



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0098782
(43) 공개일자 2018년09월05일

(51) 국제특허분류(Int. Cl.)
G06F 21/60 (2013.01) G06F 21/62 (2013.01)
(52) CPC특허분류
G06F 21/602 (2013.01)
G06F 21/6209 (2013.01)
(21) 출원번호 10-2017-0025322
(22) 출원일자 2017년02월27일
심사청구일자 2017년02월27일

(71) 출원인
주식회사 한컴시큐어
경기도 성남시 분당구 대왕판교로644번길 49 ,
9층(삼평동, 한컴타워)
(72) 발명자
나형수
서울특별시 송파구 성내천로42길 17, 비동 501호
(마천동, 푸르메하우스)
(74) 대리인
김효성

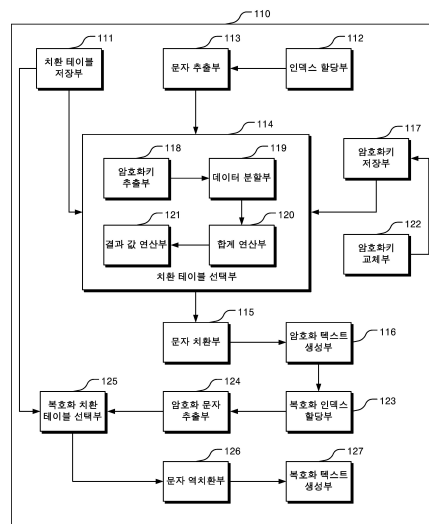
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 장문 텍스트열에 대한 고정 길이 암호화 장치 및 방법

(57) 요약

장문 텍스트열에 대한 고정 길이 암호화 장치 및 방법이 개시된다. 본 발명은 중요 정보가 포함된 장문의 텍스트열에서 중요 정보만을 선별해서 암호화하고, 나머지 정보들은 평문의 형태로 묶으로써, 추후 관리자가 상기 장문의 텍스트열을 열람할 때, 중요 정보만이 암호화되어 있는 텍스트열을 열람할 수 있도록 함으로써, 해당 텍스트열의 전체적인 문맥을 신속하게 파악할 수 있도록 지원함과 동시에, 중요 정보 노출에 따른 보안상의 위험을 최소화할 수 있는 암호화 기법을 제공할 수 있다.

대표도 - 도1



(52) CPC특허분류
G06F 21/6245 (2013.01)

명세서

청구범위

청구항 1

n (n 은 2이상의 자연수)개의 서로 다른 치환 테이블들 - 상기 치환 테이블은 복수의 숫자들과 복수의 영문자들 각각에 대해 치환 대상이 되는 다른 숫자 또는 영문자를 대응시켜 기록한 테이블로, 상기 n 개의 치환 테이블들 각각에는 상기 복수의 숫자들과 상기 복수의 영문자들 각각에 대한 치환 대상이 되는 숫자 또는 영문자들이 서로 다르게 대응되어 기록되어 있음 - 이 저장되어 있는 치환 테이블 저장부;

복수의 문자들로 구성된 텍스트열에 대한 암호화 명령이 입력되면, 상기 복수의 문자들 각각에 대해 각 문자의 나열 순번에 기초한 고유의 인덱스 값을 할당하는 인덱스 할당부;

상기 복수의 문자들 중 숫자와 영문자로 구성된 적어도 하나의 제1 문자를 추출하는 문자 추출부;

상기 n 개의 치환 테이블들 중 어느 하나인 제1 치환 테이블을 선택하는 치환 테이블 선택부;

상기 제1 치환 테이블에 기초하여 상기 적어도 하나의 제1 문자 각각을 상기 제1 치환 테이블에 기록되어 있는 치환 대상이 되는 다른 숫자 또는 영문자로 치환함으로써, 적어도 하나의 치환 문자를 생성하고, 상기 적어도 하나의 치환 문자 각각에 대해 상기 적어도 하나의 제1 문자 각각에 할당되어 있는 인덱스 값과 동일한 인덱스 값을 할당하는 문자 치환부; 및

적어도 하나의 제2 문자 - 상기 적어도 하나의 제2 문자는 상기 복수의 문자들 중 상기 적어도 하나의 제1 문자를 제외한 나머지 문자임 - 각각에 할당되어 있는 인덱스 값과 상기 적어도 하나의 치환 문자 각각에 할당되어 있는 인덱스 값에 기초한 나열 순번에 따라 상기 적어도 하나의 제2 문자와 상기 적어도 하나의 치환 문자를 일렬로 나열함으로써, 암호화된 텍스트열을 생성하는 암호화 텍스트 생성부

를 포함하는 장문 텍스트열에 대한 고정 길이 암호화 장치.

청구항 2

제1항에 있어서,

상기 n 개의 치환 테이블들 각각에는 서로 다른 순번 값이 할당되어 있고,

상기 장문 텍스트열에 대한 고정 길이 암호화 장치는

선정된(predetermined) 암호화키가 저장되어 있는 암호화키 저장부

를 더 포함하며,

상기 치환 테이블 선택부는

상기 암호화키 저장부에 저장되어 있는 상기 선정된 암호화키를 추출하고, 상기 선정된 암호화키에 대해 n 을 제수(divisor)로 하는 모듈러(modular) 연산을 수행함으로써, 결과 값을 연산한 후 상기 n 개의 치환 테이블들 중 상기 결과 값과 일치하는 순번 값이 할당되어 있는 치환 테이블을 상기 제1 치환 테이블로 선택하는 장문 텍스트열에 대한 고정 길이 암호화 장치.

청구항 3

제2항에 있어서,

상기 치환 테이블 선택부는

상기 암호화키 저장부에 저장되어 있는 상기 선정된 암호화키를 추출하는 암호화키 추출부;

상기 선정된 암호화키를 구성하는 데이터 값을 선정된 데이터 크기 단위로 분할하여 복수의 분할 데이터들을 생성하는 데이터 분할부;

상기 복수의 분할 데이터들 각각을 십진수의 숫자 데이터로 변환하고, 십진수의 숫자 데이터로 변환된 상기 복

수의 분할 데이터들의 총합을 연산하는 합계 연산부; 및

상기 연산된 총합에 대해 n 을 제수로 하는 모듈러 연산을 수행함으로써, 상기 결과 값을 연산하는 결과 값 연산부

를 포함하는 장문 텍스트열에 대한 고정 길이 암호화 장치.

청구항 4

제2항에 있어서,

선정된 주기 간격으로, 암호화키를 랜덤하게 생성한 후 상기 암호화키 저장부 상에 저장되어 있는 상기 선정된 암호화키를 상기 랜덤하게 생성된 암호화키로 교체하는 암호화키 교체부

를 더 포함하는 장문 텍스트열에 대한 고정 길이 암호화 장치.

