

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2014년 5월 8일 (08.05.2014)



(10) 국제공개번호
WO 2014/069724 A1

- (51) 국제특허분류:
G06K 9/18 (2006.01) *G06K 7/10* (2006.01)
- (21) 국제출원번호: PCT/KR2013/001886
- (22) 국제출원일: 2013년 3월 8일 (08.03.2013)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2012-0124011 2012년 11월 5일 (05.11.2012) KR
- (71) 출원인: 한국과학기술원 (KOREA ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY) [KR/KR]; 305-701 대전시 유성구 구성동 373-1, Daejeon (KR).
- (72) 발명자: 원용협 (WON, Yong Hyub); 305-701 대전시 유성구 대학로 291 한국과학기술원, Daejeon (KR). 정병주 (CHUNG, Byung-Joo); 515-913 전라남도 장성군 진원면 용산리, Jeollanam-do (KR).

(74) 대리인: 유미특허법인 (YOU ME PATENT AND LAW FIRM); 135-080 서울시 강남구 역삼동 649-10 서림빌딩, Seoul (KR).

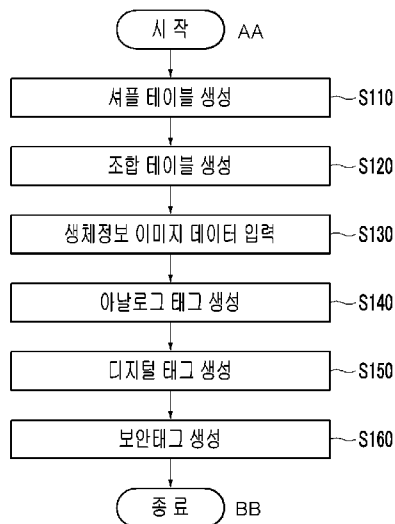
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR),

[다음 쪽 계속]

(54) Title: METHOD FOR GENERATING SECURITY TAG AND METHOD FOR RESTORING SECURITY TAG

(54) 발명의 명칭 : 보안태그 생성방법과 복원방법



(57) Abstract: Provided are a method for generating a security tag and a method for restoring a security tag, which are capable of providing high-level security. The method for generating a security tag comprises the steps of: generating an analog tag for an image including biometric information based on a shuffle table and a combination table; and generating a digital tag. The method for restoring a security tag comprises the steps of: decoding a digital tag; and decoding an analog tag so as to restore an image including biometric information.

(57) 요약서: 고도의 보안성을 제공하는 보안태그 생성방법과 복원방법이 제공되며, 보안태그 생성방법은 생체 정보를 포함하는 이미지에 대하여 셔플 테이블 및 조합 테이블에 기초하여 아날로그 태그를 생성하는 단계, 그리고 디지털 태그를 생성하는 단계를 포함하며, 보안태그 복원방법은 디지털 태그를 디코딩하는 단계, 그리고 아날로그 태그를 디코딩하여 생체 정보를 포함하는 이미지를 복원하는 단계를 포함한다.

AA ... Start
S110 ... Generate a shuffle table
S120 ... Generate a combination table
S130 ... Input biometric information image data
S140 ... Generate an analog tag
S150 ... Generate a digital tag
S160 ... Generate a security tag
BB ... End

WO 2014/069724 A1



OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

공개:
— 국제조사보고서와 함께 (조약 제 21 조(3))

명세서

발명의 명칭: 보안태그 생성방법과 복원방법

기술분야

- [1] 보안태그 생성방법과 복원방법이 제공된다.

배경기술

- [2] 종래 금융거래나 개인서류발급 절차를 보면 직원이 상주하고 있는 창구의 경우 직원이 여권, 주민등록증, 운전면허증 등의 신분증에 게시된 사진과 실물 얼굴을 육안으로 확인하여 본인 확인을 수행하고 있다. 또한, 현금 자동 입출금기(automated teller machine, ATM)나 무인 발급기의 경우 신분증이나 신용카드를 제시하거나 주민등록번호, 계좌번호, 전화번호 및 계좌비밀번호 등의 개인 신상정보만을 입력하여 본인임을 확인하는 것이 가능하다. 그러나, 이와 같은 본인확인 방법은 창구 직원들의 주관적인 판단 및 형식적인 인증절차를 수행함에 있어서 잘못된 본인인증을 야기할 수 있으며, 나아가 분식 및 도난된 신용카드나 신분증을 이용한 추가 범죄 발생 가능성을 높일 수 있다.
- [3] 이에 따라 최근에는 사용자의 바이오 정보가 저장된 전자태그로부터 추출한 데이터를 네트워크에 연결된 서버에 저장된 데이터와 비교하여 본인임을 확인하는 기술이 개발되었으나, 이러한 방법은 방대한 데이터 관리를 위한 서버 유지 비용 부담과 네트워크 전송 오류 및 해킹 위험성이 있다. 또한, 컴퓨터, 프린터, 스캐너 및 카메라와 같은 하드웨어 기술과 소프트웨어 기술의 발달로 전자태그의 복사, 위조 및 변조가 손쉽게 이루어질 수 있다.

