



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0085176
(43) 공개일자 2021년07월08일

- | | |
|--|---|
| <p>(51) 국제특허분류(Int. Cl.)
 <i>G06F 17/16</i> (2006.01) <i>G06F 11/10</i> (2006.01)
 <i>G06F 17/15</i> (2006.01) <i>H03M 13/15</i> (2015.01)
 <i>H04L 9/12</i> (2006.01)</p> <p>(52) CPC특허분류
 <i>G06F 17/16</i> (2013.01)
 <i>G06F 11/1004</i> (2013.01)</p> <p>(21) 출원번호 10-2019-0177948
 (22) 출원일자 2019년12월30일
 심사청구일자 2019년12월30일</p> | <p>(71) 출원인
 조선대학교산학협력단
 광주광역시 동구 필문대로 309 (서석동)</p> <p>(72) 발명자
 김영식
 광주광역시 서구 풍암2로 66 금호2차아파트 201동 1005호</p> <p>(74) 대리인
 김효성</p> |
|--|---|

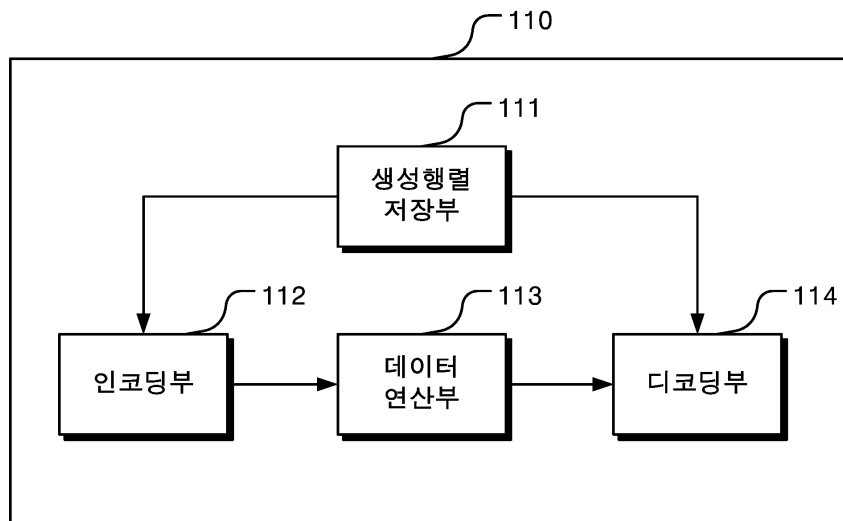
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치 및 그 동작 방법

(57) 요약

부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치 및 그 동작 방법이 개시된다. 본 발명은 컴퓨팅 장치에서 데이터 연산 처리가 수행될 때, 평문 메시지를 그대로 활용하는 것이 아니라, 메시지를 코드화한 후 코드화된 메시지를 기초로 데이터 연산 처리가 수행되도록 함으로써, 데이터 연산 과정에서의 보안을 강화할 수 있다.

대표도 - 도1



(52) CPC특허분류

G06F 17/153 (2013.01)

H03M 13/1575 (2013.01)

H04L 9/12 (2013.01)

H04L 2209/34 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711092968
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발(R&D)
연구과제명	자율 주행차를 위한 침입 감내 핵심 요소 기술 개발
기 여 율	1/1
과제수행기관명	조선대학교 산학협력단
연구기간	2019.01.01 ~ 2019.12.31

명세서

청구범위

청구항 1

부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치에 있어서,

t (t 는 자연수)비트의 코드에 대한 에러 정정 능력을 갖는 미리 설정된 $k \times n$ (k 와 n 은 2이상의 자연수로 n 은 k 보다 큰 수임)크기의 생성행렬(generator matrix)이 저장되어 있는 생성행렬 저장부;

상기 컴퓨팅 장치에서 생성된 제1 메시지와 제2 메시지에 대해 논리합이 수행되도록 하는 제1 연산 명령이 인가되면, 상기 생성행렬을 기초로 상기 제1 메시지에 대한 인코딩을 수행함으로써, 제1 코드워드(codeword)를 생성하고, 상기 생성행렬을 기초로 상기 제2 메시지에 대한 인코딩을 수행함으로써, 제2 코드워드를 생성하는 인코딩부;

상기 제1 코드워드와 상기 제2 코드워드가 생성되면, 상기 제1 코드워드와 상기 제2 코드워드를 논리합하여 제1 연산 코드워드를 생성한 후 상기 제1 연산 코드워드를 디코딩부로 전달하는 데이터 연산부; 및

상기 데이터 연산부로부터 상기 제1 연산 코드워드를 전달받아, 상기 제1 연산 코드워드에 대해 상기 생성행렬을 기초로 에러 정정 기반의 디코딩을 수행함으로써, 상기 제1 메시지와 상기 제2 메시지가 논리합된 합산 메시지를 복원하는 상기 디코딩부

를 포함하는 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치.

청구항 2

제1항에 있어서,

상기 디코딩부는

상기 생성행렬에 대응하는 패리티 검사 행렬을 생성하고, 상기 패리티 검사 행렬을 기초로 상기 제1 연산 코드워드에 대한 신드롬 디코딩(Syndrome Decoding)을 수행함으로써, 상기 제1 메시지와 상기 제2 메시지가 논리합된 상기 합산 메시지를 복원하는 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치.

