



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년05월29일
(11) 등록번호 10-1741186
(24) 등록일자 2017년05월23일

- (51) 국제특허분류(Int. Cl.)
G06F 17/30 (2006.01) G06F 11/14 (2006.01)
- (52) CPC특허분류
G06F 17/30371 (2013.01)
G06F 11/1448 (2013.01)
- (21) 출원번호 10-2015-0190137
(22) 출원일자 2015년12월30일
심사청구일자 2015년12월30일
- (56) 선행기술조사문헌
“분산 저장 시스템을 위한 완전그래프 기반 부분 접속복구 부호”, 한국통신학회 학술대회논문집(pp. 846-847), 2015년 06월*
“부분접속 복구 부호의 복구집합에 관한 연구”, 한국통신학회 학술대회논문집(pp. 591-592), 2015년 11월*
“부분접속 복구 가능한 반복분할 부호”, 한국통신학회논문지 40(9)(pp. 1741-1753), 2015년 09월
“완전다분할그래프 기반 이진 부분접속복구 부호”, 한국통신학회논문지 40(9)(pp. 1734-1740), 2015년 09월
*는 심사관에 의하여 인용된 문헌

- (73) 특허권자
조선대학교산학협력단
광주광역시 동구 필문대로 309 (서석동)
전남대학교산학협력단
광주광역시 북구 용봉로 77 (용봉동)
- (72) 발명자
김영식
광주광역시 서구 풍암2로 62 금호2차아파트 201동 1005호
박호성
광주광역시 북구 서하로 416, 대주3차아파트 102동 1107호
- (74) 대리인
김효성

전체 청구항 수 : 총 8 항

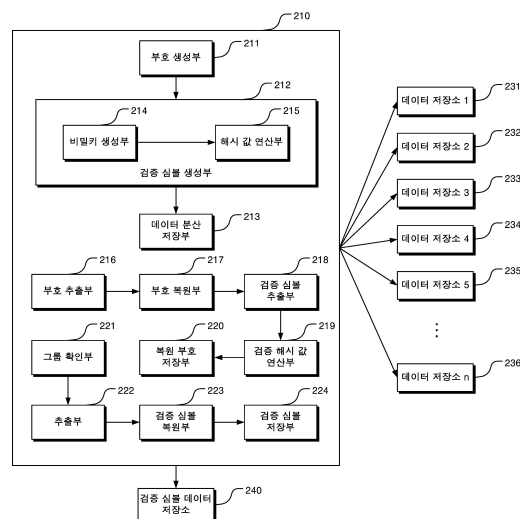
심사관 : 박승철

(54) 발명의 명칭 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 장치 및 방법

(57) 요약

부분 복구가능 부호(locally repairable code)의 검증이 가능한 데이터 분산 저장 장치 및 방법이 개시된다. 본 발명은 부분 복구가능 부호를 활용하여 데이터를 분산 저장하는 시스템에서 데이터 저장소에 분할 저장되어 있는 특정 부분 복구가능 부호가 손실됨에 따라, 해당 부분 복구가능 부호가 복원될 경우, 복원된 부분 복구가능 부호에 대한 데이터 무결성을 검증할 수 있는 장치 및 방법을 제공할 수 있다.

대표도 - 도2



(52) CPC특허분류

G06F 11/1458 (2013.01)

G06F 17/30575 (2013.01)

G06F 17/30584 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711024287

부처명 미래창조과학부

연구관리전문기관 한국연구재단

연구사업명 중견연구자지원

연구과제명 포스트 양자 암호의 설계 및 효율적 구현에 관한 연구

기 여 율 1/2

주관기관 조선대학교

연구기간 2014.05.01 ~ 2017.04.30

이 발명을 지원한 국가연구개발사업

과제고유번호 1345241259

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 이공학개인지초연구지원

연구과제명 빅데이터의 신뢰성 향상 및 효율적 관리를 위한 분산 저장 부호 기법

기 여 율 1/2

주관기관 전남대학교

연구기간 2015.11.01 ~ 2018.10.31

명세서

청구범위

청구항 1

입력 데이터에 대한 데이터 저장 명령이 인가되면, 상기 입력 데이터에 대해 부분 복구가능 부호(locally repairable code)의 생성을 위한 인코딩을 수행하여 상기 입력 데이터로부터 n (n 은 자연수)개의 부분 복구가능 부호들 - 상기 n 개의 부분 복구가능 부호들은 k (k 는 자연수)개의 그룹들로 그룹화되어, 각 그룹 내 속해있는 부호들 각각은 동일 그룹 내에 속해있는 나머지 부호들에 의해 복구가 가능하도록 구성됨 - 을 생성하는 부호 생성부;

상기 k 개의 그룹들 별로, 각 그룹 내 속해있는 부분 복구가능 부호들의 검증을 위한 검증 심볼(symbol)을 생성함으로써, 상기 k 개의 그룹들 각각에 대응하는 k 개의 검증 심볼들을 생성하는 검증 심볼 생성부; 및

상기 n 개의 부분 복구가능 부호들을 n 개의 분리된 데이터 저장소들에 각각 분할하여 저장하고, 상기 k 개의 검증 심볼들을 검증 심볼 데이터 저장소에 저장하는 데이터 분산 저장부

를 포함하고,

상기 검증 심볼 생성부는

상기 k 개의 그룹들 각각에 대응되는 서로 다른 k 개의 비밀키들을 생성하는 비밀키 생성부; 및

상기 k 개의 그룹들 별로, 각 그룹 내에 속해있는 부분 복구가능 부호들과 상기 각 그룹에 대응하는 비밀키를 선정된(predetermined) 해시 함수에 입력으로 인가하여 해시 값을 연산함으로써, 상기 k 개의 그룹들 각각에 대응하는 k 개의 해시 값들을 생성하고, 상기 생성된 k 개의 해시 값들을 상기 k 개의 그룹들 각각에 대응하는 상기 k 개의 검증 심볼들로 결정하는 해시 값 연산부

를 포함하는 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 장치.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 n 개의 분리된 데이터 저장소들 중 제1 데이터 저장소에 저장되어 있는 제1 부분 복구가능 부호가 손실된 경우, 상기 k 개의 그룹들 중 상기 제1 부분 복구가능 부호가 속해있는 제1 그룹을 확인하여 상기 제1 그룹에 속해있는 부분 복구가능 부호들 중 상기 제1 부분 복구가능 부호를 제외한 나머지 부분 복구가능 부호들이 저장되어 있는 데이터 저장소들로부터 상기 나머지 부분 복구가능 부호들을 추출하는 부호 추출부;

상기 추출된 나머지 부분 복구가능 부호들에 기초하여 상기 제1 부분 복구가능 부호를 복원하는 부호 복원부;

상기 검증 심볼 데이터 저장소로부터 상기 제1 그룹에 대응하는 제1 검증 심볼을 추출하는 검증 심볼 추출부;

상기 복원된 제1 부분 복구가능 부호와 상기 추출된 나머지 부분 복구가능 부호들 및 상기 제1 그룹에 대응하여 생성된 제1 비밀키를 상기 선정된 해시 함수에 입력으로 인가하여 제1 해시 값을 연산하는 검증 해시 값 연산부; 및

상기 추출된 제1 검증 심볼과 상기 제1 해시 값을 비교하여 상기 추출된 제1 검증 심볼이 상기 제1 해시 값과 일치하는 것으로 확인되면, 상기 복원된 제1 부분 복구가능 부호에 대한 복원이 성공인 것으로 판단하고, 상기 복원된 제1 부분 복구가능 부호를 상기 제1 데이터 저장소에 저장하는 복원 부호 저장부

를 더 포함하는 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 장치.