발명의 상세한 설명

기술적 과제

- [4] 본 발명의 일실시예가 해결하려는 과제는 보안을 필요로 하는 이미지를 대상으로 제1 암호화 및 제2 암호화를 수행하여 종래보다 보안성을 높인 보안태그 생성방법과 복원방법을 제공하는 것이다.

과제 해결 수단

- [5] 상기 과제를 해결하기 위해 본 발명의 일실시예는, 생체 정보를 포함하는 이미지를 제공하는 단계, 상기 이미지를 $N \times M$ 개(N 및 M 은 자연수)로 조각내어 랜덤하게 배열하는 어드레스를 포함하는 셔플 테이블을 생성하는 단계, 1에서 $N \times M$ 까지의 정수를 랜덤하게 2 개씩 선택하여 이루어진 정수 쌍을 포함하는 조합 테이블을 생성하는 단계, 상기 셔플 테이블을 이용하여 상기 이미지의 조각들을 셔플링하여 셔플 이미지를 생성하고, 상기 조합 테이블 및 상기 정수 쌍에 대응되는 이진 랜덤코드의 위치 변환 정보를 이용하여 셔플 이미지의 조각들을 재배치함으로써 제1 암호화된 아날로그 태그를 생성하는 단계, 그리고 상기 이진 랜덤코드를 상기 생체정보, 상기 셔플 테이블, 그리고 상기 조합 테이블을 이용하여 이진 이미지로 재조합함으로써 제2 암호화된 디지털 태그를

- 생성하는 단계를 포함하는 보안태그의 생성방법을 일실시예로 제안한다.
- [6] 여기서, 상기 위치 변환 정보는 상기 정수 쌍이 현재 위치를 유지하라는 정보 또는 상기 정수 쌍이 서로 위치를 변경하라는 정보일 수 있다.
- [7] 또한, 상기 디지털 태그를 생성하는 단계는, 셔플링 키(shuffling key)를 생성하는 단계, 상기 셔플링 키와 랜덤 키를 논리 연산하여 암호화 데이터를 생성하는 단계, 그리고 상기 암호화 데이터에 대하여 바이너리 콘볼루션 인코딩을 수행하여 컬러코드를 생성하는 단계를 포함할 수 있다.
- [8] 또한, 상기 컬러코드를 생성하는 단계는 상기 암호화 데이터의 입력 바이트와 상기 바이너리 콘볼루션에 사용되는 n 개의 입력 바이트 각각에 대하여 배타적 논리합(XOR, Exclusive OR) 연산을 통해 인접한 바이트 간에 논리 관계를 생성하는 바이너리 콘볼루션 인코딩을 수행할 수 있다.
- [9] 또한, 상기 디지털 태그를 생성하는 단계는 상기 컬러코드의 데이터 압축을 위해 4비트 컬러 인코딩을 수행하는 단계를 포함할 수 있다.
- [10] 또한, 상기 과제를 해결하기 위해 본 발명의 다른 일실시예는, 제1 암호화된 아날로그 태그 및 제2 암호화된 디지털 태그를 포함하는 보안태그를 획득하는 단계, 상기 제2 암호화에 대응하는 제1 디코딩을 수행하는 단계, 그리고 상기 제1 암호화에 대응하는 제2 디코딩을 수행하여 생체 정보를 포함하는 이미지를 복원하는 단계를 포함하는 보안태그의 복원방법을 일실시예로 제안한다.
- [11] 여기서, 상기 제1 디코딩을 수행하는 단계는 컬러코드의 저주파 노이즈를 제거하기 위하여 푸리에변환 및 역푸리에 변환을 수행하는 단계를 포함할 수 있다.
- [12] 또한, 상기 제1 디코딩을 수행하는 단계는 상기 제2 암호화가 바이너리 콘볼루션 인코딩을 통해 수행된 경우, 상기 컬러코드에 바이너리 콘볼루션 디코딩을 수행하는 단계를 포함할 수 있다.
- [13] 또한, 상기 이미지를 복원하는 단계는 상기 제1 암호화가 상기 이미지를 $N \times M$ 개(N 및 M 은 자연수)로 조각내어 랜덤하게 배열하는 어드레스를 포함하는 셔플 테이블과 1에서 $N \times M$ 까지의 정수를 랜덤하게 2 개씩 선택하여 이루어진 정수 쌍을 포함하는 조합 테이블을 이용하여 수행된 경우, 상기 조합 테이블의 정수 쌍과 상기 셔플 테이블의 어드레스를 이용하여 상기 이미지의 조각들을 재배열하는 상기 제2 디코딩을 수행하는 단계를 포함할 수 있다.