청구항 5

제2항에 있어서,

상기 암호화된 텍스트열에 대한 복호화 명령이 입력되면, 상기 암호화된 텍스트열을 구성하는 복수의 암호화 문자들 각각에 대해 각 문자의 나열 순번에 기초한 고유의 인덱스 값을 할당하는 복호화 인덱스 할당부;

상기 복수의 암호화 문자들 중 숫자와 영문자로 구성된 적어도 하나의 제1 암호화 문자를 추출하는 암호화 문자 추출부;

상기 암호화키 저장부에 저장되어 있는 상기 선정된 암호화키를 추출하고, 상기 선정된 암호화키에 대해 n 을 제수로 하는 모듈러 연산을 수행함으로써, 결과 값을 연산한 후 상기 n 개의 치환 테이블들 중 상기 결과 값과 일치하는 순번 값이 할당되어 어느 하나의 치환 테이블을 선택함으로써, 상기 제1 치환 테이블을 선택하는 복호화 치환 테이블 선택부;

상기 제1 치환 테이블에 기초하여 상기 적어도 하나의 제1 암호화 문자 각각을 상기 제1 치환 테이블에 기록되어 있는 치환 대상이 되는 숫자 또는 영문자에 대응하는 원본 숫자 또는 영문자로 역치환함으로써, 적어도 하나의 원본 문자를 생성하고, 상기 적어도 하나의 원본 문자 각각에 대해 상기 적어도 하나의 제1 암호화 문자 각각에 할당되어 있는 인덱스 값과 동일한 인덱스 값을 할당하는 문자 역치환부; 및

적어도 하나의 제2 암호화 문자 - 상기 적어도 하나의 제2 암호화 문자는 상기 복수의 암호화 문자들 중 상기 적어도 하나의 제1 암호화 문자를 제외한 나머지 문자임 - 각각에 할당되어 있는 인덱스 값과 상기 적어도 하나의 원본 문자 각각에 할당되어 있는 인덱스 값에 기초한 나열 순번에 따라 상기 적어도 하나의 제2 암호화 문자와 상기 적어도 하나의 원본 문자를 일렬로 나열함으로써, 복호화된 텍스트열을 생성하는 복호화 텍스트 생성부를 더 포함하는 장문 텍스트열에 대한 고정 길이 암호화 장치.

청구항 6

n (n 은 2이상의 자연수)개의 서로 다른 치환 테이블들 - 상기 치환 테이블은 복수의 숫자들과 복수의 영문자들 각각에 대해 치환 대상이 되는 다른 숫자 또는 영문자를 대응시켜 기록한 테이블로, 상기 n 개의 치환 테이블들 각각에는 상기 복수의 숫자들과 상기 복수의 영문자들 각각에 대한 치환 대상이 되는 숫자 또는 영문자들이 서로 다르게 대응되어 기록되어 있음 - 이 저장되어 있는 치환 테이블 저장부를 유지하는 단계;

복수의 문자들로 구성된 텍스트열에 대한 암호화 명령이 입력되면, 상기 복수의 문자들 각각에 대해 각 문자의 나열 순번에 기초한 고유의 인덱스 값을 할당하는 단계;

상기 복수의 문자들 중 숫자와 영문자로 구성된 적어도 하나의 제1 문자를 추출하는 단계;

상기 n 개의 치환 테이블들 중 어느 하나인 제1 치환 테이블을 선택하는 단계;

상기 제1 치환 테이블에 기초하여 상기 적어도 하나의 제1 문자 각각을 상기 제1 치환 테이블에 기록되어 있는 치환 대상이 되는 다른 숫자 또는 영문자로 치환함으로써, 적어도 하나의 치환 문자를 생성하고, 상기 적어도 하나의 치환 문자 각각에 대해 상기 적어도 하나의 제1 문자 각각에 할당되어 있는 인덱스 값과 동일한 인덱스 값을 할당하는 단계; 및

적어도 하나의 제2 문자 - 상기 적어도 하나의 제2 문자는 상기 복수의 문자들 중 상기 적어도 하나의 제1 문자를 제외한 나머지 문자임 - 각각에 할당되어 있는 인덱스 값과 상기 적어도 하나의 치환 문자 각각에 할당되어 있는 인덱스 값에 기초한 나열 순번에 따라 상기 적어도 하나의 제2 문자와 상기 적어도 하나의 치환 문자를 일렬로 나열함으로써, 암호화된 텍스트열을 생성하는 단계

를 포함하는 장문 텍스트열에 대한 고정 길이 암호화 방법.

청구항 7

제6항에 있어서,

상기 n개의 치환 테이블들 각각에는 서로 다른 순번 값이 할당되어 있고,

상기 장문 텍스트열에 대한 고정 길이 암호화 방법은

선정된(predetermined) 암호화키가 저장되어 있는 암호화키 저장부를 유지하는 단계

를 더 포함하며,

상기 선택하는 단계는

상기 암호화키 저장부에 저장되어 있는 상기 선정된 암호화키를 추출하고, 상기 선정된 암호화키에 대해 n을 제수(divisor)로 하는 모듈러(modular) 연산을 수행함으로써, 결과 값을 연산한 후 상기 n개의 치환 테이블들 중 상기 결과 값과 일치하는 순번 값이 할당되어 있는 치환 테이블을 상기 제1 치환 테이블로 선택하는 장문 텍스트열에 대한 고정 길이 암호화 방법.

청구항 8

제7항에 있어서,

상기 선택하는 단계는

상기 암호화키 저장부에 저장되어 있는 상기 선정된 암호화키를 추출하는 단계;

상기 선정된 암호화키를 구성하는 데이터 값을 선정된 데이터 크기 단위로 분할하여 복수의 분할 데이터들을 생성하는 단계;

상기 복수의 분할 데이터들 각각을 십진수의 숫자 데이터로 변환하고, 십진수의 숫자 데이터로 변환된 상기 복수의 분할 데이터들의 총합을 연산하는 단계; 및

상기 연산된 총합에 대해 n을 제수로 하는 모듈러 연산을 수행함으로써, 상기 결과 값을 연산하는 단계

를 포함하는 장문 텍스트열에 대한 고정 길이 암호화 방법.

청구항 9

제7항에 있어서,

선정된 주기 간격으로, 암호화키를 랜덤하게 생성한 후 상기 암호화키 저장부 상에 저장되어 있는 상기 선정된 암호화키를 상기 랜덤하게 생성된 암호화키로 교체하는 단계

를 더 포함하는 장문 텍스트열에 대한 고정 길이 암호화 방법.

청구항 10

제7항에 있어서,

상기 암호화된 텍스트열에 대한 복호화 명령이 입력되면, 상기 암호화된 텍스트열을 구성하는 복수의 암호화 문자들 각각에 대해 각 문자의 나열 순번에 기초한 고유의 인덱스 값을 할당하는 단계;

상기 복수의 암호화 문자들 중 숫자와 영문자로 구성된 적어도 하나의 제1 암호화 문자를 추출하는 단계;

상기 암호화키 저장부에 저장되어 있는 상기 선정된 암호화키를 추출하고, 상기 선정된 암호화키에 대해 n을 제수로 하는 모듈러 연산을 수행함으로써, 결과 값을 연산한 후 상기 n개의 치환 테이블들 중 상기 결과 값과 일

치하는 순번 값이 할당되어 어느 하나의 치환 테이블을 선택함으로써, 상기 제1 치환 테이블을 선택하는 단계;

상기 제1 치환 테이블에 기초하여 상기 적어도 하나의 제1 암호화 문자 각각을 상기 제1 치환 테이블에 기록되어 있는 치환 대상이 되는 숫자 또는 영문자에 대응하는 원본 숫자 또는 영문자로 역치환함으로써, 적어도 하나의 원본 문자를 생성하고, 상기 적어도 하나의 원본 문자 각각에 대해 상기 적어도 하나의 제1 암호화 문자 각각에 할당되어 있는 인덱스 값과 동일한 인덱스 값을 할당하는 단계; 및

적어도 하나의 제2 암호화 문자 - 상기 적어도 하나의 제2 암호화 문자는 상기 복수의 암호화 문자들 중 상기 적어도 하나의 제1 암호화 문자를 제외한 나머지 문자임 - 각각에 할당되어 있는 인덱스 값과 상기 적어도 하나의 원본 문자 각각에 할당되어 있는 인덱스 값에 기초한 나열 순번에 따라 상기 적어도 하나의 제2 암호화 문자와 상기 적어도 하나의 원본 문자를 일렬로 나열함으로써, 복호화된 텍스트열을 생성하는 단계

를 더 포함하는 장문 텍스트열에 대한 고정 길이 암호화 방법.