청구항 3

제1항에 있어서,

상기 인코딩부는

상기 컴퓨팅 장치에서 생성된 제3 메시지와 제4 메시지에 대해 합성곱(convolution)이 수행되도록 하는 제2 연산 명령이 인가되면, 상기 생성행렬을 기초로 상기 제3 메시지에 대한 인코딩을 수행함으로써, 제3 코드워드를 생성하고, 상기 생성행렬을 기초로 상기 제4 메시지에 대한 인코딩을 수행함으로써, 제4 코드워드를 생성하고,

상기 데이터 연산부는

상기 제3 코드워드와 상기 제4 코드워드가 생성되면, 상기 제3 코드워드와 상기 제4 코드워드를 아다마르곱(Hadamard product)하여 제2 연산 코드워드를 생성하고, 상기 제2 연산 코드워드에 대해 미리 설정된 부트스트랩 행렬을 곱하여 상기 제2 연산 코드워드를 합성곱 코드워드 - 상기 합성곱 코드워드는 상기 제3 메시지와 상기 제4 메시지를 합성곱한 결과에 대해 상기 생성행렬을 기초로 인코딩을 수행한 코드워드를 의미함 - 로 변환한 후 상기 합성곱 코드워드를 상기 디코딩부로 전달하며,

상기 디코딩부는

상기 데이터 연산부로부터 상기 합성곱 코드워드를 전달받아, 상기 합성곱 코드워드에 대해 상기 생성행렬을 기초로 에러 정정 기반의 디코딩을 수행함으로써, 상기 제3 메시지와 상기 제4 메시지가 합성곱된 합성곱 메시지를 복원하는 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치.

청구항 4

제3항에 있어서,

상기 생성행렬은

1차 리드-물러(Reed-Muller: RM) 코드 구성된 생성행렬이고,

상기 부트스트랩 행렬은

상기 제2 연산 코드워드에 적용되어 있는 2차 RM 코드 - 상기 제3 코드워드와 상기 제4 코드워드가 아다마르곱됨에 따라 상기 제3 코드워드와 상기 제4 코드워드에 각각 적용되어 있던 1차 RM 코드는 상기 제2 연산 코드워드에서 2차 RM 코드로 변환됨 - 를 1차 RM 코드로 변환함과 동시에 상기 제2 연산 코드워드에서 상기 변환된 1차 RM 코드에 따른 생성행렬에 곱해지는 메시지 값이 상기 제3 메시지와 상기 제4 메시지를 합성곱한 결과와 동일해지도록 설정된 행렬인 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치.

청구항 5

제3항에 있어서,

상기 디코딩부는

상기 생성행렬에 대응하는 패리티 검사 행렬을 생성하고, 상기 패리티 검사 행렬을 기초로 상기 합성곱 코드워드에 대한 신드롬 디코딩을 수행함으로써, 상기 제3 메시지와 상기 제4 메시지가 합성곱된 상기 합성곱 메시지를 복원하는 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치.

청구항 6

부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치의 동작 방법에 있어서,

t (t 는 자연수)비트의 코드에 대한 에러 정정 능력을 갖는 미리 설정된 $k \times n$ (k 와 n 은 2이상의 자연수로 n 은 k 보다 큰 수임)크기의 생성행렬(generator matrix)이 저장되어 있는 생성행렬 저장부를 유지하는 단계;

상기 컴퓨팅 장치에서 생성된 제1 메시지와 제2 메시지에 대해 논리합이 수행되도록 하는 제1 연산 명령이 인가되면, 인코딩부가 상기 생성행렬을 기초로 상기 제1 메시지에 대한 인코딩을 수행함으로써, 제1 코드워드(codeword)를 생성하고, 상기 생성행렬을 기초로 상기 제2 메시지에 대한 인코딩을 수행함으로써, 제2 코드워드를 생성하는 단계;

상기 제1 코드워드와 상기 제2 코드워드가 생성되면, 데이터 연산부가 상기 제1 코드워드와 상기 제2 코드워드를 논리합하여 제1 연산 코드워드를 생성한 후 상기 제1 연산 코드워드를 디코딩부로 전달하는 단계; 및

상기 디코딩부가 상기 데이터 연산부로부터 상기 제1 연산 코드워드를 전달받아, 상기 제1 연산 코드워드에 대해 상기 생성행렬을 기초로 에러 정정 기반의 디코딩을 수행함으로써, 상기 제1 메시지와 상기 제2 메시지가 논리합된 합산 메시지를 복원하는 단계

를 포함하는 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치의 동작 방법.

청구항 7

제6항에 있어서,

상기 합산 메시지를 복원하는 단계는

상기 디코딩부가 상기 생성행렬에 대응하는 패리티 검사 행렬을 생성하고, 상기 패리티 검사 행렬을 기초로 상기 제1 연산 코드워드에 대한 신드롬 디코딩(Syndrome Decoding)을 수행함으로써, 상기 제1 메시지와 상기 제2 메시지가 논리합된 상기 합산 메시지를 복원하는 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치의 동작 방법.

청구항 8

제6항에 있어서,

상기 컴퓨팅 장치에서 생성된 제3 메시지와 제4 메시지에 대해 합성곱(convolution)이 수행되도록 하는 제2 연

산 명령이 인가되면, 상기 인코딩부가 상기 생성행렬을 기초로 상기 제3 메시지에 대한 인코딩을 수행함으로써, 제3 코드워드를 생성하고, 상기 생성행렬을 기초로 상기 제4 메시지에 대한 인코딩을 수행함으로써, 제4 코드워드를 생성하는 단계;

상기 제3 코드워드와 상기 제4 코드워드가 생성되면, 상기 데이터 연산부가 상기 제3 코드워드와 상기 제4 코드워드를 아다마르곱(Hadamard product)하여 제2 연산 코드워드를 생성하고, 상기 제2 연산 코드워드에 대해 미리 설정된 부트스트랩 행렬을 곱하여 상기 제2 연산 코드워드를 합성곱 코드워드 - 상기 합성곱 코드워드는 상기 제3 메시지와 상기 제4 메시지를 합성곱한 결과에 대해 상기 생성행렬을 기초로 인코딩을 수행한 코드워드를 의미함 - 로 변환한 후 상기 합성곱 코드워드를 상기 디코딩부로 전달하는 단계; 및

상기 디코딩부가 상기 데이터 연산부로부터 상기 합성곱 코드워드를 전달받아, 상기 합성곱 코드워드에 대해 상기 생성행렬을 기초로 에러 정정 기반의 디코딩을 수행함으로써, 상기 제3 메시지와 상기 제4 메시지가 합성곱된 합성곱 메시지를 복원하는 단계

를 더 포함하는 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치의 동작 방법.