발명의 효과

- [14] 본 발명의 일실시예에 의하면 보안태그가 부착된 개인식별카드를 이용하여 고도의 보안을 요구하는 금융거래나 개인문서발급 및 출입통제 등에 있어서 안전하고 신속하게 본인 인증을 수행할 수 있다. 또한, 제1 암호화 및 제2 암호화가 수행된 보안태그를 구현함으로써 보안태그의 불법 위조 및 변조를 원천적으로 차단할 수 있으며, 보안태그가 부착된 신용카드 및 신분증을 분실하거나 도난당했을 경우 신용카드나 신분증 도용으로 인해 발생하는

불미스러운 사고를 방지할 수 있다.

도면의 간단한 설명

- [15] 도 1은 본 발명의 일실시예에 따른 보안태그를 이용하는 사용자 인증장치이다.
- [16] 도 2는 본 발명의 일실시예에 따른 보안태그의 생성방법을 도시한 순서도다.
- [17] 도 3은 본 발명의 일실시예에 따른 보안태그 생성방법에 있어서 1차 암호화 수행과정을 도시한 순서도다.
- [18] 도 4는 본 발명의 일실시예에 따른 보안태그 생성방법에 있어서 2차 암호화 수행과정을 도시한 순서도다.
- [19] 도 5는 본 발명의 일실시예에 따른 보안태그를 이용하는 사용자 인증장치의 블록도이다.
- [20] 도 6은 본 발명의 일실시예에 따른 보안태그의 복원방법을 도시한 순서도다.

발명의 실시를 위한 최선의 형태

- [21] 도 1은 본 발명의 일실시예에 따른 보안태그를 이용하는 사용자 인증장치이다.
- [22] 도 1의 사용자 인증장치는, 사용자가 보유한 개인식별카드의 삽입을 요청하고, 개인식별카드에 부착된 보안태그를 읽어들이어 보안태그에 암호화되어 저장된 사용자의 생체정보를 복원한다. 이후, 사용자의 실물 생체정보를 스캔하여 복원된 생체정보와 비교한 결과에 따라 두 개의 생체정보가 일치할 경우 사용자의 본인 인증을 수락하고 사용자의 요구사항을 처리한다.
- [23] 이때, 개인식별카드는 사용자 본인의 신분을 확인할 수 있는 증명자료로써, 일정한 지역에 거주하는 주민임을 나타내는 주민등록증, 외국을 여행하는 사람의 신분이나 국적을 증명하는 여권, 도로에서 자동차를 운전할 수 있는 자격을 증명하는 운전면허증 및 금융거래가 가능한 신분임을 증명하는 신용카드, 직불카드, 체크카드 및 현금카드 등이 될 수 있다.
- [24] 아래에서는 본 발명의 일실시예에 따른 보안태그의 생성방법에 대하여 상세히 설명한다.
- [25] 도 2는 본 발명의 일실시예에 따른 보안태그의 생성방법을 도시한 순서도다.
- [26] 먼저, 보안을 요하는 이미지 데이터를 $[N \times M]$ 개로 조각을 내고 각각의 조각에 어드레스를 부여한 후, 랜덤하게 배열할 수 있도록 1에서 $N \times M$ 까지의 정수를 섞어서 하나의 셔플 테이블(shuffle table)을 생성한다(S110). N 또는 M은 임의의 자연수이다. 셔플 테이블은 랜덤 어드레스(random address) 배열을 의미하며, 여러 개의 셔플 테이블이 생성될 수 있으며, 셔플 테이블 각각은 고유 식별번호를 갖는다. 또한, 셔플 테이블은 각각 파일 단위로 구분되어 저장될 수 있으며 데이터베이스의 레코드로 저장될 수 있다.
- [27] 예를 들어, N이 3이고 M이 2인 경우, 이미지 데이터를 하기 표 1처럼 3×2 개로 조각낼 수 있으며, 식별번호 1 및 2인 셔플 테이블이 각각 하기 표2 및 표3처럼 생성될 수 있으며, 이외에도 다양한 배열을 갖는 여러 개의 셔플 테이블이 생성될 수 있다.

[28] 표 1

[Table 1]

1	2	3
4	5	6

[29]

[30] 표 2

[Table 2]

3	1	5
4	6	2

[31]

[32] 표 3

[Table 3]

4	3	1
2	5	6

[33]

[34] 이후, 보안성을 더 높이기 위하여, 1에서 $N \times M$ 까지의 정수를 랜덤하게 2개씩 선택하여 조합 테이블을 생성한다(S120). 이때 조합 테이블 역시 여러 개로 생성될 수 있으며, 조합 테이블 각각은 셔플 테이블과 마찬가지로 고유 식별번호를 갖는다.