청구항 11

제6항 내지 제10항 중 어느 한 항의 방법을 수행하는 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 장문의 텍스트열에 대해서 효율적으로 암호화를 수행할 수 있도록 지원하는 기술에 대한 것이다.

배경 기술

[0002] 최근, 개인 정보 노출과 관련된 다양한 피해 사례가 증가함에 따라, 개인 정보 노출을 방지하기 위한 암호화 기술의 중요성이 증대되고 있다.

[0003] 특히, 최근에는 키로깅(Keylogging), 스니핑(Sniffing), 피싱(Phishing) 등 점차 고도화되어 가고 있는 해킹 기술로 인해 개인 정보가 유출되어 경제적, 사회적 피해가 발생하는 경우가 비일비재하여 개인 정보 보호의 필요성이 증가하고 있다.

[0004] 일반적으로, 은행 등과 같은 곳에서는 고객들의 개인 정보를 데이터베이스에 저장할 때, 소정의 암호화키를 이용하여 고객들의 개인 정보를 암호화한 후 저장한다.

[0005] 보통, 은행의 상담원들이 고객들과 통화를 하거나 상담을 하면서, 고객들의 개인 정보가 포함된 상담 내용을 메모 형태로 고객 관리 시스템 상에 입력하는 경우, 상담 내용에 따른 장문의 텍스트열 전체가 암호화되어 고객 데이터베이스에 저장되거나, 아예 상담 내용에 따른 장문의 텍스트열이 암호화되지 않은 상태로 고객 데이터베이스에 저장되곤 한다.

[0006] 만약, 장문의 텍스트열 전체가 암호화되어 고객 데이터베이스에 저장되는 경우, 상담원들이 자신이 남긴 메모를 열람하고자할 때, 암호화되어 있는 텍스트열을 보게 됨에 따라, 해당 메모의 내용을 파악하기가 쉽지 않고, 암호화되어 있는 텍스트열을 복호화해서 본다고 하는 경우, 해당 메모의 내용은 쉽게 파악할 수 있지만, 장문의 텍스트열의 복호화에 따른 시간이 소요되기 때문에 빠르게 메모 내용을 확인하기가 어렵다.

[0007] 반대로, 장문의 텍스트열이 암호화되지 않은 상태로 고객 데이터베이스에 저장되는 경우, 상담원들은 자신이 남긴 메모의 내용을 빠르게 열람해서 볼 수 있지만, 메모 내에 포함되어 있는 개인 정보가 쉽게 노출될 수 있는 보안상의 위험이 존재한다.

[0008] 따라서, 고객들의 개인 정보 등과 같은 중요 정보가 포함된 장문의 텍스트열을 데이터베이스 저장할 때, 해당 텍스트열에서 중요 정보만을 선별해서 암호화하고, 나머지 정보들은 평문의 형태로 둬으로써, 추후 관리자가 자신이 남긴 메모를 열람할 때, 중요 정보만이 암호화되어 있는 텍스트열을 열람할 수 있도록 함으로써, 해당 메모의 전체적인 문맥을 신속하게 파악할 수 있도록 지원함과 동시에, 중요 정보 노출에 따른 보안상의 위험을 최

소화할 수 있도록 하는 암호화 기법에 대한 연구가 필요하다.

발명의 내용

해결하려는 과제

[0009] 본 발명은 중요 정보가 포함된 장문의 텍스트열에서 중요 정보만을 선별해서 암호화하고, 나머지 정보들은 평문의 형태로 둬으로써, 추후 관리자가 상기 장문의 텍스트열을 열람할 때, 중요 정보만이 암호화되어 있는 텍스트열을 열람할 수 있도록 함으로써, 해당 텍스트열의 전체적인 문맥을 신속하게 파악할 수 있도록 지원함과 동시에, 중요 정보 노출에 따른 보안상의 위험을 최소화할 수 있는 암호화 기법을 제공하고자 한다.

과제의 해결 수단

[0010] 본 발명의 일실시예에 따른 장문 텍스트열에 대한 고정 길이 암호화 장치는 n (n 은 2이상의 자연수)개의 서로 다른 치환 테이블들 - 상기 치환 테이블은 복수의 숫자들과 복수의 영문자들 각각에 대해 치환 대상이 되는 다른 숫자 또는 영문자를 대응시켜 기록한 테이블로, 상기 n 개의 치환 테이블들 각각에는 상기 복수의 숫자들과 상기 복수의 영문자들 각각에 대한 치환 대상이 되는 숫자 또는 영문자들이 서로 다르게 대응되어 기록되어 있음 - 이 저장되어 있는 치환 테이블 저장부, 복수의 문자들로 구성된 텍스트열에 대한 암호화 명령이 입력되면, 상기 복수의 문자들 각각에 대해 각 문자의 나열 순번에 기초한 고유의 인덱스 값을 할당하는 인덱스 할당부, 상기 복수의 문자들 중 숫자와 영문자로 구성된 적어도 하나의 제1 문자를 추출하는 문자 추출부, 상기 n 개의 치환 테이블들 중 어느 하나인 제1 치환 테이블을 선택하는 치환 테이블 선택부, 상기 제1 치환 테이블에 기초하여 상기 적어도 하나의 제1 문자 각각을 상기 제1 치환 테이블에 기록되어 있는 치환 대상이 되는 다른 숫자 또는 영문자로 치환함으로써, 적어도 하나의 치환 문자를 생성하고, 상기 적어도 하나의 치환 문자 각각에 대해 상기 적어도 하나의 제1 문자 각각에 할당되어 있는 인덱스 값과 동일한 인덱스 값을 할당하는 문자 치환부 및 적어도 하나의 제2 문자 - 상기 적어도 하나의 제2 문자는 상기 복수의 문자들 중 상기 적어도 하나의 제1 문자를 제외한 나머지 문자임 - 각각에 할당되어 있는 인덱스 값과 상기 적어도 하나의 치환 문자 각각에 할당되어 있는 인덱스 값에 기초한 나열 순번에 따라 상기 적어도 하나의 제2 문자와 상기 적어도 하나의 치환 문자를 일렬로 나열함으로써, 암호화된 텍스트열을 생성하는 암호화 텍스트 생성부를 포함한다.

[0011] 또한, 본 발명의 일실시예에 따른 장문 텍스트열에 대한 고정 길이 암호화 방법은 n (n 은 2이상의 자연수)개의 서로 다른 치환 테이블들 - 상기 치환 테이블은 복수의 숫자들과 복수의 영문자들 각각에 대해 치환 대상이 되는 다른 숫자 또는 영문자를 대응시켜 기록한 테이블로, 상기 n 개의 치환 테이블들 각각에는 상기 복수의 숫자들과 상기 복수의 영문자들 각각에 대한 치환 대상이 되는 숫자 또는 영문자들이 서로 다르게 대응되어 기록되어 있음 - 이 저장되어 있는 치환 테이블 저장부를 유지하는 단계, 복수의 문자들로 구성된 텍스트열에 대한 암호화 명령이 입력되면, 상기 복수의 문자들 각각에 대해 각 문자의 나열 순번에 기초한 고유의 인덱스 값을 할당하는 단계, 상기 복수의 문자들 중 숫자와 영문자로 구성된 적어도 하나의 제1 문자를 추출하는 단계, 상기 n 개의 치환 테이블들 중 어느 하나인 제1 치환 테이블을 선택하는 단계, 상기 제1 치환 테이블에 기초하여 상기 적어도 하나의 제1 문자 각각을 상기 제1 치환 테이블에 기록되어 있는 치환 대상이 되는 다른 숫자 또는 영문자로 치환함으로써, 적어도 하나의 치환 문자를 생성하고, 상기 적어도 하나의 치환 문자 각각에 대해 상기 적어도 하나의 제1 문자 각각에 할당되어 있는 인덱스 값과 동일한 인덱스 값을 할당하는 단계 및 적어도 하나의 제2 문자 - 상기 적어도 하나의 제2 문자는 상기 복수의 문자들 중 상기 적어도 하나의 제1 문자를 제외한 나머지 문자임 - 각각에 할당되어 있는 인덱스 값과 상기 적어도 하나의 치환 문자 각각에 할당되어 있는 인덱스 값에 기초한 나열 순번에 따라 상기 적어도 하나의 제2 문자와 상기 적어도 하나의 치환 문자를 일렬로 나열함으로써, 암호화된 텍스트열을 생성하는 단계를 포함한다.

