

(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。 Int. Cl. G06K 19/073 (2006.01) G06K 19/07 (2006.01)	(45) 공고일자 (11) 등록번호 (24) 등록일자	2006년09월13일 10-0623063 2006년09월05일
--	-------------------------------------	--

(21) 출원번호 (22) 출원일자	10-2005-0037583 2005년05월04일	(65) 공개번호 (43) 공개일자
------------------------	--------------------------------	------------------------

(73) 특허권자 인하대학교 산학협력단
 인천 남구 용현동 253 인하대학교

(72) 발명자 박주성
 인천 남구 용현3동 456-610 현대빌라트 C-102

강전일
충남 공주시 옥룡동 284-1

양대현
서울 서초구 서초동 신동아아파트 3동 210호

(74) 대리인 이원희

(56) 선행기술조사문헌 JP2000165375 A JP2001266103 A JP2003337750 A * 심사관에 의하여 인용된 문헌	JP2001265658 A JP2002222402 A
--	----------------------------------

심사관 : 이승주

(54) 강제 충돌 기능을 갖는 알에프아이디 태그 및알에프아이디 시스템과 알에프아이디 태그 정보 보호 방법

요약

본 발명은 RFID 태그 정보에 태그 정보 보호를 위한 거짓 비트를 삽입하고 허가받은 리더에게만 거짓 비트의 위치를 알려 주기 위해 강제 충돌을 이용하여 RFID 태그 정보를 보호할 수 있도록 하는 강제 충돌 기능을 갖는 RFID 태그 및 RFID 시스템과 RFID 태그 정보 보호방법을 제공하는 것으로, 본 발명의 RFID 태그는 리더가 태그 정보 독취시 재기입 불가능한 메모리에 저장되어 있는 태그 정보의 보호를 위해 태그 정보에 삽입할 거짓 비트에 대한 위치값을 갖는 비트열이 저장되는 OTP(Onetime Programmable) 메모리를 구비하며, OTP 메모리에 저장되는 거짓 비트의 위치값을 바탕으로 리더로부터의 태그 정보 요구시 원래의 태그 정보에 거짓 비트를 삽입하여 전송함으로써 허가되지 않은 리더에게의 태그 정보 제공을 방지할 수 있도록 하며, 또한 소유하고 있는 태그의 정보를 보호하고자 하는 개인 사용자나 단체 등의 소비자에게 별도의 태그를 제공하여 태그 정보의 인증을 위한 키로서 이용할 수 있도록 한 것이다.

대표도

도 7

색인어

RFID 태그, OTP 메모리, 거짓 비트, 충돌

명세서

도면의 간단한 설명

도 1은 일반적인 RFID 시스템의 개략 구성도.

도 2는 본 발명에 따른 강제 충돌 기능을 갖는 RFID 태그의 구성도.

도 3은 본 발명에 따른 소비자 태그의 구성도.

도 4는 본 발명에서 태그 정보에 거짓 비트를 삽입하는 과정에 대한 흐름도.

도 5는 RFID 태그 정보 및 거짓 비트의 위치를 나타내는 비트열의 일 예도.

도 6a 내지 도 6e는 본 발명에서 태그 정보에 거짓 비트를 삽입하는 과정에 대한 설명도.

도 7은 본 발명에 따른 소비자 태그가 존재할 경우에 대한 거짓 비트 삽입과정의 흐름도.

도 8a 및 도 8b는 본 발명에 따른 소비자 태그가 존재할 경우에 대한 거짓 비트 삽입과정에 대한 설명도.

<도면의 주요 부분에 대한 부호의 설명>

100 : RFID 태그 200 : 소비자 태그

110,210,220 : 안테나 120 : ROM

130,230 : OTP 메모리

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 RFID(Radio Frequency Identification) 시스템에 관한 것으로, 특히 RFID 태그 정보에 태그 정보 보호를 위한 거짓 비트를 삽입하고 허가받은 리더에게만 거짓 비트의 위치를 알려주기 위해 강제 충돌(Forced Collision)을 이용하여 RFID 태그 정보를 보호할 수 있도록 하는 강제 충돌 기능을 갖는 RFID 태그 및 RFID 시스템과 RFID 태그 보호방법에 관한 것이다.

RFID는 바코드, 마그네틱, IC카드 등과 같은 자동인식의 한 분야로서 초단파나 장파를 이용하여 기록된 정보를 무선으로 인식하는 최첨단 방식이다.

RFID 시스템의 원리는 안테나를 통해 태그에 저장된 정보를 수신하여 이를 리더가 인식하고 분석하여 상기 태그가 장착된 물품의 고유정보를 취득할 수 있도록 하는 것으로서, 이는 주파수를 이용하기 때문에 눈, 비, 바람, 먼지, 자속 등 환경의 영향을 받지 않으며, 통과 속도가 빨라 이동 중에도 인식이 가능하다는 장점이 있다.

이러한 RFID 시스템은 슈퍼마켓, 주차관리 등에 적용되고 있으며, 예를 들어 슈퍼마켓의 경우에는 판매물품에 고유정보가 기록된 태크를 장착하면, 상기 태크를 통해 수신한 정보를 이용하여 리더와 연결된 컴퓨터에서는 현재 진열대에 남아 있는 물품수량 등을 자동으로 파악할 수 있고, 소비자가 별도로 계산을 하지 않더라도 구입해간 물품에 대한 정보도 용이하게 수집할 수 있다.

RFID 시스템은 도 1에 도시한 바와 같이, 크게 태그(10)와 리더(20)로 구성되며, 태그(10)에는 고유정보가 저장된 메모리(11) 및 통신을 위한 안테나(12)가 구비된다. 안테나(12)는 리더(20)와 태그(10) 간의 통신을 가능하게 하며, 리더(20)는 유무선으로 연결된 컴퓨터 또는 서버 또는 네트워크 인터페이스 모듈 사이의 통신을 관리한다.

상기 리더(20)는 안테나(12)를 통해 활성신호를 발산하는데 이때 안테나(12)에 의해 형성되는 RF필드에 진입하는 태그(10)가 상기 활성신호를 수신하면 자신의 정보를 리더(20)로 전송함으로써 리더(20)가 태그(10)를 인지할 수 있도록 되어 있다.