청구항 4

제1항에 있어서,

상기 검증 심볼 데이터 저장소에 저장되어 있는 상기 k개의 검증 심볼들 중 제2 검증 심볼이 손실된 경우, 상기 k개의 그룹들 중 상기 제2 검증 심볼에 대응하는 제2 그룹을 확인하는 그룹 확인부;

상기 n개의 분리된 데이터 저장소들 중 상기 제2 그룹에 속해있는 부분 복구가능 부호들이 저장되어 있는 데이터 저장소들로부터 상기 제2 그룹에 속해있는 부분 복구가능 부호들을 추출하는 추출부;

상기 추출된 제2 그룹에 속해있는 부분 복구가능 부호들과 상기 제2 그룹에 대응하여 생성된 제2 비밀키를 상기 선정된 해시 함수에 입력으로 인가하여 제2 해시 값을 연산한 후 상기 연산된 제2 해시 값을 상기 제2 검증 심볼에 대한 복원 심볼로 결정하는 검증 심볼 복원부; 및

상기 제2 검증 심볼에 대한 복원 심볼을 상기 검증 심볼 데이터 저장소에 저장하는 검증 심볼 저장부를 더 포함하는 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 장치.

청구항 5

입력 데이터에 대한 데이터 저장 명령이 인가되면, 상기 입력 데이터에 대해 부분 복구가능 부호(locally repairable code)의 생성을 위한 인코딩을 수행하여 상기 입력 데이터로부터 n(n은 자연수)개의 부분 복구가능 부호들 - 상기 n개의 부분 복구가능 부호들은 k(k는 자연수)개의 그룹들로 그룹화되어, 각 그룹 내 속해있는 부호들 각각은 동일 그룹 내에 속해있는 나머지 부호들에 의해 복구가 가능하도록 구성됨 - 을 생성하는 단계;

상기 k개의 그룹들 별로, 각 그룹 내 속해있는 부분 복구가능 부호들의 검증을 위한 검증 심볼(symbol)을 생성함으로써, 상기 k개의 그룹들 각각에 대응하는 k개의 검증 심볼들을 생성하는 단계; 및

상기 n개의 부분 복구가능 부호들을 n개의 분리된 데이터 저장소들에 각각 분할하여 저장하고, 상기 k개의 검증 심볼들을 검증 심볼 데이터 저장소에 저장하는 단계

를 포함하고,

상기 검증 심볼들을 생성하는 단계는

상기 k개의 그룹들 각각에 대응되는 서로 다른 k개의 비밀키들을 생성하는 단계; 및

상기 k개의 그룹들 별로, 각 그룹 내에 속해있는 부분 복구가능 부호들과 상기 각 그룹에 대응하는 비밀키를 선정된(predetermined) 해시 함수에 입력으로 인가하여 해시 값을 연산함으로써, 상기 k개의 그룹들 각각에 대응하는 k개의 해시 값들을 생성하고, 상기 생성된 k개의 해시 값들을 상기 k개의 그룹들 각각에 대응하는 상기 k개의 검증 심볼들로 결정하는 단계

를 포함하는 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 방법.

청구항 6

삭제

청구항 7

제5항에 있어서,

상기 n개의 분리된 데이터 저장소들 중 제1 데이터 저장소에 저장되어 있는 제1 부분 복구가능 부호가 손실된 경우, 상기 k개의 그룹들 중 상기 제1 부분 복구가능 부호가 속해있는 제1 그룹을 확인하여 상기 제1 그룹에 속해있는 부분 복구가능 부호들 중 상기 제1 부분 복구가능 부호를 제외한 나머지 부분 복구가능 부호들이 저장되어 있는 데이터 저장소들로부터 상기 나머지 부분 복구가능 부호들을 추출하는 단계;

상기 추출된 나머지 부분 복구가능 부호들에 기초하여 상기 제1 부분 복구가능 부호를 복원하는 단계;

상기 검증 심볼 데이터 저장소로부터 상기 제1 그룹에 대응하는 제1 검증 심볼을 추출하는 단계;

상기 복원된 제1 부분 복구가능 부호와 상기 추출된 나머지 부분 복구가능 부호들 및 상기 제1 그룹에 대응하여 생성된 제1 비밀키를 상기 선정된 해시 함수에 입력으로 인가하여 제1 해시 값을 연산하는 단계; 및

상기 추출된 제1 검증 심볼과 상기 제1 해시 값을 비교하여 상기 추출된 제1 검증 심볼이 상기 제1 해시 값과

일치하는 것으로 확인되면, 상기 복원된 제1 부분 복구가능 부호에 대한 복원이 성공인 것으로 판단하고, 상기 복원된 제1 부분 복구가능 부호를 상기 제1 데이터 저장소에 저장하는 단계

를 더 포함하는 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 방법.

청구항 8

제5항에 있어서,

상기 검증 심볼 데이터 저장소에 저장되어 있는 상기 k개의 검증 심볼들 중 제2 검증 심볼이 손실된 경우, 상기 k개의 그룹들 중 상기 제2 검증 심볼에 대응하는 제2 그룹을 확인하는 단계;

상기 n개의 분리된 데이터 저장소들 중 상기 제2 그룹에 속해있는 부분 복구가능 부호들이 저장되어 있는 데이터 저장소들로부터 상기 제2 그룹에 속해있는 부분 복구가능 부호들을 추출하는 단계;

상기 추출된 제2 그룹에 속해있는 부분 복구가능 부호들과 상기 제2 그룹에 대응하여 생성된 제2 비밀키를 상기 선정된 해시 함수에 입력으로 인가하여 제2 해시 값을 연산한 후 상기 연산된 제2 해시 값을 상기 제2 검증 심볼에 대한 복원 심볼로 결정하는 단계; 및

상기 제2 검증 심볼에 대한 복원 심볼을 상기 검증 심볼 데이터 저장소에 저장하는 단계

를 더 포함하는 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 방법.

청구항 9

제5항, 제7항 또는 제8항 중 어느 한 항의 방법을 수행하는 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

청구항 10

제5항, 제7항 또는 제8항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램.

발명의 설명

기술 분야

[0001] 본 발명은 부분 복구가능 부호(locally repairable code)를 활용하여 데이터를 분산 저장하는 시스템에서 데이터 저장소에 분할 저장되어 있는 특정 부분 복구가능 부호가 손실됨에 따라, 해당 부분 복구가능 부호가 복원될 경우, 복원된 부분 복구가능 부호에 대한 데이터 무결성을 검증하기 위한 기술에 대한 것이다.

배경 기술

[0002] 최근, 인터넷의 보급이 활발하게 이루어짐에 따라, 다양한 인터넷 서비스 제공 업체들이 등장하고 있다. 이러한 인터넷 서비스 제공 업체들은 이메일 서비스를 제공하거나, 블로그, 카페, 클라우드 데이터 저장 서비스 등과 같은 다양한 서비스들을 제공하고 있다.

[0003] 특히, 최근에는 소셜 네트워크 서비스의 인기가 급증함에 따라, 소셜 네트워크 서비스를 제공하는 인터넷 서비스 제공 업체들도 매우 많이 증가하고 있다.

