(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년04월14일
(11) 등록번호 10-0952803
(24) 등록일자 2010년04월06일

(51) Int. Cl.
G06F 7/00 (2006.01) *G06F 12/00* (2006.01)
(21) 출원번호 10-2005-7006614
(22) 출원일자 2003년10월14일
심사청구일자 2008년08월29일
(85) 번역문제출일자 2005년04월15일
(65) 공개번호 10-2005-0084855
(43) 공개일자 2005년08월29일
(86) 국제출원번호 PCT/EP2003/050718
(87) 국제공개번호 WO 2004/036411
국제공개일자 2004년04월29일
(30) 우선권주장
0213333 2002년10월16일 프랑스(FR)
(56) 선행기술조사문헌
US05630093 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
톰슨 라이센싱
프랑스 에프-92100 블로뉴-빌랑꾸르 꿰 아 르 걀로 46
(72) 발명자
디엘, 에릭
프랑스 에프-35340 리페르 라 버자르디에르
(74) 대리인
백만기, 전경석, 주성민

전체 청구항 수 : 총 6 항 심사관 : 김종권

(54) 소자의 리스트를 저장하기 위한 장치 및 이 장치에서소자를 저장하는 방법

(57) 요 약

본 발명은, 장치에 최종적으로 제공된 소정의 아이템(J)을 기억하기 위해서 아이템의 리스트를 기억하기 위한 장치(5)에 관한 것이다. 이 장치는, 제1 메모리 장치(3)를 포함하며, 상기 제1 메모리가 가득 차 있고, 새로운 아이템이 기억되어야 하는 경우에, 상기 제1 메모리에 기억된 아이템을 무작위로 선택하여, 이 선택된 아이템을 삭제하고, 상기 제공된 새로운 아이템을 기억시키도록 하는 수단들을 포함한다.

또한, 본 발명은 장치(5) 등에 아이템(J)을 기억시키기 위한 방법에 관한 것이다.

특허청구의 범위

청구항 1

자신에게 최종적으로 제공된 소정의 아이템(J)을 기억하기 위해서 아이템들의 리스트를 기억하고, N개(N은 자연수)의 아이템을 기억할 수 있는 장치(5)로서,

상기 장치에 최종적으로 제공된 M개의 아이템을 연속적으로 기억하도록 설계된 제1 메모리(2), 및

M은 상기 N 이하의 자연수로서,

N-M개의 다른 아이템을 기억할 수 있는 제2 메모리(3)

를 포함하는 것을 특징으로 하고,

상기 장치는, 상기 제2 메모리가 가득 차 있고 새로운 아이템이 상기 장치에 기억되어야 하는 경우에, 상기 제2 메모리에 기억된 아이템을 무작위로 선택하여 이 선택된 아이템을 삭제(remove)하고, 상기 장치에 제공되는 새로운 아이템을 기억시키도록 하는 수단을 포함하는 것을 특징으로 하는 장치.

청구항 2

제1항에 있어서, 상기 장치는, 최종적으로 자신에게 제공된 아이템(J)이 상기 장치에 이미 존재하고 있는지 여부를 나타내는 정보를 공급하도록 적응된 것을 특징으로 하는 장치.

청구항 3

제1항에 있어서, 상기 장치는 기억된 각 아이템의 사본을 1개만 포함하는 것을 특징으로 하는 장치.

청구항 4

제1항에 있어서, 상기 장치는, 각 아이템에 대해서, 해당 아이템이 상기 장치에 제공된 횟수를 기억하는 것을 특징으로 하는 장치.

청구항 5

제4항에 있어서, 상기 장치는, 최종적으로 자신에게 제공된 아이템이, 선정된 수를 초과하는 다수의 횟수로 상기 장치에 이미 제공되었는지 여부를 나타내는 정보를 공급하도록 적응된 것을 특징으로 하는 장치.

청구항 6

아이템(J)을 장치(5)에 기억시키는 방법으로서 - 상기 아이템은 상기 장치(5)에 의해 기억되지 않았음 -, 상기 방법은, 상기 장치(5)에서,

상기 아이템(J)을 수신하는 단계,

제1 메모리(2)가 가득 차 있지 않은 경우, 상기 수신된 아이템(J)을 상기 제1 메모리(2)에 기억시키는 단계,

상기 제1 메모리(2)가 가득 차 있는 경우에는,

i) 상기 제1 메모리에 기억된 가장 오래된 아이템을 제2 메모리(3)로 전송하는 단계,

ii) 상기 수신된 아이템(J)을 상기 제1 메모리(2)에 기억시키는 단계, 및

iii) 상기 제2 메모리(3)가 가득 차 있는 경우에는, 상기 제2 메모리에 기억된 아이템이 무작위로 선택되어 삭제되고, 이에 따라, 상기 제1 메모리에 기억된 가장 오래된 아이템이 상기 제2 메모리(3)로 전송될 수 있는 단계

를 더 포함하는 것을 특징으로 하는 방법.