이와 같은 RFID 시스템의 최대 강점은 각각의 태그가 포함하고 있는 메모리에 제품마다 작자의 정보를 보유할 수 있다는 것이다. 기존의 바코드 체계는 각 품종마다 고유의 번호를 제공하여 제품인식에만 사용한 반면 태그는 품종이 아닌 각 제품 한개당 서로 다른 번호를 제공할 수 있고 그로 인하여 각 제품마다 고유의 정보를 포함할 수 있다는 것이다.

또한, RFID 시스템은 메모리와 안테나만으로 구성이 가능하기 때문에 기존의 바코드처럼 물품의 외장에 인쇄되는 방법이 아닌 구성물의 내부에 삽입이 가능하다.

따라서 애완동물이나 가축에게 삽입하고 최근에는 신분확인을 목적으로 인체 내 삽입도 되었다. 지금도 다양한 방면으로 연구가 계속 이루어지고 있으나, 가장 논란의 소지를 갖고 있는 것이 프라이버시 문제이다.

이 프라이버시 문제는 바코드 시스템에서는 답을 수 없던 제품에 대한 상세한 정보가 RFID 시스템에서는 태그가 모두 담을 수 있으며, 태그가 갖고 있는 능력이 정보를 보호하기엔 역부족이기 때문에 허락받지 않은 리더에 의해 태그가 갖고 있는 정보가 쉽게 노출될 가능성이 높다는 것이다.

즉, 태그는 상품에 대한 상세한 정보를 갖고 있으며 이 정보가 노출되는 것은 소비자의 프라이버시 침해를 의미하는 것이다. 소비자 측 뿐만 아니라 기업 측에서도 프라이버시 문제가 존재한다. 허가받지 않은 리더가 계속적으로 태그의 정보를 읽는다면 쉽게 기업의 상품 출고 현황 및 재고 현황이 노출될 것이다.

따라서 태그의 정보는 기업 혹은 소비자의 입장에서 보호되어야만 한다. 즉, 태그의 정보는 허가받은 리더에게는 정확하게 읽혀져야만 하며, 그렇지 않은 경우에는 항상 보호되어야만 한다. 이에 RFID 시스템 내에서 태그 정보 보호 및 개개의 프라이버시 문제에 대하여 여러 가지 해결책을 제시하고자 많은 연구가 이루어지고 있다.

그 중 블로커 태그(Blocker Tag)는 리더의 어떠한 질의에도 'yes'라는 응답을 전송하여 리더와 태그 사이의 통신을 방해하여 태그의 정보를 보호한다. 이는 두개의 안테나를 구비하여 한쪽 안테나에서는 1을, 다른쪽 안테나에서는 0을 전송하여 어떤 질의에 대해서도 'yes'라는 대답을 가능하게 한다.

그러나 블러커 태그의 모든 질의에 대해 'yes'라고 응답하는 알고리즘을 역이용한다면 정상적인 통신을 방해하며, 리더에 대한 서비스 거부 공격도 가능하다. 또한, 블로커 태그는 보호하고자 하는 태그의 주위에 같이 존재할 때만 태그의 정보를 보호한다. 그러므로 분실이나 별도 소지 등의 소비자 실수가 발생한다면 태그의 정보는 보호받지 못하게 된다.

발명이 이루고자 하는 기술적 과제

본 발명은 이러한 점을 감안한 것으로, 본 발명의 목적은 일반적 태그에 태그정보 보호를 위한 거짓 비트를 삽입하여 태그 정보를 보호할 수 있도록 한 강제 충돌 기능을 갖는 RFID 태그를 제공함에 있다.

본 발명의 다른 목적은 일반적 태그에 태그 정보 보호를 위한 거짓 비트를 삽입하고 허가받은 리더에게만 태그에 삽입된 거짓 비트에 대한 정보를 가지고 있는 특정 태크(Ownership Tag)를 통해 충돌을 이용하여 거짓 비트의 위치를 알려줌으로써 RFID 태크 정보를 보호할 수 있도록 하는 강제 충돌 기능을 갖는 RFID 시스템 및 RFID 태그 정보 보호방법을 제공하는다.

발명의 구성 및 작용

상기 본 발명의 목적을 달성하기 위한 본 발명에 따른 강제 충돌 기능을 갖는 RFID 태그는, 소정 물품에 대한 정보가 저장되어 있는 재기입 불가능한 메모리 및 리더와의 통신을 위한 안테나를 구비하는 RFID 태그에 있어서, 상기 리더가 태그 정보 독취시 상기 메모리에 저장되어 있는 태그 정보의 보호를 위해 상기 태그 정보에 삽입할 보호 정보를 제공하기 위한 정보가 저장되는 OTP(Onetime Programmable)메모리를 더 구비함을 특징으로 한다.

상기 OTP 메모리에 저장되는 정보는 상기 보호 정보의 위치값을 나타내는 비트열이며, 이 비트열은 랜덤하게 생성된 2진 비트열이며, 상기 보호 정보는 리더가 태그 정보 독취시 태그 정보를 교란시키기 위한 거짓 비트인 것을 특징으로 한다.

또한, 상기 목적을 달성하기 위한 강제 충돌 기능을 갖는 RFID 시스템은, 소정 물품에 대한 정보를 갖는 RFID 태그 및 상기 RFID 태그 정보를 독취하는 리더를 구비하는 RFID 시스템에 있어서, 허가된 리더에게 RFID 태그의 태그 정보를 인식시키기 위한 소정의 태그가 더 구비되며, 상기 RFID 태그에는 RFID 태그의 재기입 불가능한 메모리에 저장된 태그 정보의 보호를 위해 상기 태그 정보에 삽입할 보호 정보를 제공하기 위한 정보가 저장되는 OTP(Onetime Programmable) 메모리가 구비됨을 특징으로 한다.

상기 목적을 달성하기 위한 RFID 태그 정보 보호방법은, RFID 태그와 RFID 태그의 정보를 독취하는 리더를 구비하는 RFID 시스템에서 상기 RFID 태그의 정보를 보호하기 위한 방법에 있어서, 상기 RFID 태그의 소정 메모리에 태그 정보 보호를 위한 소정의 정보를 기록하는 제1 단계; 및 허락받지 않은 리더로부터의 태그 정보 요구에 따라 상기 제1 단계에서 기록된 소정의 정보를 바탕으로 RFID 태그 정보에 태그 정보의 보호를 위한 보호 정보를 삽입하여 전송하는 제2 단계;를 포함하는 것을 특징으로 한다.

