하여 상기 비트 확장 배수를 결정할 수 있다. 또한, 상기 확장 배수 결정부(120)는 상기 암호화된 메시지를 전송할 전송 채널의 목표 전송량에 기초하여 상기 비트 확장 배수를 결정할 수 있다.

[0048] 상기 비트 확장 암호화부(130)는 상기 선택된 비트 값 각각에 대해서, 복수의 난수(random number)를 이용하여 상기 비트 값 각각의 길이를 확장하여 확장 비트열을 생성한다. 여기서, 상기 난수는 0 또는 1 중에서 무작위로 선택된 값을 가리킬 수 있다.

[0049] 즉, 상기 비트 확장 암호화부(130)는 상기 확장 배수 결정부(120)에 의해 결정된 비트 확장 배수 l 을 기준으로, 상기 복수의 난수를 이용하여 상기 확장 비트열을 상기 비트 확장 배수에 대응하는 길이의 비트열로 생성할 수 있다.

[0050] 상기 비트 확장 암호화부(130)는 상기 생성된 확장 비트열 각각을 조합하여 상기 메시지를 암호화할 수 있다.

[0051] 예를 들어, 상기 입력된 메시지의 이진 비트열이 위와 같이 '1100'이고 비트 확장 배수가 3이라고 가정한다. 이러한 경우, 상기 비트 확장 암호화부(130)는 각각의 비트 값 '1', '1', '0', '0'에 대한 확장 비트열을 각각 '111', '010', '101', '110'와 같이 생성하고, 상기 생성된 확장 비트열 각각을 조합하여 '111010101110'와 같은 이진 비트열을 출력함으로써 상기 메시지를 암호화할 수 있다.

[0052] 이를 위해, 상기 비트 확장 암호화부(130)는 비트열 생성부(210), 비트 결정부(220) 및 비트열 조합부(230)를 포함할 수 있다. 참고로, 도 2는 도 2의 비트 확장 암호화부(130)의 상세 구성을 설명하기 위해 도시한 블록도이다.

[0053] 상기 비트열 생성부(210)는 상기 확장 비트열 중 제1 비트 영역을 상기 복수의 난수를 이용하여 생성할 수 있다. 위의 예와 같이 상기 비트 확장 배수가 3인 경우, 상기 제1 비트 영역은 첫 번째 비트와 두 번째 비트를 포함하는 영역으로 정의될 수 있다.

[0054] 상기 비트 결정부(220)는 상기 생성된 제1 비트 영역의 비트 값 각각을 논리 연산한 결과 값에 기초하여, 상기 확장 비트열 중 제2 비트 영역의 비트 값을 결정할 수 있다.

[0055] 즉, 상기 비트 결정부(220)는 상기 제1 비트 영역의 비트 값 각각에 대한 배타적 논리합 연산을 수행하고, 상기 배타적 논리합 연산의 수행 결과에 기초하여 상기 제2 비트 영역의 비트 값을 결정할 수 있다.

[0056] 더욱 구체적으로 설명하면, 상기 비트 결정부(220)는 상기 배타적 논리합 연산을 수행한 결과 값을 연산자로 정의하고, 상기 연산자와 배타적 논리합 연산을 수행하는 비트 값을 피연산자로 정의할 때, 상기 연산자와 논리 연산한 결과 값이 원래의 비트 값과 동일하도록 하는 피연산자의 비트 값을 상기 제2 비트 영역의 비트 값으로 결정할 수 있다.

[0057] 여기서, 상기 제2 비트 영역은 상기 확장 비트열 내 임의(random)의 위치에 배치될 수 있다. 즉, 상기 제2 비트 영역은 상기 확장 비트열의 앞이나 중간, 뒷부분 등과 같이 임의의 위치에 배치될 수 있다. 이를 위해, 상기 비트 결정부(220)는 난수표 등을 이용하여 상기 확장 비트열 내에서 상기 제2 비트 영역이 위치할 임의의 영역을 결정할 수 있다.

[0058] 아래의 예는 상기 제2 비트 영역이 상기 확장 비트열의 마지막에 위치한다는 가정하에 설명하고 있으나, 이에 한정되지 않고 앞서 설명한 바와 같이 다른 위치에 위치할 수도 있음은 물론이다. 이처럼 상기 제2 비트 영역이 상기 확장 비트열 내 임의의 위치에 배치됨으로써 보안성이 높아질 수 있다.