[35] 예를 들어, N이 3이고 M이 2인 경우, 식별번호 1 및 2인 조합 테이블이 각각 하기 표 4 및 5처럼 생성될 수 있으며, 이외에도 다양한 조합을 갖는 여러 개의 조합 테이블이 생성될 수 있다.

[36] 표 4

[Table 4]

(1,3)	(2,5)	(4,6)
-------	-------	-------

[37]

[38] 표 5

[Table 5]

(1,5)	(2,6)	(3,4)
-------	-------	-------

[39]

[40] 이후, 사용자의 얼굴, 지문, 홍채, 혈관 및 정맥 등의 신체 고유 정보를 저장하고 있는 생체정보 이미지 데이터가 입력되면(S130), 1차 암호화를 수행하여 아날로그 태그를 생성하고(S140), 아날로그 태그에 2차 암호화를 수행하여

디지털 태그를 생성한다(S150). 1차 암호화와 2차 암호화 방법은 아래의 도 3과 도 4를 바탕으로 자세히 설명하도록 한다.

[41] 도 3은 본 발명의 일실시예에 따른 보안태그 생성방법에 있어서 1차 암호화 수행과정을 도시한 순서도다.

[42] 먼저, 생체정보 이미지 데이터를 $N \times M$ 개의 조각으로 분할한 조각 이미지 데이터를 생성하기 위하여 셔플 테이블을 이용한다. 이때, 셔플 테이블의 고유 식별번호를 통해 하나의 셔플 테이블을 랜덤하게 선택한다(S141). 이후, 선택된 셔플 테이블에 저장된 랜덤 어드레스 배열을 이용하여 생체정보 이미지 데이터의 셔플링(shuffling)을 수행하여 셔플 이미지를 생성한다(S142).

[43] 이후, 조합 테이블의 고유 식별번호를 통해 하나의 조합 테이블을 랜덤하게 선택하고(S143), 조합 테이블에 저장된 어드레스 조합 각각에 0 또는 1의 이진 랜덤코드를 랜덤하게 할당한다(S144). 이에 따라 본 발명의 일실시예에 따른 보안태그의 보안성이 더욱 개선될 수 있다. 또한, 이진 랜덤코드는 0 또는 1의 값을 가지며, $N \times M$ 개가 생성될 수 있다. 이진 랜덤코드는 셔플 이미지 조각들의 자리바꿈 또는 현재 자리 유지 등과 같은 위치 변환 정보를 포함한다. 예를 들어, 이진 랜덤코드가 0인 어드레스 조합은 현재 자리를 유지하는 정보를 포함하고, 이진 랜덤코드가 1인 어드레스 조합은 서로의 자리를 바꾸라는 정보를 포함할 수 있다. 또한, $N \times M$ 이 홀수인 경우, 조합이 구성되지 않은 1개의 어드레스는 현재 자리를 유지할 수 있다. 이후, 상기 이진 랜덤코드에 의해 셔플 이미지의 조각들을 재배치함으로써 1차 암호화된 아날로그 태그를 생성한다(도 2의 S140).

[44] 예를 들어, 전술한 표 1 내지 5의 예에서, 랜덤하게 셔플 테이블의 고유 식별번호가 1로 선택된 경우, 3×2 이미지 데이터는 상기 표 2처럼 배열된 셔플 이미지가 생성된다. 이후, 랜덤하게 조합 테이블의 고유 식별번호가 2로 선택되고, 상기 표 4의 조합 테이블에 랜덤하게 이진 랜덤코드가 하기 표 6처럼 할당되고, 이진 랜덤코드 0은 현재 자리 유지 정보를 포함하고 1은 자리바꿈 정보를 포함하는 경우, 하기 표 8처럼 배열된 이미지가 생성된다.

[45] 표 6

[Table 6]

(1,5)	(2,6)	(3,4)
1	0	1

[46]

[47] 표 7

[Table 7]