청구항 7

삭제

청구항 8

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 일반적으로 보안 로그를 기억할 필요가 있는 시스템의 보안 분야에 관한 것이다. 특히, 본 발명은 아이템의 리스트를 기억하기 위한 장치 및 이러한 장치에서 아이템을 기억하기 위한 방법에 관한 것이다.

배 경 기 술

[0002] 데이터에 불법적으로 접근을 시도하거나, 데이터에 부정적 동작을 행하는 것을 막기 위해서, 시스템에서는 일반적으로, 이벤트 로그 또는 동작의 리스트가 수행될 때 "보안"이 유지되어야 한다.

[0003] 일반적인 일 예의 기록 장치에서는 기록될 소정 콘텐츠에 대해서 1개의 사본(또는 제한된 수의 사본)만을 만들도록 인증된다. 디지털 기록 장치에 있어서, 개인적 사용에 대해서는 복사를 허용하지만, 불법적인 복사의 확산은 막을 필요가 있다. 이를 보장할 수 있는 직접적인 해결법은, 이미 장치에 의해 기록되어 있는 모든 콘텐츠의 리스트 (또는 구체적으로 모든 콘텐츠의 식별자의 리스트)를 기록 장치내에 유지시키는 것을 포함한다. 기록 장치가 특정 콘텐츠를 기록하라는 명령을 수신할 때마다, 기록 장치는, 이 콘텐츠가 이미 기록되어 있는 콘텐츠의 리스트에 존재하지 않는지를 미리 체크한다. 콘텐츠 (또는 보다 구체적으로 식별자)가 이 리스트에 포함된다면, 기록 장치는 이 콘텐츠를 기록하기를 거부한다.

[0004] 상술한 예에서는, 기록될 잠재적 콘텐츠의 수가 제한되지 않는다는 문제점이 발생한다. 따라서, 시스템의 보안은, 이미 기록되어 있는 콘텐츠의 리스트가 또한 제한되지 않아야만 보장되고, 이는 소비자 전자 장치에서는 불가능하다. 이러한 타입의 장치에서, FIFO("First In Fisrt Out"의 약자) 타입의 메모리는 일반적으로 상술한 바와 같은 리스트를 기억하는데 사용된다.

[0005] 그러나, 이러한 리스트의 목적이 시스템에서 소정의 보안을 제공하기 위한 것이라면, 상술한 예에서와 같이, 콘텐츠의 불법적 복사를 방지하도록 유지되는 리스트에 대해서, 또는 신뢰할 수 있는 조직에 의해 더이상 적합하거나 합법적이라고 고려되지 않는 암호 키 또는 장치의 식별자를 포함하는 취소 리스트에 대해서, FIFO 메모리에 이러한 리스트를 기억시키는 것으로 구성되는 해결법은 충분히 적합하지 못하다. 실제로, 메모리의 크기가 n개의 아이템을 기억할 수 있다면, 침해자(pirate)는, 기억된 제1 아이템이 리스트로부터 삭제되었다고 확신되도록, 리스트를 기억하는 장치에 n+1개의 아이템을 제공하기만 하면 되며, 이는 시스템의 보안을 명백히 손상시키는 것이다.

발명의 상세한 설명

[0006] 본 발명은 상술한 문제점들을 해결하는 것을 목적으로 한다.

[0007] 본 발명은, 장치에 최종적으로 제공된 소정의 아이템을 기억하기 위해서 아이템의 리스트를 기억하는 장치에 관한 것이다. 이 장치는, 제1 메모리를 포함하고, 또한, 제1 메모리가 가득 차 있고, 새로운 아이템이 기억되어야 하는 경우에, 제1 메모리에 기억된 아이템을 무작위로 선택하여, 이 선택된 아이템을 삭제하고, 제공된 새로운 아이템을 기억시키도록 하는 수단들을 더 포함한다.