[0004] 이러한 인터넷 서비스 제공 업체들은 이메일 서비스, 블로그, 카페, 클라우드 서비스, 소셜 네트워크 서비스 등을 제공하기 위해 다수의 클라이언트 단말들로부터 업로드되는 대용량의 데이터들을 자체의 데이터 저장소에 저장해야 하는데, 이러한 데이터들이 데이터 저장소 내에서 손실되게 되면, 고객들에게 정상적인 서비스를 제공할 수 없기 때문에 데이터의 손실을 방지하기 위한 노력이 필요하다.

[0005] 이러한 데이터 손실을 방지하기 위한 가장 손쉬운 방법으로는 데이터를 백업하는 방법이 있을 수 있지만, 데이터를 백업하기 위해서는 대용량의 데이터 저장소가 추가로 필요하고, 데이터의 일부가 손실되는 경우에도 데이터 전체에 대해 백업 데이터로 대체를 해야 한다는 점에서 비효율적일 수 밖에 없다.

[0006] 최근에는 대용량의 데이터가 저장되어야 하는 데이터 저장소에서 데이터의 일부가 손실될 경우, 해당 손실된 부분 데이터만을 복구함으로써, 효율적으로 데이터의 손실을 방지할 수 있는 방법으로 부분 복구가능 부호(locally repairable code)가 제안되었다.

- [0007] 부분 복구가능 부호란 데이터 저장소에 저장되어야 하는 입력 데이터에 대해 부분 복구가능 부호로 변환하기 위한 인코딩을 수행하여 상기 입력 데이터로부터 n (n 은 자연수)개 부분 복구가능 부호들을 생성해낸 후 상기 n 개의 부분 복구가능 부호들을 n 개의 분리된 데이터 저장소에 각각 하나씩 저장하는 방식을 말한다.
- [0008] 이때, 상기 n 개의 부분 복구가능 부호들은 k (k 는 자연수)개의 그룹들로 그룹화될 수 있는데, 각 그룹 내 속해있는 부호들 각각은 동일 그룹 내에 속해있는 나머지 부호들에 의해 복구가 가능하도록 구성되어 있다.
- [0009] 관련해서, 도 1을 참조하여 부분 복구가능 부호를 활용해서 데이터를 분산 저장하는 기법에 대해 자세히 설명하면 다음과 같다.
- [0010] 먼저, 소정의 입력 데이터에 대한 저장 명령이 인가되면, 부호 생성 장치(110)는 상기 입력 데이터에 대해 부분 복구가능 부호의 생성을 위한 인코딩을 수행하여 상기 입력 데이터로부터 n 개의 부분 복구가능 부호들을 생성한다.
- [0011] 이때, 상기 n 개의 부분 복구가능 부호들은 k 개의 그룹들로 그룹화될 수 있는데, 각 그룹 내 속해있는 부호들 각각은 동일 그룹 내에 속해있는 나머지 부호들에 의해 복구가 가능하도록 구성되어 있다.
- [0012] 예컨대, 상기 n 을 12, 상기 k 를 4라고 가정하면, 부호 생성 장치(110)는 상기 입력 데이터에 대해 인코딩을 수행하여 12개의 부분 복구가능 부호들을 생성할 수 있는데, 이때, 상기 12개의 부분 복구가능 부호들은 3개의 부호씩 4개의 그룹들로 묶이면서, 4개의 그룹들 내의 부호들 각각은 동일 그룹 내의 다른 부호들에 의해 복구가 가능하도록 구성될 수 있다.
- [0013] 관련해서, "그룹 1"에 포함되어 있는 부분 복구가능 부호들을 "부분 복구가능 부호 1, 부분 복구가능 부호 2, 부분 복구가능 부호 3"이라고 하면, "부분 복구가능 부호 1"이 손실되는 경우, 손실된 "부분 복구가능 부호 1"은 "부분 복구가능 부호 2"와 "부분 복구가능 부호 3"에 의해서 복구가 가능하게 된다.
- [0014] 이렇게, n 개의 부분 복구가능 부호들이 생성되면, 부호 생성 장치(110)는 상기 입력 데이터를 데이터 저장소에 저장하는 것이 아니라, 상기 n 개의 부분 복구가능 부호들을 n 개의 분리된 데이터 저장소들(121, 122, 123, 124, 125, 126)에 하나씩 분할해서 저장하게 된다.
- [0015] 이렇게, n 개의 부분 복구가능 부호들이 n 개의 데이터 저장소들(121, 122, 123, 124, 125, 126)에 하나씩 분할되어 저장된 이후, 특정 부분 복구가능 부호가 손실되게 되면, 상기 특정 부분 복구가능 부호와 동일 그룹에 속해있는 다른 부분 복구가능 부호들을 n 개의 분리된 데이터 저장소들(121, 122, 123, 124, 125, 126)로부터 추출하여 상기 특정 부분 복구가능 부호를 복원할 수 있다.
- [0016] 관련해서, 상기 "그룹 1"에 포함되어 있는 "부분 복구가능 부호 1, 부분 복구가능 부호 2, 부분 복구가능 부호 3"이 순서대로 데이터 저장소 1(121), 데이터 저장소 2(122), 데이터 저장소 3(123)에 저장되었다고 가정하자. 이때, 만약 "부분 복구가능 부호 1"이 손실되게 되면, 손실된 "부분 복구가능 부호 1"은 데이터 저장소 2(122)와 데이터 저장소 3(123)에 각각 저장되어 있는 "부분 복구가능 부호 2"와 "부분 복구가능 부호 3"을 기초로 복구될 수 있다.
- [0017] 결론적으로, 소정의 입력 데이터에 대해서 데이터 저장 명령이 인가되면, 부호 생성 장치(110)는 상기 입력 데이터를 데이터 저장소에 그대로 저장하는 것이 아니라, 상기 입력 데이터를 n 개의 부분 복구가능 부호들로 변환한 후 상기 n 개의 부분 복구가능 부호들을 n 개의 분리된 데이터 저장소들(121, 122, 123, 124, 125, 126)에 각각 하나씩 분할하여 저장함으로써, 특정 부분 복구가능 부호가 손실되는 경우, 나머지 부분 복구가능 부호를 기초로 언제든지 손실된 부분 복구가능 부호를 복구할 수 있도록 지원할 수 있다.
- [0018] 이렇게, 상기 입력 데이터가 상기 n 개의 부분 복구가능 부호들로 변환되어 데이터 저장소 상에 저장된 이후, 상기 입력 데이터에 대한 복원 명령이 인가되면, n 개의 분리된 데이터 저장소들(121, 122, 123, 124, 125, 126)에 저장되어 있는 상기 n 개의 부분 복구가능 부호들을 기초로 상기 n 개의 부분 복구가능 부호들을 생성하기 위해서 수행된 인코딩 기법에 대응하는 디코딩을 수행함으로써, 상기 n 개의 부분 복구가능 부호들로부터 상기 입력 데이터를 복원할 수 있다.
- [0019] 이러한 부분 복구가능 부호들을 생성하는 인코딩 기법은 다양한 기법들이 존재하고 있는데, 그 중 Tamo-Barg 기법은 앞서 설명한 부분 복구가능 부호를 생성하기 위한 기법 중 하나로, 입력 데이터로부터 n 개의 부분 복구가능 부호들을 생성하되, 상기 n 개의 부분 복구가능 부호들이 k 개의 그룹으로 구분되면서, 각 그룹 내의 속하는 각각의 부호들은 동일 그룹 내의 다른 부호들로부터 복구가 가능하도록 수행되는 인코딩 기법이다.