청구항 9

제8항에 있어서,

상기 생성행렬은

1차 리드-몰러(Reed-Muller: RM) 코드 구성된 생성행렬이고,

상기 부트스트랩 행렬은

상기 제2 연산 코드워드에 적용되어 있는 2차 RM 코드 - 상기 제3 코드워드와 상기 제4 코드워드가 아다마르곱됨에 따라 상기 제3 코드워드와 상기 제4 코드워드에 각각 적용되어 있던 1차 RM 코드는 상기 제2 연산 코드워드에서 2차 RM 코드로 변환됨 - 을 1차 RM 코드로 변환함과 동시에 상기 제2 연산 코드워드에서 상기 변환된 1차 RM 코드에 따른 생성행렬에 곱해지는 메시지 값이 상기 제3 메시지와 상기 제4 메시지를 합성곱한 결과와 동일해지도록 설정된 행렬인 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치의 동작 방법.

청구항 10

제8항에 있어서,

상기 합성곱 메시지를 복원하는 단계는

상기 디코딩부가 상기 생성행렬에 대응하는 패리티 검사 행렬을 생성하고, 상기 패리티 검사 행렬을 기초로 상기 합성곱 코드워드에 대한 신드롬 디코딩을 수행함으로써, 상기 제3 메시지와 상기 제4 메시지가 합성곱된 상기 합성곱 메시지를 복원하는 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치의 동작 방법.

청구항 11

제6항 내지 제10항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 컴퓨터 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

청구항 12

제6항 내지 제10항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램.

발명의 설명

기술 분야

[0001] 본 발명은 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치 및 그 동작 방법에 대한 것이다.

배경 기술

[0002] 최근, 다양한 분야에서 컴퓨팅 장치가 활용됨에 따라, 컴퓨팅 장치에 대한 공격에 대비할 수 있는 보안 기술이

중요한 이슈로 대두되고 있다.

- [0003] 특히, 최근에는 원자력 발전소 등과 같은 대규모 산업 시설이나 자율 주행 차량 등에도 컴퓨팅 장치가 도입됨에 따라, 외부로부터의 악의적인 공격에 방어할 수 있는 지능화된 보안 기술의 도입이 필수로 자리잡고 있다.
- [0004] 컴퓨팅 장치는 다양한 연산 처리 모듈을 통해 데이터 연산을 수행하게 된다. 만약, 컴퓨팅 장치 내부에서 데이터가 연산되는 과정에서 외부로부터의 악의적인 데이터 조작이나 에러 유발 등이 발생하게 되는 경우, 데이터 연산이 잘못 처리됨으로 인해 큰 문제가 발생할 수 있다.
- [0005] 기존의 컴퓨팅 장치에서의 데이터 연산 처리는 컴퓨팅 장치에서 생성된 평문 메시지를 그대로 이용한다는 점에서 외부로부터의 데이터 조작에 취약한 문제가 있었다. 예컨대, 컴퓨팅 장치에서 생성된 제1 메시지와 제2 메시지를 서로 논리합하는 연산을 수행한다고 하였을 때, 기존의 컴퓨팅 장치는 상기 제1 메시지와 상기 제2 메시지를 평문 메시지 상태에서 그대로 논리합하기 때문에 제3자에 의한 데이터 조작에 쉽게 노출되는 문제가 있었다.
- [0006] 따라서, 컴퓨팅 장치에서 데이터 연산 처리가 수행될 때, 평문 메시지를 그대로 활용하는 것이 아니라, 메시지를 코드화한 후 코드화된 메시지를 기초로 데이터 연산 처리가 수행되도록 함으로써, 데이터 연산 과정에서의 보안을 강화할 수 있는 기술에 대한 연구가 필요하다.

발명의 내용

해결하려는 과제

- [0007] 본 발명은 컴퓨팅 장치에서 데이터 연산 처리가 수행될 때, 평문 메시지를 그대로 활용하는 것이 아니라, 메시지를 코드화한 후 코드화된 메시지를 기초로 데이터 연산 처리가 수행되도록 함으로써, 데이터 연산 과정에서의 보안을 강화할 수 있도록 한다.