[0008] 본 발명의 특정 특성에 따르면, 장치는 자연수인 N개의 아이템을 기억할 수 있고, 또한, 장치에 최종적으로 제공된 M개이 아이템을 연속적으로 기억하도록 설계된 제2 메모리를 더 포함하고, M은 N 이하의 자연수이고, 제1 메모리는 N-M개의 다른 아이템을 기억하게 된다.

[0009] 본 발명에 따른 장치에 의해서, 기억될 아이템이 N개 이상 장치에 제공되더라도, 결국 어느 아이템(들)이 장치에서 더이상 발견되지 않는지를 알 수 있는 수단이 없다.

[0010] 본 발명의 또 다른 특성에 따르면, 장치는 또한, 장치에 제공된 아이템이 상기 장치에 이미 존재하고 있는지 여부를 나타내는 정보를 공급한다.

[0011] 본 발명의 또 다른 특성에 따르면, 장치는 기억된 각 아이템의 사본을 1개만 포함한다.

[0012] 본 발명의 특정 양상에 따르면, 장치는 또한, 각 아이템에 대해서, 이 아이템이 장치에 제공된 횟수를

기억한다.

[0013] 본 발명의 또 다른 양상에 따르면, 장치는, 최종적으로 장치에 제공된 아이템이, 선정된 수를 초과하는 다수의 횟수 동안 상기 장치에 이미 제공되었는지 여부를 나타내는 정보를 공급하도록 되어 있다.

[0014] 본 발명은 또한, 상술한 바와 같은 장치에 아이템을 기억시키는 방법에 관한 것이다. 이 방법은, (a) 장치에 제공되는 아이템 수신하는 단계; 및 (b) 이 아이템이 장치에 이미 제공되었는지 여부를 증명하는 단계를 포함하고, 이 방법에서는,

[0015] - 상기 증명이 긍정이라면, 아이템을 최종 기억된 아이템으로서 지정하고,

[0016] - 상기 증명이 부정이라면, 아이템을 상기 장치에 기억시킨다.

[0017] 일 특정 실시예에 따르면, 단계 (b)에서 증명의 결과가 부정인 경우에,

[0018] - 제2 메모리가 가득 차 있지 않은 경우, 수신된 아이템은 제2 메모리에 기억되고,

[0019] - 제2 메모리가 가득 차 있는 경우에는,

[0020] ⅰ) 제2 메모리에 기억된 가장 오래된 아이템은 제1 메모리로 전송되고,

[0021] ⅱ) 수신된 아이템은 제2 메모리에 기억되고,

[0022] ⅲ) 제1 메모리가 가득 차 있는 경우에는, 제1 메모리에 기억된 아이템이 무작위로 선택되어, 삭제되고, 이에 따라, 제2 메모리에 기억된 가장 오래된 아이템이 제1 메모리로 전송될 수 있다.

실 시 예

[0024] 본 발명의 기억 장치는, 최대 N개의 아이템, 예를 들어, 기억될 콘텐츠의 식별자를 포함하도록 설계된다. 도 1에서 참조 번호 5로 나타낸 이 장치는 특히 디지털 기록 장치에 집적된다.

[0025] 장치(5)는 2개의 메모리 A 및 B를 포함한다. 참조 번호 2인 메모리 A는 최대 M개의 아이템을 포함하고, 참조 번호 3인 메모리 B는 최대 P개의 아이템을 포함하며, 여기에서 N=M+P이고, N, M, 및 P는 자연수이다.

[0026] 메모리 A는 항상 장치에 기억되어 있는 최종 M개의 아이템을 포함한다. 메모리 B는, 최종 M개의 아이템 이전에 기억되어 있는 아이템들을 포함한다.

[0027] 새로운 아이템 J가 장치에 제공될 때, 예를 들어, 기억 장치가 새로운 콘텐츠를 기록하라는 명령을 수신할 때, (아이템 J에 상응하는) 콘텐츠 식별자가 기억 장치에 제공되어, 장치(5)내에 기억된 리스트에 이 콘텐츠 식별자가 이미 포함되어 있는지 여부를 입증한다.

[0028] 아이템 J가 이미 메모리 A에 존재한다면, 다음으로 아이템 J는 기억된 최종 아이템으로서 메모리 A에 표시된다. 아이템 J가 이미 메모리 B에 존재한다면, 이 아이템 J는 메모리 A로 이동되어, 기억된 최종 아이템의 위치에 제공된다. 두가지 경우에 모두, 장치(5)는 아이템 J가 존재한다는 정보를 반환한다.