발명의 효과

[0012] 본 발명은 중요 정보가 포함된 장문의 텍스트열에서 중요 정보만을 선별해서 암호화하고, 나머지 정보들은 평문의 형태로 둬으로써, 추후 관리자가 상기 장문의 텍스트열을 열람할 때, 중요 정보만이 암호화되어 있는 텍스트열을 열람할 수 있도록 함으로써, 해당 텍스트열의 전체적인 문맥을 신속하게 파악할 수 있도록 지원함과 동시에, 중요 정보 노출에 따른 보안상의 위험을 최소화할 수 있는 암호화 기법을 제공할 수 있다.

도면의 간단한 설명

- [0013] 도 1은 본 발명의 일실시예에 따른 장문 텍스트열에 대한 고정 길이 암호화 장치의 구조를 도시한 도면이다.
- 도 2와 도 3은 본 발명의 일실시예에 따른 장문 텍스트열에 대한 고정 길이 암호화 장치의 동작을 설명하기 위한 도면이다.
- 도 4는 본 발명의 일실시예에 따른 장문 텍스트열에 대한 고정 길이 암호화 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

- [0014] 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.
- [0015] 도 1은 본 발명의 일실시예에 따른 장문 텍스트열에 대한 고정 길이 암호화 장치의 구조를 도시한 도면이다.
- [0016] 도 1을 참조하면, 본 발명의 일실시예에 따른 장문 텍스트열에 대한 고정 길이 암호화 장치(110)는 치환 테이블 저장부(111), 인덱스 할당부(112), 문자 추출부(113), 치환 테이블 선택부(114), 문자 치환부(115) 및 암호화 텍스트 생성부(116)를 포함한다.
- [0017] 치환 테이블 저장부(111)에는 n (n 은 2이상의 자연수)개의 서로 다른 치환 테이블들이 저장되어 있다.
- [0018] 여기서, 상기 치환 테이블은 복수의 숫자들과 복수의 영문자들 각각에 대해 치환 대상이 되는 다른 숫자 또는 영문자를 대응시켜 기록한 테이블로, 상기 n 개의 치환 테이블들 각각에는 상기 복수의 숫자들과 상기 복수의 영문자들 각각에 대한 치환 대상이 되는 숫자 또는 영문자들이 서로 다르게 대응되어 기록되어 있다.
- [0019] 관련해서, 상기 치환 테이블에는 하기의 표 1과 같이 정보가 기록되어 있을 수 있다.

표 1

원본 숫자와 영문자	치환 대상 숫자와 영문자
1	a
2	b
...	...
a	e
b	t
...	...

- [0023] 이때, 치환 테이블 저장부(111)에 저장되어 있는 상기 n 개의 치환 테이블들은 상기 표 1과 같은 형태의 치환 테이블에서 치환 대상이 되는 숫자와 영문자들에 대한 정보가 모두 서로 다르게 기록되어 있다.
- [0024] 여기서, 치환 테이블 저장부(111)는 장문 텍스트열에 대한 고정 길이 암호화 장치(110)에 포함될 수 있는 치환 테이블 저장 유지부(미도시)를 통해서 유지 및 관리될 수 있다.
- [0025] 인덱스 할당부(112)는 복수의 문자들로 구성된 텍스트열에 대한 암호화 명령이 입력되면, 상기 복수의 문자들 각각에 대해 각 문자의 나열 순번에 기초한 고유 인덱스 값을 할당한다.
- [0026] 문자 추출부(113)는 상기 복수의 문자들 중 숫자와 영문자로 구성된 적어도 하나의 제1 문자를 추출한다.
- [0027] 치환 테이블 선택부(114)는 상기 n 개의 치환 테이블들 중 어느 하나인 제1 치환 테이블을 선택한다.
- [0028] 문자 치환부(115)는 상기 제1 치환 테이블에 기초하여 상기 적어도 하나의 제1 문자 각각을 상기 제1 치환 테이블에 기록되어 있는 치환 대상이 되는 다른 숫자 또는 영문자로 치환함으로써, 적어도 하나의 치환 문자를 생성하고, 상기 적어도 하나의 치환 문자 각각에 대해 상기 적어도 하나의 제1 문자 각각에 할당되어 있는 인덱스

값과 동일한 인덱스 값을 할당한다.

- [0029] 암호화 텍스트 생성부(116)는 적어도 하나의 제2 문자(상기 적어도 하나의 제2 문자는 상기 복수의 문자들 중 상기 적어도 하나의 제1 문자를 제외한 나머지 문자임)각각에 할당되어 있는 인덱스 값과 상기 적어도 하나의 치환 문자 각각에 할당되어 있는 인덱스 값에 기초한 나열 순번에 따라 상기 적어도 하나의 제2 문자와 상기 적어도 하나의 치환 문자를 일렬로 나열함으로써, 암호화된 텍스트열을 생성한다.
- [0030] 이때, 본 발명의 일실시예에 따르면, 상기 n개의 치환 테이블들 각각에는 서로 다른 순번 값이 할당되어 있고, 장문 텍스트열에 대한 고정 길이 암호화 장치(110)는 선정된(predetermined) 암호화키가 저장되어 있는 암호화키 저장부(117)를 더 포함할 수 있다.
- [0031] 여기서, 암호화키 저장부(117)는 장문 텍스트열에 대한 고정 길이 암호화 장치(110)에 포함될 수 있는 암호화키 저장 유지부(미도시)를 통해서 유지 및 관리될 수 있다.
- [0032] 이때, 치환 테이블 선택부(114)는 암호화키 저장부(117)에 저장되어 있는 상기 선정된 암호화키를 추출하고, 상기 선정된 암호화키에 대해 n을 제수(divisor)로 하는 모듈러(modular) 연산을 수행함으로써, 결과 값을 연산한 후 상기 n개의 치환 테이블들 중 상기 결과 값과 일치하는 순번 값이 할당되어 있는 치환 테이블을 상기 제1 치환 테이블로 선택할 수 있다.
- [0033] 이때, 본 발명의 일실시예에 따르면, 치환 테이블 선택부(114)는 암호화키 추출부(118), 데이터 분할부(119), 합계 연산부(120) 및 결과 값 연산부(121)를 포함할 수 있다.
- [0034] 암호화키 추출부(118)는 암호화키 저장부(117)에 저장되어 있는 상기 선정된 암호화키를 추출한다.
- [0035] 데이터 분할부(119)는 상기 선정된 암호화키를 구성하는 데이터 값을 선정된 데이터 크기 단위로 분할하여 복수의 분할 데이터들을 생성한다.
- [0036] 합계 연산부(120)는 상기 복수의 분할 데이터들 각각을 십진수의 숫자 데이터로 변환하고, 십진수의 숫자 데이터로 변환된 상기 복수의 분할 데이터들의 총합을 연산한다.
- [0037] 결과 값 연산부(121)는 상기 연산된 총합에 대해 n을 제수로 하는 모듈러 연산을 수행함으로써, 상기 결과 값을 연산한다.
- [0038] 또한, 본 발명의 일실시예에 따르면, 장문 텍스트열에 대한 고정 길이 암호화 장치(110)는 암호화키 교체부(122)를 더 포함할 수 있다.
- [0039] 암호화키 교체부(122)는 선정된 주기 간격으로, 암호화키를 랜덤하게 생성한 후 암호화키 저장부(117) 상에 저장되어 있는 상기 선정된 암호화키를 상기 랜덤하게 생성된 암호화키로 교체한다.
- [0040] 이하에서는 본 발명에 따른 장문 텍스트열에 대한 고정 길이 암호화 장치(110)의 동작에 대해 도 2와 도 3을 참조하여 상세하게 설명하기로 한다.
- [0041] 도 2와 도 3은 본 발명의 일실시예에 따른 장문 텍스트열에 대한 고정 길이 암호화 장치(110)의 동작을 설명하기 위한 도면이다.
- [0042] 우선, 도 2의 도면부호 210에 도시된 바와 같이, "홍길동, 주민번호:123456-1234567, 계좌번호:1234-1234-1234-1234, 여권번호:NA1234567"라고 하는 장문의 텍스트열을 암호화하는 경우를 가정하기로 하고, 치환 테이블 저장부(111)에는 상기 표 1과 같은 형태의 서로 다른 10개의 치환 테이블들이 저장되어 있다고 가정하며, 상기 서로 다른 10개의 치환 테이블들 각각에는 "0"부터 "9"까지의 고유 순번이 할당되어 있다고 가정하자.
- [0043] 이때, 인덱스 할당부(112)는 "홍길동, 주민번호:123456-1234567, 계좌번호:1234-1234-1234-1234, 여권번호:NA1234567"를 구성하는 복수의 문자들 각각에 대해 도면부호 220에 도시된 바와 같이, 각 문자의 나열 순번에 기초한 고유의 인덱스 값을 할당할 수 있다.
- [0044] 그리고, 문자 추출부(113)는 "홍길동, 주민번호:123456-1234567, 계좌번호:1234-1234-1234-1234, 여권번호:NA1234567"를 구성하는 상기 복수의 문자들 중 도면부호 230에 도시된 바와 같이, 숫자와 영문자로 구성된 적어도 하나의 제1 문자인 "12345612345671234123412341234NA1234567"을 추출할 수 있다.
- [0045] 그 이후, 치환 테이블 선택부(114)에 포함되어 있는 암호화키 추출부(118)는 암호화키 저장부(117)에 저장되어 있는 선정된 암호화키를 추출할 수 있고, 데이터 분할부(119)는 상기 선정된 암호화키를 구성하는 데이터 값을