[0059] 예컨대, 상기 입력된 메시지의 이진 비트열이 위와 같이 '1100'이고 비트 확장 배수가 3이라고 가정한다. 이러한 경우, 상기 비트열 생성부(210)에 의해 상기 비트 값 각각에 대한 확장 비트열 중 첫 번째 비트와 두 번째 비트, 즉 제1 비트 영역이 '11', '01', '10', '11'과 같이 생성될 수 있다. 이에 따라, 상기 비트 결정부(220)는 상기 확장 비트열의 제2 비트 영역, 즉 마지막 비트 하나를 결정하게 되는데, 이때 상기 제1 비트 영역의 첫 번째 비트와 두 번째 비트의 배타적 논리합 연산(XOR)을 수행한 결과 값에 기초하여 '11', '01', '10', '11' 각각에 대해 '1', '0', '1', '0'을 마지막 비트로 결정할 수 있다.

[0060] 다시 말해, 상기 비트 결정부(220)는 상기 배타적 논리합 연산을 수행한 결과 값과 배타적 논리합 연산을 수행

하여 원래의 비트 값이 나오도록 하는 비트 값을 상기 확장 비트열의 제2 비트 영역의 비트 값으로 결정할 수 있다. 이로써, 상기 입력된 메시지의 이진 비트열로부터 선택된 각각의 비트 값 '1', '1', '0', '0'에 대한 확장 비트열은 '111', '010', '101', '110'으로 생성될 수 있다.

- [0061] 상기 비트열 조합부(230)는 상기 제1 비트 영역 및 상기 제2 비트 영역을 포함하는 확장 비트열을 각각 조합할 수 있다.
- [0062] 예를 들어, 상기 비트열 조합부(230)는 상기 생성된 각각의 확장 비트열 '111', '010', '101', '110' 각각을 조합할 수 있으며, 이에 따라 '111010101110'와 같은 이진 비트열을 출력함으로써 상기 메시지를 암호화할 수 있다.
- [0063] 도 3은 본 발명의 다른 실시예에 따른 비트 확장 방식을 이용한 암호화 장치를 설명하기 위해 도시한 블록도이다.
- [0064] 도 3을 참조하면, 본 발명의 다른 실시예에 따른 비트 확장 방식을 이용한 암호화 장치(300)는 외부 인코딩부(310), 및 내부 인코딩부(320)를 포함할 수 있다.
- [0065] 상기 외부 인코딩부(310)는 메시지를 입력받아 선행 부호화 알고리즘을 이용하여 부호화하는 역할을 한다. 여기서, 상기 선행 부호화 알고리즘은 해밍 부호화 알고리즘을 포함할 수 있다.
- [0066] 상기 내부 인코딩부(320)는 상기 외부 인코딩부(310)에 의해 부호화된 메시지를 입력받아 암호화를 수행하는 역할을 한다. 이를 위해, 상기 내부 인코딩부(320)는 비트 선택부(322), 확장 배수 결정부(324) 및 비트 확장 암호화부(326)를 포함할 수 있다.
- [0067] 상기 비트 선택부(322)는 상기 외부 인코딩부(310)에 의해 부호화된 메시지의 이진 비트열로부터 각각의 비트 값을 선택한다. 이를 위해, 상기 비트 선택부(322)는 상기 부호화된 메시지를 분석하여 이진 비트열을 추출하고, 상기 추출된 이진 비트열로부터 순차적으로 각각의 비트 값을 선택할 수 있다.
- [0068] 상기 확장 배수 결정부(324)는 상기 비트 값 각각의 길이를 확장하기 위한 비트 확장 배수를 결정한다. 여기서, 상기 비트 확장 배수는 앞서 설명한 바와 같이 상기 비트 값 각각의 길이를 확장하기 위한 배수 값으로서, 상기 비트 확장 배수가 ℓ (2 이상의 자연수)일 경우, 상기 비트 값 각각은 ℓ 비트의 길이로 확장될 수 있다.
- [0069] 이때, 상기 확장 배수 결정부(324)는 메시지의 길이와 보안성을 고려하여 상기 비트 확장 배수를 결정할 수 있다.
- [0070] 예컨대, 상기 확장 배수 결정부(324)는 암호화된 메시지를 전송할 전송 채널의 보안성에 따른 목표 정보 손실률을 결정하고, 상기 결정된 목표 정보 손실률에 기초하여 상기 비트 확장 배수를 결정할 수 있다. 또한, 상기 확장 배수 결정부(324)는 상기 암호화된 메시지를 전송할 전송 채널의 수를 고려하여 상기 비트 확장 배수를 결정할 수 있다. 또한, 상기 확장 배수 결정부(324)는 상기 암호화된 메시지를 전송할 전송 채널의 목표 전송량에 기초하여 상기 비트 확장 배수를 결정할 수 있다.
- [0071] 상기 비트 확장 암호화부(326)는 상기 선택된 비트 값 각각에 대해서, 복수의 난수(random number)를 이용하여 상기 비트 값 각각의 길이를 확장하여 확장 비트열을 생성한다.
- [0072] 즉, 상기 비트 확장 암호화부(326)는 상기 확장 배수 결정부(324)에 의해 결정된 비트 확장 배수 ℓ 을 기준으로, 상기 복수의 난수를 이용하여 상기 확장 비트열을 상기 비트 확장 배수에 대응하는 길이의 비트열로 생성할 수 있다.
- [0073] 상기 비트 확장 암호화부(326)는 상기 생성된 확장 비트열 각각을 조합하여 상기 메시지를 암호화할 수 있다.
- [0074] 도 4 내지 도 6은 본 발명의 일 실시예에 따른 비트 확장 방식을 이용한 암호화 방법을 설명하기 위해 도시한 흐름도이다.
- [0075] 먼저 도 1 및 도 4를 참조하면, 단계(410)에서 상기 암호화 장치(100)의 비트 선택부(110)는 입력된 메시지의 이진 비트열로부터 각각의 비트 값을 선택한다.