[0029] 아이템 J가 메모리 A 또는 B에 존재하지 않는다면, 다음으로 아이템 J는 메모리 A에 기억된다. 메모리 A가 M개의 아이템을 이미 포함한다면, 다음에는 메모리 A에 기억된 가장 오래된 아이템이 메모리 B로 전송되어 메모리 B에 기록된다. 이 아이템이 메모리 A로부터 삭제됨과 동시에 아이템 J를 위한 룸(room)이 생성된다. 메모리 B도 또한 가득 차 있다면, 즉, 메모리 B가 이미 P개의 아이템을 포함하고 있다면, 다음으로 메모리 B에 이미 기억되어 있는 아이템은 삭제되도록 무작위로 선택되어, 메모리 A의 가장 오래된 아이템으로 교체된다. 그 다음, 장치(5)는, 아이템 J가 존재하지 않는지, 그러나 현재 기억되어 있는지에 따라서 이 정보를 반환한다.

[0030] 도 1을 보다 구체적으로 참조하면, 기억 장치(5)는 제어 장치(1) 및 2개의 메모리 A 및 B를 포함하며, 이들 메모리는 각각 참조 번호 2 및 3으로 나타낸다.

[0031] 제어 장치(1)는 3개의 입력(10, 13, 및 15) 및 3개의 출력(11, 12, 및 14)을 포함한다. 입력(10)은 기억할 아이템 J를 수신하여, 제어 장치의 출력(12)으로 보낸다.

[0032] 출력(11)은 아이템 J가 기억 장치(5)에 이미 기억되어 있는지를 나타내는 불 연산 신호(boolean signal)이다. 아이템 J가 이미 기억되어 있다면, 출력(11)에서의 신호는 "1"("참")이고, 아이템 J가 기억되어 있지 않다면, 신호는 "0"("거짓")이다. 입력(13 및 15) 및 출력(14) 또한 불 연산 신호이며, 다음에서 설명된다.

[0033] 메모리 A는 2개의 입력(20 및 21) 및 2개의 출력(22 및 23)을 포함한다. 입력(20)은 제어 장치의 출력(12)을

수신하여, 기억되거나, 메모리 A에서의 존재가 결정되어야만 하는 아이템 J를 보낸다. 제어 장치(1)의 출력(14)에 접속되어 있는 입력(21)은, 그 값이 "1"(참)일 때, 입력(20)에서 수신된 아이템 J가 메모리 A에 기억되어야만 한다는 것을 나타내는 불 연산 신호이다.

[0034] 메모리 A의 출력(22)은 또한 불 연산 신호이고, 이 신호는 그 값이 "1"(참)일 때, 입력(20)에 제공된 아이템 J가 이미 메모리 A에 존재한다는 것을 나타내는 것이다. 이 출력(22)은 제어 장치(1)의 입력(15)에 연결되어 있다.

[0035] 메모리 A의 출력(23)은, 메모리 A가 가득 차 있으며, 입력(20)에 제공된 새로운 아이템이 기억되어야만 하는 경우에만 사용된다. 이 경우에, 출력(23)은 메모리 A에 기억된 가장 오래된 아이템을 공급한다. 그렇지 않으면, 출력(23)은 어떠한 신호도 공급하지 않는다.

[0036] 메모리 B에 대해서, 메모리 B는 2개의 입력(30 및 32)과 하나의 출력(31)을 포함한다. 입력(30)은 제어 장치(1)의 출력(12)에 연결되어, 메모리 B에 존재하는지가 입증되어야만 하는 아이템 J를 수신한다. 출력(31)은, 입력(30)에서 수신된 아이템 J가 메모리 B에 존재할 때, 값 "1"("참")을 갖는 불 연산 신호이고, 이 출력(31)은 제어 장치(1)의 입력(13)에 연결된다.

[0037] 메모리 B의 입력(32)에 대해서, 이 입력(32)은, 메모리 A가 가득차 있을 때, 메모리 A로부터 나온 기억할 아이템을 수신한다. 입력(32)은 이를 위해서 메모리 A의 출력(23)과 연결된다.