또한, 본 발명의 다른 실시 예에 따른 RFID 태그 정보 보호방법은, RFID 태그 및 리더; 허가된 리더에게 상기 RFID 태그 정보를 인식시키기 위한 소정의 태그;를 구비하는 RFID 시스템에서의 태그 정보 보호 방법에 있어서, 상기 RFID 태그의 메모리 및 상기 소정 태그의 메모리에 상기 RFID 태그의 태그 정보 보호를 위한 소정의 정보를 기록하는 제1 단계; 상기 허가된 리더로부터의 RFID 태그 정보 요구에 따라 상기 제1 단계에서 RFID 태그의 메모리에 기록된 태그 정보 보호를 위한 소정의 정보에 따라 RFID 태그 정보에 태그 정보의 보호 정보를 삽입하여 전송하는 제2 단계; 및 상기 소정 태그의 메모리에 기록된 태그 정보 보호를 위한 정보에 따라 상기 보호 정보가 RFID 태그의 원래 태그 정보가 아님을 인식시키기 위한 충돌정보를 전송하는 제3 단계;를 포함하는 것을 특징으로 한다.

이하, 본 발명의 바람직한 실시 예를 첨부된 도면을 참조하여 보다 상세하게 설명한다. 단, 하기 실시 예는 본 발명을 예시하는 것일 뿐 본 발명의 내용이 하기 실시 예에 한정되는 것은 아니다.

도 2는 본 발명에 따른 강제 충돌 기능을 갖는 RFID 태그의 구성을 나타낸 것으로, RFID 태그(100)는 1개의 안테나(110), 1개의 ROM(120), 1개의 OTP(Onetime Programmable) 메모리(130) 및 3개의 포인터(140-160)로 구성된다.

상기 안테나(110)는 도시하지 않은 리더와 통신하며, ROM(120)에는 태그를 갖는 물품에 대한 정보가 저장되고, OTP 메모리(130)에는 태그 정보 보호를 위한 거짓 비트의 위치값을 나타내는 비트열이 저장된다.

상기 포인터(140-160)는 각각 데이터 포인터(140), 거짓 비트 포인터(150), 거짓 비트 위치 포인터(160)로, 각자 리더에 응답할 비트를 가리키는 역할을 한다.

데이터 포인터(140)는 ROM(120)에 저장된 태그 데이터 부분에 맨 앞쪽으로 초기화되어 있는 포인터로, 한번 수행될 때마다 한 셀씩 증가하며, 태그 데이터를 불러준다. 거짓 비트 포인터(150)는 데이터 부분에 맨 뒤쪽으로 초기화되어 있는 포인터로, 한번 수행될 때마다 한 셀씩 감소하며 진행하는데 이 포인터는 삽입될 거짓 비트 값을 가리킨다.

거짓 비트 위치 포인터(160)는 OTP 메모리(130)의 맨 앞쪽에 초기화되어 있는 포인터로, 거짓 비트가 삽입될 위치값을 포인팅하며, 수행시마다 한 셀씩 증가한다.

또한, 본 발명은 RFID 태그(100) 정보 보호를 위한 별도의 태그인 소비자 태그(Ownership Tag)(200)를 더 구비하게 되는데, 소비자 태그(200)는 상기 RFID 태그(100)의 거짓 비트의 삽입 위치를 담고 있는 랜덤하게 생성된 비트열과 같은 비트열을 갖고 있는 것으로, 소유하고 있는 태그의 정보를 보호하고자 하는 개인 사용자나 단체 등의 소비자가 자신의 태그 정

보가 읽혀지게 하고 싶을 때 키처럼 제시하는 방식으로 일단 제시된 소비자 태그(200)는 리더의 질의를 듣고 있다가 RFID 태그(100)의 거짓 비트값이 질의에 대한 응답으로 전송될 때 고의적으로 충돌을 일으킨 뒤 충돌방지 메카니즘에 의해 재 질의를 할 때는 침묵함으로써 리더에게 삽입된 거짓 비트의 위치를 알려주게 된다.

도 3은 소비자 태그(200)의 구성을 나타낸 것으로, 2개의 안테나(210),(220), 1개의 OTP 메모리(230) 및 1개의 거짓 비트 위치 추종 포인터(240)로 구성된다.

안테나(210),(220)는 충돌을 발생시키기 위해 2개의 안테나가 필요로 된 것이며, OTP(230) 메모리에는 RFID 태그(100)의 OTP 메모리(130)에 저장된 태그의 거짓 비트의 위치값과 동일한 비트열이 저장되며, 거짓 비트 위치 추종 포인터(240)는 리더의 질의를 청취하며, RFID 태그(100)의 거짓 비트의 위치를 나타내는 비트열에 맞춰 진행하도록 구성된다.

이와 같이 구성된 RFID 태그(100)의 태그 정보를 보호하기 위해서 리더는 도 4의 흐름도에 도시한 바와 같이, 모든 상품의 태그에 대한 정보를 알아내는 질의 동작을 수행한 후(S110), 이에 해당하는 정보를 도시하지 않은 데이터베이스에서 찾아 상품명과 가격 등 상품에 대한 정보를 알아내며, 이러한 과정 수행 후 리더는 RFID 태그(100)의 OTP 메모리(130)에 거짓 비트의 위치값을 나타내기 위해 완전 랜덤하게 생성한 거짓 비트열을 삽입한다(S120).

여기서, 거짓 비트의 위치값을 나타내는 비트열을 삽입하기 전에 리더는 구입한 물품의 RFID 태그(100)를 읽고 완전이진 트리가 생기는 부분을 체크하며, 비트열을 RFID 태그(100)의 OTP 메모리(130)에 삽입하기 전에 RFID 태그 데이터들이 완전한 이진트리를 구성하는 레벨(또는 깊이(Depth))을 체크하여 해당하는 부분을 0으로 만들고(이 부분은 거짓 비트가 삽입되면 안되므로 0으로 만들어줌) 그 외의 모든 비트들은 랜덤하게 생성하여 삽입하게 된다.