- [0076] 다음으로, 단계(420)에서 상기 암호화 장치(100)의 확장 배수 결정부(120)는 상기 비트 값 각각의 길이를 확장하기 위한 비트 확장 배수를 결정한다.
- [0077] 다음으로, 단계(430)에서 상기 암호화 장치(100)의 비트 확장 암호화부(130)는 상기 결정된 비트 확장 배수를 기준으로, 상기 복수의 난수를 이용하여 상기 비트 값 각각의 길이를 확장하여 확장 비트열을 생성한다.
- [0078] 즉, 상기 암호화 장치(110)의 비트 확장 암호화부(130)는 상기 복수의 난수를 이용하여 상기 확장 비트열을 상기 비트 확장 배수에 대응하는 길이의 비트열로 생성할 수 있다.
- [0079] 상기 단계(430)에 대해 도 5를 참조하여 상세히 설명하면 다음과 같다.
- [0080] 즉, 도 2 및 도 5를 참조하면, 단계(510)에서 상기 비트 확장 암호화부(130)의 비트열 생성부(210)는 상기 확장 비트열 중 제1 비트 영역을 상기 복수의 난수를 이용하여 생성한다.
- [0081] 이후, 단계(520)에서 상기 비트 확장 암호화부(130)의 비트 결정부(220)는 상기 생성된 제1 비트 영역의 비트 값 각각을 논리 연산한 결과 값에 기초하여, 상기 확장 비트열 중 제2 비트 영역의 비트 값을 결정한다.
- [0082] 상기 단계(520)에 대해 도 6을 참조하여 상세히 설명하면 다음과 같다.
- [0083] 즉, 도 2 및 도 6을 참조하면, 단계(610)에서 상기 비트 확장 암호화부(130)의 비트 결정부(220)는 상기 제1 비트 영역의 비트 값 각각에 대한 배타적 논리합 연산을 수행한다.
- [0084] 이어서, 단계(620)에서 상기 비트 확장 암호화부(130)의 비트 결정부(220)는 상기 배타적 논리합 연산의 수행 결과에 기초하여 상기 제2 비트 영역의 비트 값을 결정한다.
- [0085] 다시 말해서, 상기 배타적 논리합 연산을 수행한 결과 값을 연산자로 정의하고, 상기 연산자와 배타적 논리합 연산을 수행하는 비트 값을 피연산자로 정의할 때, 상기 비트 확장 암호화부(130)의 비트 결정부(220)는 상기 연산자와 논리 연산한 결과 값이 원래의 비트 값과 동일하도록 하는 피연산자의 비트 값을 상기 제2 비트 영역의 비트 값으로 결정할 수 있다.
- [0086] 여기서, 상기 제2 비트 영역은 상기 확장 비트열 내 임의의 위치에 배치될 수 있다. 예를 들어 상기 제2 비트 영역은 상기 확장 비트열 중 마지막 비트 하나를 포함하는 영역일 수 있다. 즉, 상기 확장 비트열이 '110'이라 가정하면, 복수의 난수를 이용하여 생성되는 상기 제1 비트 영역은 '11'이고, 상기 제1 비트 영역의 배타적 논리합 연산 수행 결과에 기초하여 결정되는 상기 제2 비트 영역은 '0'이라 할 수 있다.
- [0087] 다시 도 1 및 도 4를 참조하면, 단계(440)에서 상기 암호화 장치(100)의 비트 확장 암호화부(130)는 상기 생성된 확장 비트열 각각을 조합하여 상기 메시지를 암호화한다.
- [0088] 도 7은 본 발명의 다른 실시예에 따른 비트 확장 방식을 이용한 암호화 방법을 설명하기 위해 도시한 흐름도이다.
- [0089] 도 3 및 도 7을 참조하면, 단계(710)에서 상기 암호화 장치(300)의 외부 인코딩부(310)는 선형 부호화 알고리즘을 이용하여 입력된 메시지를 부호화 한다. 여기서, 상기 선형 부호화 알고리즘은 해밍 부호화 알고리즘을 포함할 수 있다.
- [0090] 다음으로, 상기 암호화 장치(300)의 내부 인코딩부(320)는 상기 외부 인코딩부(310)에 의해 부호화된 메시지를 입력받아 암호화를 수행한다.
- [0091] 즉, 먼저 단계(720)에서 상기 내부 인코딩부(320)의 비트 선택부(322)는 상기 부호화된 메시지의 이진 비트열로부터 각각의 비트 값을 선택한다.
- [0092] 이를 위해, 상기 내부 인코딩부(320)의 비트 선택부(322)는 상기 부호화된 메시지를 분석하여 이진 비트열을 추출하고, 상기 추출된 이진 비트열로부터 순차적으로 각각의 비트 값을 선택할 수 있다.
- [0093] 이후, 단계(730)에서 상기 내부 인코딩부(320)의 확장 배수 결정부(324)는 상기 비트 값 각각의 길이를 확장하기 위한 비트 확장 배수를 결정한다.
- [0094] 여기서, 상기 비트 확장 배수는 상기 비트 값 각각의 길이를 확장하기 위한 배수 값으로서, 상기 비트 확장 배수가 ℓ (2 이상의 자연수)일 경우, 상기 비트 값 각각은 ℓ 비트의 길이로 확장될 수 있다.