4	5	1
3	6	2

- [48]
- [49] 도 4는 본 발명의 일실시예에 따른 보안태그 생성방법에 있어서 2차 암호화 수행과정을 도시한 순서도다.
- [50] 먼저, 아날로그 태그 생성시 사용되었던 이진 랜덤코드가 생체정보 이미지 데이터와 셔플 테이블의 고유 식별번호 및 조합 테이블의 고유 식별번호와 결합하여 이진 이미지로 재조합되고 셔플링 키(shuffling key)를 생성한다(S151).
- [51] 이후, 셔플링 키와 랜덤 키(random key)를 논리 연산하여 암호화 데이터를 생성한다(S152). 이때, 랜덤 키는 셔플링 키를 암호화하기 위한 위상 및 진폭 정보를 포함하며, 셔플링 키와 배타적 논리합(XOR, Exclusive OR) 연산을 수행하여 암호화 데이터를 생성한다.
- [52] 이후, 암호화 데이터에 대하여 바이너리 콘볼루션 인코딩(binary convolution encoding)을 수행하여 컬러코드를 생성한다(S153). 이때, 바이너리 콘볼루션 인코딩은 암호화 데이터의 입력 바이트와 바이너리 콘볼루션에 사용되는 n개의 입력 바이트 각각에 대하여 배타적 논리합(XOR, Exclusive OR) 연산을 통해 인접한 바이트 간에 논리 관계를 생성하는 과정이다.
- [53] 이후, 컬러 코드의 압축을 위해 4비트 컬러 인코딩을 수행하고(S154), 2차 암호화된 디지털 태그를 생성한다(도 2의 S150).
- [54] 다시 도 2의 설명으로 돌아가서, 도 3과 도 4에 의해 각각 생성된 아날로그 태그와 디지털 태그가 모두 기록되어 있는 보안태그를 생성한다(S160). 이때, 아날로그 태그와 디지털 태그는 간섭계를 이용하는 광학적 방식 또는 레이저 빔의 출력을 이용하는 전자적 방식을 통해 보안태그에 기록될 수 있다.
- [55] 도 5는 본 발명의 일실시예에 따른 보안태그를 이용하는 사용자 인증장치 of 블록도이다.
- [56] 도 5의 사용자 인증장치는 개인식별카드(100)와, 사용자 인증부(200)와, 민원처리부(300) 및 표시부(500)를 포함할 수 있다.
- [57] 개인식별카드(100)는 암호화된 사용자의 생체정보가 저장된 컬러코드 형태의 보안태그(110)를 포함할 수 있다.
- [58] 사용자 인증부(200)는 사용자가 본인임을 확인하여 사용자의 요구사항 처리를 지시하며, 보안태그 판독부(210)와 개인정보 입력부(220) 및 생체정보 매칭부(230)를 포함할 수 있다.
- [59] 보안태그 판독부(210)는 개인식별카드의 보안태그(110)를 촬영한 이미지를 제공하는 촬영부(211)와 이미지로부터 암호화된 사용자의 생체정보를 복원하는 데이터 복원부(212)를 포함할 수 있으며, 데이터 복원부(212)의 데이터 복원방법은 아래의 도 6을 통해 상세히 설명하도록 한다.
- [60] 도 6은 본 발명의 일실시예에 따른 보안태그의 복원방법을 도시한 순서도다.
- [61] 먼저, 촬영부(211)를 이용하여 보안태그의 컬러코드(110)를 제공한다(S210). 이후, 컬러코드(110)에 4비트 컬러 디코딩을 수행하고(S220), 바이너리 콘볼루션 디코딩을 수행한다(S230).

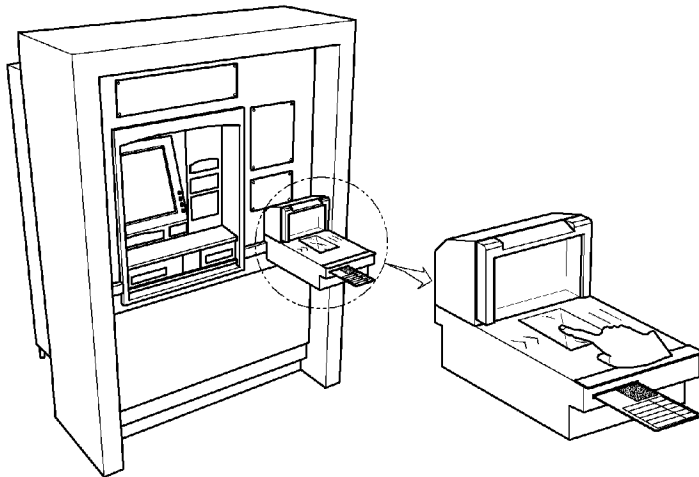
- [62] 이후, 도 4의 암호화 데이터 생성 단계에서 사용된 랜덤 키를 이용하여 2차 디코딩을 수행함으로써 컬러코드의 디지털 정보에 대한 디코딩을 완료한다(S240). 이때, 컬러코드에 고속 푸리에 변환(FFT, fast fourier transform)과 고속 역푸리에 변환(IFFT, inverse fast fourier transform)을 수행하여 저주파 노이즈를 제거할 수 있다.
- [63] 이후, 디코딩된 디지털 정보로부터 이진 랜덤코드와 컬러코드에 저장된 생체정보 이미지 데이터와 셔플 테이블의 고유 식별번호 및 조합 테이블의 고유 식별번호를 추출한다. 또한, 추출된 조합 테이블의 고유 식별번호에 해당하는 조합 테이블을 불러들이고, 상기 추출된 이진 랜덤코드를 이용하여 생체정보 이미지 데이터 조각들에 대해 1차 재배열을 수행한다(S250).
- [64] 이후, 추출된 셔플 테이블의 고유 식별번호에 해당하는 셔플 테이블을 불러들이고 셔플 테이블에 저장된 랜덤 어드레스 배열에 따라 2차 재배열을 수행하고, 생체정보 이미지 데이터를 복원한다(S260).
- [65] 다시 도 5의 설명으로 돌아가서, 개인정보 입력부(220)는 사용자의 실물 생체정보를 스캔하여 읽어들이며 이미지 스캐너와 같은 화상 정보 입력장치로 구현될 수 있다. 이때, 실물 생체정보를 스캔하는 단계와 생체정보 이미지 데이터를 복원하는 단계는 어느 하나의 단계가 먼저 수행될 수 있으며, 동시에 수행될 수도 있다.
- [66] 생체정보 매칭부(230)는 복원된 생체정보 이미지 데이터와 실물 생체정보의 매칭 여부를 판단한다. 판단결과, 복원된 생체정보와 실물 생체정보가 매칭되면 사용자의 인증요청을 수락하고 민원처리부(300)를 통해 사용자의 요구사항을 처리한다. 이때, 매칭 결과 및 사용자의 요구사항 처리 결과는 표시부(400)를 통해 실시간으로 출력된다.
- [67] 이상에서는 보안태그를 이용하는 사용자 인증장치에 대하여 설명하였으며, 사용자 인증장치는 현금 자동 입출금기, 신용카드 결제기, 기밀 서류 열람 및 출입 통제 등의 분야에 적용되는 인증장치일 수 있다.
- [68] 이상에서는 본 발명의 일실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리 범위에 속하는 것이다.