도 5는 이러한 과정을 거쳐 생성되는 RFID 태그의 OTP 메모리(130)의 비트열의 일 예를 나타낸 것으로, RFID 태그(100)의 앞부분은 태그 정보 즉, 태그를 갖는 물품에 대한 정보를 갖는 데이터(Original Data) 부분이고, 뒷부분은 태그 정보 보호를 위한 거짓 비트(Bogus Bits)의 삽입 위치를 나타내는 비트열이다.

이와 같이 RFID 태그(100)의 OTP 메모리(130)에 거짓 비트의 삽입 위치를 나타내는 비트열이 삽입된 후, 허락받지 않은 리더로부터의 요청시 원래의 태그 정보에 상기 거짓 비트의 위치값을 나타내는 비트열에 따라 거짓 비트를 삽입하여 응답하게 된다(S130).

상기와 같이 거짓 비트의 위치값을 나타내는 비트열이 삽입된 RFID 태그(100)가 리더의 질의에 어떻게 작동하는지 도 6을 참조로 보다 상세히 살펴본다.

우선, 좌측은 일반적인 태그의 정보가 들어가는 메모리 셀을 나타내며, 우측은 삽입된 거짓 비트의 위치를 담고 있는 메모리 셀이다.

리더는 Anti-Collision 기법 중 이진탐색트리 기법을 사용하는 것으로 가정할 경우, RFID 태그(100)의 첫 번째 비트값부터 마지막 비트까지 순차적으로 알아내기 위해서 질의를 전송할 것이다.

이 질의에 대해 RFID 태그(100)는 물품의 정보를 담고 있는 데이터에 일련의 규칙에 따라 거짓 비트를 삽입하게 된다.

이때, 거짓 비트의 삽입 위치를 나타내는 비트열 중 0은 널(Null)로 인식하여 무시하고, 1은 거짓 비트의 삽입을 알리는 것으로, 원래 태그 정보의 크기가 n이라면 n번째부터 역순으로 거짓 비트가 삽입된다.

또한, 리더의 홀수 번째 질문에는 데이터 부분을, 짝수 번째 질문에는 거짓 비트 부분을 응답하게 되는데, 이때 데이터 부분에 맨 뒤쪽으로 초기화되어 있는 포인터인 거짓 비트 포인터(150)가 가리키고 있는 비트값을 삽입할 거짓 비트 값으로 보내준다.

즉, 리더의 질문에 대하여 RFID 태그(100)는 도 6a와 같이 맨 처음 홀수 번째 질문에는 데이터 포인터(140)가 가리키고 있는 데이터 부분의 맨 처음 데이터 값인 1을 응답으로 보내준다.

그 다음 짝수 번째 질문에는 도 6b와 같이 거짓 비트 부분을 응답하기 위해 거짓 비트 위치 포인터(160)가 가리키고 있는 값을 판단하여 이 값이 1이므로 데이터 부분에 맨 뒤쪽으로 초기화되어 있는 포인터인 거짓 비트 포인터(150)가 가리키고 있는 비트값인 0을 보내준다.

그 다음 홀수 번째 질문에는 도 6c와 같이 데이터 포인터(140)가 가리키고 있는 데이터 부분의 데이터 값인 0을 응답으로 보내준다.

다음의 짝수 번째 질문에는 도 6d와 같이 거짓 비트 위치 포인터(160)가 가리키고 있는 값을 판단하여 이 값이 0이므로 널 (Null)로 인식하여 무시하고, 다음의 홀수 번째 질문에서 데이터 포인터(140)가 가리키고 있는 데이터 부분의 데이터 값인 1을 응답으로 보내주며, 다음의 짝수 번째 질문에는 도 6e와 같이 거짓 비트 위치 포인터(160)가 가리키고 있는 값이 1이므로 거짓 비트 포인터(150)가 가리키고 있는 비트값인 1을 응답으로 보내준다.

따라서 최종적으로 도 6e와 같이 '10011'의 값이 생성되며, 이는 물품의 정보를 나타내는 태그 정보의 데이터에 OTP 메모리(130)에 저장된 거짓 비트 위치값을 나타내는 비트열에 따라 ROM(120)에 저장된 원래 태그 정보에 거짓 비트가 삽입된 형태의 새로운 정보이다.

따라서 허락되지 않은 리더들은 이와 같은 태그 정보를 읽어도 원래 태그 정보를 전혀 파악할 수 없게 되므로 태그 정보를 보호할 수 있게 되는 것이다.

다음은 소비자 태그(200)가 존재할 경우에 대하여 도 7의 흐름도와 함께 살펴본다.

소비자 태그(200)가 존재할 경우, 상기 도 4와 마찬가지로 리더는 모든 상품의 태그에 대한 정보를 알아내는 질의 동작을 수행한 후(S210), 이에 해당하는 정보를 도시하지 않은 데이터베이스에서 찾아 상품명과 가격 등 상품에 대한 정보를 알아내며, 이러한 과정 수행 후 리더는 RFID 태그(100)의 OTP 메모리(130)에 거짓 비트의 위치값을 나타내기 위해 완전 랜덤하게 생성한 2진 비트열을 삽입한다.

이때, 소비자 태그(200)의 OTP 메모리(230)에도 RFID 태그(100)의 OTP 메모리(130)와 동일한 거짓 비트의 위치값을 나타내는 비트열이 저장된다(S220).

이와 같이 RFID 태그(100)의 OTP 메모리(130) 및 소비자 태그(200)의 OTP 메모리(230)에 거짓 비트의 삽입 위치를 나타내는 비트열이 기록된 후, 리더로부터의 질의에 따라 원래의 태그 정보에 거짓 비트의 위치값을 나타내는 비트열에 따라 거짓 비트를 삽입하여 응답하게 된다.

이때, 소비자 태그(200)는 RFID 태그(100)와 리더 사이의 통신을 청취하고 있으며, 질의에 따라서 거짓 비트 위치 포인터(160)가 진행하는 것과 동일하게 진행하며, 원래의 태그 정보에 거짓 비트 삽입시 안테나(210),(220)를 통해 충돌정보인 0과 1의 정보를 보내 충돌을 발생시킨다(S230).