- [0020] 이렇게, 대용량 저장소에 저장되는 데이터에 대한 부분 손실이 발생했을 때, 부분적으로 손실된 데이터만을 복구하는 기법이 도입되었지만, 부분적으로 손실된 데이터가 복구되었을 때, 복구된 데이터가 정말 제대로 복구된 데이터가 맞는지에 대한 데이터의 무결성을 검증하는 기법에 대해서는 아직까지 제안된 연구가 존재하고 있지 않다.
- [0021] 예컨대, 도 1에서 상기 "그룹 1"에 포함되어 있는 "부분 복구가능 부호 1, 부분 복구가능 부호 2, 부분 복구가능 부호 3"이 순서대로 데이터 저장소 1(121), 데이터 저장소 2(122), 데이터 저장소 3(123)에 저장된 이후, "부분 복구가능 부호 1"이 손실됨에 따라 데이터 저장소 2(122)와 데이터 저장소 3(123)에 각각 저장되어 있는 "부분 복구가능 부호 2"와 "부분 복구가능 부호 3"을 기초로 "부분 복구가능 부호 1"을 복구하였다고 가정하자.
- [0022] 이때, 상기 복구된 "부분 복구가능 부호 1"이 정말로 원래 존재하였던 "부분 복구가능 부호 1"과 동일한지 여부를 검증하는 기법이 기존에는 제안되어 있지 않았다.
- [0023] 이로 인해서, 데이터가 n 개의 부분 복구가능 부호들로 구분되어 데이터 저장소에 분할 저장된 이후, 공격자에 의해서 특정 부분 복구가능 부호들이 조작되게 되면, 부분 복구가능 부호의 손실이 발생하여 데이터 복구를 수행할 때, 조작된 부분 복구가능 부호들을 기초로 데이터 복구가 수행되어 잘못된 데이터가 복구되었음에도 불구하고 해당 복구 데이터에 대한 무결성을 검증할 방법이 없어, 잘못 복구된 데이터가 그대로 다시 데이터 저장소에 저장되게 되는 문제가 발생할 수 있다.
- [0024] 따라서, 부분 복구가능 부호를 이용하여 데이터를 분산 저장하는 시스템에서 손실된 부분 복구가능 부호가 복원되었을 때, 복원된 부분 복구가능 부호에 대한 데이터의 무결성을 검증할 수 있는 기법에 대한 연구가 필요하다.

발명의 내용

해결하려는 과제

- [0025] 본 발명은 부분 복구가능 부호(locally repairable code)를 활용하여 데이터를 분산 저장하는 시스템에서 데이터 저장소에 분할 저장되어 있는 특정 부분 복구가능 부호가 손실됨에 따라, 해당 부분 복구가능 부호가 복원될 경우, 복원된 부분 복구가능 부호에 대한 데이터 무결성을 검증할 수 있는 장치 및 방법을 제공하고자 한다.

과제의 해결 수단

- [0026] 본 발명의 일실시예에 따른 부분 복구가능 부호(locally repairable code)의 검증이 가능한 데이터 분산 저장 장치는 입력 데이터에 대한 데이터 저장 명령이 인가되면, 상기 입력 데이터에 대해 부분 복구가능 부호의 생성을 위한 인코딩을 수행하여 상기 입력 데이터로부터 n (n 은 자연수)개의 부분 복구가능 부호들 - 상기 n 개의 부분 복구가능 부호들은 k (k 는 자연수)개의 그룹들로 그룹화되어, 각 그룹 내 속해있는 부호들 각각은 동일 그룹 내에 속해있는 나머지 부호들에 의해 복구가 가능하도록 구성됨 - 을 생성하는 부호 생성부, 상기 k 개의 그룹들 별로, 각 그룹 내 속해있는 부분 복구가능 부호들의 검증을 위한 검증 심볼(symbol)을 생성함으로써, 상기 k 개의 그룹들 각각에 대응하는 k 개의 검증 심볼들을 생성하는 검증 심볼 생성부 및 상기 n 개의 부분 복구가능 부호들을 n 개의 분리된 데이터 저장소들에 각각 분할하여 저장하고, 상기 k 개의 검증 심볼들을 검증 심볼 데이터 저장소에 저장하는 데이터 분산 저장부를 포함한다.
- [0027] 또한, 본 발명의 일실시예에 따른 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 방법은 입력 데이터에 대한 데이터 저장 명령이 인가되면, 상기 입력 데이터에 대해 부분 복구가능 부호의 생성을 위한 인코딩을 수행하여 상기 입력 데이터로부터 n (n 은 자연수)개의 부분 복구가능 부호들 - 상기 n 개의 부분 복구가능 부호들은 k (k 는 자연수)개의 그룹들로 그룹화되어, 각 그룹 내 속해있는 부호들 각각은 동일 그룹 내에 속해있는 나머지 부호들에 의해 복구가 가능하도록 구성됨 - 을 생성하는 단계, 상기 k 개의 그룹들 별로, 각 그룹 내 속해있는 부분 복구가능 부호들의 검증을 위한 검증 심볼을 생성함으로써, 상기 k 개의 그룹들 각각에 대응하는 k 개의 검증 심볼들을 생성하는 단계 및 상기 n 개의 부분 복구가능 부호들을 n 개의 분리된 데이터 저장소들에 각각 분할하여 저장하고, 상기 k 개의 검증 심볼들을 검증 심볼 데이터 저장소에 저장하는 단계를 포함한다.

발명의 효과

- [0028] 본 발명은 부분 복구가능 부호(locally repairable code)를 활용하여 데이터를 분산 저장하는 시스템에서 데이

터 저장소에 분할 저장되어 있는 특정 부분 복구가능 부호가 손실됨에 따라, 해당 부분 복구가능 부호가 복원될 경우, 복원된 부분 복구가능 부호에 대한 데이터 무결성을 검증할 수 있는 장치 및 방법을 제공할 수 있다.

도면의 간단한 설명

[0029] 도 1은 종래의 부분 복구가능 부호(locally repairable code)를 이용한 데이터 분산 저장 기법을 설명하기 위한 도면이다.

도 2는 본 발명의 일실시예에 따른 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 장치의 구조를 도시한 도면이다.

도 3은 본 발명의 일실시예에 따른 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0030] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 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 사용하였다.

[0031] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0032] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0033] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0034] 이하에서, 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다.

[0035] 도 2는 본 발명의 일실시예에 따른 부분 복구가능 부호(locally repairable code)의 검증이 가능한 데이터 분산 저장 장치의 구조를 도시한 도면이다.

[0036] 도 2를 참조하면, 본 발명의 일실시예에 따른 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 장치(210)는 부호 생성부(211), 검증 심볼(symbol) 생성부(212) 및 데이터 분산 저장부(213)를 포함한다.

[0037] 부호 생성부(211)는 입력 데이터에 대한 데이터 저장 명령이 인가되면, 상기 입력 데이터에 대해 부분 복구가능 부호의 생성을 위한 인코딩을 수행하여 상기 입력 데이터로부터 n (n 은 자연수)개의 부분 복구가능 부호들을 생성한다.

[0038] 이때, 상기 n 개의 부분 복구가능 부호들은 k (k 는 자연수)개의 그룹들로 그룹화되어, 각 그룹 내 속해있는 부호들 각각은 동일 그룹 내에 속해있는 나머지 부호들에 의해 복구가 가능하도록 구성된다.