과제의 해결 수단

- [0008] 본 발명의 일실시예에 따른 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치는 t (t 는 자연수)비트의 코드에 대한 에러 정정 능력을 갖는 미리 설정된 $k \times n$ (k 와 n 은 2이상의 자연수로 n 은 k 보다 큰 수임)크기의 생성행렬(generator matrix)이 저장되어 있는 생성행렬 저장부, 상기 컴퓨팅 장치에서 생성된 제1 메시지와 제2 메시지에 대해 논리합이 수행되도록 하는 제1 연산 명령이 인가되면, 상기 생성행렬을 기초로 상기 제1 메시지에 대한 인코딩을 수행함으로써, 제1 코드워드(codeword)를 생성하고, 상기 생성행렬을 기초로 상기 제2 메시지에 대한 인코딩을 수행함으로써, 제2 코드워드를 생성하는 인코딩부, 상기 제1 코드워드와 상기 제2 코드워드가 생성되면, 상기 제1 코드워드와 상기 제2 코드워드를 논리합하여 제1 연산 코드워드를 생성한 후 상기 제1 연산 코드워드를 디코딩부로 전달하는 데이터 연산부 및 상기 데이터 연산부로부터 상기 제1 연산 코드워드를 전달받아, 상기 제1 연산 코드워드에 대해 상기 생성행렬을 기초로 에러 정정 기반의 디코딩을 수행함으로써, 상기 제1 메시지와 상기 제2 메시지가 논리합된 합산 메시지를 복원하는 상기 디코딩부를 포함한다.
- [0009] 또한, 본 발명의 일실시예에 따른 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치의 동작 방법은 t (t 는 자연수)비트의 코드에 대한 에러 정정 능력을 갖는 미리 설정된 $k \times n$ (k 와 n 은 2이상의 자연수로 n 은 k 보다 큰 수임)크기의 생성행렬이 저장되어 있는 생성행렬 저장부를 유지하는 단계, 상기 컴퓨팅 장치에서 생성된 제1 메시지와 제2 메시지에 대해 논리합이 수행되도록 하는 제1 연산 명령이 인가되면, 인코딩부가 상기 생성행렬을 기초로 상기 제1 메시지에 대한 인코딩을 수행함으로써, 제1 코드워드를 생성하고, 상기 생성행렬을 기초로 상기 제2 메시지에 대한 인코딩을 수행함으로써, 제2 코드워드를 생성하는 단계, 상기 제1 코드워드와 상기 제2 코드워드가 생성되면, 데이터 연산부가 상기 제1 코드워드와 상기 제2 코드워드를 논리합하여 제1 연산 코드워드를 생성한 후 상기 제1 연산 코드워드를 디코딩부로 전달하는 단계 및 상기 디코딩부가 상기 데이터 연산부로부터 상기 제1 연산 코드워드를 전달받아, 상기 제1 연산 코드워드에 대해 상기 생성행렬을 기초로 에러 정정 기반의 디코딩을 수행함으로써, 상기 제1 메시지와 상기 제2 메시지가 논리합된 합산 메시지를 복원하는 단계를 포함한다.

발명의 효과

- [0010] 본 발명은 컴퓨팅 장치에서 데이터 연산 처리가 수행될 때, 평문 메시지를 그대로 활용하는 것이 아니라, 메시지를 코드화한 후 코드화된 메시지를 기초로 데이터 연산 처리가 수행되도록 함으로써, 데이터 연산 과정에서의

보안을 강화할 수 있다.

도면의 간단한 설명

[0011] 도 1은 본 발명의 일실시예에 따른 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치의 구조를 도시한 도면이다.

도 2는 본 발명의 일실시예에 따른 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치의 동작 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0012] 이하에서는 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명하기로 한다. 이러한 설명은 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였으며, 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 본 명세서 상에서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 사람에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다.

[0013] 본 문서에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있다는 것을 의미한다. 또한, 본 발명의 다양한 실시예들에 있어서, 각 구성요소들, 기능 블록들 또는 수단들은 하나 또는 그 이상의 하부 구성요소로 구성될 수 있고, 각 구성요소들이 수행하는 전기, 전자, 기계적 기능들은 전자회로, 집적회로, ASIC(Application Specific Integrated Circuit) 등 공지된 다양한 소자들 또는 기계적 요소들로 구현될 수 있으며, 각각 별개로 구현되거나 2 이상이 하나로 통합되어 구현될 수도 있다.

[0014] 한편, 첨부된 블록도의 블록들이나 흐름도의 단계들은 범용 컴퓨터, 특수용 컴퓨터, 휴대용 노트북 컴퓨터, 네트워크 컴퓨터 등 데이터 프로세싱이 가능한 장비의 프로세서나 메모리에 탑재되어 지정된 기능들을 수행하는 컴퓨터 프로그램 명령들(instructions)을 의미하는 것으로 해석될 수 있다. 이들 컴퓨터 프로그램 명령들은 컴퓨터 장치에 구비된 메모리 또는 컴퓨터에서 판독 가능한 메모리에 저장될 수 있기 때문에, 블록도의 블록들 또는 흐름도의 단계들에서 설명된 기능들은 이를 수행하는 명령 수단을 내포하는 제조물로 생산될 수도 있다. 아울러, 각 블록 또는 각 단계는 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 명령들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또, 몇 가지 대체 가능한 실시예들에서는 블록들 또는 단계들에서 언급된 기능들이 정해진 순서와 달리 실행되는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 실질적으로 동시에 수행되거나, 역순으로 수행될 수 있으며, 경우에 따라 일부 블록들 또는 단계들이 생략된 채로 수행될 수도 있다.

[0015] 도 1은 본 발명의 일실시예에 따른 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치의 구조를 도시한 도면이다.

[0016] 도 1을 참조하면, 본 발명에 따른 컴퓨팅 장치(110)는 생성행렬 저장부(111), 인코딩부(112), 데이터 연산부(113) 및 디코딩부(114)를 포함한다.

[0017] 생성행렬 저장부(111)에는 t (t 는 자연수)비트의 코드에 대한 에러 정정 능력을 갖는 미리 설정된 $k \times n$ (k 와 n 은 2이상의 자연수로 n 은 k 보다 큰 수임)크기의 생성행렬(generator matrix)이 저장되어 있다.