상기와 같이 소비자 태그(200)가 존재할 경우에도 역시 상기 도 4와 마찬가지로 거짓 비트의 위치값을 나타내는 비트열을 삽입하기 전에 리더는 구입한 물품의 RFID 태그(100)를 읽고 완전이진트리가 생기는 부분을 체크하며, 비트열을 RFID 태그(100) 및 소비자 태그(200)의 OTP 메모리(130),(230)에 삽입하기 전에 완전이진트리가 되는 값이에 해당하는 부분을 0으로 만들고 그 외의 모든 비트들은 랜덤하게 생성하여 삽입하게 된다.

이는 충돌 방지 메카니즘 중 완전이진트리를 형성시키는 값이에서는 충돌이 거짓 비트의 위치를 밝힐 수 없으므로, 거짓 비트의 위치값을 나타내는 비트열을 RFID 태그(100)에 삽입하기 전에 완전이진트리가 되는 값이에 해당하는 부분을 0으로 만들어 추후 거짓 비트가 삽입된 태그 정보로부터 리더가 원래의 데이터를 알아낼 수 있도록 하기 위한 것이다.

소비자 태그(200)가 존재할 경우 리더의 질의에 대한 응답에 대하여 도 8을 참조로 보다 상세히 살펴보면, 도 8a와 같이 맨 처음 홀수 번째 질의에 대해서는 데이터 포인터(140)가 가리키는 1을 응답으로 보내준다.

그 다음 짝수 번째 질문에서는 도 8b와 같이 거짓 비트 위치 포인터(160)가 가리키고 있는 값이 1이므로 데이터 부분에 맨 뒤쪽으로 초기화되어 있는 포인터인 거짓 비트 포인터(150)가 가리키고 있는 비트값인 0을 보내주게 된다.

이때, 소비자 태그(200)의 거짓 비트 위치 추종 포인터(240)는 리더의 질의를 수신하며, RFID 태그(100)의 OTP 메모리(130)에 저장되어 있는 거짓 비트 위치값인 거짓 비트열에 맞춰 진행하도록 되어 있음에 따라 현재 거짓 비트값이 질의에 대한 응답으로 전송되므로 안테나(210),(220)를 통해 0과 1을 동시에 보내 고의적인 충돌(Collision)을 일으킨다.

따라서 리더는 RFID 시스템의 충돌방지방법인 이진탐색트리기법에 따라 충돌한 위치를 기억하면서 충돌 다음 비트를 물어보는 질의를 전송하게 된다. 이때 소비자 태그(200)는 침묵을 함으로써 그 충돌이 강제로 만든 충돌 즉, 거짓 비트를 알려주는 충돌이라고 리더에게 알릴 수 있게 된다.

리더는 거짓 비트를 알려주기 위한 강제 충돌을 인식하면 해당 비트의 위치인 충돌 위치를 기억해 내어 해당 비트값을 삭제하거나 무시하며, 이에 따라 이진탐색트리 방식에 의한 리더의 질의가 모두 끝난 뒤에 남은 값으로 원래의 데이터를 알아내게 된다.

여기서, 원래의 태그 데이터가 101010라 가정할 경우, 이 원본 태그 데이터를 이루는 비트들 사이에 1*0*1*0*1*0와 같이 거짓 비트(*)가 삽입될 수 있다.

만약, 1100110으로 앞에서부터 두 번째, 네 번째, 여섯 번째에 거짓 비트가 삽입 되었다면 소비자 태그(200) 부재시에 앞의 모든 비트열이 전송되고 소비자 태그(200)가 존재시에는 거짓 비트의 위치에서 강제 충돌이 발생된다.

충돌이 발생하였을 때 이진트리기법에 의해 리더는 재질의를 하게 되고 이 질의에 어떠한 응답도 하지 않는 것으로 소비자 태그(200)는 거짓 비트의 존재와 위치를 알려주게 되며, 질의를 하였음에도 불구하고 어떠한 응답도 오지 않을 경우, 리더는 해당 위치가 거짓 비트라고 판단한다.

이와 같이 거짓비트의 위치를 알아내어 그 해당 위치의 비트값을 무시하고 다음에 들어오는 비트들을 충돌전에 정상적으로 들어온 비트들과 이어 원본 데이터를 알아내게 되는 것이다.

상술한 바와 같이, 본 발명의 바람직한 실시 예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 또는 변형하여 실시할 수 있다.

발명의 효과

이상에서 살펴본 바와 같이, 본 발명은 무작위 추출로 생성된 일련의 비트들을 거짓 비트로서 원래의 정보를 갖고 있는 데이터 안에 삽입함으로써 노출시에도 원래의 데이터가 아닌 아무 뜻도 없을 뿐만 아니라 혼동을 주는 거짓 비트들이 섞인 데이터를 전송함으로써 공격자 또는 허가받지 않은 불법적인 리더에 의해서 태그의 데이터가 노출되었을 때에도 태그의 정보를 보호할 수 있게 된다.

또한, 일반적인 태그 외에 소비자의 인증키 역할을 하는 별도의 태그를 이용하여 태그 정보를 읽어들이는 때 충돌을 임의로 발생시켜 데이터의 보호를 위하여 삽입된 일련의 거짓 정보를 무시하게 하여 원래의 데이터를 복원할 수 있도록 함으로써 태그 정보를 보호하여 향후 실구매자 확인 및 위조에 대한 보호 등에 이용될 수 있을 것이며, 분실 시에 태그 정보는 소비자 태그와 함께 있지 않으면 항상 보호되므로 분실물에 대한 보호 및 악용에 대한 보호가 가능하게 된다.

뿐만 아니라, 소비자들의 프라이버시에 대한 불안감 또는 논란의 여지를 해소할 수 있게 되므로 소비자들의 신뢰를 확보할 수 있으며, 기업의 입장에서 다양한 용도로 활용될 수 있는 가능성이 있음에 따라 기업화 전망이 매우 밝은 이점이 있다.

(57) 청구의 범위

청구항 1.