[0039] 검증 심볼 생성부(212)는 상기 k 개의 그룹들 별로, 각 그룹 내 속해있는 부분 복구가능 부호들의 검증을 위한 검증 심볼을 생성함으로써, 상기 k 개의 그룹들 각각에 대응하는 k 개의 검증 심볼들을 생성한다.

[0040] 이때, 본 발명의 일실시예에 따르면, 검증 심볼 생성부(212)는 비밀키 생성부(214) 및 해시 값 연산부(215)를 포함할 수 있다.

[0041] 비밀키 생성부(214)는 상기 k 개의 그룹들 각각에 대응되는 서로 다른 k 개의 비밀키들을 생성한다.

- [0042] 해시 값 연산부(215)는 상기 k개의 그룹들 별로, 각 그룹 내에 속해있는 부분 복구가능 부호들과 상기 각 그룹에 대응하는 비밀키를 선정된(predetermined) 해시 함수에 입력으로 인가하여 해시 값을 연산함으로써, 상기 k개의 그룹들 각각에 대응하는 k개의 해시 값들을 생성하고, 상기 생성된 k개의 해시 값들을 상기 k개의 그룹들 각각에 대응하는 상기 k개의 검증 심볼들로 결정한다.
- [0043] 데이터 분산 저장부(213)는 상기 n개의 부분 복구가능 부호들을 n개의 분리된 데이터 저장소들(231, 232, 233, 234, 235, 236)에 각각 분할하여 저장하고, 상기 k개의 검증 심볼들을 검증 심볼 데이터 저장소(240)에 저장한다.
- [0044] 이때, 본 발명의 일실시예에 따르면, 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 장치(210)는 부호 추출부(216), 부호 복원부(217), 검증 심볼 추출부(218), 검증 해시 값 연산부(219), 복원 부호 저장부(220)를 더 포함할 수 있다.
- [0045] 부호 추출부(216)는 n개의 분리된 데이터 저장소들(231, 232, 233, 234, 235, 236) 중 제1 데이터 저장소에 저장되어 있는 제1 부분 복구가능 부호가 손실된 경우, 상기 k개의 그룹들 중 상기 제1 부분 복구가능 부호가 속해있는 제1 그룹을 확인하여 상기 제1 그룹에 속해있는 부분 복구가능 부호들 중 상기 제1 부분 복구가능 부호를 제외한 나머지 부분 복구가능 부호들이 저장되어 있는 데이터 저장소들로부터 상기 나머지 부분 복구가능 부호들을 추출한다.
- [0046] 부호 복원부(217)는 상기 추출된 나머지 부분 복구가능 부호들에 기초하여 상기 제1 부분 복구가능 부호를 복원한다.
- [0047] 검증 심볼 추출부(218)는 검증 심볼 데이터 저장소(240)로부터 상기 제1 그룹에 대응하는 제1 검증 심볼을 추출한다.
- [0048] 검증 해시 값 연산부(219)는 상기 복원된 제1 부분 복구가능 부호와 상기 추출된 나머지 부분 복구가능 부호들 및 상기 제1 그룹에 대응하여 생성된 제1 비밀키를 상기 선정된 해시 함수에 입력으로 인가하여 제1 해시 값을 연산한다.
- [0049] 복원 부호 저장부(220)는 상기 추출된 제1 검증 심볼과 상기 제1 해시 값을 비교하여 상기 추출된 제1 검증 심볼이 상기 제1 해시 값과 일치하는 것으로 확인되면, 상기 복원된 제1 부분 복구가능 부호에 대한 복원이 성공인 것으로 판단하고, 상기 복원된 제1 부분 복구가능 부호를 상기 제1 데이터 저장소에 저장한다.
- [0050] 또한, 본 발명의 일실시예에 따르면, 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 장치(210)는 그룹 확인부(221), 추출부(222), 검증 심볼 복원부(223) 및 검증 심볼 저장부(224)를 더 포함할 수 있다.
- [0051] 그룹 확인부(221)는 검증 심볼 데이터 저장소(240)에 저장되어 있는 상기 k개의 검증 심볼들 중 제2 검증 심볼이 손실된 경우, 상기 k개의 그룹들 중 상기 제2 검증 심볼에 대응하는 제2 그룹을 확인한다.
- [0052] 추출부(222)는 n개의 분리된 데이터 저장소들(231, 232, 233, 234, 235, 236) 중 상기 제2 그룹에 속해있는 부분 복구가능 부호들이 저장되어 있는 데이터 저장소들로부터 상기 제2 그룹에 속해있는 부분 복구가능 부호들을 추출한다.
- [0053] 검증 심볼 복원부(223)는 상기 추출된 제2 그룹에 속해있는 부분 복구가능 부호들과 상기 제2 그룹에 대응하여 생성된 제2 비밀키를 상기 선정된 해시 함수에 입력으로 인가하여 제2 해시 값을 연산한 후 상기 연산된 제2 해시 값을 상기 제2 검증 심볼에 대한 복원 심볼로 결정한다.
- [0054] 검증 심볼 저장부(224)는 상기 제2 검증 심볼에 대한 복원 심볼을 검증 심볼 데이터 저장소(240)에 저장한다.
- [0055] 이하에서는 본 발명에 따른 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 장치(210)의 동작에 대해 예를 들어 상세히 설명하기로 한다.
- [0056] 먼저, 부호 생성부(211)는 입력 데이터에 대한 데이터 저장 명령이 인가되면, 상기 입력 데이터에 대해 부분 복구가능 부호의 생성을 위한 인코딩을 수행하여 상기 입력 데이터로부터 n(n은 자연수)개의 부분 복구가능 부호들(상기 n개의 부분 복구가능 부호들은 k(k는 자연수)개의 그룹들로 그룹화되어, 각 그룹 내 속해있는 부호들 각각은 동일 그룹 내에 속해있는 나머지 부호들에 의해 복구가 가능하도록 구성됨)을 생성할 수 있다.
- [0057] 관련하여, 상기 n을 12, 상기 k를 4라고 가정하면, 부호 생성부(211)는 상기 입력 데이터에 대해 인코딩을 수행하여 12개의 부분 복구가능 부호들을 생성할 수 있는데, 이때, 상기 12개의 부분 복구가능 부호들은 3개의 부호

씩 4개의 그룹들로 묶이면서, 4개의 그룹들 내의 부호들 각각은 동일 그룹 내의 다른 부호들에 의해 복구가 가능하도록 구성될 수 있다.