[0018] 생성행렬은 데이터 전송측이 데이터 수신측으로 데이터를 전송할 때, 데이터 수신측이 에러 정정을 수행할 수 있도록 코드워드(codeword)를 생성하는데 사용되는 행렬로, 데이터 전송측이 소정의 생성행렬을 기초로 코드워드를 생성하여 데이터 수신측으로 전송하면, 데이터 수신측에서는 생성행렬에 대응하는 패리티 검사 행렬을 통해 수신된 데이터로부터 에러와 원본 데이터를 복원할 수 있게 된다.

[0019] 인코딩부(112)는 컴퓨팅 장치(110)에서 생성된 제1 메시지와 제2 메시지에 대해 논리합이 수행되도록 하는 제1 연산 명령이 인가되면, 상기 생성행렬을 기초로 상기 제1 메시지에 대한 인코딩을 수행함으로써, 제1 코드워드를 생성하고, 상기 생성행렬을 기초로 상기 제2 메시지에 대한 인코딩을 수행함으로써, 제2 코드워드를 생성한다.

[0020] 예컨대, 상기 생성행렬을 'G'라고 하고, 상기 제1 메시지에 대한 메시지 벡터를 ' m_1 ', 상기 제2 메시지에 대한

메시지 벡터를 ' m_2 '라고 하는 경우, 인코딩부(112)는 하기의 수학식 1의 연산에 따라 상기 제1 코드워드 ' c_1 '을 생성할 수 있고, 하기의 수학식 2의 연산에 따라 상기 제2 코드워드 ' c_2 '를 생성할 수 있다.

수학식 1

$$c_1 = m_1 G$$

수학식 2

$$c_2 = m_2 G$$

데이터 연산부(113)는 상기 제1 코드워드와 상기 제2 코드워드가 생성되면, 상기 제1 코드워드와 상기 제2 코드워드를 논리합하여 제1 연산 코드워드를 생성한 후 상기 제1 연산 코드워드를 디코딩부로 전달한다.

관련해서, 데이터 연산부(113)는 하기의 수학식 3의 연산에 따라 상기 제1 연산 코드워드 ' c_1+c_2 '를 생성할 수 있다.

수학식 3

$$c_1 + c_2 = m_1 G + m_2 G = (m_1 + m_2) G$$

디코딩부(114)는 데이터 연산부(113)로부터 상기 제1 연산 코드워드를 전달받아, 상기 제1 연산 코드워드에 대해 상기 생성행렬을 기초로 에러 정정 기반의 디코딩을 수행함으로써, 상기 제1 메시지와 상기 제2 메시지가 논리합된 합산 메시지를 복원한다.

이때, 본 발명의 일실시예에 따르면, 디코딩부(114)는 상기 생성행렬에 대응하는 패리티 검사 행렬을 생성하고, 상기 패리티 검사 행렬을 기초로 상기 제1 연산 코드워드에 대한 신드롬 디코딩(Syndrome Decoding)을 수행함으로써, 상기 제1 메시지와 상기 제2 메시지가 논리합된 상기 합산 메시지를 복원할 수 있다.

우선, 패리티 검사 행렬은 데이터 전송측이 소정의 생성행렬을 기반으로 인코딩된 코드워드를 데이터 수신측으로 전송하였을 때, 데이터 수신측이 수신한 데이터에 에러가 발생하였는지 여부를 검증하기 위한 행렬로, $k \times n$ 크기의 생성행렬 ' G '에 대응하는 패리티 검사 행렬 ' H '는 크기가 $(n-k) \times n$ 이고, 상기 생성행렬 ' G '와의 관계에서 하기의 수학식 4와 같은 특성을 갖는다.

수학식 4

$$GH^T = 0$$

[0037] 여기서, H^T 는 상기 패리티 검사 행렬의 전치 행렬을 의미한다.

[0038] 관련해서, 디코딩부(114)는 데이터 연산부(113)로부터 상기 제1 연산 코드워드가 전달되면, 상기 생성행렬에 대응하는 패리티 검사 행렬을 생성한 후 상기 제1 연산 코드워드에 대해 상기 패리티 검사 행렬을 기초로 하기의 수학식 5에 따른 연산을 수행할 수 있다.

수학식 5

[0040]
$$rH^T = S$$

[0042] 여기서, 'r'은 데이터 연산부(113)에서 전달된 상기 제1 연산 코드워드로, 상기 제1 연산 코드워드는 원래 수학식 3에서 나타낸 바와 같이, $(m_1+m_2)G$ 이지만 데이터 연산 과정이나 데이터 전달 과정에서 소정의 에러가 적용될 수 있다. 만약, 상기 제1 연산 코드워드에 적용된 에러에 따른 에러 벡터를 'e'라고 하는 경우, 상기 수학식 5는 하기의 수학식 6과 같이 나타낼 수 있다.

수학식 6

[0044]
$$\begin{aligned} rH^T &= ((m_1 + m_2)G \oplus e)H^T \\ &= (m_1 + m_2)GH^T \oplus eH^T \\ &= eH^T \end{aligned}$$

[0046] 여기서, $\oplus$ 는 배타적 논리합 연산을 의미한다. 상기 수학식 5에서와 같은 연산을 통해 산출된 'S'를 신드롬(Syndrome)이라고 하는데, 상기 수학식 5에 따라 연산되는 신드롬 'S'는 상기 수학식 6에서 나타낸 바와 같이, eH^T 와 동일하기 때문에, 디코딩부(114)는 상기 수학식 5의 연산을 통해 신드롬 'S'를 산출한 후 상기 신드롬 'S'와 상기 패리티 검사 행렬을 기초로 $S = eH^T$ 를 만족하는 에러 벡터 'e'를 찾아낼 수 있다.