- [0095] 이후, 단계(740)에서 상기 내부 인코딩부(320)의 비트 확장 암호화부(326)는 상기 결정된 비트 확장 배수를 기준으로, 복수의 난수를 이용하여 상기 비트 값 각각의 길이를 확장하여 상기 확장 비트열을 생성한다.
- [0096] 여기서, 상기 확장 비트열은 상기 비트 확장 배수에 대응하는 길이의 비트열로 생성될 수 있다.
- [0097] 이후, 단계(750)에서 상기 내부 인코딩부(320)의 비트 확장 암호화부(326)는 상기 생성된 확장 비트열 각각을 조합하여 상기 메시지를 암호화한다.
- [0098] 이와 같이, 본 발명의 일 실시예에서는 암호화하고자 하는 메시지의 비트 값의 길이를 확장하여 암호화함으로써 정보 전달 채널(주 전송 채널)의 보안성을 향상시킬 수 있으며, 이를 통해 도청 채널로의 정보 전달을 최소화하여 다양한 환경에서 목표된 정보 손실량을 보장할 수 있다.
- [0099] 또한, 본 발명의 일 실시예에서는 비트 길이의 확장 시 메시지의 길이와 보안성을 고려하여 비트 확장 배수를 결정함으로써, 정보 전달 채널로의 전송에 최적으로 확장된 길이의 비트로 메시지를 암호화할 수 있으며, 이를 통해 정보 전달 채널로 전송되는 메시지에 대한 보안성을 보다 향상시킬 수 있다.
- [0100] 또한, 본 발명의 일 실시예에서는 복수의 난수, 및 난수들과의 논리 연산을 통해 결정된 비트 값을 이용하여 비트 길이를 확장시킴으로써, 보안에 강하면서도 한정된 자원과 시간에서 효율적인 암호 및 복원이 가능하도록 할 수 있다.
- [0101] 본 발명의 실시예들은 다양한 컴퓨터로 구현되는 동작을 수행하기 위한 프로그램 명령을 포함하는 컴퓨터 판독 가능 매체를 포함한다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광기록 매체, 플롭티컬 디스크와 같은 자기-광 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.
- [0102] 지금까지 본 발명에 따른 구체적인 실시예에 관하여 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서는 여러 가지 변형이 가능함은 물론이다. 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허 청구의 범위뿐만 아니라 이 특허 청구의 범위와 균등한 것들에 의해 정해져야 한다.
- [0103] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 이는 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명 사상은 아래에 기재된 특허청구범위에 의해서만 파악되어야 하고, 이의 균등 또는 등가적 변형 모두는 본 발명 사상의 범주에 속한다고 할 것이다.