- [0058] 예컨대, 상기 4개의 그룹들 중 "그룹 1"에 포함되어 있는 부분 복구가능 부호들을 "부분 복구가능 부호 1, 부분 복구가능 부호 2, 부분 복구가능 부호 3"이라고 하면, "부분 복구가능 부호 1"이 손실되는 경우, 손실된 "부분 복구가능 부호 1"은 "부분 복구가능 부호 2"와 "부분 복구가능 부호 3"에 의해서 복구가 가능하게 된다.
- [0059] 이렇게, 부호 생성부(211)에 의해 상기 12개의 부분 복구가능 부호들이 생성되면, 검증 심볼 생성부(212)에 포함된 비밀키 생성부(214)는 4개의 그룹들 각각에 대응하는 서로 다른 4개의 비밀키들을 생성할 수 있다.
- [0060] 그러고 나서, 검증 심볼 생성부(212)에 포함된 해시 값 연산부(215)는 상기 4개의 그룹들 별로, 각 그룹 내에 속해있는 부분 복구가능 부호들과 상기 각 그룹에 대응하는 비밀키를 상기 선정된 해시 함수에 입력으로 인가하여 해시 값을 연산함으로써, 상기 4개의 그룹들 각각에 대응하는 4개의 해시 값들을 생성할 수 있고, 상기 4개의 해시 값들을 상기 4개의 그룹들 각각에 대응하는 4개의 검증 심볼들로 결정할 수 있다.
- [0061] 관련해서, 비밀키 생성부(214)에 의해 "그룹 1"에 대응하여 생성된 비밀키로 "비밀키 1"이 생성되었다고 가정하면, 해시 값 연산부(215)는 상기 선정된 해시 함수에 대해 "부분 복구가능 부호 1, 부분 복구가능 부호 2, 부분 복구가능 부호 3"과 "비밀키 1"을 입력으로 인가하여 상기 "그룹 1"에 대응하는 해시 값으로 "해시 값 1"을 연산할 수 있다.
- [0062] 이러한 방식으로 해시 값 연산부(215)는 상기 4개의 그룹들 각각에 대응하는 4개의 해시 값을 연산할 수 있고, 상기 4개의 해시 값들을 상기 4개의 그룹들 각각에 대응하는 4개의 검증 심볼들로 결정할 수 있다.
- [0063] 그 이후, 데이터 분산 저장부(213)는 상기 12개의 부분 복구가능 부호들을 12개의 분리된 데이터 저장소들(231, 232, 233, 234, 235, 236)에 각각 분할하여 저장할 수 있고, 상기 4개의 검증 심볼들을 검증 심볼 데이터 저장소(240)에 저장할 수 있다.
- [0064] 이러한 방식으로 본 발명에 따른 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 장치(210)는 입력 데이터에 대한 분산 저장을 수행할 수 있다.
- [0065] 이하에서는 상기 12개의 부분 복구가능 부호들이 12개의 분리된 데이터 저장소들(231, 232, 233, 234, 235, 236)에 각각 분할 저장되고, 상기 4개의 검증 심볼들이 검증 심볼 데이터 저장소(240)에 저장된 이후, 소정의 시간이 경과하여 데이터 저장소 1(231)에 저장되어 있는 "부분 복구가능 부호 1"에 대한 데이터 손실이 발생한 경우를 가정해서 "부분 복구가능 부호 1"이 복구되는 과정을 설명하기로 한다.
- [0066] 데이터 저장소 1(231)에 저장되어 있는 "부분 복구가능 부호 1"이 손실되면, 부호 추출부(216)는 상기 4개의 그룹들 중 "부분 복구가능 부호 1"이 속해 있는 그룹인 "그룹 1"을 확인하여 "그룹 1"에 속해있는 "부분 복구가능 부호 1, 부분 복구가능 부호 2, 부분 복구가능 부호 3" 중에서 "부분 복구가능 부호 1"을 제외한 나머지 부분 복구가능 부호인 "부분 복구가능 부호 2, 부분 복구가능 부호 3"이 저장되어 있는 데이터 저장소 2(232)와 데이터 저장소 3(233)으로부터 "부분 복구가능 부호 2"와 "부분 복구가능 부호 3"을 추출할 수 있다.
- [0067] 그리고, 부호 복원부(217)는 상기 추출된 "부분 복구가능 부호 2"와 "부분 복구가능 부호 3"에 기초하여 "부분 복구가능 부호 1"을 복원할 수 있다.
- [0068] 이때, 검증 심볼 추출부(218)는 검증 심볼 데이터 저장소(240)로부터 "그룹 1"에 대응하는 검증 심볼을 추출할 수 있다. 본 실시예에서는 "그룹 1"에 대응하는 검증 심볼을 "검증 심볼 1"이라고 명하기로 한다. 이때, 상기 "검증 심볼 1"은 앞서 설명한 바와 같이, 해시 값 연산부(215)에 의해 상기 선정된 해시 함수에 "부분 복구가능 부호 1, 부분 복구가능 부호 2, 부분 복구가능 부호 3"과 "비밀키 1"이 입력으로 인가되어 연산된 해시 값인 "해시 값 1"을 의미한다.
- [0069] 그러고 나서, 검증 해시 값 연산부(219)는 상기 복원된 "부분 복구가능 부호 1"과 상기 추출된 "부분 복구가능 부호 2, 부분 복구가능 부호 3" 및 비밀키 생성부(214)에 의해 생성되었던 "그룹 1"에 대응하는 비밀키인 "비밀키 1"을 상기 선정된 해시 함수에 입력으로 인가하여 "검증 해시 값 1"을 연산할 수 있다.
- [0070] 이때, 복원 부호 저장부(220)는 상기 추출된 "검증 심볼 1"과 상기 연산된 "검증 해시 값 1"을 비교하여 상기 추출된 "검증 심볼 1"과 상기 연산된 "검증 해시 값 1"이 일치하는지 여부를 확인할 수 있다.
- [0071] 즉, 복원 부호 저장부(220)는 "검증 심볼 1"에 해당하는 "해시 값 1"과 "검증 해시 값 1"이 서로 일치하는지 여부를 확인할 수 있다.