[0047] 그리고 나서, 디코딩부(114)는 상기 에러 벡터 'e'를 기초로 에러가 제거된 상기 제1 연산 코드워드인 $(m_1+m_2)G$ 을 복원하고, 상기 제1 연산 코드워드로부터 상기 제1 메시지와 상기 제2 메시지가 논리합된 합산 메시지인 (m_1+m_2) 를 복원할 수 있다.

[0048] 본 발명의 일실시예에 따르면, 인코딩부(112)는 컴퓨팅 장치(110)에서 생성된 제3 메시지와 제4 메시지에 대해 합성곱(convolution)이 수행되도록 하는 제2 연산 명령이 인가되면, 상기 생성행렬을 기초로 상기 제3 메시지에 대한 인코딩을 수행함으로써, 제3 코드워드를 생성하고, 상기 생성행렬을 기초로 상기 제4 메시지에 대한 인코딩을 수행함으로써, 제4 코드워드를 생성할 수 있다.

[0049] 예컨대, 상기 생성행렬을 'G'라고 하고, 상기 제3 메시지에 대한 메시지 벡터를 'm₃', 상기 제4 메시지에 대한 메시지 벡터를 'm₄'라고 하는 경우, 인코딩부(112)는 하기의 수학식 7의 연산에 따라 상기 제3 코드워드 'c₃'을

생성할 수 있고, 하기의 수학식 8의 연산에 따라 상기 제4 코드워드 ' c_4 '를 생성할 수 있다.

수학식 7

$$c_3 = m_3 G$$

[0051]

수학식 8

$$c_4 = m_4 G$$

[0053]

[0055] 이때, 데이터 연산부(113)는 상기 제3 코드워드와 상기 제4 코드워드가 생성되면, 상기 제3 코드워드와 상기 제4 코드워드를 아다마르곱(Hadamard product)하여 제2 연산 코드워드를 생성하고, 상기 제2 연산 코드워드에 대해 미리 설정된 부트스트랩 행렬을 곱하여 상기 제2 연산 코드워드를 합성곱 코드워드로 변환한 후 상기 합성곱 코드워드를 디코딩부(114)로 전달할 수 있다.

[0056] 여기서, 상기 합성곱 코드워드는 상기 제3 메시지와 상기 제4 메시지를 합성곱한 결과에 대해 상기 생성행렬을 기초로 인코딩을 수행한 코드워드를 의미한다.

[0057] 또한, 아다마르 곱이란 같은 크기의 벡터나 행렬에서 각 성분을 곱하는 연산을 의미하는 것으로, $[a \ b \ c]$ 와 $[x \ y \ z]$ 라는 벡터가 존재할 때, 두 벡터 간의 아다마르 곱은 $[ax \ by \ cz]$ 로 연산될 수 있다.

[0058] 관련해서, 데이터 연산부(113)는 하기의 수학식 9의 연산에 따라, 상기 제2 연산 코드워드를 상기 합성곱 코드워드 ' c_{cov} '로 변환할 수 있다.

수학식 9

$$c_{cov} = (c_3 \circ c_4) B$$

[0060]

[0062] 여기서, ' B '는 상기 부트스트랩 행렬, ' $\circ$ '는 아다마르곱을 의미한다. 상기 부트스트랩 행렬은 상기 수학식 9를 통해 연산되는 결과가 상기 제3 메시지와 상기 제4 메시지를 합성곱한 결과에 대해 상기 생성행렬을 기초로 인코딩을 수행한 코드워드와 같아지도록 미리 설계된 행렬이기 때문에, 상기 수학식 9에서 연산된 합성곱 코드워드는 하기의 수학식 10과 같이, 상기 제3 메시지와 상기 제4 메시지를 합성곱한 결과에 대해 상기 생성행렬을 기초로 인코딩을 수행한 코드워드와 같아지게 된다.

수학식 10

$$\begin{aligned} c_{cov} &= (c_3 \circ c_4)B \\ &= (m_3 * m_4)G \end{aligned}$$

[0064]

[0066]

여기서, ' $*$ '은 합성곱을 의미한다.

[0067]

이때, 본 발명의 일실시예에 따르면, 생성행렬 저장부(111)에 저장되어 있는 상기 생성행렬은 1차 리드-물러(Reed-Muller: RM) 코드 구성된 생성행렬일 수 있다.

[0068]

이때, 상기 제3 코드워드와 상기 제4 코드워드가 아다마르곱됨에 따라 상기 제3 코드워드와 상기 제4 코드워드 각각 적용되어 있던 1차 RM 코드는 상기 제2 연산 코드워드에서 2차 RM 코드로 변환되게 된다. 즉, 상기 수학식 7과 8에서 상기 제3 코드워드와 상기 제4 코드워드에 적용되어 있던 생성행렬 'G'를 구성하는 1차 RM 코드는 ' $c_3 \circ c_4$ '와 같이, 상기 제2 연산 코드워드로의 연산이 수행됨에 따라 2차 RM 코드로 변환된다.

[0069]

이때, 상기 부트스트랩 행렬은 상기 제2 연산 코드워드에 적용되어 있는 2차 RM 코드를 1차 RM 코드로 변환함과 동시에 상기 제2 연산 코드워드에서 상기 변환된 1차 RM 코드에 따른 생성행렬에 곱해지는 메시지 값이 상기 제3 메시지와 상기 제4 메시지를 합성곱한 결과와 동일해지도록 설정된 행렬일 수 있다.

[0070]

즉, 상기 부트스트랩 행렬은 ' $c_3 \circ c_4$ '라는 상기 제2 연산 코드워드가 생성되었을 때, 상기 제2 연산 코드워드를 소정의 메시지 ' m_k '와 1차 RM 코드에 따른 생성행렬의 곱의 형태인 ' $m_k G$ '로 변환하되, 메시지 ' m_k '가 상기 제3 메시지와 상기 제4 메시지를 합성곱한 결과인 ' $(m_3 * m_4)$ '와 동일해지도록 미리 설정된 행렬일 수 있다.