소정 물품에 대한 정보가 저장되어 있는 재기입 불가능한 메모리 및 리더와의 통신을 위한 안테나를 구비하는 RFID 태그에 있어서,

상기 리더가 태그 정보 독취시 상기 메모리에 저장되어 있는 태그 정보의 보호를 위해 상기 태그 정보에 삽입할 보호 정보를 제공하기 위한 정보가 저장되는 OTP(Onetime Programmable)메모리를 더 구비함을 특징으로 하는 강제 충돌 기능을 갖는 RFID 태그.

청구항 2.

제 1 항에 있어서, 상기 OTP 메모리에 저장되는 정보는

상기 보호 정보의 위치값을 나타내는 비트열인 것을 특징으로 하는 강제 충돌 기능을 갖는 RFID 태그.

청구항 3.

제 2 항에 있어서, 상기 비트열은

랜덤하게 생성된 2진 비트열인 것을 특징으로 하는 강제 충돌 기능을 갖는 RFID 태그.

청구항 4.

제 1 항에 있어서, 상기 보호 정보는 리더가 태그 정보 독취시 태그 정보를 교란시키기 위한 거짓 비트인 것을 특징으로 하는 강제 충돌 기능을 갖는 RFID 태그.

청구항 5.

제 4 항에 있어서, 상기 거짓 비트의 삽입을 위해 상기 RFID 태그는

태그 정보를 구성하는 데이터 부분의 맨 앞쪽으로 초기화되어 한번 수행될 때마다 한 셀씩 증가하며 상기 태그 정보를 구성하는 데이터 값을 포인팅 하는 데이터 포인터;

상기 태그 정보를 구성하는 데이터 부분의 맨 뒤쪽으로 초기화되어 한번 수행될 때마다 한 셀씩 감소하며 상기 태그 정보에 삽입될 거짓 비트 값을 포인팅 하는 거짓 비트 포인터; 및

상기 OTP 메모리에 저장된 비트열의 맨 앞쪽에 초기화되어 한번 수행될 때마다 한 셀씩 증가하며 상기 거짓 비트가 삽입될 위치값을 포인팅 하는 거짓 비트 위치 포인터;

를 더 구비함을 특징으로 하는 강제 충돌 기능을 갖는 RFID 태그.

청구항 6.

소정 물품에 대한 정보를 갖는 RFID 태그 및 상기 RFID 태그 정보를 독취하는 리더를 구비하는 RFID 시스템에 있어서,

허가된 리더에게 RFID 태그의 태그 정보를 인식시키기 위한 소정의 태그가 더 구비됨을 특징으로 하는 강제 충돌 기능을 갖는 RFID 시스템.

청구항 7.

제 6 항에 있어서, 상기 RFID 태그에는

RFID 태그의 재기입 불가능한 메모리에 저장된 태그 정보의 보호를 위해 상기 태그 정보에 삽입할 보호 정보를 제공하기 위한 정보가 저장되는 OTP(Onetime Programmable) 메모리가 구비됨을 특징으로 하는 강제 충돌 기능을 갖는 RFID 시스템.

청구항 8.

제 7 항에 있어서, 상기 OTP 메모리에 저장되는 정보는

상기 보호 정보의 위치값을 나타내는 비트열인 것을 특징으로 하는 강제 충돌 기능을 갖는 RFID 시스템.

청구항 9.

제 7 항에 있어서, 상기 보호 정보는 리더가 태그 정보 독취시 태그 정보를 교란시키기 위한 거짓 비트인 것을 특징으로 하는 강제 충돌 기능을 갖는 RFID 시스템.

청구항 10.

제 7 항에 있어서, 상기 소정의 태그는

2개의 안테나;

상기 RFID 태그의 OTP 메모리에 저장되는 정보와 동일한 정보가 저장되는 OTP 메모리;

상기 리더의 질의를 청취하며 상기 RFID 태그의 OTP 메모리에 저장된 비트열에 맞춰 진행하도록 된 포인터;

를 구비함을 특징으로 하는 강제 충돌 기능을 갖는 RFID 시스템.

청구항 11.

RFID 태그와 RFID 태그의 정보를 독취하는 리더를 구비하는 RFID 시스템에서 상기 RFID 태그의 정보를 보호하기 위한 방법에 있어서,

상기 RFID 태그의 소정 메모리에 태그 정보 보호를 위한 소정의 정보를 기록하는 제1 단계; 및

허락받지 않은 리더로부터의 태그 정보 요구에 따라 상기 제1 단계에서 기록된 소정의 정보를 바탕으로 RFID 태그 정보에 태그 정보의 보호를 위한 보호 정보를 삽입하여 전송하는 제2 단계;

를 포함하는 것을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 12.

제 11 항에 있어서, 상기 소정 메모리는

OTP(Onetime Programmable) 메모리인 것을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 13.

제 11 항에 있어서, 상기 제1 단계의 소정의 정보는

태그 정보에 삽입할 보호 정보의 위치값을 나타내는 비트열인 것을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 14.

제 13 항에 있어서, 상기 비트열은

소비자가 소정 물품 구입시 해당 태그 정보를 읽게 되는 리더에 의해 기록되는 것을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 15.

제 11 항에 있어서, 상기 태그 정보에 삽입할 보호 정보는

허락받지 않은 리더가 태그 정보 독취시 원래의 태그 정보를 교란시키기 위한 거짓 비트인 것을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 16.

제 15 항에 있어서, 상기 거짓 비트는 상기 보호 정보의 위치값을 나타내는 비트열의 해당 값이 0이면 널(Null)로 인식하여 무시하고, 1이면 원래의 태그 정보에 해당 보호 정보가 삽입되어 형성되는 것을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 17.

제 15 항에 있어서, 상기 거짓 비트는

원래 태그 정보의 데이터 크기가 n 이면 태그 정보의 n 번째 데이터부터 역순으로 삽입되는 것을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 18.

제 17 항에 있어서, 리더의 홀수 번째 질문에는 태그 정보를 구성하는 데이터 부분을 응답하고, 짝수 번째 질문에는 보호 정보의 위치값을 나타내는 비트열에 따라 태그 정보를 구성하는 데이터의 맨 뒤쪽으로 초기화되어 있는 거짓 비트 포인터가 가리키고 있는 비트값을 삽입할 거짓 비트 값으로 응답하는 것을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 19.

제 11 항에 있어서, 상기 제1 단계 수행 전에 상기 RFID 태그 정보를 구성하는 RFID 태그 데이터에 대하여 완전한 이진트리를 구성하는 레벨을 체크하여 해당 부분을 0으로 만드는 것을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 20.