[0038] 어셈블리는 다음 방식으로 동작한다. 제어 장치(1)가 입력(10)에서 아이템 J를 수신하면, 제어 장치(1)는 이 아이템 J를 그 출력(12)에 공급한다. 이 아이템 J가 메모리 A에 있다면, 신호 "1"("참")이 제어 장치(1)의 입력(15)에 수신된다. 아이템 J가 메모리 B에 있다면, 신호 "1"("참")이 제어 장치(1)의 입력(13)에 수신된다.

[0039] 제어 장치의 입력(13 및 15)에서 수신된 2개의 불 연산 신호가 값 "0"(즉, "거짓")을 갖는다면, 이는 입력(10)에서 수신된 아이템 J가 메모리 A 또는 메모리 B에 존재하지 않는다는 것을 의미한다. 이 경우에, 제어 장치(1)는 "0" 신호("거짓")를 출력(11)에 공급하고, "1" 신호를 출력(14)에 공급하며, 이는 아이템 J가 메모리 A에 기록되어야만 한다는 것을 의미한다.

[0040] 입력(15)에서 수신된 불 연산 신호가, 아이템 J가 이미 메모리 A에 존재하고 있다는 것을 의미하는 값 "1"("참")을 갖는다면, 제어 장치(1)는 "1" 신호를 출력(11)에 공급하며, "0" 신호를 출력(14)에 공급한다.

[0041] 입력(13)에서 수신된 불 연산 신호가, 아이템 J가 이미 메모리 B에 존재하고 있다는 것을 의미하는 값 "1"("참")을 갖는다면, 제어 장치(1)는 "1" 신호를 출력(11)에 공급하며, "1" 신호를 출력(14)에 공급한다.

[0042] 메모리 A가 자신의 입력(20)에서 아이템 J를 수신하는 경우, 메모리 A는 먼저 메모리 A가 이 아이템을 갖는지를 증명한다. 아이템 J가 이미 메모리 A에 존재한다면, 출력(22)에서의 신호는 값이 "1"("참")이 된다. 그 다음, 아이템 J가 메모리 A에 의해 최종적으로 기억된 아이템으로 지정된다. 예를 들어, 메모리 A가 스택 구조를 갖는다면, 아이템 J는 스택의 최상부에 위치하고, 그렇지 않으면, 메모리에 저장된 아이템의 인덱스 표가 갱신된다.

[0043] 그렇지 않으면(J가 메모리 A에 존재하지 않으면), 출력(22)은 값 "0"("거짓")을 취한다.

[0044] 메모리 A의 입력(21)에서 수신된 신호가, 입력(20)에서 제공되는 아이템 J가 메모리 A에 기억되어야만 한다는 것을 의미하는, "참"(값 "1")이면, 2개의 가능성이 존재한다. 하나의 가능성은, 메모리 A가 M 보다 적은 아이템을 포함하고, 최종적으로 기억된 아이템이 되는 새로운 아이템 J를 기억하는 것이다. 나머지 다른 가능성은, 메모리 A가 이미 M개의 아이템을 포함하고 있다는 것이다. 후자의 경우에, 메모리 A는 가장 오래된 아이템을 그 출력(23)에 배치하고, 가장 최근 아이템으로서 새로운 아이템 J를 기억하기 위해서 이 아이템을 메모리 A로부터 삭제한다.

[0045] 메모리 B는 메모리 A와 다르게 동작한다. 아이템 J가 메모리 B의 입력(30)에서 수신될 때, 메모리 B는 자신이 이 아이템 J를 이미 포함하고 있는지 여부를 체크한다. 이 체크 결과가 참이면, 그 다음, 출력(31)은 값 "1"을 취하고, 그렇지 않으면(J가 메모리 B에 존재하지 않으면), 출력(31)은 값 "0"을 취한다.

[0046] 메모리 A로부터 나온 아이템 J가 메모리 B의 입력(32)에 수신된다면, 2개의 가능성이 존재한다. 하나의 가능성은 신호(31)가 "참"(값 "1")이고, 다른 가능성은 신호(31)가 "거짓"(값 "0")이다.

[0047] 신호(31)가 "참"이면, 메모리 B의 입력(32)에서 수신된 새로운 아이템이, (메모리 A로 전달되는) 입력(30)에 그

값이 존재하는 아이템을 대체한다.