선정된 데이터 크기 단위로 분할하여 복수의 분할 데이터들을 생성할 수 있다.

- [0046] 예컨대, 상기 선정된 암호화키가 32개의 숫자와 영문자로 구성된 32byte 크기의 데이터라고 하고, 상기 선정된 데이터 크기 단위를 1byte라고 하는 경우, 데이터 분할부(119)는 상기 32byte 크기의 상기 선정된 암호화키를 1byte 단위로 분할하여 32개의 분할 데이터들을 생성할 수 있다.
- [0047] 이때, 합계 연산부(120)는 상기 복수의 분할 데이터들 각각을 십진수의 숫자 데이터로 변환하고, 십진수의 숫자 데이터로 변환된 상기 복수의 분할 데이터들의 총합을 연산할 수 있다. 관련해서, 합계 연산부(120)는 상기 32개의 분할 데이터들 각각을 십진수의 숫자 데이터로 변환한 후 각 숫자 데이터들의 총합을 연산할 수 있다.
- [0048] 예컨대, 상기 분할 데이터들 중 하나가 "A"라고 하는 영문자에 대한 데이터인 경우, 해당 영문자에 대한 데이터는 아스키(ASCII) 코드표에 따른 16진수의 데이터 값(Hex)이 "41"이므로, 합계 연산부(120)는 "A"라는 분할 데이터를 "65"라고 하는 십진수의 숫자 데이터로 변환할 수 있다.
- [0049] 이러한 방식으로, 합계 연산부(120)는 상기 32개의 분할 데이터들에 대한 십진수의 숫자 데이터들을 생성하고, 32개의 숫자들을 모두 합산함으로써, 총합을 연산할 수 있다.
- [0050] 그러고 나서, 결과 값 연산부(121)는 상기 연산된 총합에 대해서 치환 테이블 저장되어 있는 치환 테이블들의 개수인 "10"을 제수로 하는 모듈러 연산을 수행하여 결과 값을 연산할 수 있다.
- [0051] 즉, 결과 값 연산부(121)는 상기 연산된 총합을 "10"으로 나눈 나머지 값을 상기 결과 값으로 연산할 수 있다. 이때, 상기 연산된 결과 값은 "10"으로 나눈 나머지 값이기 때문에 "0"~"9" 사이의 값이 산출되게 된다.
- [0052] 이렇게, 상기 결과 값의 연산이 완료되면, 치환 테이블 선택부(114)는 "0"~"9"라고 하는 순번 값이 각각 할당되어 있는 10개의 치환 테이블들 중 상기 연산된 결과 값과 일치하는 순번 값이 할당되어 있는 치환 테이블을 제1 치환 테이블로 선택할 수 있다.
- [0053] 이렇게, 치환 테이블 선택부(114)에서 상기 10개의 치환 테이블들 중 상기 제1 치환 테이블의 선택이 완료되면, 문자 치환부(115)는 도 3의 도면부호 240에 도시된 바와 같이, 상기 제1 치환 테이블에 기초하여 상기 적어도 하나의 제1 문자인 "12345612345671234123412341234NA1234567" 각각을 상기 제1 치환 테이블에 기록되어 있는 치환 대상이 되는 다른 숫자 또는 영문자로 치환함으로써, 적어도 하나의 치환 문자인 "BCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz"를 생성하고, 상기 적어도 하나의 치환 문자 각각에 대해 상기 적어도 하나의 제1 문자 각각에 할당되어 있는 인덱스 값과 동일한 인덱스 값을 할당할 수 있다.
- [0054] 이때, 본 발명의 일실시예에 따르면, 문자 치환부(115)는 상기 적어도 하나의 제1 문자인 "12345612345671234123412341234NA1234567" 각각을 상기 제1 치환 테이블에 기초하여 상기 적어도 하나의 치환 문자로 바로 치환할 수도 있지만, 보안을 강화하기 위해, 상기 적어도 하나의 제1 문자인 "12345612345671234123412341234NA1234567"에 대해 형태 보존 암호화(Format Preserving Encryption: FPE)를 수행하여 형태가 그대로 보존되는 소정의 암호화 값을 생성한 후 해당 암호화 값에 대해 상기 제1 치환 테이블에 기초하여 문자 치환을 수행함으로써, 상기 적어도 하나의 치환 문자를 생성할 수도 있다.
- [0055] 여기서, 형태 보존 암호화란 암호문이 평문의 형태를 보존하도록 하는 특성을 가진 암호 알고리즘을 의미한다.
- [0056] 이렇게, 상기 적어도 하나의 치환 문자인 "BCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz"의 생성이 완료되면, 암호화 텍스트 생성부(116)는 상기 복수의 문자들인 "홍길동, 주민번호:123456-1234567, 계좌번호:1234-1234-1234-1234, 여권번호:NA1234567"에서 상기 적어도 하나의 제1 문자인 "12345612345671234123412341234NA1234567"이 제외된 적어도 하나의 제2 문자 각각에 할당되어 있는 인덱스 값과 상기 적어도 하나의 치환 문자인 "BCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz" 각각에 할당되어 있는 인덱스 값에 기초한 나열 순번에 따라 도면부호 250에 도시되어 있는 바와 같이, 상기 적어도 하나의 제2 문자와 상기 적어도 하나의 치환 문자를 일렬로 나열함으로써, 암호화된 텍스트열을 생성할 수 있다.
- [0057] 그 결과, 도면부호 260에 도시되어 있는 바와 같이, "홍길동, 주민번호:BCDEFG-HIJKLMN, 계좌번호:OPQR-STUV-WXYZ-abcd, 여권번호:efghijkiA"이라는 암호문이 최종 생성될 수 있다.
- [0058] 도면부호 260에 도시되어 있는 암호문에서는 주민번호나 계좌번호와 같은 중요 정보만이 암호화되어 있고, "홍길동, 주민번호, 계좌번호, 여권번호"와 같은 나머지 정보는 암호화되어 있지 않기 때문에 관리자가 도면부호 260과 같은 암호문을 바로 보더라도 해당 암호문의 전체적인 맥락을 쉽게 파악할 수 있어서, 장문의 텍스트열에 대한 신속한 열람이 가능하면서도 중요 정보에 대한 노출은 최소화될 수 있다.