[0071]

이렇게, 데이터 연산부(113)에서 상기 합성곱 코드워드가 생성되면, 디코딩부(114)는 데이터 연산부(113)로부터 상기 합성곱 코드워드를 전달받아, 상기 합성곱 코드워드에 대해 상기 생성행렬을 기초로 에러 정정 기반의 디코딩을 수행함으로써, 상기 제3 메시지와 상기 제4 메시지가 합성곱된 합성곱 메시지를 복원할 수 있다.

[0072]

이때, 본 발명의 일실시예에 따르면, 디코딩부(114)는 상기 생성행렬에 대응하는 패리티 검사 행렬을 생성하고, 상기 패리티 검사 행렬을 기초로 상기 합성곱 코드워드에 대한 신드롬 디코딩을 수행함으로써, 상기 제3 메시지와 상기 제4 메시지가 합성곱된 상기 합성곱 메시지를 복원할 수 있다.

[0073]

관련해서, 디코딩부(114)는 데이터 연산부(113)로부터 상기 합성곱 코드워드가 전달되면, 상기 생성행렬에 대응하는 패리티 검사 행렬을 생성한 후 상기 합성곱 연산 코드워드에 대해 상기 패리티 검사 행렬을 기초로 하기의 수학식 11에 따른 연산을 수행할 수 있다.

수학식 11

$$r_{cov} H^T = S_{cov}$$

[0075]

[0077]

여기서, ' r_{cov} '은 데이터 연산부(113)에서 전달된 상기 합성곱 코드워드, 상기 합성곱 코드워드는 원래 수학식 10에서 나타난 바와 같이, ' $(m_3 * m_4) G$ '이지만 데이터 연산 과정이나 데이터 전달 과정에서 소정의 에러

가 적용될 수 있다. 만약, 상기 합성곱 코드워드에 적용된 에러에 따른 에러 벡터를 ' e_1 '이라고 하는 경우, 상기 수학식 11는 하기의 수학식 12와 같이 나타낼 수 있다.

수학식 12

$$\begin{aligned} r_{cov}H^T &= ((m_1 * m_2)G \oplus e_1)H^T \\ &= (m_1 * m_2)GH^T \oplus e_1H^T \\ &= e_1H^T \end{aligned}$$

[0079]

[0081] 이때, 디코딩부(114)는 상기 수학식 11의 연산을 통해 신드롬 ' S_{cov} '를 산출한 후 상기 신드롬 ' S_{cov} '와 상기 패리티 검사 행렬을 기초로 $S_{cov} = e_1H^T$ 를 만족하는 에러 벡터 ' e_1 '를 찾아낼 수 있다.

[0082] 그리고 나서, 디코딩부(114)는 상기 에러 벡터 ' e_1 '을 기초로 에러가 제거된 상기 합성곱 코드워드인 ' $(m_3 * m_4)G$ '을 복원하고, 상기 합성곱 코드워드로부터 상기 제3 메시지와 상기 제4 메시지가 합성곱된 합성곱 메시지인 ' $(m_3 * m_4)$ '를 복원할 수 있다.

[0083] 도 2는 본 발명의 일실시예에 따른 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치의 동작 방법을 도시한 순서도이다.

[0084] 단계(S210)에서는 t (t 는 자연수)비트의 코드에 대한 에러 정정 능력을 갖는 미리 설정된 $k \times n$ (k 와 n 은 2이상의 자연수로 n 은 k 보다 큰 수임)크기의 생성행렬이 저장되어 있는 생성행렬 저장부를 유지한다.

[0085] 단계(S220)에서는 상기 컴퓨팅 장치에서 생성된 제1 메시지와 제2 메시지에 대해 논리합이 수행되도록 하는 제1 연산 명령이 인가되면, 인코딩부가 상기 생성행렬을 기초로 상기 제1 메시지에 대한 인코딩을 수행함으로써, 제1 코드워드를 생성하고, 상기 생성행렬을 기초로 상기 제2 메시지에 대한 인코딩을 수행함으로써, 제2 코드워드를 생성한다.

[0086] 단계(S230)에서는 상기 제1 코드워드와 상기 제2 코드워드가 생성되면, 데이터 연산부가 상기 제1 코드워드와 상기 제2 코드워드를 논리합하여 제1 연산 코드워드를 생성한 후 상기 제1 연산 코드워드를 디코딩부로 전달한다.

[0087] 단계(S240)에서는 상기 디코딩부가 상기 데이터 연산부로부터 상기 제1 연산 코드워드를 전달받아, 상기 제1 연산 코드워드에 대해 상기 생성행렬을 기초로 에러 정정 기반의 디코딩을 수행함으로써, 상기 제1 메시지와 상기 제2 메시지가 논리합된 합산 메시지를 복원한다.

[0088] 이때, 본 발명의 일실시예에 따르면, 단계(S240)에서는 상기 디코딩부가 상기 생성행렬에 대응하는 패리티 검사 행렬을 생성하고, 상기 패리티 검사 행렬을 기초로 상기 제1 연산 코드워드에 대한 신드롬 디코딩을 수행함으로써, 상기 제1 메시지와 상기 제2 메시지가 논리합된 상기 합산 메시지를 복원할 수 있다.