- [0072] 만약, "검증 심볼 1"과 "검증 해시 값 1"이 서로 일치하는 경우, 복원 부호 저장부(220)는 상기 복원된 "부분 복구가능 부호 1"에 대한 복원이 성공인 것으로 판단하고, 상기 복원된 "부분 복구가능 부호 1"을 데이터 저장소 1(231)에 저장할 수 있다.
- [0073] 결국, 본 발명에 따른 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 장치(210)는 상기 "검증 심볼 1"을 기초로 상기 복원된 "부분 복구가능 부호 1"이 제대로 복원된 데이터가 맞는지 여부를 확인함으로써, 복원된 데이터에 대한 무결성을 검증할 수 있다.
- [0074] 이렇게, 본 발명에 따른 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 장치(210)는 검증 심볼 데이터 저장소(240)에 저장된 상기 4개의 그룹들 각각에 대응하는 4개의 검증 심볼들을 기초로 특정 부분 복구가능 부호의 손실이 발생함에 따라 복원된 데이터에 대한 무결성 검증을 수행할 수 있지만, 이와 동시에 검증 심볼 데이터 저장소(240)에 저장되어 있는 상기 4개의 검증 심볼들에 대해서 손실이 발생하였을 때, 12개의 분리된 데이터 저장소들(231, 232, 233, 234, 235, 236)에 저장되어 있는 상기 12개의 부분 복구가능 부호들에 기초하여 손실이 발생한 검증 심볼을 다시 생성할 수도 있다.
- [0075] 관련해서, 검증 심볼 데이터 저장소(240)에 저장되어 있는 상기 4개의 검증 심볼들 중 "검증 심볼 1"에 대한 데이터 손실이 발생하여 "검증 심볼 1"이 재생성되는 예를 설명하기로 한다.
- [0076] 검증 심볼 데이터 저장소(240)에 저장되어 있는 상기 4개의 검증 심볼들 중 "검증 심볼 1"이 손실된 경우, 그룹 확인부(221)는 상기 4개의 그룹들 중 "검증 심볼 1"에 대응하는 그룹인 "그룹 1"을 확인할 수 있다.
- [0077] 그리고, 추출부(222)는 12개의 분리된 데이터 저장소들(231, 232, 233, 234, 235, 236) 중 "그룹 1"에 속해 있는 부분 복구가능 부호들인 "부분 복구가능 부호 1, 부분 복구가능 부호 2, 부분 복구가능 부호 3"이 저장되어 있는 데이터 저장소인 데이터 저장소 1(231), 데이터 저장소 2(232), 데이터 저장소 3(233)으로부터 "부분 복구가능 부호 1, 부분 복구가능 부호 2, 부분 복구가능 부호 3"을 추출할 수 있다.
- [0078] 이때, 검증 심볼 복원부(223)는 상기 추출된 "부분 복구가능 부호 1, 부분 복구가능 부호 2, 부분 복구가능 부호 3"과 비밀키 생성부(214)에 의해서 생성되었던 "그룹 1"에 대응하는 "비밀키 1"을 상기 선정된 해시 함수에 입력으로 인가하여 "복원 해시 값 1"을 연산한 후 상기 연산된 "복원 해시 값 1"을 상기 손실된 "검증 심볼 1"에 대한 복원 심볼로 결정할 수 있다.
- [0079] 그러고 나서, 검증 심볼 저장부(224)는 상기 손실된 "검증 심볼 1"에 대한 복원 심볼을 검증 심볼 데이터 저장소(240)에 저장할 수 있다.
- [0080] 이를 통해, 본 발명에 따른 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 장치(210)는 검증 심볼 데이터 저장소(240)에 저장된 검증 심볼들에 대한 손실이 발생하더라도 12개의 분리된 데이터 저장소들(231, 232, 233, 234, 235, 236)에 분할 저장되어 있는 부분 복구가능 부호들과 비밀키 생성부(214)가 생성한 각 그룹별 대응 비밀키를 기초로 손실된 검증 심볼을 다시 생성할 수 있다.
- [0081] 도 3은 본 발명의 일실시예에 따른 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 방법을 도시한 순서도이다.
- [0082] 단계(S310)에서는 입력 데이터에 대한 데이터 저장 명령이 인가되면, 상기 입력 데이터에 대해 부분 복구가능 부호의 생성을 위한 인코딩을 수행하여 상기 입력 데이터로부터 n (n 은 자연수)개의 부분 복구가능 부호들(상기 n 개의 부분 복구가능 부호들은 k (k 는 자연수)개의 그룹들로 그룹화되어, 각 그룹 내 속해있는 부호들 각각은 동일 그룹 내에 속해있는 나머지 부호들에 의해 복구가 가능하도록 구성됨)을 생성한다.
- [0083] 단계(S320)에서는 상기 k 개의 그룹들 별로, 각 그룹 내 속해있는 부분 복구가능 부호들의 검증을 위한 검증 심볼을 생성함으로써, 상기 k 개의 그룹들 각각에 대응하는 k 개의 검증 심볼들을 생성한다.
- [0084] 단계(S330)에서는 상기 n 개의 부분 복구가능 부호들을 n 개의 분리된 데이터 저장소들에 각각 분할하여 저장하고, 상기 k 개의 검증 심볼들을 검증 심볼 데이터 저장소에 저장한다.
- [0085] 이때, 본 발명의 일실시예에 따르면, 단계(S320)에서는 상기 k 개의 그룹들 각각에 대응되는 서로 다른 k 개의 비밀키들을 생성하는 단계 및 상기 k 개의 그룹들 별로, 각 그룹 내에 속해있는 부분 복구가능 부호들과 상기 각 그룹에 대응하는 비밀키를 선정된 해시 함수에 입력으로 인가하여 해시 값을 연산함으로써, 상기 k 개의 그룹들 각각에 대응하는 k 개의 해시 값들을 생성하고, 상기 생성된 k 개의 해시 값들을 상기 k 개의 그룹들 각각에 대응하는 상기 k 개의 검증 심볼들로 결정하는 단계를 포함할 수 있다.

- [0086] 이때, 본 발명의 일실시예에 따르면, 상기 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 방법은 단계(S330)이후에 상기 n개의 분리된 데이터 저장소들 중 제1 데이터 저장소에 저장되어 있는 제1 부분 복구가능 부호가 손실된 경우, 상기 k개의 그룹들 중 상기 제1 부분 복구가능 부호가 속해있는 제1 그룹을 확인하여 상기 제1 그룹에 속해있는 부분 복구가능 부호들 중 상기 제1 부분 복구가능 부호를 제외한 나머지 부분 복구가능 부호들이 저장되어 있는 데이터 저장소들로부터 상기 나머지 부분 복구가능 부호들을 추출하는 단계, 상기 추출된 나머지 부분 복구가능 부호들에 기초하여 상기 제1 부분 복구가능 부호를 복원하는 단계, 상기 검증 심볼 데이터 저장소로부터 상기 제1 그룹에 대응하는 제1 검증 심볼을 추출하는 단계, 상기 복원된 제1 부분 복구가능 부호와 상기 추출된 나머지 부분 복구가능 부호들 및 상기 제1 그룹에 대응하여 생성된 제1 비밀키를 상기 선정된 해시 함수에 입력으로 인가하여 제1 해시 값을 연산하는 단계 및 상기 추출된 제1 검증 심볼과 상기 제1 해시 값을 비교하여 상기 추출된 제1 검증 심볼이 상기 제1 해시 값과 일치하는 것으로 확인되면, 상기 복원된 제1 부분 복구가능 부호에 대한 복원이 성공인 것으로 판단하고, 상기 복원된 제1 부분 복구가능 부호를 상기 제1 데이터 저장소에 저장하는 단계를 더 포함할 수 있다.
- [0087] 또한, 본 발명의 일실시예에 따르면, 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 방법은 단계(S330)이후에 상기 검증 심볼 데이터 저장소에 저장되어 있는 상기 k개의 검증 심볼들 중 제2 검증 심볼이 손실된 경우, 상기 k개의 그룹들 중 상기 제2 검증 심볼에 대응하는 제2 그룹을 확인하는 단계, 상기 n개의 분리된 데이터 저장소들 중 상기 제2 그룹에 속해있는 부분 복구가능 부호들이 저장되어 있는 데이터 저장소들로부터 상기 제2 그룹에 속해있는 부분 복구가능 부호들을 추출하는 단계, 상기 추출된 제2 그룹에 속해있는 부분 복구가능 부호들과 상기 제2 그룹에 대응하여 생성된 제2 비밀키를 상기 선정된 해시 함수에 입력으로 인가하여 제2 해시 값을 연산한 후 상기 연산된 제2 해시 값을 상기 제2 검증 심볼에 대한 복원 심볼로 결정하는 단계 및 상기 제2 검증 심볼에 대한 복원 심볼을 상기 검증 심볼 데이터 저장소에 저장하는 단계를 더 포함할 수 있다.
- [0088] 이상, 도 3을 참조하여 본 발명의 일실시예에 따른 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 방법에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 방법은 도 2를 이용하여 설명한 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 장치(210)의 동작에 대한 구성과 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.
- [0089] 본 발명의 일실시예에 따른 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 방법은 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다.
- [0090] 또한, 본 발명의 일실시예에 따른 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 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. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [0091] 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.
- [0092] 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.