청구범위

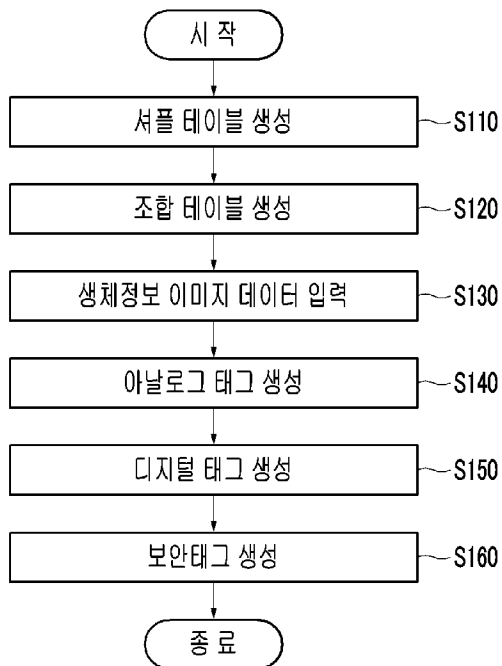
- [청구항 1] 생체 정보를 포함하는 이미지를 제공하는 단계,
상기 이미지를 $N \times M$ 개(N 및 M 은 자연수)로 조각내어 랜덤하게 배열하는 어드레스를 포함하는 셔플 테이블을 생성하는 단계,
1에서 $N \times M$ 까지의 정수를 랜덤하게 2 개씩 선택하여 이루어진 정수 쌍을 포함하는 조합 테이블을 생성하는 단계,
상기 셔플 테이블을 이용하여 상기 이미지의 조각들을 셔플링하여 셔플 이미지를 생성하고, 상기 조합 테이블 및 상기 정수 쌍에 대응되는 이진 랜덤코드의 위치 변환 정보를 이용하여 셔플 이미지의 조각들을 재배치함으로써 제1 암호화된 아날로그 태그를 생성하는 단계, 그리고
상기 이진 랜덤코드를 상기 생체정보, 상기 셔플 테이블, 그리고 상기 조합 테이블을 이용하여 이진 이미지로 재조합함으로써 제2 암호화된 디지털 태그를 생성하는 단계를 포함하는 보안태그의 생성방법.
- [청구항 2] 제1항에서,
상기 위치 변환 정보는 상기 정수 쌍이 현재 위치를 유지하라는 정보 또는 상기 정수 쌍이 서로 위치를 변경하라는 정보인 보안태그의 생성방법.
- [청구항 3] 제2항에서,
상기 디지털 태그를 생성하는 단계는,
셔플링 키(shuffling key)를 생성하는 단계,
상기 셔플링 키와 랜덤 키를 논리 연산하여 암호화 데이터를 생성하는 단계, 그리고
상기 암호화 데이터에 대하여 바이너리 콘볼루션 인코딩을 수행하여 컬러코드를 생성하는 단계를 포함하는 보안태그의 생성방법.
- [청구항 4] 제3항에서,
상기 컬러코드를 생성하는 단계는 상기 암호화 데이터의 입력 바이트와 상기 바이너리 콘볼루션에 사용되는 n 개의 입력 바이트 각각에 대하여 배타적 논리합(XOR, Exclusive OR) 연산을 통해 인접한 바이트 간에 논리 관계를 생성하는 바이너리 콘볼루션 인코딩을 수행하는 보안태그의 생성방법.
- [청구항 5] 제3항에서,
상기 디지털 태그를 생성하는 단계는 상기 컬러코드의 데이터 압축을 위해 4비트 컬러 인코딩을 수행하는 단계를 포함하는 보안태그의 생성방법.