- [0059] 이때, 본 발명의 일실시예에 따른 장문 텍스트열에 대한 고정 길이 암호화 장치(110)는 관리자가 암호화키 저장부(117)에 저장되어 있는 상기 치환 테이블을 선택하는데 사용하기 위한 상기 선정된 암호화키를 주기적으로 변경해 줌으로써, 데이터 암호화에 사용될 치환 테이블이 주기적으로 변경되도록 하여 데이터 암호화에 있어서 보안을 강화할 수 있다.
- [0060] 또한, 본 발명의 일실시예에 따른 장문 텍스트열에 대한 고정 길이 암호화 장치(110)는 관리자가 상기 선정된 암호화키를 수동적으로 변경하는 것이 아니라, 선정된 주기 간격으로, 암호화키를 랜덤하게 생성한 후 암호화키 저장부(117) 상에 저장되어 있는 상기 선정된 암호화키를 상기 랜덤하게 생성된 암호화키로 교체하는 암호화키 교체부(122)를 더 포함함으로써, 데이터 암호화에 사용될 치환 테이블이 매 주기마다 다르게 선택되도록 지원할 수 있다.
- [0061] 지금까지 도 2와 도 3을 참조하여, 본 발명에 따른 장문 텍스트열에 대한 고정 길이 암호화 장치(110)가 장문 텍스트열에 대해 암호화를 수행하는 과정에 대해 설명하였다. 본 발명에 따른 장문 텍스트열에 대한 고정 길이 암호화 장치(110)는 암호화된 장문 텍스트열에 대한 복호화를 수행하는 구성도 포함할 수 있는 바, 이에 대해 상세히 설명하기로 한다.
- [0062] 본 발명의 일실시예에 따르면, 장문 텍스트열에 대한 고정 길이 암호화 장치(110)는 복호화 인덱스 할당부(123), 암호화 문자 추출부(124), 복호화 치환 테이블 선택부(125), 문자 역치환부(126) 및 복호화 텍스트 생성부(127)를 더 포함할 수 있다.
- [0063] 복호화 인덱스 할당부(123)는 암호화 텍스트 생성부(116)에 의해서 생성된 상기 암호화된 텍스트열에 대한 복호화 명령이 입력되면, 상기 암호화된 텍스트열을 구성하는 복수의 암호화 문자들 각각에 대해 각 문자의 나열 순번에 기초한 고유의 인덱스 값을 할당한다.
- [0064] 암호화 문자 추출부(124)는 상기 복수의 암호화 문자들 중 숫자와 영문자로 구성된 적어도 하나의 제1 암호화 문자를 추출한다.
- [0065] 복호화 치환 테이블 선택부(125)는 암호화키 저장부(117)에 저장되어 있는 상기 선정된 암호화키를 추출하고, 상기 선정된 암호화키에 대해 n 을 제수로 하는 모듈러 연산을 수행함으로써, 결과 값을 연산한 후 상기 n 개의 치환 테이블들 중 상기 결과 값과 일치하는 순번 값이 할당되어 어느 하나의 치환 테이블을 선택함으로써, 상기 제1 치환 테이블을 선택한다.
- [0066] 문자 역치환부(126)는 상기 제1 치환 테이블에 기초하여 상기 적어도 하나의 제1 암호화 문자 각각을 상기 제1 치환 테이블에 기록되어 있는 치환 대상이 되는 숫자 또는 영문자에 대응하는 원본 숫자 또는 영문자로 역치환함으로써, 적어도 하나의 원본 문자를 생성하고, 상기 적어도 하나의 원본 문자 각각에 대해 상기 적어도 하나의 제1 암호화 문자 각각에 할당되어 있는 인덱스 값과 동일한 인덱스 값을 할당한다.
- [0067] 복호화 텍스트 생성부(127)는 적어도 하나의 제2 암호화 문자(상기 적어도 하나의 제2 암호화 문자는 상기 복수의 암호화 문자들 중 상기 적어도 하나의 제1 암호화 문자를 제외한 나머지 문자임) 각각에 할당되어 있는 인덱스 값과 상기 적어도 하나의 원본 문자 각각에 할당되어 있는 인덱스 값에 기초한 나열 순번에 따라 상기 적어도 하나의 제2 암호화 문자와 상기 적어도 하나의 원본 문자를 일렬로 나열함으로써, 복호화된 텍스트열을 생성한다.
- [0068] 관련해서, 도 2와 도 3에 도시된 도면에 따라, "홍길동, 주민번호:BCDEFG-HIJKLMN, 계좌번호:OPQR-STUV-WXYZ-abcd, 여권번호:efghijklA"이라는 암호화된 텍스트열이 생성된 상황에서 상기 암호화된 텍스트열에 대한 복호화 명령이 입력되면, 복호화 인덱스 할당부(123)는 "홍길동, 주민번호:BCDEFG-HIJKLMN, 계좌번호:OPQR-STUV-WXYZ-abcd, 여권번호:efghijklA"를 구성하는 복수의 암호화 문자들 각각에 대해 고유의 인덱스 값을 할당할 수 있다.
- [0069] 그리고, 암호화 문자 추출부(124)는 상기 복수의 암호화 문자들 중 숫자와 영문자로 구성된 "BCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz"라고 하는 적어도 하나의 제1 암호화 문자를 추출할 수 있다.
- [0070] 그리고 나서, 복호화 치환 테이블 선택부(125)는 상기 선정된 암호화키를 기초로 상기 제1 치환 테이블을 선택할 수 있고, 문자 역치환부(126)는 상기 제1 치환 테이블에 기초하여 상기 적어도 하나의 제1 암호화 문자인 "BCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz" 각각을 상기 제1 치환 테이블에 기록되어 있는 치환 대상이 되는 숫자 또는 영문자에 대응하는 원본 숫자 또는 영문자로 역치환함으로써, "1234561234567123412341234NA1234567"이라는 적어도 하나의 원본 문자를 생성하고, 상기 적어도 하나의 원본 문자 각각에 대해 상기 적어도 하나의 제1 암호화 문자 각각에 할당되어 있는 인덱스 값과 동일한 인덱스

값을 할당할 수 있다.