[0089] 또한, 본 발명의 일실시예에 따르면, 상기 컴퓨팅 장치의 동작 방법은 상기 컴퓨팅 장치에서 생성된 제3 메시지와 제4 메시지에 대해 합성곱이 수행되도록 하는 제2 연산 명령이 인가되면, 상기 인코딩부가 상기 생성행렬을 기초로 상기 제3 메시지에 대한 인코딩을 수행함으로써, 제3 코드워드를 생성하고, 상기 생성행렬을 기초로 상기 제4 메시지에 대한 인코딩을 수행함으로써, 제4 코드워드를 생성하는 단계, 상기 제3 코드워드와 상기 제4 코드워드가 생성되면, 상기 데이터 연산부가 상기 제3 코드워드와 상기 제4 코드워드를 아다마르곱하여 제2 연산 코드워드를 생성하고, 상기 제2 연산 코드워드에 대해 미리 설정된 부트스트랩 행렬을 곱하여 상기 제2 연산 코드워드를 합성곱 코드워드(상기 합성곱 코드워드는 상기 제3 메시지와 상기 제4 메시지를 합성곱한 결과에 대

해 상기 생성행렬을 기초로 인코딩을 수행한 코드워드를 의미함)로 변환한 후 상기 합성곱 코드워드를 상기 디코딩부로 전달하는 단계 및 상기 디코딩부가 상기 데이터 연산부로부터 상기 합성곱 코드워드를 전달받아, 상기 합성곱 코드워드에 대해 상기 생성행렬을 기초로 에러 정정 기반의 디코딩을 수행함으로써, 상기 제3 메시지와 상기 제4 메시지가 합성곱된 합성곱 메시지를 복원하는 단계를 더 포함할 수 있다.

[0090] 이때, 본 발명의 일실시예에 따르면, 상기 생성행렬은 1차 RM 코드 구성된 생성행렬이고, 상기 부트스트랩 행렬은 상기 제2 연산 코드워드에 적용되어 있는 2차 RM 코드(상기 제3 코드워드와 상기 제4 코드워드가 아다마르곱됨에 따라 상기 제3 코드워드와 상기 제4 코드워드에 각각 적용되어 있던 1차 RM 코드는 상기 제2 연산 코드워드에서 2차 RM 코드로 변환됨)를 1차 RM 코드로 변환함과 동시에 상기 제2 연산 코드워드에서 상기 변환된 1차 RM 코드에 따른 생성행렬에 곱해지는 메시지 값이 상기 제3 메시지와 상기 제4 메시지를 합성곱한 결과와 동일해지도록 설정된 행렬일 수 있다.

[0091] 또한, 본 발명의 일실시예에 따르면, 상기 합성곱 메시지를 복원하는 단계는 상기 디코딩부가 상기 생성행렬에 대응하는 패리티 검사 행렬을 생성하고, 상기 패리티 검사 행렬을 기초로 상기 합성곱 코드워드에 대한 신드롬 디코딩을 수행함으로써, 상기 제3 메시지와 상기 제4 메시지가 합성곱된 상기 합성곱 메시지를 복원할 수 있다.

[0092] 이상, 도 2를 참조하여 본 발명의 일실시예에 따른 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치의 동작 방법에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치의 동작 방법은 도 1을 이용하여 설명한 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치(110)의 동작에 대한 구성과 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.

[0093] 본 발명의 일실시예에 따른 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치의 동작 방법은 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다.

[0094] 또한, 본 발명의 일실시예에 따른 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치의 동작 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 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(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 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.

[0095] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

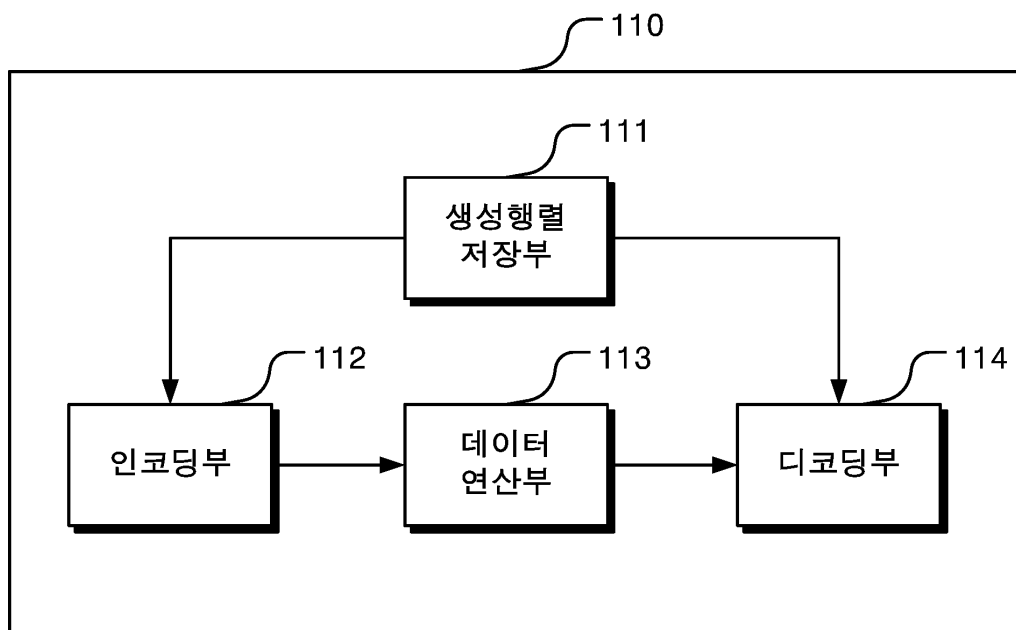
[0096] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

- [0097] 110: 부호 기반의 데이터 연산 처리가 가능한 컴퓨팅 장치
111: 생성행렬 저장부
112: 인코딩부
113: 데이터 연산부
114: 디코딩부

도면

도면1



도면2