RFID 태그 및 리더; 허가된 리더에게 상기 RFID 태그 정보를 인식시키기 위한 소정의 태그;를 구비하는 RFID 시스템에서의 태그 정보 보호 방법에 있어서,

상기 RFID 태그의 메모리 및 상기 소정 태그의 메모리에 상기 RFID 태그의 태그 정보 보호를 위한 소정의 정보를 기록하는 제1 단계;

상기 허가된 리더로부터의 RFID 태그 정보 요구에 따라 상기 제1 단계에서 RFID 태그의 메모리에 기록된 태그 정보 보호를 위한 소정의 정보에 따라 RFID 태그 정보에 태그 정보의 보호 정보를 삽입하여 전송하는 제2 단계; 및

상기 소정 태그의 메모리에 기록된 태그 정보 보호를 위한 정보에 따라 상기 보호 정보가 RFID 태그의 원래 태그 정보가 아님을 인식시키기 위한 충돌정보를 전송하는 제3 단계;

를 포함하는 것을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 21.

제 20 항에 있어서, 상기 메모리는

OTP(Onetime Programmable) 메모리인 것을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 22.

제 20 항에 있어서, 상기 태그 정보 보호를 위한 소정의 정보는

태그 정보에 삽입할 보호 정보의 위치값을 나타내는 비트열인 것을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 23.

제 22 항에 있어서, 상기 비트열은

소비자가 소정 물품 구입시 태그 정보를 읽게 되는 리더에 의해 기록되는 것을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 24.

제 20 항에 있어서, 상기 보호 정보는 허락받지 않은 리더가 태그 정보 독취시 원래의 태그 정보를 교란시키기 위한 거짓 비트인 것을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 25.

제 24 항에 있어서, 상기 거짓 비트는 상기 보호 정보의 위치값을 나타내는 비트열의 해당 값이 0이면 널(Null)로 인식하여 무시하고, 1이면 원래의 태그 정보에 보호 정보가 삽입되어 형성되는 것을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 26.

제 24 항에 있어서, 상기 거짓 비트는 원래 태그 정보의 데이터 크기가 n이면 태그 정보의 n번째 데이터부터 역순으로 삽입되는 것을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 27.

제 26 항에 있어서, 리더의 홀수 번째 질문에는 태그 정보를 구성하는 데이터 부분을 응답하고, 짝수 번째 질문에는 거짓 비트의 위치값을 나타내는 비트열에 따라 태그 정보를 구성하는 데이터의 맨 뒤쪽으로 초기화되어 있는 거짓 비트 포인터가 가리키고 있는 비트값을 삽입할 거짓 비트 값으로 응답하는 것을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 28.

제 20 항에 있어서, 상기 제1 단계 수행 전에 상기 RFID 태그 정보를 구성하는 RFID 태그 데이터에 대하여 완전한 이진트리를 구성하는 레벨을 체크하여 해당 부분을 0으로 만드는 것을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 29.

제 20 항에 있어서, 상기 충돌정보는

0과 1로 구성된 정보임을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 30.

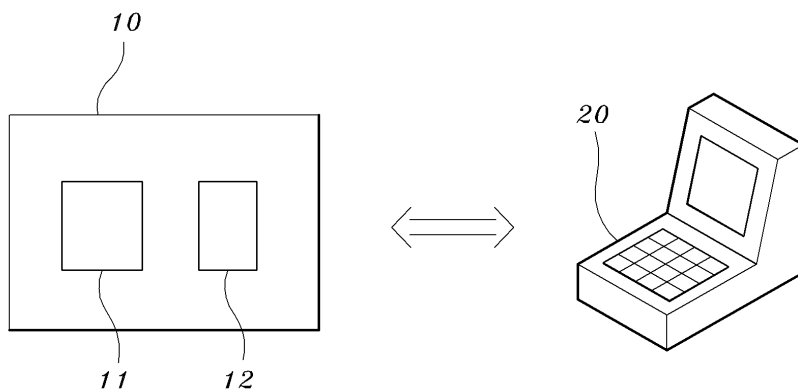
제 20 항에 있어서, 리더는 상기 충돌정보 수신 후, 충돌방지 메카니즘에 따라 재질의를 전송하고 도착한 재질의에 대하여 상기 소정의 태그가 침묵하면 해당 비트가 태그의 원래 정보가 아닌 태그 정보의 보호를 위해 삽입한 보호 정보로 인식하도록 된 것을 특징으로 하는 RFID 태그 정보 보호방법.

청구항 31.

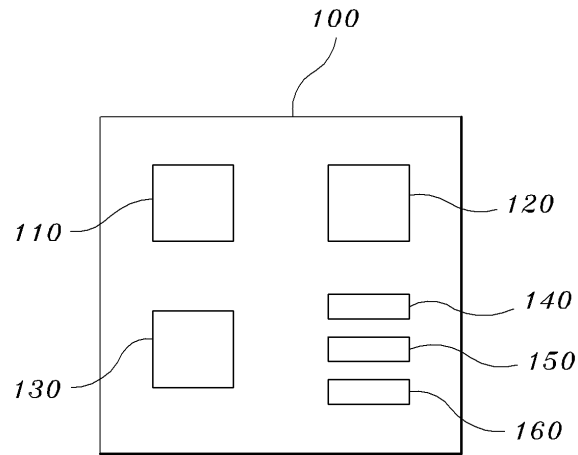
제 30 항에 있어서, 리더는 이진탐색트리를 갖고 있는 메커니즘에 따라 동작하여 상기 태그로부터 아무런 응답이 없으면 상기 소정의 태그가 존재한다고 인식하도록 된 것을 특징으로 하는 RFID 태그 정보 보호방법.