- [0071] 그 이후, 복호화 텍스트 생성부(127)는 "홍길동, 주민번호:BCDEFG-HIJKLMN, 계좌번호:OPQR-STUV-WXYZ-abcd, 여권번호:efghijklA"를 구성하는 복수의 암호화 문자들 중 상기 적어도 하나의 제1 암호화 문자가 제외된 나머지 문자인 적어도 하나의 제2 암호화 문자와 상기 적어도 하나의 원본 문자를 각 문자에 할당되어 있는 인덱스 값에 기초한 나열 순번에 따라 일렬로 나열함으로써, "홍길동, 주민번호:123456-1234567, 계좌번호:1234-1234-1234-1234, 여권번호:NA1234567"이라는 복호화된 텍스트열을 생성할 수 있다.
- [0072] 도 4는 본 발명의 일실시예에 따른 장문 텍스트열에 대한 고정 길이 암호화 방법을 도시한 순서도이다.
- [0073] 단계(S410)에서는 n (n 은 2이상의 자연수)개의 서로 다른 치환 테이블들이 저장되어 있는 치환 테이블 저장부를 유지한다.
- [0074] 여기서, 상기 치환 테이블은 복수의 숫자들과 복수의 영문자들 각각에 대해 치환 대상이 되는 다른 숫자 또는 영문자를 대응시켜 기록한 테이블로, 상기 n 개의 치환 테이블들 각각에는 상기 복수의 숫자들과 상기 복수의 영문자들 각각에 대한 치환 대상이 되는 숫자 또는 영문자들이 서로 다르게 대응되어 기록되어 있다.
- [0075] 단계(S420)에서는 복수의 문자들로 구성된 텍스트열에 대한 암호화 명령이 입력되면, 상기 복수의 문자들 각각에 대해 각 문자의 나열 순번에 기초한 고유의 인덱스 값을 할당한다.
- [0076] 단계(S430)에서는 상기 복수의 문자들 중 숫자와 영문자로 구성된 적어도 하나의 제1 문자를 추출한다.
- [0077] 단계(S440)에서는 상기 n 개의 치환 테이블들 중 어느 하나인 제1 치환 테이블을 선택한다.
- [0078] 단계(S450)에서는 상기 제1 치환 테이블에 기초하여 상기 적어도 하나의 제1 문자 각각을 상기 제1 치환 테이블에 기록되어 있는 치환 대상이 되는 다른 숫자 또는 영문자로 치환함으로써, 적어도 하나의 치환 문자를 생성하고, 상기 적어도 하나의 치환 문자 각각에 대해 상기 적어도 하나의 제1 문자 각각에 할당되어 있는 인덱스 값과 동일한 인덱스 값을 할당한다.
- [0079] 단계(S460)에서는 적어도 하나의 제2 문자(상기 적어도 하나의 제2 문자는 상기 복수의 문자들 중 상기 적어도 하나의 제1 문자를 제외한 나머지 문자임)각각에 할당되어 있는 인덱스 값과 상기 적어도 하나의 치환 문자 각각에 할당되어 있는 인덱스 값에 기초한 나열 순번에 따라 상기 적어도 하나의 제2 문자와 상기 적어도 하나의 치환 문자를 일렬로 나열함으로써, 암호화된 텍스트열을 생성한다.
- [0080] 이때, 본 발명의 일실시예에 따르면, 상기 n 개의 치환 테이블들 각각에는 서로 다른 순번 값이 할당되어 있고, 상기 장문 텍스트열에 대한 고정 길이 암호화 방법은 선정된 암호화키가 저장되어 있는 암호화키 저장부를 유지하는 단계를 더 포함할 수 있다.
- [0081] 이때, 단계(S440)에서는 상기 암호화키 저장부에 저장되어 있는 상기 선정된 암호화키를 추출하고, 상기 선정된 암호화키에 대해 n 을 제수로 하는 모듈러 연산을 수행함으로써, 결과 값을 연산한 후 상기 n 개의 치환 테이블들 중 상기 결과 값과 일치하는 순번 값이 할당되어 있는 치환 테이블을 상기 제1 치환 테이블로 선택할 수 있다.
- [0082] 이때, 본 발명의 일실시예에 따르면, 단계(S440)에서는 상기 암호화키 저장부에 저장되어 있는 상기 선정된 암호화키를 추출하는 단계, 상기 선정된 암호화키를 구성하는 데이터 값을 선정된 데이터 크기 단위로 분할하여 복수의 분할 데이터들을 생성하는 단계, 상기 복수의 분할 데이터들 각각을 십진수의 숫자 데이터로 변환하고, 십진수의 숫자 데이터로 변환된 상기 복수의 분할 데이터들의 총합을 연산하는 단계 및 상기 연산된 총합에 대해 n 을 제수로 하는 모듈러 연산을 수행함으로써, 상기 결과 값을 연산하는 단계를 포함할 수 있다.
- [0083] 또한, 본 발명의 일실시예에 따르면, 장문 텍스트열에 대한 고정 길이 암호화 방법은 선정된 주기 간격으로, 암호화키를 랜덤하게 생성한 후 상기 암호화키 저장부 상에 저장되어 있는 상기 선정된 암호화키를 상기 랜덤하게 생성된 암호화키로 교체하는 단계를 더 포함할 수 있다.
- [0084] 또한, 본 발명의 일실시예에 따르면, 상기 장문 텍스트열에 대한 고정 길이 암호화 방법은 상기 암호화된 텍스트열에 대한 복호화 명령이 입력되면, 상기 암호화된 텍스트열을 구성하는 복수의 암호화 문자들 각각에 대해 각 문자의 나열 순번에 기초한 고유의 인덱스 값을 할당하는 단계, 상기 복수의 암호화 문자들 중 숫자와 영문자로 구성된 적어도 하나의 제1 암호화 문자를 추출하는 단계, 상기 암호화키 저장부에 저장되어 있는 상기 선정된 암호화키를 추출하고, 상기 선정된 암호화키에 대해 n 을 제수로 하는 모듈러 연산을 수행함으로써, 결과 값을 연산한 후 상기 n 개의 치환 테이블들 중 상기 결과 값과 일치하는 순번 값이 할당되어 어느 하나의 치환 테이블을 선택함으로써, 상기 제1 치환 테이블을 선택하는 단계, 상기 제1 치환 테이블에 기초하여 상기 적어도

하나의 제1 암호화 문자 각각을 상기 제1 치환 테이블에 기록되어 있는 치환 대상이 되는 숫자 또는 영문자에 대응하는 원본 숫자 또는 영문자로 역치환함으로써, 적어도 하나의 원본 문자를 생성하고, 상기 적어도 하나의 원본 문자 각각에 대해 상기 적어도 하나의 제1 암호화 문자 각각에 할당되어 있는 인덱스 값과 동일한 인덱스 값을 할당하는 단계 및 적어도 하나의 제2 암호화 문자(상기 적어도 하나의 제2 암호화 문자는 상기 복수의 암호화 문자들 중 상기 적어도 하나의 제1 암호화 문자를 제외한 나머지 문자임) 각각에 할당되어 있는 인덱스 값과 상기 적어도 하나의 원본 문자 각각에 할당되어 있는 인덱스 값에 기초한 나열 순번에 따라 상기 적어도 하나의 제2 암호화 문자와 상기 적어도 하나의 원본 문자를 일렬로 나열함으로써, 복호화된 텍스트열을 생성하는 단계를 더 포함할 수 있다.

[0085] 이상, 도 4를 참조하여 본 발명의 일실시예에 따른 장문 텍스트열에 대한 고정 길이 암호화 방법에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 장문 텍스트열에 대한 고정 길이 암호화 방법은 도 1 내지 도 3을 이용하여 설명한 장문 텍스트열에 대한 고정 길이 암호화 장치(110)의 동작에 대한 구성과 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.

[0086] 본 발명의 일실시예에 따른 장문 텍스트열에 대한 고정 길이 암호화 방법은 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다.

[0087] 또한, 본 발명의 일실시예에 따른 장문 텍스트열에 대한 고정 길이 암호화 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.

[0088] 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.