- [청구항 6] 제1 암호화된 아날로그 태그 및 제2 암호화된 디지털 태그를 포함하는 보안태그를 획득하는 단계,
상기 제2 암호화에 대응하는 제1 디코딩을 수행하는 단계, 그리고
상기 제1 암호화에 대응하는 제2 디코딩을 수행하여 생체 정보를 포함하는 이미지를 복원하는 단계
를 포함하는 보안태그의 복원방법.
- [청구항 7] 제6항에서,
상기 제1 디코딩을 수행하는 단계는 컬러코드의 저주파 노이즈를 제거하기 위하여 푸리에변환 및 역푸리에 변환을 수행하는 단계를 포함하는 보안태그의 복원방법.
- [청구항 8] 제6항에서,
상기 제1 디코딩을 수행하는 단계는 상기 제2 암호화가 바이너리 콘볼루션 인코딩을 통해 수행된 경우, 상기 컬러코드에 바이너리 콘볼루션 디코딩을 수행하는 단계를 포함하는 보안태그의 복원방법.
- [청구항 9] 제8항에서,
상기 이미지를 복원하는 단계는 상기 제1 암호화가 상기 이미지를 $N \times M$ 개(N 및 M 은 자연수)로 조각내어 랜덤하게 배열하는 어드레스를 포함하는 셔플 테이블과 1에서 $N \times M$ 까지의 정수를 랜덤하게 2 개씩 선택하여 이루어진 정수 쌍을 포함하는 조합 테이블을 이용하여 수행된 경우, 상기 조합 테이블의 정수 쌍과 상기 셔플 테이블의 어드레스를 이용하여 상기 이미지의 조각들을 재배열하는 상기 제2 디코딩을 수행하는 단계를 포함하는 보안태그의 복원방법.

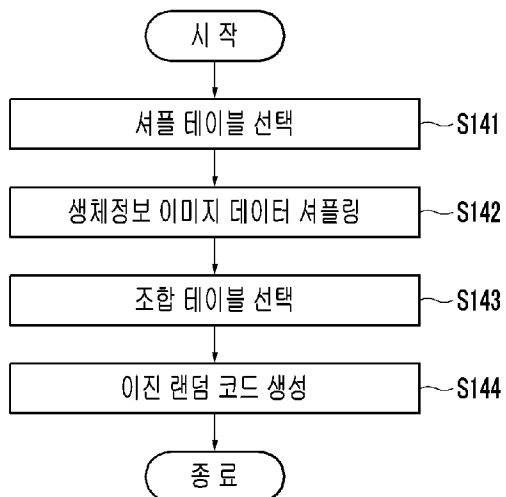
[Fig. 1]



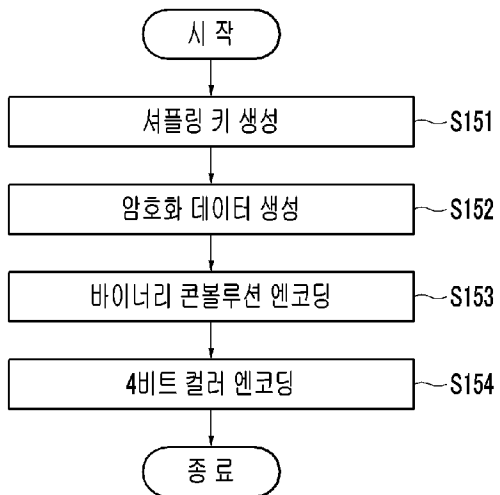
[Fig. 2]



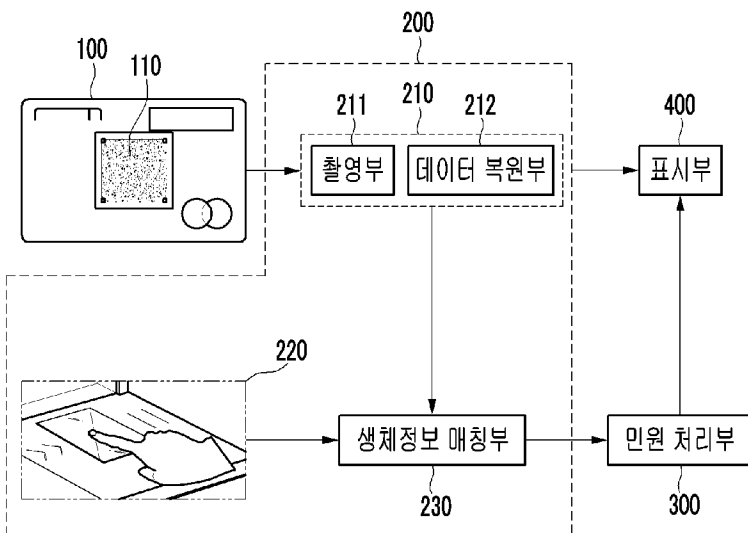
[Fig. 3]