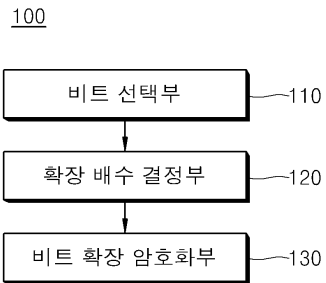
부호의 설명

- [0104] 110, 322: 비트 선택부
- 120, 324: 확장 배수 결정부
- 130, 326: 비트 확장 암호화부
- 210: 비트열 생성부
- 220: 비트 결정부
- 230: 비트열 조합부
- 310: 외부 인코딩부

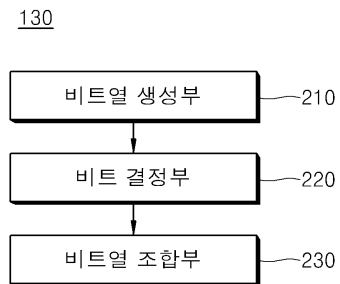
320: 내부 인코딩부

도면

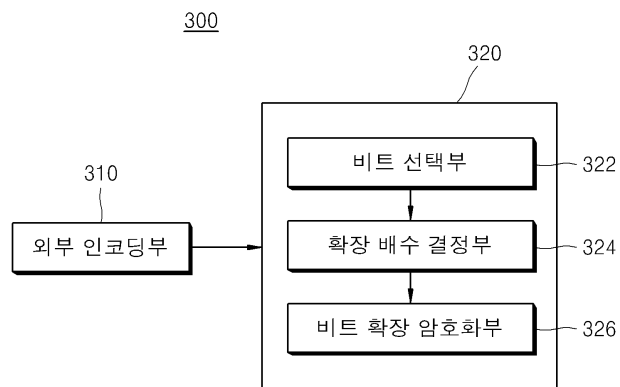
도면1



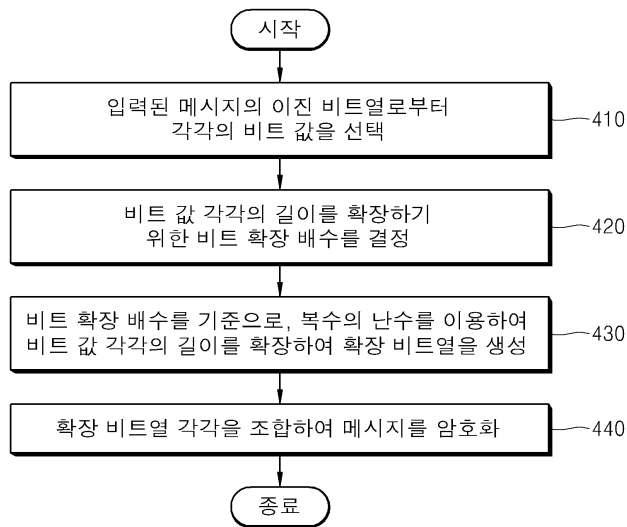
도면2



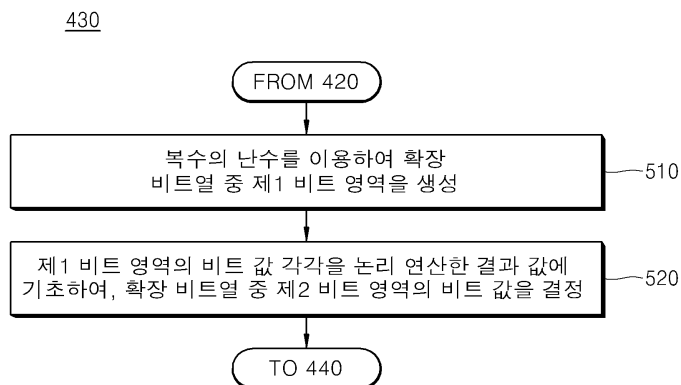
도면3



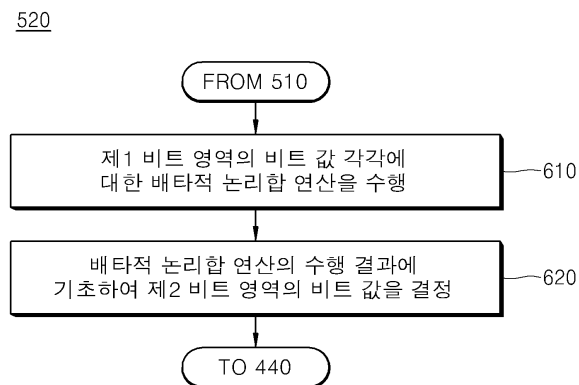
도면4



도면5



도면6



도면7