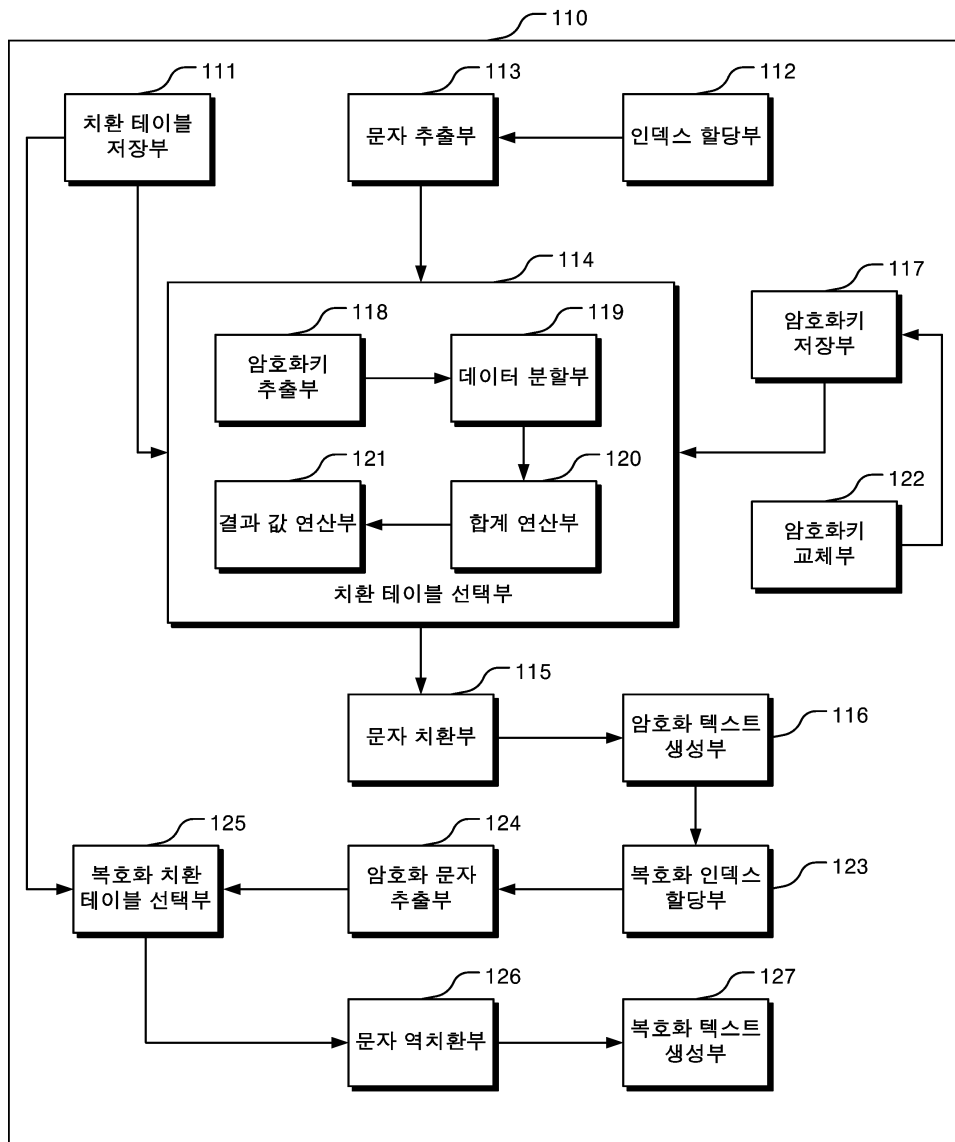
[0089] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

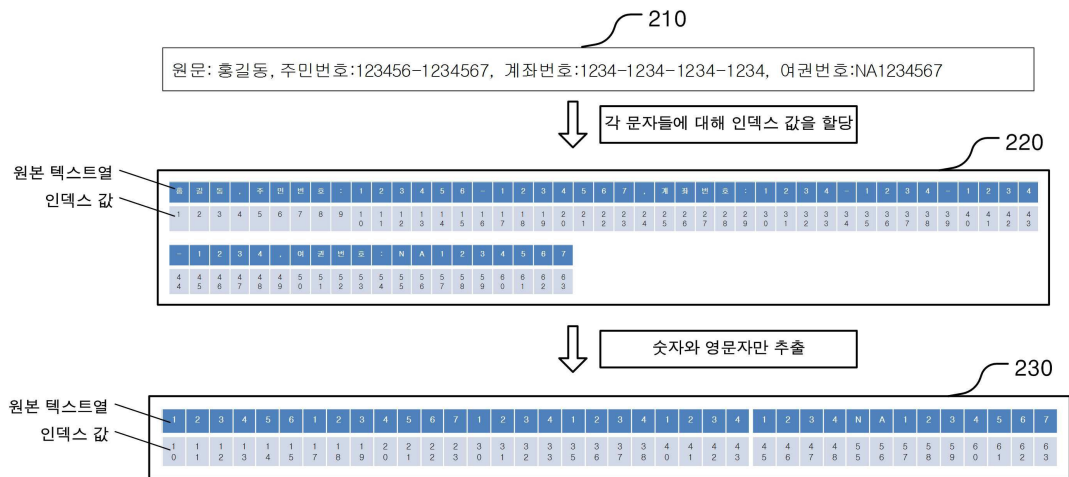
[0090] 110: 장문 텍스트열에 대한 고정 길이 암호화 장치
111: 치환 테이블 저장부 112: 인덱스 할당부
113: 문자 추출부 114: 치환 테이블 선택부
115: 문자 치환부 116: 암호화 텍스트 생성부
117: 암호화키 저장부 118: 암호화키 추출부
119: 데이터 분할부 120: 합계 연산부
121: 결과 값 연산부 122: 암호화키 교체부
123: 복호화 인덱스 할당부 124: 암호화 문자 추출부
125: 복호화 치환 테이블 선택부 126: 문자 역치환부
127: 복호화 텍스트 생성부

도면

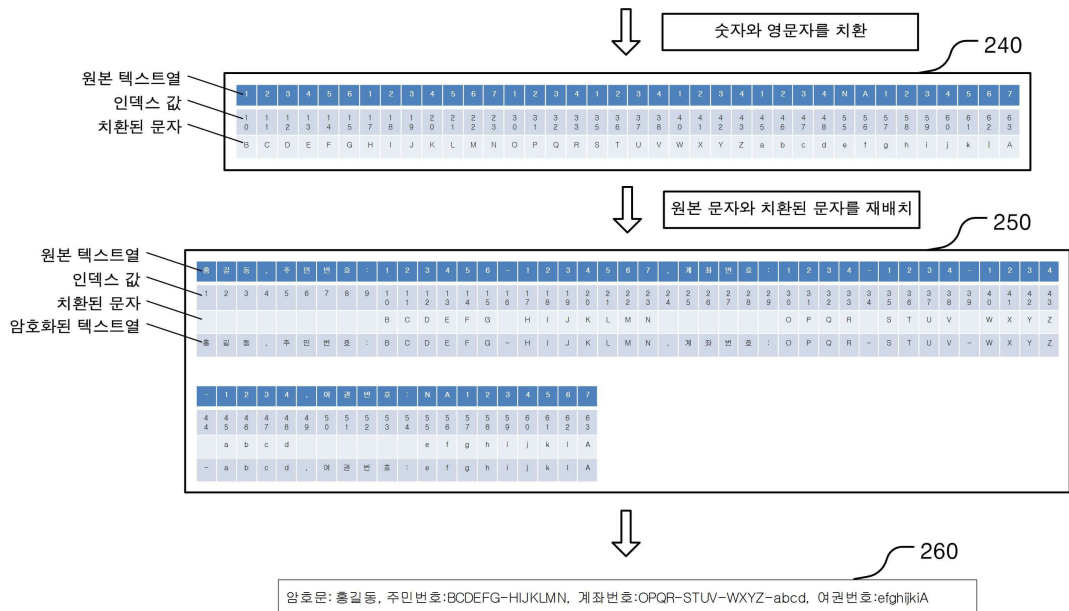
도면1



도면2



도면3



도면4