[Fig. 4]



[Fig. 5]



[Fig. 6]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2013/001886**A. CLASSIFICATION OF SUBJECT MATTER****G06K 9/18(2006.01)i, G06K 7/10(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06K 9/18; G06F 17/10; G06F 15/00; G11C 7/00; G05B 19/00; G06F 21/20; G06K 19/067; H04L 9/32; G06T 1/00; G06K 7/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility models: IPC as above

Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: living body image, split, shuffle, encoding, combination, security, tag

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2009-0001382 A (GOLD & KEY CO.,LTD) 08 January 2009 See abstract, paragraphs <45>-<46>, <145>-<146>, claim 5 and figures 1, 8.	1-9
A	US 2007-0011464 A1 (GORELIK et al.) 11 January 2007 See abstract, paragraphs [0034]-[0044] and figures 1-2.	1-9
A	US 2010-0066493 A1 (RACHLIN) 18 March 2010 See paragraphs [0029]-[0033] and figure 5.	1-9
A	JP 2007-272776 A (SECOM CO., LTD.) 18 October 2007 See paragraphs [0025]-[0040] and figures 3-5.	1-9
A	JP 2005-209018 A (KDDI CORP.) 04 August 2005 See paragraphs [0020]-[0037] and figures 5-6.	1-9



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

13 AUGUST 2013 (13.08.2013)

Date of mailing of the international search report

13 AUGUST 2013 (13.08.2013)

Name and mailing address of the ISA/KR



Korean Intellectual Property Office
Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2013/001886

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2009-0001382 A	08/01/2009	WO 2009-005259 A2	08/01/2009
US 2007-0011464 A1	11/01/2007	US 7783893 B2	24/08/2010
US 2010-0066493 A1	18/03/2010	CA 2678210 A1	15/03/2010
		CN 101676923 A	24/03/2010
		EP 2164019 A1	17/03/2010
		EP 2166477 A1	24/03/2010
		US 8384515 B2	26/02/2013
JP 2007-272776 A	18/10/2007	JP 04884052 B2	22/02/2012
JP 2005-209018 A	04/08/2005	JP 04283126 B2	24/06/2009

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06K 9/18(2006.01)i, G06K 7/10(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06K 9/18; G06F 17/10; G06F 15/00; G11C 7/00; G05B 19/00; G06F 21/20; G06K 19/067; H04L 9/32; G06T 1/00; G06K 7/10

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 생체 이미지, 분할, 셔플, 암호화, 조합, security, tag

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2009-0001382 A (골드엔키 주식회사) 2009.01.08 요약, 문단부호 <45>-<46>, <145>-<146>, 청구항 5 및 도면 1, 8 참조.	1-9
A	US 2007-0011464 A1 (GORELIK et al.) 2007.01.11 요약, 문단부호 [0034]-[0044] 및 도면 1-2 참조.	1-9
A	US 2010-0066493 A1 (RACHLIN) 2010.03.18 문단부호 [0029]-[0033] 및 도면 5 참조.	1-9
A	JP 2007-272776 A (SECOM CO., LTD.) 2007.10.18 문단부호 [0025]-[0040] 및 도면 3-5 참조.	1-9
A	JP 2005-209018 A (KDDI CORP.) 2005.08.04 문단부호 [0020]-[0037] 및 도면 5-6 참조.	1-9

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

“A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

“T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

“X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

“L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

“Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

“O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2013년 08월 13일 (13.08.2013)

국제조사보고서 발송일

2013년 08월 13일 (13.08.2013)

ISA/KR의 명칭 및 우편주소

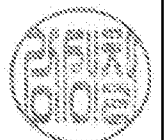
대한민국 특허청
(302-701) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)

팩스 번호 +82-42-472-7140

심사관

강성철

전화번호 +82-42-481-8405



국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2009-0001382 A	2009/01/08	WO 2009-005259 A2	2009/01/08
US 2007-0011464 A1	2007/01/11	US 7783893 B2	2010/08/24
US 2010-0066493 A1	2010/03/18	CA 2678210 A1	2010/03/15
		CN 101676923 A	2010/03/24
		EP 2164019 A1	2010/03/17
		EP 2166477 A1	2010/03/24
		US 8384515 B2	2013/02/26
JP 2007-272776 A	2007/10/18	JP 04884052 B2	2012/02/22
JP 2005-209018 A	2005/08/04	JP 04283126 B2	2009/06/24