[0048] 신호(31)가 "거짓"이어도 2개의 가능성이 존재한다. 이 중 하나는, 메모리 B가 P보다 적은 아이템을 포함하고, 새로운 아이템 J를 기억하는 것이고, 다른 하나는, 메모리 B가 이미 P개의 아이템을 포함하는 것으로서, 즉, 메모리 B가 가득차 있는 경우이다. 후자의 경우에, 메모리 B는 메모리 B에 이미 기억되어 있는 아이템을 무작위로 선택하여, 이를 제거하고, 무작위로 선택된 아이템을 대신해서 입력(32)에서 수신된 새로운 아이템을 기억한다.

[0049] 따라서, 메모리 B는 무작위적인 방식으로 비워진다. 따라서, 기억 장치(5)의 아이템을 삭제하기를 원하는 침해자는 단순한 FIFO 메모리 방식의 경우보다 보다 많은 시도를 해야만 한다. 실제로, 메모리의 전체 사이즈가 N 아이템이라면, 침해자는, 메모리로부터 아이템을 삭제하기 위해서 평균 N 보다 더 많이 시도해야 한다.

[0050] 도 1에서 분리되어 나타낸 메모리 A 및 B는 실제로 물리적으로 동일한 메모리의 2개의 하부어셈블리가 될 수 있다.

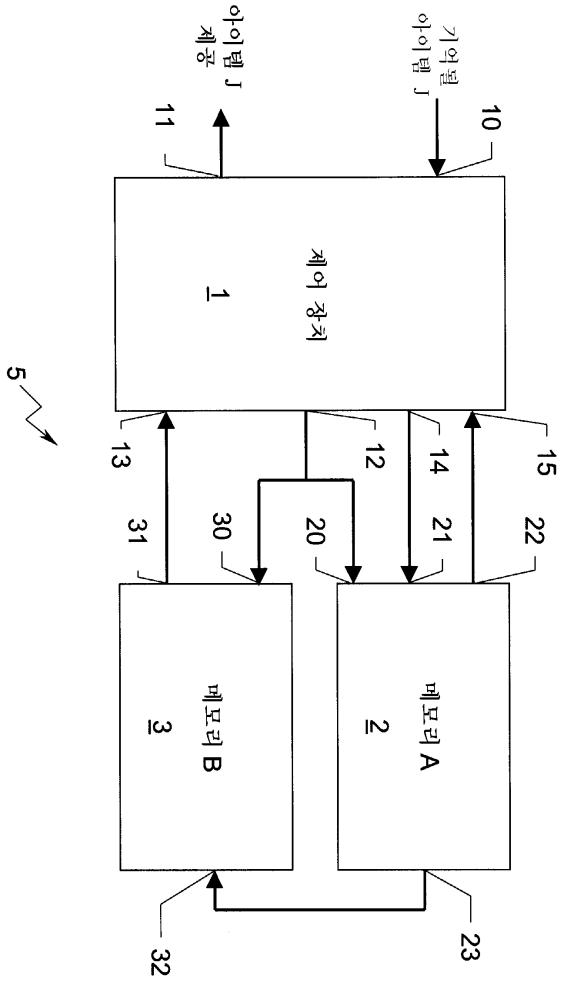
[0051] 본 발명은 상술한 실시예로서 한정되는 것은 아니다. 변형예로서, 기억 장치(5)는 실제로 널(null) 사이즈의 메모리 A를 포함할 수 있다. 다른 변형으로서, 사용자는 주어진 횟수만큼 각 아이템을 기억 장치에 제공할 수 있다. 예를 들어, 이 장치가 기록 장치에 집적되고, 이 기록 장치가 각 콘텐츠에 대해 x개의 사본을 만들도록 인증된다면, 메모리는, 애플리케이션에 의해 이미 기록된 각 콘텐츠 식별자와 함께, 기록을 위해 장치에 제공된 콘텐츠를 y번 만큼 저장할 것이다. 주어진 콘텐츠 제공 횟수 y가 넘버 x가 되면, 이 콘텐츠를 더이상 기록할 수 없으며, 기억 장치(5)는 상응하는 정보의 아이템을 기록 장치로 반환할 것이다.

도면의 간단한 설명

[0023] 도 1은 본 발명에 따른 기억 장치를 개략적으로 도시하는 도면으로서, 본 발명의 다른 특성들 및 장점들은, 본 발명의 비제한적인 특정 실시예의 설명을 통해서 나타나며, 첨부된 도 1을 통해서 명확해질 것이다.

도면

도면1


5
제어 장치
1
메모리 A
2
메모리 B
3
기억될 아이템 J
10
아이템 J 제공
11
12
13
14
15
20
21
22
23
30
31
32