도면

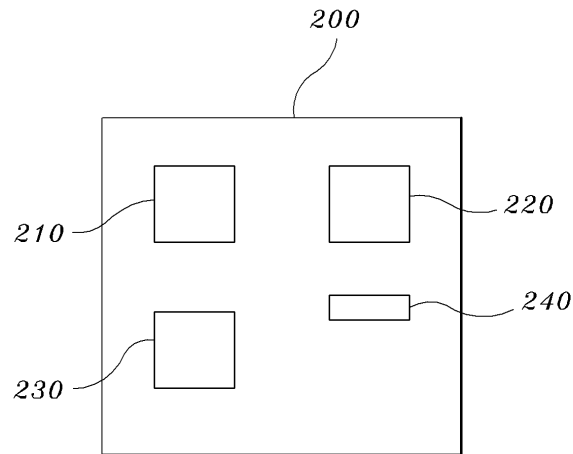
도면1



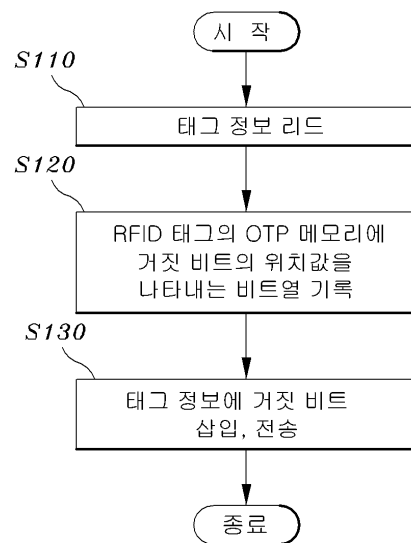
도면2



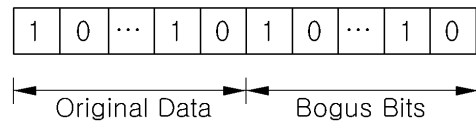
도면3



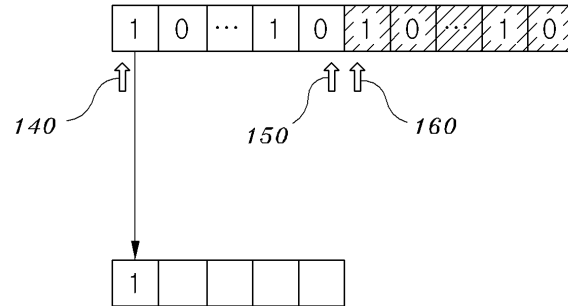
도면4



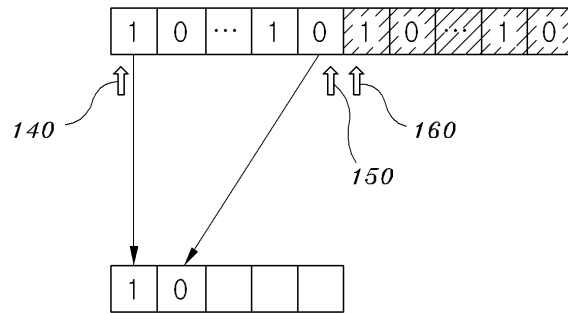
도면5



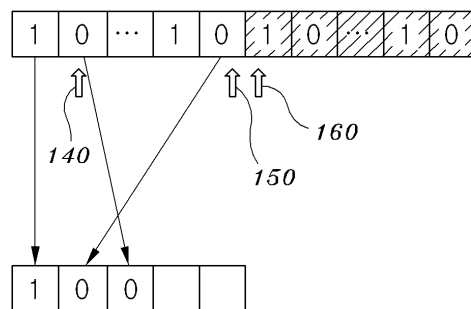
도면6a



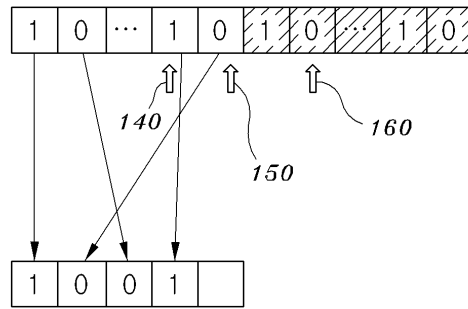
도면6b



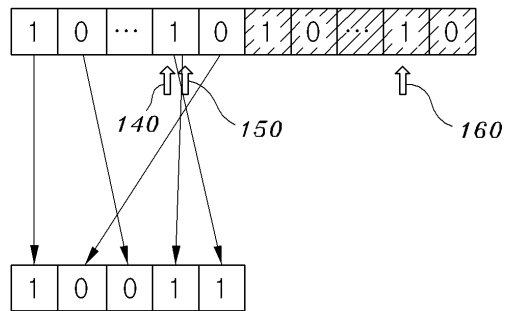
도면6c



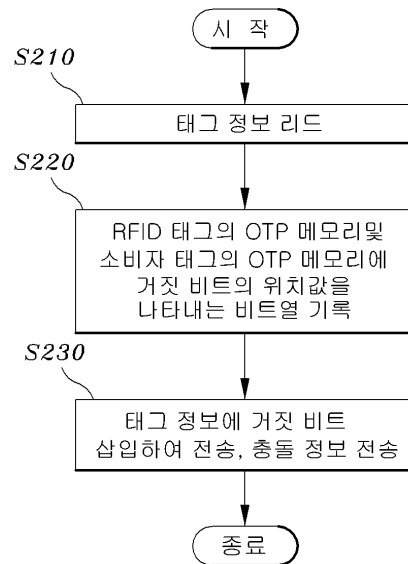
도면6d



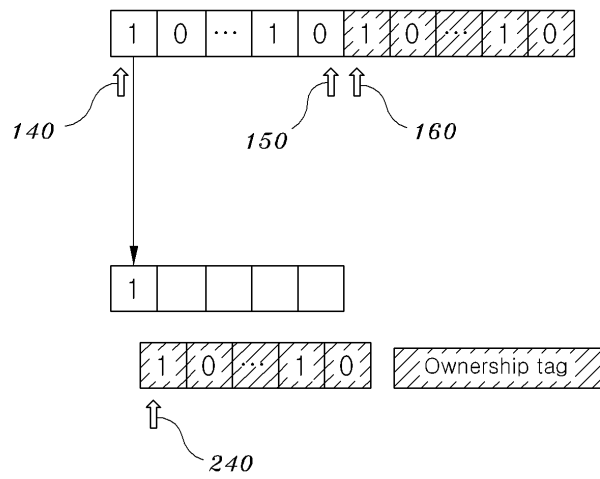
도면6e



도면7



도면8a



도면8b