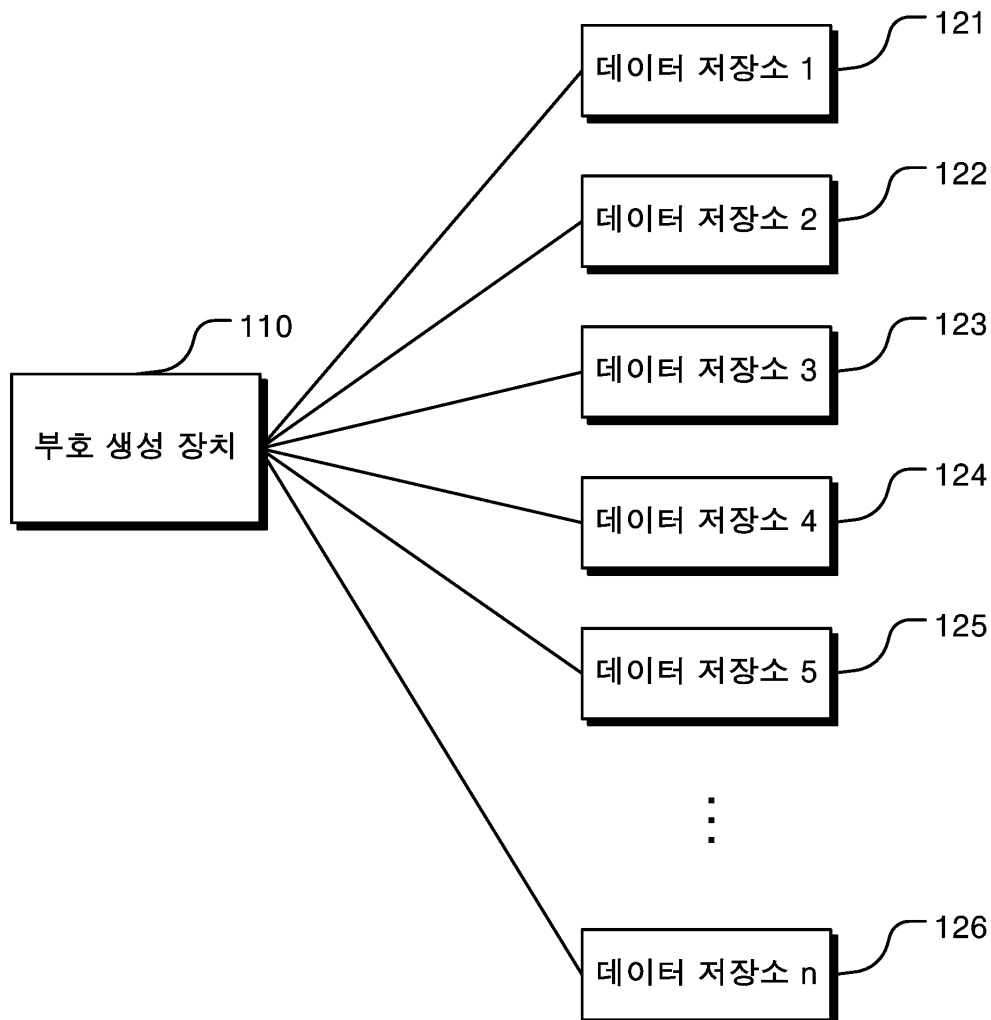
부호의 설명

- [0093] 110: 부호 생성 장치
- 121, 122, 123, 124, 125, 126: n개의 분리된 데이터 저장소들

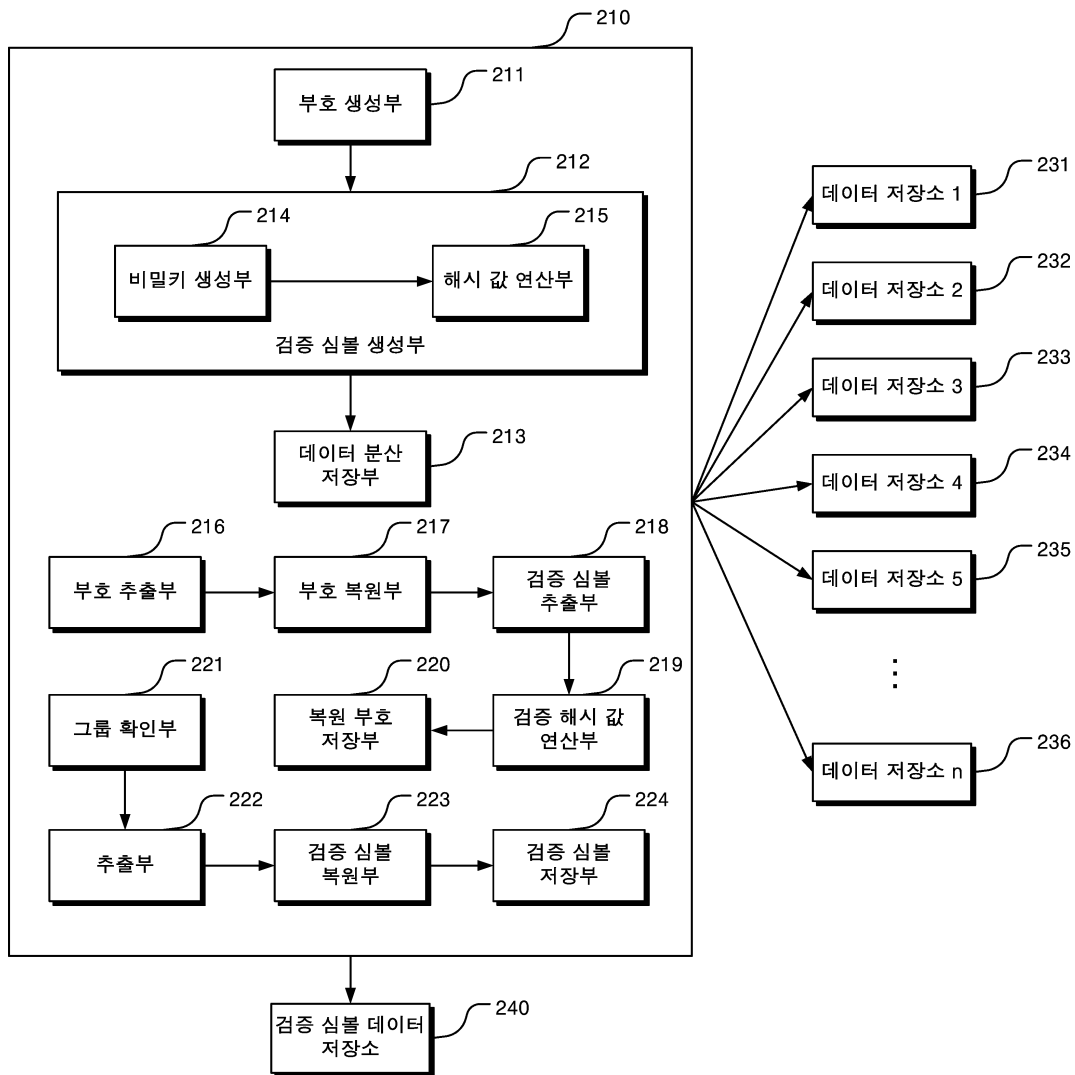
210: 부분 복구가능 부호의 검증이 가능한 데이터 분산 저장 장치
 211: 부호 생성부
 212: 검증 심볼 생성부
 213: 데이터 분산 저장부
 214: 비밀키 생성부
 215: 해시 값 연산부
 216: 부호 추출부
 217: 부호 복원부
 218: 검증 심볼 추출부
 219: 검증 해시 값 연산부
 220: 복원 부호 저장부
 221: 그룹 확인부
 222: 추출부
 223: 검증 심볼 복원부
 224: 검증 심볼 저장부
 231, 232, 233, 234, 235, 236: n개의 분리된 데이터 저장소들

도면

도면1



도면2



도면3

